



Configuring Citrix XenDesktop 7.6 and NetScaler Gateway 10.5 with PIV Smart Card Authentication

This guide is intended for those who are deploying smart cards with Citrix products. It provides step-by-step instructions for deployment in United States federal environments.

Carel Grove
Citrix Authentication Platforms Group

Table of Contents

Introduction	1
How this guide is organized	1
Future editions: What is not in this first edition	1
Test environment	2
Objectives	2
Constraints	3
Assumptions	3
Section 1 Configuration Steps (on every machine in the test environment)	4
Your Organization's Root Certification Authority	5
Test environment assumptions	5
Prerequisites	5
Configuration Steps	5
Your Organization's Issuing Certificate Authority	6
Test environment assumptions	6
Prerequisites	6
Configuration Steps	6
Domain Controller	14
Test environment assumptions	14
Prerequisites	14
Configuration Steps	14
User Account Settings – Map AD user account to the PIV authentication certificate	18
PKI certificate configuration	24
Virtual Delivery Agent (VDA)	29
Test environment assumptions	29
Prerequisites	29
Configuration Steps	29
Delivery Controller	38
Test environment assumptions	38
Prerequisites	38
Configuration Steps	39
StoreFront	65
Test environment assumptions	65

Prerequisites	65
Configuration Steps	66
Configure StoreFront	69
NetScaler Gateway	81
Test Environment assumptions	81
Configuration Steps	82
Hardware security module (HSM) configuration and FIPS key generation	86
Certificate configuration	90
LDAP server configuration	107
NetScaler Gateway virtual server configuration for fed-nsg	111
NetScaler Gateway virtual server configuration for fed-callback	152
Windows 7 (64 bit) Domain-Joined External Endpoint	161
Test environment assumptions	161
Prerequisites	161
Configuration Steps	161
Section 2 Smart Card Single Sign-on	173
Introduction	174
PIN Prompt Origin	175
No reduction (four PIN prompts)	176
Smart card Single Sign-on state A	177
Resultant smart card Single Sign-On behavior A	177
First reduction (three PIN prompts)	178
Smart card Single Sign-on state B (three PIN prompts)	182
Resultant smart card Single Sign-on behavior B	182
Second reduction (two PIN prompts)	183
Smart card Single Sign-on state C (two PIN prompts)	186
Resultant smart card Single Sign-on behavior C	186
Third reduction (one PIN prompt)	187
Smart card Single Sign-on state D (one PIN prompt)	203
Resultant smart card Single Sign-on behavior D	203
Appendices	204
Appendix A: NIST PIV Test Card Certificates, Keys and Chain of Trust	205
Appendix B: Obtaining CA Certificates from Root and Issuing Certificate Authorities	209

Appendix C: Manually validate the CA Chain of Trust From a Leaf Certificate to its Corresponding Root Certificate.....	210
Appendix D: Publishing Certificates to Active Directory Containers	213
Appendix E: Install ActivClient 7.0.2 on Windows 7 x64.....	214
Appendix F: How NetScaler Gateway Certificate and LDAP Authentication Policies Map to an Active Directory User Account.....	224

Introduction

This guide describes how to configure a “test environment” from beginning to end.

How this guide is organized

The test environment consists of the essential components that constitute a typical Citrix deployment (XenDesktop, Delivery Controller, StoreFront, and virtual desktops accessed via NetScaler Gateway).

Each Citrix component is deployed on a dedicated machine. Supporting infrastructure (such as the domain controller and certificate authorities) is also on dedicated machines.

The guide describes how to configure each machine, step by step, in chronological order, starting with the root certificate authority and ending with the endpoint. This way, when working on any given configuration step, the reader is assured that all tasks that predicate each configuration step have been completed.

There are a few exceptions to this where “jumps” are necessary. Those are clearly indicated and cross-referenced.

Additionally, many notes are included to provide contextual background, and there are also appendices that provide additional in-depth insight.

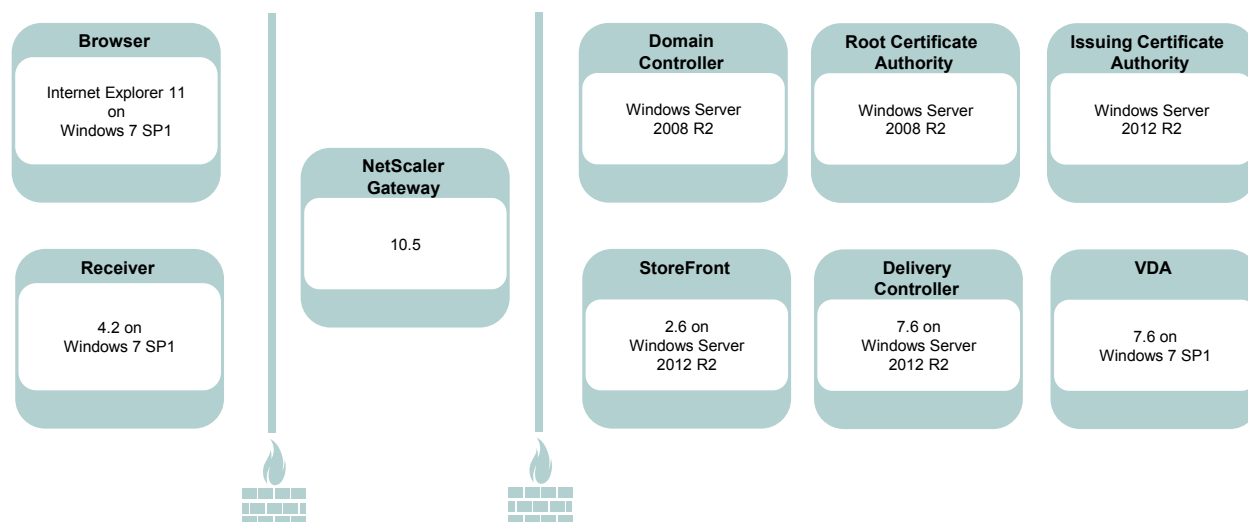
Future editions: What is not in this first edition

Topics that are not included in the first edition of the guide:

- Multi-domain and multi-forest Active Directory environments
- Non UPN-based smart card certificate to Active Directory account mapping (such as Alternate Security Identity)
- XenApp coverage
- Double-hop from the Virtual Delivery Agent to XenApp
- Additional smart card middleware (only ActivClient is covered in this edition)
- Additional endpoint coverage (such as Linux, thin clients, Windows 8.1/10, Mac OS X, iOS, Android, nondomain-joined Windows, etc.)
- Information on nonauthentication operations with smart cards (such as S/MIME)
- PKCS#11 configuration (to use smart cards with browsers such as Firefox)
- Notes on how CAC and SIPR diverge from PIV, where appropriate

Test environment

The test environment can be represented as follows:



Objectives

A guide dispensing smart card configuration advice should be:

- Self-contained: Detailed configuration steps for every product – hence step-by-step instructions for installing and configuring products and areas that are not specifically related to smart card authentication, such as installing and configuring the Delivery Controller).
- Explicitly tested: The documentation itself must be tested.
- Fool-proof: Cautions against obvious mistakes.

It was determined that both military and civilian domains should not be covered in a single document; therefore, CAC cards and SIPR tokens are not discussed.

In order to achieve the above objectives, we have to pin down a specific environment. Because there are so many possible variations in a federal environment configuration, a “model” environment could be tricky to pin down. For example, there could be dozens of different types of endpoints alone.

The priority for the first edition was not to cover as many topics or platforms as possible but to ensure that the topics that are covered—the essential components of a Citrix deployment—are covered in detail and are technically accurate. The topics were researched, and the environment was configured, tested, verified, and finally, documented. When blocking issues were discovered, workarounds were also researched, tested, and documented.

Constraints

Some components can be deployed in different ways (or using different methods), depending on the scale of the deployment. For example, the Delivery Controller could use a stand-alone dedicated database server in the case of a large deployment. In a small deployment, SQL Server Express can be installed on the Delivery Controller as part of the Delivery Controller installation to perform the same function.

In the test environment, small-scale methods are used. This way, it is complete and self-contained without requiring vast preparation sections.

Some notable examples: installing Receiver manually, not using Machine Creation Services (MCS) to provision Virtual Delivery Agents (VDA), not configuring High Availability (HA) on the NetScaler Gateway, and so on.

Assumptions

- The NIST PIV Test Card #1 is the smart card used throughout.
- Every Windows machine has a server certificate in its personal certificate store, and the machine has access to the associated private key.
- Active Directory Group Policy settings are configured in the default domain policy. The default domain policy is linked at the domain level.

Section 1 Configuration Steps (on every machine in the test environment)

Your Organization's Root Certification Authority

Test environment assumptions

- Operating system is Windows Server 2008 R2

Prerequisites

- Active Directory Certificate Services is installed and configured

Configuration Steps

Export root CA certificate to file

To see how this step fits in the overall PKI Configuration process, see the diagram in [Appendix D: Publishing Certificates to Active Directory Containers](#).

- Open up an instance of the command prompt as an administrator and enter:

```
certutil -ca.cert <filename.cer>
```

For example:

```
certutil -ca.cert Root_CA_F2-DC-CA.cer
```

This should result in the output as follows:

```
C:\Users\Administrator>certutil -ca.cert Root_CA_F2-DC-CA.cer
CA cert[0]: 3 -- Valid
CA cert[0]:
-----BEGIN CERTIFICATE-----
MIIDUTCAsj2gAwIBAgIQQAkxYZSHBrZFyfsfZQdvETANBgkqhkiG9w0BAQ0FADA9
MRQwEgYKCZImiZPyLGBGRYEV3R4czESMBAGCgmsJomT8ixkARkWAmyMREwDwYD
UQQDEwhGMiIEQy1DQTaeFw0xMzA4MDgxMzQyNTNaFw0xODA4MDgxMzUyNTJaMD0x
FDASBgoJkiaJk/IsZAEZFgRjdHhZMRIwEAYKCZImiZPyLGBGRYEV3R4czESMBAGCgmsJomT8ixkARkWAmyMREwDwYD
UQQDEwhGMiIEQy1DQTaeFw0xMzA4MDgxMzQyNTNaFw0xODA4MDgxMzUyNTJaMD0x
BAMTCEYyLURDLUNBMTI1BIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAn8cJ
LcNgYZj1SDNCvIkPAoaxrv67TITyQLhooH1+DcN5kRS4brGXOSfNfT0kwdvZmdd
Pyn0cNLDFGS1EI2wQiZwfgFW6w902mSUORk6cBPukZ7tI/6kHrwPQXpBm8Uf/0J0
8HhZndiBSB3RP/a6WzYyBHRGhzHb5JPYlrkEppk0U1XkGp0lQ8Ia6Wgekyl+IOPK
GXAg3+D4Egi2Y0zeZdItb+Jhsme60Dxh0JafvUYo3CGipoBvrf6eX9CrEv00gauJ
k2ix15fq/K8xrF2YHBYEYJfQE6tqMFbPuS6PYANDiyizU3loBxktwaxSI9fhg70b
Cchz7XIyeU/DfD2XmQIDAQABo1EwTzALBgNVHQ8EBAMCAYYwDwYDUVR0TAQH/BAUw
AwEB/zAdBgNVHQ4EFgQUkbFLaxUgDQt5y7gt2d04dfBTiQkwEAYJKwYBBAGCNxUB
BAMCAQAwDQYJKoZIhvcNAQENBQADggEBABy6lucBoLDdQgHNOQ6dZvW02N1RTQf9
CD20Uj9xSBDWdJ6epL0H1J4T2M1tBIhSRXoHtn64d1WzAH6m6ibOTmrjyenLvL2d
GnI+af8KEffupFh6KQ69e8r/SJUy4/5sw6U2oUgIkn0zDKPDv2rxln7Po3Fa9pCf
qbS32ejldEaHje/f7o14CR/zBcFkU2IPaT+pkjl1JvL0ruD084mNjlvRlNyn6vC
FOfbUF4Cgt1+3/2hcBDwdXhLgSqUtJentH9L3/Kqd2ezNfPLAR0gd90BI9UN+Dv/
4+zmfpKLPtTBsVOSJB742ytd5WYY7LazhGj4gdAH6UDHaa0x7Uk6bes=
-----END CERTIFICATE-----

CertUtil: -ca.cert command completed successfully.
```

The file Root_CA_F2-DC-CA.cer will appear in the current directory.

Your Organization's Issuing Certificate Authority

Test environment assumptions

- Operating system is Windows Server 2012 R2
- The issuing CA trusts the trust root CA
- IIS is installed and configured
- IIS port 443 bound to server certificate
- Active Directory Certificate Services is installed and configured, including web enrollment.

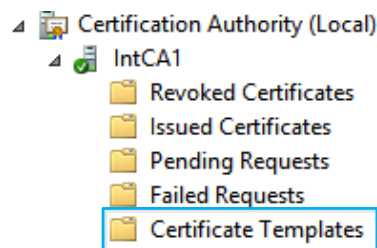
Prerequisites

- The issuing certificate authority server trusts your organization's root certificate authority. In other words, a copy of the root CA certificate for your organization's root certificate authority is located in the issuing certificate authority's Local Computer Trusted Root Certification Authorities store.

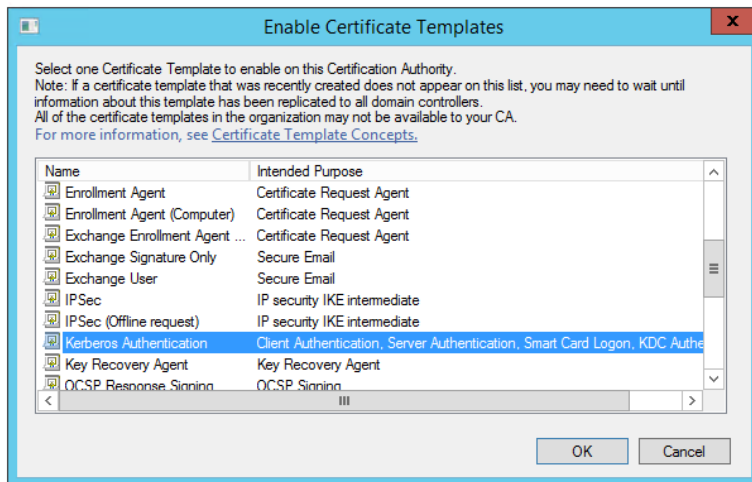
Configuration Steps

Ensure the Key Distribution Center (KDC) template is available to the issuing certificate authority

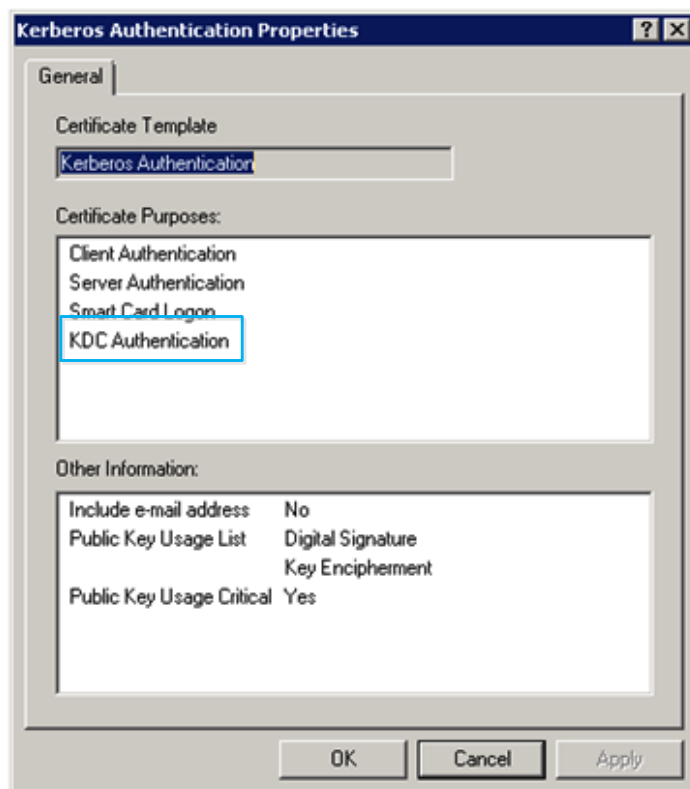
1. Start an instance of the Microsoft Management Console (MMC). From the File menu, choose **Add/Remove Snap In**. From the **Available** snap-ins list, select **Certification Authority**, and click **Add**. The Certification Authority dialog box will appear. Select the local computer as the computer you want the snap-in to manage. Click **Finish**, and then click OK.
2. Navigate to **Certificate Templates**:



3. Right-click **Certificate Templates**. Select **New** and then **Certificate Template to Issue**. The Enable Certificate Templates dialog appears:



4. Select the **Kerberos Authentication** template, and click **OK**. The Kerberos Authentication template should now be listed under Certificate Templates on your issuing CA. The key purpose of this certificate template is KDC authentication:



5. Restart the CA service.

Submit certificate signing requests (CSR) to your organization's issuing CA

NOTE

You cannot complete this step until you have generated the CSR files in section [Create Certificate Signing Requests \(CSR\) for each SSL FIPS key](#) of this guide. If you haven't generated the CSR files yet you can skip the rest of this section and continue with configuration of the [Domain Controller](#).

Have the CSR files you generated on the NetScaler Gateway device at hand:

 fed-callback-csr	14/12/2014 00:29	File	2 KB
 fed-nsg-csr	14/12/2014 00:28	File	2 KB
 fed-sson-session-csr	14/12/2014 00:31	File	2 KB

NOTE

You might want to **temporarily** turn off IE Enhanced Security Configuration in the test environment: Server Manager > Local Server > IE Enhanced Security Configuration. Remember to turn it back on when this step is completed.

6. Start Internet Explorer and point to the following URL:

```
https:<FQDN of your Organization's Issuing CA>/certsrv
```

For example:

```
https://a-ica1.f2.ctxs/certsrv/
```

NOTE

If the page is not available, you need to ensure that IIS and the appropriate Active Directory Certificate Services (such as Certificate Enrollment Web Service) is installed in server roles on the issuing CA server.

7. If you are prompted for credentials, provide admin credentials.

The following page will be displayed:

Microsoft Active Directory Certificate Services -- IntCA1
Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

8. Click **Request a Certificate**. The following page is displayed:

Microsoft Active Directory Certificate Services -- IntCA1 [Home](#)

Request a Certificate

Select the certificate type:
[User Certificate](#)

Or, submit an [advanced certificate request](#).

9. Click **Advanced Certificate Request**. The following page is displayed:

Microsoft Active Directory Certificate Services -- IntCA1 [Home](#)

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

[Create and submit a request to this CA.](#)

[Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.](#)

10. Click **Submit a Certificate Request** by using a base-64-encoded CMC or PKCS#10 file, or submit a renewal request by using a base-64-encoded PKCS#7 file. The following page is displayed:

Microsoft Active Directory Certificate Services -- IntCA1 [Home](#)

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

Certificate Template:

User

Additional Attributes:

Attributes:

11. Use Notepad to open the first CSR file. (In this example, fed-nsg-csr):
12. Select all the text in the file and then copy and paste it into the Base-64-encoded certificate request field in the Saved Request section.

13. Select **Web Server** in the Certificate Template section.

Microsoft Active Directory Certificate Services -- IntCA1 Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN NEW CERTIFICATE REQUEST-----
1bNzesObShBGLAggCloeal97mfMLoKSpx66YU12L
0Kcjgvvo4VxWKlQT7q5FZ7t/qLnPaFDcShEE0QAm/
xPu6ATecdgMI12XUxmindiQcpnNN+/SPPUJrExgK
iQZAnfYMqURG3ZeCFmMEZIOsC8nG/vxJFHY/
-----END NEW CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >

14. Click **Submit**. The following is displayed:

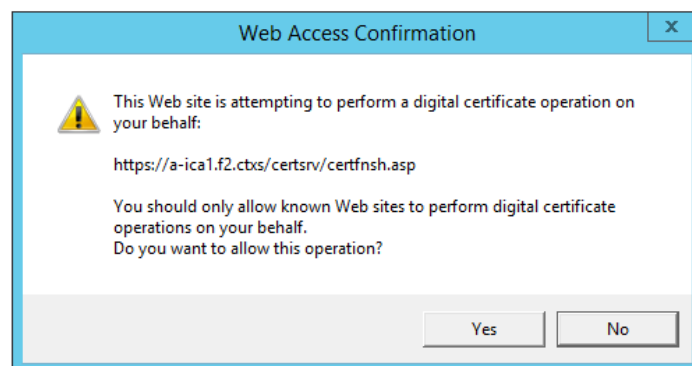
Microsoft Active Directory Certificate Services -- IntCA1 Home

Certificate Issued

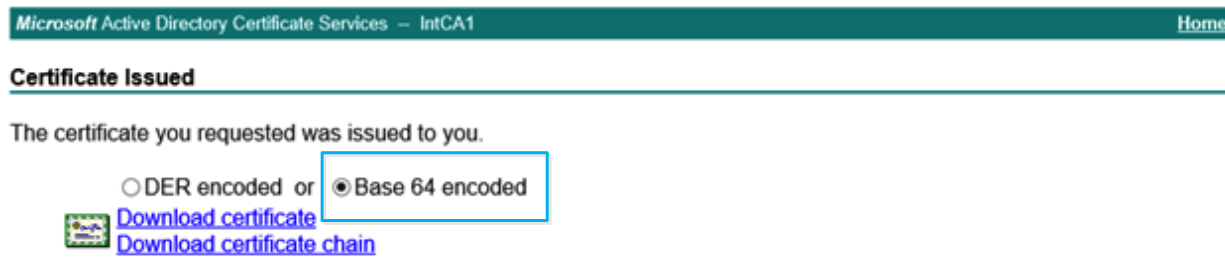
The certificate you requested was issued to you.

☒ DER encoded or ☐ Base 64 encoded

 [Download certificate](#)
[Download certificate chain](#)



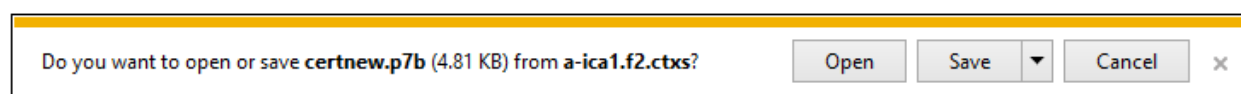
15. Click **Yes**.



16. In the Certificate Issued section, change the encoding format to **Base 64 encoded**.

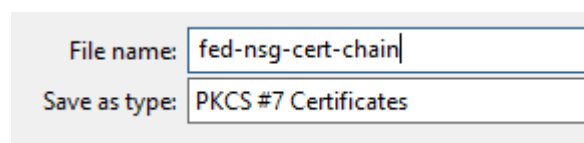
17. Click Download Certificate Chain.

You will be prompted to open or save the file:



18. Select the drop-down arrow next to Save, and click **Save As**.

It is useful to give the certificate a descriptive name. In this example, the certificate is saved as fed-nsg-cert-chain:



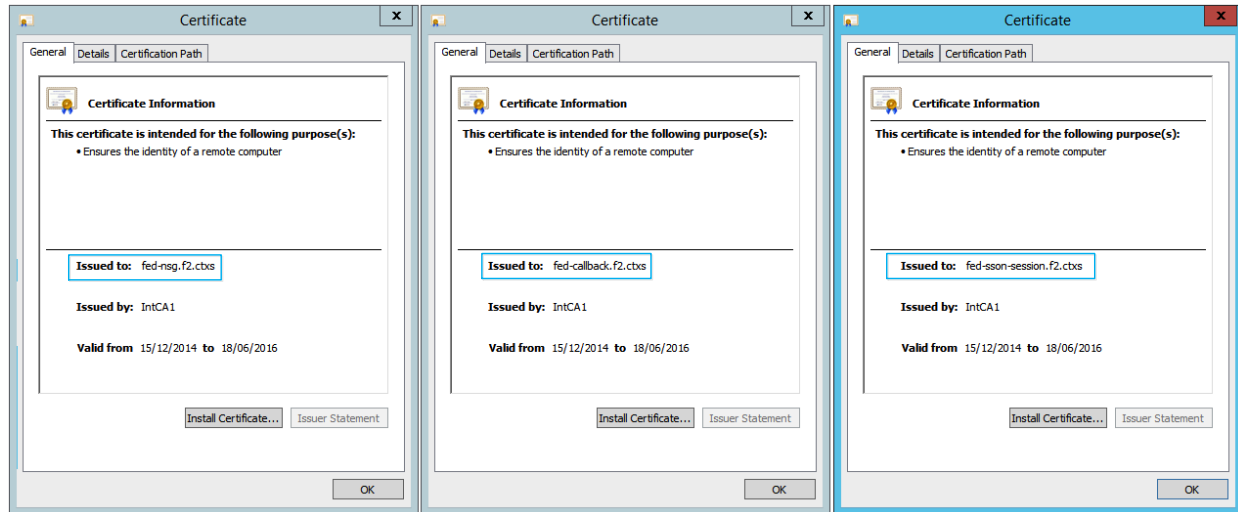
When the file is opened, it should contain three certificates:

Issued To^	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Template
 F2-DC-CA	F2-DC-CA	08/08/2018	<All>	<None>	R	
 fed-nsg.f2.ctxs	IntCA1	18/06/2016	Server Authentication	<None>	R	Web Server
 IntCA1	F2-DC-CA	18/06/2016	<All>	<None>	R	Subordinate Certification Authority

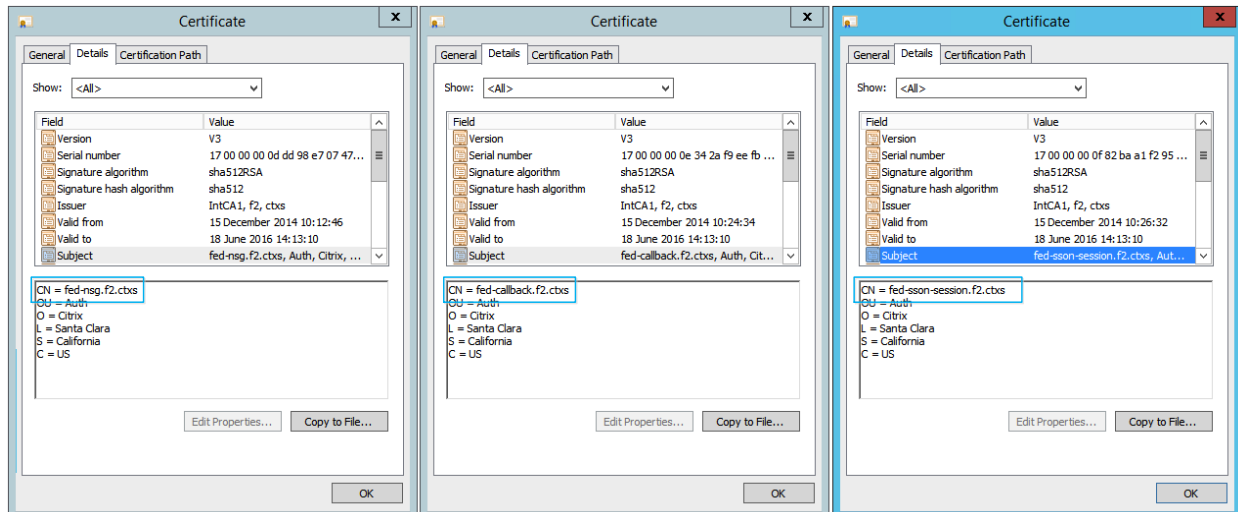
19. Repeat the process for the remaining two CSRs:

- fed-callback-csr
- fed-sson-session-csr

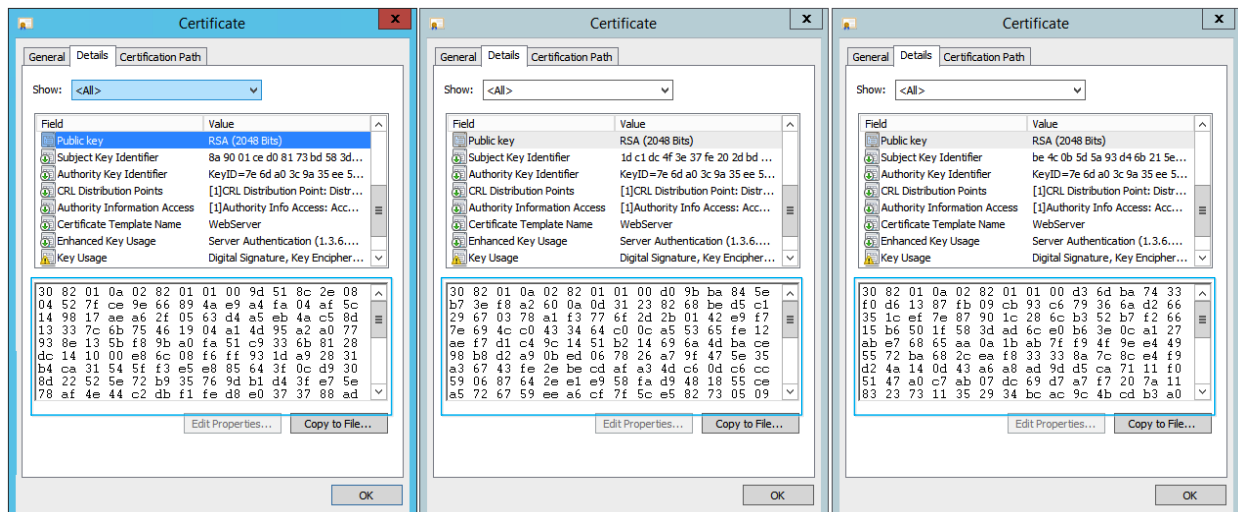
Before continuing, it is worth inspecting the certificates to ensure that you did not accidentally select the wrong template or copy the text for the same CSR more than once:



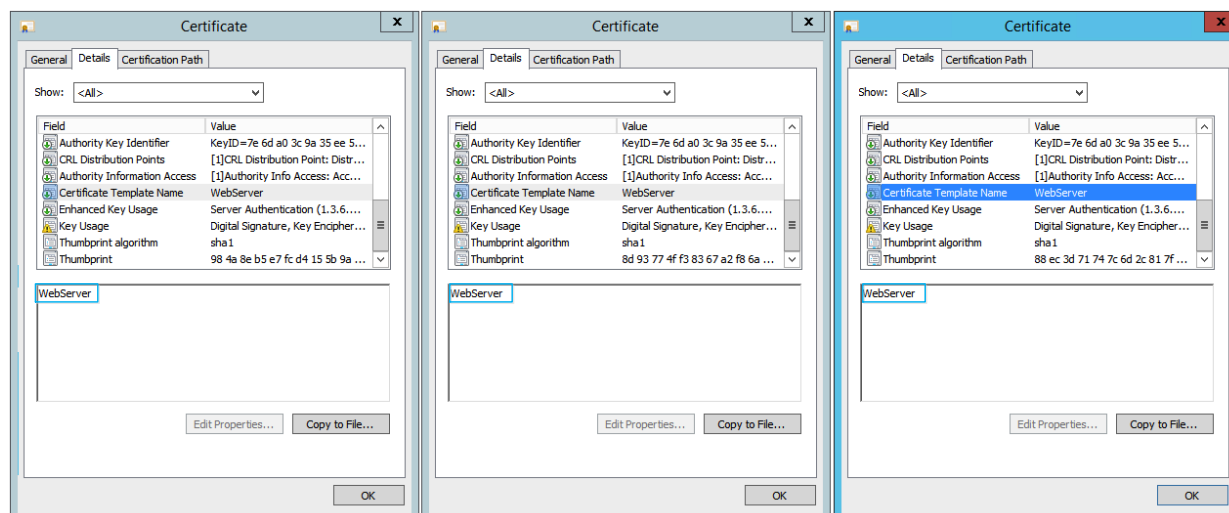
The Subject CN values are as expected:



Public keys are all different:



Certificate Template Name is WebServer for all three:



NOTE

If you temporarily turned off IE Enhanced Security Configuration in the test environment: Server Manager > Local Server > IE Enhanced Security Configuration, you should turn it back on now.

20. Export the certificates to individual files as follows:

Name	Date modified	Type	Size
f2-dc-ca-root-ca-cert	15/12/2014 17:26	Security Certificate	2 KB
fed-callback-cert	15/12/2014 17:25	Security Certificate	2 KB
fed-nsg-cert	15/12/2014 17:32	Security Certificate	2 KB
fed-sson-session-cert	15/12/2014 17:33	Security Certificate	2 KB
intca1-issuing-ca-cert	15/12/2014 17:31	Security Certificate	2 KB

Once the files are exported, jump back to section [Copy certificate files to NetScaler](#).

Domain Controller

Test environment assumptions

- Operating system is Windows Server 2008 R2

Prerequisites

- Enterprise PKI MMC snap-in is installed.
- The Domain Controller trusts your organization's root and intermediate certificate authorities. In other words, copies of the CA certificates for your organization's root and issuing certificate authorities are located in the Domain Controller's Local Computer Trusted Root Certification Authorities and Intermediate Certification Authorities stores, respectively.

Configuration Steps

Group policy settings

There are a number of group policy settings to configure. The level that you link your group policy settings (local, site, domain, Organizational Unit) depends on your organizational requirements.

NOTE

The group policy settings will only become active on target machines once the group policy has refreshed. This is governed by the Group Policy Refresh Interval setting.

FIPS Mode = On

1. Enable the following policy setting:

Policy > Computer Configuration Policies > Windows Settings > Security Settings > Local Policies > Security: "System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing"

 **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** Enabled

Add the Citrix icaclient administrative policy template (ADM) file

Citrix provides a Microsoft group policy template file that enables central administration of certain Citrix Receiver configuration settings. Some of the Citrix Receiver settings that can be toggled through the icaclient ADM template govern Single Sign-on/PIN prompt behavior.

The icaclient.adm template is copied to the following default location on the endpoint when Citrix Receiver is installed on a 64-bit Windows 7 endpoint:

C:\Program Files (x86)\Citrix\ICA Client\Configuration

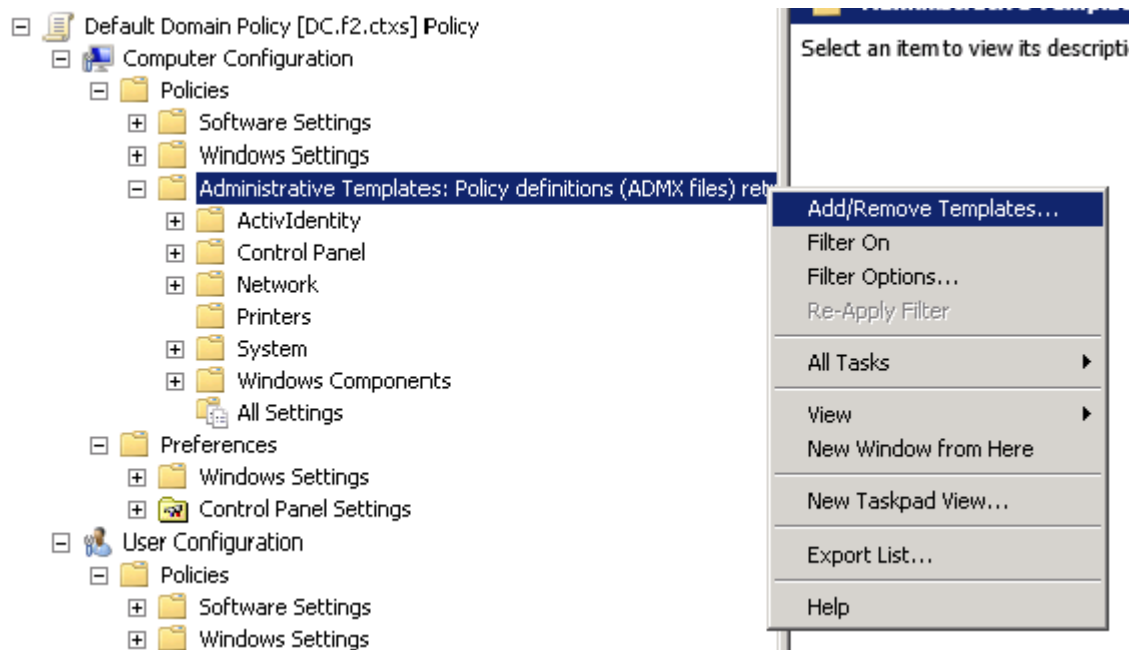
 icaclient.adm	10/29/2014 5:23 PM	ADM File	132 KB
--	--------------------	----------	--------

NOTE

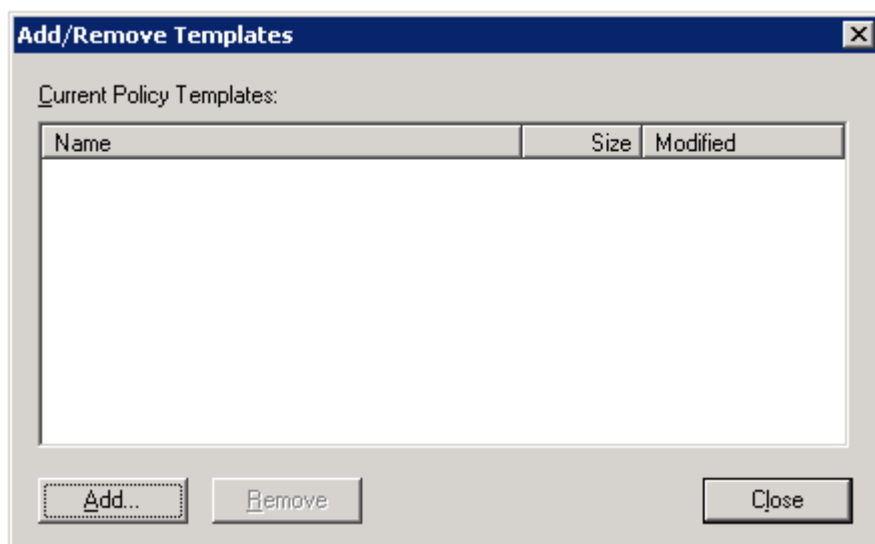
Ensure that you are using the icaclient.adm template from the latest version of Citrix Receiver.

Once you've installed Citrix Receiver on an endpoint in section [Install Citrix Receiver](#), you will be directed back to this section to complete this step. Until then, you can skip ahead to section [Import smart card middleware Administrative Policy Template file \(ADM\)](#)

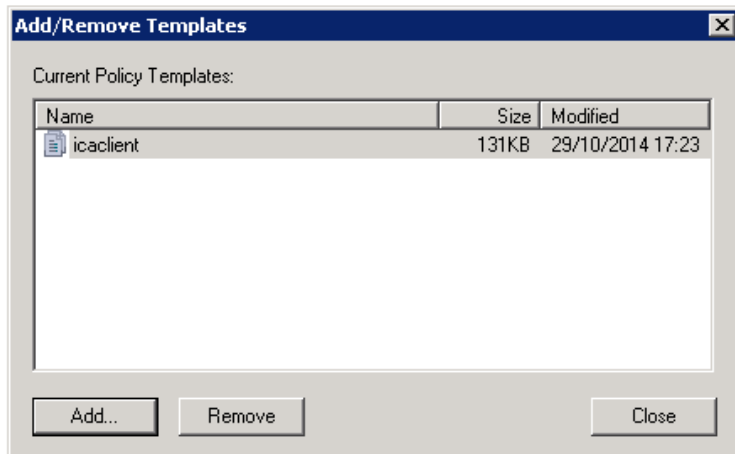
1. In the group policy mmc-snap-in editor, right-click on **Administrative Templates**. Select **Add/Remove Templates**.



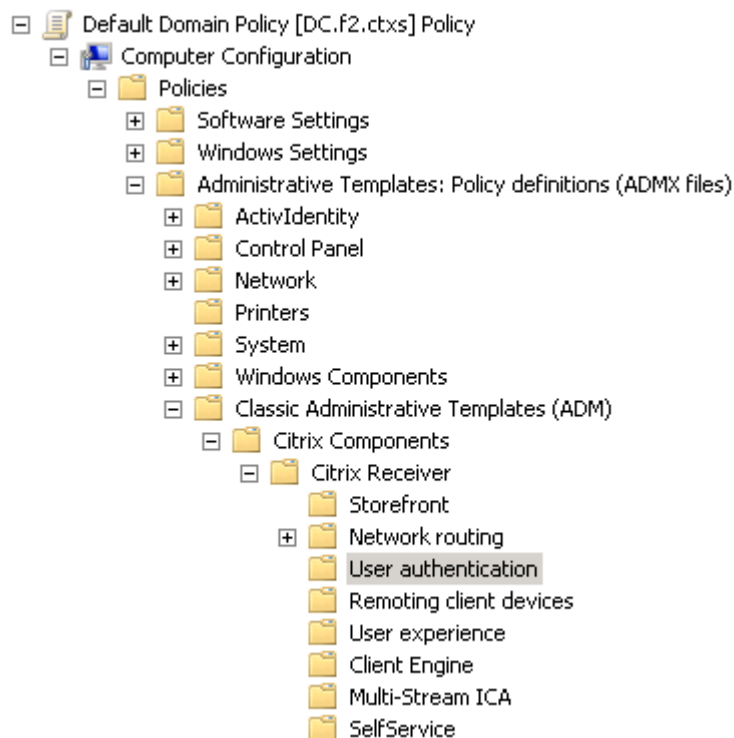
The Add/Remove Templates dialog will be displayed:



2. Click **Add**.
3. Select the `icaclient.adm` file that you copied to the Domain Controller after installing Citrix Receiver in section [Group policy ADM](#). Click **Open**. The Add/Remove Templates dialog box will be populated as follows:



4. Click **Close**.
5. Ensure that the Citrix Receiver user authentication settings have been loaded into the Group Policy Editor:



Import smart card middleware Administrative Policy Template file (ADM)

Many smart card vendors provide a Microsoft group policy template file that enables central administration of certain middleware configuration settings (for example, some of these middleware settings govern the PIN caching mechanisms in the middleware).

For ActivIdentity ActivClient 7.02, the procedure to add the Administrative Template is described in Chapter 2 of the *ActivIdentity ActivClient for Windows Administration Guide*:

“Locate the ActivClient.**adm**x template files in the \Admin\Configuration folder on your ActivClient distribution and copy them to C:\Windows\PolicyDefinitions.”

and

“Locate the ActivClient.**admi** template files in the \Admin\Configuration\EN-US folder on your ActivClient distribution and copy them to C:\Windows\PolicyDefinitions\en-US.”

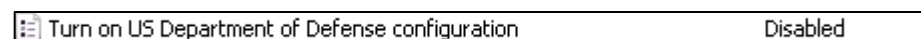
1. Start an instance of the Microsoft Management Console. Add the Group Policy Management Editor snap-in. The Group Policy Wizard is spawned. Click **Browse** to select the Group Policy Object (GPO) to manage. Ensure that the GPO that you select governs the site, domain or OU that contains the machine accounts for computers where ActivClient is (or will be) installed (Windows endpoint and VDA). Click **Finish**.
2. The ActivClient configuration settings will be accessible from <Name of Policy> Policy > Computer Configuration > Policies > Administrative Templates > ActivIdentity.

NOTE

The policy deployed using the GPO linked at the site, domain or OU level overrides the same policy if that policy is set locally (for example, manually by a power user on an endpoint).

Set PIV to take precedence

1. To prevent a local user or administrator from accidentally turning off PIV and turning on CAC, navigate to <Name of Policy> Policy > Computer Configuration > Policies > Administrative Templates > ActivIdentity > ActivClient > Smart Card. Disable “Turn on US Department of Defense configuration.”



If this setting is enabled, ActivClient will communicate with the smart card in GSC-IS mode. That mode is used to communicate with Department of Defense Common Access Cards (CAC).

If this setting is disabled, ActivClient will communicate with the smart card in PIV mode.

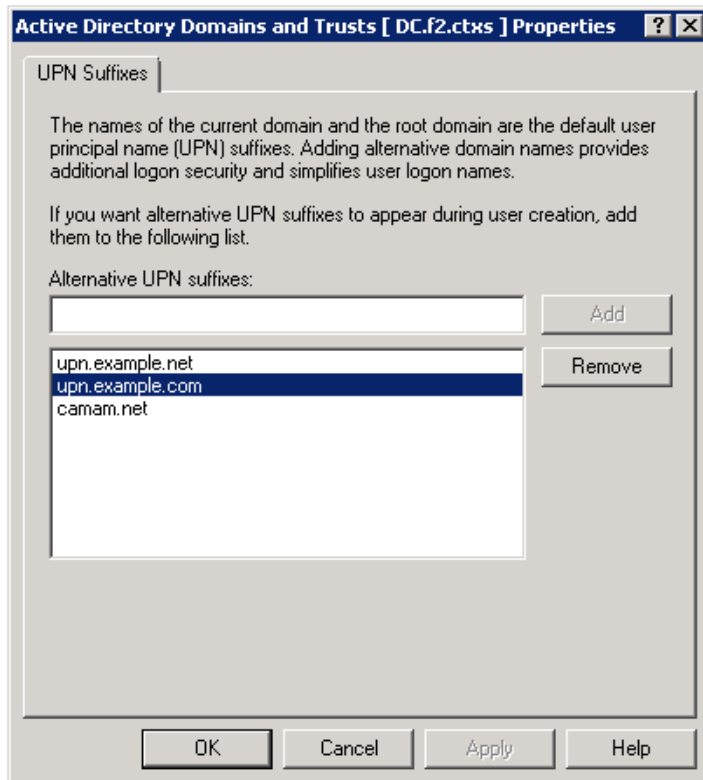
Smart card removal behavior policy setting in group policy

1. Navigate to <Name of Policy> Policy > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options.
2. Set the “Interactive Logon: Smart card removal behavior” policy to reflect the desired behavior in your organization. There are four options: No Action, Lock Workstation, Force Logoff, and Disconnect If a Remote Desktop Service Session.

User Account Settings – Map AD user account to the PIV authentication certificate

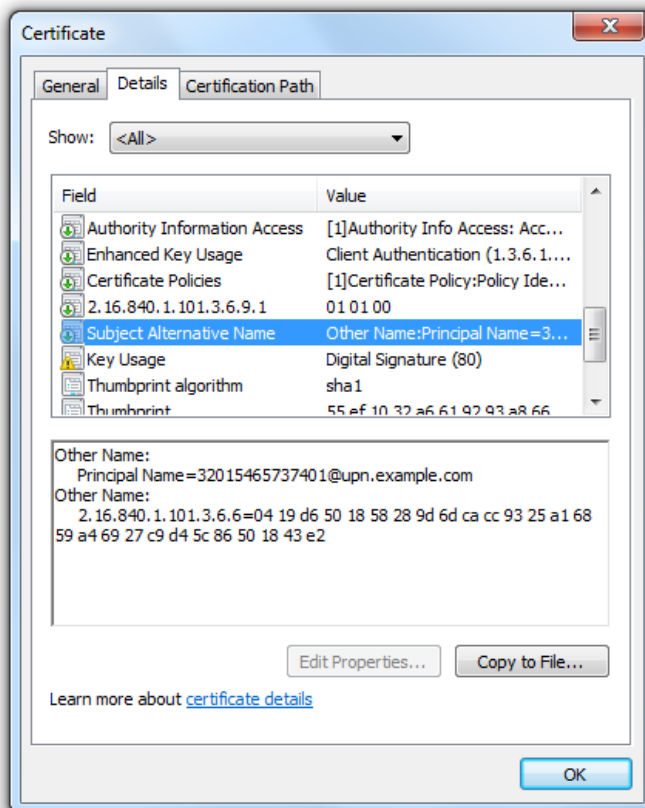
Create alternate UPN

1. If it is not already running, start an instance of the Microsoft Management Console. Add the Active Directory domains and trusts snap-in. Right-click on **Active Directory Domains and Trusts**, click **Properties**. The Active Directory Domains and Trusts Properties dialog box is displayed.
2. In the Alternate UPN Suffixes textbox, enter **upn.example.com**, and click **Add**:



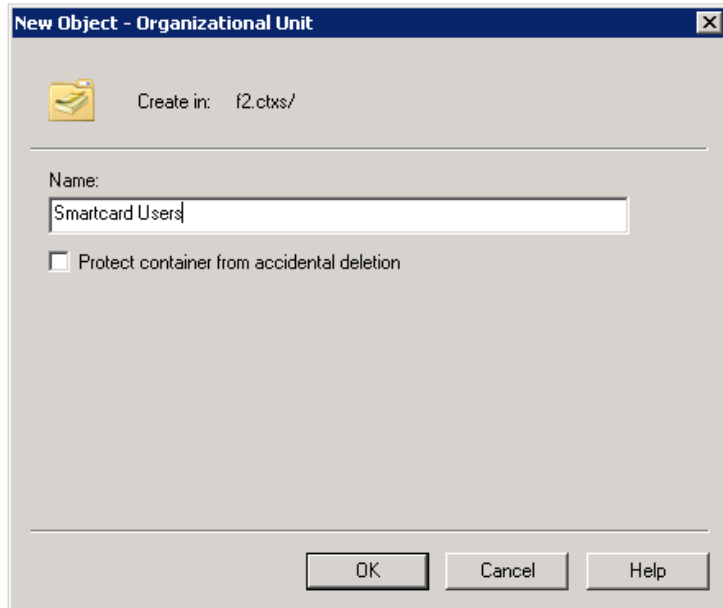
3. Click **OK**.

“upn.example.com” is the suffix of the principal name in the Subject Alternate Name field of the PIV Authentication certificate on NIST PIV Test Card # 1:



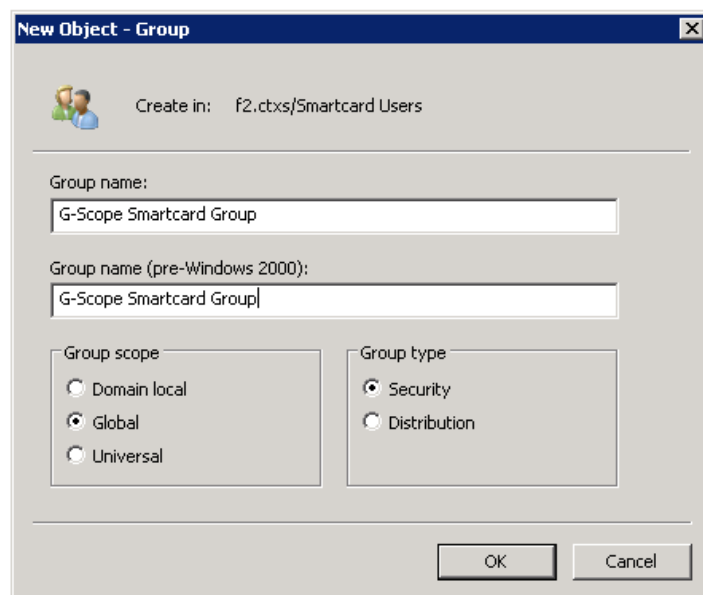
Create OU for PIV user accounts

1. If it is not already running, start an instance of the Microsoft Management Console. Add the Active Directory Users and Computers snap-in.
2. Right-click on the **domain object**, hover the cursor over **New**, and then select **Organizational Unit**. Name the new OU Smartcard Users. Click **OK**:



Create user group

1. Right-click on the newly created Smartcard Users OU, hover the cursor over **New**, and click **Group**. Name the group **G-Scope Smartcard Group**. Note that the group scope is Global and the group type is Security:



2. Click **OK**.

Create user account

1. Right-click on the **Smartcard Users OU**, hover the cursor over **New**, and click **User**. Fill out the New Object – User dialog box as follows:

New Object - User

Create in: f2.ctxs/Smartcard Users

First name: NIST_PIV_01 Initials:

Last name: PIV_Authentication_Cert

Full name: NIST_PIV_01 PIV_Authentication_Cert

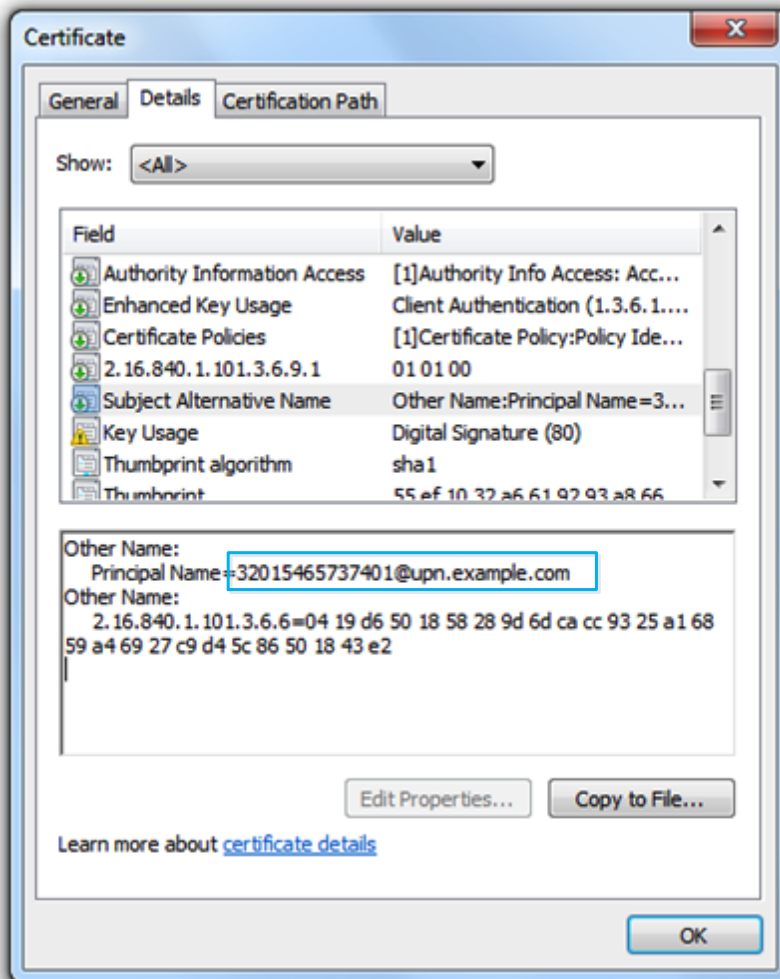
User logon name: 32015465737401 @upn.example.com

User logon name (pre-Windows 2000): F2\ 32015465737401

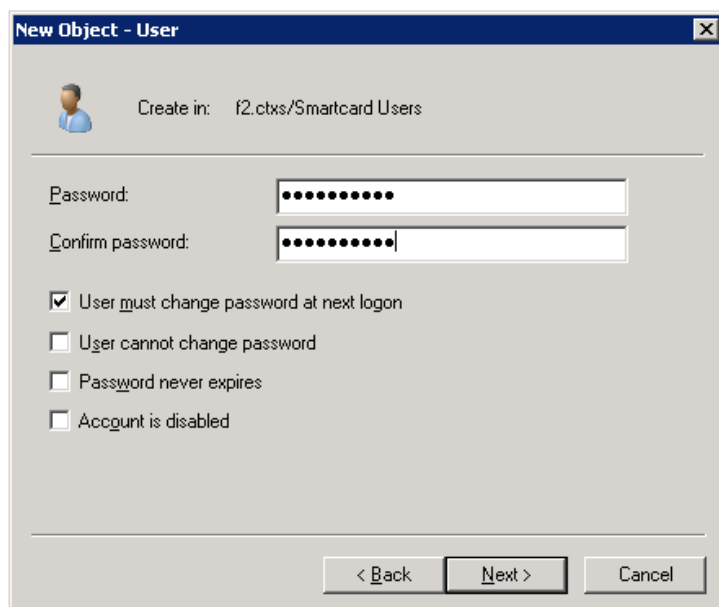
< Back Next > Cancel

Note that the user logon name matches principal name in the Subject Alternate Name field of the PIV Authentication Certificate on NIST PIV Test Card #1:

Friendly name	Issuer	Subject	Expiry Date
PIV Authentication - Test Cardholder	Test RSA 2048-bit CA for Test PIV Cards	Test Cardholder	10/01/2030
Digital Signature - Test Cardholder	Test RSA 2048-bit CA for Test PIV Cards	Test Cardholder	10/01/2030
Key Management - Test Cardholder	Test RSA 2048-bit CA for Test PIV Cards	Test Cardholder	10/01/2030
Card Authentication	Test RSA 2048-bit CA for Test PIV Cards	SERIALNUMBER=D6...	10/01/2030



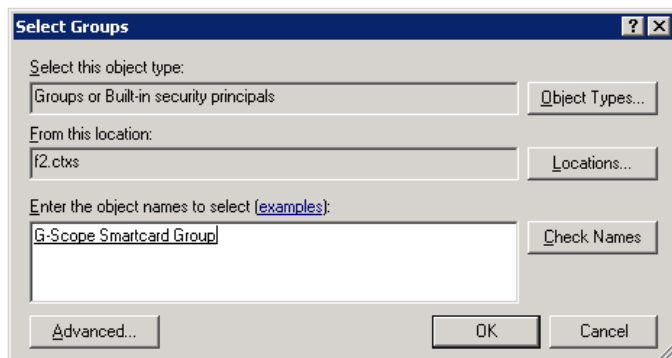
2. Click Next.



3. Provide a password, and click **Next**, and then click **Finish**.

Add user to G-Scope Smartcard Group

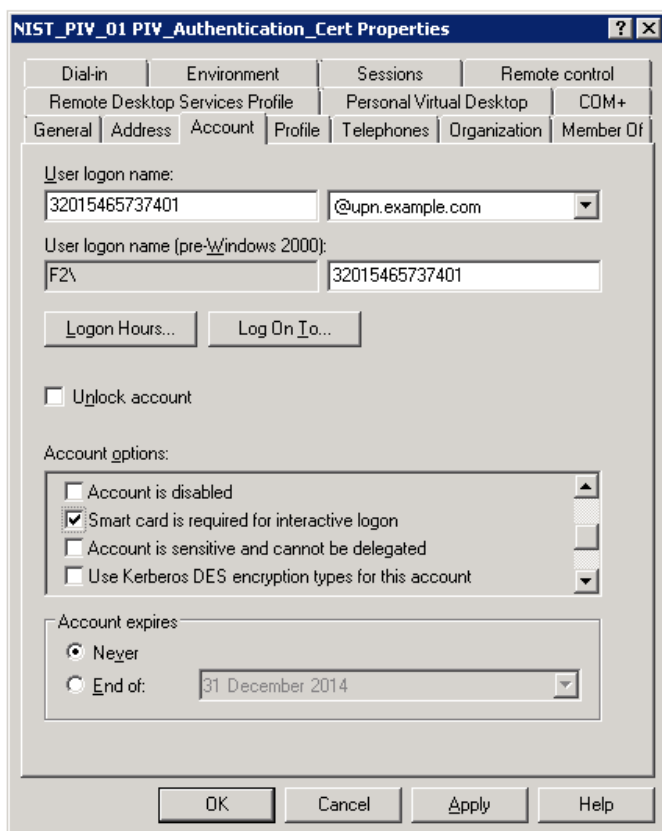
1. Right-click on the **NIST_PIV_01 PIV Authentication Cert** user account, hover the cursor over **All Tasks**, and click **Add to a group**. Enter the following:



2. Click **OK**.

Set smart card required for interactive logon

1. Right-click on the **NIST_PIV_01 PIV Authentication Cert** user account, and click **Properties**. Click on the **Account** tab. In the **Account options** section, deselect **User must change password at next logon**, and select **Smart card is required for interactive logon**:



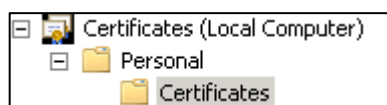
NOTE

When you check the **Smart card is required for interactive logon** box, the operating system takes over user password management. It assigns a maximum-length password that is equivalent to 255 characters and ensures that it meets complexity requirements, effectively blocking the user from logging on to the network using a password. This can also be set via group policy.

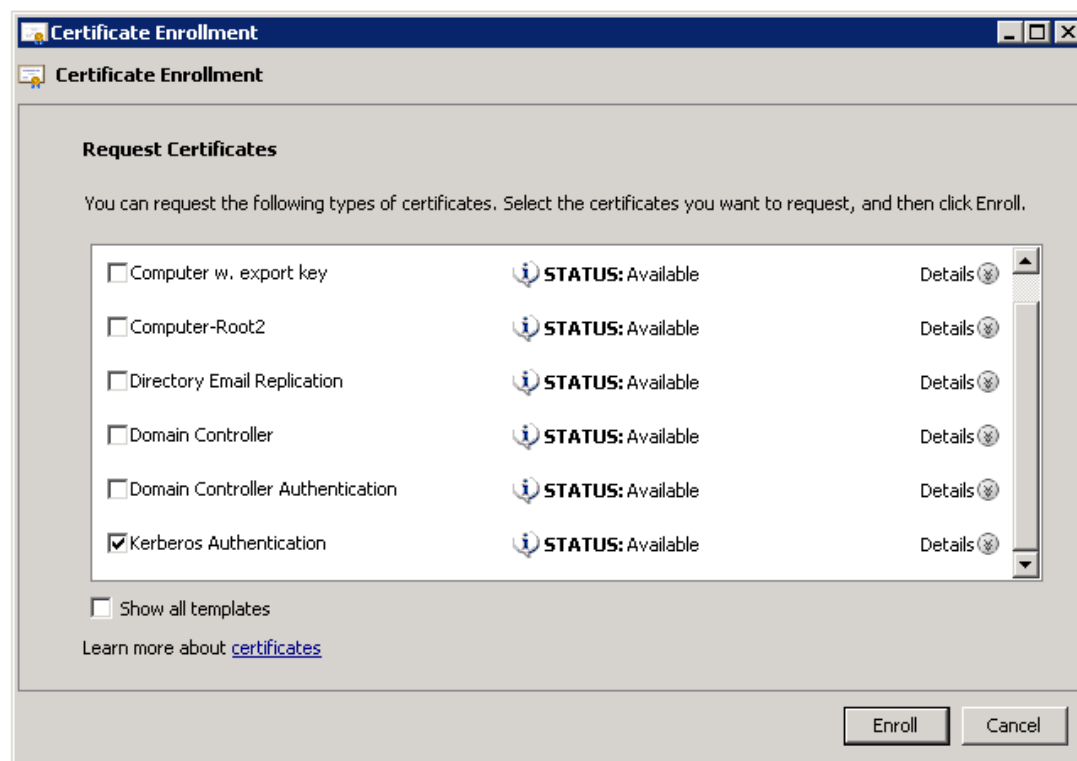
PKI certificate configuration

Request KDC Certificate from your organization's issuing CA

1. Refer to steps 2 and 5 in [Appendix D: Publishing Certificates in Active Directory](#) for a graphical representation of the steps below.
2. Start an instance of the Microsoft Management Console (MMC). From the File menu, choose **Add/Remove Snap In**. From the **Available** snap-ins list, select **Certificates**, and click **Add**. The Certificates dialog box will appear. Select the local computer as the computer you want the snap-in to manage. Click **Finish**, and then click **OK**.



3. Navigate to Personal > Certificates. Right-click on **Certificates**, choose **All Tasks**, and click on **Request New Certificate**. The Certificate Enrollment wizard opens. Click **Next**. Select the appropriate Certificate Enrollment Policy. Click **Next**.

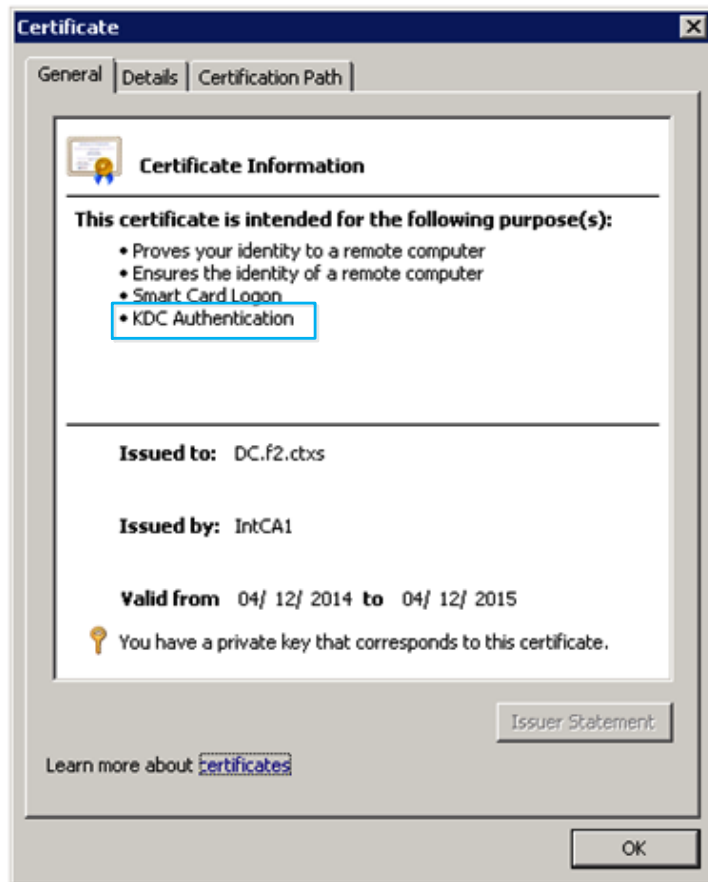


4. Select Kerberos Authentication, and click Enroll.

NOTE

If Kerberos Authentication is not listed, you will need to adjust the enroll permissions in the Security tab of the Kerberos Authentication Certificate Template Properties using the Certificate Templates mmc snap-in on the issuing CA.

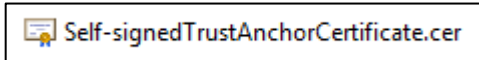
The certificate is intended for the following purposes:



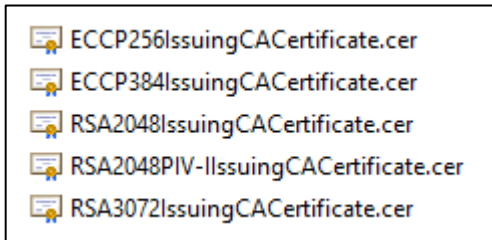
Certificate file consolidation

You should now have the following certificate files at hand:

The NIST test PIV self-signed CA certificate:



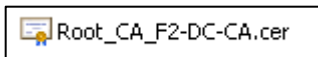
The NIST test PIV issuing CA certificates:



NOTE

Of the five NIST test PIV issuing certificates, the one that is relevant to the steps in the guide is RSA2048IssuingCACertificate.cer because it is in the PIV authentication certificate's trust chain.

Your organization's exported RootCA certificate:



Publish certificates to Active Directory certificate containers

Using this method, the certificates are automatically propagated throughout. This way you do not have to manually install certificates in certificate stores on machines individually.

1. Refer to [Appendix D: Publishing Certificates in Active Directory](#) for a diagrammatic representation of the process that follows.

NOTE

You must run these commands using a user account with enterprise administrative privileges. Do not use an account that is a member of the domain admins group but not the enterprise admins group.

- Copy the certificate files to a directory. Run a command prompt. Change the prompt to that directory. Then run the following commands from the command prompt:

Publish your organization's root CA certificate to Certification Authorities (RootCA) container (Refers to step 6 in [Appendix D: Publishing Certificates in Active Directory](#))

Syntax:

```
certutil -dspublish -f <Your Organization's Root CA Certificate file>.cer
```

Example:

```
certutil -dspublish -f Root_CA_F2-DC-CA.cer
```

Publish your organization's root CA certificate to NTAUTH certificates (NTAuth) container (Refers to step 7 in [Appendix D: Publishing Certificates in Active Directory](#))

Syntax:

```
certutil -dspublish -f <Your Organization's Root CA Certificate file>.cer NTAuthCA
```

Example:

```
certutil -dspublish -f Root_CA_F2-DC-CA.cer NTAuthCA
```

Publish the NIST test PIV root CA certificate to Certification Authorities (RootCA) container (Refers to step 8 in [Appendix D: Publishing Certificates in Active Directory](#))

Syntax:

```
certutil -dspublish -f <NIST Test PIV Root CA Certificate file>.cer
```

Example:

```
certutil -dspublish -f Self-signedTrustAnchorCertificate.cer
```

Publish the NIST test PIV issuing CA certificate to NTAUTH container (Refers to step 9 in [Appendix D: Publishing Certificates in Active Directory](#))

Syntax:

```
certutil -dspublish -f <NIST Test PIV Issuing CA Certificate file>.cer NTAuthCA
```

Example:

```
certutil -dspublish -f RSA2048IssuingCACertificate.cer NTAuthCA
```

Publish the NIST test PIV issuing CA certificate to AIA (SubCA) container (Refers to step 10 in [Appendix D: Publishing Certificates in Active Directory](#))

Syntax:

```
certutil -dspublish -f <NIST Test PIV Issuing CA Certificate file>.cer subCA
```

Example:

```
certutil -dspublish -f RSA2048IssuingCACertificate.cer subCA
```

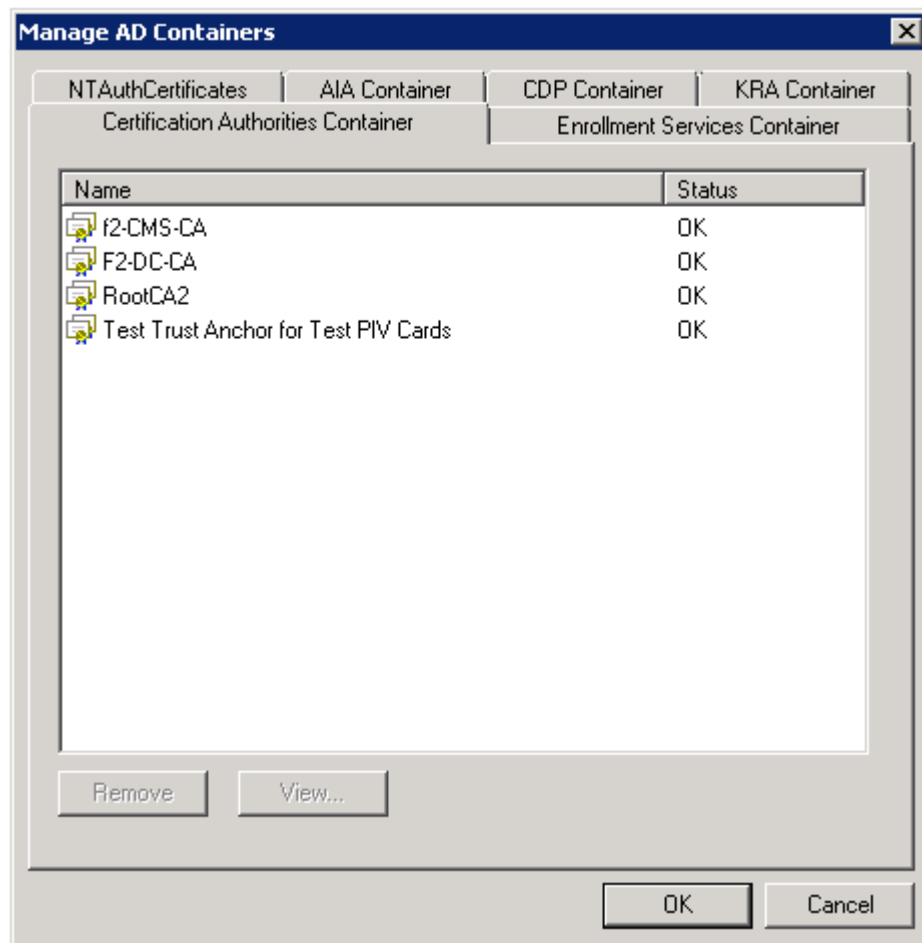
Propagation does not occur until a group policy refresh. Manually force-refresh using the following command:

```
Gpupdate /Force
```

Enterprise PKI snap-in

1. To view the published certificates in the graphical user interface, you need the enterprise PKI snap-in. All of the relevant AD Containers can be viewed. However, it is not possible to add certificates to the AIA (subCA) Container using the snap-in.

<http://technet.microsoft.com/en-us/library/cc771085.aspx>



NOTE

If anything is showing as untrusted, refresh the group policy to ensure it propagates and is trusted.

Virtual Delivery Agent (VDA)

Test environment assumptions

- Operating system is 64 bit Windows 7 with Service Pack 1
- Citrix Virtual Delivery Agent is 7.6.0.5026
- The smart card middleware is 64-bit ActivClient 7.0.2
- Machine is domain-joined

Prerequisites

- The VDA trusts your organization's root and intermediate certificate authorities. In other words, copies of the CA certificates for your organization's root and intermediate certificate authorities are located in the VDA's Local Computer Trusted Root Certification Authorities and Intermediate Certification Authorities stores, respectively.

Configuration Steps

Install middleware

1. Refer to [Appendix E: Install ActivClient 7.0.2 on Windows 7 x64](#) for detailed steps.

NOTE

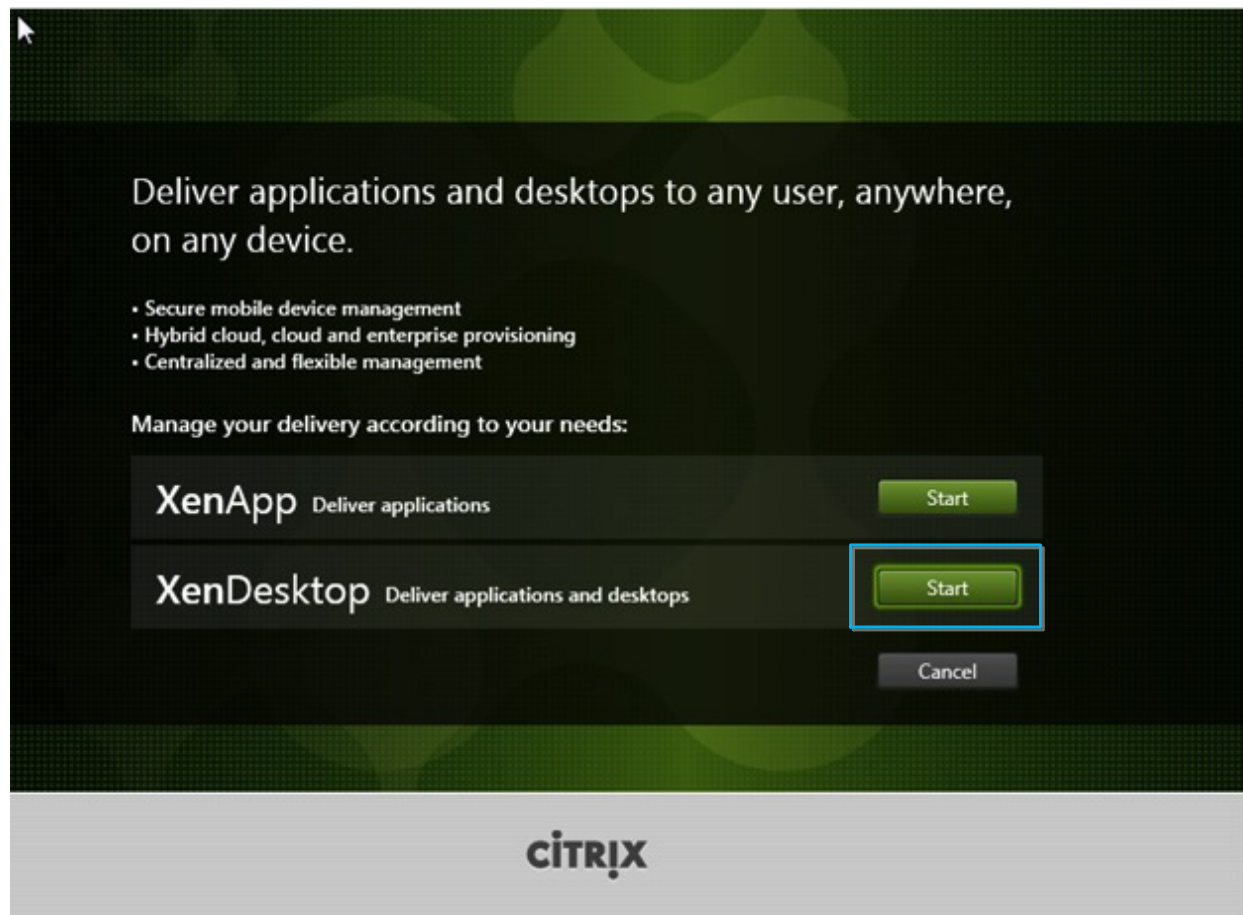
Smart Card **reader** drivers are *not* required on the VDA.

Install VDA for Windows Desktop OS

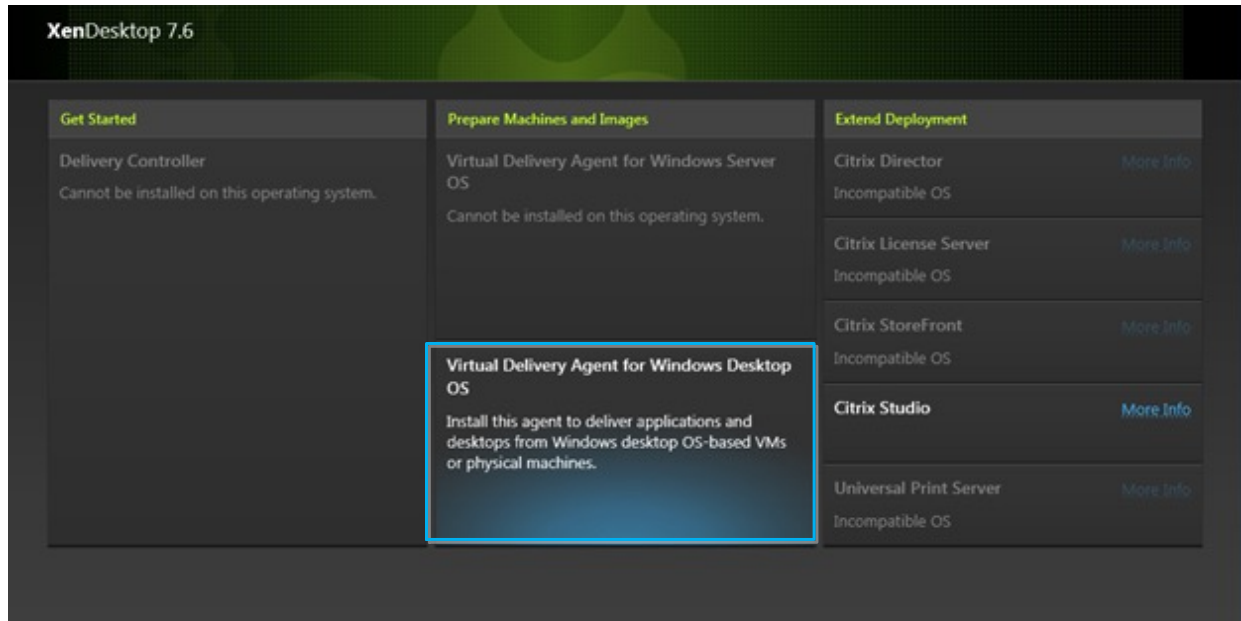
1. Perform the installation on the VDA machine console, not remotely via a remote desktop protocol such as RDP.
2. Insert the Citrix installation media, and run the AutoSelect.exe file:



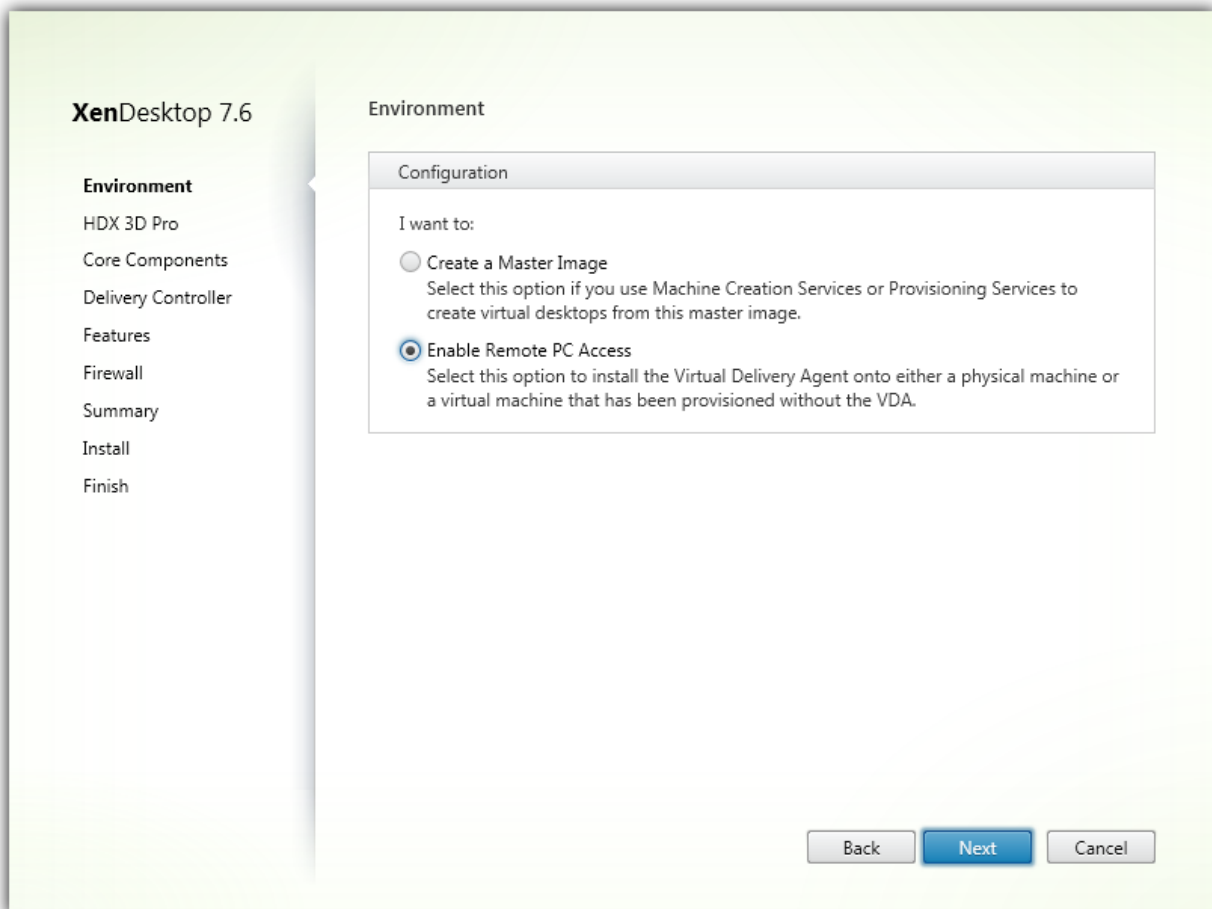
The XenApp and XenDesktop installer opens:



3. Click Start for XenDesktop. Then click Virtual Delivery Agent for Windows Desktop OS:



4. Select the Enable Remote PC Access option.



NOTE

For a production environment, you likely will want to use a master image. Refer to the Citrix Product Documentation site for more information about how to configure and use a master image:

<http://support.citrix.com/proddocs/topic/xenapp-xendesktop-76/xad-mach-cat-create.html>

HDX 3D Pro

HDX 3D Pro optimizes the performance of graphics-intensive programs and media-rich applications.

Configuration**Install the Virtual Delivery Agent (VDA) for HDX 3D Pro?**

- ☒ No, install the standard VDA
Recommended for most desktops, including those enabled with Microsoft RemoteFX.
- ☐ Yes, install the VDA for HDX 3D Pro
Recommended if the machine will access a graphics processor for 3D rendering.

5. For Core Components, install only the VDA. Do not install Citrix Receiver.

Core Components

Location: C:\Program Files\Citrix Change...

Virtual Delivery Agent (Required)
The software agent that is installed on the virtual or physical machine that provides the virtual desktop or application to the user.

☐ **Citrix Receiver**
Client software that enables users to access their documents, applications, and desktops from any device, including smartphones, tablets, and PCs.

NOTE

Citrix Receiver is typically installed on the VDA in double-hop scenarios (when a user launches a XenApp session from within a XenDesktop session). If you intend to perform double-hop deployments with smart card Single Sign-on (Please note that double-hop deployments are outside the scope of the first edition of this guide): You must install Receiver on the VDA from the command line and add the `/includeSSON` command line switch or the Citrix Single Sign-on service component will not be installed when Receiver is installed. In addition, the build of Receiver that you want to use may not be the same Receiver build that ships with the VDA build (that is consumed by the VDA installation wizard).

6. Enter the FQDN of the Delivery Controller. For this example, it is `a-ddc.f2.ctxs`.

Delivery Controller**NOTE**

There is no need to click “Test connection...” if the Delivery Controller is not configured yet. (Which will be the case if you are following the steps in the guide sequentially.) Be absolutely sure the Controller address entered here is identical to the address you plan to use for the Delivery Controller later.

7. Click **Next**.

8. Leave Features at default.

Features

☐	Feature (Select all)
☒	Optimize performance Optimize desktop settings. Learn more
☒	Use Windows Remote Assistance Enable Windows Remote Assistance and open TCP port 3389. Learn more
☒	Use Real-Time Audio Transport for audio Uses UDP ports 16500 - 16509. Learn more
☐	Personal vDisk Enable Personal vDisk for the Virtual Delivery Agent. Learn more

9. Leave Firewall at default.

Firewall

The default ports are listed below.

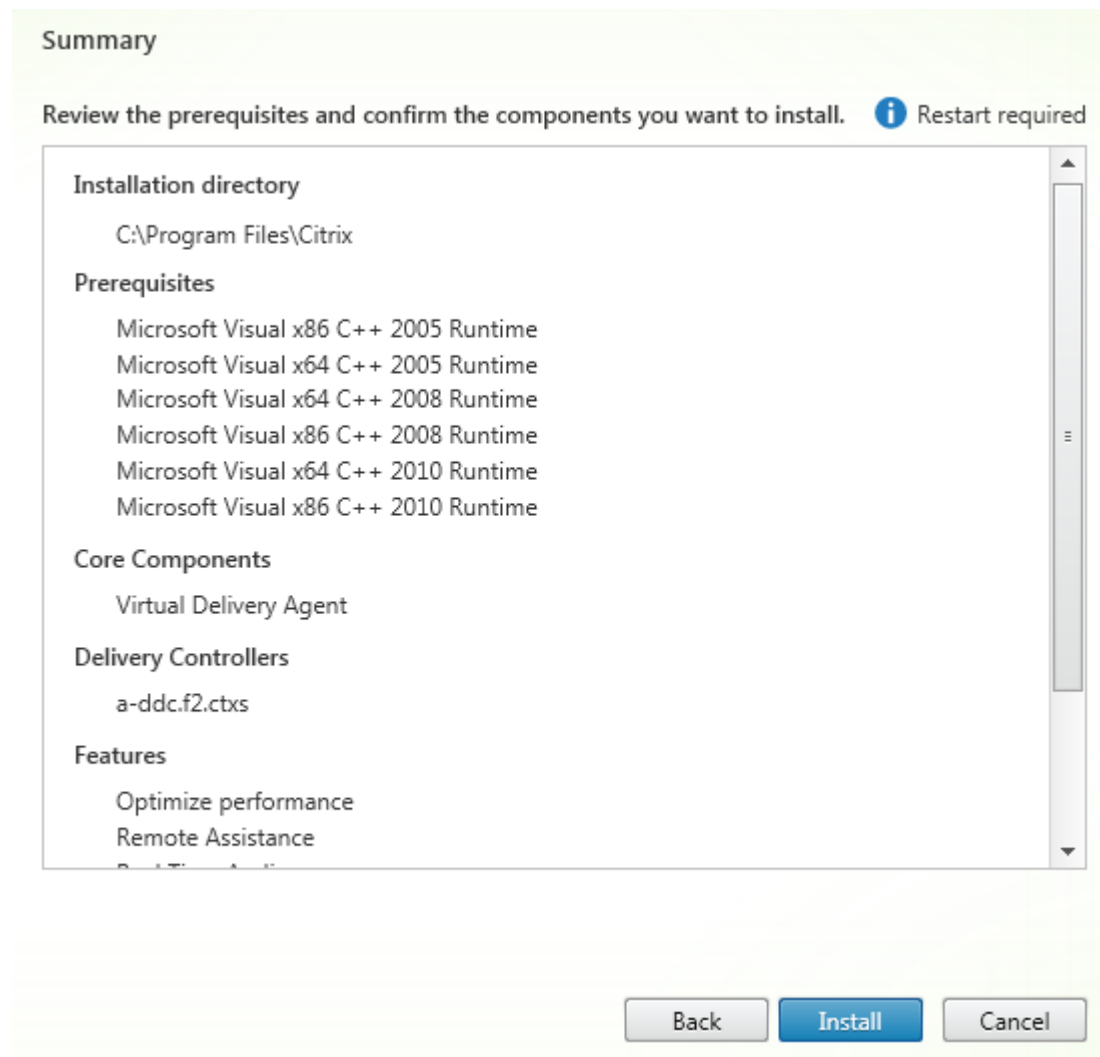
[Printable version](#)

Controller Communications	Remote Assistance	Real Time Audio
80 TCP 1494 TCP 2598 TCP 8008 TCP	3389 TCP	16500 - 16509 UDP

Configure firewall rules:

- ☒ Automatically
Select this option to automatically create the rules in the Windows Firewall. The rules will be created even if the Windows Firewall is turned off.
- ☐ Manually
Select this option if you are not using Windows Firewall or if you want to create the rules yourself.

A summary will be displayed:



10. Click **Install**.

Finish Installation

The installation completed successfully.

✓ Success

Prerequisites

✓ Microsoft Visual x86 C++ 2005 Runtime	Installed
✓ Microsoft Visual x64 C++ 2005 Runtime	Installed
✓ Microsoft Visual x64 C++ 2008 Runtime	Installed
✓ Microsoft Visual x86 C++ 2008 Runtime	Installed
✓ Microsoft Visual x64 C++ 2010 Runtime	Installed
✓ Microsoft Visual x86 C++ 2010 Runtime	Installed

Core Components

✓ Virtual Delivery Agent	Installed
--------------------------	-----------

Post Install

✓ Component Initialization	Initialized
----------------------------	-------------

☒ Restart machine

Back

Finish

Delivery Controller

Test environment assumptions

- Operating system is Windows Server 2012 R2.
- Citrix XenDesktop is version 7.6.0.5026.
- The Delivery Controller runs on a dedicated server (StoreFront is also installed on a separate dedicated server of its own.).
- No stand-alone database server is used. During Delivery Controller installation, SQL Server 2012 Express SP1 is automatically installed on and used by the Delivery Controller.
- Machine Management/Machine Creation Services (MCS) is not used.
- Microsoft Internet Information Services (IIS) is installed on the Delivery Controller, which possesses a server certificate with corresponding private key, and the server certificate is used to bind https to port 443 in IIS: <http://support.citrix.com/proddocs/topic/xendesktop-7/cds-mng-cntrlr-ssl.html>.

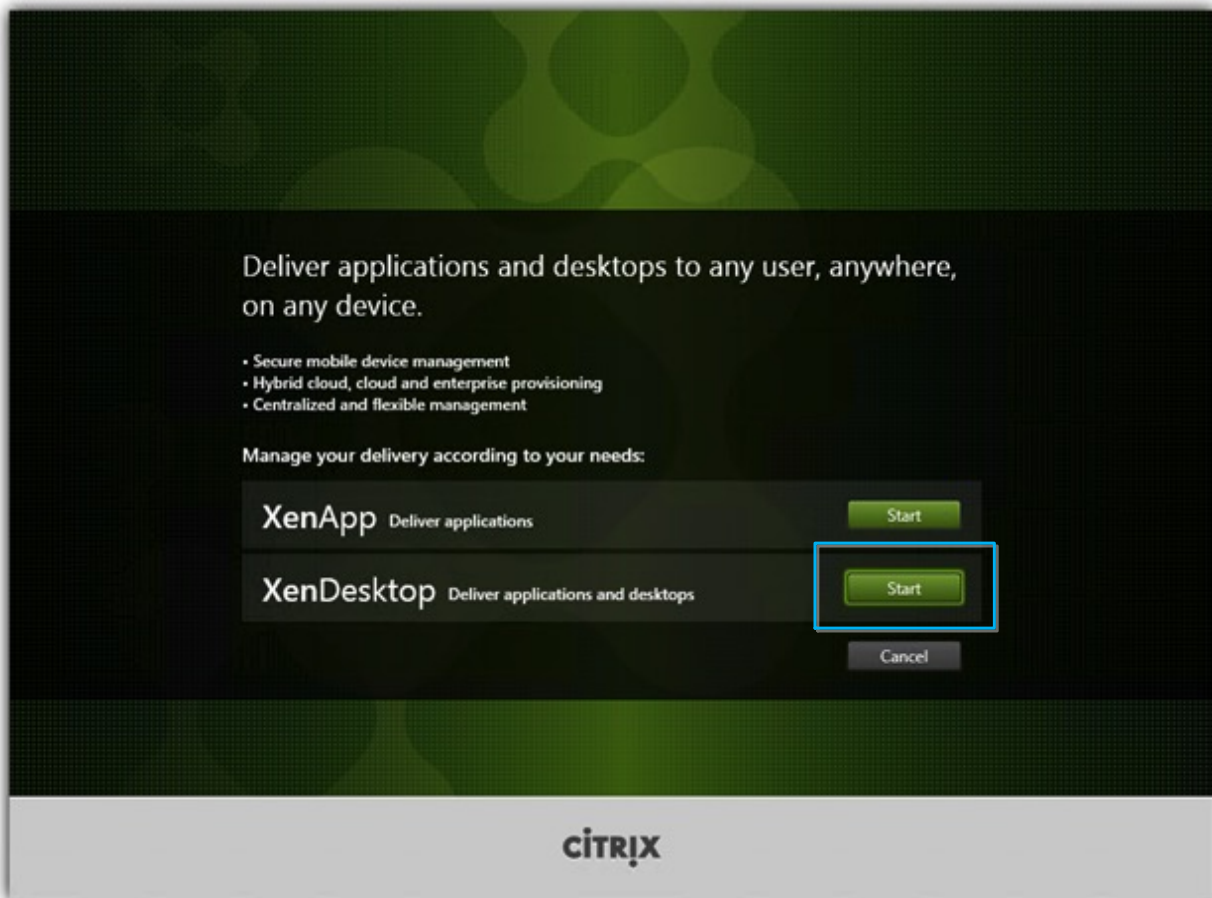
Prerequisites

- Citrix License Server is up and running (configuring the License Server is outside the scope of this guide).
- The Delivery Controller trusts your organization's root and intermediate certificate authorities. In other words, copies of the CA certificates for your organization's root and issuing certificate authorities are located in the Delivery Controller's Local Computer Trusted Root Certification Authorities and Intermediate Certification Authorities stores, respectively.

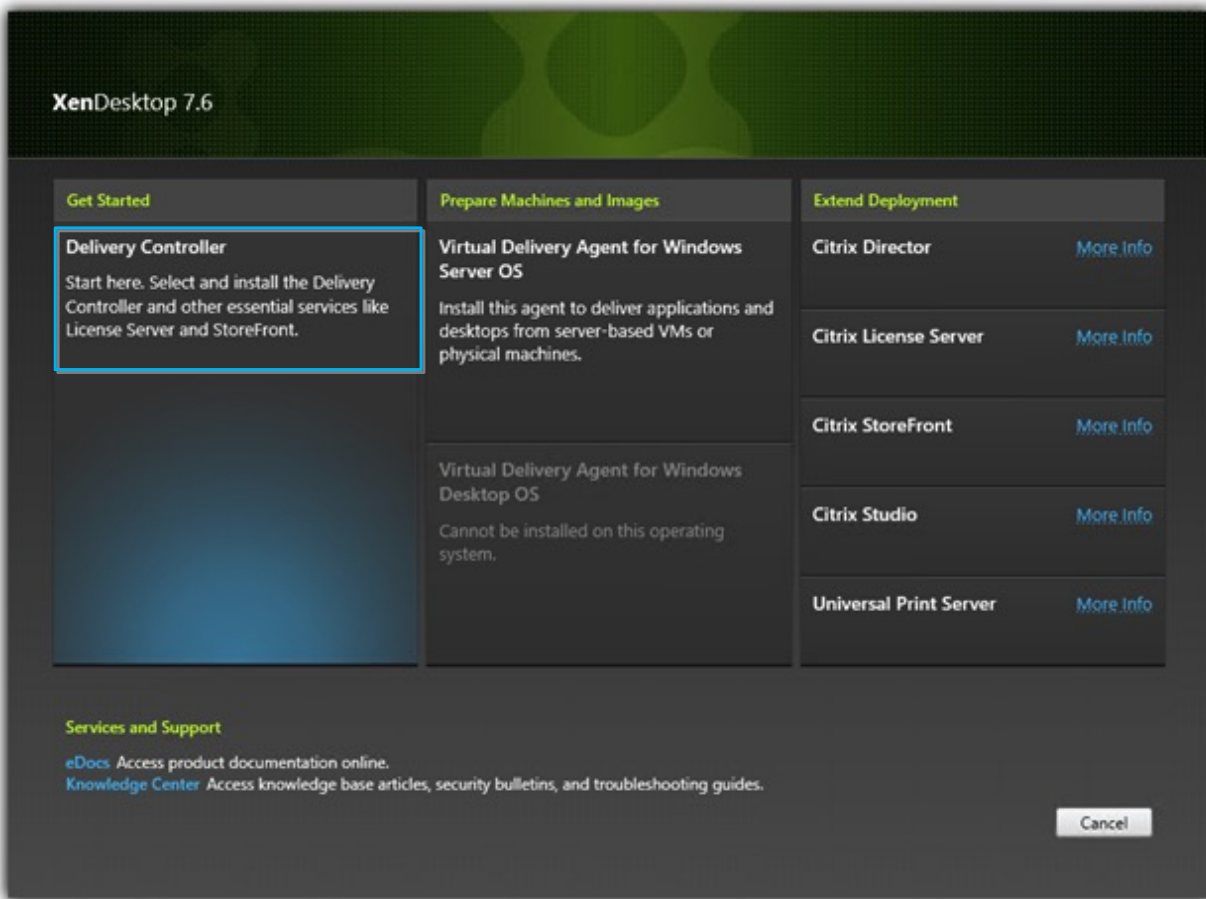
Configuration Steps

Delivery Controller installation

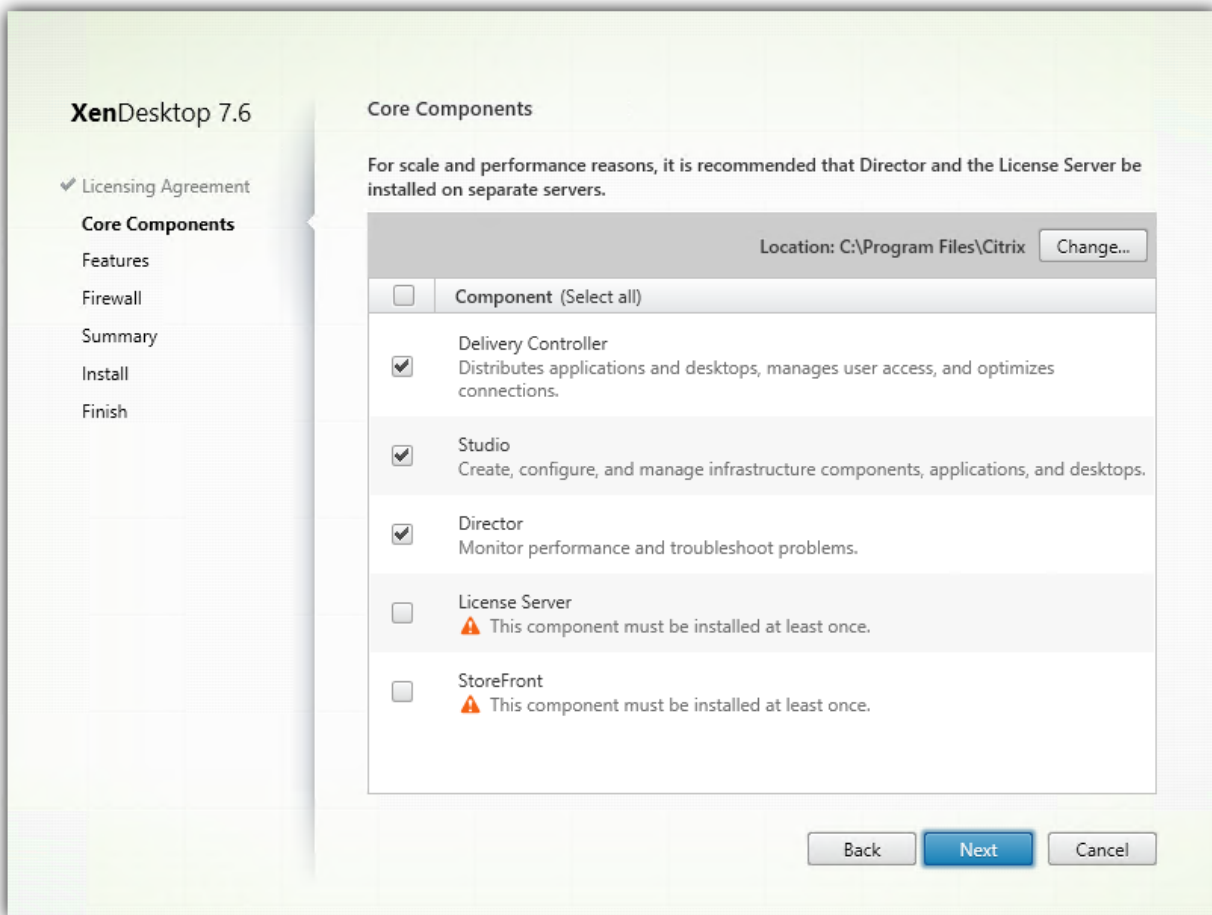
1. Start from the installation media. Click **Start** for XenDesktop. Note that XenDesktop can deliver applications and desktops.



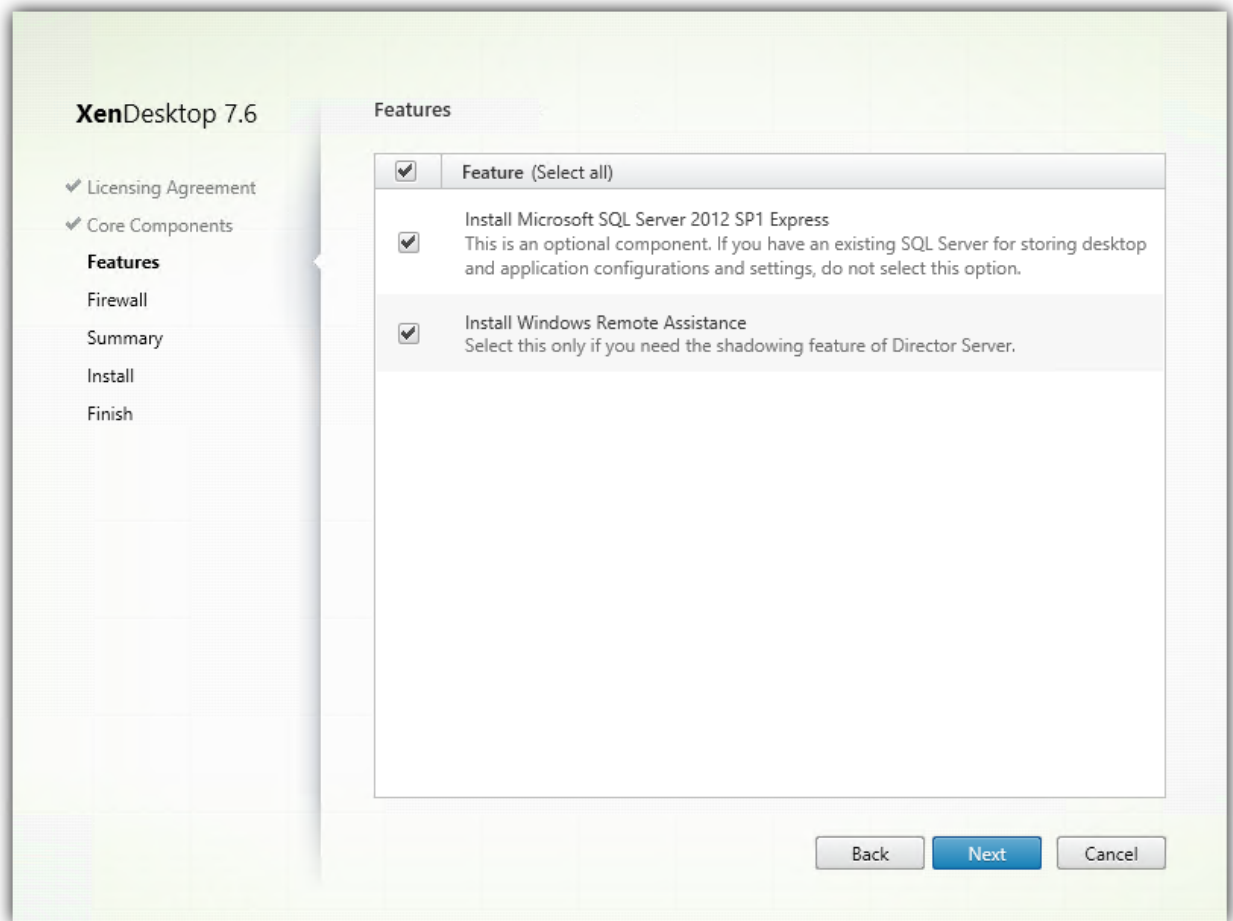
2. Click Delivery Controller in the Get Started section.



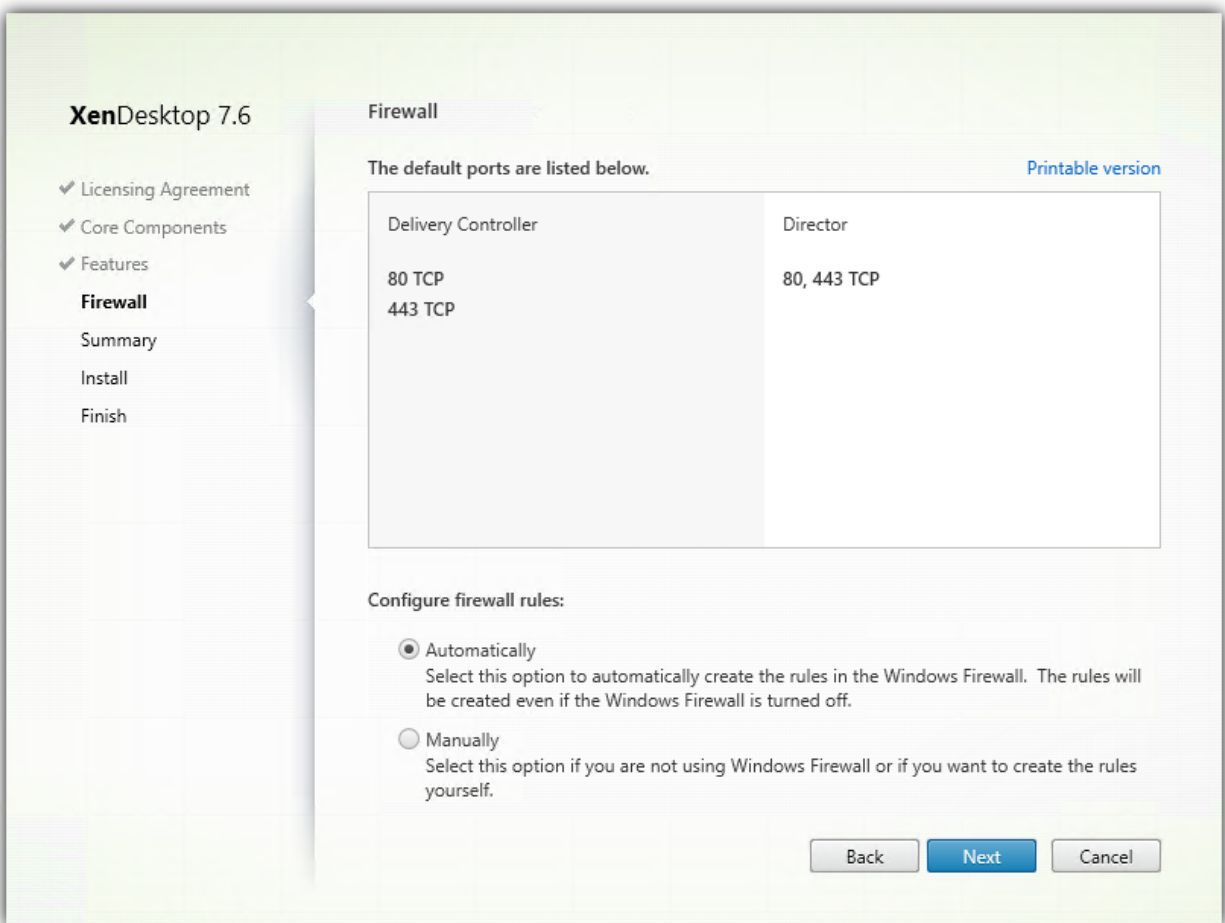
3. Select the following Core Components:



4. By default, License Server and StoreFront are selected. Configuring License Server is beyond the scope of this guide. It is assumed that a License Server is available to which to point. StoreFront will be installed separately on a dedicated server. (Refer to section [StoreFront](#) for details.) Click **Next**.
5. Leave features at default as shown below.

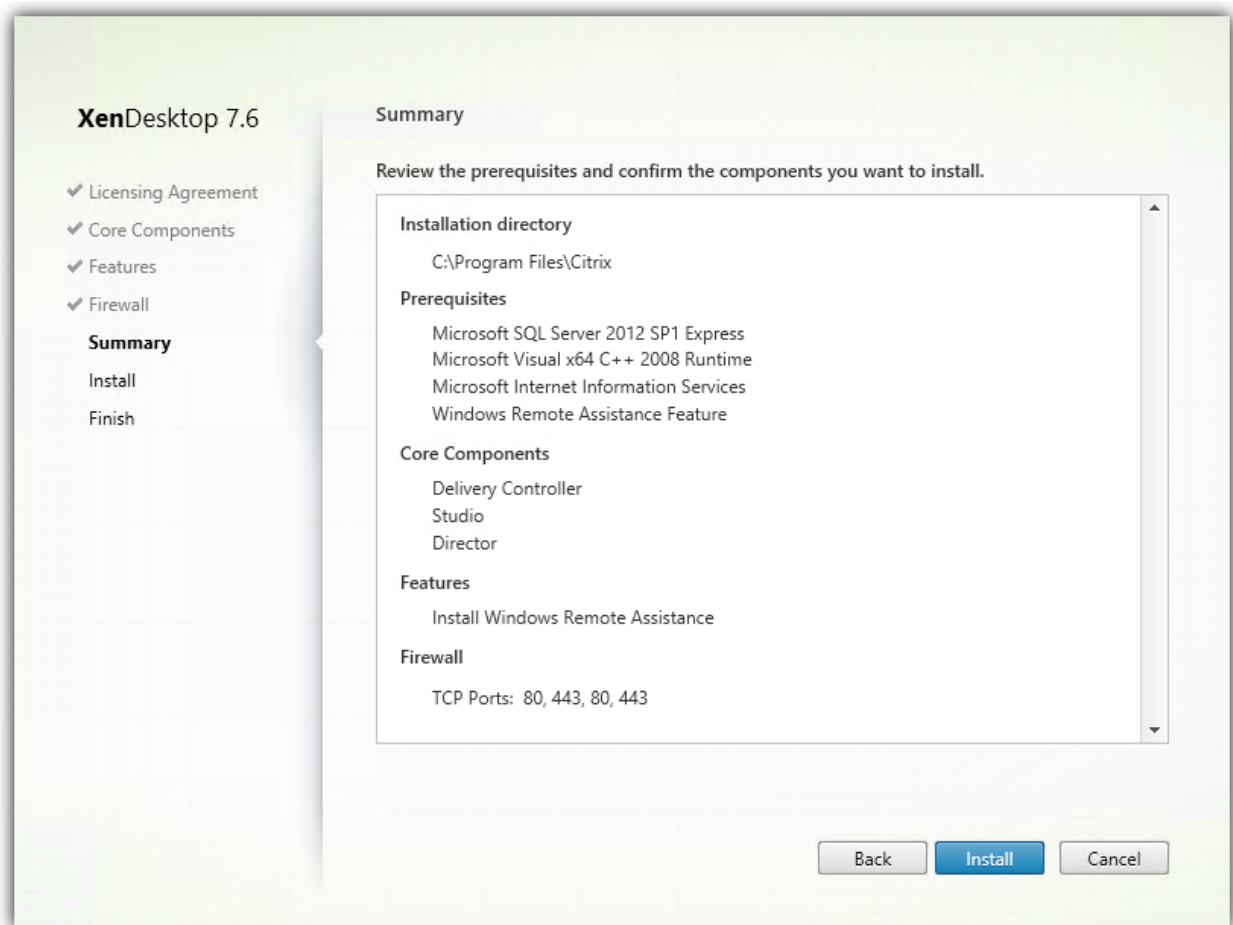


6. Click **Next**.
7. Leave Firewall settings at default as displayed below.

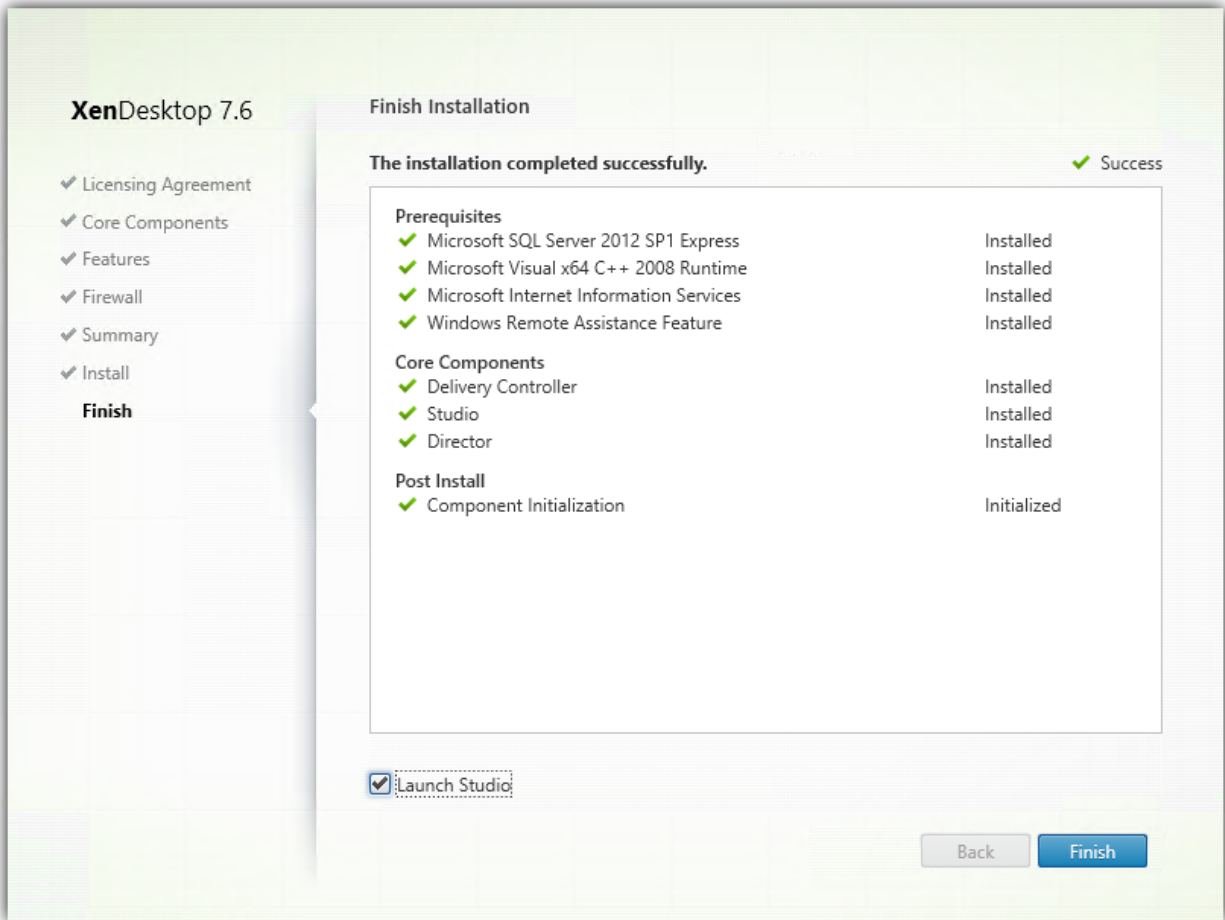


8. Click **Next**.

9. Then click **Install**.



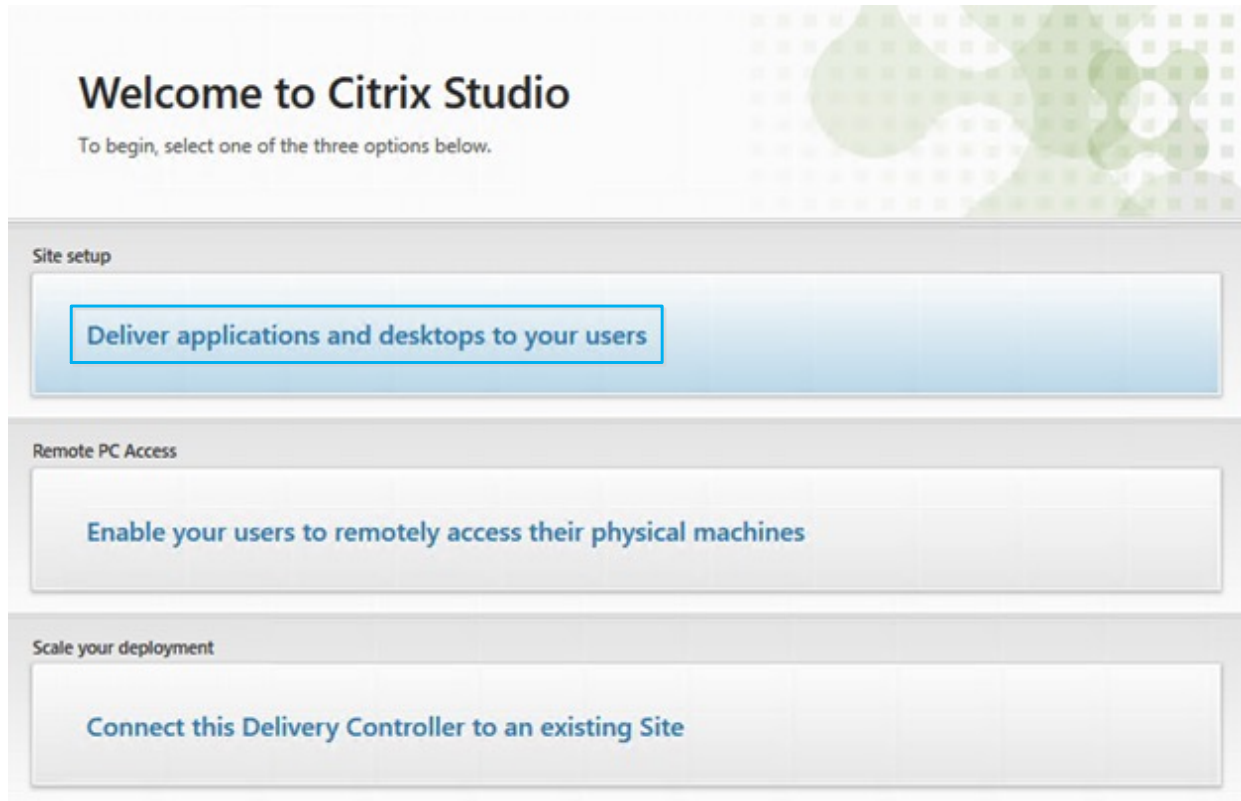
10. Click **Finish**.



Site setup

Configuration

1. When Citrix Studio is launched for the first time, the following is displayed:



2. Click Deliver applications and desktops to your users.

The Site Setup Wizard opens:

The screenshot shows the 'Site Setup' window in Citrix Studio. On the left is a navigation pane with the following items: Studio, Introduction (selected), Database, Licensing, Connection, Network, Storage, App-V Publishing, and Summary. The main area is titled 'Introduction' and contains the following text: 'You have two options when creating a new Site. The simplest option is to automatically create a fully configured, production-ready Site. The second, more advanced option is to create an empty Site, which you must configure yourself.' Below this text is the question 'What kind of Site do you want to create?' with two radio button options: 'A fully configured, production-ready Site (recommended for new users)' (which is selected) and 'An empty, unconfigured Site'. Below the radio buttons is a text field labeled 'Site name:' containing the text 'Columbia'. At the bottom right of the window are three buttons: 'Back', 'Next' (highlighted in blue), and 'Cancel'.

3. Select **A fully configured, production-ready Site**, and give the Site a name. Click **Next**.
4. Leave Database settings at default. Click **Next**.

The screenshot shows the 'Site Setup' wizard in Citrix Studio. On the left, a navigation pane lists steps: Introduction (checked), Database (selected), Licensing, Connection, Network, Storage, App-V Publishing, and Summary. The main area is titled 'Database' and contains the following text: 'The database stores all Site configuration, logging, and monitoring data.' Below this, there are two input fields: 'Database server location:' with the value '.\SQLEXPRESS' and 'Database name:' with the value 'CitrixColumbia'. To the right of the 'Database name' field is a 'Test connection...' button. Below these fields, there is a note: 'If you do not have permission to edit this database, generate a script to give to your database administrator.' and a 'Generate database script...' button followed by '(Optional)'. At the bottom right of the wizard are three buttons: 'Back', 'Next' (highlighted in blue), and 'Cancel'.

The following message is displayed:

The screenshot shows a message box titled 'Studio'. It contains a question mark icon and the text: 'No database was found on the database server.' Below this, it says: 'Click OK if you want Studio to create the database automatically.' Further down, there is a paragraph: 'If your Studio user credentials do not include the required server/database role permissions, and you configured SQL Server to allow access to a Windows user account with required permissions, you will be asked for those credentials. (Windows authentication is required; you cannot authenticate if you configured an explicit username and password on the SQL Server.)' At the bottom, it says: 'Alternatively, if you would prefer to use the database schema to create a database, click Cancel.' At the bottom right of the message box are two buttons: 'OK' (highlighted in blue) and 'Cancel'.

5. Click OK.
6. In the licensing step that follows, enter your license server details. (In the test environment, the Citrix XenDesktop Platinum Product with User/Device Model is used.)

I want to:

☐ Use the free 30-day trial
You can add a license later.

☒ Use an existing license
The product list below is generated by the license server.

Product	Model
☐ Citrix XenApp Platinum	Concurrent
☒ Citrix XenDesktop Platinum	User/Device
☐ Citrix XenDesktop App	Concurrent
☐ Citrix XenDesktop Enterprise	User/Device
☐ Citrix XenApp Advanced	Concurrent

 You have "read only" access to the license server. To add licenses, contact your license server administrator.

7. Click **Next**.
8. For Connection type, select **No machine management**, and click **Next**.

Site Setup

Studio

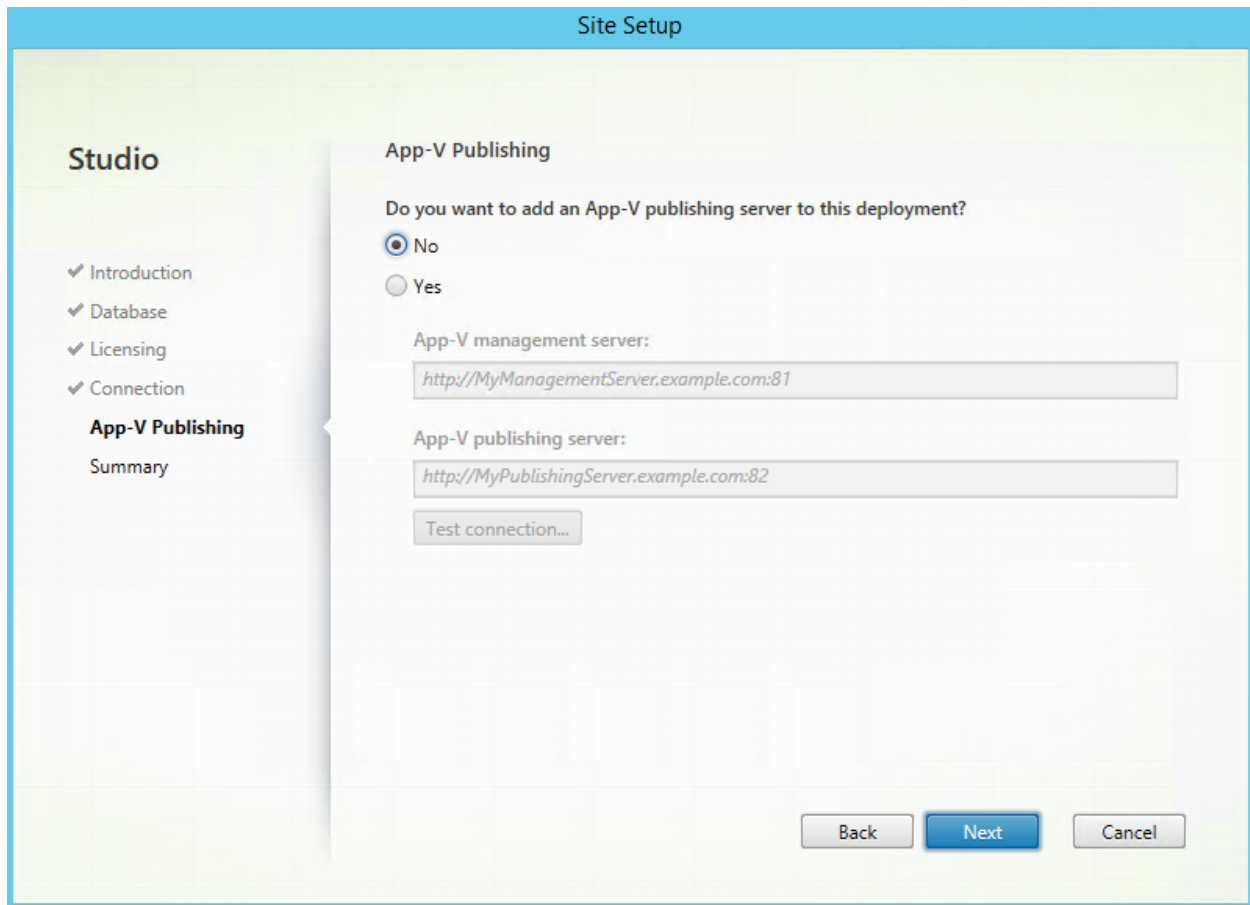
- ✓ Introduction
- ✓ Database
- ✓ Licensing
- Connection**
- App-V Publishing
- Summary

Connection

Select a Connection type. If machine management is not used (for example when using physical hardware), select 'No machine management.'

Connection type: No machine management

9. Keep the default App-V Settings. Click **Next**.



The image shows the 'Site Setup' window with the 'App-V Publishing' tab selected. On the left, a 'Studio' sidebar lists steps: Introduction, Database, Licensing, Connection, App-V Publishing (selected), and Summary. The main area asks 'Do you want to add an App-V publishing server to this deployment?' with 'No' selected. Below are fields for 'App-V management server' (http://MyManagementServer.example.com:81) and 'App-V publishing server' (http://MyPublishingServer.example.com:82), followed by a 'Test connection...' button. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

Site Setup

Studio

- ✓ Introduction
- ✓ Database
- ✓ Licensing
- ✓ Connection
- App-V Publishing**
- Summary

App-V Publishing

Do you want to add an App-V publishing server to this deployment?

☒ No

☐ Yes

App-V management server:

http://MyManagementServer.example.com:81

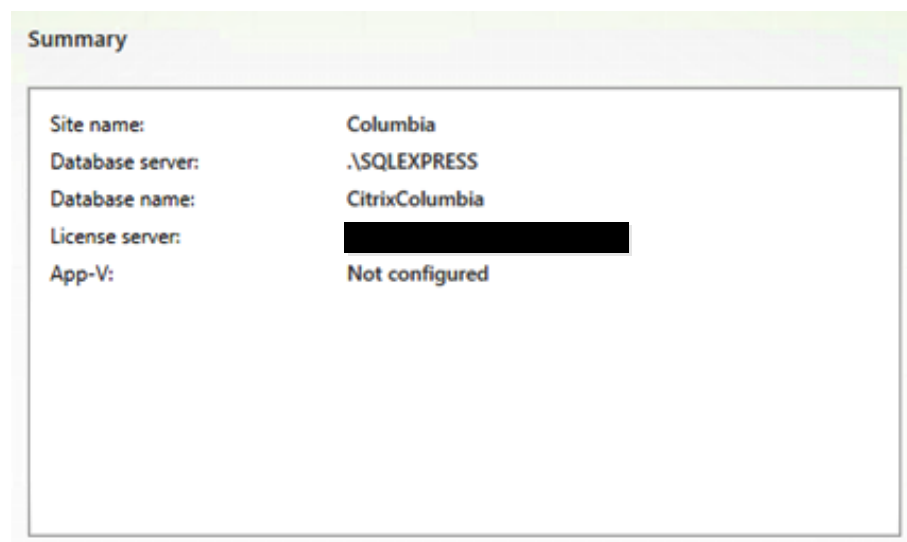
App-V publishing server:

http://MyPublishingServer.example.com:82

Test connection...

Back Next Cancel

A summary will be displayed.



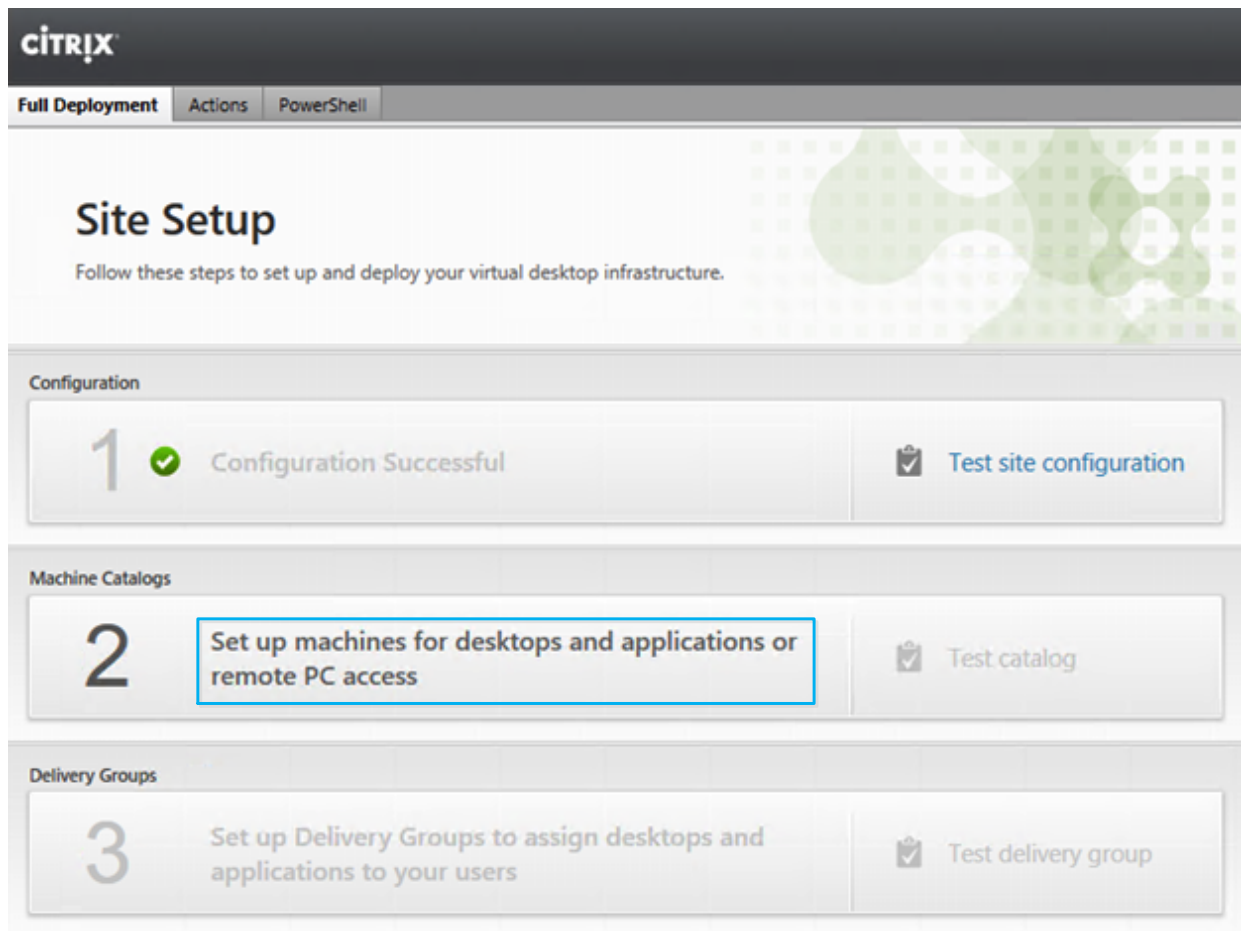
The image shows the 'Summary' window with a table of configuration details.

Summary

Site name:	Columbia
Database server:	.\SQLEXPRESS
Database name:	CitrixColumbia
License server:	[REDACTED]
App-V:	Not configured

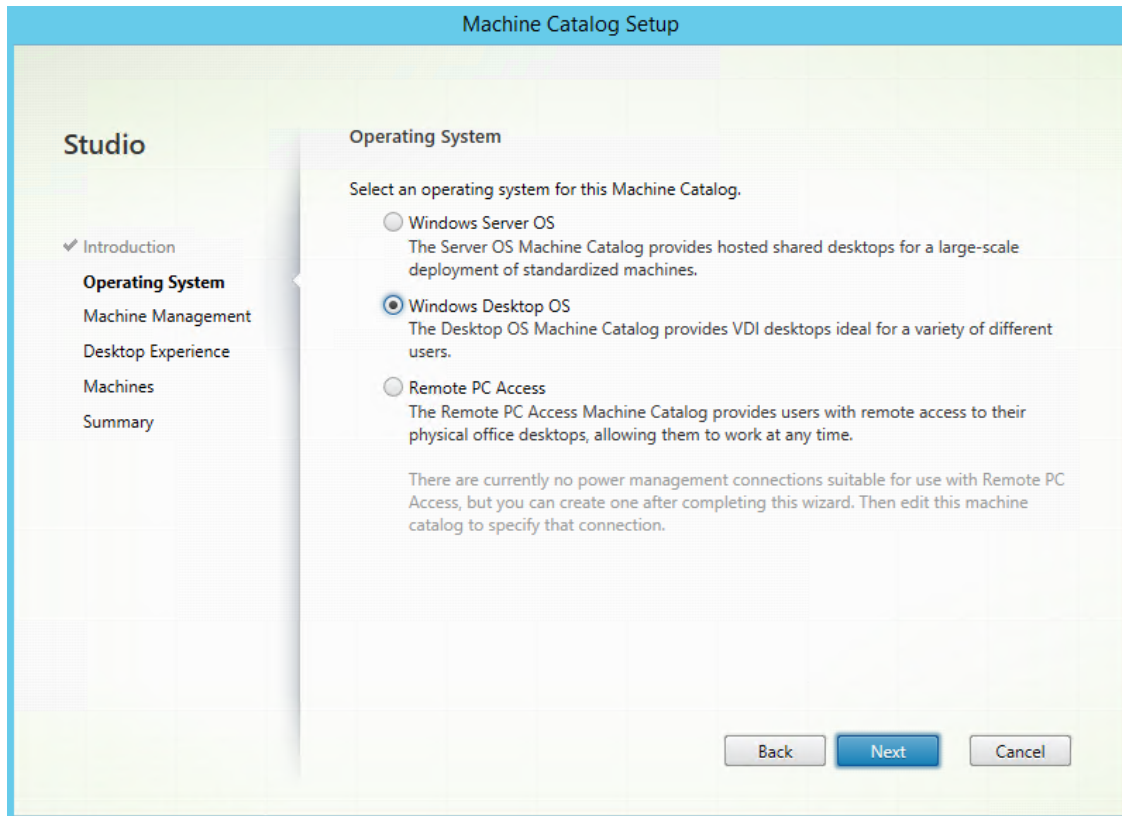
10. Click **Finish**.

When the process is complete, the following will be displayed:

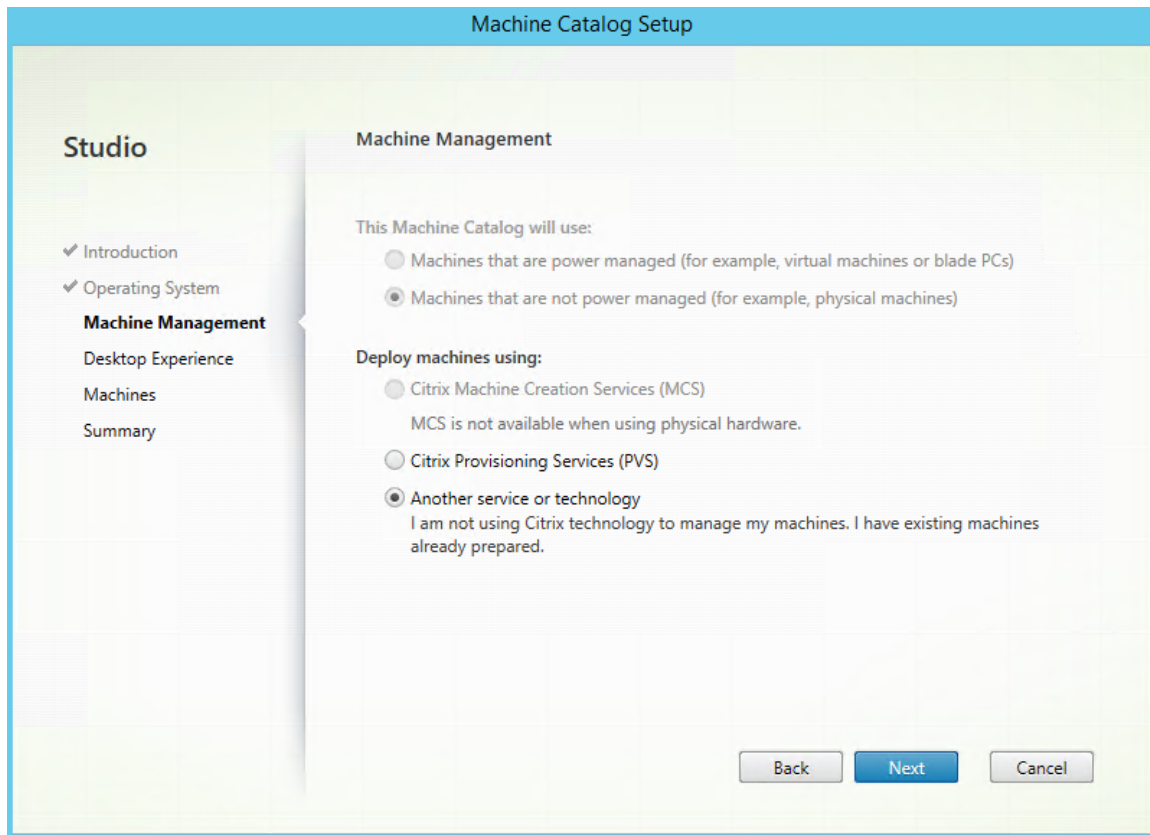


Machine Catalogs

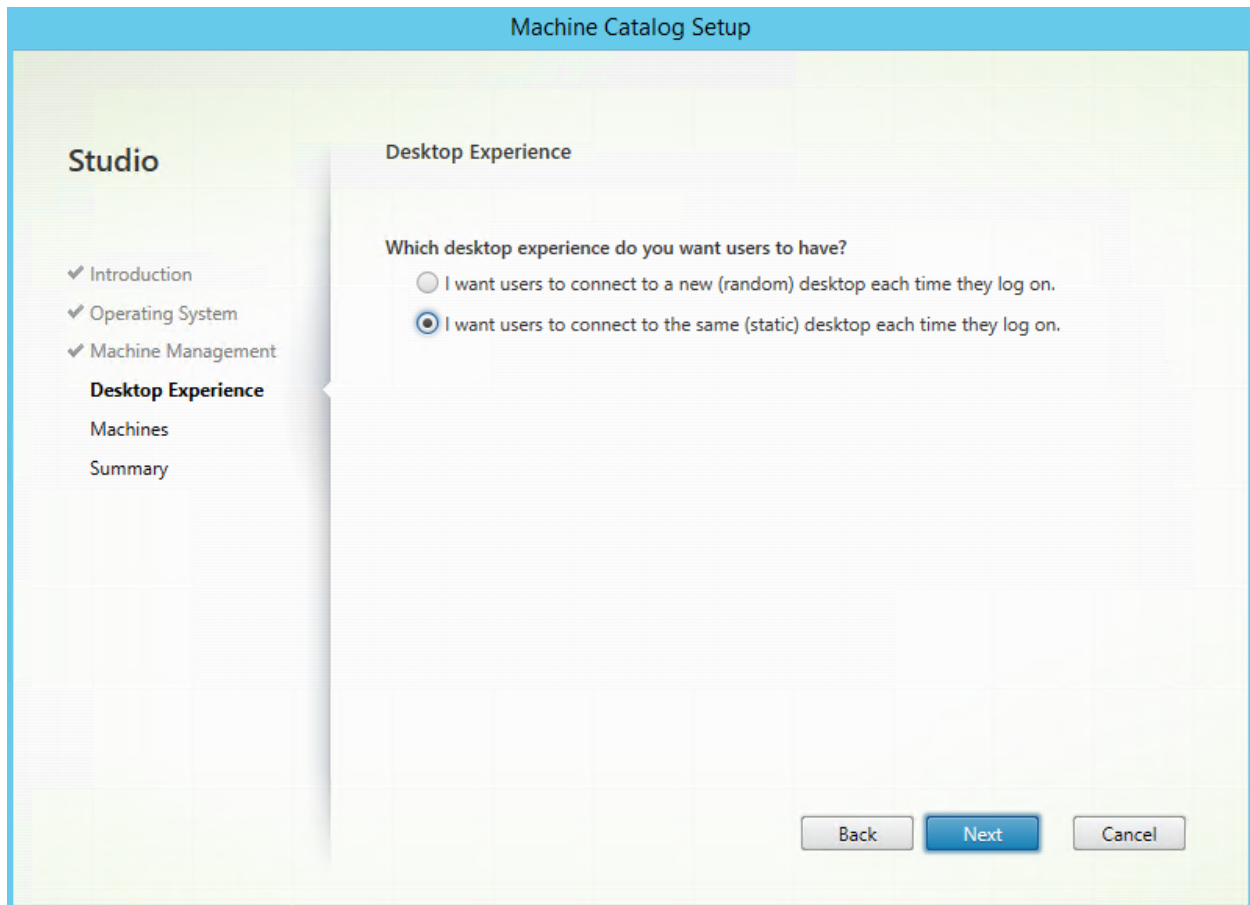
1. Click **Set up machines for desktops and applications or remote PC access**.
2. In the Operating System step, select **Windows Desktop OS**. Click **Next**.



3. In the Machine Management step, select **Another service or technology**. Click **Next**.



4. In the Desktop Experience step, select I want users to connect to the same (static) desktop each time they log on. Click Next.



NOTE

For the purpose of this guide, choose static because only one VDA is configured in the test environment.

5. In the Machines and Users step, select the Computer AD account for the VDA that you prepared in section [Virtual Delivery Agent \(VDA\)](#). Choose 7.6 as the VDA version installed from the drop-down list. Click **Next**.

The screenshot shows the 'Machine Catalog Setup' wizard in Citrix Studio. The left sidebar shows the 'Studio' navigation pane with the following items: Introduction, Operating System, Machine Management, Desktop Experience, **Machines and Users** (selected), and Summary. The main area is titled 'Machines and Users' and contains the following content:

Import or add machine accounts and optionally assign to users:

Computer AD account	User names
F2\A-V764-2\$	-

Below the table are buttons: Remove, Import list..., Export list..., and Add computers....

Select the VDA version installed on these machines:

7.6 (recommended, to access the latest features)

Machines will require the selected VDA version (or newer) in order to register in Delivery Groups that reference this machine catalog. [Learn more](#)

At the bottom are buttons: Back, Next, and Cancel.

6. In the Summary step, enter an appropriate machine catalog name. Click **Finish**.

Machine Catalog Setup

Studio

- ✓ Introduction
- ✓ Operating System
- ✓ Machine Management
- ✓ Desktop Experience
- ✓ Machines and Users
- Summary**

Summary

Machine type:	Windows Desktop OS
Machine management:	Physical
Provisioning method:	Another service or technology
Desktop experience:	Users connect to the same desktop each time they log on
Number of machines added:	1
VDA version:	7.6 (recommended, to access the latest features)
Scopes:	-

Machine Catalog name:

Windows 7 x64 MCat

Machine Catalog description for administrators: (Optional)

Windows 7 x64 CatDesc

To complete the deployment, assign this Machine Catalog to a Delivery Group by selecting Delivery Groups and then Create or Edit a Delivery Group.

Back Finish Cancel

You will be returned to the Site Setup screen:

Site Setup

Follow these steps to set up and deploy your virtual desktop infrastructure.

Configuration

1  Configuration Successful

 [Test site configuration](#)

Machine Catalogs

2  Catalog created successfully

 [Test catalog](#)

Delivery Groups

3

Set up Delivery Groups to assign desktops and applications to your users

 [Test delivery group](#)

Delivery Groups

1. Click Set up Delivery Groups to assign desktops and applications for your users.
2. In the Machines step, the machine catalog you created earlier will be listed. Increment the number of machines for the delivery group to 1, and click **Next**.

Create Delivery Group

Studio

- ✓ Introduction
- Machines**
- Delivery Type
- Users
- StoreFront
- Summary

Machines

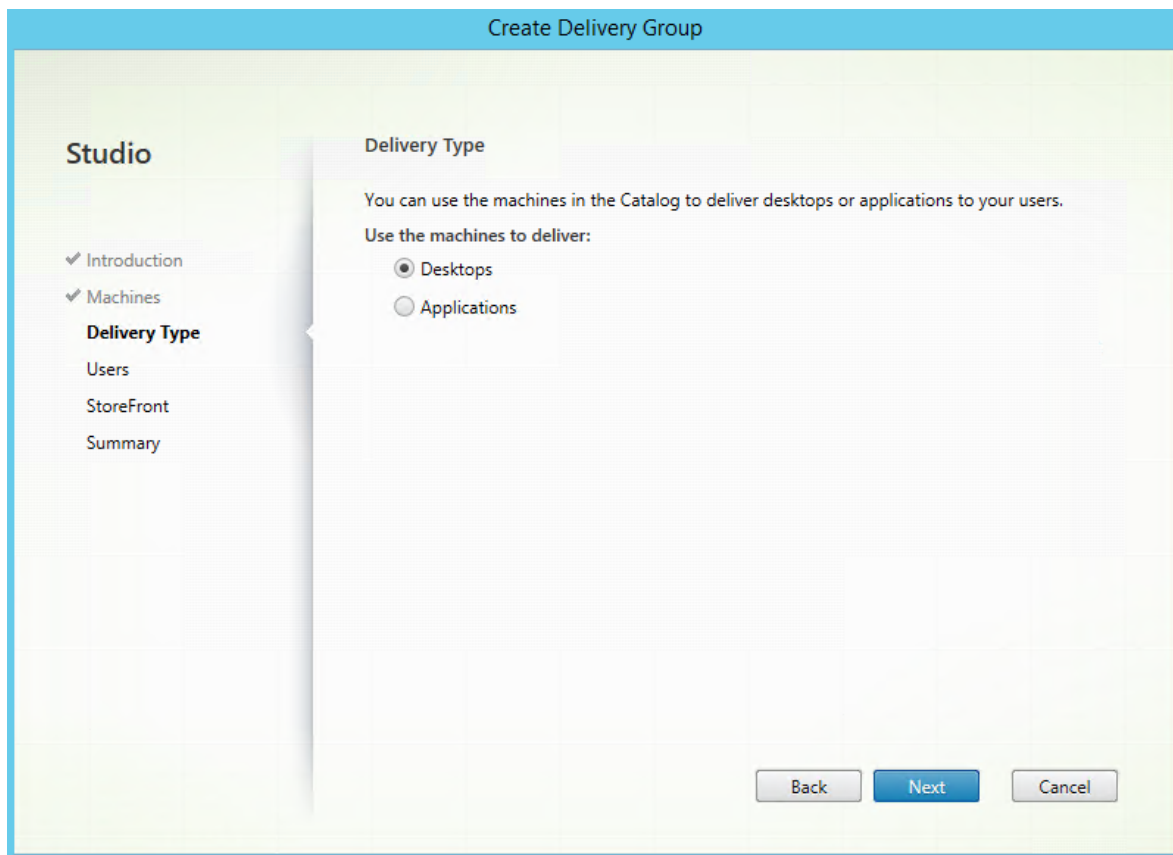
Select a Machine Catalog. The Type column is a summary of choices made when the Catalog was created.

Catalog	Type	Machines
☒ Windows 7 x64 MCat	VDI Manual Static Local Disk	1
Windows 7 x64 CatDesc		

Choose the number of machines for this Delivery Group: - +

Back Next Cancel

3. In the Delivery Type step, choose **Desktops** and click **Next**.



4. In the Users step, Click **Add** and then enter the group name (G-Scope Smartcard Group) you created earlier in section [Add user to G-Scope Smartcard Group](#) of which the PIV card user is a member. Click **Next**.

The screenshot shows the 'Create Delivery Group' wizard in Citrix Studio. The left sidebar is titled 'Studio' and contains a list of steps: Introduction, Machines, Delivery Type, Users (selected), StoreFront, and Summary. The main area is titled 'Users' and contains the following text: 'Specify who can use the applications and desktops in this Delivery Group. You can assign users and user groups who log on with valid credentials.' Below this text is a section labeled 'Assign users:' with a text box containing 'F2\G-Scope Smartcard Group'. At the bottom of the text box are 'Add...' and 'Remove' buttons. At the bottom of the wizard are 'Back', 'Next', and 'Cancel' buttons.

5. In the StoreFront step, choose **Manually**. Click **Next**

Create Delivery Group

Studio

- ✓ Introduction
- ✓ Machines
- ✓ Delivery Type
- ✓ Users
- StoreFront**
- Summary

StoreFront

You can configure Receiver on the machines in this Delivery Group so that users can access additional applications that aren't on the machines. Receiver can use a different StoreFront server (that you select here or in the Configuration > StoreFront node) compared with the servers (listed in the Citrix StoreFront console) used for connections to the machines themselves.

How do you want to configure Receiver on the machines in this Delivery Group?

☒ Manually, using a StoreFront server address that I will provide later

☐ Automatically, using the StoreFront servers selected below

Select the StoreFront servers for Receiver:

No StoreFront servers have been added.
Add a StoreFront server.

Add new...

Back Next Cancel

NOTE

Configuring Receiver on the machines in this Delivery Group relates to double-hop scenarios, which are beyond the scope of the first edition of this guide.

6. In the Summary step, enter appropriate names, and click **Finish**.

The screenshot shows the 'Create Delivery Group' wizard in Citrix Studio, specifically the 'Summary' step. On the left, the 'Studio' pane shows a navigation tree with 'Introduction', 'Machines', 'Delivery Type', 'Users', 'StoreFront', and 'Summary' (selected). The main area displays a summary of the configuration and fields for naming the delivery group.

Summary	
Machine Catalog:	Windows 7 x64 MCat
Machine type:	Windows Desktop OS
Allocation type:	Static
Machines added:	1 unassigned
Delivery type:	Desktops
Users:	F2\G-Scope Smartcard Group
Scopes:	-

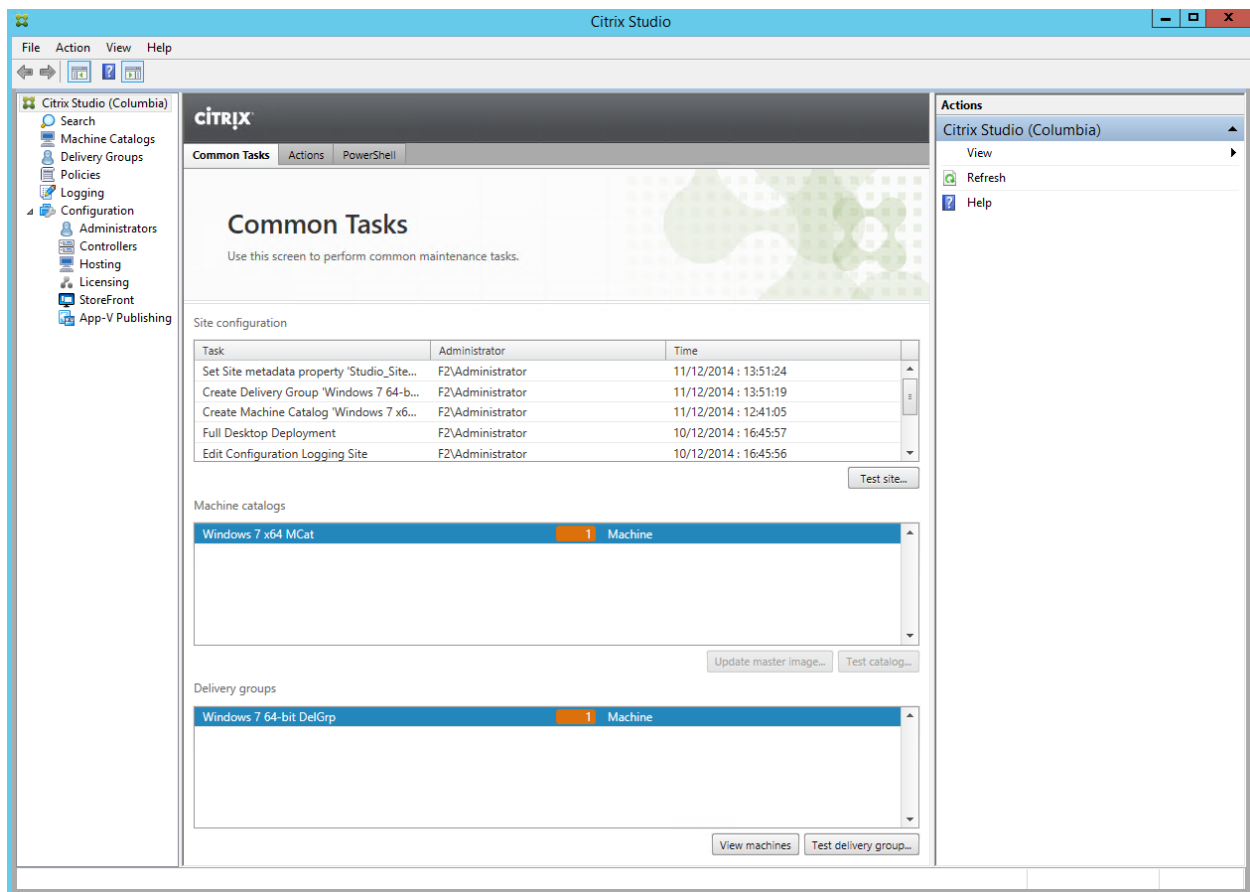
Delivery Group name:

Display name:

Delivery Group description, used as label in Receiver (optional):

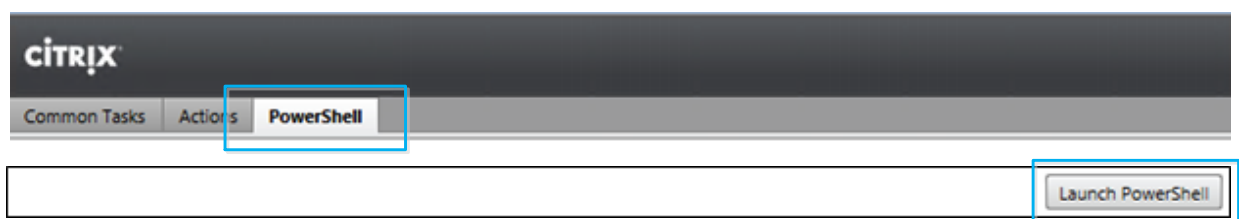
At the bottom right, there are three buttons: 'Back', 'Finish' (highlighted in blue), and 'Cancel'.

The following will be displayed:



Set XML Service to trust requests

1. Click the **PowerShell** tab. Then click the **Launch PowerShell** button at the bottom right:



2. Enter the following to verify the Citrix cmdlets are available:

```
asnp Citrix*
```

3. Run the following command to set trust:

```
Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
```

4. Run the following command to verify that the trusts are set to true:

```
Get-BrokerSite
```

5. Verify that TrustRequestsSentToTheXmlServicePort=True:

```
PS C:\Program Files\Citrix\Desktop Studio> asnp Citrix*
PS C:\Program Files\Citrix\Desktop Studio> Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
PS C:\Program Files\Citrix\Desktop Studio> Get-BrokerSite

BaseOU                                     :
BrokerServiceGroupUid                     : 6af0c487-dbf5-48cc-a91a-291533a2a170
ColorDepth                                : TwentyFourBit
ConfigurationServiceGroupUid              : 68314c9c-415c-4d2e-a81f-a1670e08c6a9
ConnectionLeasingEnabled                   : True
DesktopGroupIconUid                       : 1
DnsResolutionEnabled                      : False
LicenseEdition                            : PLT
LicenseGraceSessionsRemaining              :
LicenseModel                              : UserDevice
LicenseServerName                         :
LicenseServerPort                         : 27000
LicensedSessionsActive                     : 0
LicensingBurnIn                           : 2014.0815
LicensingBurnInDate                       : 15/08/2014 01:00:00
LicensingGraceHoursLeft                   :
LicensingGracePeriodActive                 : False
LicensingOutOfBoxGracePeriodActive         : False
MetadataMap                               : {}
Name                                       : Columbia
SecureIcaRequired                         : False
TrustRequestsSentToTheXmlServicePort      : True

PS C:\Program Files\Citrix\Desktop Studio> _
```

StoreFront

Test environment assumptions

- Operating system is Windows Server is 2012 R2.
- Citrix StoreFront is version 2.6.0.5031 (XenDesktop version 7.6.0.5026).
- StoreFront runs on a dedicated server (Not installed on the same server as the Delivery Controller).

Prerequisites

- The StoreFront server trusts your organization's root and intermediate certificate authorities. In other words, copies of the CA certificates for your organization's root and issuing certificate authorities are located in the StoreFront server's Local Computer Trusted Root Certification Authorities and Intermediate Certification Authorities stores, respectively.
- Microsoft Internet Information Services (IIS) is installed on the StoreFront server, which possesses a server certificate with corresponding private key, and the server certificate is used to bind https to port 443 in IIS.

NOTE

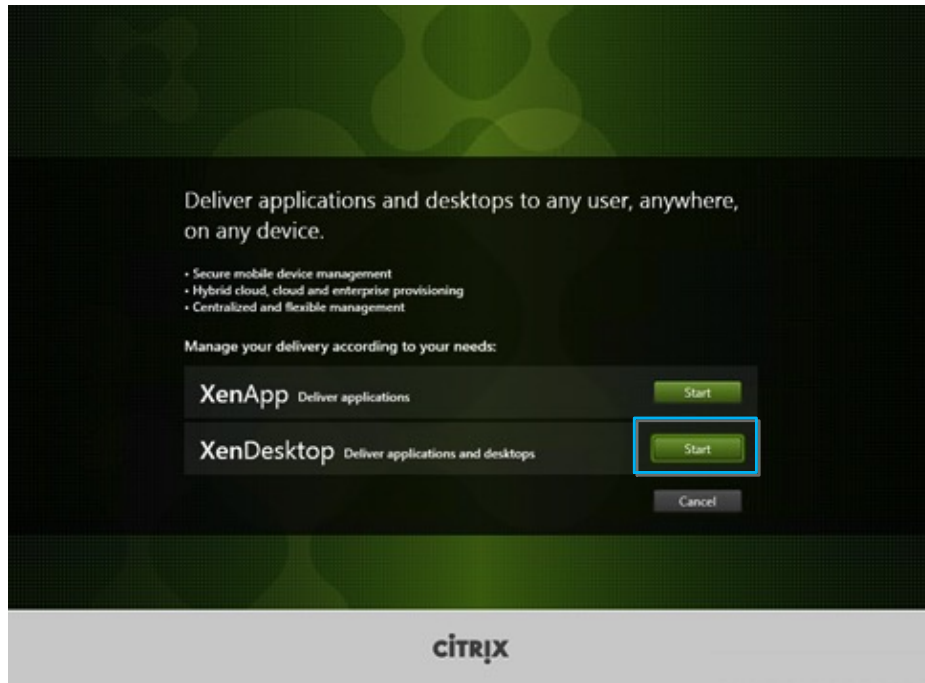
There is currently a known issue with NetScaler that could impact StoreFront configuration (introduced in NetScaler build 10.5.53.9). NetScaler Gateway sends its own virtual server hostname (in the test environment "fed-nsg.f2.ctxs" (instead of the StoreFront hostname: "a-sf.f2.ctxs") as host header to StoreFront in the http host header field. This may result in the IIS that is hosting StoreFront to return an http 404: Not Found error to the NetScaler. In order to prevent this, ensure that the host name field in the Site Binding in IIS on the StoreFront server is blank. (See below). A fix for the issue is planned to release in NetScaler 11.

The screenshot shows the 'Edit Site Binding' dialog box. The 'Type' dropdown is set to 'https'. The 'IP address' dropdown is set to 'All Unassigned'. The 'Port' text box contains '443'. The 'Host name' text box is empty and is highlighted with a red rectangle. Below the 'Host name' field is a checkbox labeled 'Require Server Name Indication' which is unchecked. At the bottom, the 'SSL certificate' dropdown is set to 'webserver exp key'. To the right of this dropdown are 'Select...' and 'View...' buttons. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

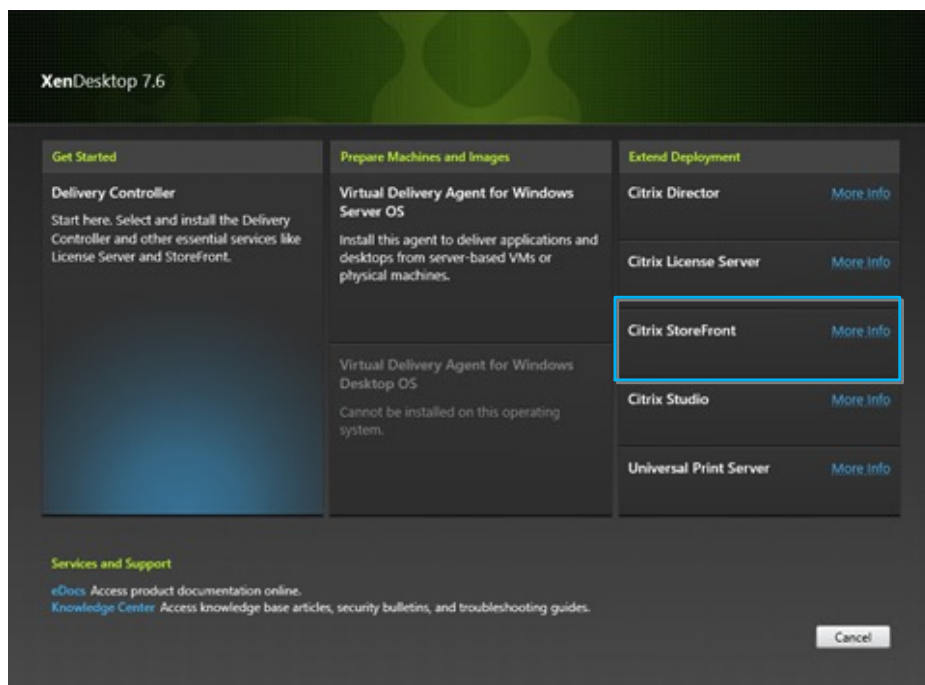
Configuration Steps

StoreFront installation

1. Start the installation media, and click **Start** for XenDesktop.

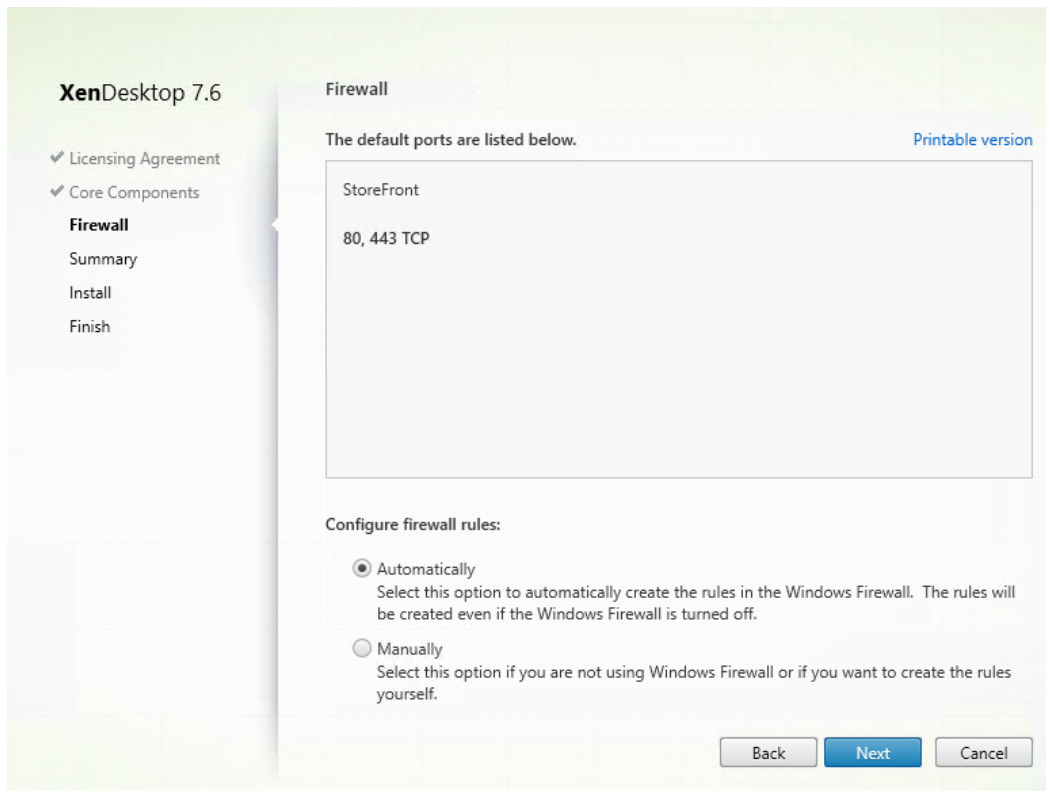


2. Click Citrix StoreFront in the Extend Deployment section.

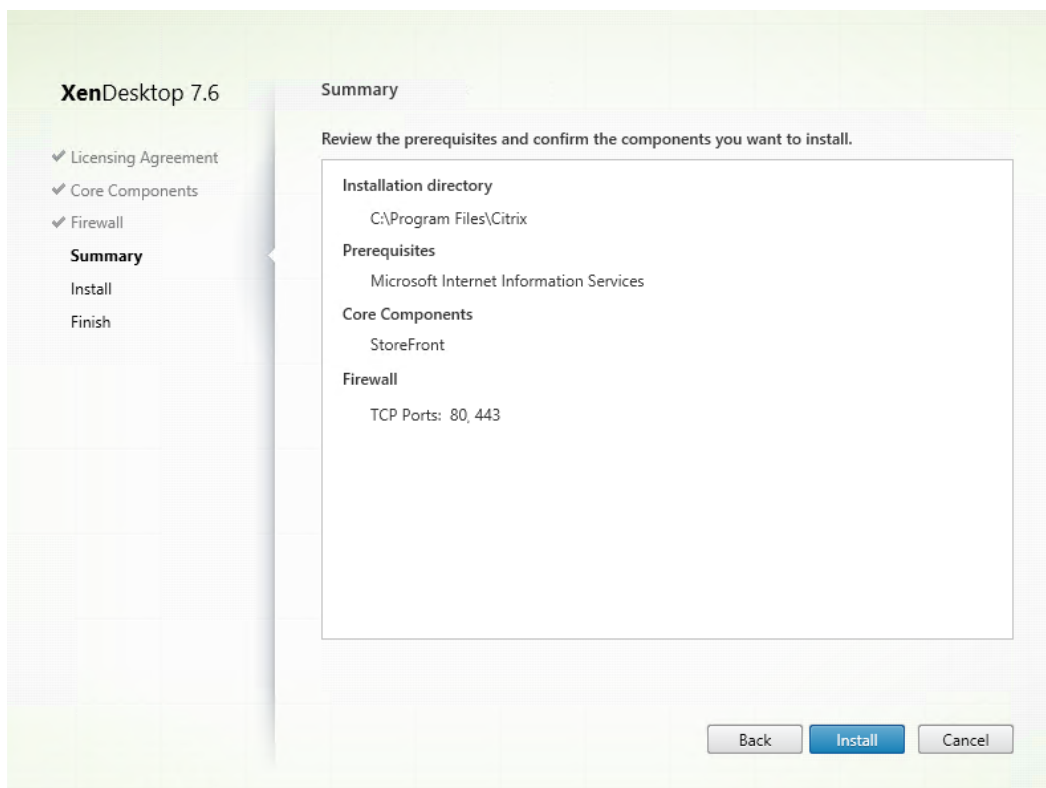


3. In the Core Components step, StoreFront is shown as a required mandatory option. Click **Next**.

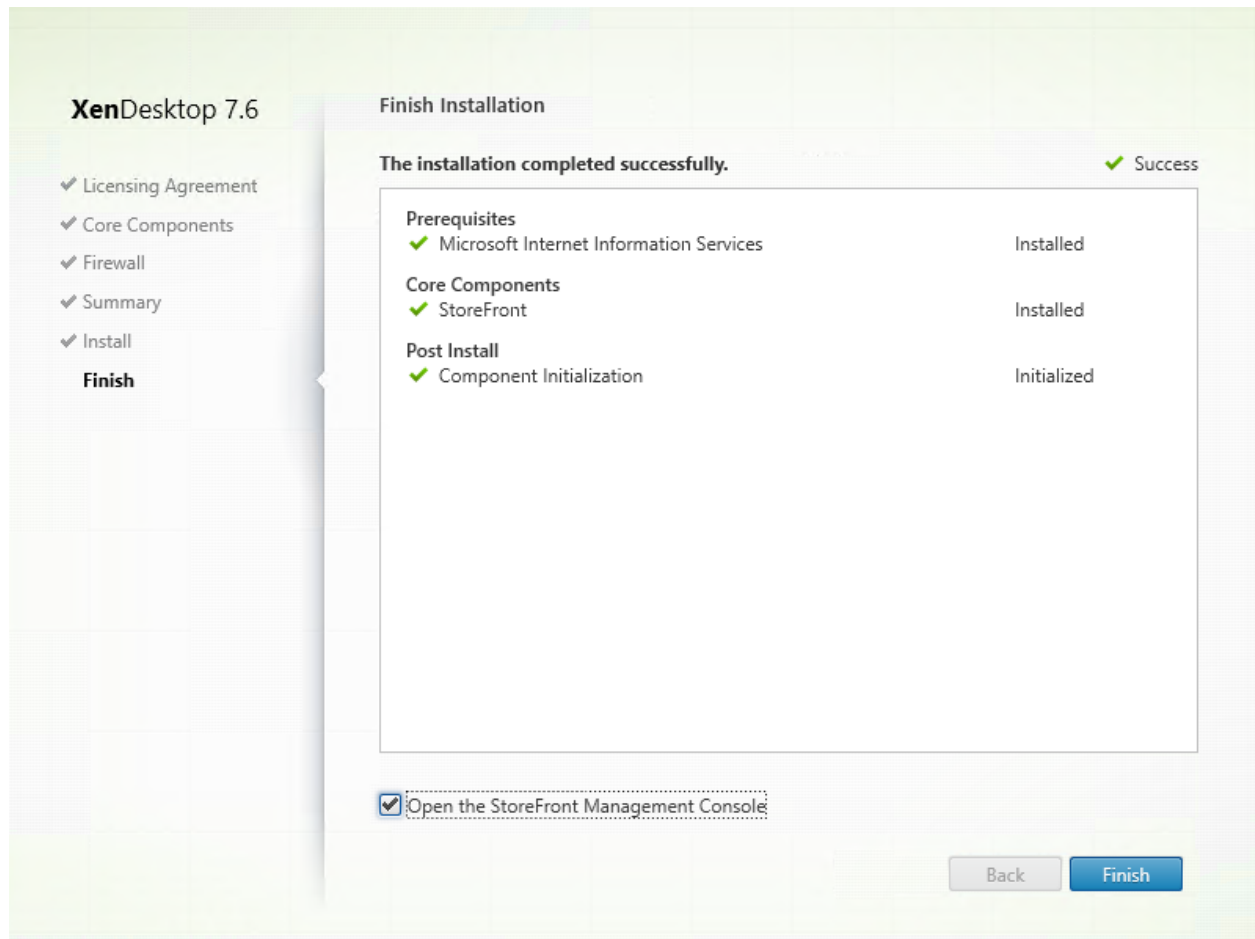
4. In the Firewall step, choose **Automatically**, and click **Next**.



5. In the Summary step, click **Install**.



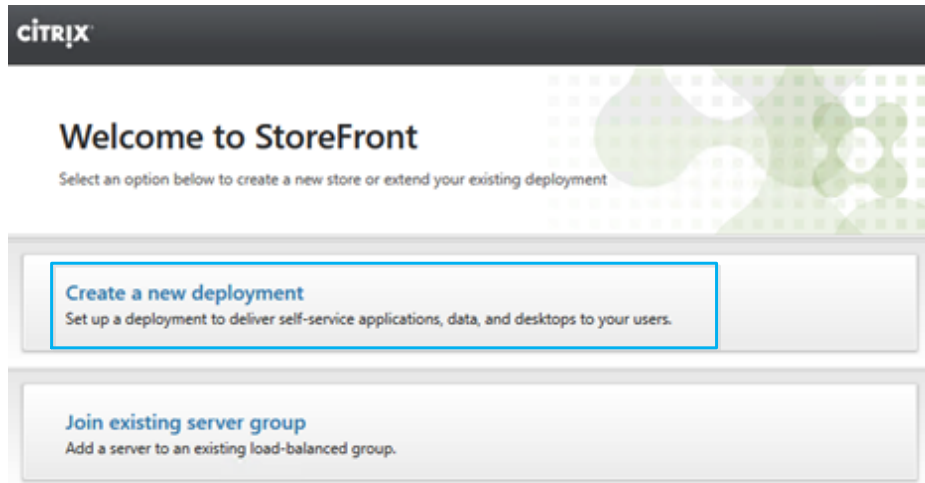
6. Once installation completes successfully, click **Finish**.



Configure StoreFront

Create a new deployment

1. Click Create new deployment:



The Create New Deployment wizard opens.

2. In the Base URL step, the FQDN of the server on which StoreFront is installed will be displayed. You can leave the default Base URL as is. Click **Next**.

Create New Deployment

StoreFront

Base URL

Store Name

Delivery Controllers

Remote Access

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.

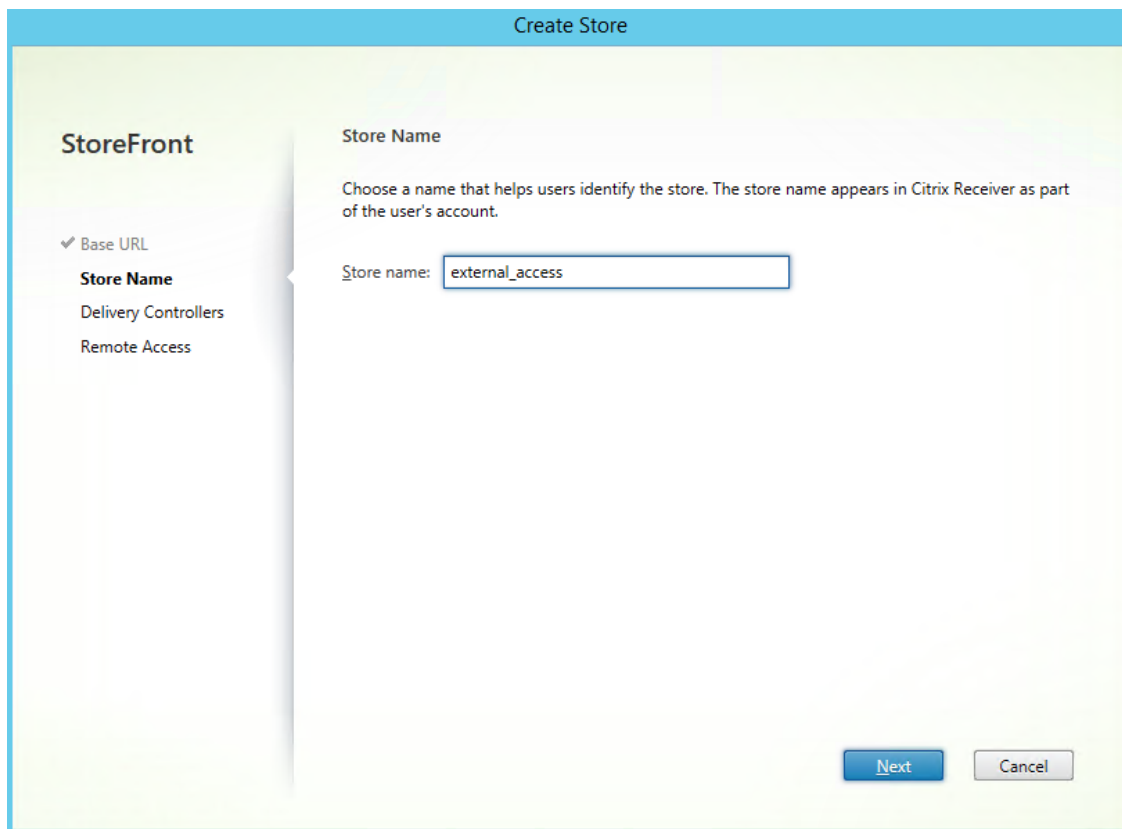
Base URL:

Next **Cancel**

NOTE

The test environment assumes that there is only one StoreFront server. In cases where there are multiple StoreFront servers with a load balancer in front of them, the base URL should be the FQDN of the load balancer, not the StoreFront server.

3. In the Store Name step, enter **external_access** in the Store Name field. Click **Next**.

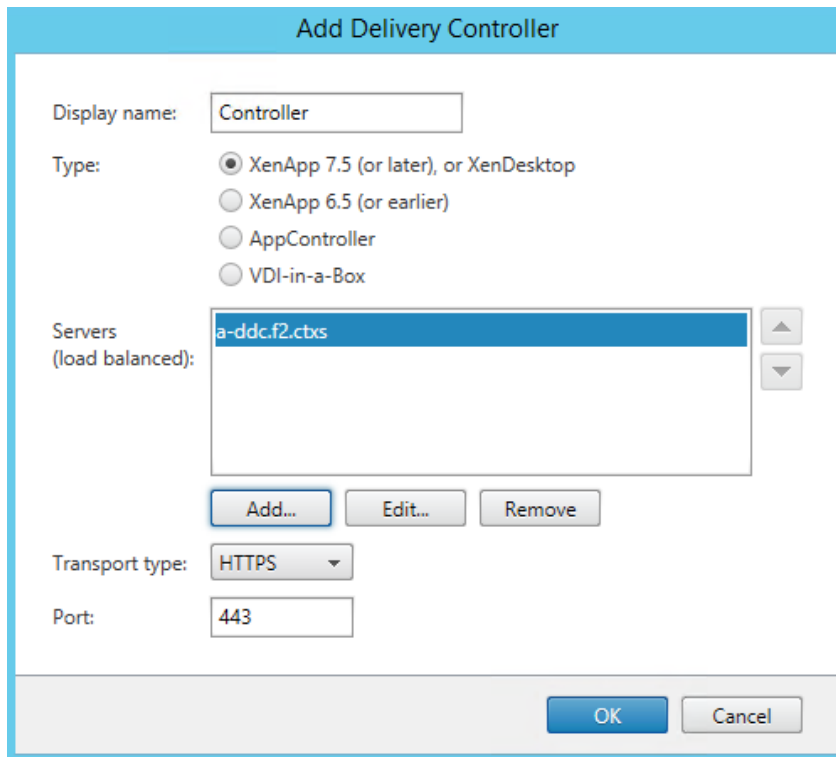


The screenshot shows the 'Create Store' wizard in Citrix StoreFront. The title bar is 'Create Store'. On the left, under the 'StoreFront' header, there is a sidebar with the following items: 'Base URL' (checked), 'Store Name' (selected), 'Delivery Controllers', and 'Remote Access'. The main area is titled 'Store Name' and contains the instruction: 'Choose a name that helps users identify the store. The store name appears in Citrix Receiver as part of the user's account.' Below this, there is a text input field labeled 'Store name:' with the value 'external_access' entered. At the bottom right, there are two buttons: 'Next' and 'Cancel'.

NOTE

This store will be for external access through NetScaler Gateway.

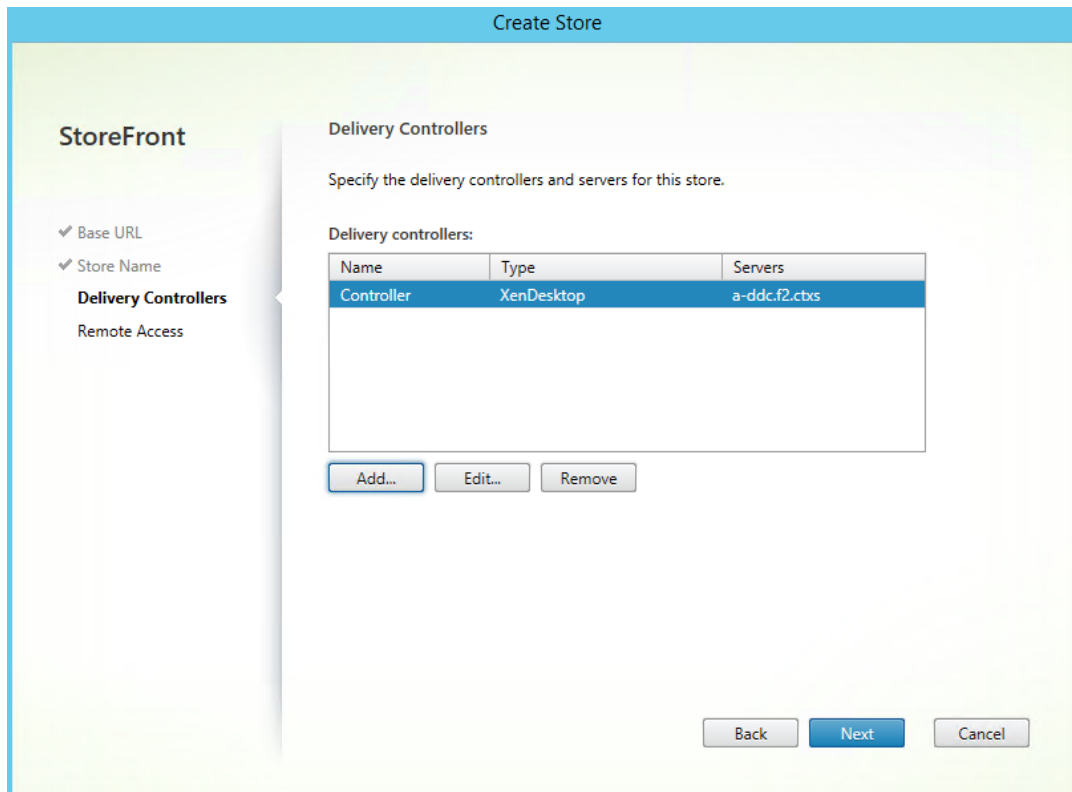
4. In the Delivery Controllers step, click **Add**. Enter the information as shown below, and click **OK**.



The "Add Delivery Controller" dialog box is shown. It has a title bar "Add Delivery Controller". Inside, there are several fields and buttons:

- Display name:** A text box containing "Controller".
- Type:** A group of four radio buttons:
 - ☒ XenApp 7.5 (or later), or XenDesktop
 - ☐ XenApp 6.5 (or earlier)
 - ☐ AppController
 - ☐ VDI-in-a-Box
- Servers (load balanced):** A list box containing "a-ddc.f2.ctxs". To the right of the list box are up and down arrow buttons.
- Below the list box are three buttons: "Add...", "Edit...", and "Remove".
- Transport type:** A dropdown menu showing "HTTPS".
- Port:** A text box containing "443".
- At the bottom right are "OK" and "Cancel" buttons.

5. Click **Next**.



The "Create Store" dialog box is shown. It has a title bar "Create Store". On the left is a "StoreFront" sidebar with a tree view containing:

- Base URL (checked)
- Store Name (checked)
- Delivery Controllers** (selected)
- Remote Access

The main area is titled "Delivery Controllers" and contains the text "Specify the delivery controllers and servers for this store." Below this is a section "Delivery controllers:" containing a table:

Name	Type	Servers
Controller	XenDesktop	a-ddc.f2.ctxs

Below the table are "Add...", "Edit...", and "Remove" buttons. At the bottom right are "Back", "Next", and "Cancel" buttons.

6. In the Remote Access step, select **No VPN tunnel**, and click **Add**.

The screenshot shows the 'Create Store' wizard in the Citrix management console. The 'Remote Access' step is active, showing options for remote access. The 'Remote access' section has three radio buttons: 'None', 'No VPN tunnel' (selected), and 'Full VPN tunnel'. Below this is a section for 'NetScaler Gateway appliances' with an empty list and an 'Add...' button. At the bottom, there is a 'Default appliance' dropdown menu. The 'StoreFront' sidebar on the left shows the progress: 'Base URL', 'Store Name', 'Delivery Controllers', and 'Remote Access' (highlighted). At the bottom right are 'Back', 'Create', and 'Cancel' buttons.

7. For the next step, you will require knowledge of how you plan to configure your NetScaler Gateway. (NetScaler Gateway configuration is described in detail in section [NetScaler Gateway](#).)
- NetScaler Gateway URL: The FQDN of the NetScaler Gateway virtual server to which external users outside the network will connect. The endpoint must be able to resolve the IP address that corresponds to this FQDN from an external DNS server.
 - Version: Choose 10.0 (Build 69.4) or later.
 - Subnet IP address: This is the NetScaler's SNIP.
 - Logon type: Choose Smart card.
 - Smart card fallback: Select None.
 - Callback URL: The FQDN of the NetScaler Gateway virtual callback server. The callback server is only accessed by the StoreFront server and not directly by users. The StoreFront server must be able to resolve the IP address that corresponds to the callback server's FQDN from an internal DNS server. The callback URL cannot be the same as the NetScaler Gateway URL, especially when smart card authentication is used. Each of the two respective URLs (NetScaler Gateway and Callback) must belong to two **different** virtual servers that will be created on the NetScaler Gateway.
8. Click **Next**.

Add NetScaler Gateway Appliance

StoreFront

General Settings

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

Display name: NetScaler Gateway

NetScaler Gateway URL: https://fed-nsg.f2.ctxs

Version: 10.0 (Build 69.4) or later

Subnet IP address (optional): 10.217.205.75

Logon type: Smart card ⚠

Smart card fallback: None

Callback URL (required): https://fed-callback.f2.ctxs /CitrixAuthService/AuthService.asmx

Next Cancel

9. In the Secure Ticket Authority (STA) step, click **Add**.

The STA is running on the Delivery Controller. Be sure to precede the FQDN of your Delivery Controller with **https://**.

The /scripts/ctxsta.dll suffix is automatically added for your convenience.

10. Click **OK**.

Add Secure Ticket Authority URL

STA URL: https://a-ddc.f2.ctxs /scripts/ctxsta.dll

OK Cancel

11. Ensure **Enable session reliability** is selected, and 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:

https://a-ddc.f2.ctxs/scripts/ctxsta.dll	▲	▼
--	---	---

☒ **Enable session reliability**

☐ Request tickets from two STAs, where available

12. Back in the Remote Access step, the NetScaler Gateway appliance box is automatically populated as shown below. Click **Create**.

The screenshot shows the 'Create Store' wizard in the Citrix management console. The 'Remote Access' tab is active, and the 'NetScaler Gateway' appliance is selected in the 'NetScaler Gateway appliances' list. The 'Default appliance' dropdown is also set to 'NetScaler Gateway'. The 'Remote access' section shows 'No VPN tunnel' selected. The 'StoreFront' sidebar on the left shows 'Base URL', 'Store Name', and 'Delivery Controllers' as completed steps, with 'Remote Access' being the current step.

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 ⓘ

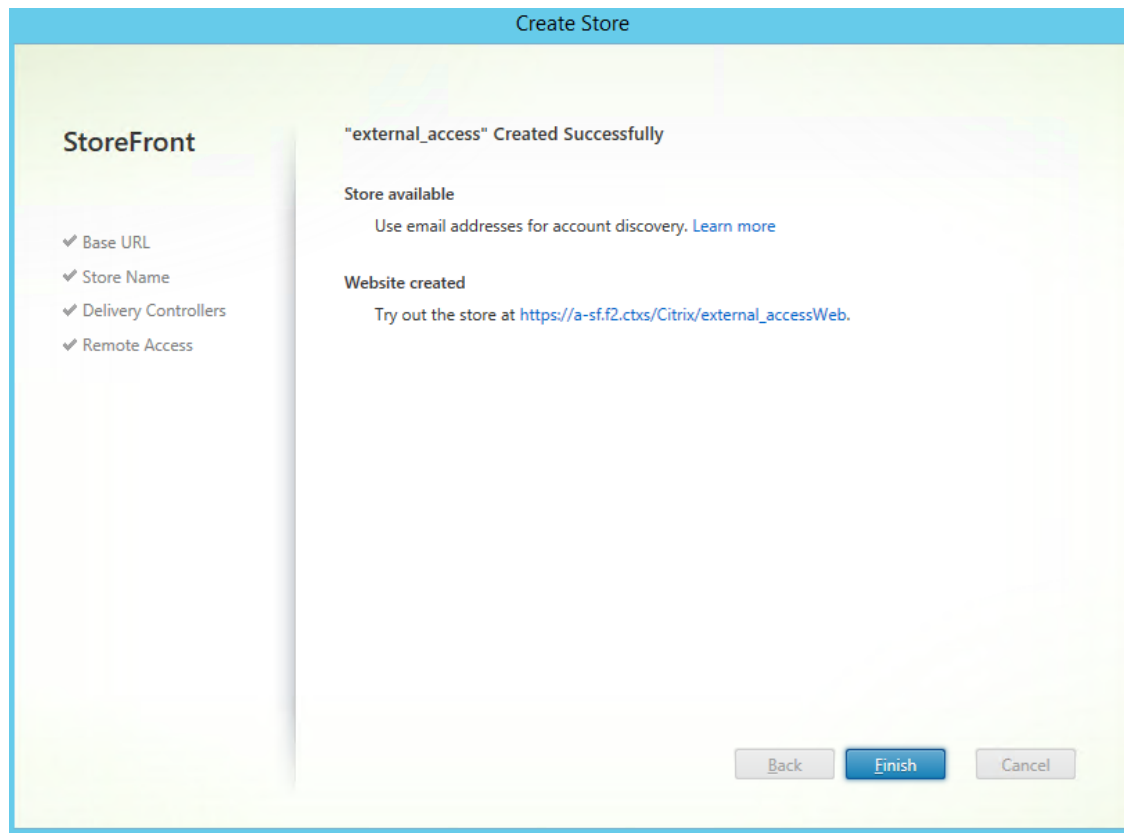
NetScaler Gateway appliances: ☒ NetScaler Gateway ⓘ

Add...

Default appliance: NetScaler Gateway ▼

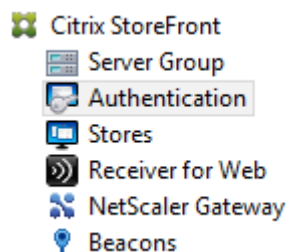
Back Create Cancel

- The store is created. Note that a Receiver for Web site (to access the Store using a web browser from the endpoint without a native Citrix Receiver) is also created. Click **Finish**.



Configure Authentication

- Select the **Authentication** option in the left panel:

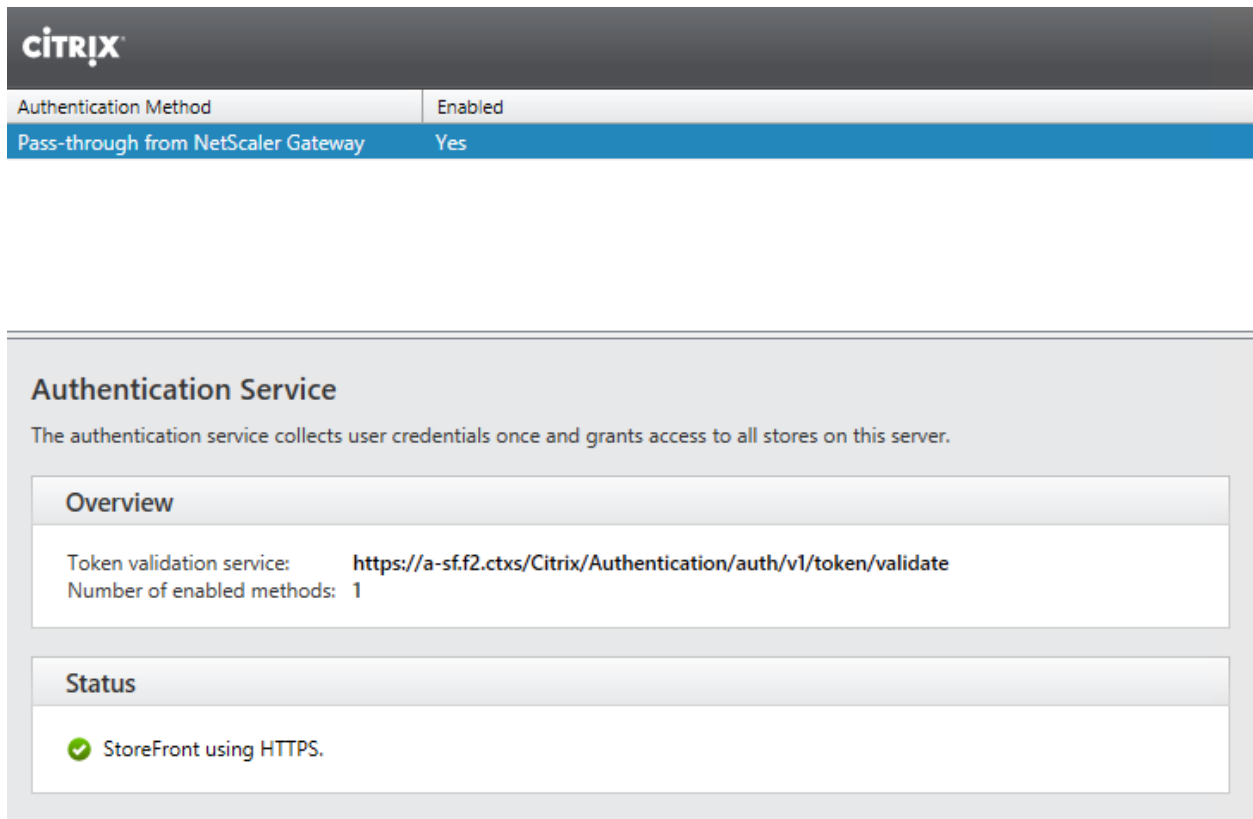


- In the Actions Panel on the right, click **Add/Remove Methods**. The Add/Remove Methods dialog box will be displayed. Deselect the user name and password. Only **Pass-through from NetScaler Gateway** should be selected. Click **OK**.

NOTE

Only pass-through from the NetScaler Gateway is selected because it is the only option that is required to configure the test environment. Adding additional authentication methods will not break the test environment, but they are not required in the context of this guide.

The authentication screen should now look as follows:

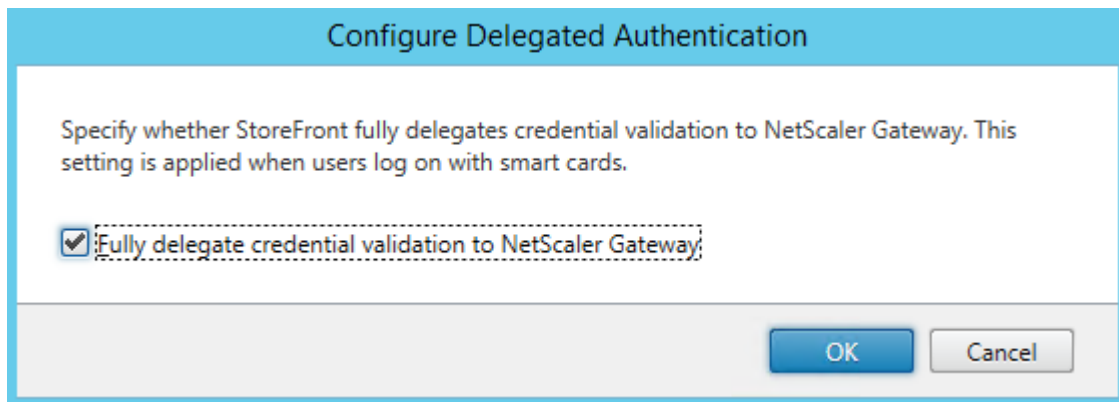


The image shows the Citrix Authentication Service configuration interface. At the top, the Citrix logo is displayed. Below it, a table shows the authentication method and its status:

Authentication Method	Enabled
Pass-through from NetScaler Gateway	Yes

Below the table, the 'Authentication Service' section is shown. It includes a description: 'The authentication service collects user credentials once and grants access to all stores on this server.' Under the 'Overview' tab, the token validation service URL is 'https://a-sf.f2.ctxs/Citrix/Authentication/auth/v1/token/validate' and the number of enabled methods is '1'. Under the 'Status' tab, a green checkmark indicates 'StoreFront using HTTPS.'

3. In the Actions Panel on the right, click **Configure Delegated Authentication**. Ensure that **Fully delegate credential validation to NetScaler Gateway** is selected:



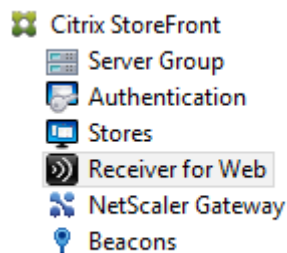
The image shows the 'Configure Delegated Authentication' dialog box. It has a blue header with the title 'Configure Delegated Authentication'. The main text reads: 'Specify whether StoreFront fully delegates credential validation to NetScaler Gateway. This setting is applied when users log on with smart cards.' Below this text, there is a checkbox labeled 'Fully delegate credential validation to NetScaler Gateway' which is checked. At the bottom right, there are 'OK' and 'Cancel' buttons.

NOTE

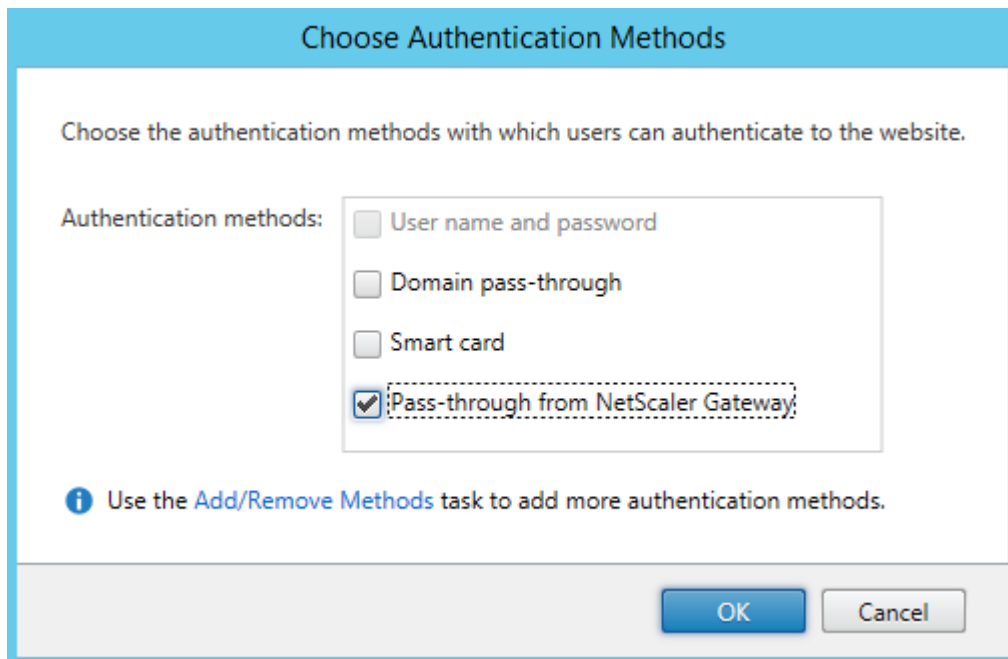
For smart card authentication via a NetScaler Gateway, the only authentication option method that is required is pass-through from NetScaler Gateway. You do not need to enable the smart card authentication method when users will be logging on with smart cards from an external network through NetScaler Gateway. The smart card authentication method should only be enabled when users will be logging in with smart cards from the internal network directly through StoreFront. Smart card authentication from the internal network (without NetScaler Gateway) is outside the scope of the first edition of this guide.

Configure Receiver for web authentication methods

1. Select **Receiver for Web** in the left panel:

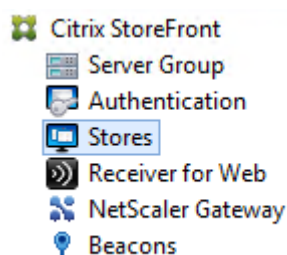


2. Click **Choose Authentication Methods** from the Actions panel on the right:
3. Ensure that only the **Pass-through from NetScaler Gateway** authentication method is selected:



Export Provisioning file

1. Select **Stores** in the left panel:



2. Select **Export Provisioning File** from the Actions pane on the right side:

Export Provisioning File

Distribute this file to your users to automate Citrix Receiver setup.

Name: external_access
 URL: https://a-sf.f2.ctxs/Citrix/external_access
 Access: Internal and external networks

Details ^

Default NetScaler Gateway appliance: NetScaler Gateway
 Other appliances:

Internal beacons: https://a-sf.f2.ctxs/
 External beacons: https://fed-nsg.f2.ctxs, http://www.citrix.com

Export Cancel

NOTE

A provisioning file is a XML file that includes the necessary information to allow Receiver to decide whether it should connect directly to StoreFront or through NetScaler Gateway. This decision is made by using the beacon addresses included in the file. If Receiver is able to resolve the internal beacon address, it will connect directly to StoreFront. By default, the internal beacon address is set to the load balancing hostname for the StoreFront servers; although, this can be changed in the beacons menu inside StoreFront.

The test environment in this guide assumes that a provisioning file is used. It is, however, possible to use the Account Services auto-discovery service. This requires an additional configuration setting on the NetScaler Gateway and an SRV record on the DNS server that the endpoint uses to resolve hostnames. For more information see section [Create session policy for Citrix Receiver client](#).

Keep the provisioning file at hand. You will be using it when configuring Citrix Receiver on the endpoint.

NetScaler Gateway

Test Environment assumptions

- NetScaler Gateway hardware platform is NSMPX-10500 8*CPU+2*E1K+8*E1K+2*IX+1*NGFIPS 766600
- NetScaler Gateway software build is NetScaler NS10.5: Build 53.9.nc, Date: Oct. 30, 2014, 20:48:24
- FIPS HSM model is NITROX XL CN1620-NFBE
- FIPS HSM hardware version is 2.0-G
- FIPS HSM firmware Version is 1.1
- UI theme is set to Green Bubble in Global NetScaler Gateway Settings > Client Experience
- IP addresses in use by the NetScaler Gateway can be resolved either internally or externally or both as appropriate. Below is a summary of IP addresses used in the test environment:

NetScaler IP (NSIP)	10.217.206.29
NetScaler Gateway Hostname	trenton
Virtual IP (VIP) for fed-nsg.f2.ctxs	10.217.205.72
Virtual IP (VIP) for fed-callback.f2.ctxs	10.217.205.73
Virtual IP (VIP) for fed-sson-session.f2.ctxs	10.217.205.74
Subnet IP (SNIP)	10.217.205.75
DNS Server	10.70.131.23

Configuration Steps

Summary of user names and passwords in the test environment example

Administrator user name	nsroot
Administrator password	open.sesame
Hardware Security Module (HSM) label	ns-hsm
Hardware Security Module (HSM) Security Officer (SO) password	so54321
Hardware Security Module (HSM) user password	user123

NOTE

The passwords used in the test environment example are not strong and therefore not suitable for use in production environments. **Do not use these passwords in your environment under any circumstances.**

Initial configuration

1. Download and install the appropriate NetScaler build. The build used throughout this document is:

 Build

Release 10.5 Build 53.9 (nCore)
 SHA256 checksum =
 16b49501af32b5fb81b6fadad10fc0111a33c666b559755f87472eca25485be2
 Nov 3, 2014

Download
 File Size: 250 MB
 File Type: .tgz

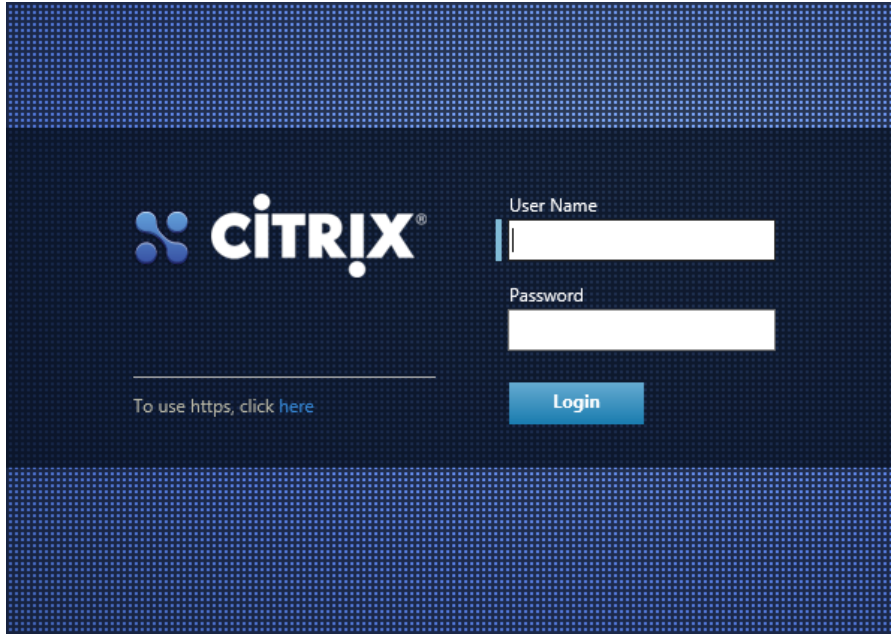
2. Perform an initial configuration, specifying the NSIP, subnet mask and default gateway for the NetScaler Gateway appliance.

NOTE

How to perform an initial configuration on a NetScaler Gateway appliance is described here:

<http://support.citrix.com/proddocs/topic/netscaler-hrdwre-installation-10-5/ns-initial-config-wrapper-con.html>

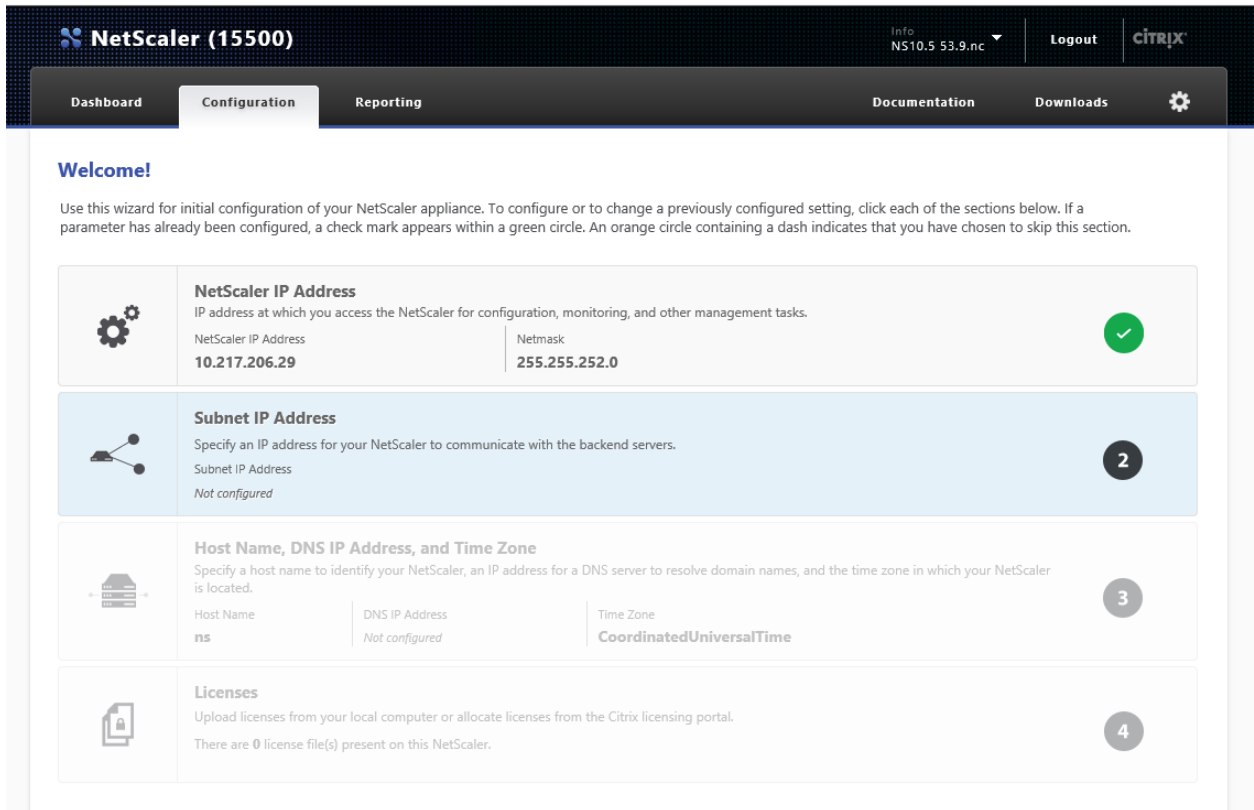
3. Once the initial configuration is complete, you will be able to log on to the graphical user interface (GUI) with a web browser by entering the NSIP into the web browser's address bar:



The image shows the Citrix login page. On the left is the Citrix logo. To its right are two input fields: 'User Name' and 'Password'. Below the 'User Name' field is a blue 'Login' button. A link 'To use https, click here' is located below the input fields. The background is a dark blue with a subtle dot pattern.

The default user name and the default password are both “nsroot”.

4. After logging in via the GUI for the first time, you will be directed to the Configuration page:



The image shows the NetScaler Configuration page. The top navigation bar includes 'Dashboard', 'Configuration' (selected), 'Reporting', 'Documentation', and 'Downloads'. The main content area is titled 'Welcome!' and contains a wizard for initial configuration. The wizard has four steps:

Step	Section	Status
1	NetScaler IP Address IP address at which you access the NetScaler for configuration, monitoring, and other management tasks. NetScaler IP Address: 10.217.206.29 Netmask: 255.255.252.0	Completed (Green checkmark)
2	Subnet IP Address Specify an IP address for your NetScaler to communicate with the backend servers. Subnet IP Address: Not configured	Not completed (Orange circle with dash)
3	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: ns DNS IP Address: Not configured Time Zone: CoordinatedUniversalTime	Not completed (Orange circle with dash)
4	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.	Not completed (Orange circle with dash)

Specify the SNIP

- Step 1 will be shown as already completed. Click on **Subnet IP address** (Step 2). You will be prompted to enter a suitable SNIP.



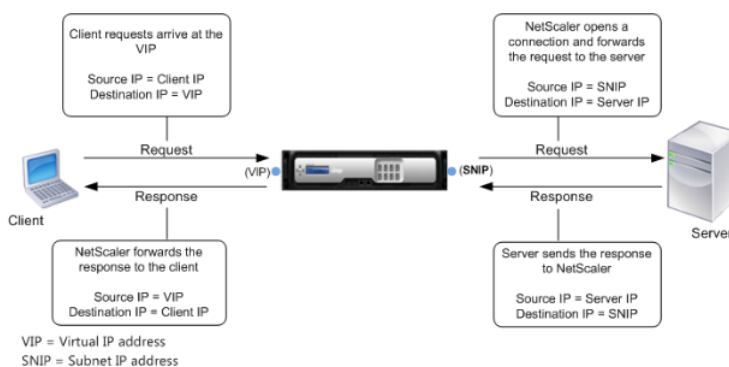
Subnet IP Address

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](#).



Subnet IP Address*

10 . 217 . 205 . 75

Netmask*

255 . 255 . 252 . 0

Done Do It Later

- Click **Done**.

Specify host name, DNS IP address, and time zone



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

trenton

DNS IP Address

10 . 70 . 131 . 23 +

Time Zone*

GMT-08:00-PST-Pacific/Pitcairn

Done Back

NOTE

From this point onwards, the CLI commands that correspond to the instructions shown in the GUI will be provided.

```
set ns param -timezone "GMT-08:00-PST-Pacific/Pitcairn" -grantQuotaMaxClient 10
```

```
set ns hostName trenton
```

```
add dns nameServer 10.70.131.23 -state ENABLED
```

Specify license(s)

1. Upload your license file(s). Once you have uploaded and installed all the licenses, NetScaler will prompt you to perform a reboot.

Change admin password

1. Navigate to:

NetScaler > System > User Administration > Users

2. In the NetScaler GUI:

NetScaler > System > User Administration > Users						Refresh	Help	Save
<div> Add Edit Delete Change Password </div> <div>Search</div>								
User Name	CLI Prompt	Prompt inherited from	Idle Session Timeout (secs)	Idle Session Timeout inherited from	External Authentication	Logging Privilege		
nsroot			36000	User	ENABLED	ENABLED		

Select the nsroot user, and click **Change Password**.

```
set system user nsroot -password "*****" -externalAuth ENABLED -logging ENABLED
```

NOTE

Changing the administrator password to a nondefault value is imperative. In a production environment, it is suggested that you change the user name to something other than the default value of nsroot, as well.

Configure basic features

1. The following two basic features are the minimum required features that must be enabled:

Configure Basic Features

☒ SSL Offloading	☐ HTTP Compression
☐ Load Balancing	☐ Content Switching
☐ Content Filter	☐ Integrated Caching
☐ Rewrite	☒ NetScaler Gateway
☐ Authentication, Authorization and Auditing	☐ Application Firewall

OK Close

```
enable ns feature SSL SSLVPN
enable ns feature SSLVPN
```

Hardware security module (HSM) configuration and FIPS key generation

Initialize the HSM

A FIPS-compliant NetScaler appliance ships with a built-in HSM—a physical device that securely stores cryptographic keys and perform cryptographic operations. You must initialize the HSM before you can use it.

The following instructions are for configuring the HSM on an MPX 9700/10500/12500/15500 FIPS appliance by using the command line interface:

1. Log on to the appliance with an SSH client (such as Putty) as the superuser. (In this case nsroot).
2. Save the NetScaler configuration.

```
save ns config
```

3. Show FIPS.

```
show ssl fips
```

4. If the HSM is uninitialized, the following will be displayed:

```
FIPS Card is not configured
```

5. Reset the FIPS card.

```
reset ssl fips
```

6. Reboot.

```
reboot -warm
```

7. Initialize HSM.

```
set ssl fips -initHSM Level-2 so54321 so12345 user123 -hsmLabel ns-hsm
```

NOTE

The passwords used in the test environment example are not strong and therefore are not suitable for use in production environments. **Do not use these passwords in your environment under any circumstances.**

The above command erases all the data on the FIPS card, initializes the HSM at FIPS level 2, changes the security officer password, sets the user password, and assigns a label to the HSM. For more details see the table below:

```
set ssl fips -initHSM Level-2 <new SO password> <old SO password> <user password> [-hsmLabel <string>]
```

initHSM	The FIPS initialization level. The appliance currently supports Level-2 (FIPS 140-2 Level-2). Possible value: Level 2.
hsmLabel	The label to identify the HSM. Maximum length: 31.
newSOpassword	The security officer password that will be in effect after you have configured the HSM. Maximum length on 9010 and 9950 FIPS appliances: 31 characters. Maximum length on MPX 9700/10500/12500/15500 FIPS appliances: 14 characters.
oldSOpassword	The old security office password. Default on MPX 9700/10500/12500/15500 FIPS appliances: so12345. Default on 9010 and 9950 FIPS appliances: sopin123.
userPassword	The user password. Default on MPX 9700/10500/12500/15500 FIPS appliances: user123. Default on 9010 and 9950 FIPS appliances: userpin123. Maximum length on 9010 and 9950 FIPS appliances: 31 characters. Maximum length on MPX 9700/10500/12500/15500 FIPS appliances: 14 characters.

NOTE

After the HSM is initialized, the current configuration on the appliance needs to be saved. If this is not done, the card will not function after the appliance is restarted, and three unsuccessful attempts to change the SO password will cause the card to be locked.

8. Save the NetScaler configuration.

```
save ns config
```

9. Reboot.

```
reboot -warm
```

10. Show FIPS.

```
show ssl fips
```

```
> show ssl fips
  FIPS HSM Info:
    HSM Label       : ns-hsm
    Initialization  : FIPS-140-2 Level-2
    HSM Serial Number : 2.1G1111-IC001220
    HSM State       : 2
    HSM Model       : NITROX XL CN1620-NFBE

    Hardware Version : 2.0-G
    Firmware Version  : 1.1
    Firmware Release Date : Jun04,2010

    Max FIPS Key Memory : 3996
    Free FIPS Key Memory : 3994
    Total SRAM Memory   : 467348
    Free SRAM Memory    : 62544
    Total Crypto Cores  : 3
    Enabled Crypto Cores : 3

Done
```

Generate RSA keypairs inside the HSM

1. Create a keypair for the fed-nsg.f2.ctxs virtual server.

```
create ssl fipsKey fed-nsg-key -modulus 2048 -exponent F4
```

2. Create a keypair for the fed-callback.f2.ctxs virtual server.

```
create ssl fipsKey fed-callback-key -modulus 2048 -exponent F4
```

3. Create a keypair for the fed-sson-session.f2.ctxs virtual server.

```
create ssl fipsKey fed-sson-session-key -modulus 2048 -exponent F4
```

```
create ssl fipsKey <fipsKeyName> -modulus <positive_integer> [-exponent ( 3 | F4 )]
```

fipsKeyName	The object name for the FIPS key. Maximum length: 31.
modulus	The modulus of the key to be created. The modulus value should be a multiple of 64. Possible values on 9010 and 9950 FIPS appliances: 512, 1024, 2048. Possible values on MPX 9700/10500/12500/15500 FIPS appliances: 1024, 2048.
exponent	The exponent value for the RSA key to be created. There are two possible choices: 3. This is the numeric value 3 (hexadecimal 0x3) and corresponds to the Fermat number F0. It

is the default value.

F4. This is the numeric value 65537 (hexadecimal 0x10001) and corresponds to the Fermat number F4. It is the more common value used for Internet deployments.

4. You can verify that the keys have been generated by typing:

```
show ssl fipsKey
```

```
> show ssl fipsKey
1)    FIPS Key Name: fed-nsg-key
2)    FIPS Key Name: fed-callback-key
3)    FIPS Key Name: fed-sson-session-key
Done
```

5. For details of any given key, type **show ssl fipsKey** followed by the key name:

```
show ssl fipsKey fed-nsg-key
```

```
> show ssl fipsKey fed-nsg-key
    FIPS Key Name: fed-nsg-key      Modulus: 2048   Public Exponent: F4 (Hex: 0x10001)
Done
```

NOTE

The fed-sson-session key pertains to Single Sign-on. More details on how to fully configure the fed-sson-session virtual server as well as other settings are described in detail in section [Smart Card Single Sign-on](#). Key and certificate configuration for this virtual server is included in the NetScaler section of the document because it makes sense to generate all the keys and perform the certificate configuration for all the virtual servers together. However, if you have no interest in achieving Single Sign-on, the fed-sson-session key and certificate configuration parts can be skipped.

Note that the keys are not stored in the NetScaler's file system (the default file system location for cryptographic objects such as keys is /nsconfig/ssl). This can be verified by examining the NetScaler file system with a tool such as WinSCP. Only the default objects and keys exist:

/flash/nsconfig/ssl				
Name	Ext	Size	Changed	Rights
			13/12/2014 22:49:51	rwxt-r-x
ns-root.cert		1,269 B	27/11/2014 22:51:53	rw-r--r--
ns-root.key		887 B	27/11/2014 22:51:53	rw-r--r--
ns-root.req		672 B	27/11/2014 22:51:53	rw-r--r--
ns-root.srl		3 B	27/11/2014 22:51:54	rw-r--r--
ns-server.cert		1,249 B	27/11/2014 22:51:54	rw-r--r--
ns-server.key		887 B	27/11/2014 22:51:53	rw-r--r--
ns-server.req		672 B	27/11/2014 22:51:53	rw-r--r--
server_cert.pem		1,151 B	15/05/2013 19:33:17	rw-r--r--
server_key.pem		887 B	15/05/2013 19:33:17	rw-r--r--

The FIPS keys are stored securely in the HSM.

Certificate configuration

Create Certificate Signing Requests (CSR) for each SSL FIPS key

1. Create CSRs

A CSR includes the **public** key from the private/public key pair. A CSR is submitted to your organization's issuing CA.

The issuing CA will then use the CSR to generate, sign, and issue a certificate. You then bind this certificate to its corresponding virtual server on the NetScaler Gateway appliance.

The following are the CLI commands to generate three CSRs (one for every virtual server).

```
create ssl certReq fed-nsg-csr -fipsKeyName fed-nsg-key -keyform DER -
countryName US -stateName California -organizationName Citrix -
organizationUnitName Auth -localityName "Santa Clara" -commonName fed-
nsg.f2.ctxs
```

```
create ssl certReq fed-callback-csr -fipsKeyName fed-callback-key -keyform
DER -countryName US -stateName California -organizationName Citrix -
organizationUnitName Auth -localityName "Santa Clara" -commonName fed-
callback.f2.ctxs
```

```
create ssl certReq fed-sson-session-csr -fipsKeyName fed-sson-session-key -
keyform DER -countryName US -stateName California -organizationName Citrix -
organizationUnitName Auth -localityName "Santa Clara" -commonName fed-sson-
session.f2.ctxs
```

NOTE

In this example, the keyform is encoded as DER. The alternative is PEM.

2. Ensure it has been created:

/flash/nsconfig/ssl				
Name	Ext	Size	Changed	Rights
 ..			14/12/2014 00:26:58	rw-r--r--
 fed-callback-csr		1,033 B	14/12/2014 00:29:50	rw-r--r--
 fed-nsg-csr		1,025 B	14/12/2014 00:28:07	rw-r--r--
 fed-sson-session-csr		1,037 B	14/12/2014 00:31:53	rw-r--r--
 ns-root.cert		1,269 B	27/11/2014 22:51:53	rw-r--r--
 ns-root.key		887 B	27/11/2014 22:51:53	rw-r--r--
 ns-root.req		672 B	27/11/2014 22:51:53	rw-r--r--
 ns-root.srl		3 B	27/11/2014 22:51:54	rw-r--r--
 ns-server.cert		1,249 B	27/11/2014 22:51:54	rw-r--r--
 ns-server.key		887 B	27/11/2014 22:51:53	rw-r--r--
 ns-server.req		672 B	27/11/2014 22:51:53	rw-r--r--
 server_cert.pem		1,151 B	15/05/2013 19:33:17	rw-r--r--
 server_key.pem		887 B	15/05/2013 19:33:17	rw-r--r--

```
create ssl certReq <reqFile> (-keyFile <input_filename> | -fipsKeyName <string>) [-keyform ( DER
| PEM ) {-PEMPassPhrase }] -countryName <string> -stateName <string> -organizationName
<string> [-organizationUnitName <string>] [-localityName <string>] [-commonName <string>] [-
emailAddress <string>] {-challengePassword } [-companyName <string>]
```

reqFile	The file name where the generated CSRs are stored. The default output path for the CSR file is /nsconfig/ssl/. Maximum value: 63
keyFile	The key file name to be used. The key can be an RSA or a DSA key. The default input path for the key file is /nsconfig/ssl/. Maximum value: 63
fipsKeyName	The FIPS key name to be used. FIPS keys are created inside the FIPS HSM (Hardware Security Module). This is applicable only to the SSL FIPS system.
keyform	The format for the input key file specified in the keyFileName: PEM: Privacy Enhanced Mail DER: Distinguished Encoding Rule Possible values: DER, PEM Default value: FORMAT_PEM
countryName	Country Name – Two-letter ISO code for your country. For example, US for United States.
stateName	State or Province Name - Full name for the state or province where your organization is located. Maximum characters allowed: 63. Do not abbreviate.
organizationName	Organization Name - Name of the organization. The organization name (corporation, limited partnership, university, or government agency) must be registered with some authority at the national, state, or city level. Use the legal name under which the organization is registered. Maximum characters allowed are 63. Do not abbreviate the organization name and do not use the following characters in the name: < > ~ ! @ # 0 ^ * / () ?.
organizationUnitName	Organization Unit Name - Division or Section name in the organization that will use the certificate. Maximum characters allowed: 63.
localityName	Locality Name - Name of the city or town in which your organization's head office is located. Maximum characters allowed: 127.
commonName	Common Name - Fully qualified domain name for the company/website. The common name is the fully qualified domain name (FQDN) for the company/website. The common name must match the name used by DNS servers to do a DNS lookup of your server (for example, www.mywebsite.com <http://www.mywebsite.com>). Most browsers use this information for authenticating the server's certificate during the SSL handshake. If the server name does not match the common name as given in the server certificate, the browsers will terminate the SSL handshake or prompt the user with a warning message. Maximum characters allowed: 63. CAUTION: Do not use wildcard characters such as * or ?, and do not use an IP address as the common name. The common name should be without the protocol specifier <http://> or <https://>.
emailAddress	The contact person's email address.
challengePassword	Challenge password for this certificate.

Submit CSRs to your organization's issuing CA

1. Jump to section [Submit certificate signing requests \(CSR\) to your organization's issuing CA](#) and complete the certificate issuance procedure on your organizations issuing CA server.

Copy certificate files to NetScaler

1. Have the following certificate files at hand:
 - The certificates that were issued for the virtual servers by your organization's CA that will be configured on your NetScaler Gateway:

 fed-sson-session-cert	15/12/2014 17:33	Security Certificate	2 KB
 fed-nsg-cert	15/12/2014 17:32	Security Certificate	2 KB
 fed-callback-cert	15/12/2014 17:25	Security Certificate	2 KB

- Your organization's issuing CA certificate:

 intca1-issuing-ca-cert	15/12/2014 17:31	Security Certificate	2 KB
---	------------------	----------------------	------

- Your organization's root CA certificate:

 f2-dc-ca-root-ca-cert	15/12/2014 17:26	Security Certificate	2 KB
--	------------------	----------------------	------

- The NIST PIV test card #1 issuing CA certificate:

 RSA2048IssuingCACertificate	07/01/2011 10:57	Security Certificate	2 KB
--	------------------	----------------------	------

- The root CA certificate for the NIST PIV test cards:

 Self-signedTrustAnchorCertificate	09/10/2012 16:23	Security Certificate	2 KB
--	------------------	----------------------	------

NOTE

The certificate authority certificates shown here are for the NIST PIV test card #1. If you want to use production PIV cards, you may need to add other root and issuing CA certificates depending on the chaining from the particular PIV card. The NIST PIV test card #1 used the chain shown in this document. (All four certificates on the card chain to the root CA via a single issuing CA.) Production environments may use more than one chain. (For example, a PIV card with four certificates: The certificates all chain to the same root CA, but through more than one issuing CA. In such a case, additional issuing CA certificates may have to be copied and imported onto the NetScaler Gateway device. However, the scope of the instructions in this version of the document is restricted to authentication only. As such, only the PIV authentication certificate is applicable because the PIV authentication certificate is the certificate that is purposed for smart card login. For more information, see section [Appendix A: NIST PIV Test Card Certificates, Keys and Chain of Trust](#) for detailed information on the certificate chain in the NIST PIV test kit.

- Copy the seven certificate files onto /flash/nsconfig/ssl directory on the NetScaler Gateway device using a tool such as WinSCP:

/flash/nsconfig/ssl					
Name	Ext	Size	Changed	Rights	Owner
..			15/12/2014 21:11:16	rw-r--r--	root
f2-dc-ca-root-ca-cert.cer		1,236 B	15/12/2014 17:26:55	rw-r--r--	root
fed-callback-cert.cer		1,922 B	15/12/2014 17:25:45	rw-r--r--	root
fed-callback-csr		1,033 B	14/12/2014 00:29:50	rw-r--r--	root
fed-nsg-cert.cer		1,914 B	15/12/2014 17:32:25	rw-r--r--	root
fed-nsg-csr		1,025 B	14/12/2014 00:28:07	rw-r--r--	root
fed-sson-session-cert.cer		1,926 B	15/12/2014 17:33:31	rw-r--r--	root
fed-sson-session-csr		1,037 B	14/12/2014 00:31:53	rw-r--r--	root
intca1-issuing-ca-cert.cer		1,834 B	15/12/2014 17:31:32	rw-r--r--	root
ns-root.cert		1,269 B	27/11/2014 22:51:53	rw-r--r--	root
ns-root.key		887 B	27/11/2014 22:51:53	rw-r--r--	root
ns-root.req		672 B	27/11/2014 22:51:53	rw-r--r--	root
ns-root.srl		3 B	27/11/2014 22:51:54	rw-r--r--	root
ns-server.cert		1,249 B	27/11/2014 22:51:54	rw-r--r--	root
ns-server.key		887 B	27/11/2014 22:51:53	rw-r--r--	root
ns-server.req		672 B	27/11/2014 22:51:53	rw-r--r--	root
RSA2048IssuingCACertificate.cer		1,800 B	07/01/2011 10:57:10	rw-r--r--	root
Self-signedTrustAnchorCertificate.cer		1,214 B	09/10/2012 16:23:26	rw-r--r--	root
server_cert.pem		1,151 B	15/05/2013 19:33:17	rw-r--r--	root
server_key.pem		887 B	15/05/2013 19:33:17	rw-r--r--	root

Install the NIST PIV test root CA certificate file on NetScaler

- In the NetScaler GUI, navigate to:

NetScaler > Traffic Management > SSL > SSL Certificates

- Click **Install**, and then enter the following information:

Install Certificate

Certificate-Key Pair Name*

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

Certificate File Name*

FIPS Key Name

Certificate Format

☐ PEM ☒ DER

☒ Notify When Expires

Notification Period

NOTE

You only need to enter the Certificate-Key Pair Name (this will become the label) and Certificate File Name, and change the certificate format to DER. Only NIST possesses the private key for this certificate.

- Click **Install**.

```
add ssl certKey nist-piv-root-ca -cert Self-signedTrustAnchorCertificate.cer
-inform DER -expiryMonitor ENABLED -notificationPeriod 30
```

The following will be displayed in the GUI:

NetScaler > Traffic Management > SSL > SSL Certificates					
<input type="button" value="Install"/> <input type="button" value="Update"/> <input type="button" value="Delete"/> <input type="button" value="Action"/>			Search ▼		
Name	Days to Expire	Status			
▶ nist-piv-root-ca	5768	Valid			

Install the NIST PIV test issuing CA certificate file on NetScaler

- In the NetScaler GUI, navigate to:

NetScaler > Traffic Management > SSL > SSL Certificates

- Click **Install**, and then enter the following information:

Install Certificate

Certificate-Key Pair Name*

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

Certificate File Name*

FIPS Key Name

Certificate Format

☐ PEM ☒ DER

☒ Notify When Expires

Notification Period

NOTE

You only need to enter the Certificate-Key Pair Name (this will become the label) and Certificate File Name, and change the certificate format to DER. Only NIST possesses the private key for this certificate.

- Click **Install**.

```
add ssl certKey nist-piv-issuing-ca -cert RSA2048IssuingCACertificate.cer -
inform DER -expiryMonitor ENABLED -notificationPeriod 30
```

The following will be displayed in the GUI:

NetScaler > Traffic Management > SSL > SSL Certificates

Install

Update

Delete

Action

Search

Name	Days to Expire	Status
▶ nist-piv-root-ca	5768	Valid
▶ nist-piv-issuing-ca	5768	Valid

Link the test NIST PIV issuing CA certificate to the test NIST PIV root CA certificate

1. In the NetScaler GUI, navigate to:

NetScaler > Traffic Management > SSL > SSL Certificates

2. Select the **nist-piv-issuing-ca** certificate, and then choose **Link** from the Action drop-down list. The following is displayed:

Link Server Certificate(s)

CA Certificate Name*

3. Ensure that **nist-piv-root-ca** is selected in the CA Certificate Name drop-down box. Click **OK**.

```
link ssl certKey nist-piv-issuing-ca nist-piv-root-ca
```

4. To confirm that the certificates are correctly linked:

Select the **nist-piv-issuing-ca** certificate, and then choose **Cert Links** from the Action drop-down list. The following is displayed:

Configure Certificate-key pair	
Certificate-Key Pair Name	CA Certificate Name
nist-piv-issuing-ca	nist-piv-root-ca

5. At this point, save the NetScaler configuration by clicking the disk button in the GUI:

NetScaler > Traffic Management > SSL > SSL Certificates



Or by typing the following in the CLI:

```
save ns config
```

Install the fed-nsg certificate file on NetScaler

1. In the NetScaler GUI, navigate to:

NetScaler > Traffic Management > SSL > SSL Certificates

2. Click **Install**, and then enter the following information:

Install Certificate

Certificate-Key Pair Name*

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

FIPS Key Name

Certificate Format
☒ PEM ☐ DER

Password

☐ Certificate Bundle
☒ Notify When Expires

Notification Period

3. Click **Install**.

```
add ssl certKey fed-nsg -cert fed-nsg-cert.cer -fipsKey fed-nsg-key -inform
PEM -expiryMonitor ENABLED -notificationPeriod 30 -bundle NO
```

The following will be displayed in the GUI:

NetScaler > Traffic Management > SSL > SSL Certificates

Install

Update

Delete

Action

Search

Name	Days to Expire	Status
▶ nist-piv-root-ca	5768	Valid
▶ nist-piv-issuing-ca	5768	Valid
▶ fed-nsg	550	Valid

Install the fed-callback certificate file on NetScaler

1. In the NetScaler GUI, navigate to:

NetScaler > Traffic Management > SSL > SSL Certificates

2. Click **Install**, and then enter the following information:

Install Certificate

Certificate-Key Pair Name*

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

FIPS Key Name

Certificate Format
☒ PEM ☐ DER

Password

☐ Certificate Bundle
☒ Notify When Expires

Notification Period

```
add ssl certKey fed-callback -cert fed-callback-cert.cer -fipsKey fed-callback-key -inform PEM -expiryMonitor ENABLED -notificationPeriod 30 -bundle NO
```

The following will be displayed in the GUI:

NetScaler > Traffic Management > SSL > SSL Certificates					
<input type="button" value="Install"/> <input type="button" value="Update"/> <input type="button" value="Delete"/> <input type="button" value="Action"/>			Search ▼		
Name	Days to Expire	Status			
▶ nist-piv-root-ca	5768	Valid			
▶ nist-piv-issuing-ca	5768	Valid			
▶ fed-nsg	550	Valid			
▶ fed-callback	550	Valid			

Install the fed-sson-session certificate file on NetScaler

1. In the NetScaler GUI, navigate to:

NetScaler > Traffic Management > SSL > SSL Certificates

2. Click **Install**, and then enter the following information:

Install Certificate

Certificate-Key Pair Name*

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

FIPS Key Name

Certificate Format
☒ PEM ☐ DER

Password

☐ Certificate Bundle
☒ Notify When Expires

Notification Period

3. Click **Install**.

```
add ssl certKey fed-sson-session -cert fed-sson-session-cert.cer -fipsKey
fed-sson-session-key -inform PEM -expiryMonitor ENABLED -notificationPeriod
30 -bundle NO
```

The following will be displayed in the GUI:

NetScaler > Traffic Management > SSL > SSL Certificates

InstallUpdateDeleteAction

Search

Name	Days to Expire	Status
▶ nist-piv-root-ca	5768	Valid
▶ nist-piv-issuing-ca	5768	Valid
▶ fed-nsg	550	Valid
▶ fed-callback	550	Valid
▶ fed-sson-session	550	Valid

Install your organization's root CA certificate file on NetScaler

1. In the NetScaler GUI, navigate to:

NetScaler > Traffic Management > SSL > SSL Certificates

2. Click **Install**, and then enter the following information:

Install Certificate

Certificate-Key Pair Name*

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

FIPS Key Name

Certificate Format
☒ PEM ☐ DER

Password

☐ Certificate Bundle
☒ Notify When Expires

Notification Period

```
add ssl certKey f2-root-ca -cert f2-dc-ca-root-ca-cert.cer -inform PEM -
expiryMonitor ENABLED -notificationPeriod 30 -bundle NO
```

The following will be displayed in the GUI:

NetScaler > Traffic Management > SSL > SSL Certificates

InstallUpdateDeleteAction

Search

Name	Days to Expire	Status
▸ nist-piv-root-ca	5768	Valid
▸ nist-piv-issuing-ca	5768	Valid
▸ fed-nsg	550	Valid
▸ fed-callback	550	Valid
▸ fed-sson-session	550	Valid
▸ f2-root-ca	1331	Valid

Install your organization's issuing CA certificate file on NetScaler

1. In the NetScaler GUI, navigate to:

NetScaler > Traffic Management > SSL > SSL Certificates

2. Click **Install**, and then enter the following information:

Install Certificate

Certificate-Key Pair Name*

f2-issuing-ca

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

Certificate File Name*

intca1-issuing-ca-cert.cer

Browse ▼ +

FIPS Key Name

▼ +

Certificate Format

☒ PEM ☐ DER

Password

☐ Certificate Bundle

☒ Notify When Expires

Notification Period

30

Install **Close**

3. Click **Install**.

```
add ssl certKey f2-issuing-ca -cert intca1-issuing-ca-cert.cer -inform PEM -  
expiryMonitor ENABLED -notificationPeriod 30 -bundle NO
```

The following will be displayed in the GUI:

NetScaler > Traffic Management > SSL > SSL Certificates			Refresh	Help	Save
<div> <div>Install</div> <div>Update</div> <div>Delete</div> <div>Action ▼</div> </div>			Search ▼		
Name	Days to Expire	Status			
▶ nist-piv-root-ca	5768	Valid			
▶ nist-piv-issuing-ca	5768	Valid			
▶ fed-nsg	550	Valid			
▶ fed-callback	550	Valid			
▶ fed-sson-session	550	Valid			
▶ f2-root-ca	1331	Valid			
▶ f2-issuing-ca	550	Valid			

Link your organization's issuing CA certificate to your organization's root CA certificate

1. In the NetScaler GUI, navigate to:

NetScaler > Traffic Management > SSL > SSL Certificates

2. Select the **f2-issuing-ca** certificate, and then choose **Link** from the Action drop-down list. The following is displayed:

Link Server Certificate(s)

CA Certificate Name*

f2-root-ca ▼

OK

Close

3. Ensure that **f2-root-ca** is selected as the CA certificate. Click **OK**.

```
link ssl certKey f2-issuing-ca f2-root-ca
```

4. To confirm that the certificates are correctly linked:

Select the **f2-issuing-ca** certificate, and then choose **Cert Links** from the Action drop-down list. The following is displayed:

Configure Certificate-key pair	
Certificate-Key Pair Name	CA Certificate Name
f2-issuing-ca	f2-root-ca
<div>Close</div>	

Link the fed-nsg certificate to your organization's issuing CA certificate

1. In the NetScaler GUI, navigate to:

NetScaler > Traffic Management > SSL > SSL Certificates

2. Select the **fed-nsg** certificate, and then choose **Link** from the Action drop-down list. The following is displayed:

Link Server Certificate(s)

CA Certificate Name*

3. Ensure that **f2-issuing-ca** is selected as the CA certificate. Click **OK**.

```
link ssl certKey fed-nsg f2-issuing-ca
```

4. To confirm that the certificates are correctly linked:

Select the **fed-nsg** certificate, and then choose **Cert Links** from the Action drop-down list. The following is displayed:

Configure Certificate-key pair	
Certificate-Key Pair Name	CA Certificate Name
fed-nsg	f2-issuing-ca
<input type="button" value="Close"/>	

Link the fed-callback certificate to your organization's issuing CA certificate

1. In the NetScaler GUI, navigate to:

NetScaler > Traffic Management > SSL > SSL Certificates

2. Select the **fed-callback** certificate, and then choose **Link** from the Action drop-down list. The following is displayed:

Link Server Certificate(s)

CA Certificate Name*

3. Ensure that **f2-issuing-ca** is selected as the CA certificate. Click **OK**.

```
link ssl certKey fed-callback f2-issuing-ca
```

4. To confirm that the certificates are correctly linked:

Select the **fed-callback** certificate, and then choose **Cert Links** from the Action drop-down list. The following is displayed:

Configure Certificate-key pair	
Certificate-Key Pair Name	CA Certificate Name
fed-callback	f2-issuing-ca

Close

Link the **fed-sson-session** certificate to your organization's issuing CA certificate

1. In the NetScaler GUI, navigate to:

NetScaler > **Traffic Management** > **SSL** > **SSL Certificates**

2. Select the **fed-sson-session** certificate, and then choose link from the Action drop-down list. The following is displayed:

Link Server Certificate(s)
CA Certificate Name* <input type="text" value="f2-issuing-ca"/>

OK Close

3. Ensure that **f2-issuing-ca** is selected as the CA certificate. Click **OK**.

```
link ssl certKey fed-sson-session f2-issuing-ca
```

4. To confirm that the certificates are correctly linked:

Select the **fed-sson-session** certificate, and then choose **Cert Links** from the Action drop-down list. The following is displayed:

Configure Certificate-key pair	
Certificate-Key Pair Name	CA Certificate Name
fed-sson-session	f2-issuing-ca

Close

CLI verification and save

1. Type the following in the CLI:

```
show ssl certLink
```

Five links should be displayed as follows:

```
> show ssl certLink
1)    Cert Name: nist-piv-issuing-ca    CA Cert Name: nist-piv-root-ca
2)    Cert Name: fed-nsg                CA Cert Name: f2-issuing-ca
3)    Cert Name: fed-callback           CA Cert Name: f2-issuing-ca
4)    Cert Name: fed-sson-session        CA Cert Name: f2-issuing-ca
5)    Cert Name: f2-issuing-ca          CA Cert Name: f2-root-ca
Done
```

2. Type the following to save the configuration:

```
save ns conf
```

LDAP server configuration

The LDAP server, in conjunction with an LDAP policy that is bound to the NetScaler Gateway virtual server forms an integral part in smart card certificate to LDAP user account mapping. For complete details on how the mapping process works, see section [Appendix F: How NetScaler Gateway Certificate and LDAP Authentication Policies Map to an Active Directory User Account](#)

Create LDAP server

1. In the NetScaler GUI, navigate to:

NetScaler > System > Authentication > LDAP > Servers

2. Ensure that the **Servers** tab is selected. Click **Add**.

The Create Authentication LDAP server page is displayed.

3. Populate as follows (depending on your organization's Active Directory environment):

NOTE

The test environment in this document is not using LDAP over TLS. (Security Type is set to PLAINTEXT.) To use LDAP over TLS, you should configure your LDAP server appropriately and set Security Type and Port for LDAP Server to TLS (instead of PLAINTEXT shown here). In the case of Microsoft Active Directory, the following is applicable:

<http://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx>

The connection settings refer to the account that the NetScaler Gateway will use to query the LDAP server. Substitute Base DN and Administrator BIND DN as appropriate for your organization's environment.

NOTE

For production environments, you should create a separate account on the LDAP server with appropriate permissions. Under no circumstances should a default domain administrative account be used in a production environment for querying the LDAP server.

4. Populate the Other Settings section as follows. Ensure that the Authentication and User Required check boxes are not checked:

Other Settings

Server Logon Name Attribute
 --<< New >>--
 userPrincipalName

Search Filter

Group Attribute
 memberOf

Sub Attribute Name
 CN

SSO Name Attribute
 --<< New >>--
 userPrincipalName

Default Authentication Group

☐ Authentication
☐ User Required
☐ Referrals

Maximum Referral Level
 1

NOTE

Authentication check box: When Authentication is not selected, the LDAP NetScaler Gateway Server cannot be used for authentication purposes, but only to fetch information from the LDAP server (for example, the Active Directory domain controller).

Referrals check box: The LDAP server can have referrals configured. If the LDAP server has referrals configured, it will be able to refer the NetScaler Gateway LDAP query to another LDAP server. If Referrals is selected here, the NetScaler Gateway will follow the referral if the LDAP server provides it. If not selected, the NetScaler Gateway will ignore any referral information it receives from the LDAP server.

```
add authentication ldapAction f2-ldap-server -serverName dc.f2.ctxs -
serverPort 389 -authTimeout 3 -ldapBase "DC=f2,DC=ctxs" -ldapBindDn
administrator@f2.ctxs -ldapLoginName samAccountName -groupAttrName memberOf -
subAttributeName CN -secType PLAINTEXT -svrType AD -ssoNameAttribute
userPrincipalName -authentication ENABLED -requireUser YES -passwdChange
DISABLED -nestedGroupExtraction OFF -followReferrals OFF -validateServerCert
NO
```

The following will be displayed in the GUI:

NetScaler > System > Authentication > LDAP > Servers						Refresh	Help	Save
Policies		Servers						
Add		Edit	Delete	Search ▾				
Name	Server Name	IP Address	Port	Server Type	Time-out (seconds)			
f2-ldap-server	dc.f2.ctxs		389	AD	3			

Create LDAP policy

1. In the NetScaler GUI, navigate to:

NetScaler > System > Authentication > LDAP > Policies

2. Ensure that the **Policies** tab is selected. Click **Add**.

The Create Authentication LDAP Policy page is displayed.

3. Populate as follows:

Create Authentication LDAP Policy

Name*

Server*

☐

Expression*

Operators ▾

Saved Policy Expressions ▾

Frequently Used Expressions ▾

Clear

4. Click **Create**.

```
add authentication ldapPolicy f2-ldap-pol ns_true f2-ldap-server
```

The following will be displayed in the GUI:

NetScaler > System > Authentication > LDAP > Policies							
Policies Servers							
Add Edit Delete Show Bindings Global Bindings					Search ▾		
Name	Expression	Request Server	Globally Bound?	Priority			
f2-ldap-pol	ns_true	f2-ldap-server		0			

NetScaler Gateway virtual server configuration for fed-nsg

Create fed-nsg virtual server

1. In the NetScaler GUI, navigate to:

NetScaler > NetScaler Gateway > NetScaler Gateway Virtual Servers

The following is displayed:

Name	State	IP Address	Port	Protocol	Maximum Users	Current Users
No items						

2. Click **Add**.
3. Enter the following information:

VPN Virtual Server

Basic Settings

Name*
fed-nsg.f2.ctxs

IPAddress*
10 . 217 . 205 . 72 ☐ IPv6

Port*
443

► More

OK Cancel

4. Click **OK**.

```
add vpn vserver fed-nsg.f2.ctxs SSL 10.217.205.72 -range 1 443 -state ENABLED
-authentication ON -doubleHop DISABLED -maxAAAUsers 0 -icaOnly OFF -
icaProxySessionMigration OFF -deviceCert OFF -downStateFlush DISABLED -
Listenpolicy none -appflowLog DISABLED -icmpVsrResponse PASSIVE -RHstate
PASSIVE -cginfraHomePageRedirect ENABLED -l2Conn OFF -deploymentType NONE -
```

The following is displayed:

VPN Virtual Server

Basic Settings					
Name	fed-nsg.f2.ctxs	Max Users		Double Hop	false
IPAddress	10.217.205.72	Max Login Attempts		Down State Flush	false
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		

Certificates	
No Server Certificate	>
No CA Certificate	>

OK

Bind fed-nsg virtual server certificate

NOTE

Regarding certificate bindings: You don't have to bind the CA certificates (from the CA that issued the virtual server's server certificate to the NetScaler Gateway virtual server) in order to have an SSL/TLS connection between the endpoint and the NetScaler Gateway virtual server. (The *endpoint* must trust this CA chain, not the NetScaler Gateway.) However, if you want an SSL/TLS connection from the NetScaler Gateway to the backend (StoreFront), then you need to bind the CA certificate of the CA that issued the *backend servers'* server certificate(s).

The CA certificate that gets bound to the virtual server is to make the NetScaler Gateway trust the server certificate from the back-end server and is not related to the front-end SSL/TLS connection. The fact that in this example environment the fed-nsg.f2.ctxs virtual server certificate is issued by the same CA that issued the backend servers' server certificates is incidental.

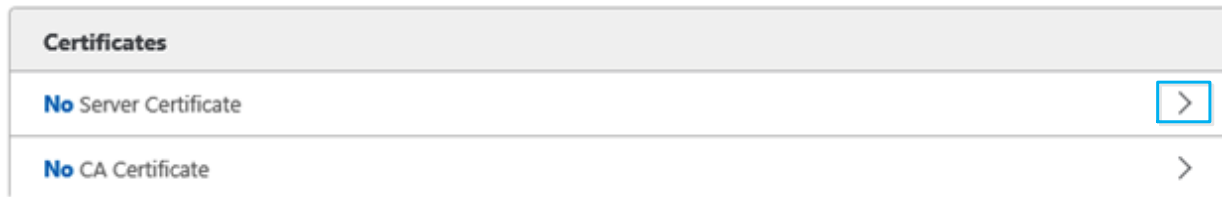
In the screenshot below, the f2-root-ca and f2-issuing CA are only bound to the fed-nsg.f2.ctxs virtual server because the F2 issuing CA also issued the backend server's server certificates.

SSL Virtual Server CA Certificate Binding		
SSL Virtual Server CA Certificate Binding		
<input type="button" value="Add Binding"/> <input type="button" value="Unbind"/>		
Certificate	CRL and OCSP Check	Skip CA
nist-piv-root-ca	OCSP Optional	✗
nist-piv-issuing-ca	OCSP Optional	✗
f2-root-ca	OCSP Optional	✗
f2-issuing-ca	OCSP Optional	✗
<input type="button" value="Close"/>		

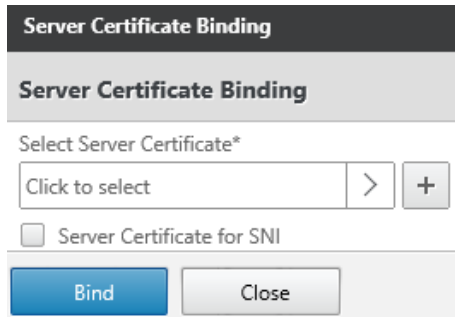
However, for *certificate authentication* to occur when the SSL/TLS connection is made from the endpoint to the fed-nsg.f2.ctxs virtual server, the CA that issued the certificate that the user is using to authenticate with must be bound to the fed-nsg.f2.ctxs virtual server. (In the case above, the nist-piv-issuing-ca issued the PIV authentication certificate that the user is proffering.)

Regarding OCSP and CRL check: When set to mandatory, OCSP/CRL will check revocation. If revocation cannot be checked for whatever reason, logon will fail. When set to optional, if revocation cannot be checked for whatever reason, it will go ahead. **It is imperative that revocation be checked in production environments.**

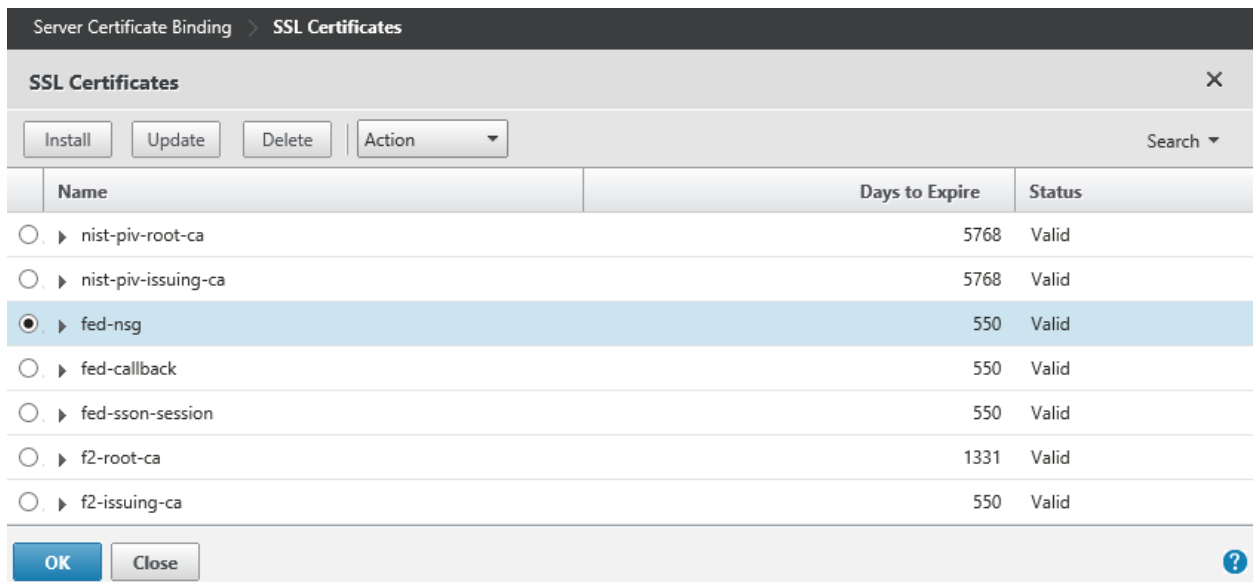
- Under the Certificates section, click the arrow on the right-hand side:



The Server Certificate Binding page is displayed:



- Click to select a server certificate. Choose the fed-nsg certificate that you installed in section [Install the fed-nsg certificate file on NetScaler](#).



- Click OK.
- Click Bind.

```
bind ssl vsriver fed-nsg.f2.ctxs -priority 0 -certkeyName fed-nsg -crlCheck
Optional
```

The following is displayed in the GUI:

Certificates	
1 Server Certificate	>
No CA Certificate	>

Bind f2-root-ca certificate

1. Under the Certificates section, click the arrow on the right-hand side.
2. Click to select a CA certificate.
3. Select the f2-root-ca certificate:

CA Certificate Binding > SSL Certificates			
SSL Certificates			
<input type="button" value="Install"/> <input type="button" value="Update"/> <input type="button" value="Delete"/> <input type="button" value="Action"/>		Search ▾	
Name	Days to Expire	Status	
☐ ▶ nist-piv-root-ca	5768	Valid	
☐ ▶ nist-piv-issuing-ca	5768	Valid	
☐ ▶ fed-nsg	550	Valid	
☐ ▶ fed-callback	550	Valid	
☐ ▶ fed-sson-session	550	Valid	
☒ ▶ f2-root-ca	1331	Valid	
☐ ▶ f2-issuing-ca	550	Valid	
<input type="button" value="OK"/> <input type="button" value="Close"/>		?	

4. Click OK.
5. Click Bind.

```
bind ssl vserver fed-nsg.f2.ctxs -priority 0 -certkeyName f2-root-ca -CA -
crlCheck Optional
```

The following will be displayed in the GUI:

Certificates	
1 Server Certificate	>
1 CA Certificate	>

Bind f2-intermediate-ca certificate

1. Under the Certificates section, click the arrow on the right-hand side.

The following page is displayed:

The screenshot shows the 'SSL Virtual Server CA Certificate Binding' dialog box. It has a title bar with the same text and a close button (X). Below the title bar are 'Add Binding' and 'Unbind' buttons. The main area is a table with three columns: 'Certificate', 'CRL and OCSP Check', and 'Skip CA'. The first row contains 'f2-root-ca', 'OCSP Optional', and 'X'. At the bottom is a 'Close' button.

Certificate	CRL and OCSP Check	Skip CA
f2-root-ca	OCSP Optional	X

2. Click Add Binding.
3. Click to select CA certificate.
4. Select the f2-issuing-ca certificate:

The screenshot shows the 'SSL Certificates' dialog box. It has a breadcrumb trail: 'SSL Virtual Server CA Certificate Binding > CA Certificate Binding > SSL Certificates'. Below the title bar are 'Install', 'Update', 'Delete', and 'Action' buttons, along with a 'Search' dropdown. The main area is a table with three columns: 'Name', 'Days to Expire', and 'Status'. The table lists several certificates, with 'f2-issuing-ca' selected (indicated by a radio button and a blue highlight). At the bottom are 'OK' and 'Close' buttons, and a help icon (?) on the right.

Name	Days to Expire	Status
nist-piv-root-ca	5768	Valid
nist-piv-issuing-ca	5768	Valid
fed-nsg	550	Valid
fed-callback	550	Valid
fed-sson-session	550	Valid
f2-root-ca	1331	Valid
f2-issuing-ca	550	Valid

5. Click OK.
6. Click Bind.

```
bind ssl vserver fed-nsg.f2.ctxs -priority 0 -certkeyName f2-issuing-ca -CA -
crlCheck Optional
```

The following is displayed in the GUI:

SSL Virtual Server CA Certificate Binding		
SSL Virtual Server CA Certificate Binding		
<input type="button" value="Add Binding"/> <input type="button" value="Unbind"/>		
Certificate	CRL and OCSP Check	Skip CA
f2-root-ca	OCSP Optional	×
f2-issuing-ca	OCSP Optional	×
<input type="button" value="Close"/>		

- Click **Close**.

The following is displayed in the GUI:

Certificates	
1 Server Certificate	>
2 CA Certificates	>

Bind the NIST Root CA certificate

- In the Certificates section for the fed-nsg virtual server, click on the arrow on the right-hand side:

Certificates	
1 Server Certificate	>
2 CA Certificates	>

The following is displayed:

SSL Virtual Server CA Certificate Binding		
SSL Virtual Server CA Certificate Binding		
<input type="button" value="Add Binding"/> <input type="button" value="Unbind"/>		
Certificate	CRL and OCSP Check	Skip CA
f2-root-ca	OCSP Optional	×
f2-issuing-ca	OCSP Optional	×
<input type="button" value="Close"/>		

- Click **Add Binding**.

The following is displayed:

SSL Virtual Server CA Certificate Binding > **CA Certificate Binding**

CA Certificate Binding ✕

Select CA Certificate*

Click to select > +

CRL and OCSP Check

▼

☐ Skip CA

Bind Close

3. Click the arrow on the right-hand side to select a CA certificate.

The following is displayed:

SSL Virtual Server CA Certificate Binding > CA Certificate Binding > **SSL Certificates**

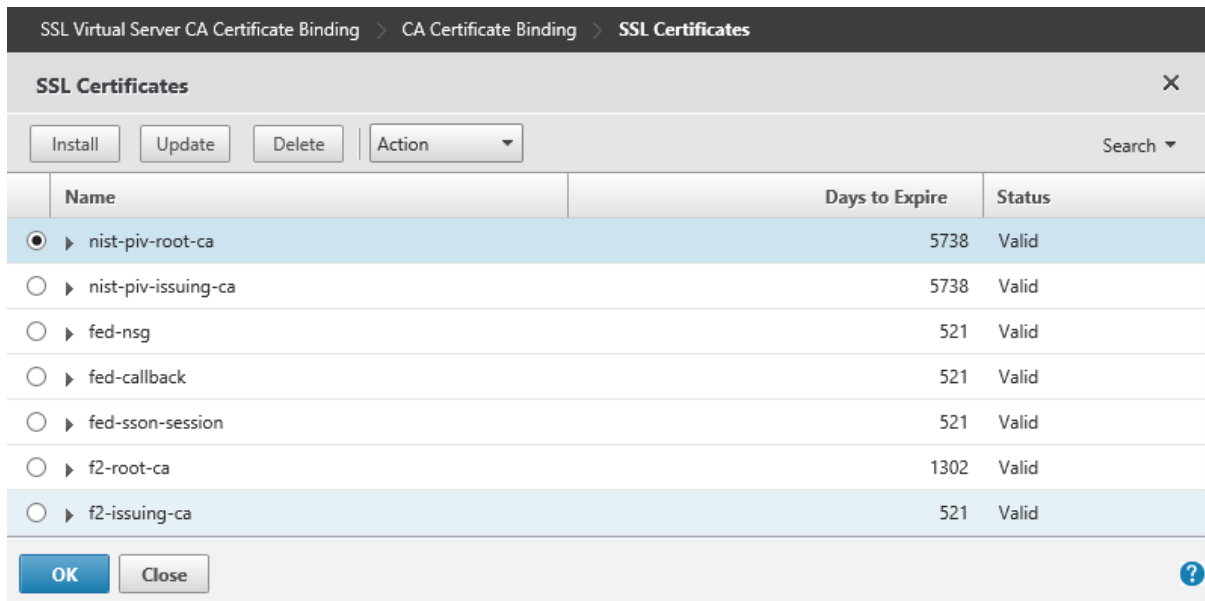
SSL Certificates ✕

Install Update Delete Action ▼ Search ▼

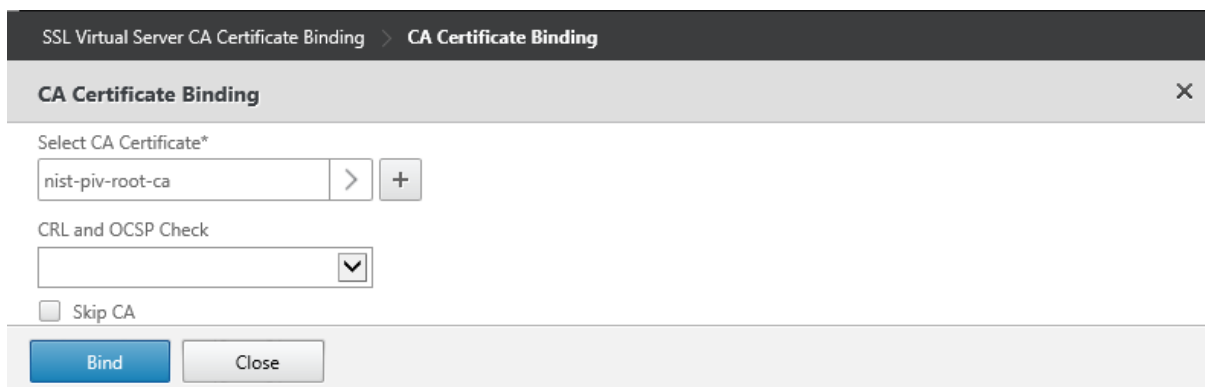
Name	Days to Expire	Status
☐ ▶ nist-piv-root-ca	5738	Valid
☐ ▶ nist-piv-issuing-ca	5738	Valid
☐ ▶ fed-nsg	521	Valid
☐ ▶ fed-callback	521	Valid
☐ ▶ fed-sson-session	521	Valid
☐ ▶ f2-root-ca	1302	Valid
☐ ▶ f2-issuing-ca	521	Valid

OK Close ?

4. Select **nist-piv-root-ca**, and click **OK**.



The following is displayed:



5. Click **Bind**.

```
bind ssl vserver fed-nsg.f2.ctxs -priority 0 -certkeyName nist-piv-root-ca -
CA -crlCheck Optional
```

The following is displayed:

SSL Virtual Server CA Certificate Binding		
SSL Virtual Server CA Certificate Binding		
<div>Add Binding Unbind</div>		
Certificate	CRL and OCSP Check	Skip CA
nist-piv-root-ca	OCSP Optional	✗
f2-root-ca	OCSP Optional	✗
f2-issuing-ca	OCSP Optional	✗
<div>Close</div>		

Bind the NIST issuing CA certificate

1. Click **Add Binding**.

The following is displayed:

SSL Virtual Server CA Certificate Binding > CA Certificate Binding

CA Certificate Binding

Select CA Certificate*

Click to select > +

CRL and OCSP Check

☐ Skip CA

Bind

Close

2. Click on the arrow on the right-hand side to select a CA certificate.

The following is displayed:

SSL Virtual Server CA Certificate Binding > CA Certificate Binding > SSL Certificates

SSL Certificates ✕

Search ▾

Name	Days to Expire	Status
☐ ▶ nist-piv-root-ca	5738	Valid
☐ ▶ nist-piv-issuing-ca	5738	Valid
☐ ▶ fed-nsg	521	Valid
☐ ▶ fed-callback	521	Valid
☐ ▶ fed-sson-session	521	Valid
☐ ▶ f2-root-ca	1302	Valid
☐ ▶ f2-issuing-ca	521	Valid

?

3. Select nist-piv-issuing-ca.

SSL Virtual Server CA Certificate Binding > CA Certificate Binding > SSL Certificates

SSL Certificates ✕

Search ▾

Name	Days to Expire	Status
☐ ▶ nist-piv-root-ca	5738	Valid
☒ ▶ nist-piv-issuing-ca	5738	Valid
☐ ▶ fed-nsg	521	Valid
☐ ▶ fed-callback	521	Valid
☐ ▶ fed-sson-session	521	Valid
☐ ▶ f2-root-ca	1302	Valid
☐ ▶ f2-issuing-ca	521	Valid

?

4. Click OK.

The following is displayed:

- Click **Bind**.

```
bind ssl vserver fed-nsg.f2.ctxs -priority 0 -certkeyName nist-piv-issuing-ca
-CA -crlCheck Optional
```

- Click **Close**.

Certificates should now look like this in the GUI:

Certificates	
1 Server Certificate	>
4 CA Certificates	>

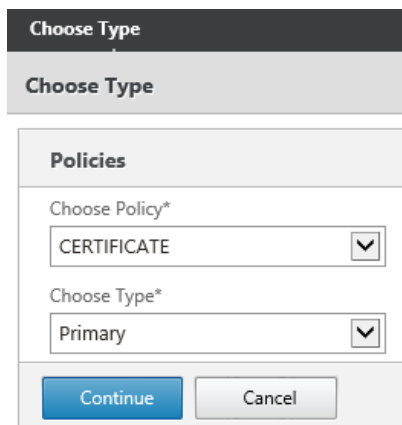
Create certificate authentication policy

NOTE

For detailed information on how the certificate authentication policy works in conjunction with the LDAP authentication policy to map the PIV authentication certificate from the smart card to an Active Directory user account, refer to section [Appendix F: How NetScaler Gateway Certificate and LDAP Authentication Policies Map to an Active Directory User Account](#)

- Under the Authentication section, click the plus icon on the right-hand side:

2. Choose **Certificate Policy** and set the type to **Primary**:



Choose Type

Choose Type

Policies

Choose Policy*

CERTIFICATE

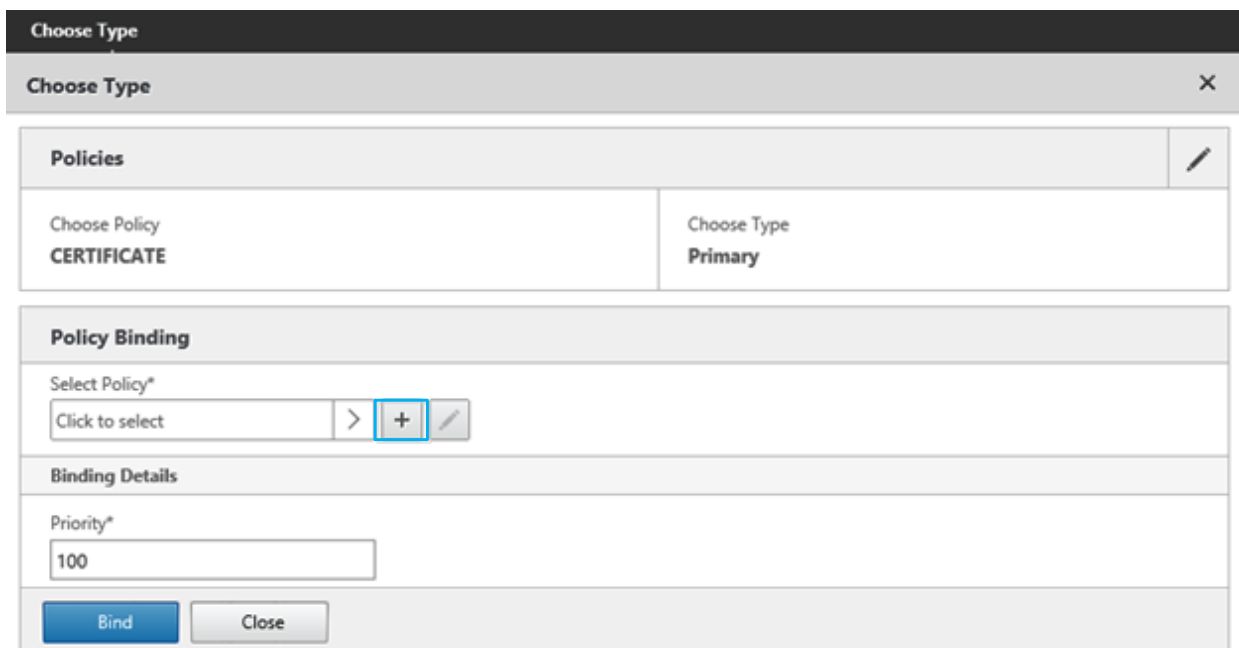
Choose Type*

Primary

Continue Cancel

3. Click **Continue**.

The following page is displayed:



Choose Type

Choose Type

Policies

Choose Policy

CERTIFICATE

Choose Type

Primary

Policy Binding

Select Policy*

Click to select

Binding Details

Priority*

100

Bind Close

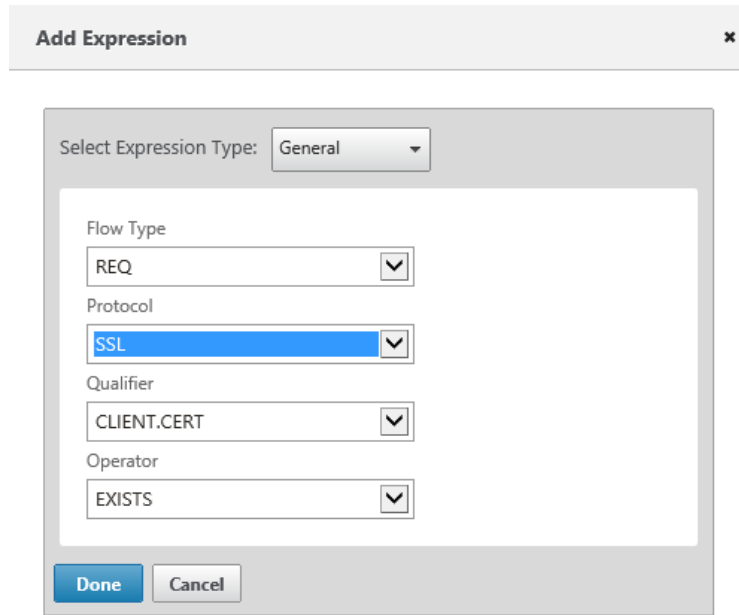
- Click the plus icon in the Policy Binding area. The following page is displayed:

- Click the plus icon in the Authentication CERT Policy area. Then populate the Authentication CERT Server page as follows:

- Provide a suitable name, set Two Factor to OFF, and set User Name Field to SubjectAltName:PrincipalName.
- Click **Create**.

```
add authentication certAction f2-cert-server -twoFactor OFF -userNameField
SubjectAltName:PrincipalName
```

- On the Authentication CERT Policy page, provide a suitable policy name, select the server you just created from the server drop-down list, and enter the following policy expression:



Add Expression [X]

Select Expression Type: **General** [v]

Flow Type: **REQ** [v]

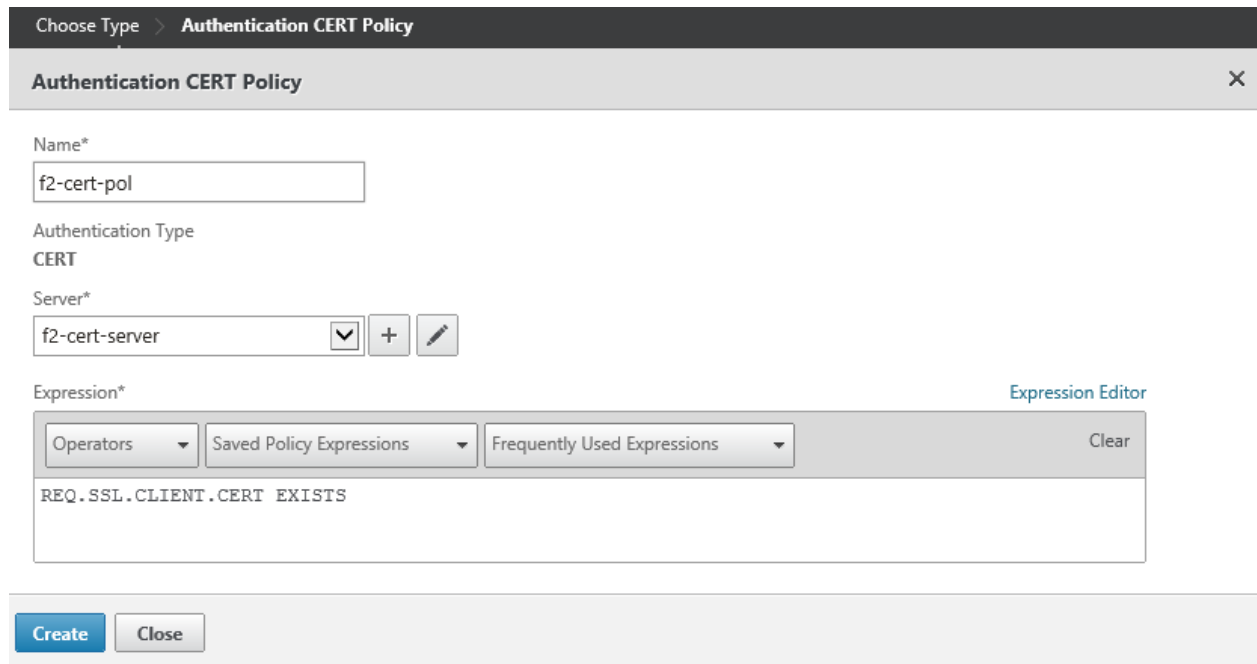
Protocol: **SSL** [v]

Qualifier: **CLIENT.CERT** [v]

Operator: **EXISTS** [v]

Done **Cancel**

The Authentication CERT Policy page should now look like this:



Choose Type > Authentication CERT Policy

Authentication CERT Policy [X]

Name*
f2-cert-pol

Authentication Type
CERT

Server*
f2-cert-server [v] [+] [edit]

Expression* Expression Editor

Operators [v] Saved Policy Expressions [v] Frequently Used Expressions [v] Clear

REQ.SSL.CLIENT.CERT EXISTS

Create **Close**

- Click **Create**.

```
add authentication certPolicy f2-cert-pol "REQ.SSL.CLIENT.CERT EXISTS" f2-
cert-server
```

The Choose Type page should now be populated as follows:

Choose Type	
Choose Type ×	
Policies ✎	
Choose Policy CERTIFICATE	Choose Type Primary
Policy Binding	
Select Policy* <input type="text" value="f2-cert-pol"/> > + ✎	
More	
Binding Details	
Priority* <input type="text" value="100"/>	
<input type="button" value="Bind"/> <input type="button" value="Close"/>	

10. Click **Bind**.

```
bind vpn vserver fed-nsg.f2.ctxs -policy f2-cert-pol -priority 100
```

NOTE

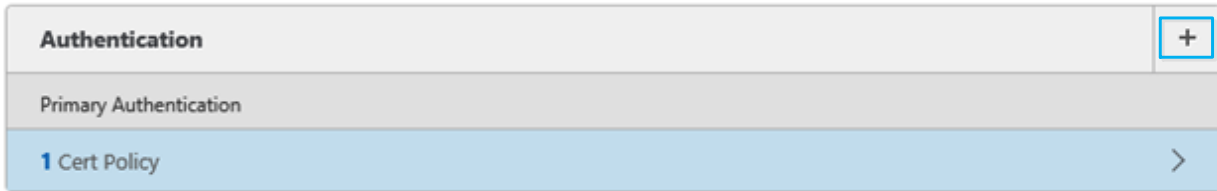
The certificate authentication policy binding must have a higher priority (lower number) than the LDAP authentication policy binding. In this example, the priority for the certificate authentication policy is set to 100. The priority for the LDAP authentication policy will be set to a lower priority (110) in the next section.

The Authentication section should now look as follows:

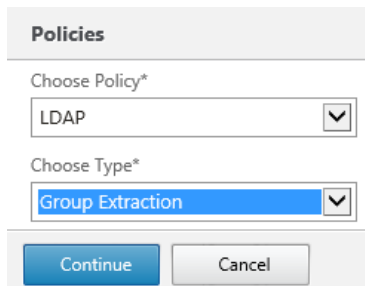
Authentication	+
Primary Authentication	
1 Cert Policy	>

Bind LDAP authentication policy

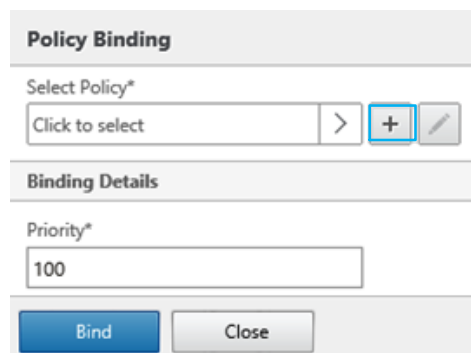
1. In the Authentication section, click the plus icon on the right-hand side to add another Authentication Policy:



2. Choose LDAP as policy, and select Group Extraction as Type:



3. Click Continue.
4. In the Policy Binding section, click the plus icon to create a policy:



5. Provide a suitable name, select the LDAP server you created earlier, and enter the Expression.

Choose Type > **Authentication LDAP Policy**

Authentication LDAP Policy

Name*

Server*
   

Expression*

Operators 
Saved Policy Expressions 
Frequently Used Expressions 

Create
Close

6. Click **Create**.

```
add authentication ldapPolicy f2-ldap-policy ns_true f2-ldap-server
```

The following is displayed:

Policies

Choose Policy
LDAP

Choose Type
Group Extraction

Policy Binding

Select Policy*
   

▶ **More**

Binding Details

Priority*

Bind
Close

- Change the priority in the Binding Details section to a value that is higher numerically (and therefore have lower priority: 110 in this example) than the certificate authentication policy (set to 100):

Choose Type

Choose Type

Policies

Choose Policy LDAP	Choose Type Group Extraction
------------------------------	--

Policy Binding

Select Policy*

f2-ldap-policy > + ✎

► More

Binding Details

Priority*

110 x ?

Bind **Close**

- Click **Bind**.

```
bind vpn vserver fed-nsg.f2.ctxs -policy f2-ldap-policy -priority 110
```

The Authentication section will now look as follows:

Authentication		+
Primary Authentication		
1 LDAP Policy		>
1 Cert Policy		>

Set SSL parameters

1. Click the **Edit** icon in the SSL Parameters section:

SSL Parameters			
Enable DH Param	DISABLED	Clear Text Port	0
Enable Ephemeral RSA	DISABLED	Enable Cipher Redirect	DISABLED
Enable Session Reuse	ENABLED	Client Authentication	DISABLED
Time-out	120	Send Close-Notify	YES
SSL Redirect	DISABLED	PUSH Encryption Trigger	Always
		SNI Enable	DISABLED
		SSLv2 Redirect	DISABLED
		SSLv2	DISABLED
		SSLv3	ENABLED
		TLSv1	ENABLED
		TLSv11	DISABLED
		TLSv12	DISABLED

2. Select the Client Authentication check box. Once selected, you can choose whether Client Certificate should be optional or mandatory. Select **Mandatory**. Deselect the SSLv3 check box. (Only TLSv1 should be selected).

SSL Parameters	
☐ Enable DH Param ☐ Enable Ephemeral RSA ☒ Enable Session Reuse Time-out <input type="text" value="120"/> ☐ Enable Cipher Redirect ☐ SSLv2 Redirect ☒ Client Authentication Client Certificate* <input type="text" value="Mandatory"/>	☐ SSL Redirect ☐ SNI Enable ☒ Send Close-Notify Clear Text Port <input type="text" value="0"/> PUSH Encryption Trigger <input type="text" value="Always"/>
Protocol ☐ SSLv2 ☐ SSLv3 ☒ TLSv1 ☐ TLSv11 ☐ TLSv12	
<input type="button" value="OK"/>	

3. Click **OK**.

```
set ssl vserver fed-nsg.f2.ctxs -clearTextPort 0 -dh DISABLED -dhCount 0 -
eRSA DISABLED -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -
sslv2Redirect DISABLED -clientAuth ENABLED -clientCert Mandatory -sslRedirect
DISABLED -redirectPortRewrite DISABLED -nonFipsCiphers DISABLED -ssl2
DISABLED -ssl3 DISABLED -tls1 ENABLED -tls11 DISABLED -tls12 DISABLED -
SNIEnable DISABLED -pushEncTrigger Always -sendCloseNotify YES
```

The following will be displayed in the GUI:

SSL Parameters							
Enable DH Param	DISABLED	Clear Text Port	0	SSLv2 Redirect	DISABLED		
Enable Ephemeral RSA	DISABLED	Enable Cipher Redirect	DISABLED	SSLv2	DISABLED		
Enable Session Reuse	ENABLED	Client Authentication	ENABLED	SSLv3	DISABLED		
Time-out	120	Client Certificate	Mandatory	TLSv1	ENABLED		
SSL Redirect	DISABLED	Send Close-Notify	YES	TLSv11	DISABLED		
		PUSH Encryption Trigger	Always	TLSv12	DISABLED		
		SNI Enable	DISABLED				

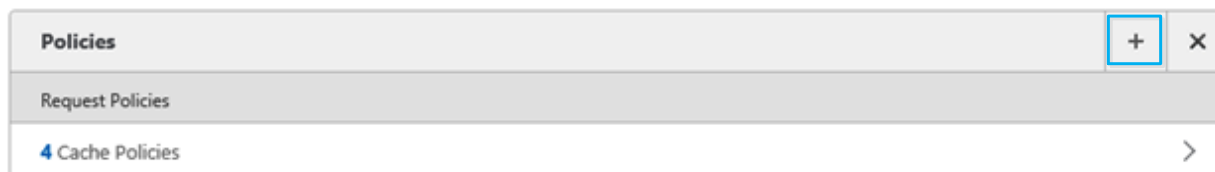
Create session policy for Citrix Receiver client

1. This policy will be configured to kick in when users access the NetScaler Gateway via Citrix Receiver.

NOTE

When a user (for example, User A) logs on to the NetScaler Gateway and session policy is applied, the relevant action would be applied to that particular user. Any parameter that is not applied in the policy will get inherited from the global VPN parameters.

2. In the Policies section, click the plus icon on the right-hand side to add a new session policy:



3. Choose **Session** under Policy and **Request** under Type:

Policies

Choose Policy*
 Session

Choose Type*
 Request

Continue
 Cancel

4. Click **Continue**. The following will be displayed in the GUI:

Policies

Choose Policy
Session

Choose Type
Request

Policy Binding

Select Policy*

Click to select > **+** ✎

Binding Details

Priority*

100 x ?

Bind **Close**

5. Click on the plus icon in the Policy Binding section to create a new policy.
6. In the Action area, click the plus icon to create a new policy:

Action*

▼ **+** ✎

The following page is displayed:

|| ?

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

Network Configuration Client Experience Security Published Applications

Override Global

DNS Virtual Server

WINS Server IP

Kill Connections*

OFF

☐ **Advanced Settings**

Create **Close**

7. Enter a suitable name:

✕
?

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

Network Configuration	Client Experience	Security	Published Applications
<div>Override Global</div> <div> DNS Virtual Server <input type="text"/> ☐ </div> <div> WINS Server IP <input type="text"/> ☐ </div> <div> Kill Connections* <input type="text" value="OFF"/> ☐ ? </div> <div> ☐ Advanced Settings </div>			

Create

Close

8. Leave the Network Configuration tab at defaults.

9. Click on the **Client Experience** tab, and populate as follows:

☐ Display Home Page ☐

Home Page

URL for Web-Based Email
 ☐

Split Tunnel*
 ☐

Session Time-out (mins)
 ☐

Client Idle Time-out (mins)
 ☐

Clientless Access*
 ☒

Clientless Access URL Encoding*
 ☒

Clientless Access Persistent Cookie*
 ☐

Plug-in Type*
 ☐

☒ Single Sign-on to Web Applications ☒

Credential Index*
 ☐

KCD Account
 ☐

Single Sign-on with Windows*
 ☐

Client Cleanup Prompt*
 ☐

10. Clientless Access set to **On**.

NOTE

Clientless Access set to ON: The Full VPN plug-in for Receiver on the Endpoint will **not** launch.

Clientless Access set to OFF: The Full VPN plug-in for Receiver on the Endpoint will launch.

Clientless Access set to ALLOW: NetScaler Gateway will check the Remote Access setting on the StoreFront server:

If StoreFront Remote Access is configured with “No VPN Tunnel,” the Full VPN plug-in for Receiver on the Endpoint will **not** launch.

If StoreFront Remote Access is configured with “Full VPN Tunnel,” the Full VPN plug-in for Receiver on the Endpoint will launch.

Clientless Access URL Encoding set to **Clear**.

Clientless Access Persistent Cookie set to **DENY**.

NOTE

The clientless access persistent cookie is not relevant to StoreFront at the time of publishing this document. It's mostly useful if you are accessing a SharePoint portal or a website that is published through cVPN. In such cases, persistent cookies are used.

Plug-in Type set to **Windows/MAC OS X**.

NOTE

Plug-in Type refers to Full VPN only (not ICA Proxy or cVPN).

Options are Windows/MAC OS X or Java.

Only use Java when there is not a full plug-in available for the client machine. There is a separate setting on the NetScaler Gateway configuration that must be toggled in order for the Java plug-in to work.

You may need to use Java even for Windows or Mac clients in cases where users do not have permission to install the plug-in and happen to have JRE installed; this can be used to launch a tunnel but requires additional configuration and falls outside of the scope of this document.

Single-Sign-on to Web Applications must be selected.

NOTE

When selected, NetScaler Gateway caches logon credentials and submits them to any backend asking for credentials.

In the Security tab, set the Default Authorization Action to **ALLOW**:

Network Configuration	Client Experience	Security	Published Applications
-----------------------	-------------------	-----------------	------------------------

Override Global

Default Authorization Action*

☒

☐ Secure Browse ☐

☐ **Advanced Settings**

11. Click on the **Published Applications** tab, and populate as follows:

Network Configuration	Client Experience	Security	Published Applications
Override Global			
ICA Proxy*			
<input type="text" value="ON"/>		☒ ?	
Web Interface Address			
<input type="text" value="https://a-sf.f2.ctxs/Citrix/external_acc"/>		☒	
Web Interface Address Type*			
<input type="text" value="IPV4"/>			
Web Interface Portal Mode*			
<input type="text"/>		☐	
Single Sign-on Domain			
<input type="text"/>		☐	
Citrix Receiver Home Page			
<input type="text"/>		☐	
Account Services Address			
<input type="text" value="https://a-sf.f2.ctxs/Citrix/Roaming/Ac"/>		☒	

Set ICA Proxy to **ON** (this will enable ICA Proxy mode, also referred to as XenApp mode).

Set Web Interface Address to the StoreFront Store URL:

Store URL
https://a-sf.f2.ctxs/Citrix/external_access

Single Sign-on Domain can be left blank for this example because the environment is configured within a single Active Directory domain.

NOTE

If your backend is configured to work with a single domain, then you do not have to enter a value here. You only need to specify the Single Sign-on domain if the backend (StoreFront) is explicitly looking for this information.

Single-Sign-on domain syntax should be the NETBIOS name of your organization's Active Directory domain. (Such as F2. Not F2.ctxs)

If the server in the backend (StoreFront) requires the domain name in the credential that is forwarded to it, then the value in the Single Sign-on domain will be inserted along with the user name that the user enters when logging on. So if the user types "user1" in the user name field and Single Sign-on domain is set here as "F2," then the NetScaler Gateway will send "F2\user1" to the StoreFront server in the backend.

If a user types "F2\user1" in the user name field, the NetScaler Gateway detect this and only send the domain name once.

This setting can be overwritten by the domain that users specify at the time of logon or by the domain that the authentication server returns.

If the user enters the user name in UPN format ([user1@f2.ctxs](#)), then the UPN will be sent, and the domain name will not be prefixed.

Note that the information entered in the Single Sign-on domain field here is sent to the backend server after user authentication to the NetScaler has succeeded. The LDAP authentication policy (if configured) would have finished processing before the value in this field from the session policy (that kicks in after the authentication policy has processed successfully) is sent to the backend server (in this case, StoreFront).

Set Account Services Address to [https<FQDN of your StoreFront Server>/Citrix/Roaming/Accounts](#) (in the example test environment: <https://a-sf.f2.ctxs/Citrix/Roaming/Accounts>).

NOTE

This is optional but useful. To simplify the Receiver provisioning process, StoreFront has introduced an auto-discovery service called Account Services. Available beginning with Receiver 3.3 Standard for Windows (Mac 11.6, iOS 5.6, Android 3.1), this feature allows Receiver to automatically provision a user for internal and remote access. This service eliminates the need for users to download provisioning files and manually import them into Receiver. To allow users outside the corporate network to provision Receiver, NetScaler 10 build 69.4.nc and later now includes a new entry in the session policy profile where the StoreFront Account Services URL is specified.

The DNS server that the endpoint uses for name resolution will also require an SRV record. Details on how to configure this can be found here:

<http://support.citrix.com/proddocs/topic/dws-storefront-26/dws-plan-user-access.html#dws-plan-citrix-receiver-1>

12. Click **Create**.

```
add vpn sessionAction nsg-receiver-pol-act -winsIP 0.0.0.0 -
defaultAuthorizationAction ALLOW -SSO ON -icaProxy ON -wihome "https://a-
sf.f2.ctxs/Citrix/external_access" -wihomeAddressType IPV4 -clientlessVpnMode
ON -storefronturl "https://a-sf.f2.ctxs/Citrix/Roaming/Accounts"
```

13. Enter the following in the NetScaler Gateway Session Policy page:

NetScaler Gateway Session Policy

Name*

Action*
   

Expression*

14. Click **Create**.

```
add vpn sessionPolicy nsg-receiver-pol "REQ.HTTP.HEADER User-Agent CONTAINS
CitrixReceiver && REQ.HTTP.HEADER X-Citrix-Gateway EXISTS" nsg-receiver-pol-
act
```

The following will be displayed in the GUI:

Policies	
Choose Policy Session	Choose Type Request

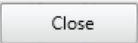
Policy Binding

Select Policy*
   

► **More**

Binding Details

Priority*

15. Click **Bind**.

```
bind vpn vserver fed-nsg.f2.ctxs -policy nsg-receiver-pol -priority 100
```

The following will be displayed in the Policies section in the GUI:

Policies		+	×
Request Policies			
1	Session Policy	>	
4	Cache Policies	>	

Create session policy for web browser client

This policy will be configured to kick in when users access the NetScaler Gateway via a web browser.

1. In the Policies section, click the plus icon on the right-hand side to add a new session policy:

Policies		+	×
Request Policies			
1	Session Policy	>	
4	Cache Policies	>	

2. Choose the following type of policy:

Policies

Choose Policy*

Session

Choose Type*

Request

Continue

Cancel

3. Click Continue.

The following is displayed in the GUI:

Policies			
Choose Policy Session		Choose Type Request	
<div> Add Binding Unbind Edit </div> <div>Search</div>			
Priority	Policy Name	Expression	Action
100	nsg-receiver-pol	REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiv...	nsg-receiver-pol-act
<div>Close</div>			

4. Click the **Add Binding** button. The Policy Binding page is displayed:

Choose Type > **Policy Binding**

Policy Binding

Select Policy*

Click to select > +

Binding Details

Priority*

110 x ?

Bind

Close

5. Click the plus icon to create a new policy:

The following is displayed in the GUI:

Choose Type > Policy Binding > NetScaler Gateway Session Policy

NetScaler Gateway Session Policy

Name*

Action*

nsg-receiver-pol-act

Expression*

Operators Saved Policy Expressions Frequently Used Expressions

Create Close

- Do not use the action for the web browser policy that you created for the Receiver policy earlier (that is displayed by default). Click the plus icon to create a new session policy action.

Choose Type > Policy Binding > NetScaler Gateway Session Policy > NetScaler Gateway Session Profile

NetScaler Gateway Session Profile

Name*

nsg-web-pol-act

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

Network Configuration Client Experience Security Published Applications

Override Global

DNS Virtual Server

WINS Server IP

Kill Connections*

OFF

Advanced Settings

- Provide an appropriate policy action name. In this case, **nsg-web-pol-act**.

8. Leave the Network Configuration tab with defaults.
9. Click on the **Client Experience** tab, and populate as follows:

☐ Display Home Page ☐

Home Page

URL for Web-Based Email
 ☐

Split Tunnel*
 ☐

Session Time-out (mins)
 ☐

Client Idle Time-out (mins)
 ☐

Clientless Access*
 ☒

Clientless Access URL Encoding*
 ☒

Clientless Access Persistent Cookie*
 ☐

Plug-in Type*
 ☒

☒ Single Sign-on to Web Applications ☒

Credential Index*
 ☐

KCD Account
 ☐

Single Sign-on with Windows*
 ☐

Client Cleanup Prompt*
 ☐

10. Leave Display Home Page deselected. (In this example configuration, we will be using ICA proxy mode).

NOTE

Display Home Page is relevant when operating in cVPN (clientless VPN) or full VPN mode, but not ICA proxy mode (also known as XenApp mode). In this example, we will be using ICA proxy (Toggled in the Published Applications tab).

If operating in cVPN mode and “Display Home Page” is left blank, the user will be directed to the NavUI when operating in cVPN or full VPN mode.

To automatically direct the user directly to StoreFront instead of the NavUI when operating in cVPN mode, the StoreFront Receiver for Web URL must be entered in the Home Page field.

The Citrix Receiver client has rewrite logic built-in. However for cVPN to work with a web browser client, the NetScaler Gateway device must perform the rewrites. The following article describes how to configure those:

<http://support.citrix.com/proddocs/topic/netScaler-gateway-105/ng-clg-custom-clientless-access-rfweb-tsk.html>

Additionally, the FQDN of your StoreFront server should be added to the Allowed Domains list: NetScaler Gateway > Global Settings > Clientless Access > Configure Domains for Clientless Access

Lastly, it is also possible to give users a choice of what mode they want to use when logging on by selecting the “Client Choices” option in the Advanced Settings section under the Client Experience tab. If selected, the user will be presented with the following page after authenticating to the NetScaler Gateway:

Please select one of the following:



11. Set Clientless Access to **On**.

NOTE

Clientless Access set to ON: The Full VPN plug-in for Receiver on the Endpoint will **not** launch.

Clientless Access set to OFF: The Full VPN plug-in for Receiver on the Endpoint will launch.

Clientless Access set to ALLOW: NetScaler Gateway will check the Remote Access setting on the StoreFront server:

If StoreFront Remote Access is configured with “No VPN Tunnel,” the full VPN plug-in for Receiver on the endpoint will **not** launch.

If StoreFront Remote Access is configured with “Full VPN Tunnel,” the full VPN plug-in for Receiver on the endpoint will launch.

Clientless Access URL Encoding set to **Clear**.

Clientless Access Persistent Cookie set to **DENY**.

NOTE

The clientless access persistent cookie is not relevant to StoreFront at time of publishing this document. Mostly useful if you are accessing a SharePoint portal or a website that is published through cVPN. In such cases, persistent cookies get used.

Plug-in Type set to **Windows/MAC OS X**.

NOTE

Plug-in Type refers to full VPN only (not ICA proxy or cVPN).

Options are Windows/MAC OS X or Java.

Only use Java when there is not a full plug-in available for the client machine. There is a separate setting on the NetScaler Gateway configuration that must be toggled in order for the Java plug-in to work.

You may need to use Java even for Windows or Mac clients in cases where users do not have permission to install the plug-in and happen to have JRE installed; this can be used to launch a tunnel but requires additional configuration and falls outside of the scope of this document.

Single Sign-on to web applications should be selected

NOTE

When selected, NetScaler Gateway caches logon credentials and submits them to any backend asking for credentials.

In the Security tab, set the Default Authorization Action to **ALLOW**:

Network Configuration	Client Experience	Security	Published Applications
-----------------------	-------------------	-----------------	------------------------

Override Global

Default Authorization Action*

ALLOW

▼

✓

☐ Secure Browse
 ☐

☐ **Advanced Settings**

12. Click on the **Published Applications** tab, and populate as follows:

Network Configuration	Client Experience	Security	Published Applications
Override Global			
ICA Proxy*			
<input type="text" value="ON"/>			☒
Web Interface Address			
<input type="text" value="https://a-sf.f2.ctxs/Citrix/external_acc"/>			☒
Web Interface Address Type*			
<input type="text" value="IPV4"/>			
Web Interface Portal Mode*			
<input type="text" value="NORMAL"/>			☒
Single Sign-on Domain			
<input type="text"/>			☐
Citrix Receiver Home Page			
<input type="text"/>			☐
Account Services Address			
<input type="text"/>			☐

Set ICA Proxy to **ON** (this will enable ICA Proxy mode, also referred to as XenApp mode).

Set Web Interface Address to the StoreFront **Receiver for Web Website URL (not the Store URL)**.

Website URL
https://a-sf.f2.ctxs/Citrix/external_accessWeb

Web Interface Portal mode can be set to **NORMAL**.

Single Sign-on Domain can be left blank for this example because the environment is configured within a single Active Directory domain.

NOTE

If your backend is configured to work with a single domain, then you do not have to enter a value here. You only need to specify the Single Sign-on domain if the backend (StoreFront, for example) is explicitly looking for this information.

Single Sign-on domain syntax should be the NETBIOS name of your organization's Active Directory domain. (For example, F2. Not F2.ctxs.)

If the server in the backend (StoreFront, for example) requires the domain name in the credential that is forwarded to it, then the value in the Single Sign-on domain will be inserted along with the user name the user enters when logging on. So if the user types "user1" in the user name field, and Single Sign-on domain is set here as "F2," then the NetScaler Gateway will send "F2\user1" to the StoreFront server in the backend.

If a user types "F2\user1" in the user name field, the NetScaler Gateway detect this and only sends the domain name once.

This setting can be overwritten by the domain that users specify at the time of logon or by the domain that the authentication server returns.

If the user enters the user name in UPN format (for example, [user1@f2.ctxs](#)), then the UPN will be sent, and the domain name will not be prefixed.

Note that the information entered in the Single Sign-on domain field here is sent to the backend server after user authentication to the NetScaler has succeeded. The LDAP authentication policy (if configured) would have finished processing before the value in this field from the session policy (that kicks in after the authentication policy has processed successfully) is sent to the backend server (in this case, StoreFront).

13. Click **Create**.

```
add vpn sessionAction nsg-web-pol-act -winsIP 0.0.0.0 -
transparentInterception ON -defaultAuthorizationAction ALLOW -SSO ON -
icaProxy ON -wihome "https://a-sf.f2.ctxs/Citrix/external_accessWeb" -
wihomeAddressType IPV4 -wiPortalMode NORMAL -clientlessVpnMode ON -
clientlessModeUrlEncoding TRANSPARENT
```

14. In the NetScaler Gateway Session Policy page, provide a name, ensure that the action you select is the one that was just created, and enter the following Policy Expression:

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

NetScaler Gateway Session Policy

Name

nsg-web-pol

Action*

nsg-web-pol-act

Expression*

Operators

Saved Policy Expressions

Frequently Used Expressions

REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver

NOTE

Some documents indicate that “REQ.HTTP.HEADER Referer EXISTS” be included as well in the Receiver for Web policy expression. This is not necessary. In addition, there are currently issues with certain web browsers that will prevent the policy from ever kicking in if “REQ.HTTP.HEADER Referer EXISTS” is included in the expression.

15. Click **Create**.

```
add vpn sessionPolicy nsg-web-pol ns_true nsg-web-pol-act
```

The Policy Binding page is displayed:

Choose Type > Policy Binding

Policy Binding

Select Policy*

nsg-web-pol

More

Binding Details

Priority*

110

Bind

Close

16. Click **Bind**.

```
bind vpn vserver fed-nsg.f2.ctxs -policy nsg-web-pol -priority 110
```

The following is displayed in the GUI:

<div> Add Binding Unbind Edit </div> <div>Search</div>			
Priority	Policy Name	Expression	Action
100	nsg-receiver-pol	REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiv...	nsg-receiver-pol-act
110	nsg-web-pol	REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixR...	nsg-web-pol-act
<div>Close</div>			

17. Click **Close**.

The Policies section will now appear as follows in the GUI:

Policies	+	×
Request Policies		
2 Session Policies	>	
4 Cache Policies	>	

Set STA server details

1. In the Advanced section, click **Published Applications**:

Advanced
+ SSL Profile
+ SSL Ciphers
+ SSL Policies
+ Profiles
+ Intranet IP Addresses
+ Intranet Applications
+ Published Applications
+ Other Settings

The Published Applications section will be shown:

Published Applications	×
No Next HOP Server	>
No STA Server	>
No Url	>

- Click on **STA Server**.
- Enter the name of the server where the STA service is running. The Delivery Controller hosts the STA service. The syntax is `https://<FQDN of STA Server>`

STA Server Binding

STA Server Binding

Secure Ticket Authority Server*

https://a-ddc.f2.ctxs

Secure Ticket Authority Server Address Type

IPV4

Bind

Close

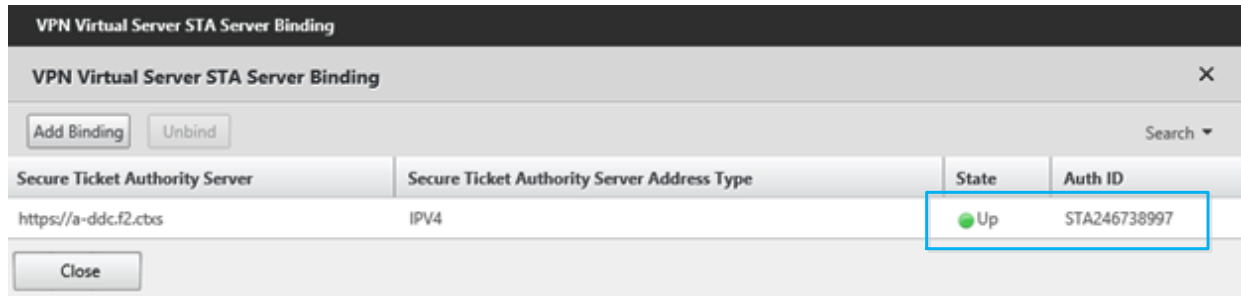
- Click **Bind**.

```
bind vpn vserver fed-nsg.f2.ctxs -staServer "https://a-ddc.f2.ctxs" -
staAddressType IPV4
```

The Published Applications section in the GUI will now appear as follows:

Published Applications	×
No Next HOP Server	>
1 STA Server	>
No Url	>

- Click **STA Server** to ensure that the State is **Up** and an Auth ID is listed:



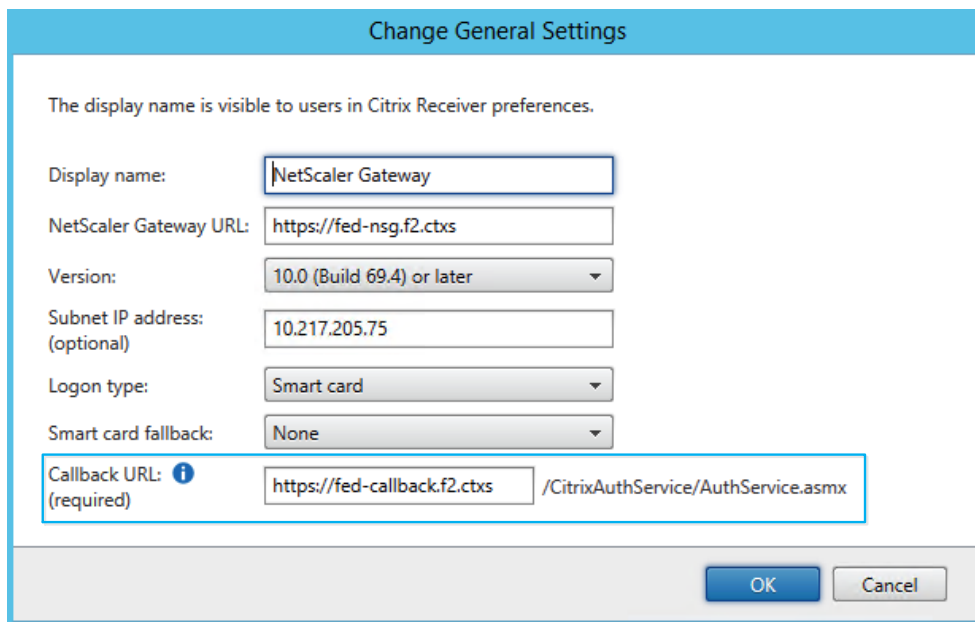
6. Click **Close**.
7. Save ns conf

NOTE

Ensure that **external** DNS servers can resolve the IP address of the NetScaler Gateway Virtual Server.

NetScaler Gateway virtual server configuration for fed-callback

Only StoreFront uses the callback virtual server. The callback URL **must** be different from the NetScaler Gateway Virtual Server URL, particularly when the SSL parameter for the NetScaler Gateway Virtual Server is set to mandatory client certificate authentication (as it would be in a smart card environment). This prevents the StoreFront server from performing client authentication when establishing the TLS session with the NetScaler Gateway, which it would be forced to do if it performed the callback to the same virtual server that users connect to. The URL for the callback server is configured in the NetScaler Gateway pane on the StoreFront server:



The callback virtual server on the NetScaler Gateway requires only a virtual server that is bound to a certificate and corresponding key. There is no need to bind any authentication or session policies to the callback virtual server.

NOTE

The StoreFront server calls back to the NetScaler Gateway to verify that the user's session originated from the same NetScaler Gateway device that is known to and trusted by StoreFront. During the callback, StoreFront provides the NetScaler Gateway with the user name (typically the UPN quoted to it by the NetScaler — NetScaler having done the LDAP mapping (for details refer to section [Appendix F: How NetScaler Gateway Certificate and LDAP Authentication Policies Map to an Active Directory User Account](#)) and password, if StoreFront has it) and the session identifier. The NetScaler Gateway then checks to see if the user name, password, and session identifier that StoreFront sent it during the callback match the user name, password, and session identifier that the NetScaler Gateway device provided to StoreFront in the first place. Doing this effectively provides the equivalent assurance that would be achieved if the NetScaler Gateway had digitally signed a SAML token.

After the callback succeeds, the StoreFront server performs a Kerberos S4U information lookup on the domain controller against the user name and extracts a list of user and group SIDs that the StoreFront server passes on to the Delivery Controller.

Create fed-callback virtual server

1. In the NetScaler GUI, navigate to:

NetScaler > NetScaler Gateway > NetScaler Gateway Virtual Servers

The following will be displayed:

Add Edit Delete Statistics Action Search ▼						
Name	State	IP Address	Port	Protocol	Maximum Users	Current Users
fed-nsg.f2.ctxs	Up	10.217.205.72	443	SSL	0	0

2. Click Add.
3. Enter the name, IP address and port:

VPN Virtual Server

Basic Settings

Name*

IPAddress*
 ☐ IPv6

Port*

▶ More

- Click **OK**.

```
add vpn vserver fed-callback.f2.ctxs SSL 10.217.205.73 -range 1 443 -state
ENABLED -authentication ON -doubleHop DISABLED -maxAAAUsers 0 -icaOnly OFF -
icaProxySessionMigration OFF -deviceCert OFF -downStateFlush DISABLED -
Listenpolicy none -appflowLog DISABLED -icmpVsrResponse PASSIVE -RHISTate
PASSIVE -cginfraHomePageRedirect ENABLED -l2Conn OFF -deploymentType NONE
```

The following is displayed in the GUI:

VPN Virtual Server

Basic Settings			
Name	fed-callback.f2.ctxs	Max Users	
IPAddress	10.217.205.73	Max Login Attempts	
Port	443	Failed Login Timeout	
		State	true
		ICA Only	false
		Enable Authentication	true
		Double Hop	false
		Down State Flush	false
		AppFlow Logging	false
		ICA Proxy Session Migration	false
		Enable Device Certificate	false

Certificates	
No Server Certificate	>
No CA Certificate	>
<input type="button" value="OK"/>	

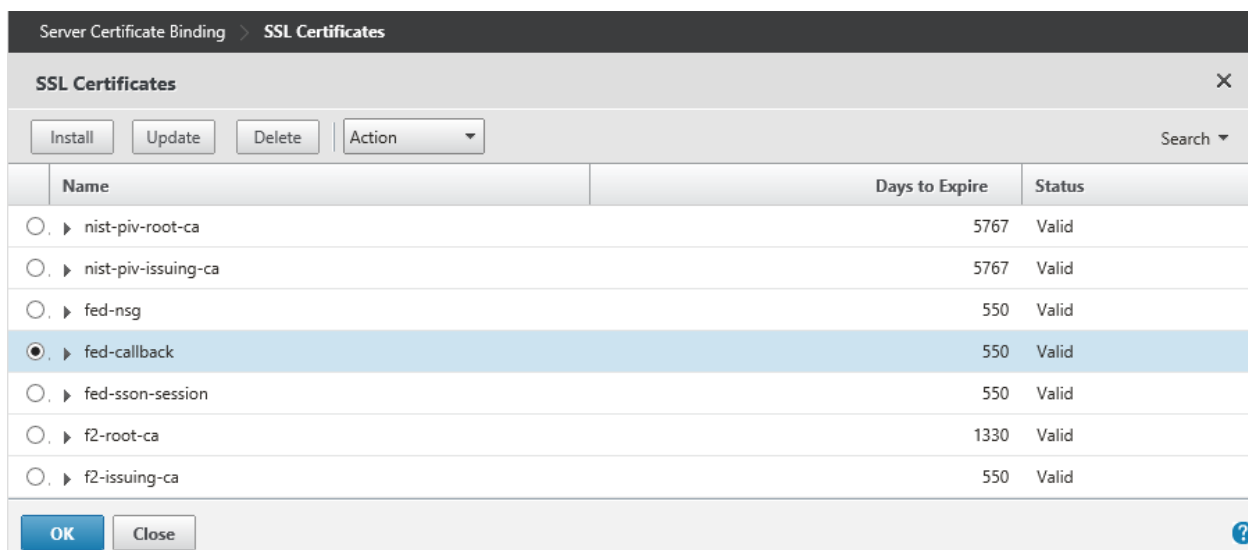
Bind fed-callback virtual server certificate

- In the Certificates section, click on **Server Certificate**. The Server Certificate Binding page is displayed. Click on the arrow to select a certificate:

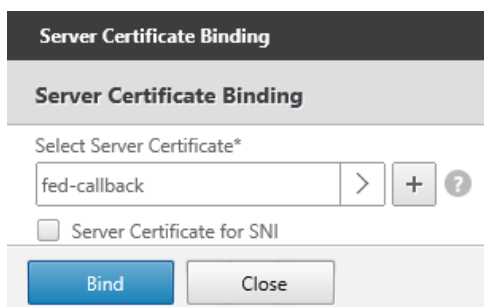
Select Server Certificate*

Click to select	>	<input type="button" value="+"/>
-----------------	---	----------------------------------

- Select the fed-callback certificate you installed in section [Install the fed-callback certificate file on NetScaler](#).



3. Click **OK**. The following is displayed in the GUI:



4. Click **Bind**.

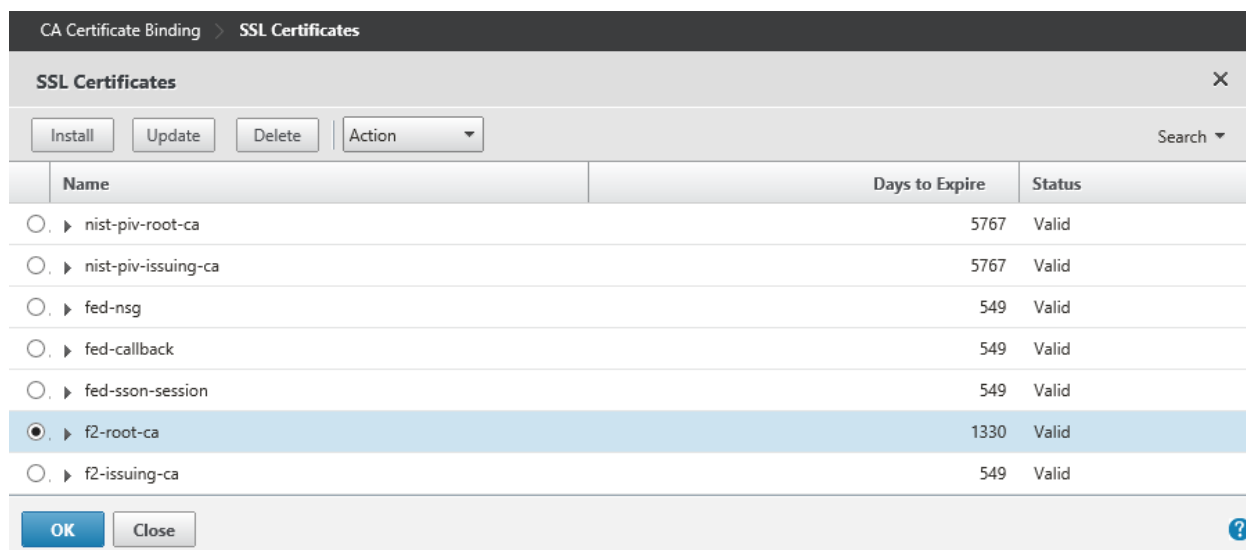
```
bind ssl vserver fed-callback.f2.ctxs -priority 0 -certkeyName fed-callback -
crlCheck Optional
```

The Certificate section in the GUI now appears as follows:



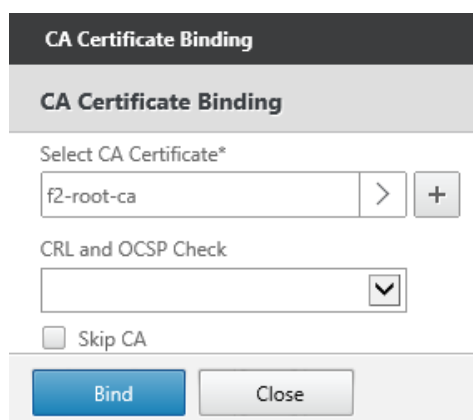
Bind your organization's root CA certificate to the callback virtual server

1. In the Certificates section, click on **CA Certificate**.
2. Select your organization's root CA certificate that you installed in section [Install your organization's root CA certificate file on NetScaler](#)



3. Click **OK**.

The following is displayed in the GUI:



4. Click **Bind**.

```
bind ssl vserver fed-callback.f2.ctxs -priority 0 -certkeyName f2-root-ca -CA -crlCheck Optional
```

The Certificate section in the GUI now appears as follows:

Certificates	
1 Server Certificate	>
1 CA Certificate	>

Bind your organization's issuing CA certificate to the callback virtual server

1. Click on **CA Certificate** in the Certificate section. The following is displayed in the GUI:

The screenshot shows the 'SSL Virtual Server CA Certificate Binding' dialog box. It has a title bar with the same text. Below the title bar, there are two buttons: 'Add Binding' and 'Unbind'. The main area is a table with three columns: 'Certificate', 'CRL and OCSP Check', and 'Skip CA'. The first row shows 'f2-root-ca' under 'Certificate', 'OCSP Optional' under 'CRL and OCSP Check', and an 'X' under 'Skip CA'. At the bottom, there is a 'Close' button.

Certificate	CRL and OCSP Check	Skip CA
f2-root-ca	OCSP Optional	X

2. Click **Add Binding**. The CA Certificate Binding page is displayed.
3. Click on the arrow to select a certificate:

Select CA Certificate*

The screenshot shows a dropdown menu with the text 'Click to select' and a right-pointing arrow button. There is also a '+' button to the right of the arrow button.

4. Select your organization's issuing CA certificate that you installed in section [Install your organization's issuing CA certificate file on NetScaler](#):

The screenshot shows the 'SSL Certificates' page in the NetScaler GUI. The breadcrumb trail at the top is 'SSL Virtual Server CA Certificate Binding > CA Certificate Binding > SSL Certificates'. Below the breadcrumb trail, there are buttons for 'Install', 'Update', 'Delete', and an 'Action' dropdown menu. There is also a 'Search' dropdown menu. The main area is a table with three columns: 'Name', 'Days to Expire', and 'Status'. The table contains several rows of certificates. The row for 'f2-issuing-ca' is selected, indicated by a blue background.

Name	Days to Expire	Status
nist-piv-root-ca	5767	Valid
nist-piv-issuing-ca	5767	Valid
fed-nsg	549	Valid
fed-callback	549	Valid
fed-sson-session	549	Valid
f2-root-ca	1330	Valid
f2-issuing-ca	549	Valid

5. Click **OK**.

The following is displayed in the GUI:

6. Click **Bind**.

```
bind ssl vserver fed-callback.f2.ctxs -priority 0 -certkeyName f2-issuing-ca
-CA -crlCheck Optional
```

The following is displayed in the GUI:

Certificate	CRL and OCSP Check	Skip CA
f2-root-ca	OCSP Optional	X
f2-issuing-ca	OCSP Optional	X

7. Click **Close**.

The Certificates section in the GUI now appear as follows:

Certificates
1 Server Certificate >
2 CA Certificates >

NOTE

Ensure that your organization's **internal** DNS server can resolve the IP address of the callback virtual server.

Set SSL parameters

1. Click on the **Edit** pencil icon in the SSL Parameters section:

SSL Parameters			
Enable DH Param	DISABLED	Clear Text Port	0
Enable Ephemeral RSA	DISABLED	Enable Cipher Redirect	DISABLED
Enable Session Reuse	ENABLED	Client Authentication	DISABLED
Time-out	120	Send Close-Notify	YES
SSL Redirect	DISABLED	PUSH Encryption Trigger	Always
		SNI Enable	DISABLED
		SSLv2 Redirect	DISABLED
		SSLv2	DISABLED
		SSLv3	ENABLED
		TLSv1	ENABLED
		TLSv11	DISABLED
		TLSv12	DISABLED

2. Set parameters as follows:

SSL Parameters	
☐ Enable DH Param ☐ Enable Ephemeral RSA ☒ Enable Session Reuse Time-out <input type="text" value="120"/> ☐ Enable Cipher Redirect ☐ SSLv2 Redirect ☐ Client Authentication	☐ SSL Redirect ☐ SNI Enable ☒ Send Close-Notify Clear Text Port <input type="text" value="0"/> PUSH Encryption Trigger <input type="text" value="Always"/>
Protocol ☐ SSLv2 ☐ SSLv3 ? ☒ TLSv1 ☐ TLSv11 ☐ TLSv12	
<input type="button" value="OK"/>	

3. Ensure the Client Authentication check box is blank and that only TLSv1 is selected in the Protocol section.
4. Click **OK**.

```
set ssl vserver fed-callback.f2.ctxs -clearTextPort 0 -dh DISABLED -dhCount 0
-eRSA DISABLED -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -
sslv2Redirect DISABLED -clientAuth DISABLED -sslRedirect DISABLED -
redirectPortRewrite DISABLED -nonFipsCiphers DISABLED -ssl2 DISABLED -ssl3
DISABLED -tls1 ENABLED -tls11 DISABLED -tls12 DISABLED -SNIEnable DISABLED -
pushEncTrigger Always -sendCloseNotify YES
```

The SSL Parameters Section in the GUI should now appear as follows:

SSL Parameters							
Enable DH Param	DISABLED	Clear Text Port	0	SSLv2 Redirect	DISABLED		
Enable Ephemeral RSA	DISABLED	Enable Cipher Redirect	DISABLED	SSLv2	DISABLED		
Enable Session Reuse	ENABLED	Client Authentication	DISABLED	SSLv3	DISABLED		
Time-out	120	Send Close-Notify	YES	TLSv1	ENABLED		
SSL Redirect	DISABLED	PUSH Encryption Trigger	Always	TLSv11	DISABLED		
		SNI Enable	DISABLED	TLSv12	DISABLED		

5. Click **Done**.

6. Now is a good time to save your configuration:

```
save ns conf
```

NOTE

How to configure the SSON session virtual server is described in section [Third reduction \(one PIN prompt\)](#)

Windows 7 (64 bit) Domain-Joined External Endpoint

Test environment assumptions

- Operating system is 64-bit Windows 7 with Service Pack 1.
- Citrix Receiver is version 4.2 (Add/Remove Programs reports 14.2.0.10).
- The smart card middleware is 64-bit ActivClient 7.0.2.
- Mozilla Firefox is installed on the endpoint (Certain middleware requires a PKCS#11 application to be installed in order to install the PKCS#11 middleware libraries during middleware installation). However, configuring a browser (including Firefox) to work with smart cards is outside of the scope of the first edition of this guide.
- PIN caching is not turned on in the smart card middleware.
- The endpoint is domain-joined
- The endpoint machine cannot directly access the machines on the internal network (such as the StoreFront server, VDA etc.).

Prerequisites

- The endpoint trusts your organization's root and intermediate certificate authorities. In other words, copies of the CA certificates for your organization's root and issuing certificate authorities are located in the endpoint's Local Computer Trusted Root Certification Authorities and Intermediate Certification Authorities stores, respectively.

Configuration Steps

Install middleware

1. Follow the instructions in section [Appendix E: Install ActivClient 7.0.2 on Windows 7 x64](#)

Install card reader driver

1. Connect a physical USB smart card reader to the computer. Provided that an Internet connection is available and automatic fetching of device drivers is not disabled via policy, Windows will automatically install an appropriate device driver for the smart card reader.

NOTE

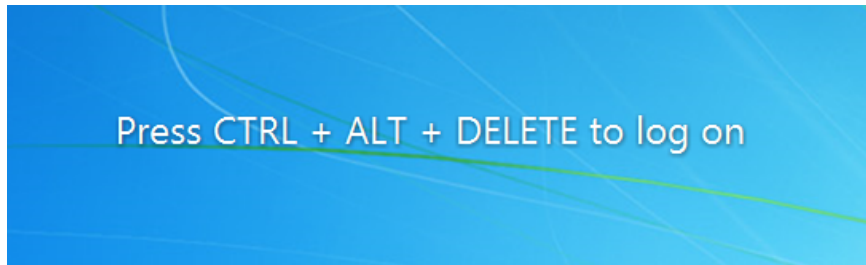
The smart card reader device driver and middleware are often incorrectly assumed to be the same thing. A type 1 CCID-compliant smart card reader is just another peripheral device (such as a mouse or keyboard).

NOTE

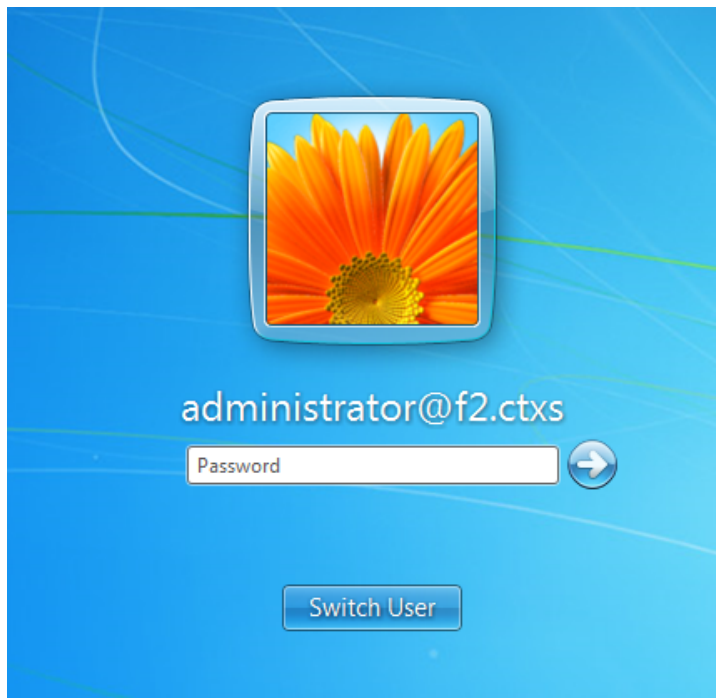
This step assumes that you are using a USB-based CCID-compliant ZKA type 1 smart card reader and will be using card reader drivers provided via the Microsoft Update Catalog. OEM card reader drivers can be installed instead if your organization requires it.

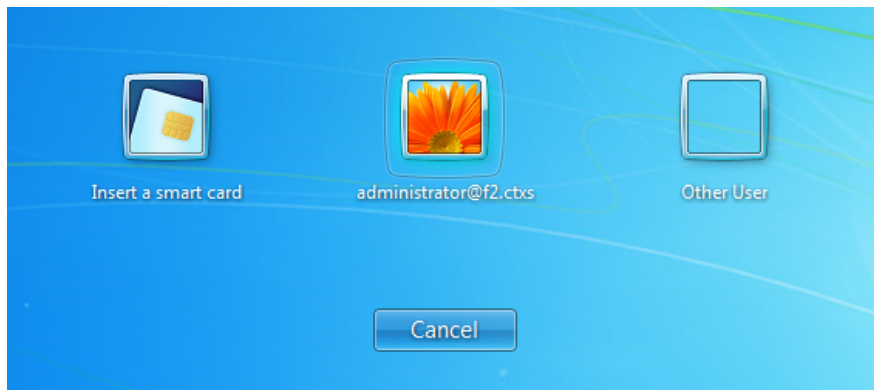
Test smart card logon to Windows

1. Ensure that the smart card reader is physically attached to the endpoint. Start up the Windows 7 computer. The logon screen will be displayed as follows:

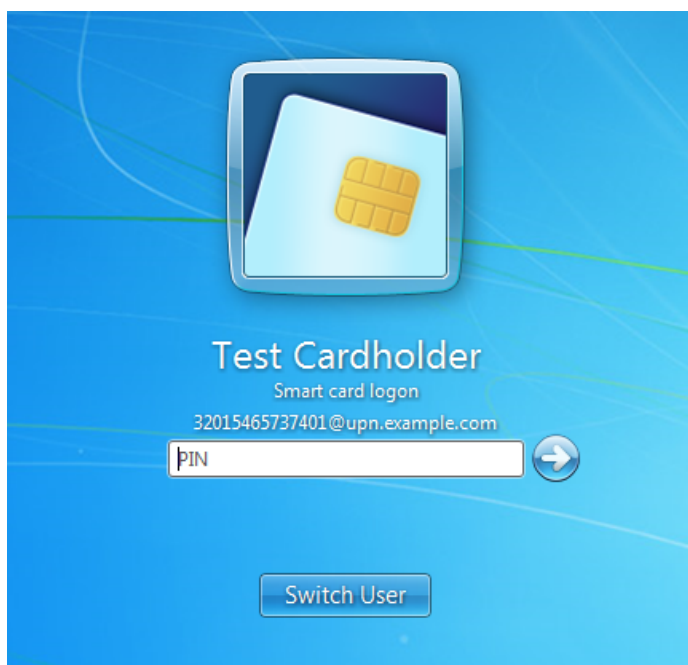


2. Press **CTRL + ALT + DELETE**. The logon tile for the computer's most recent user will be displayed (in this case, the administrator of the F2 domain).
3. Click **Switch User**.





A new tile for a smart card user will be displayed. Click on the smart card tile, and then insert the NIST PIV test card #1. The card will be read, and the following will be displayed:



4. Enter the PIN, and press **Enter**.

NOTE

The default PIN for NIST PIV test card #1 is 123456.

Logon should succeed, and the Test Cardholder user will be logged on to Windows.

Install Citrix Receiver

1. Log off from the Windows machine as Test Cardholder, and log on as an administrator.
2. Copy CitrixReceiver.exe to an appropriate temporary folder on the endpoint.
3. As an administrative user, from the command line, in the directory where the CitrixReceiver.exe file resides, type the following:

```
CitrixReceiver.exe /includeSSON
```

For example:

```
C:\Temp>CitrixReceiver.exe /includeSSON
```

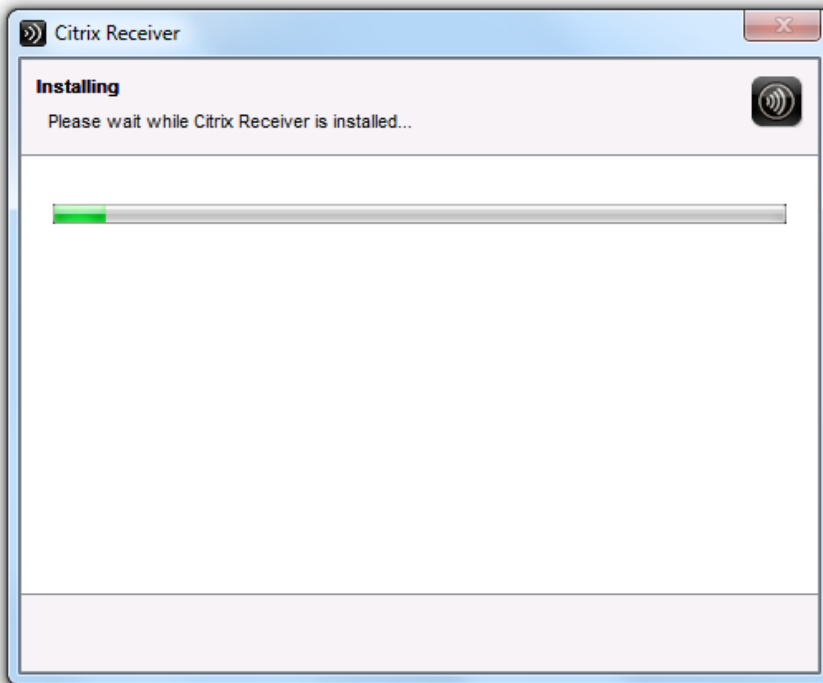
NOTE

Installing Citrix Receiver with the /includeSSON switch will install the Citrix Single Sign-on service component. However, the component will not start up until the appropriate Citrix Receiver User Component group policy has been configured via Active Directory Group Policy. The Citrix Receiver installer contains the Citrix ADM Group Policy administrative template. Where to get the Group Policy ADM administrative template post-Receiver installation on the endpoint is described later in this section. How to install the group policy snap-in on the domain controller is described in section [Add the Citrix icaclient administrative policy template \(ADM\) file](#). How to configure it is described in section [Turn on the Single Sign-on Service using group policy](#).

4. The Citrix Receiver Setup wizard opens. Click **Next**.



5. The license agreement is shown. Provided you accept the agreement, select "I accept the license agreement," and click **Install**.



6. When completed, click **Finish**.



Group policy ADM

1. Locate the `icaclient.adm` file on the endpoint. The default location is:

```
C:\Program Files (x86)\Citrix\ICA Client\Configuration\icaclient.adm
```

2. Copy the `icaclient.adm` to a temporary location on the domain controller (you will be directed to work with it in the Single Sign-on section).
3. Reboot the endpoint.

Import StoreFront provisioning file

1. Log on to the Windows endpoint as the NIST PIV test smart card user.
2. Copy the provisioning file you exported from the StoreFront server in section [Export Provisioning file](#) onto the endpoint:

The default provisioning file name is `ReceiverConfig.cr`.

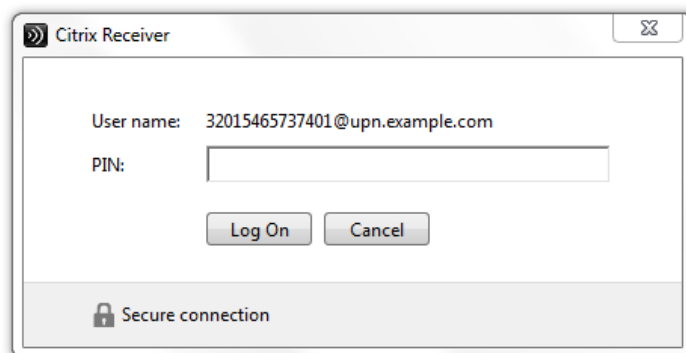
NOTE

A provisioning file is a XML file that includes the necessary information to allow Receiver to decide whether it should connect directly to StoreFront or through NetScaler Gateway. This decision is made by using the beacon addresses included in the file. If Receiver is able to resolve the internal beacon address, it will connect directly to StoreFront. By default, the internal beacon address is set to the load balancing hostname for the StoreFront servers; although, this can be changed in the beacons menu inside StoreFront.

The test environment in this guide assumes that a provisioning file is used. It is, however, possible to use the Account Services auto-discovery service. This requires an additional configuration setting on the NetScaler Gateway and an SRV record on the DNS server that the endpoint uses to resolve hostnames. For more information, refer to section [Create session policy for Citrix Receiver client](#).

3. Right-click on the provisioning file, and select **Open**.

The following dialog box will be displayed:

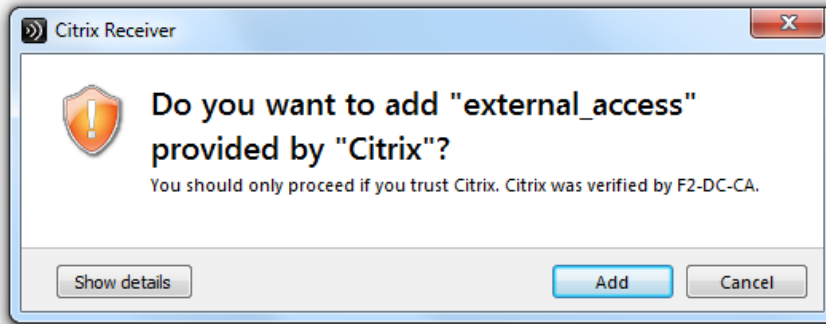


4. Enter the smart card PIN, and click **Log On**.

NOTE

The screenshots that follow contain the maximum number of possible PIN prompts. It assumes that PIN caching is turned off in the middleware and Single Sign-on is not enabled in group policy yet. In order to reduce PIN prompts, refer to section [Smart Card Single Sign-on](#)

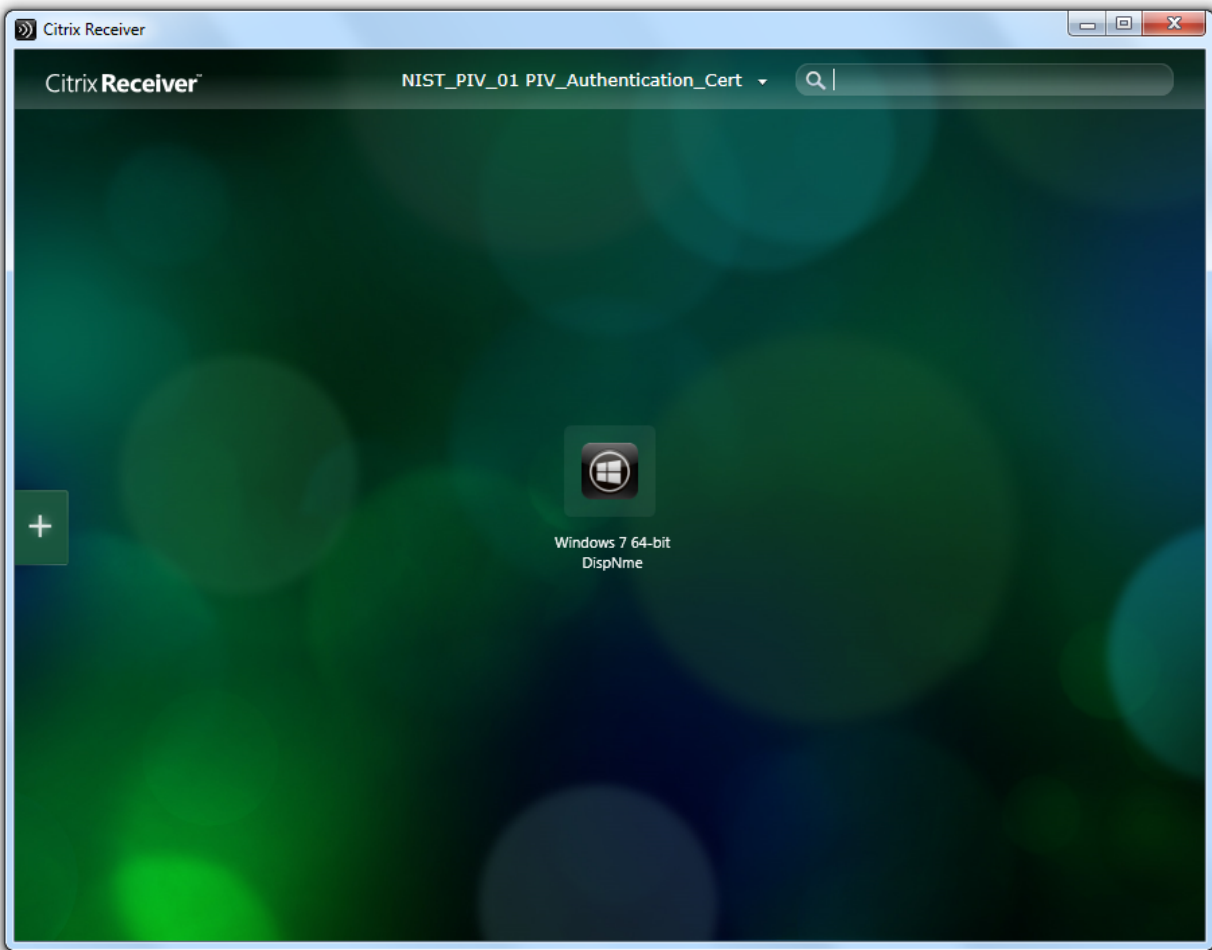
The following dialog box will be displayed:



5. Click Add.

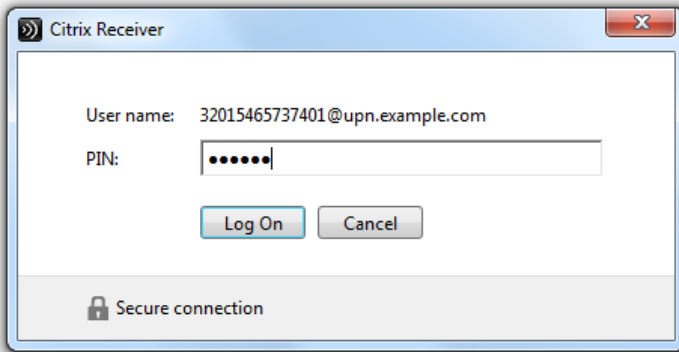
Launch Citrix Receiver

1. Receiver will launch with the NIST PIV test smart card user logged on:

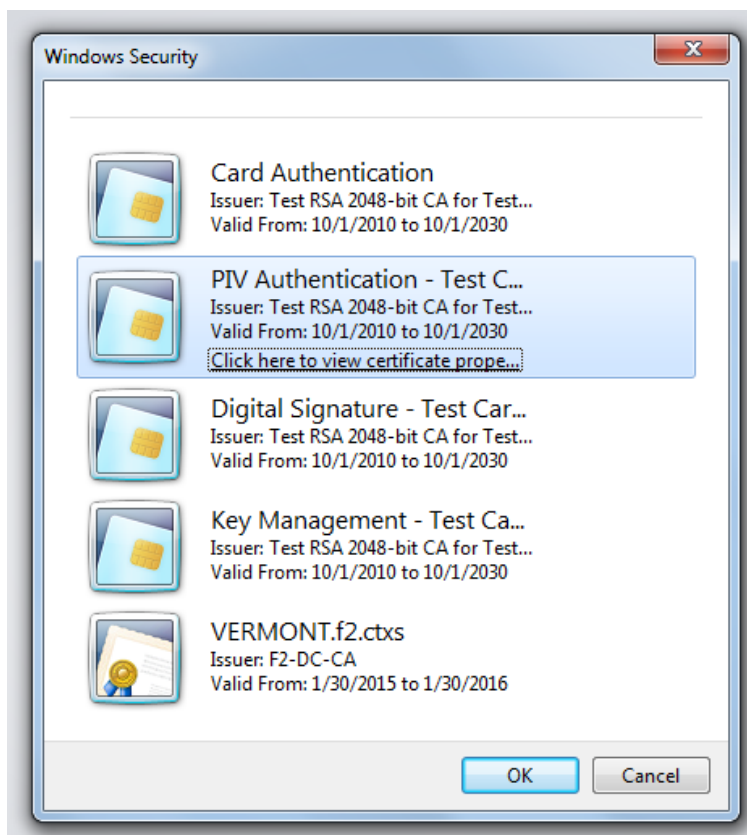


Launch desktop

1. Click on the desktop “Windows 7 64-bit DispNme” icon to launch the XenDesktop session:
2. Enter the PIN, and click **Log On**.



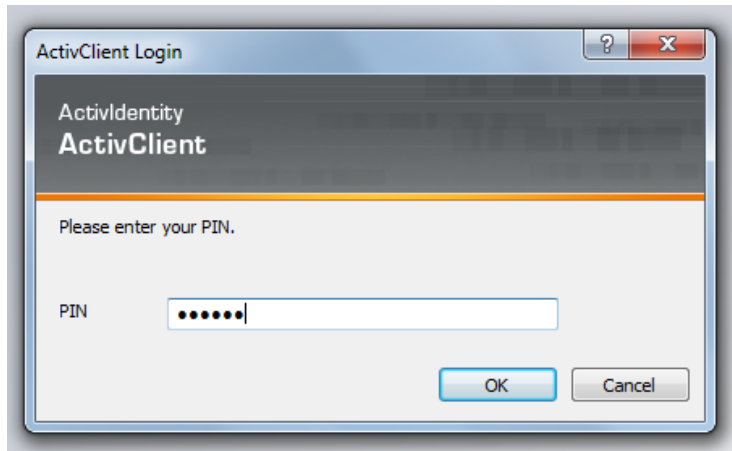
Once the Desktop Viewer launches, depending on the exact version of Citrix Receiver, the following credential tiles will be displayed:



NOTE

The credential tiles that are displayed (if at all) are predicated on the exact version of Citrix Receiver, the certificates that are present in the endpoint machine's certificate key store and whether Single Sign-on is configured.

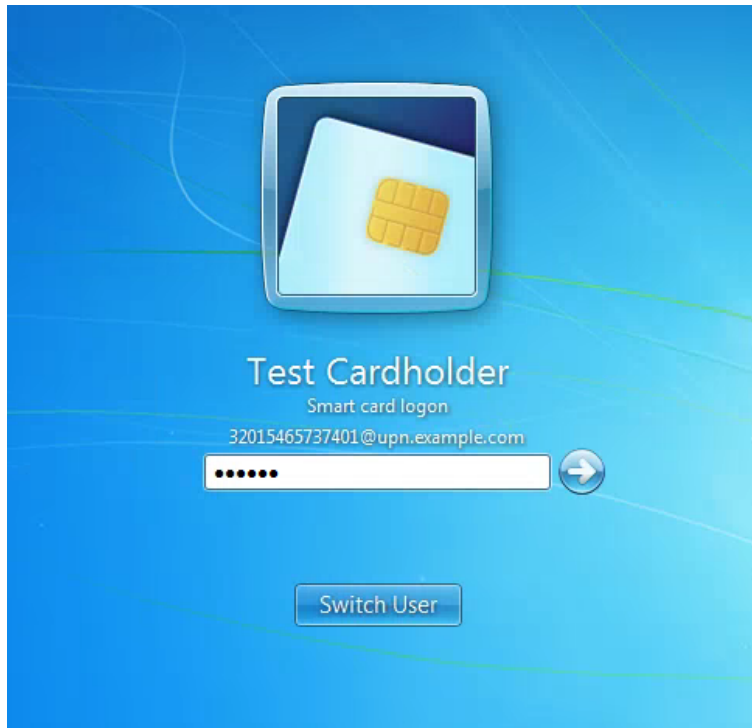
3. Click on the PIV authentication certificate.
4. Enter the PIN, and click **OK**.



The following will be displayed:



5. You will be prompted for the PIN again. Enter the PIN, and press **Enter**. The user will be logged on.

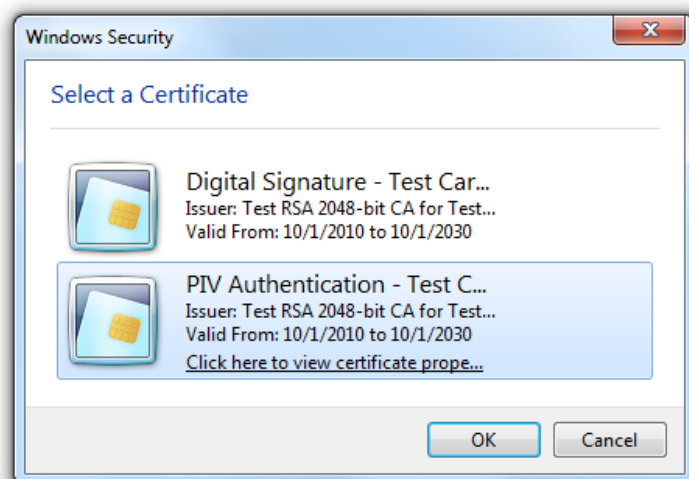


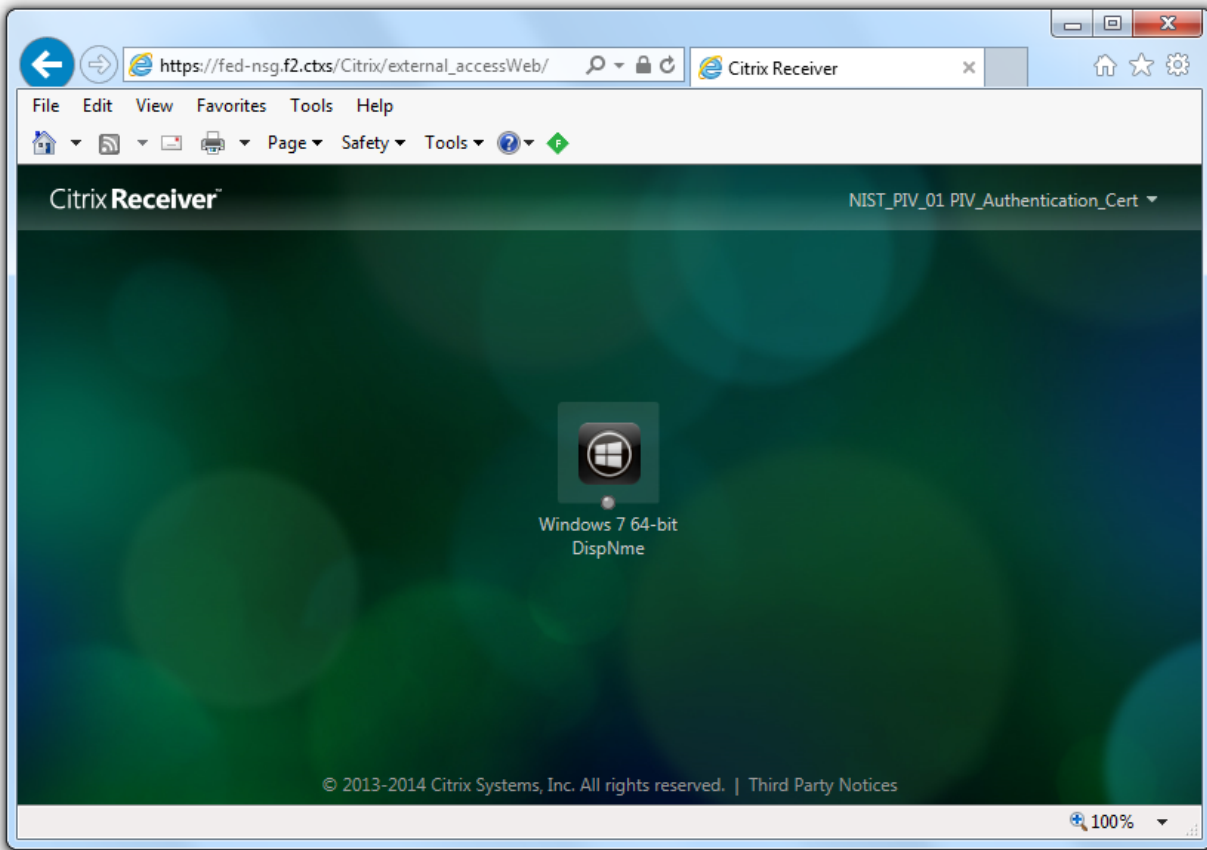
Receiver for Web

1. To connect using a web browser, launch Internet Explorer.
2. Enter the NetScaler Gateway URL preceded by https:

`https://fed-nsg.f2.ctxs`

3. If prompted for a certificate, select the PIV Authentication certificate, and click **OK**.





Section 2

Smart Card Single Sign-on

Introduction

This section contains detailed instructions for achieving Single Sign-on with a smart card by reducing PIN prompts one-by-one from four prompts to one for a *single use case* with *specific settings*.

NOTE

The initial PIN prompt when logging on to Windows at the endpoint is counted as a PIN prompt in this section. As a result, even after eliminating all other PIN prompts, the PIN prompt count will never be zero because the PIN must be entered at least once when the user first logs on.

The use case is as follows:

- Endpoint platform is Windows 7; VDA platform is Windows 7
- Endpoint is domain-joined
- Client is Receiver build 4.2 (not web browser)
- Endpoint connects via NetScaler Gateway
- Accounts and Resources are in the same domain
- Forest and domain functional level is Windows Server 2008 R2
- Card type is NIST PIV test #1
- Middleware is ActivClient 7.02
- Double-hop is not deployed.

The settings (that apply specifically to this use case) are as follows:

Group Policy > Smart Card Authentication > Allow Smart Card Authentication	Enabled
Group Policy > Smart Card Authentication > Use Pass-through authentication for PIN	Enabled
Group Policy > Local username and password > Enable pass-through authentication	Enabled
Group Policy > Local username and password > Allow pass-through authentication for all ICA connections	Enabled
StoreFront > PowerShell > Set-DSOptimalGatewayForFarms	Configured
NetScaler Gateway > SSON Virtual Server	Configured

NOTE

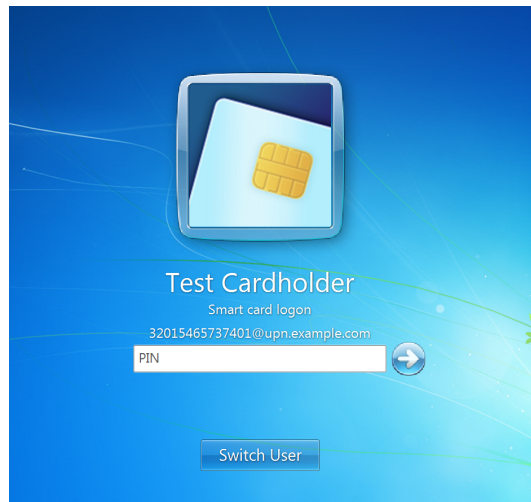
If any entity (such as using a web browser instead of Citrix Receiver on the endpoint) in the use case changes, the settings required to achieve smart card Single Sign-on under those conditions are likely to change and/or require additional settings to be configured. Documenting every permutation is a vast undertaking and beyond the scope of the first edition of this document.

The instructions that follow for achieving Single Sign-on with a smart card is organized around the number of PIN prompts the user encounters from initial endpoint logon until launching an ICA session. There are four sections, starting at the default state (no reductions – four PIN prompts) to the final state (three reductions – one PIN prompt). The instructions are cumulative and should be followed sequentially. Each section finishes with a summary. The summary consists of a Smart Card Single Sign-on State table showing what settings were changed to achieve the reduction, followed by a Resultant Smart Card Single Sign-on Behavior table.

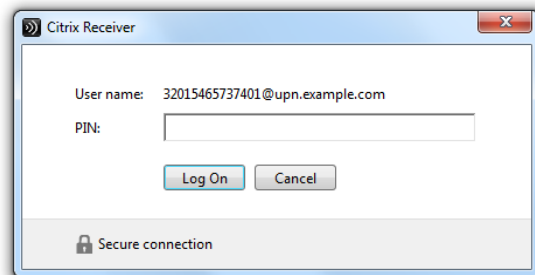
PIN Prompt Origin

The Resultant Behavior table for each state has a column for PIN Prompt Origin. PIN Prompt Origin refers to the component that is prompting the user for a PIN. There are three possibilities in the test environment described in this guide. The table below indicates what each component's PIN prompt looks like to the user:

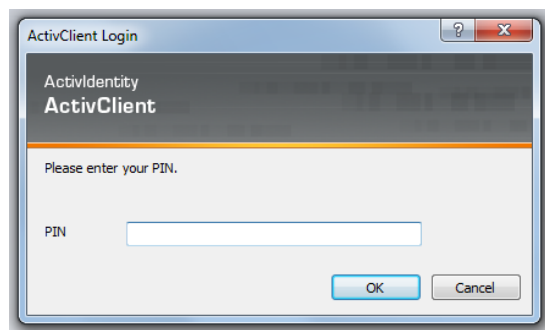
Windows 7



Citrix Authentication Manager



ActivClient Middleware



No reduction (four PIN prompts)

This is the state that the environment is in if no action is taken to reduce the number of PIN prompts.

Every table contains a list of 22 potential settings (even though only six of them are applicable to the use case that was selected for the Smart Card Single Sign-on section) Every one of the settings are known to affect smart card Single Sign-on, depending on the entities in the use case.

They are included here to provide context.

Smart card Single Sign-on state A

Use Case		
Endpoint platform is Windows 7; VDA platform is Windows 7; Endpoint is domain-joined; Client is Receiver build 4.2 (not web browser); Endpoint connects via NetScaler Gateway; Accounts and Resources are in the same domain; Forest and domain functional level is Windows Server 2008 R2; Card type is NIST PIV test #1; Middleware is ActivClient 7.02; Double-hop is not deployed		
Settings		
1	Group Policy > Smart Card Authentication > Allow Smart Card Authentication	Not Conf.
2	Group Policy > Smart Card Authentication > Use Pass-through authentication for PIN	Not Conf.
3	Group Policy > Kerberos authentication	Not Conf.
4	Group Policy > Local username and password > Enable pass-through authentication	Not Conf.
5	Group Policy > Local username and password > Allow pass-through authentication for all ICA connections	Not Conf.
6	Domain Controller > Machine Account > KCD	Off
7	Middleware > PIN Caching > Number of minutes before PIN cache is cleared	0
8	Middleware > PIN Caching > Allow per-process PIN caching	Disabled
9	Middleware > PIN Caching > Enable PIN caching for 'PIN always' private keys	Disabled
10	StoreFront > Default.ica > DisableCtrlAltDel=Off	Absent
11	StoreFront > Default.ica > UseLocalUserAndPassword=On	Absent
12	StoreFront > Auth Methods Enabled	Pt. f. NSG
13	StoreFront > PowerShell > Set-DSOptimalGatewayForFarms	Absent
14	Endpoint > Reg > HKLM\Software\[Wow6432Node\Citrix\AuthManager:CertificateSelectionMode={ Prompt SmartCardDefault LatestExpiry}	Absent
15	Endpoint > Reg > HKLM\Software\[Wow6432Node\Citrix\AuthManager:SmartCardPINEntry=CSP	Absent
16	Endpoint > Reg > HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify SmartCardLogonNotify	1
17	Endpoint > IE > NetScaler Gateway URL in Trusted Sites Zone	N/A
18	Endpoint > IE > Trusted Zone Custom: "Automatic logon w. current username and password"	N/A
19	Endpoint > IE > NetScaler Gateway URL domain added to Compatibility View list	N/A
20	Endpoint > Network Connections > Network Provider Priority > "Citrix Single Sign-on" at the top of the list	No
21	NetScaler Gateway > Callback Virtual Server	Configured
22	NetScaler Gateway > SSON Virtual Server	Absent

Resultant smart card Single Sign-On behavior A

Event	Certificate Selection Prompt?	PIN Prompt?	PIN Prompt Origin
1 Endpoint Windows OS Logon	N	Y	Windows
2 Citrix Receiver Logon	N	Y	Citrix Authentication Manager
3 Desktop Launch	Y	Y	ActivClient Middleware
4 VDA Windows OS Logon	N	Y	Windows
TOTAL	1	4	

First reduction (three PIN prompts)

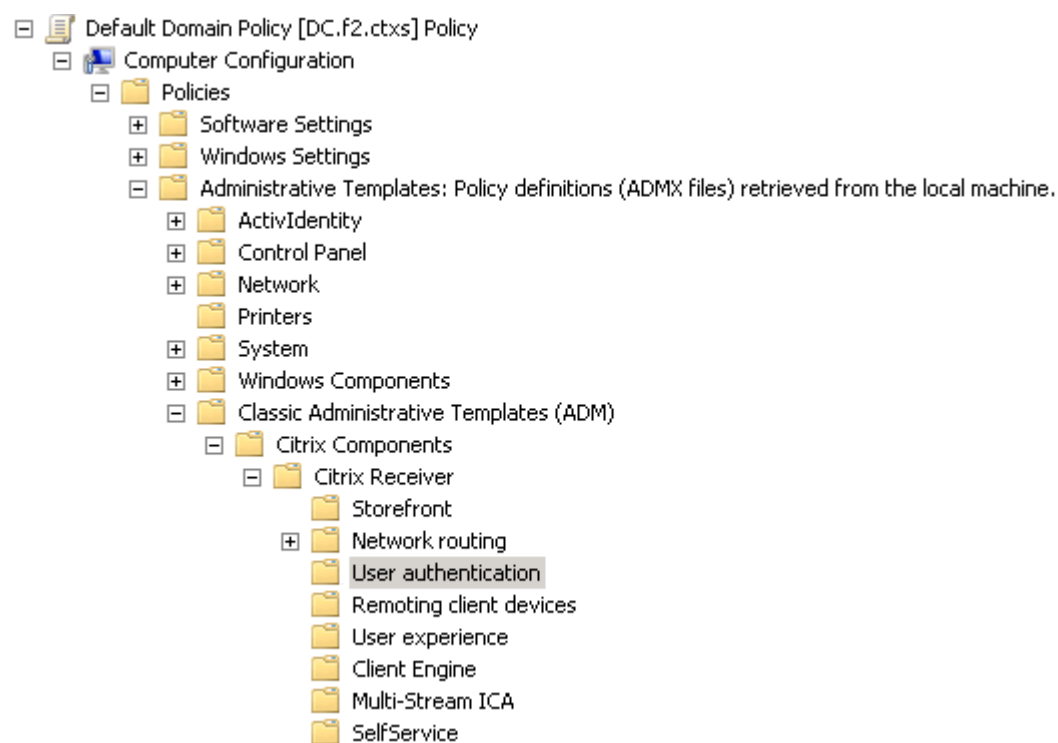
Turn on the Single Sign-on Service using group policy

Before completing this step, you must have installed the Single-Sign on service component during your Citrix Receiver installation. The Single Sign-on service is not installed by default.

NOTE

Installing Receiver with the SSON setting is described in section [Install Citrix Receiver](#). How to get the ADM file to configure group policy is described in section [Group policy ADM](#). How to import the ADM file into Active Directory is described in section [Add the Citrix icaclient administrative policy template \(ADM\) file](#)

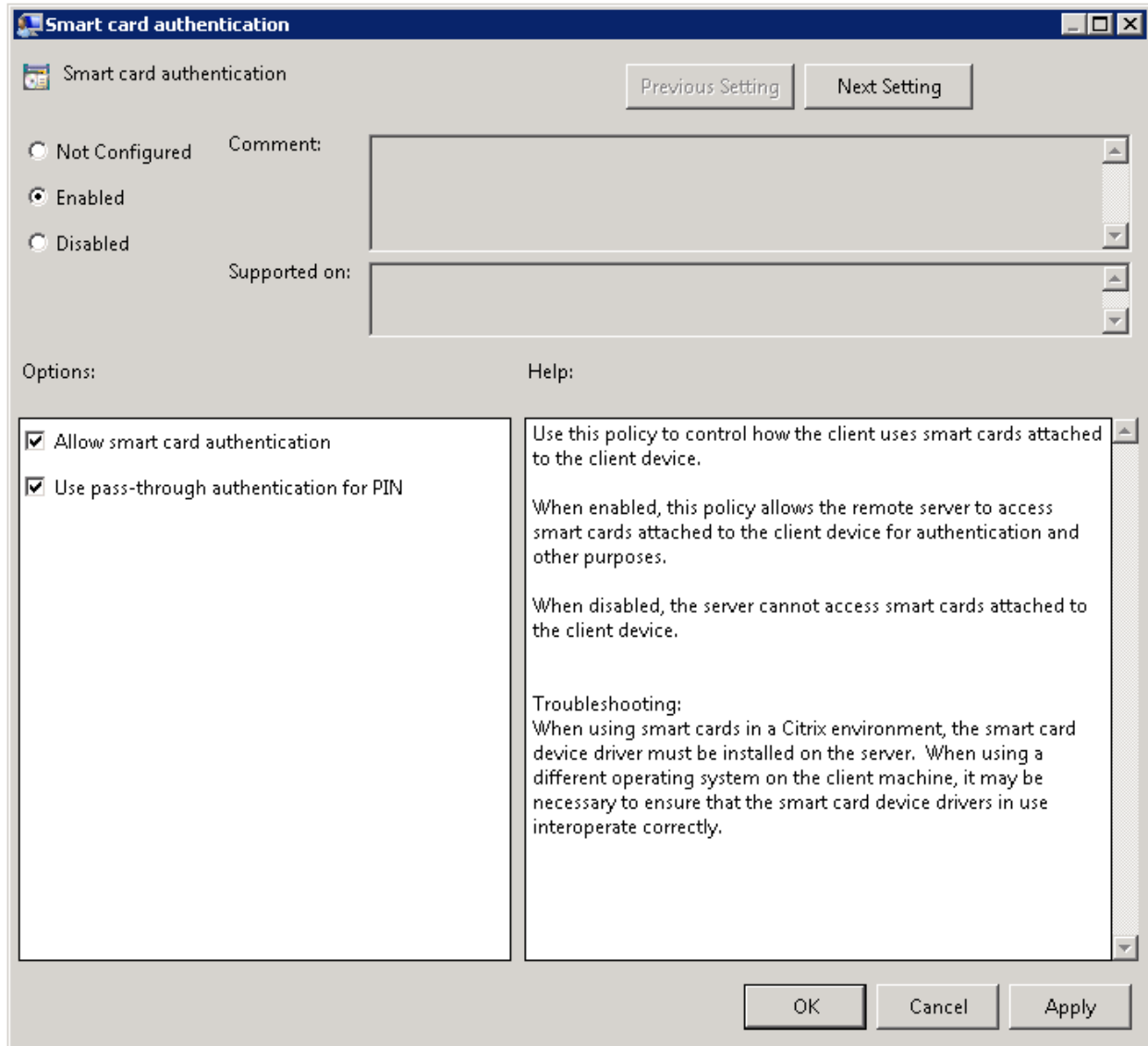
1. On the domain controller, navigate to User Authentication under the Citrix Components section in the group policy snap-in:



The following settings and their corresponding states will be shown:

Setting	State
Smart card authentication	Not configured
Kerberos authentication	Not configured
Local user name and password	Not configured
Web Interface authentication ticket	Not configured

2. Double-click on **Smart card authentication**, select **Enabled**, and then select **Allow smart card authentication** and **Use pass-through authentication for PIN**:



The image shows a Windows-style configuration window titled "Smart card authentication". At the top, there are "Previous Setting" and "Next Setting" buttons. Below the title bar, there are three radio buttons: "Not Configured", "Enabled" (which is selected), and "Disabled". To the right of these is a "Comment:" text box. Below the radio buttons is a "Supported on:" section with a list box. At the bottom left, under "Options:", there are two checked checkboxes: "Allow smart card authentication" and "Use pass-through authentication for PIN". To the right of these is a "Help:" section containing explanatory text and a "Troubleshooting:" section. At the bottom right, there are "OK", "Cancel", and "Apply" buttons.

Smart card authentication

Smart card authentication

Previous Setting Next Setting

☐ Not Configured
☒ Enabled
☐ Disabled

Comment:

Supported on:

Options:

☒ Allow smart card authentication
☒ Use pass-through authentication for PIN

Help:

Use this policy to control how the client uses smart cards attached to the client device.

When enabled, this policy allows the remote server to access smart cards attached to the client device for authentication and other purposes.

When disabled, the server cannot access smart cards attached to the client device.

Troubleshooting:
 When using smart cards in a Citrix environment, the smart card device driver must be installed on the server. When using a different operating system on the client machine, it may be necessary to ensure that the smart card device drivers in use interoperate correctly.

OK Cancel Apply

3. Click **OK**.

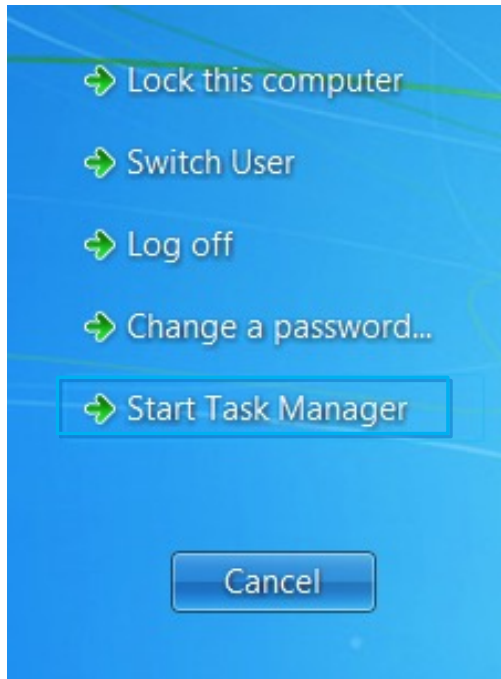
NOTE

Refresh group policy to propagate changes. The group policy refresh interval is governed by its own group policy (Policies > Administrative Templates > System > Group Policy). You can also manually update group policy by entering the following from the command line on the endpoint:

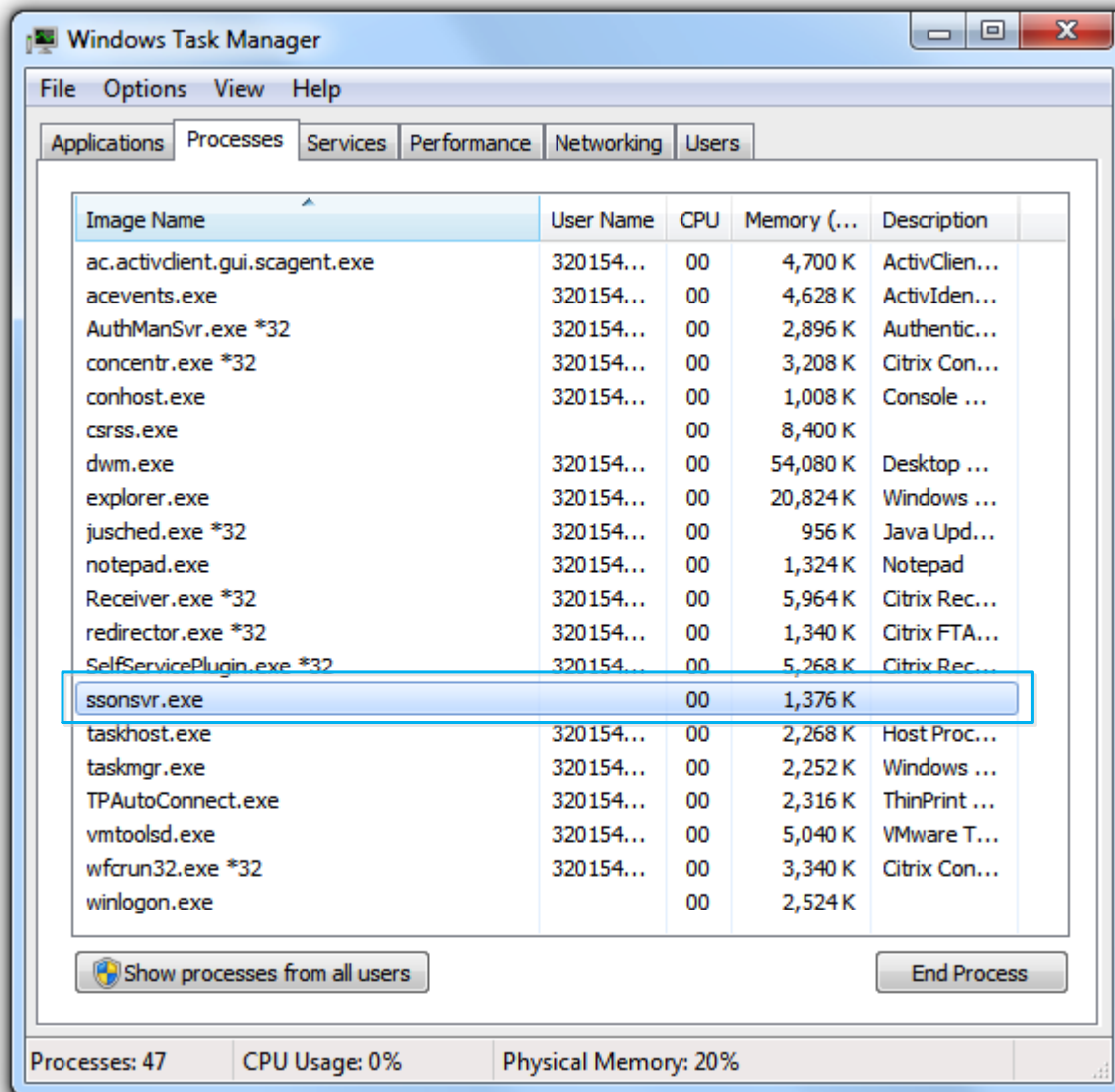
```
gpupdate /force
```

Verify the Single Sign-on service is running on the endpoint

1. Reboot the endpoint. Log on as the NIST PIV test card user. Press **Ctrl+Alt+Del** to start Windows Task Manager.



2. Navigate to the Processes tab in the Windows Task Manager window, and verify that the ssonsvr.exe process is running:



Smart card Single Sign-on state B (three PIN prompts)

Use Case		
Endpoint platform is Windows 7; VDA platform is Windows 7; Endpoint is domain-joined; Client is Receiver build 4.2 (not web browser); Endpoint connects via NetScaler Gateway; Accounts and Resources are in the same domain; Forest and domain functional level is Windows Server 2008 R2; Card type is NIST PIV test #1; Middleware is ActivClient 7.02; Double-hop is not deployed		
Settings		
1	Group Policy > Smart Card Authentication > Allow Smart Card Authentication	Enabled
2	Group Policy > Smart Card Authentication > Use Pass-through authentication for PIN	Enabled
3	Group Policy > Kerberos authentication	Not Conf.
4	Group Policy > Local username and password > Enable pass-through authentication	Not Conf.
5	Group Policy > Local username and password > Allow pass-through authentication for all ICA connections	Not Conf.
6	Domain Controller > Machine Account > KCD	Off
7	Middleware > PIN Caching > Number of minutes before PIN cache is cleared	0
8	Middleware > PIN Caching > Allow per-process PIN caching	Disabled
9	Middleware > PIN Caching > Enable PIN caching for 'PIN always' private keys	Disabled
10	StoreFront > Default.ica > DisableCtrlAltDel=Off	Absent
11	StoreFront > Default.ica > UseLocalUserAndPassword=On	Absent
12	StoreFront > Auth Methods Enabled	Pt. f. NSG
13	StoreFront > PowerShell > Set-DSOptimalGatewayForFarms	Absent
14	Endpoint > Reg > HKLM\Software\[Wow6432Node\Citrix\AuthManager:CertificateSelectionMode={ Prompt SmartCardDefault LatestExpiry}	Absent
15	Endpoint > Reg > HKLM\Software\[Wow6432Node\Citrix\AuthManager:SmartCardPINEntry=CSP	Absent
16	Endpoint > Reg > HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify SmartCardLogonNotify	1
17	Endpoint > IE > NetScaler Gateway URL in Trusted Sites Zone	n/a
18	Endpoint > IE > Trusted Zone Custom: "Automatic logon w. current username and password"	n/a
19	Endpoint > IE > NetScaler Gateway URL domain added to Compatibility View list	n/a
20	Endpoint > Network Connections > Network Provider Priority > "Citrix Single Sign-on" at the top of the list	No
21	NetScaler Gateway > Callback Virtual Server	Configured
22	NetScaler Gateway > SSON Server / Routing on launch configured	Absent

Resultant smart card Single Sign-on behavior B

Event	Certificate Selection Prompt?	PIN Prompt?	PIN Prompt Origin
1 Endpoint Windows OS Logon	N	Y	Windows
2 Citrix Receiver Logon	N	N	Citrix Authentication Manager
3 Desktop Launch	Y (4)	Y	ActivClient Middleware
4 VDA Windows OS Logon	N	Y	Windows
TOTAL	1	3	

Second reduction (two PIN prompts)

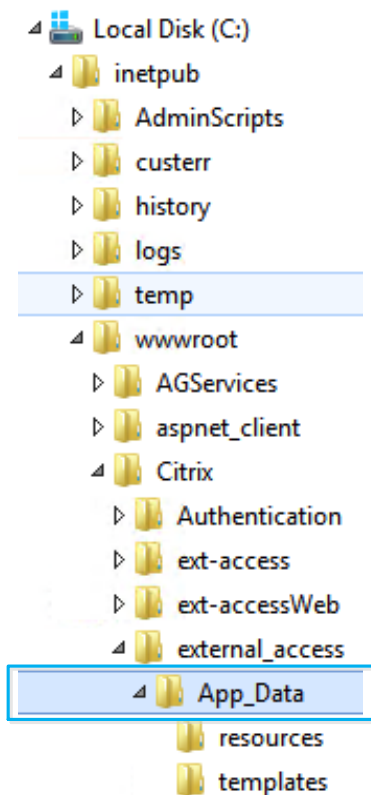
Add setting to default.ica file on the StoreFront server

1. On the StoreFront server, locate the default.ica file for the StoreFront Store you wish to configure.

The default location for the default.ica file is:

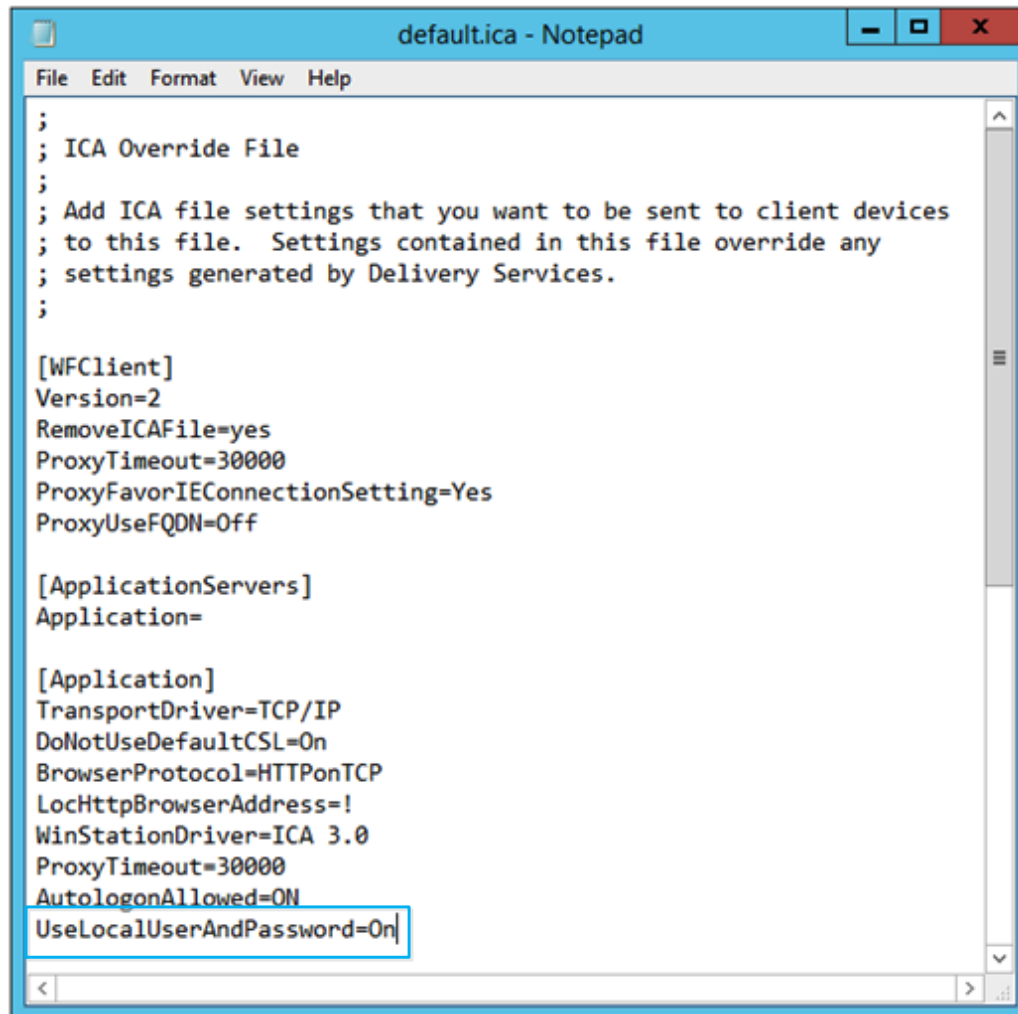
```
\inetpub\wwwroot\Citrix\<Your-Site-Name>\App_Data\default.ica
```

In this example, we will configure the default.ica file for the external_access store:



2. Open the default.ica file with a text editor, such as Notepad.
3. Add the following string to the Application section:

```
UseLocalUserAndPassword=On
```



4. Save the file.

Local user name and password group policy setting

1. On the domain controller, navigate to User Authentication under the Citrix Components section in the group policy snap-in. Double-click on the **Local User Name and Password** setting.
2. Select **Enable pass-through authentication** and **Allow pass-through authentication for all ICA connections**:

Local user name and password

Local user name and password

Previous Setting Next Setting

☐ Not Configured
 ☒ Enabled
 ☐ Disabled

Comment:

Supported on:

Options:

☒ Enable pass-through authentication
☒ Allow pass-through authentication for all ICA connections
☐ Use Novell Directory Server credentials

Help:

Use this policy to instruct the client to use the same logon credentials (pass-through authentication) for the Citrix XenApp server as the client computer.

When this policy is enabled, the client can be prevented from using the current user's logon credentials to authenticate to the remote server by clearing the "Enable pass-through authentication" check box.

The client imposes certain restrictions specifying when pass-through authentication can occur (for details, see Citrix eDocs at <http://support.citrix.com/proddocs/>). If these restrictions are too strict for your environment, select the "Allow pass-through authentication for all ICA connections" check box to bypass the pass-through authentication restrictions.

When run in a Novell Directory Server environment, selecting the "Use Novell Directory Server credentials" check box requests that the client uses the user's NDS credentials.

OK Cancel Apply

3. Click OK.

NOTE

Refresh group policy to ensure changes are propagated. The group policy refresh interval is governed by its own group policy (Policies > Administrative Templates > System > Group Policy). You can also manually update group policy by entering the following from the command line on the endpoint:

```
gpupdate /force
```

Smart card Single Sign-on state C (two PIN prompts)

Use Case		
Endpoint platform is Windows 7; VDA platform is Windows 7; Endpoint is domain-joined; Client is Receiver build 4.2 (not web browser); Endpoint connects via NetScaler Gateway; Accounts and Resources are in the same domain; Forest and domain functional level is Windows Server 2008 R2; Card type is NIST PIV test #1; Middleware is ActivClient 7.02; Double-hop is not deployed		
Settings		
1	Group Policy > Smart Card Authentication > Allow Smart Card Authentication	Enabled
2	Group Policy > Smart Card Authentication > Use Pass-through authentication for PIN	Enabled
3	Group Policy > Kerberos authentication	Not Conf.
4	Group Policy > Local username and password > Enable pass-through authentication	Enabled
5	Group Policy > Local username and password > Allow pass-through authentication for all ICA connections	Enabled
6	Domain Controller > Machine > KCD	Off
7	Middleware > PIN Caching > Number of minutes before PIN cache is cleared	0
8	Middleware > PIN Caching > Allow per-process PIN caching	Disabled
9	Middleware > PIN Caching > Enable PIN caching for 'PIN always' private keys	Disabled
10	StoreFront > Default.ica > DisableCtrlAltDel=Off	Absent
11	StoreFront > Default.ica > UseLocalUserAndPassword=On	Absent
12	StoreFront > Auth Methods Enabled	Pt. f. NSG
13	StoreFront > PowerShell > Set-DSOptimalGatewayForFarms	Absent
14	Endpoint > Reg > HKLM\Software\[Wow6432Node\Citrix\AuthManager:CertificateSelectionMode={ Prompt SmartCardDefault LatestExpiry}	Absent
15	Endpoint > Reg > HKLM\Software\[Wow6432Node\Citrix\AuthManager:SmartCardPINEntry=CSP	Absent
16	Endpoint > Reg > HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify SmartCardLogonNotify	1
17	Endpoint > IE > NetScaler Gateway URL in Trusted Sites Zone	n/a
18	Endpoint > IE > Trusted Zone Custom: "Automatic logon w. current username and password"	n/a
19	Endpoint > IE > NetScaler Gateway URL domain added to Compatibility View list	n/a
20	Endpoint > Network Connections > Network Provider Priority > "Citrix Single Sign-on" at the top of the list	No
21	NetScaler Gateway > Callback Virtual Server	Configured
22	NetScaler Gateway > SSON Server	Absent

Resultant smart card Single Sign-on behavior C

Event	Certificate Selection Prompt?	PIN Prompt?	PIN Prompt Origin
1 Endpoint Windows OS Logon	N	Y	Windows
2 Citrix Receiver Logon	N	N	Citrix Authentication Manager
3 Desktop Launch	Y	Y	ActivClient Middleware
4 VDA Windows OS Logon	N	N	Windows
TOTAL	1	2	

Third reduction (one PIN prompt)

The method described below is a workaround to overcome a current limitation in the HDX Engine in Citrix Receiver. Normally, the user would connect to a single virtual server on the NetScaler Gateway for initial authentication and application enumeration as well as the subsequent launching of an ICA session. However, the virtual server on the NetScaler Gateway to which the user connects for initial authentication and application enumeration (fed-nsg.f2.ctxs in the test environment) will prompt for a PIN. This is because the SSL session parameter for this virtual server is set to perform mandatory client authentication when the SSL connection between the endpoint and the virtual server is established.

To prevent the user from receiving a manual PIN prompt when the ICA session is launched, the HDX Engine in Citrix Receiver must consume the PIN that was cached by the Authentication Manager component in Citrix Receiver. At the time this guide was published, the HDX Engine does not consume the cached PIN. As a result, the user will be prompted to manually enter the PIN again when the session is launched.

The method in this section overcomes this limitation by creating an additional virtual server on the NetScaler Gateway (fed-sson-session.f2.ctxs in the test environment). The “session” virtual server is configured to not perform mandatory client authentication when the SSL connection is established between the virtual server and the endpoint at session launch time. Additional configuration is performed (described in detail in this section) so that StoreFront will insert the hostname of the “session” virtual server in the ICA file that it sends to the endpoint (instead of the initial virtual server that was used for authentication and application enumeration).

Before implementing this workaround, you should ensure that deploying it in this fashion complies with your organization’s security policy.

Create Single Sign-On session virtual server on NetScaler Gateway

NOTE

This step assumes that you generated the **keys** (in section [Generate RSA keypairs inside the HSM](#)), generated the **CSRs** (in section [Create Certificate Signing Requests \(CSR\) for each SSL FIPS key](#)) and issued (via your organizations Issuing Certificate Authority) the **certificate** for the fed-sson-session virtual server (in section [Submit certificate signing requests \(CSR\) to your organization’s issuing CA](#))

1. In the NetScaler GUI, navigate to:

NetScaler > NetScaler Gateway > NetScaler Gateway Virtual Servers

The following is displayed:

Add Edit Delete Statistics Action						
Search ▼						
Name	State	IP Address	Port	Protocol	Maximum Users	Current Users
fed-nsg.f2.ctxs	Up	10.217.205.72	443	SSL	0	0
fed-callback.f2.ctxs	Up	10.217.205.73	443	SSL	0	0

- Click **Add**. The Basic Settings page is displayed. Populate as follows:

Basic Settings

Name*

IPAddress*
 ☐ IPv6

Port*

- Click **More**. Deselect **Enable Authentication**:

☐ ICA Only
 ☐ Enable Authentication ?

☐ Double Hop
 ☐ Down State Flush

☐ AppFlow Logging
 ☐ ICA Proxy Session Migration

☒ State

☐ Range

☐ Enable Device Certificate

- Click **OK**.

```
add vpn vserver fed-sson-session.f2.ctxs SSL 10.217.205.74 -range 1 443 -
state ENABLED -authentication OFF -doubleHop DISABLED -maxAAAUsers 0 -icaOnly
OFF -icaProxySessionMigration OFF -deviceCert OFF -downStateFlush DISABLED -
Listenpolicy none -appflowLog DISABLED -icmpVsrResponse PASSIVE -RHistate
PASSIVE -cginfraHomePageRedirect ENABLED -l2Conn OFF -deploymentType NONE
```

The following will be displayed:

Basic Settings			
Name	fed-sson-session.f2.ctxs	Max Users	
IPAddress	10.217.205.74	Max Login Attempts	
Port	443	Failed Login Timeout	
		State	true
		ICA Only	false
		Enable Authentication	false
		Double Hop	false
		Down State Flush	false
		AppFlow Logging	false
		ICA Proxy Session Migration	false
		Enable Device Certificate	false

Certificates	
No Server Certificate	>
No CA Certificate	>

Authentication	
To add, please click on the + icon	
<div>Continue</div>	

NOTE

Ensure that the new virtual server name can be resolved via DNS from an external host.

Certificate configuration for Single Sign-On session virtual server

Configure the server certificate

- On the VPN virtual server page for the fed-sson-session.f2.ctxs, scroll to the Certificates section:

Certificates	
No Server Certificate	>
No CA Certificate	>

- Click **No Server Certificate**. The Server Certificate Binding page will be displayed. Click in the **Select Server Certificate** field. Choose fed-sson-session, and click **OK**.

Server Certificate Binding > SSL Certificates

SSL Certificates

Install Update Delete Action

Name	Days to Expire	Status
☐ ▶ nist-piv-root-ca	5702	Valid
☐ ▶ nist-piv-issuing-ca	5702	Valid
☐ ▶ fed-nsg	485	Valid
☐ ▶ fed-callback	485	Valid
☒ ▶ fed-sson-session	485	Valid
☐ ▶ f2-root-ca	1266	Valid
☐ ▶ f2-issuing-ca	485	Valid

OK Close

The following will be displayed:

Server Certificate Binding

Server Certificate Binding

Select Server Certificate*

fed-sson-session > +

☐ Server Certificate for SNI

Bind Close

3. Click **Bind**.

```
bind ssl vserver fed-sson-session.f2.ctxs -priority 0 -certkeyName fed-sson-session -crlCheck Optional
```

The following will be displayed:

Certificates

1 Server Certificate >

No CA Certificate >

Configure issuing CA certificate

1. Click **No CA Certificate**. The CA Certificate Binding page is displayed. Click the **Select CA Certificate** field.
2. Then select **f2-issuing-ca**, and click **OK**, as shown below.

CA Certificate Binding > SSL Certificates

SSL Certificates

Install Update Delete Action

Name	Days to Expire	Status
☐ nist-piv-root-ca	5702	Valid
☐ nist-piv-issuing-ca	5702	Valid
☐ fed-nsg	485	Valid
☐ fed-callback	485	Valid
☐ fed-sson-session	485	Valid
☐ f2-root-ca	1266	Valid
☒ f2-issuing-ca	485	Valid

OK Close

The following will be displayed:

CA Certificate Binding

CA Certificate Binding

Select CA Certificate*

f2-issuing-ca > +

CRL and OCSP Check

☐ Skip CA

Bind Close

3. Click **Bind**.

```
bind ssl vserver fed-sson-session.f2.ctxs -priority 0 -certkeyName f2-issuing-ca -CA -crlCheck Optional
```

The following will be displayed:

Certificates	
1 Server Certificate	>
1 CA Certificate	>

Configure root CA certificate

1. Click on **1 CA Certificate**. The following will be displayed:

SSL Virtual Server CA Certificate Binding

SSL Virtual Server CA Certificate Binding

Add Binding Unbind

Certificate	CRL and OCSP Check	Skip CA
f2-issuing-ca	OCSP Optional	✗

Close

2. Click **Add Binding**. The CA Certificate Binding page is displayed. Click in the **Select CA Certificate** field.
3. Select **f2-root-ca**, and click **OK**, as shown below.

SSL Virtual Server CA Certificate Binding > CA Certificate Binding > SSL Certificates

SSL Certificates

Install Update Delete Action

Name	Days to Expire	Status
☐ ▶ nist-piv-root-ca	5702	Valid
☐ ▶ nist-piv-issuing-ca	5702	Valid
☐ ▶ fed-nsg	485	Valid
☐ ▶ fed-callback	485	Valid
☐ ▶ fed-sson-session	485	Valid
☒ ▶ f2-root-ca	1266	Valid
☐ ▶ f2-issuing-ca	485	Valid

OK Close

The following will be displayed:

SSL Virtual Server CA Certificate Binding > CA Certificate Binding

CA Certificate Binding

Select CA Certificate*

f2-root-ca

CRL and OCSP Check

☐ Skip CA

Bind Close

- Click **Bind**.

```
bind ssl vserver fed-sson-session.f2.ctxs -priority 0 -certkeyName f2-root-ca
-CA -crlCheck Optional
```

The following will be displayed:

SSL Virtual Server CA Certificate Binding

SSL Virtual Server CA Certificate Binding

Add Binding Unbind

Certificate	CRL and OCSP Check	Skip CA
f2-root-ca	OCSP Optional	X
f2-issuing-ca	OCSP Optional	X

Close

- Click **Close**.

Configure STA for Single Sign-on session virtual server

- In the NetScaler GUI, navigate to:

NetScaler > NetScaler Gateway > NetScaler Gateway Virtual Servers

- Select the **fed-sson-session.f2.ctxs** virtual server, and click **Edit**. In the Advanced section, click **Published Applications**:

Advanced
 SSL Profile
 SSL Ciphers
 SSL Policies
 Profiles
 Intranet IP Addresses
 Intranet Applications
 Published Applications
 Other Settings

The following will be displayed:

Published Applications	×
No Next HOP Server	>
No STA Server	>
No Url	>

3. Click STA Server.

The STA Server Binding page is displayed. Enter the URL of the Secure Ticket Authority Server and Address Type. (In this example, the Delivery Controller and IPv4):

STA Server Binding

STA Server Binding

Secure Ticket Authority Server*

✕
?

Secure Ticket Authority Server Address Type

▼

Bind

Close

- Click **Bind**.

```
bind vpn vserver fed-sson-session.f2.ctxs -staServer "https://a-ddc.f2.ctxs"
-staAddressType IPV4
```

The following will be displayed:

Published Applications		✕
No	Next HOP Server	>
1	STA Server	>
No	Url	>

- Click on **STA Server** again. Verify that the State is **Up** and an Auth ID is shown:

VPN Virtual Server STA Server Binding			
VPN Virtual Server STA Server Binding			
<div>Add Binding</div> <div>Unbind</div>		Search ▼	
Secure Ticket Authority Server	Secure Ticket Authority Server Address Type	State	Auth ID
https://a-ddc.f2.ctxs	IPV4	Up	STA246738997
Close			

Verify SSL parameters for Single Sign-on session virtual server

- In the NetScaler GUI, navigate to:

NetScaler > NetScaler Gateway > NetScaler Gateway Virtual Servers

The following will be displayed:

Add Edit Delete Statistics Action Search ▼						
Name	State	IP Address	Port	Protocol	Maximum Users	Current Users
fed-nsg.f2.ctxs	Up	10.217.205.72	443	SSL	0	0
fed-callback.f2.ctxs	Up	10.217.205.73	443	SSL	0	0
fed-sson-session.f2.ctxs	Up	10.217.205.74	443	SSL	0	0

2. Select the **fed-sson-session.f2.ctxs** virtual server, and click **Edit**.
3. Scroll to the SSL Parameters section, and verify that Client Authentication is set to **DISABLED**:

SSL Parameters							
Enable DH Param	DISABLED	Clear Text Port	0	SSLv2 Redirect	DISABLED		
Enable Ephemeral RSA	DISABLED	Enable Cipher Redirect	DISABLED	SSLv2	DISABLED		
Enable Session Reuse	ENABLED	Client Authentication	DISABLED	SSLv3	DISABLED		
Time-out	120	Send Close-Notify	YES	TLSv1	ENABLED		
SSL Redirect	DISABLED	PUSH Encryption Trigger	Always	TLSv11	DISABLED		
		SNI Enable	DISABLED	TLSv12	DISABLED		

NOTE

It is highly recommended to disable SSLv3 and only use TLS v1 in SSL Parameters.

Configure optimal NetScaler Gateway routing for the external store on the StoreFront server

NOTE

Additional information about optimal NetScaler Gateway routing and PowerShell parameters can be found here: <http://support.citrix.com/proddocs/topic/dws-storefront-26/dws-configure-ha-optimal.html>

Load PowerShell snap-ins

1. On the StoreFront server, start the Windows PowerShell ISE environment.
2. Import appropriate PowerShell snap-ins using the following command:

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

The following will be displayed:

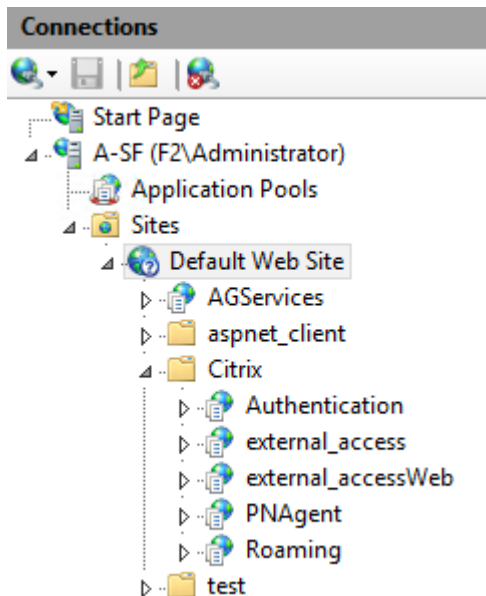
[illegible]

Determine values for PowerShell parameters in your environment

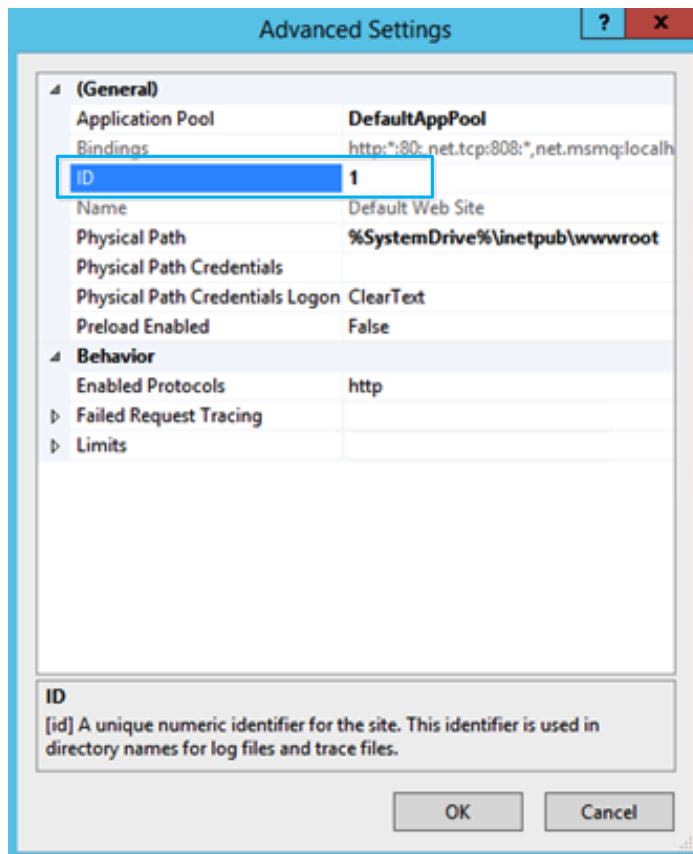
Before running the PowerShell command to configure optimal routing, determine the values of the following parameters:

SiteId

1. In IIS MMC Snap-In on the StoreFront Server, Navigate to Default Web Site:



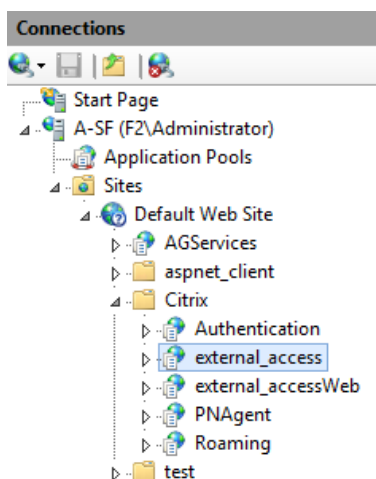
2. With **Default Web Site** selected in the Connections Pane, click on **Advanced Settings** in the Actions Pane. The **Advanced Setting** dialog box will be displayed:



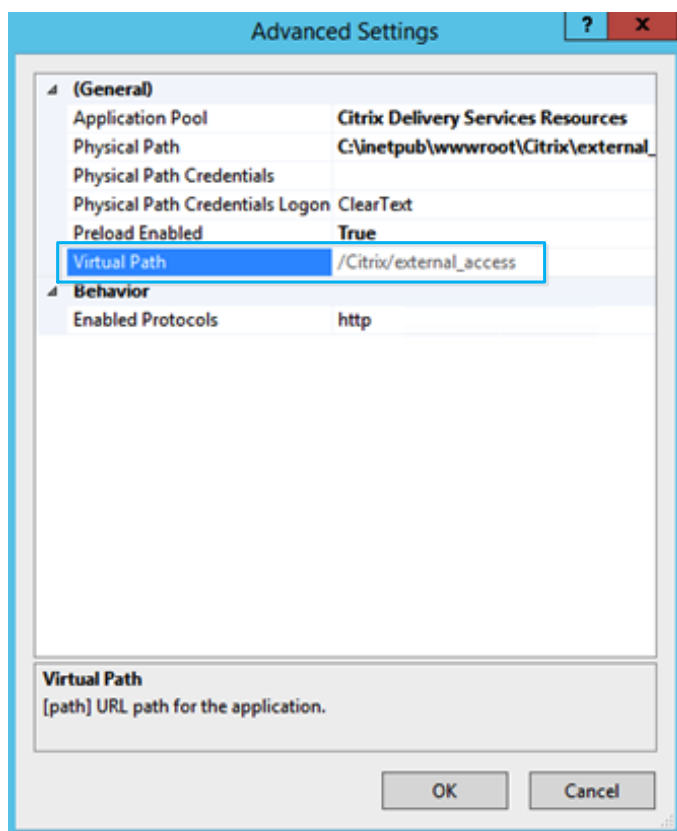
The SiteID you should use is displayed next to the ID attribute. The default (as is also the case in this example is 1).

ResourcesVirtualPath

3. In IIS MMC Snap-In on the StoreFront Server, Navigate to the StoreFront site you want to configure. (In this example, the external_access site):



4. Click Advanced Settings in the corresponding Actions Pane. The Advanced Settings Dialog box will be displayed:



ResourcesVirtualPath is shown in Virtual Path attribute field. (In this case, /Citrix/external_access.)

GatewayName

GatewayName does not refer to anything that you have configured on the StoreFront server. It represents a label that you can define right here for the first time. In this example, we will use GatewayForICASession.

Hostnames

Hostnames refer to the FQDN (including port number) of the NetScaler Gateway virtual server that you intend to use for the Single Sign-on ICA session. (In this example, fed-sson-session.f2.ctxs):

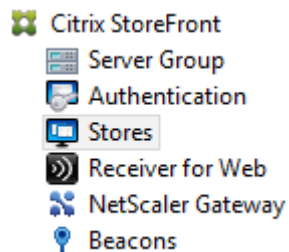
NetScaler > NetScaler Gateway > NetScaler Gateway Virtual Servers						?	?	?
Add	Edit	Delete	Statistics	Action	Search			
Name	State	IP Address	Port	Protocol	Maximum Users	Current Users		
fed-nsg.f2.ctxs	Up	10.217.205.72	443	SSL	0	0		
fed-callback.f2.ctxs	Up	10.217.205.73	443	SSL	0	0		
fed-sson-session.f2.ctxs	Up	10.217.205.74	443	SSL	0	0		

NOTE

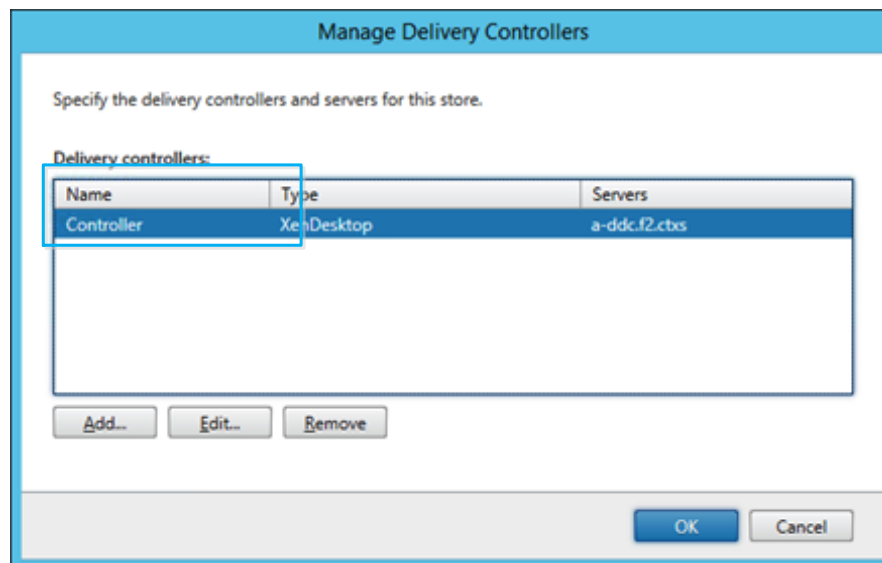
FQDN does not necessarily match what you entered as the name as it does in the example above.

Farms

1. In the StoreFront Management Console, navigate to **Stores**:



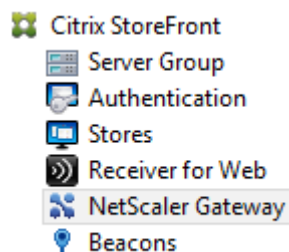
2. Select the appropriate Store (in this example external_access), and click **Manage Delivery Controllers**. The Manage Delivery Controllers dialog box will be displayed:



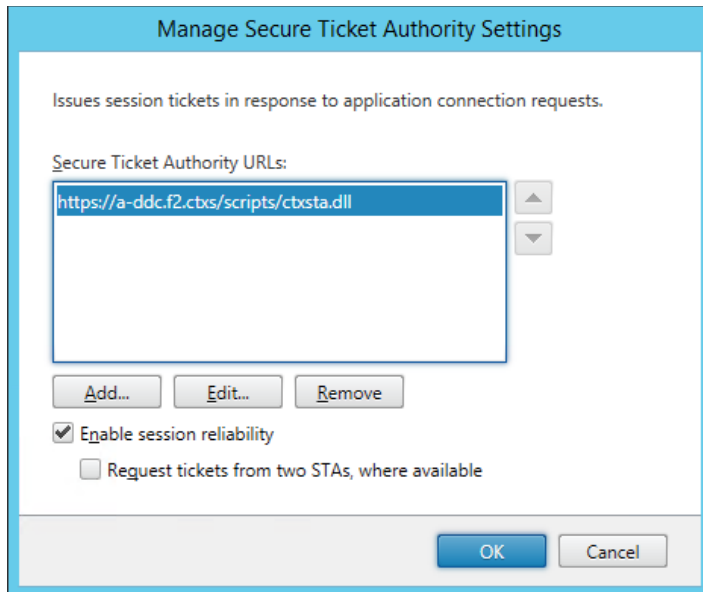
Farms refer to the value of the name attribute. In this example, the value of the name attribute is Controller.

StaUrls

1. In the StoreFront Management Console, navigate to **NetScaler Gateway**:



2. In the corresponding Action Pane, click **Secure Ticket Authority**. The Manage Secure Ticket Authority Settings dialog box is displayed:



The value for STAUrls including its parameters must match the values defined here.

Run PowerShell command Set-DSOptimalGatewayForFarms

1. Run the following command in PowerShell, substituting values as appropriate:

```
Set-DSOptimalGatewayForFarms -SiteId 1 -ResourcesVirtualPath
"/Citrix/external_access" -GatewayName "GatewayForICASession" -Hostnames
"fed-sson-session.f2.ctxs:443" -Farms "Controller" -StaUrls "https://a-
ddc.f2.ctxs/scripts/ctxsta.dll" -StasUseLoadBalancing $false -
StasBypassDuration 00.02:00:00 -EnableSessionReliability $true -UseTwoTickets
$false -EnabledOnDirectAccess $true
```

The command should execute without displaying any errors.

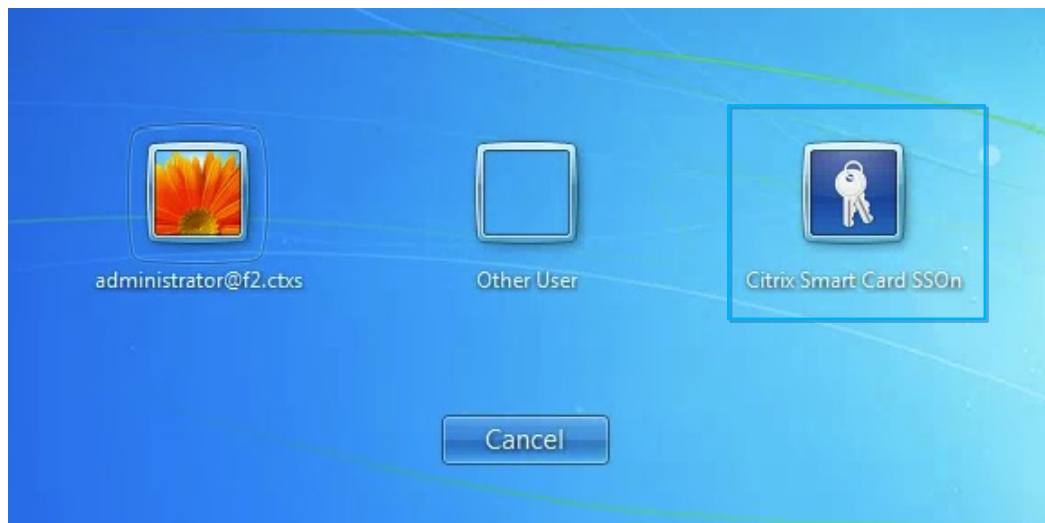
NOTE

To remove the optimal gateway routing setting on the StoreFront Server for whatever reason, use the following command:

```
Remove-DSOptimalGatewayForFarms -SiteId 1 -ResourcesVirtualPath
"/Citrix/external_access"
```

Launch

When launching a VDA, you will notice a new logon tile: Citrix Smart Card SSO:



The user does not have to select it manually. It will be chosen automatically, and the user will be logged on.

Smart card Single Sign-on state D (one PIN prompt)

Use Case		
Endpoint platform is Windows 7; VDA platform is Windows 7; Endpoint is domain-joined; Client is Receiver build 4.2 (not web browser); Endpoint connects via NetScaler Gateway; Accounts and Resources are in the same domain; Forest and domain functional level is Windows Server 2008 R2; Card type is NIST PIV test #1; Middleware is ActivClient 7.02; Double-hop is not deployed		
Variables		
1	Group Policy > Smart Card Authentication > Allow Smart Card Authentication	Enabled
2	Group Policy > Smart Card Authentication > Use Pass-through authentication for PIN	Enabled
3	Group Policy > Kerberos authentication	Not Conf.
4	Group Policy > Local username and password > Enable pass-through authentication	Enabled
5	Group Policy > Local username and password > Allow pass-through authentication for all ICA connections	Enabled
6	Domain Controller > Machine Account > KCD	Off
7	Middleware > PIN Caching > Number of minutes before PIN cache is cleared	0
8	Middleware > PIN Caching > Allow per-process PIN caching	Disabled
9	Middleware > PIN Caching > Enable PIN caching for 'PIN always' private keys	Disabled
10	StoreFront > Default.ica > DisableCtrlAltDel=Off	Absent
11	StoreFront > Default.ica > UseLocalUserAndPassword=On	Absent
12	StoreFront > Auth Methods Enabled	Pt. f. NSG
13	StoreFront > PowerShell > Set-DSOptimalGatewayForFarms	Configured
14	Endpoint > Reg > HKLM\Software\[Wow6432Node\Citrix\AuthManager: CertificateSelectionMode={ Prompt SmartCardDefault LatestExpiry}	Absent
15	Endpoint > Reg > HKLM\Software\[Wow6432Node\Citrix\AuthManager:SmartCardPINEntry=CSP	Absent
16	Endpoint > Reg > HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify SmartCardLogonNotify	1
17	Endpoint > IE > NetScaler Gateway URL in Trusted Sites Zone	n/a
18	Endpoint > IE > Trusted Zone Custom: "Automatic logon w. current username and password"	n/a
19	Endpoint > IE > NetScaler Gateway URL domain added to Compatibility View list	n/a
20	Endpoint > Network Connections > Network Provider Priority > "Citrix Single Sign-on" at the top of the list	No
21	NetScaler Gateway > Callback Virtual Server	Configured
22	NetScaler Gateway > SSON Virtual Server	Configured

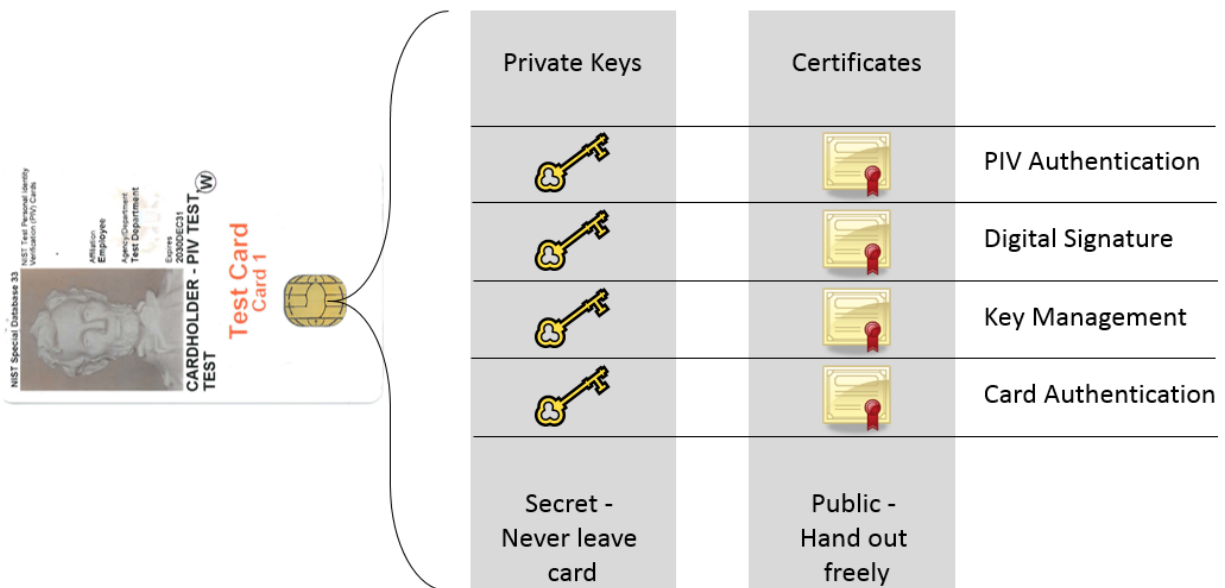
Resultant smart card Single Sign-on behavior D

Event	Certificate Selection Prompt?	PIN Prompt?	PIN Prompt Origin
1 Endpoint Windows OS Logon	N	Y	Windows
2 Citrix Receiver Logon	N	N	Citrix Authentication Manager
3 Desktop Launch	N	N	ActivClient Middleware
4 VDA Windows OS Logon	N	N	Windows
TOTAL	0	1	

Appendices

Appendix A: NIST PIV Test Card Certificates, Keys and Chain of Trust

The NIST PIV Test Card #1 contains the following:



The microchip on the card contains four certificates. Each certificate contains a public key, and each public key has a corresponding private key, which is stored on the card's microchip. The card freely gives out the certificates that contain the public key whenever they are requested. However, the corresponding private keys are protected. The private keys *never leave the card*. When the card is personalized (when a user is “enrolled”), the private keys are either securely generated by the microchip in the card itself or securely injected with a GlobalPlatform-capable Card Management System from a Hardware Security Module (HSM).

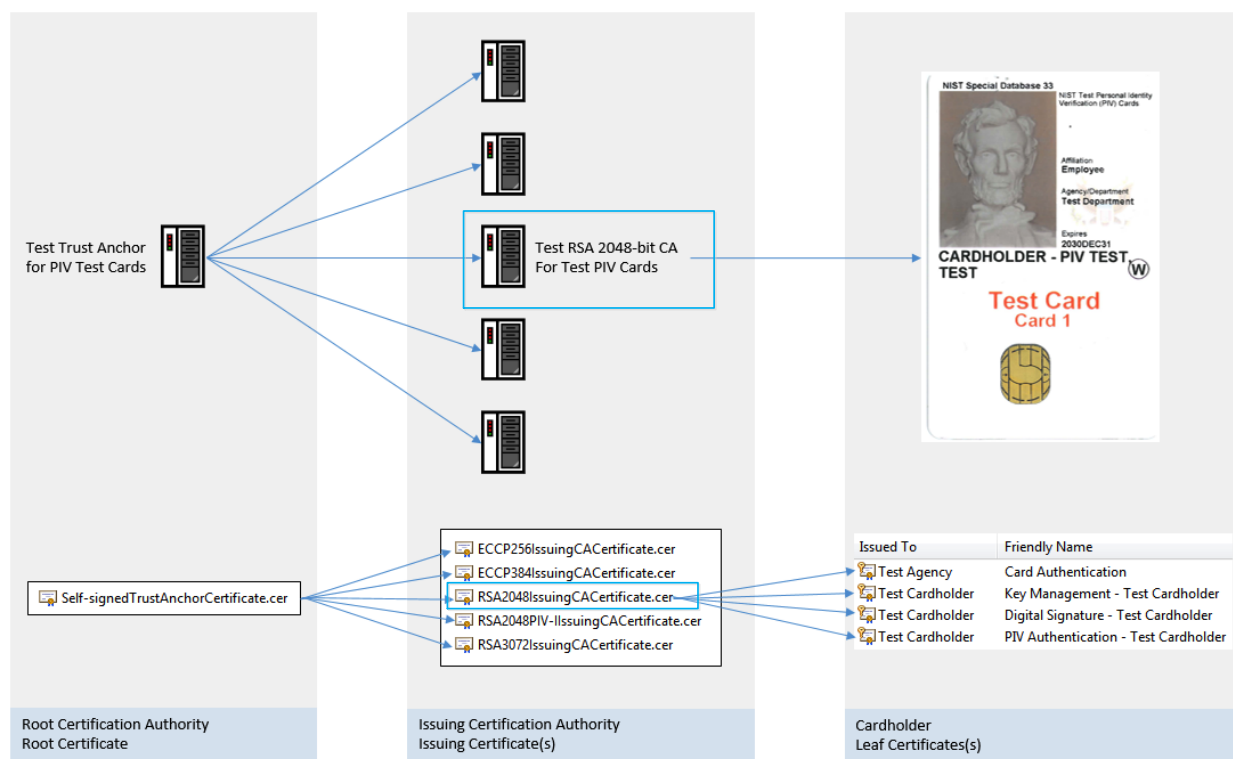
Because this document addresses authentication, we will focus on the PIV authentication certificate (the certificate used for logon).

NOTE

A certificate and its corresponding private key on the card can only be used for the purpose(s) (such as smart card logon—among others—in the case of the PIV authentication certificate) specified when the certificate is issued. The purpose(s) can usually be determined by examining the key usage and (if available) the enhanced key usage attributes of the certificate. For example, the digital signature certificate is used when digitally signing a document. Its key usage is shown as “Digital Signature, Non-Repudiation.”

The certificates on the card are issued as part of the personalization (user enrollment) process. In the case of NIST PIV test card #1, all four certificates were issued by the same issuing (intermediate) CA: Test RSA 2048-bit CA for Test PIV Cards.

Test RSA 2048-bit CA for Test PIV Cards, in turn, had its signing certificate issued by another CA: Test Trust Anchor for Test PIV Cards:

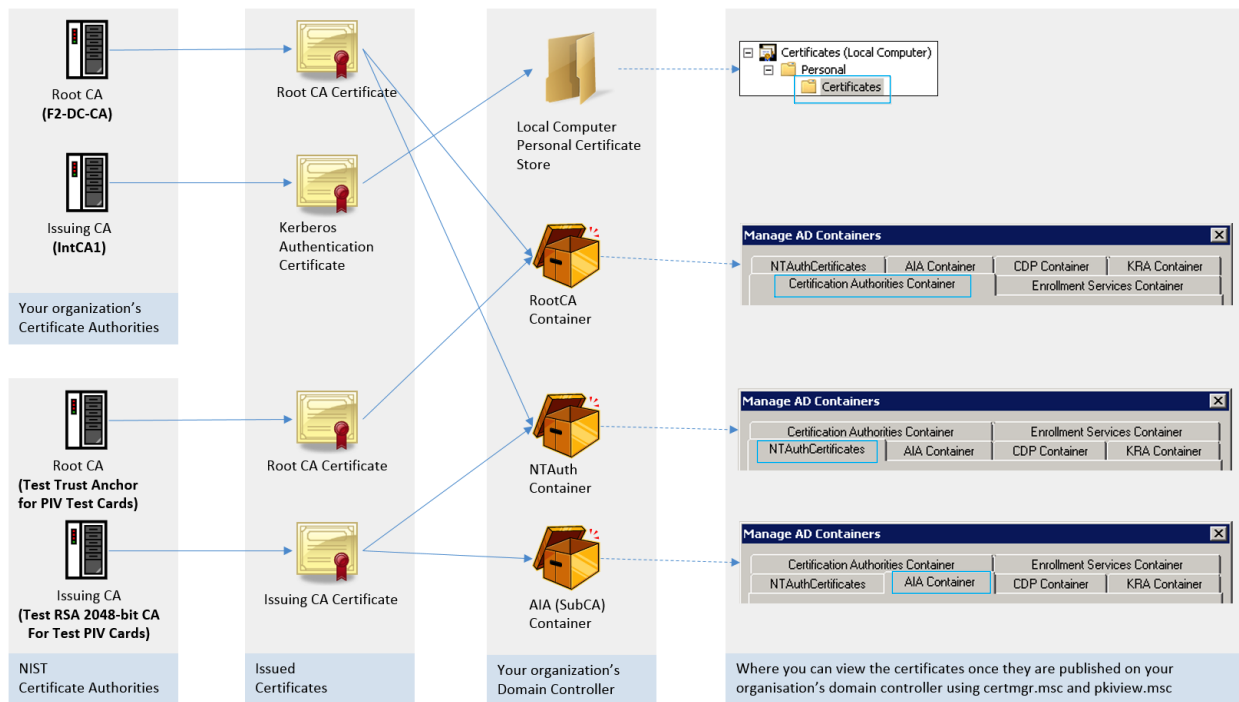


The chain ends at Test Trust Anchor for Test PIV Cards because it is signed by itself (not another CA). Self-signed CAs are also referred to as root CAs.

NOTE

For NIST PIV Test Card #1, all leaf certificates on the card have been issued by the same issuing CA. Leaf certificates on production cards are typically issued by at least two issuing CAs.

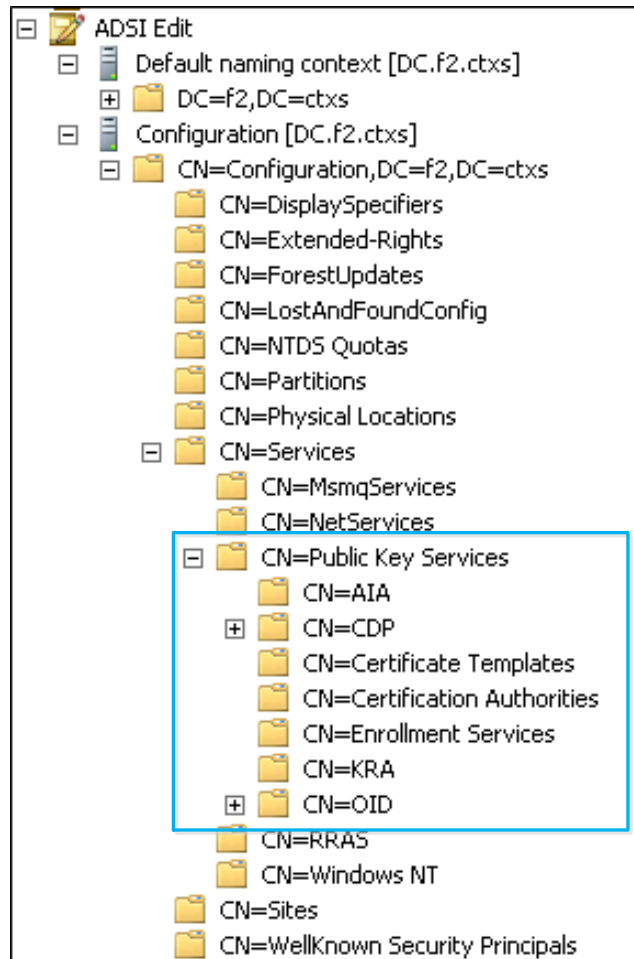
This chain of trust will be integrated into your Active Directory environment as follows:



NOTE

Viewing the AD Containers on your Active Directory domain controller via a GUI (as shown above) requires the Enterprise PKI snap-in. More information on how to install the Enterprise PKI snap-in can be found here: <https://technet.microsoft.com/en-us/library/cc771085.aspx>.

Another way to view the AD containers is via ADSI Edit: Configuration Naming Context > Services > Public Key Services (see below).



Appendix B: Obtaining CA Certificates from Root and Issuing Certificate Authorities

You can locate the root and issuing CA certificates for the NIST PIV Test kit from NIST:

<http://csrc.nist.gov/groups/SNS/piv/testcards.html>

CSRC HOME > GROUPS > SRET > PIV

NIST PERSONAL IDENTITY VERIFICATION TEST CARDS

In order to facilitate the development of applications and middleware that support the Personal Identity Verification (PIV) Card, the National Institute of Standards and Technology (NIST) has developed a set of test PIV Cards, which are available for purchase as a [NIST Special Database](#). An overview of the test PIV Cards is provided in [NISTIR 7870](#). [NIST Test Personal Identity Verification \(PIV\) Cards](#). [Technical Specifications for Personal Identity Verification \(PIV\) Test Cards](#) contains technical details about the contents of each of the test cards in the set.

All of the certificates on the test PIV Cards were issued from a test public key infrastructure (PKI), which was established to support the test cards. The PKI consists of a two-level hierarchy. In order to be able to validate the certificates on the test cards, it will be necessary to install the root certification authority (CA) from the PKI as a trust anchor in the software that will be validating the certificates. A self-signed CA certificate for the root CA, which may be used to establish the root CA as a trust anchor, is available at <http://csrc.nist.gov/groups/SNS/piv/documents/Self-signedTrustAnchorCertificate.cer>.

 Self-signedTrustAnchorCertificate.cer

As is required by FIPS 201-1, all of the certificates in the test PKI contain authorityInfoAccess and subjectInfoAccess extensions, where appropriate, with both LDAP and HTTP URIs that point to the intermediate CA certificates that are needed to create certification paths to validate the end-entity certificates on the PIV Cards. Not all software, however, is capable of using the information in these extensions to automatically retrieve the necessary certificates. In order to validate the test certificates with such software, it will be necessary to manually install the intermediate CA certificates in addition to the trust anchor certificate.

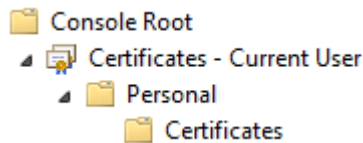
A [ZIP file](#) containing all of the intermediate CA certificates in the test PKI is available.

 ECCP256IssuingCACertificate.cer
 ECCP384IssuingCACertificate.cer
 RSA2048IssuingCACertificate.cer
 RSA2048PIV-1IssuingCACertificate.cer
 RSA3072IssuingCACertificate.cer

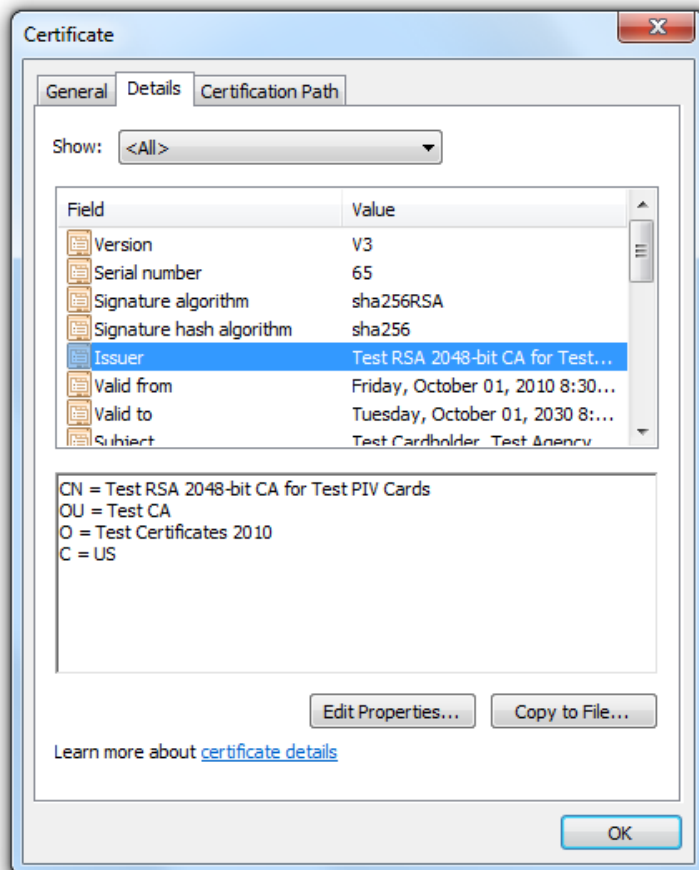
Appendix C: Manually validate the CA Chain of Trust From a Leaf Certificate to its Corresponding Root Certificate

This procedure can be performed with any smart card. In this example, the NIST PIV Test Card #1 is used.

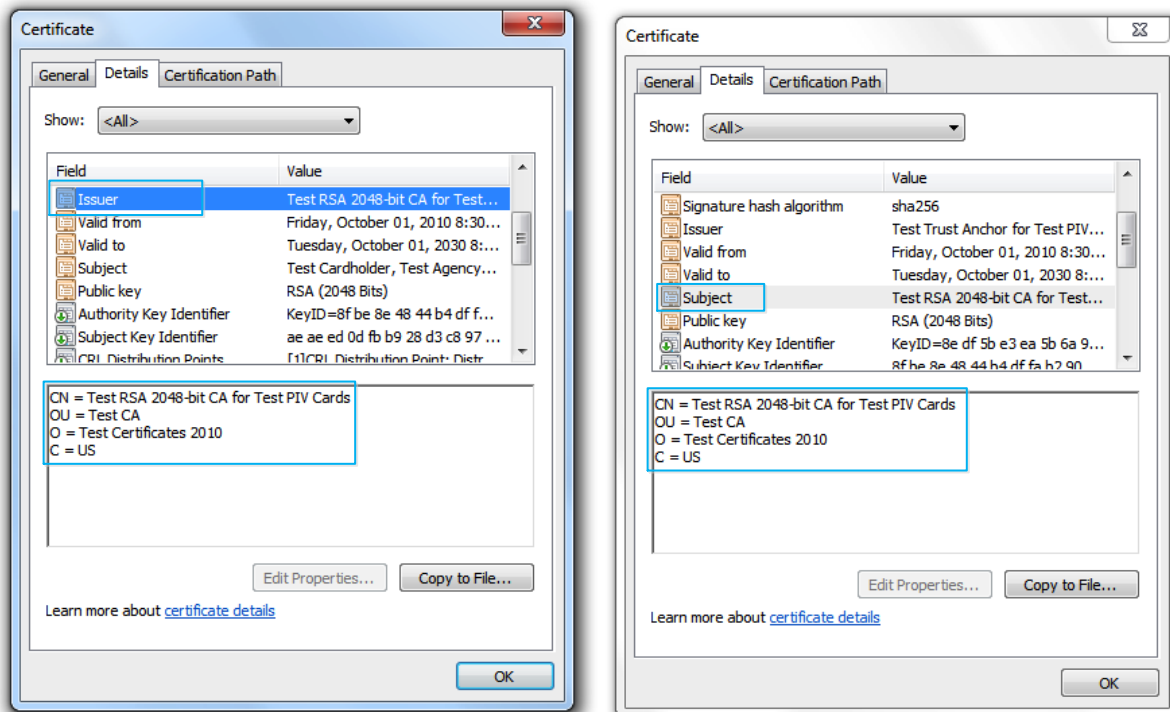
1. On a Windows machine with the appropriate smart card middleware installed:
2. Log on to the machine, and then insert the smart card. The certificates on the card should be copied from the card to the logged-on user's personal certificate store:



3. Open the PIV Authentication Certificate. Look at the Issuer field:

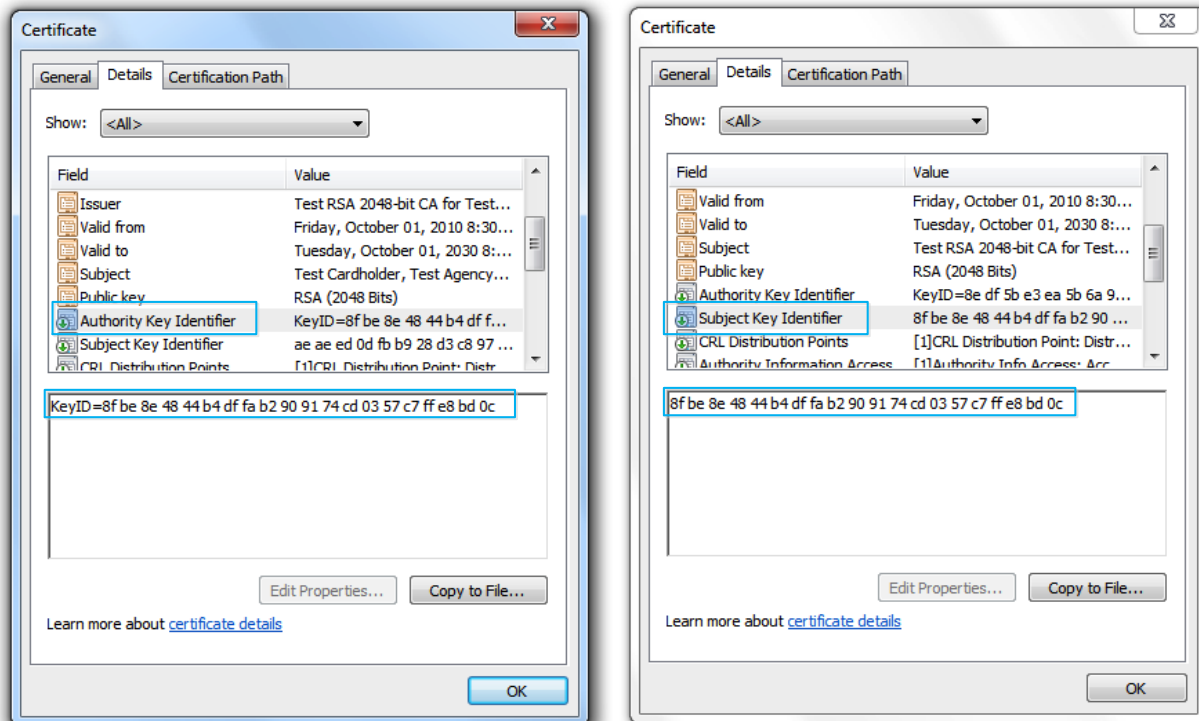


4. Locate the certificate from the issuer (NIST) with a subject field that matches the issuer field of the PIV authentication certificate:



The certificate on the left is the PIV authentication certificate on the smart card that is associated with the smart card user. The certificate on the right is associated with the issuing CA that issued the PIV authentication certificate.

- Confirm that the certificate from the issuing CA is the correct one by comparing the Authority key identifier field of the PIV authentication certificate with the Subject Key identifier field of the issuing CA certificate. They should match exactly.



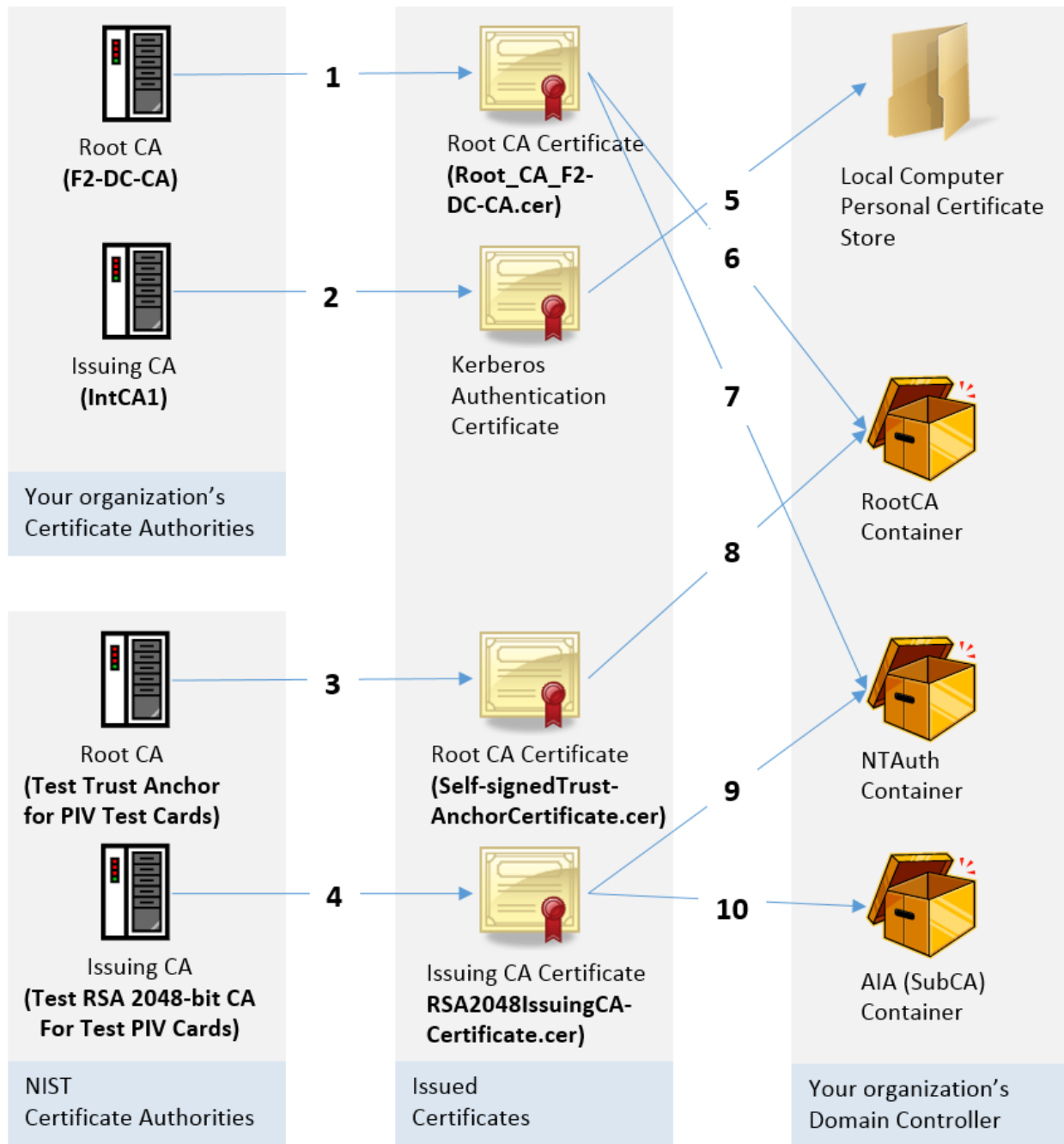
6. Repeat for the issuing and the root certificates.

NOTE

You know you have reached the end of the trust chain when you reach a certificate that is self-signed. That is, the issuer and subject are the same.

When using production cards, you will be able to repeat this procedure but will need to get the intermediate and root certificates from the appropriate source. Do not use the NIST PIV Test CA certificates in a production environment.

Appendix D: Publishing Certificates to Active Directory Containers

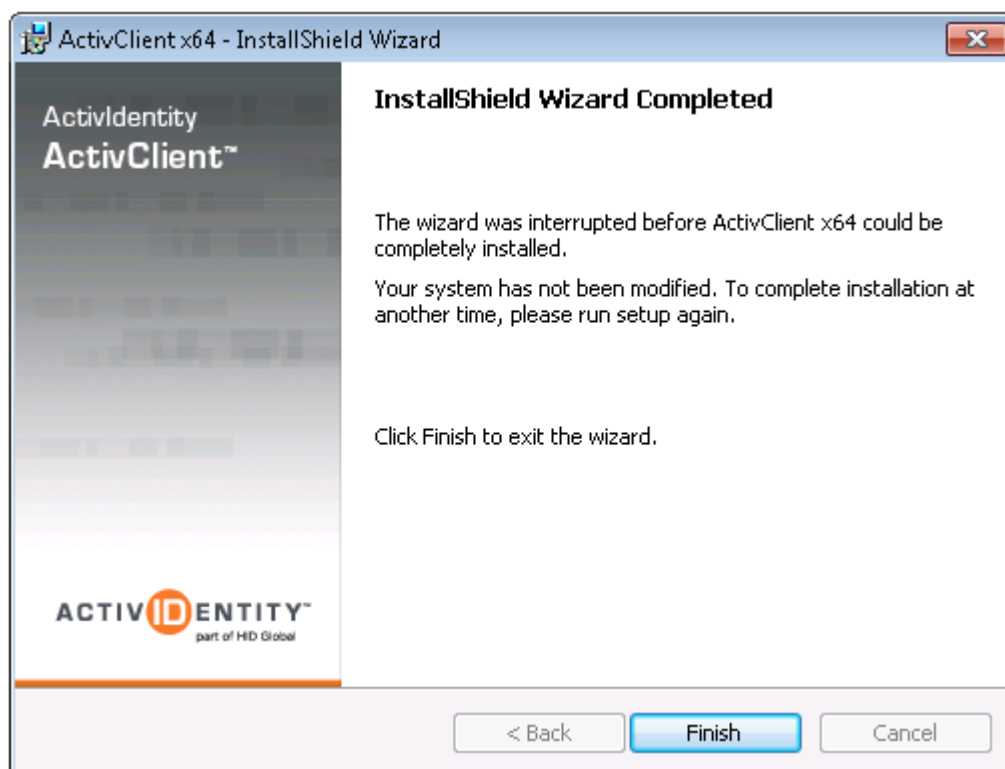


Appendix E:

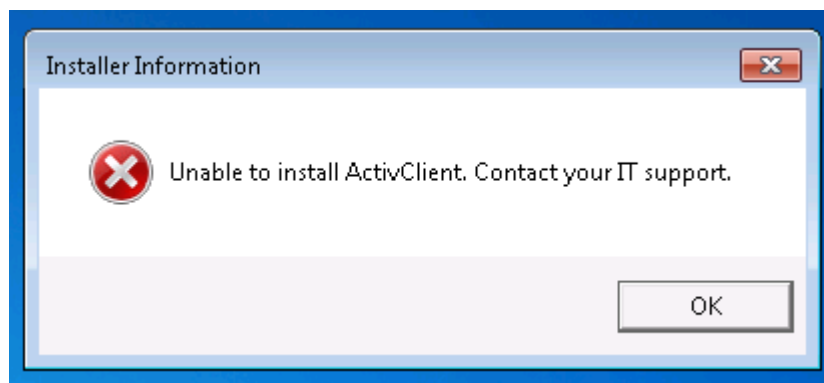
Install ActivClient 7.0.2 on Windows 7 x64

Warning: Do not install middleware from more than one vendor or different versions of the same middleware from the same vendor on the same machine at the same time because it can cause unpredictable behavior.

Warning: Do not install ActivClient 7.0.2 from a remote console (for example, by connecting to the machine using remote desktop connection). If you do, at the end of the installation process, installation will automatically roll back and then display the following message:



When you click **Finish**, this Installer Information dialog box will appear:

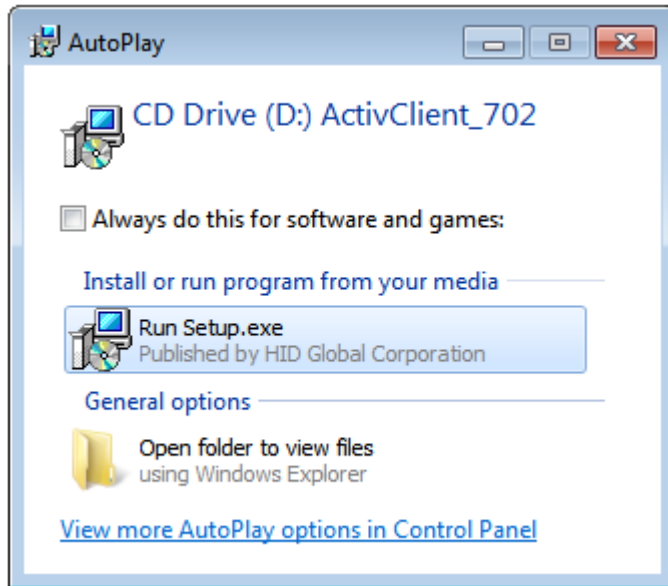


You must install ActivClient directly from the local machine console.

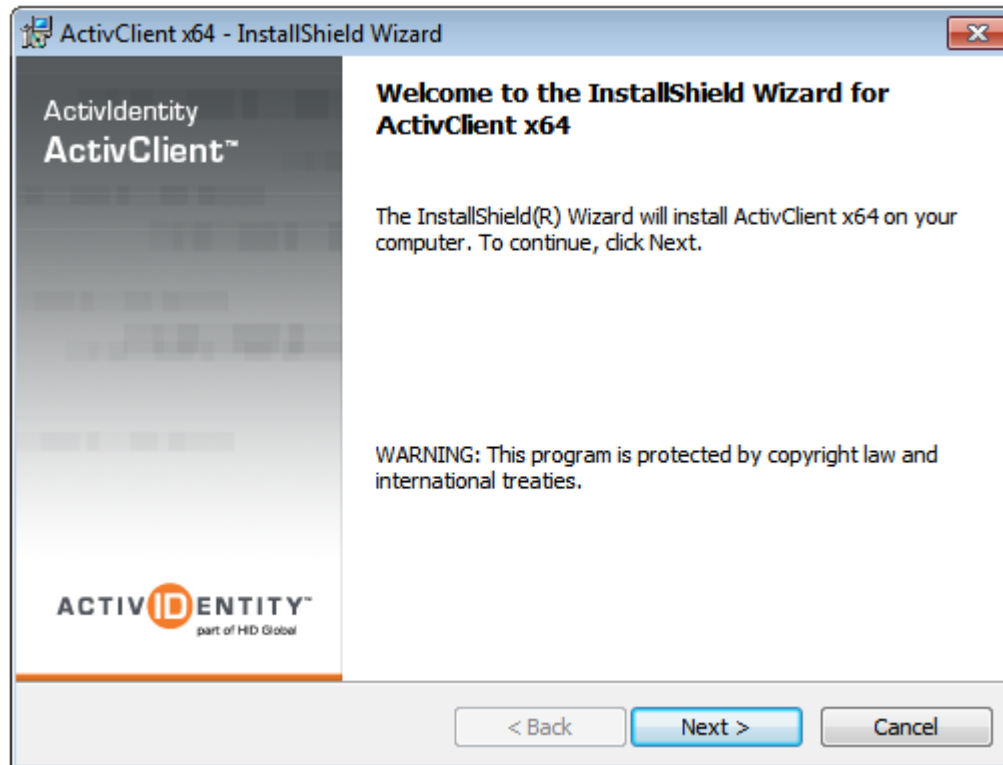
NOTE

If you want to install Microsoft Outlook Usability Enhancements and PKCS#11 support (required by applications such as Mozilla Firefox), you will have to install Microsoft Office and Mozilla Firefox prior to running the ActivClient installer.

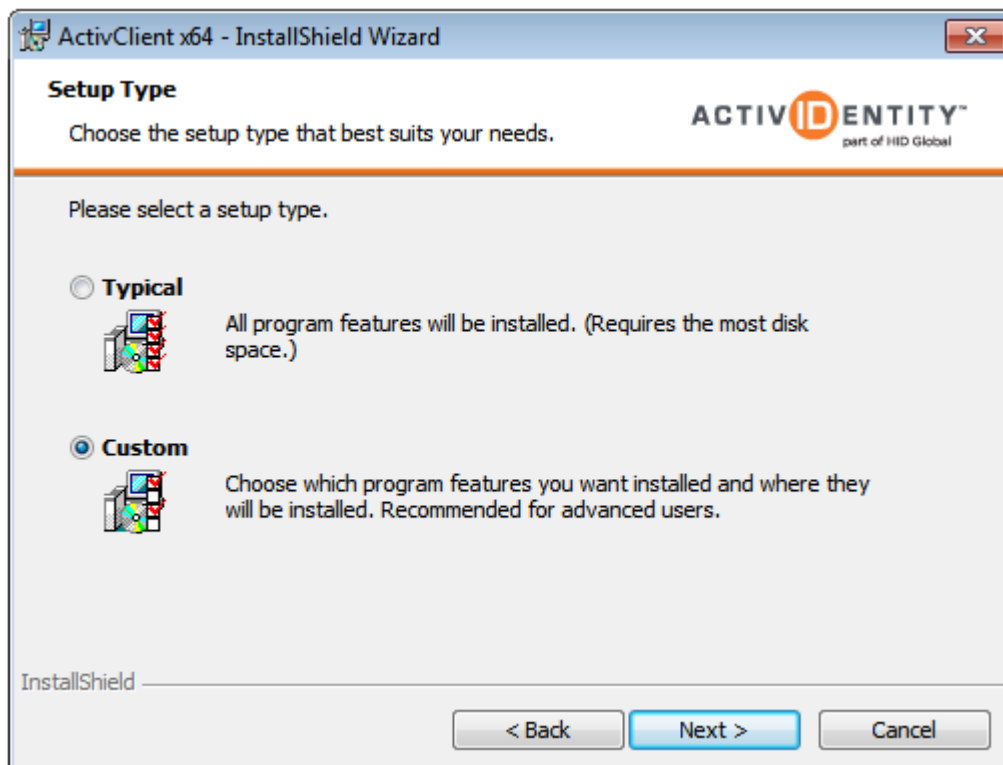
1. Insert the ActivClient installation media, and run Setup.exe:



The ActivClient x64 InstallShield Wizard opens:



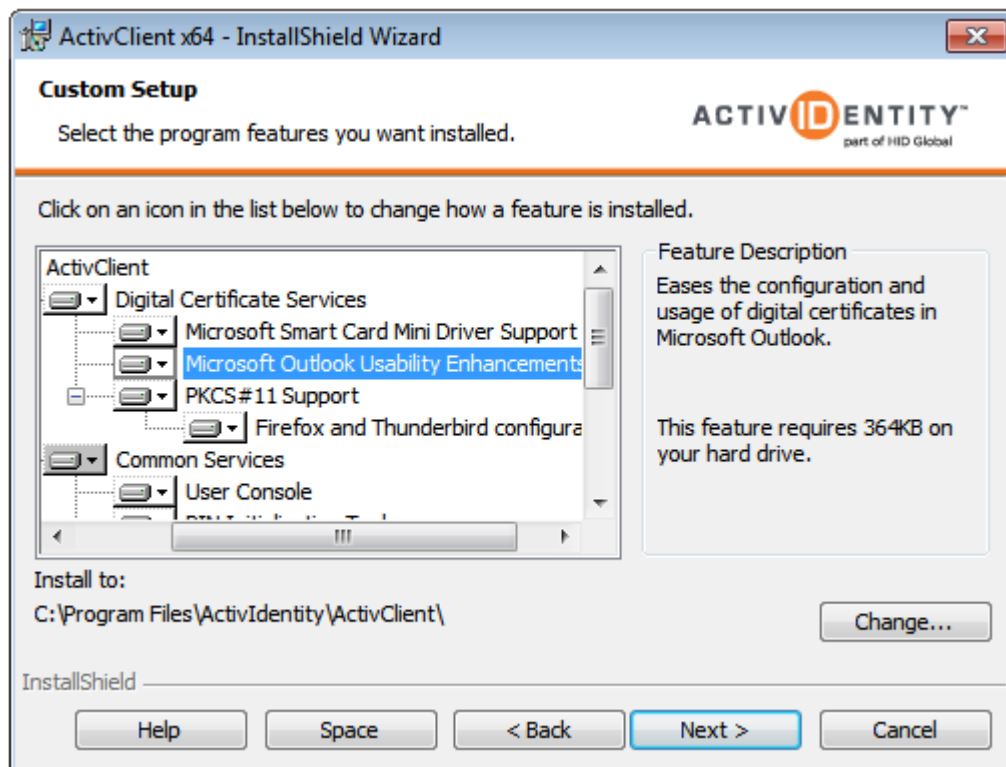
2. You will be prompted to choose a setup type:



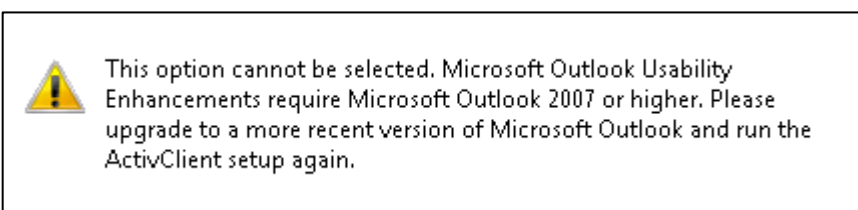
3. Select Custom.

NOTE

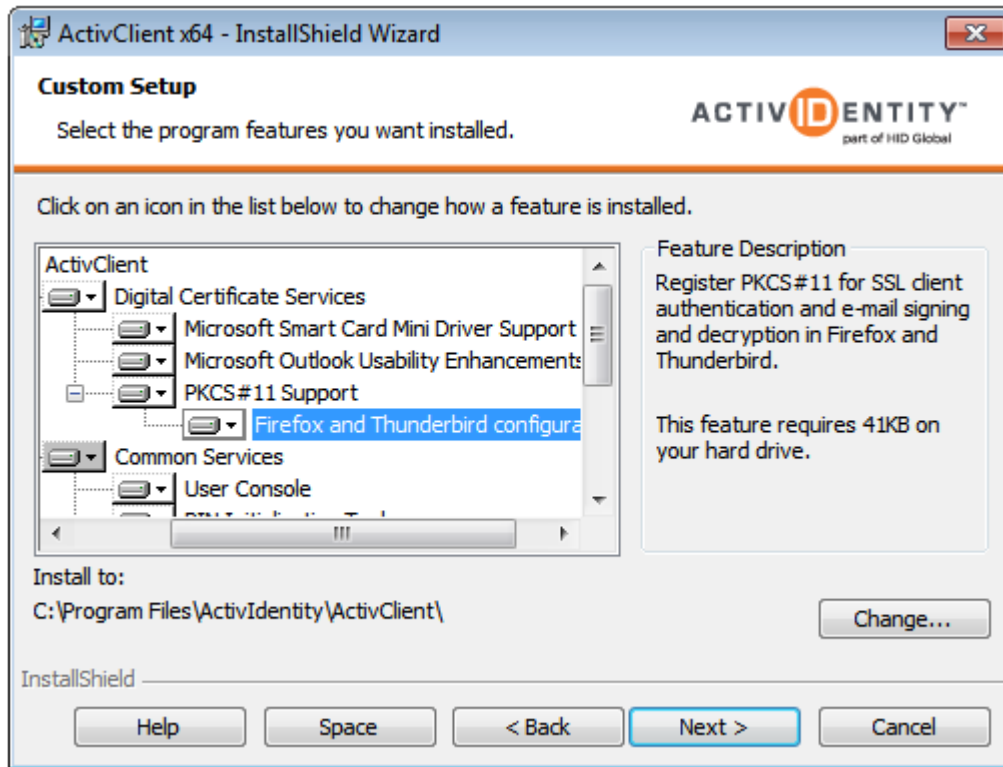
Installation options that are shown in screenshots below will possibly differ in your environment depending on your requirements. You do not have to duplicate every selection depicted below.



If Microsoft Outlook is installed on the machine prior to running the ActivClient installer, you can opt to install Microsoft Outlook Usability Enhancements. If you select this option and Microsoft Outlook is not installed, the following message will be displayed:

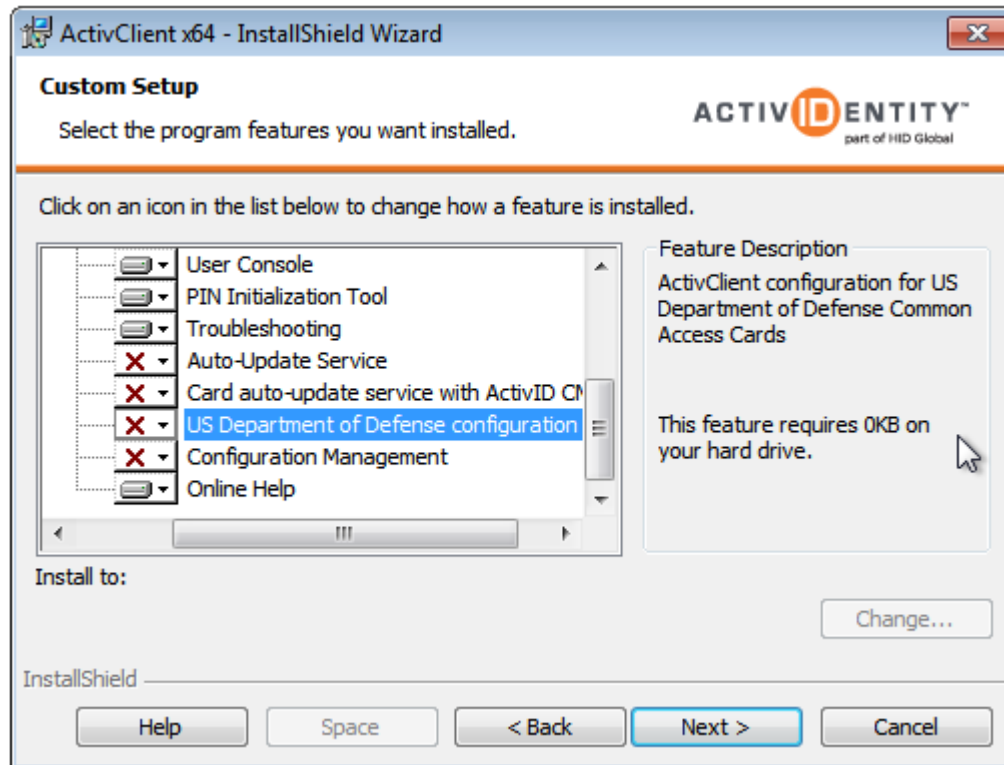


If Mozilla Firefox is installed on the machine prior to running the ActivClient installer, you can opt to install PKCS#11 Support:



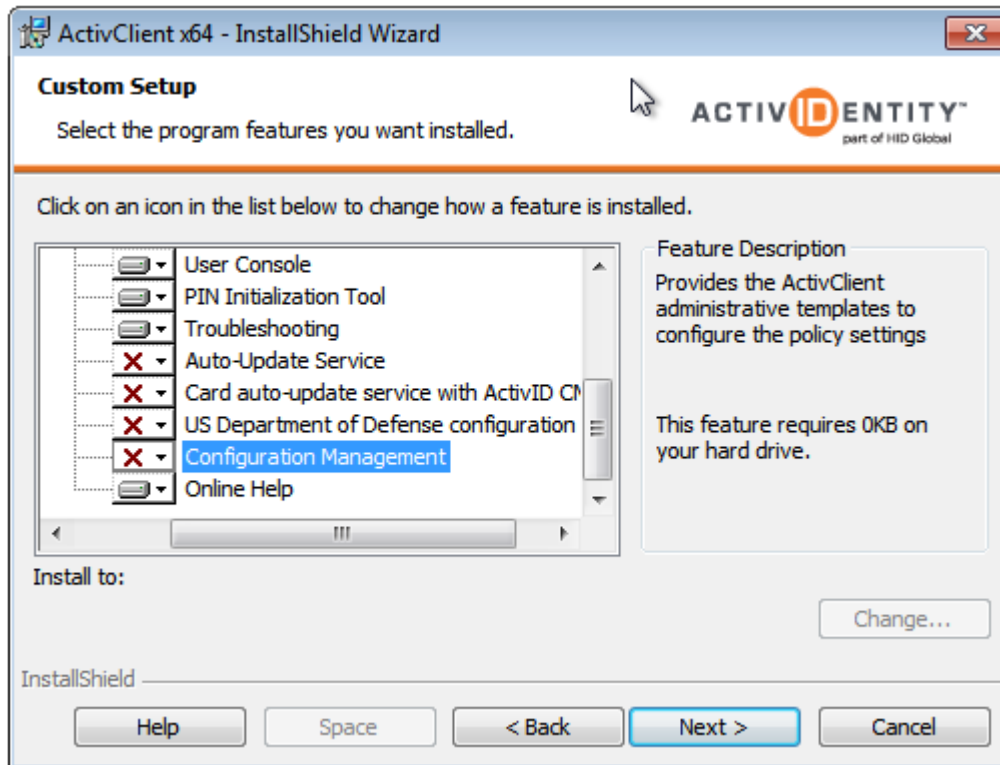
PKCS#11 libraries are required for certain applications (such as Mozilla Firefox, Adobe Reader, and others) that do not utilize Microsoft CAPI/CNG to communicate with a smart card.

4. Do not install US Department of Defense configuration:

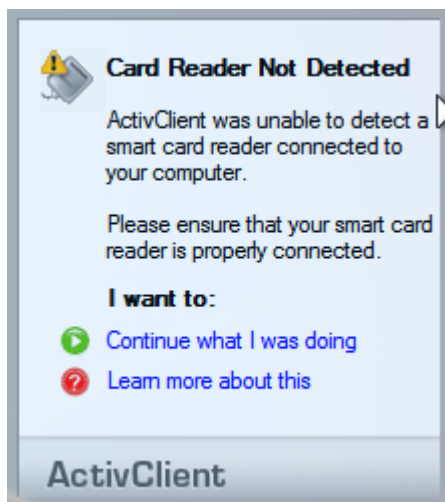


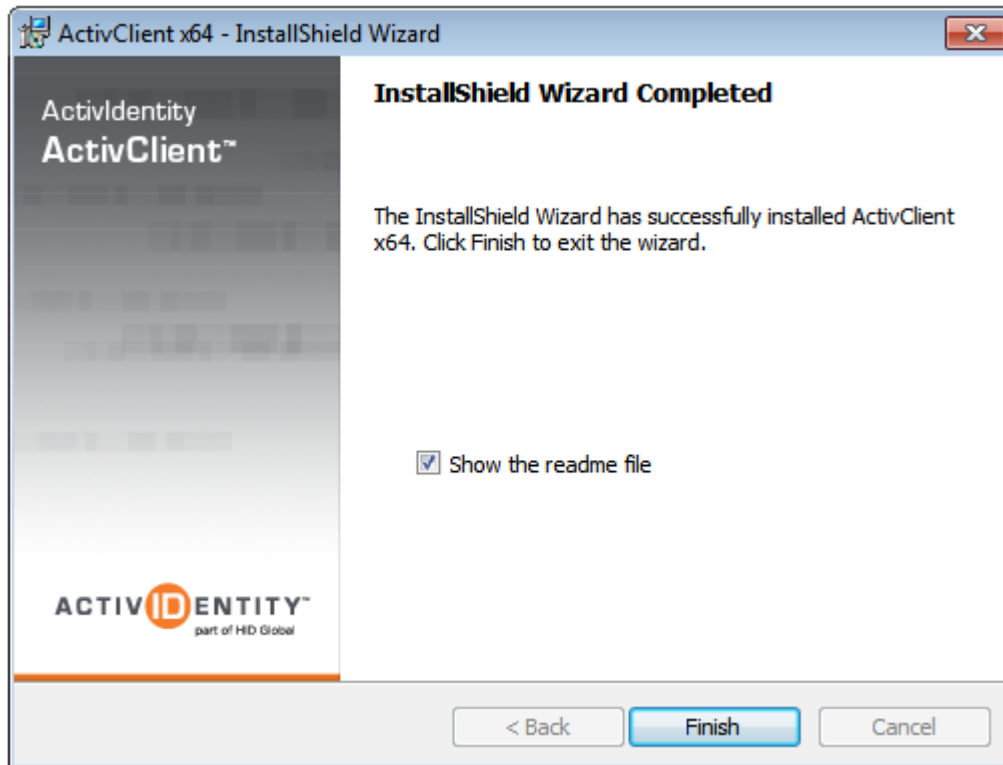
This option can be toggled later via group policy, if it is ever required. When selected, ActivClient will communicate with inserted smart cards using the GSC-IS standard. GSC-IS is used with Department of Defense Common Access Cards (CAC). If "US Department of Defense configuration" is not selected during ActivClient installation, ActivClient will communicate with the inserted smart cards using the PIV standard.

If you want local machine control of advanced ActivClient configuration settings, you can install Configuration Management. These are the same advanced configuration settings that can be centrally administered via the Microsoft Active Directory Group Policy Administrative Template.



- When finished, the ActivClient Agent will mention that there is no reader connected. This can be safely ignored.



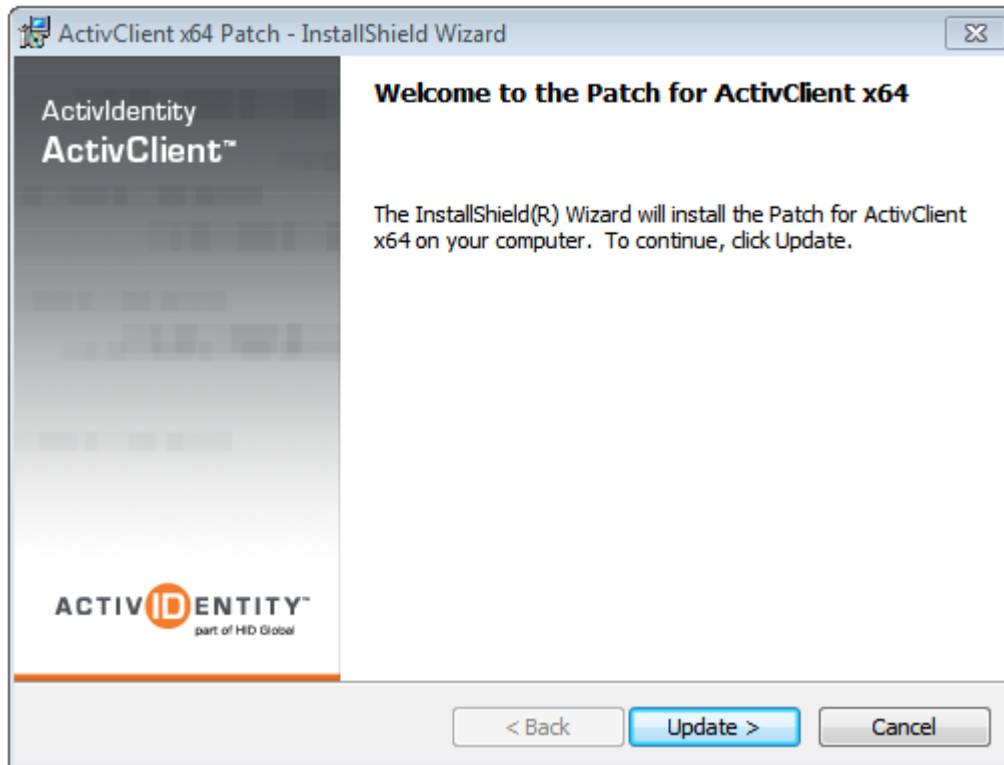


6. Click **Finish**.
7. Reboot the computer.
8. Log on as a user with administrative privileges.
9. Install the ActivClient hotfix (if required).

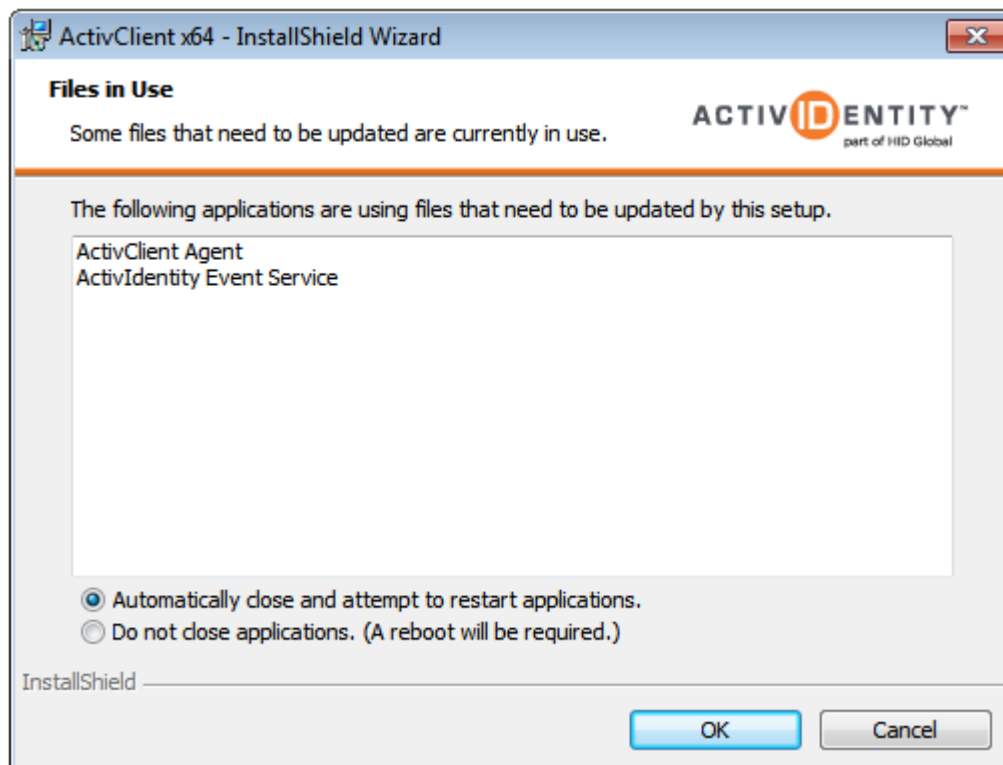
NOTE

Latest hotfix at time of writing:

ActivClient® Hot Fix FIXS1412004.msp / Version 7.0.2.409 / Published on 2014-12-03



10. Click Update.



11. Click OK and then Finish.

12. Reboot the machine.

Appendix F:

How NetScaler Gateway Certificate and LDAP Authentication Policies Map to an Active Directory User Account

User certificate to LDAP user account mapping with a NetScaler Gateway can be flexible.

What follows is an elaboration on the rationale for using the example from the test environment in the main document. It will also show how and where you can change mappings to suit your own environment.

There are four parts involved in mapping user certificates to LDAP user accounts using NetScaler Gateway:

- 1) What authentication policies to use ([NetScaler Authentication Policies](#))
- 2) The role of the certificate policy ([The Certificate Authentication Policy is used to map an attribute in the user's certificate to the User Name Field.](#))
- 3) The role of the LDAP Policy part 1 ([The Server Logon Name Attribute in the LDAP Authentication Policy is used to specify the attribute to search against on the Active Directory domain controller.](#))
- 4) The role of the LDAP policy part 2 ([The SSO Name Attribute in the LDAP Authentication Policy is used to specify the user account attribute and corresponding value the LDAP server should return to the NetScaler Gateway.](#))

NetScaler authentication policies

The recommended configuration is to have a NetScaler Gateway virtual server with two authentication policies bound to the virtual server; Certificate Policy of Type Primary and LDAP of type Group Extraction:

Policies	Policies
Choose Policy*	Choose Policy*
<input type="text" value="CERTIFICATE"/>	<input type="text" value="LDAP"/>
Choose Type*	Choose Type*
<input type="text" value="Primary"/>	<input type="text" value="Group Extraction"/>

NOTE

The difference between primary, secondary, and group extraction authentication policies are as follows: Primary and secondary policies are used for user authentication. Group extraction is used to obtain information from an LDAP server (for example, Active Directory domain controller) that the NetScaler Gateway can use in an Action; it is not used for user authentication. Primary policies are processed before secondary policies. Group extraction is performed once primary and/or secondary policies have been processed successfully.

If there is more than one primary policy bound to a NetScaler Gateway virtual server, the primary policies will process in order of priority. In order for primary authentication to succeed, only one of the primary authentication policies need to process successfully. The NetScaler Gateway is using an OR condition to determine authentication success between primary policies. For example, if there are four primary policies bound to a NetScaler Gateway virtual server, and three fail but one succeeds, primary authentication will succeed.

Once a primary policy has processed successfully, NetScaler Gateway will move on to the secondary policies if they are defined and bound. There can be multiple secondary policies, which are also processed in order of priority. Only one secondary authentication policy needs to process successfully in order for secondary authentication to succeed. As with primary, NetScaler Gateway is using an OR condition to determine success for the secondary policies.

If both primary and secondary authentication policies are defined and bound to a NetScaler Gateway virtual server, then at least one primary and at least one secondary authentication policy must process successfully for authentication to succeed. The NetScaler Gateway is using an AND condition to determine authentication success between primary and secondary authentication policies. If one Primary policy succeeds but no secondary policy succeeds, then authentication for the user will fail.

After the TLS connection between the client and the NetScaler Gateway Virtual Server is established (this TLS connection's behavior is governed in the SSL Parameters section of the NetScaler Gateway virtual server's settings), the authentication policies work as follows:

The Certificate Authentication Policy is used to map an attribute in the user's certificate to the User Name Field.

The user's certificate is the certificate on the user's smart card that is purposed for smart card logon. In the case of a NIST PIV card, this certificate is the PIV authentication certificate.

NOTE

There is currently a known issue with certificate filtering in Citrix Receiver under certain conditions. As a result, the user may be prompted to select the certificate manually. In future builds of Citrix Receiver, it is likely that Receiver will filter out all certificates that are not purposed for smart card logon and automatically use the appropriate certificate if only one of the certificates is purposed for smart card logon without having to prompt the user to select the certificate.

The Certificate Authentication Policy must be primary and have higher processing priority (for example, 100) than the LDAP Authentication Policy (for example, 110).

The exact certificate attribute you wish to use for mapping can be specified in the User Name Field in the Authentication Certificate Server on the NetScaler Gateway:

Authentication CERT Server

Name

f2-cert-server

Authentication Type

CERT

Two Factor



ON



OFF

User Name Field

SubjectAltName:PrincipalName



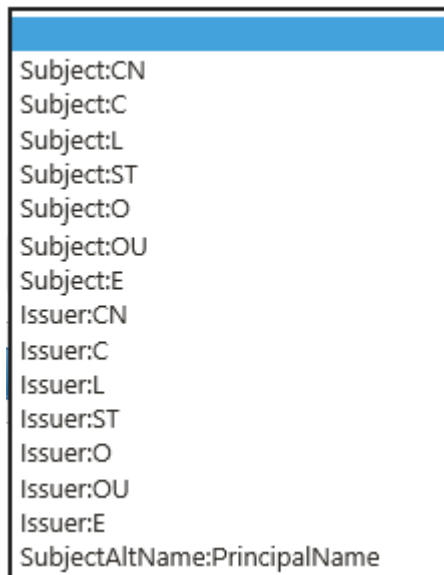
Group Name Field



Default Authentication Group

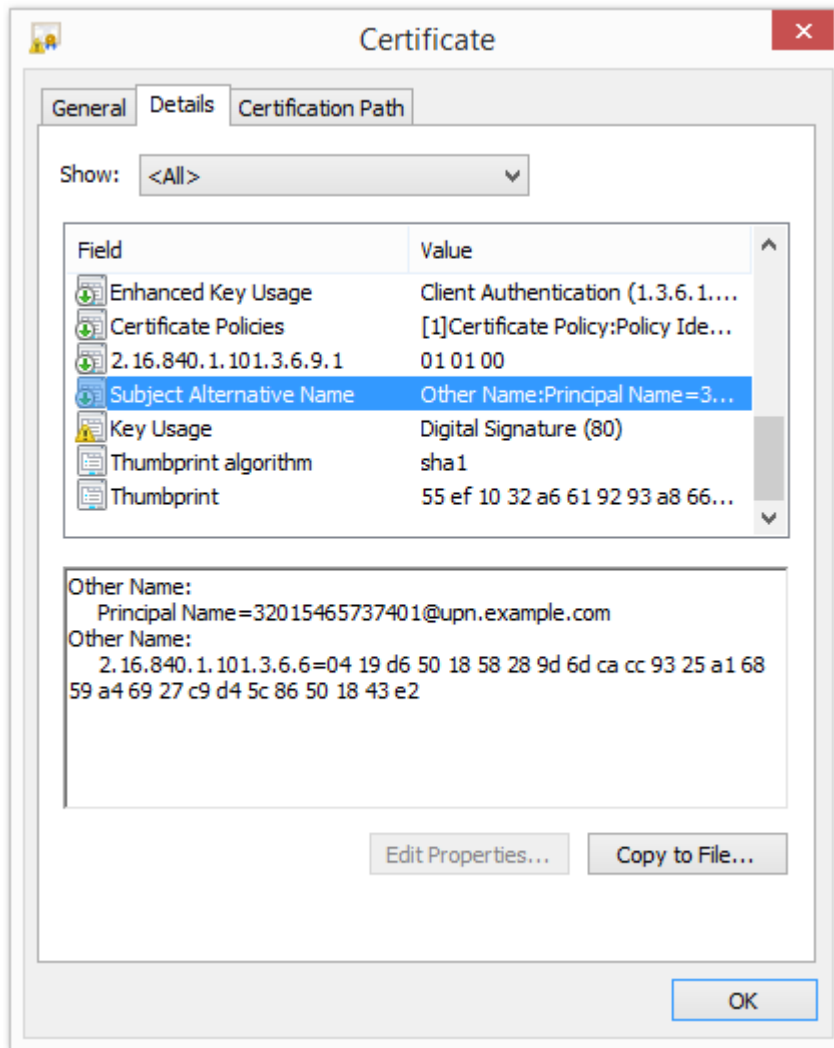


The User Name Field can be set to map any of the following certificate attributes from the user's certificate:



For NIST PIV Test Card #1, we select SubjectAltName:PrincipalName.

SubjectAltName is a certificate attribute, and PrincipalName is a sub-attribute. It appears as follows in the PIV authentication certificate on NIST PIV Test Card #1:



NOTE

2.16.840.1.101.3.6.6 is the OID (Object Identifier) for pivFASC-N. According to NIST FIPS PUB 201-2: Personal Identity Verification (PIV) of Federal Employees and Contractors:

“The pivFASC-N OID may appear as a name type in the otherName field of the subjectAltName extension of X.509 certificates or a signed attribute in CMS external signatures. Where used as a name type, the syntax is OCTET STRING. Where used as an attribute, the attribute value is of type OCTET STRING. In each case, the value specifies the FASC-N of the PIV Card.”

FASC-N stands for Federal Agency Smart Credential Number. The FASC-N is the primary identification string to be used on all government issued credentials.

The FASC-N is defined in the Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems, Version 2.3E [PACS 2.3E]. It consists of 40 total characters encoded as Packed Binary Coded Decimal (BCD) format with odd parity creating a 200-bit (25 byte) record:

	Field Name	Length (BCD Digits)	Field Description
Uniquely Identifies Card	Agency Code	4	Identifies the government agency issuing the credential
	System Code	4	Identifies the system the card is enrolled in and is unique for each site
	Credential Number	6	Encoded by the issuing agency. For a given system no duplicate numbers are active.
	Credential Series (Series Code)	1	Extends the Credential Number
	Individual Credential Issue	1	Extends the Credential Number
Uniquely Identifies Card Holder	Person Identifier	10	Numeric Code used by the identity source to uniquely identify the token carrier
	Organization Category	1	Type of Organization the individual is affiliated with
	Organization Identifier	4	The Identifier that identifies the organization the individual is affiliated with.
	Person/Organization Association Category	1	Indicates the affiliation type the individual has with the Organization.

Interesting fact: When a DoD CAC (Department of Defense Common Access Card) is issued, it does not contain a PIV authentication certificate (a PIV authentication certificate/key and applet can be loaded on certain cards post-issuance). With CAC cards, the signing certificate is used for smart card login.

NetScaler Gateway extracts the value in the user's certificate (in this case, 32015465737401@upn.example.com) for the certificate attribute (in this case, Subject Alternative Name) as specified in User Name Field in the Certificate Authentication Server setting on the NetScaler Gateway (in this case, SubjectAltName:PrincipalName).

The Server Logon Name Attribute in the LDAP Authentication Policy is used to specify the attribute to search against on the Active Directory domain controller

NOTE

Even though the LDAP policy—when set to be of type Group Extraction—does not actually authenticate the user, it achieves the following: It confirms that a corresponding Active Directory user account exists. It can also be used (albeit not in this example) by the NetScaler Gateway to extract Active Directory group membership for the matching user and then in turn use that information to inform a NetScaler Gateway policy that is based on group membership. It can be used to dynamically place a user in a NetScaler Gateway AAA group that is defined in the NetScaler Gateway User Administration area.

This setting is configured in the Authentication LDAP Server settings on the NetScaler Gateway:

Authentication LDAP Server

Other Settings

Server Logon Name Attribute
 --<< New >>--
 userPrincipalName

Search Filter

Group Attribute
 memberOf

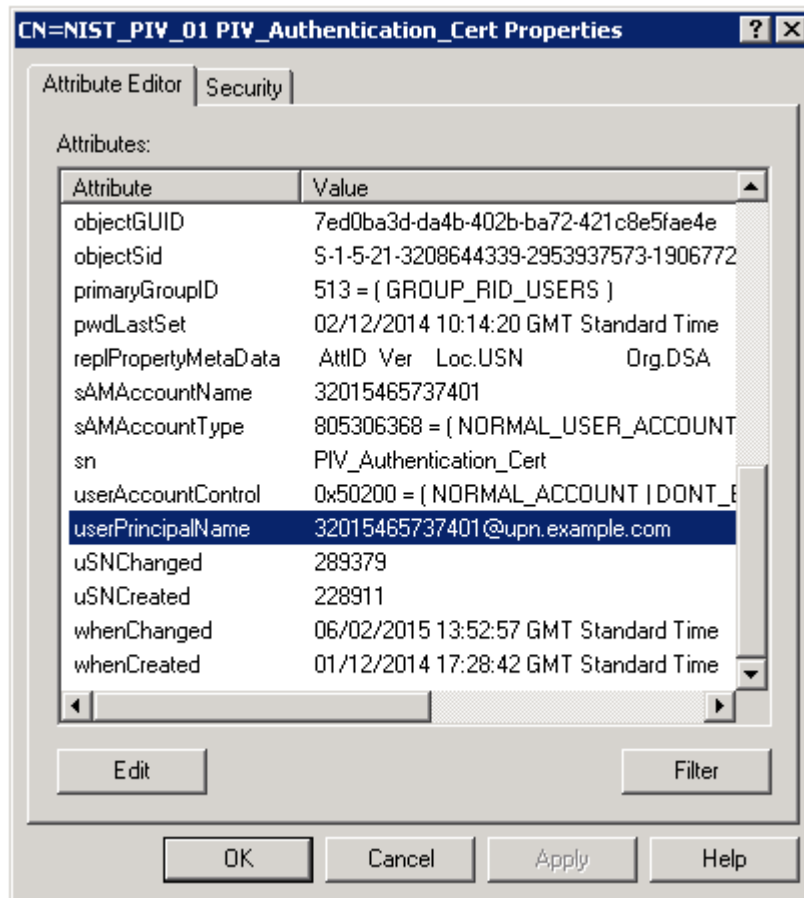
Sub Attribute Name
 CN

SSO Name Attribute
 --<< New >>--
 userPrincipalName

NetScaler Gateway uses the value of the attribute that you specify in Server Logon Name Attribute (in this example userPrincipalName) to query the LDAP server (In this case an Active Directory Domain Controller).

The NetScaler Gateway is asking the domain controller to find the Active Directory user account where the value of the Server Logon Name Attribute (in this case the userPrincipalName Active Directory account attribute) matches the value extracted as the User Name Field in the user's certificate (in this case the SubjectAltName:PrincipalName which is 32015465737401@upn.example.com on NIST PIV Test Card #1)

The potential attributes that can be used with their corresponding values for a given account can be inspected with ADSI Edit on an Active Directory Domain Controller:



The SSO name attribute in the LDAP authentication policy is used to specify the user account attribute and corresponding value the LDAP server should return to the NetScaler Gateway

Once the LDAP Server (in this example, the Active Directory domain controller) has located the user account object based on the attribute that was specified in the Server Logon Name Attribute, it can return a value from a different attribute for that user account back to the NetScaler Gateway.

This attribute is specified in the SSO Name Attribute area:

Authentication LDAP Server

Other Settings

Server Logon Name Attribute

--< New >--

userPrincipalName

Search Filter

Group Attribute

memberOf

Sub Attribute Name

CN

SSO Name Attribute

--< New >--

userPrincipalName

The NetScaler Gateway will take the value it receives for the SSO name attribute and pass that as the user name to the StoreFront server. The most useful attribute that can be sent to StoreFront is the userPrincipalName. (StoreFront in turn performs an S4U operation with the domain controller to extract SIDs. StoreFront sending the userPrincipalName it is very helpful in multidomain scenarios).

NOTE

Because the User Principal Name was available from the PIV Authentication certificate on the NIST PIV Test Card #1 used in this example, User Principal Name was used in both the Server Logon Name Attribute to search Active Directory and in the SSO Name Attribute to be returned from Active Directory.

There may be use cases (different smart cards or standards) where the User Principal Name is not available in the certificate. In such a case, you have to specify a different Server Logon Name Attribute (for example, sAMAccountName, or a host of others).

Ultimately, when using StoreFront, you want the SSO Name Attribute always to be userPrincipalName.

For customers who are using Web Interface with XenApp: If “PIN Prompt” is selected in Web Interface Authentication methods, the SSO Name Attribute should be sAMAccountName. In addition, when using Web Interface with XenApp, you should specify the Single Sign-on domain in the Published Applications section of the NetScaler Gateway Session Profile.

The reason for doing this when using “PIN Prompt” smart card authentication with Web Interface and XenApp:

- 1) User logs on to NetScaler Gateway.
- 2) The NetScaler Gateway sends domain\user name to Web Interface through the CitrixAGBasic protocol.
- 3) Web Interface sends requests to the XML service with the domain\user name and no password (Requires that SID enumeration be enabled on XenApp, as per <http://support.citrix.com/article/ctx117489>)
- 4) The XML service uses SID enumeration to discover the user's identity and is then able to retrieve the user's applications.

The XML service requests being made in step 3 (with SID enumeration enabled and lacking a password) would only work if the identity is provided in domain\user name format. When a UPN was used, the XML service returns an error.

About Citrix

Citrix (NASDAQ:CTXS) is a leader in mobile workspaces, providing virtualization, mobility management, networking and cloud services to enable new ways to work better. Citrix solutions power business mobility through secure, personal workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud.

Copyright © 2015 Citrix Systems, Inc. All rights reserved. Citrix Receiver, HDX, NetScaler, NetScaler Gateway, StoreFront, XenApp, XenDesktop are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.