TOMCAT 8.5.4 SAML SSO with ADFS

Prepared

Active Directory Server

OS: Windows server 2012 R2

IP:192.168.56.254

Computer Name:addc.inpanya.local

Domain name: inpanya.local

ADFS Server

OS: Windows server 2012 R2

IP:192.168.56.252

Computer Name:adfs2012.inpanya.local

Domain name: inpanya.local

ADFS Service : adfs.inpanya.local

Certificate Authority Server :

OS: Windows server 2012 R2

IP:192.168.56.253

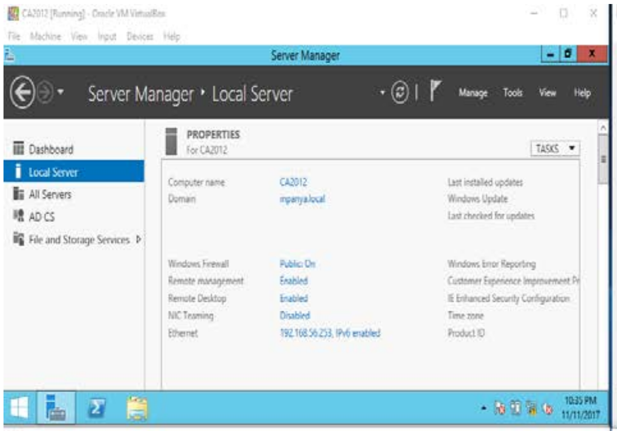
Computer Name:ac2012.inpanya.local

Tomcat Server :

OS: Windows server 2012 R2

Computer Name :samlsp.inpanya.local

Domain address:tomcat1.inpanya.local


CA2012 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager ‣ Local Server
Manage Tools View Help
Dashboard
Local Server
All Servers
AD CS
File and Storage Services
TASKS
10:35 PM
11/11/2017

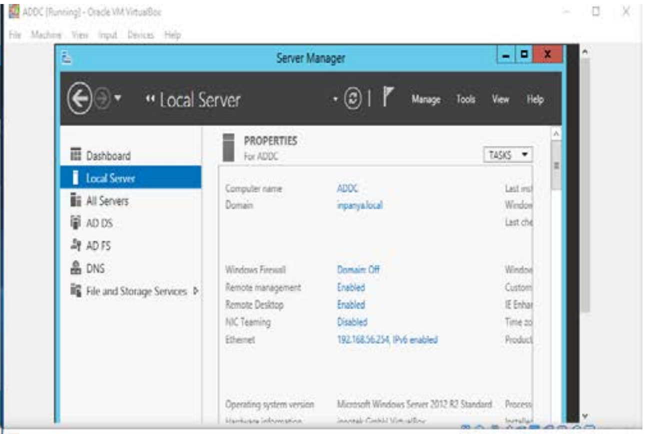
PROPERTIES
For CA2012

Computer name CA2012
Domain inpanya.local

Last installed updates
Windows Update
Last checked for updates

Windows Firewall Public: On
Remote management Enabled
Remote Desktop Enabled
NIC Teaming Disabled
Ethernet 192.168.56.253, IPv6 enabled

Windows Error Reporting
Customer Experience Improvement Pr
IE Enhanced Security Configuration
Time zone
Product ID



PROPERTIES
For ADDC

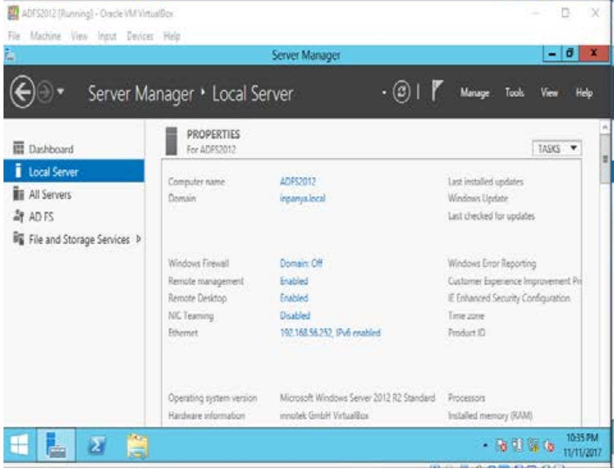
Computer name ADDC
Domain inpanya.local

Last ins
Window
Last che

Windows Firewall Domain: Off
Remote management Enabled
Remote Desktop Enabled
NIC Teaming Disabled
Ethernet 192.168.56.254, IPv6 enabled

Window
Custom
IE Enhar
Time zo
Product

Operating system version Microsoft Windows Server 2012 R2 Standard
Process
Hardware information innotek GmbH VirtualBox
Installed


ADFS2012 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager ‣ Local Server
Manage Tools View Help
Dashboard
Local Server
All Servers
AD FS
File and Storage Services
TASKS
10:35 PM
11/11/2017

PROPERTIES
For ADFS2012

Computer name ADFS2012
Domain inpanya.local

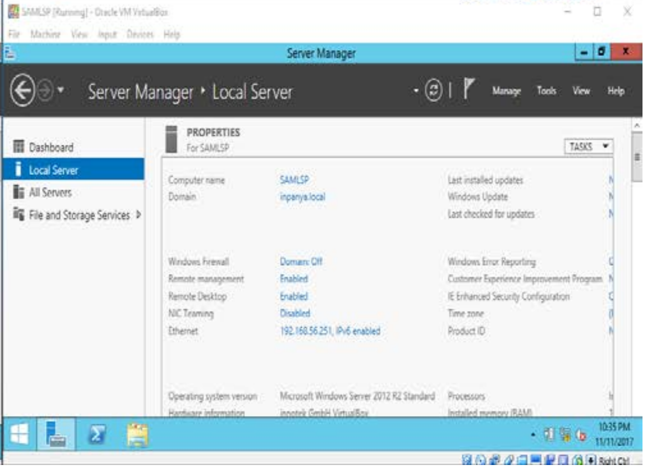
Last installed updates
Windows Update
Last checked for updates

Windows Firewall Domain: Off
Remote management Enabled
Remote Desktop Enabled
NIC Teaming Disabled
Ethernet 192.168.56.252, IPv6 enabled

Windows Error Reporting
Customer Experience Improvement Pr
IE Enhanced Security Configuration
Time zone
Product ID

Operating system version Microsoft Windows Server 2012 R2 Standard
Hardware information innotek GmbH VirtualBox

Processors
Installed memory (RAM)


SAMLSP [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager ‣ Local Server
Manage Tools View Help
Dashboard
Local Server
All Servers
File and Storage Services
TASKS
10:35 PM
11/11/2017
Right Ctrl

PROPERTIES
For SAMLSP

Computer name SAMLSP
Domain inpanya.local

Last installed updates
Windows Update
Last checked for updates

Windows Firewall Domain: Off
Remote management Enabled
Remote Desktop Enabled
NIC Teaming Disabled
Ethernet 192.168.56.251, IPv6 enabled

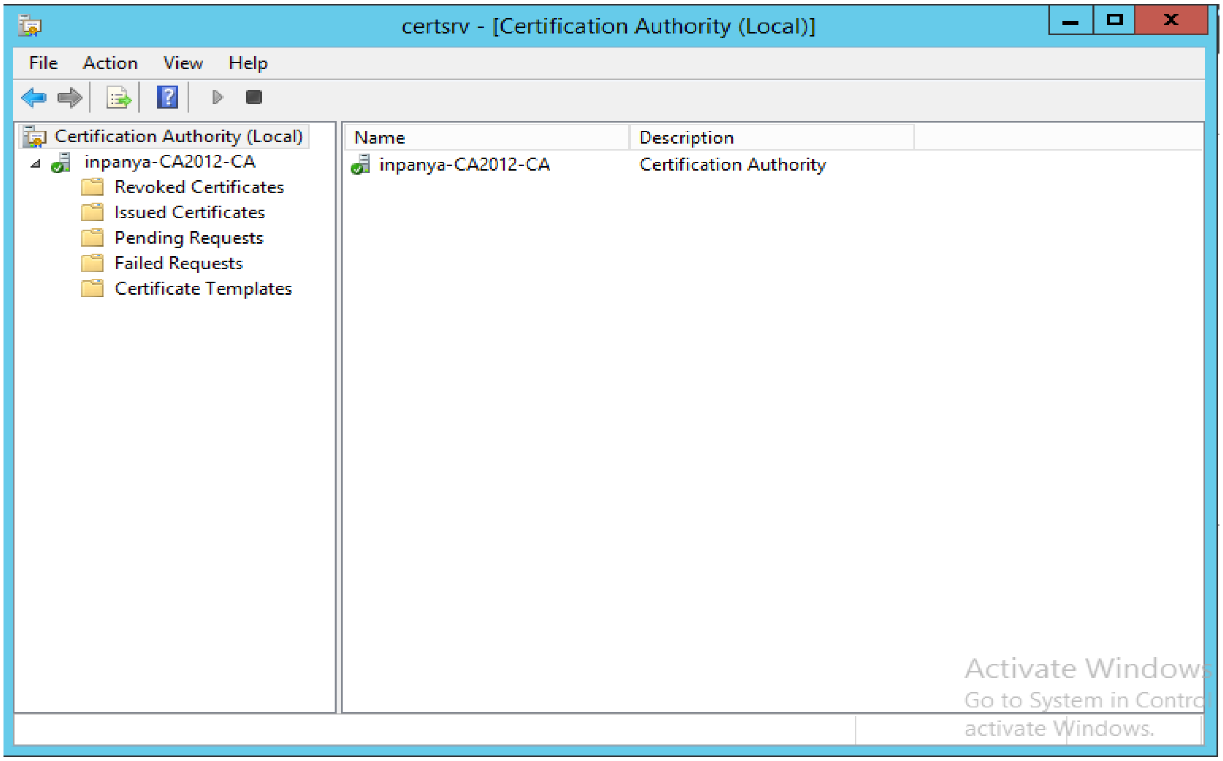
Windows Error Reporting
Customer Experience Improvement Program
IE Enhanced Security Configuration
Time zone
Product ID

Operating system version Microsoft Windows Server 2012 R2 Standard
Hardware information innotek GmbH VirtualBox

Processors
Installed memory (RAM)

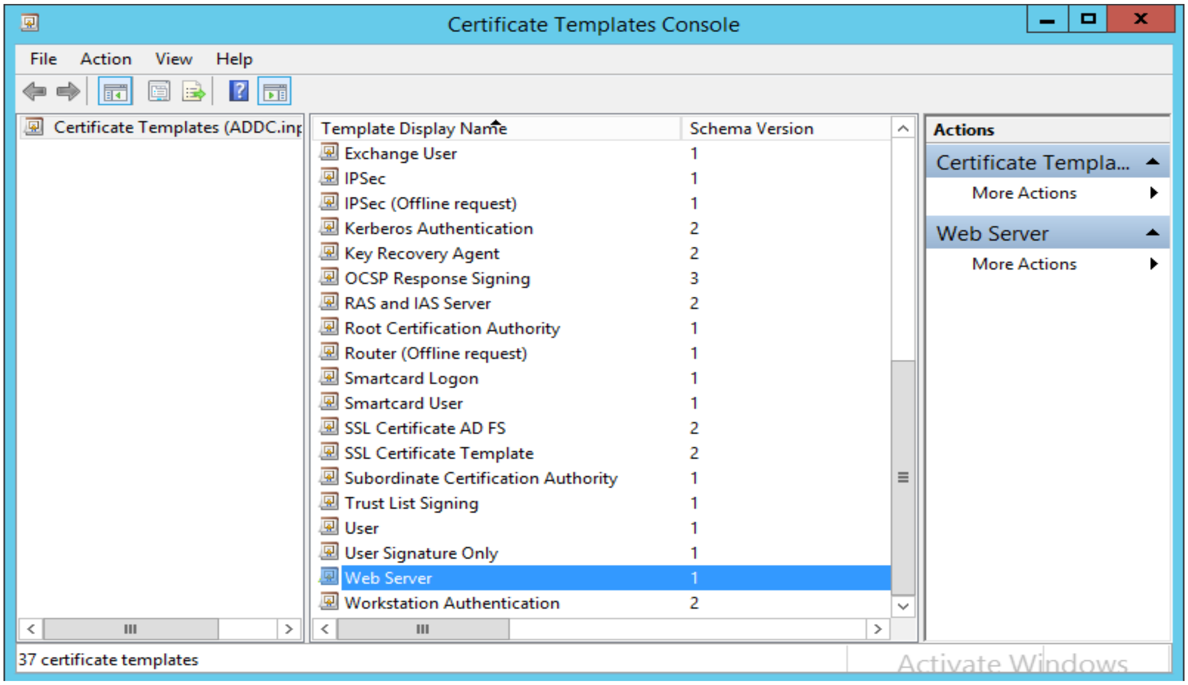
Generate Certificate for ADFS ‘ Computer

1. Open server manager ->Tool->Certification Authority



Name	Description
inpanya-CA2012-CA	Certification Authority

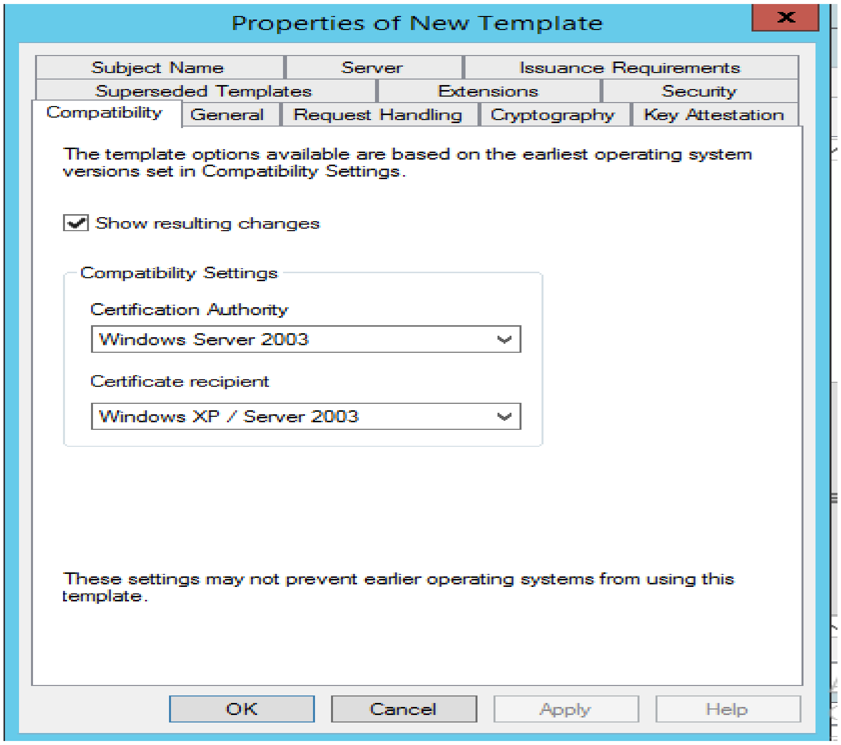
2. Right click Certificate Template -> Manage



Template Display Name	Schema Version
Exchange User	1
IPSec	1
IPSec (Offline request)	1
Kerberos Authentication	2
Key Recovery Agent	2
OCSP Response Signing	3
RAS and IAS Server	2
Root Certification Authority	1
Router (Offline request)	1
Smartcard Logon	1
Smartcard User	1
SSL Certificate AD FS	2
SSL Certificate Template	2
Subordinate Certification Authority	1
Trust List Signing	1
User	1
User Signature Only	1
Web Server	1
Workstation Authentication	2

37 certificate templates

3. Right click Web Server and select Duplicate Template



The template options available are based on the earliest operating system versions set in Compatibility Settings.

☑ Show resulting changes

Compatibility Settings

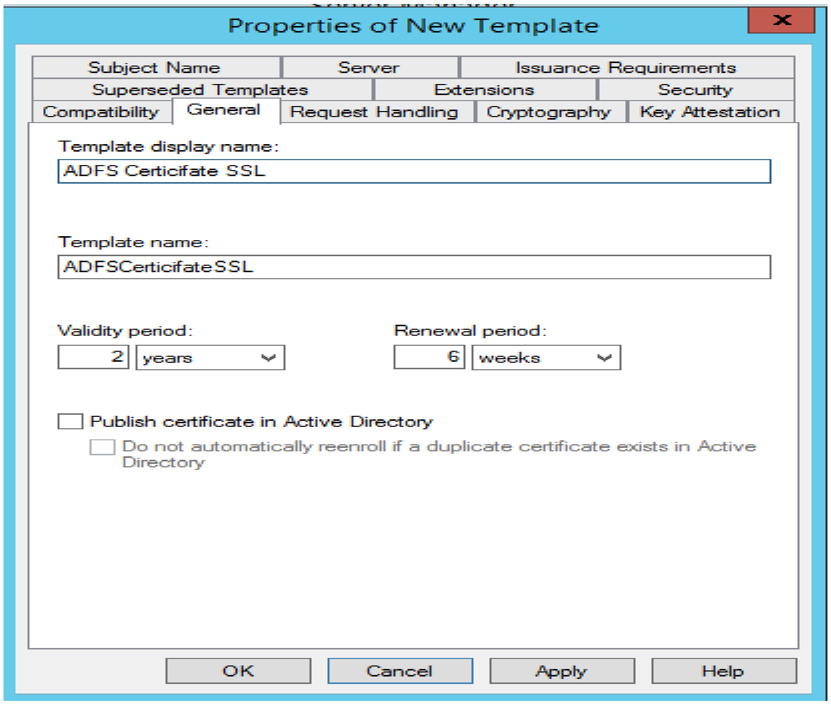
Certification Authority: Windows Server 2003

Certificate recipient: Windows XP / Server 2003

These settings may not prevent earlier operating systems from using this template.

On General tab->Template Display name

Enter: ADFS Certificate SSL



Template display name: ADFS Certicifate SSL

Template name: ADFSCerticifateSSL

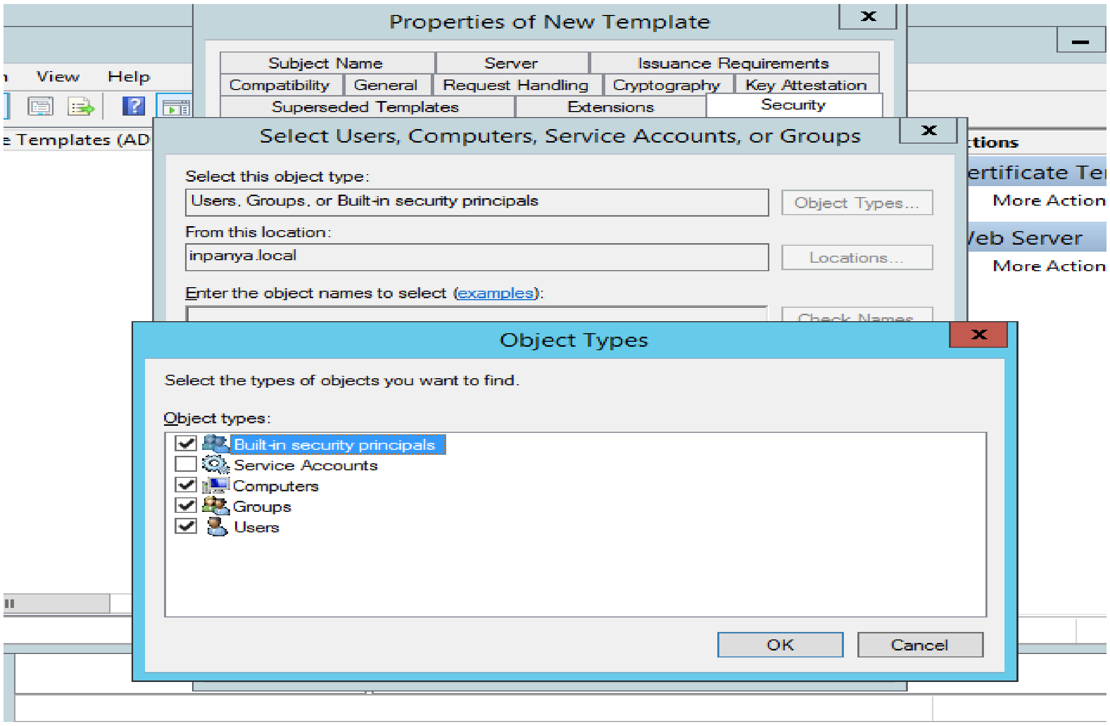
Validity period: 2 years

Renewal period: 6 weeks

□ Publish certificate in Active Directory

□ Do not automatically reenroll if a duplicate certificate exists in Active Directory

On Security tab click Add →click Object Type → checked Computers →click OK



Select Users, Computers, Service Accounts, or Groups

Select this object type:
Users, Groups, or Built-in security principals

From this location:
inpanya.local

Enter the object names to select (examples):

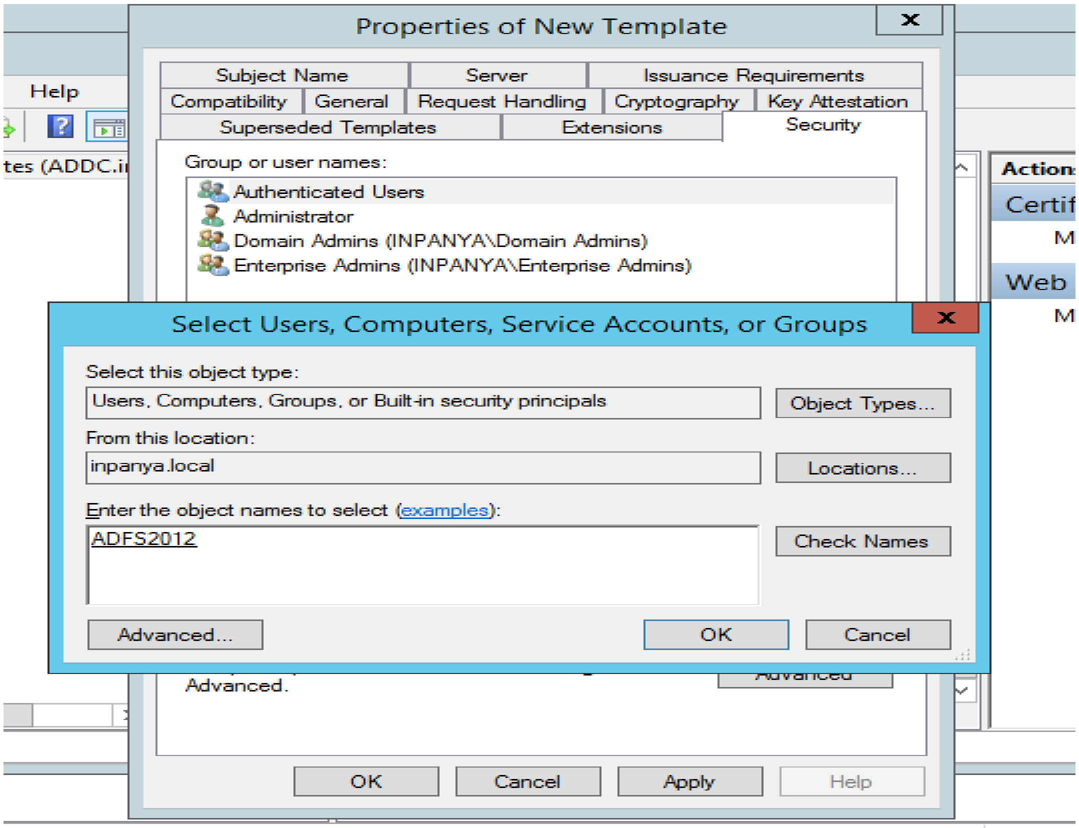
Object Types

Select the types of objects you want to find.

Object types:

- ☑ Built-in security principals
- ☐ Service Accounts
- ☑ Computers
- ☑ Groups
- ☑ Users

Enter computer name :ADFS2012 then click Check Names and click OK



Group or user names:

- Authenticated Users
- Administrator
- Domain Admins (INPANYA\Domain Admins)
- Enterprise Admins (INPANYA\Enterprise Admins)

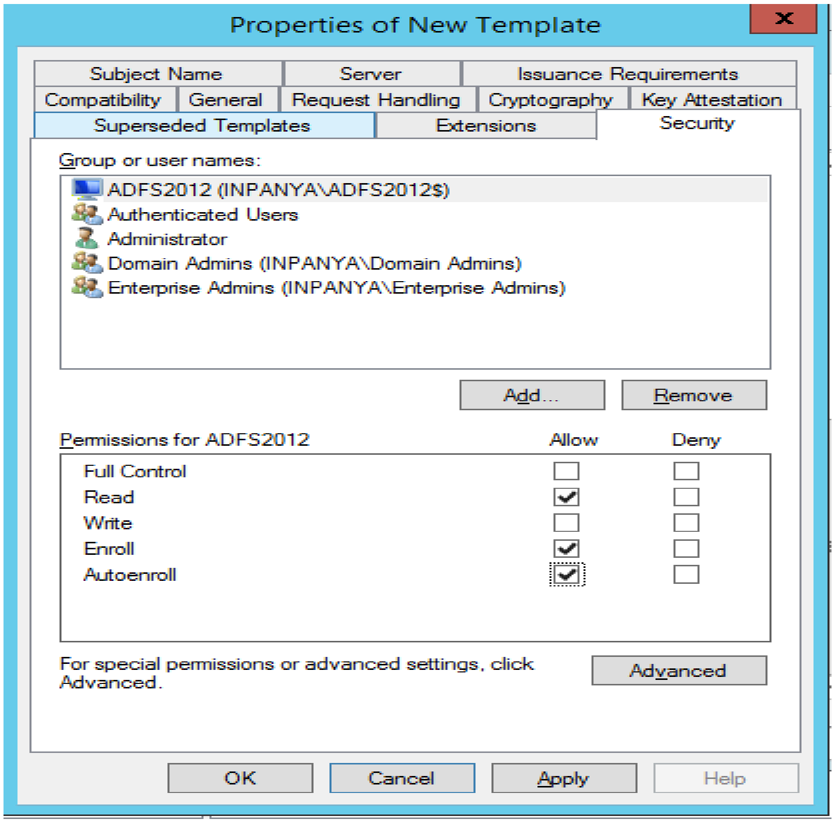
Select Users, Computers, Service Accounts, or Groups

Select this object type:
Users, Computers, Groups, or Built-in security principals

From this location:
inpanya.local

Enter the object names to select (examples):
ADFS2012

On the permissions for ADFS2012 checked Allow Read,Enroll,Autoenroll and then click OK

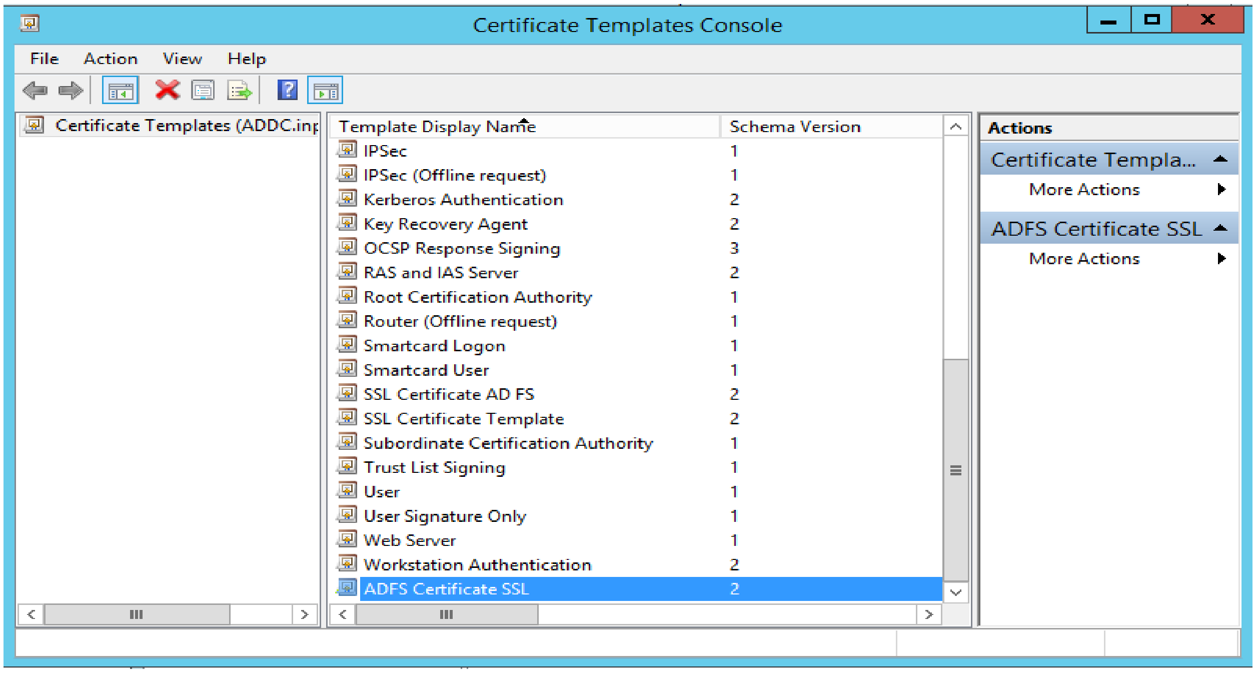


Group or user names:

- ADFS2012 (INPANYA\ADFS2012$)
- Authenticated Users
- Administrator
- Domain Admins (INPANYA\Domain Admins)
- Enterprise Admins (INPANYA\Enterprise Admins)

Permissions for ADFS2012	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	☑	□

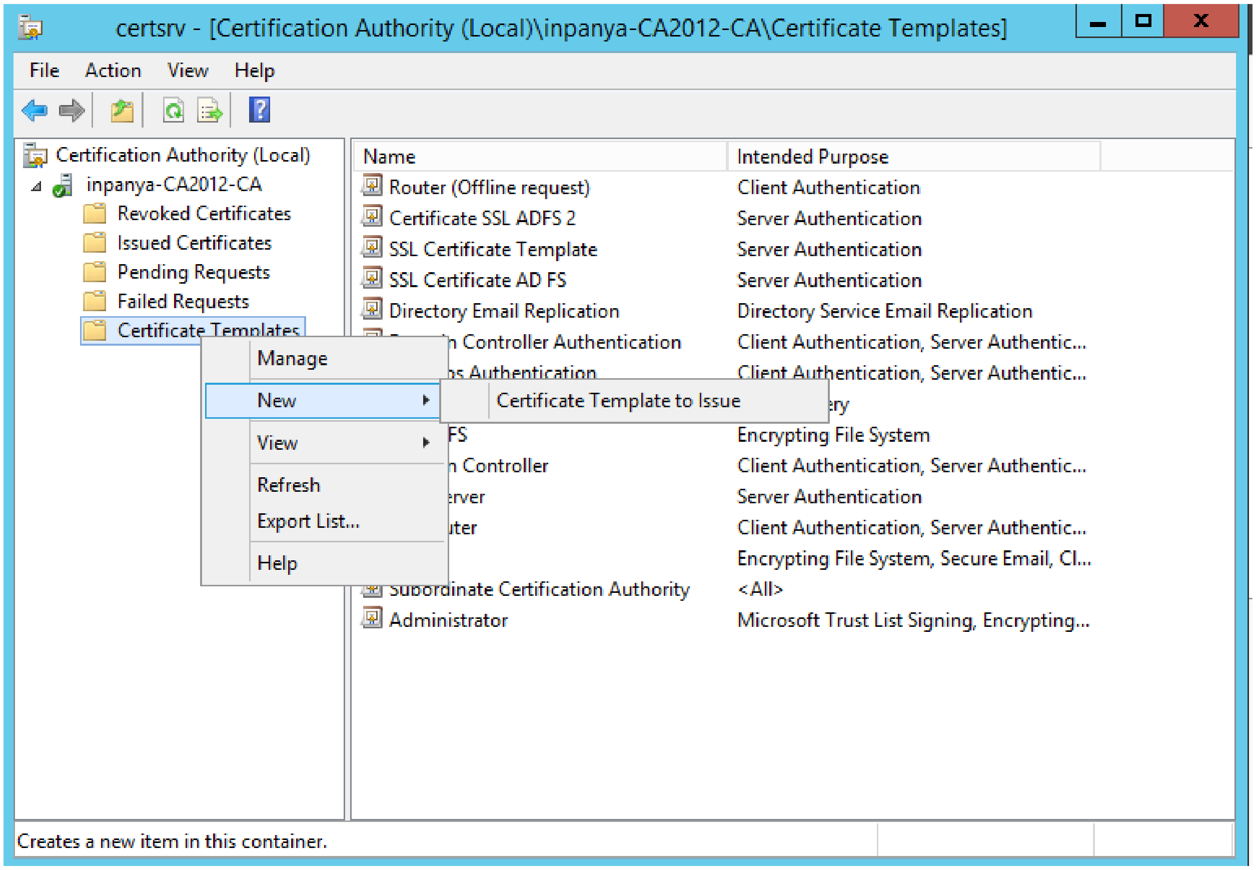
For special permissions or advanced settings, click Advanced.



Template Display Name	Schema Version
IPSec	1
IPSec (Offline request)	1
Kerberos Authentication	2
Key Recovery Agent	2
OCSP Response Signing	3
RAS and IAS Server	2
Root Certification Authority	1
Router (Offline request)	1
Smartcard Logon	1
Smartcard User	1
SSL Certificate AD FS	2
SSL Certificate Template	2
Subordinate Certification Authority	1
Trust List Signing	1
User	1
User Signature Only	1
Web Server	1
Workstation Authentication	2
ADFS Certificate SSL	2

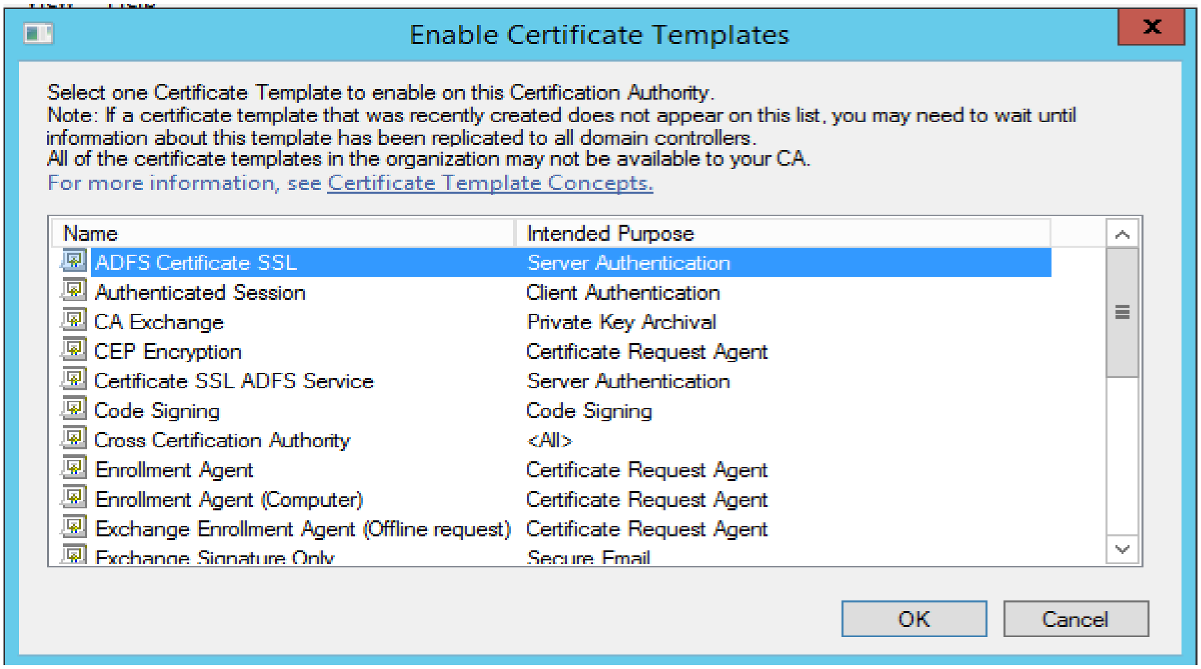
And close Certificate Template Console

Back to certsrv console right click Certificate Templates ->New ->Certificate Template to Issue



Name	Intended Purpose
Router (Offline request)	Client Authentication
Certificate SSL ADFS 2	Server Authentication
SSL Certificate Template	Server Authentication
SSL Certificate AD FS	Server Authentication
Directory Email Replication	Directory Service Email Replication
n Controller Authentication	Client Authentication, Server Authentic...
s Authentication	Client Authentication, Server Authentic...
	ry
FS	Encrypting File System
n Controller	Client Authentication, Server Authentic...
rver	Server Authentication
ter	Client Authentication, Server Authentic...
	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting...

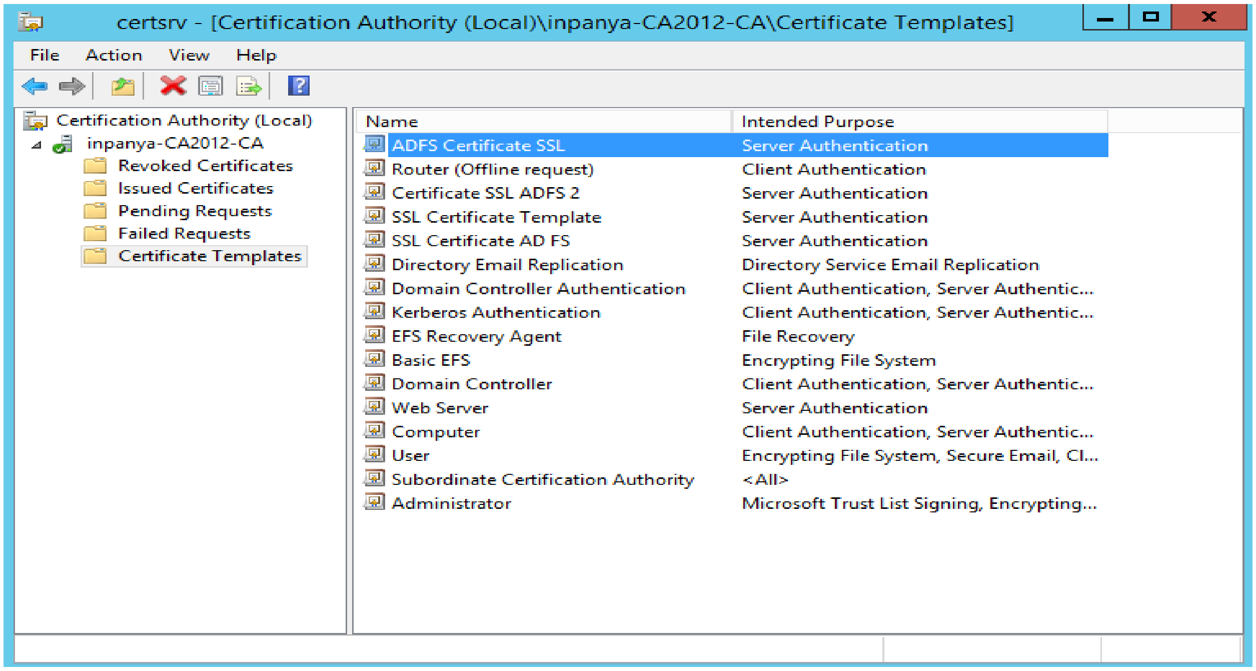
Creates a new item in this container.



Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

Name	Intended Purpose
ADFS Certificate SSL	Server Authentication
Authenticated Session	Client Authentication
CA Exchange	Private Key Archival
CEP Encryption	Certificate Request Agent
Certificate SSL ADFS Service	Server Authentication
Code Signing	Code Signing
Cross Certification Authority	<All>
Enrollment Agent	Certificate Request Agent
Enrollment Agent (Computer)	Certificate Request Agent
Exchange Enrollment Agent (Offline request)	Certificate Request Agent
Exchange Signature Only	Secure Email

Select ADFS Certificate SSL then click OK.

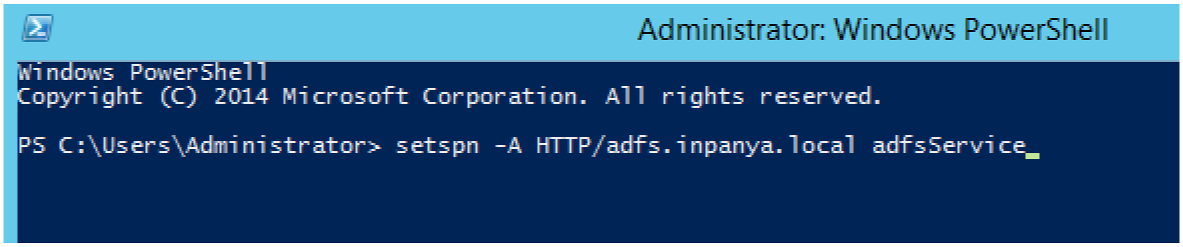


Name	Intended Purpose
ADFS Certificate SSL	Server Authentication
Router (Offline request)	Client Authentication
Certificate SSL ADFS 2	Server Authentication
SSL Certificate Template	Server Authentication
SSL Certificate AD FS	Server Authentication
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting...

Domain controller configuration

Create User for ADFS Service account on Domain Controller : adfsService

Set SPN for adfsService

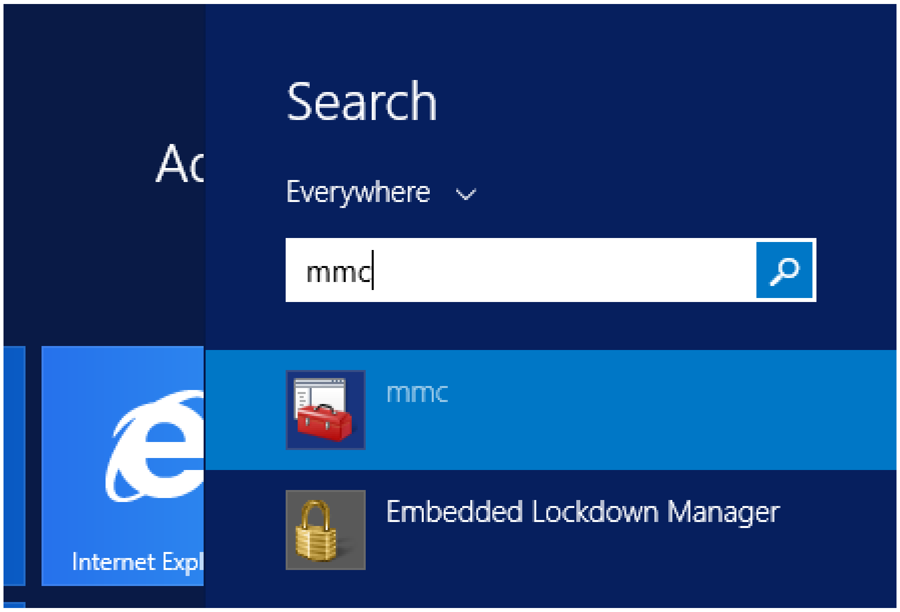


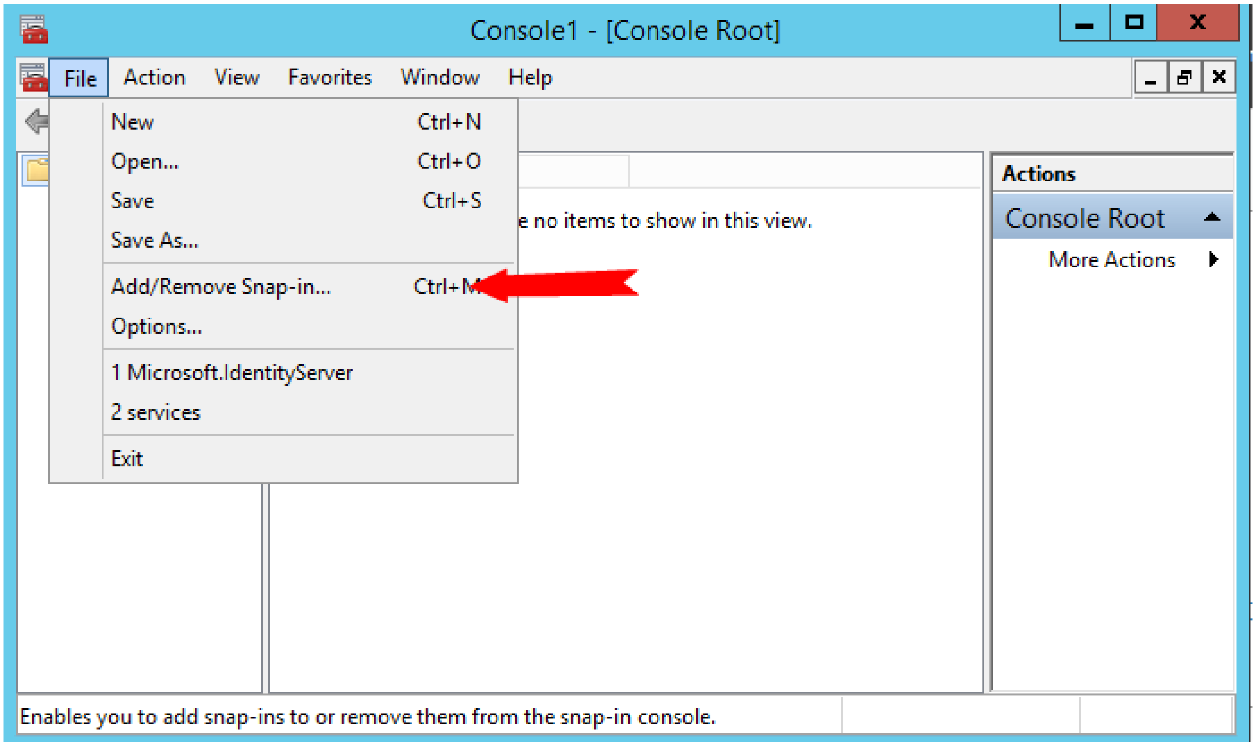
```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> setspn -A HTTP/adfs.inpanya.local adfsService
```

ADFS Configuration

Import certificate to ADFS Server

Execute mmc

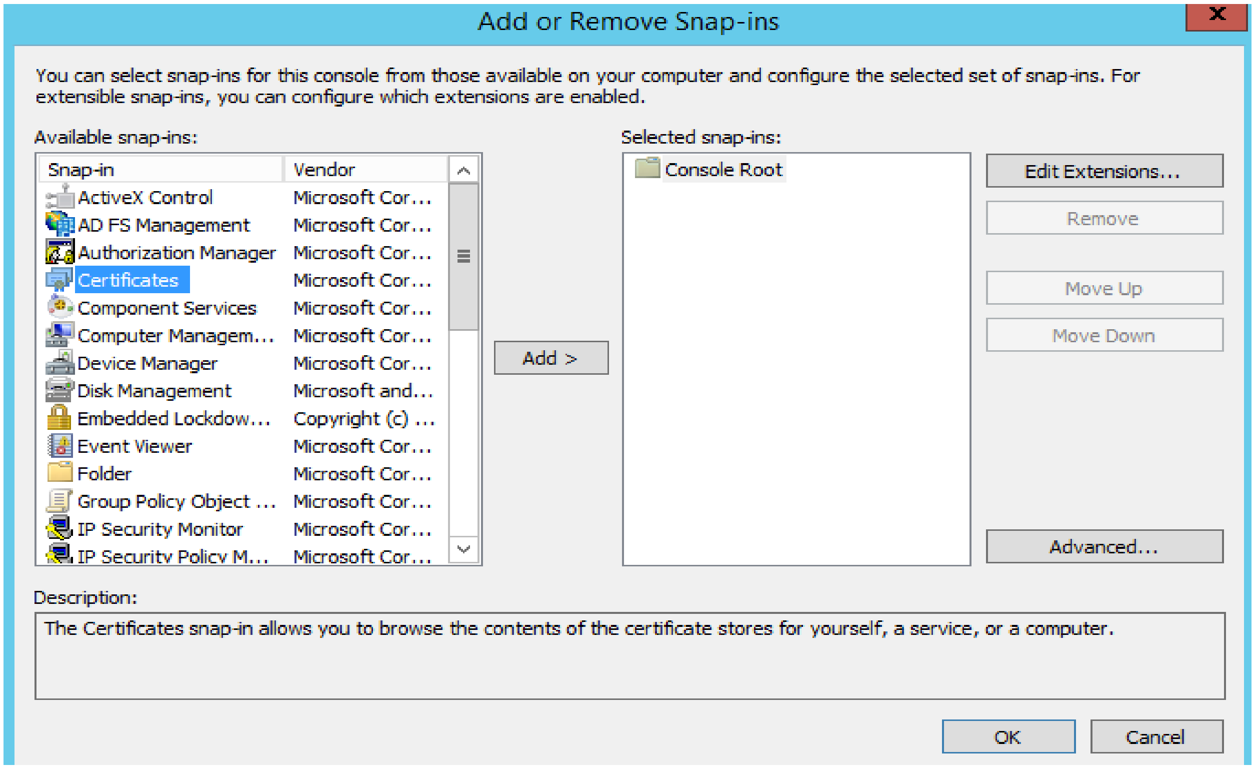




e no items to show in this view.

Enables you to add snap-ins to or remove them from the snap-in console.

Click File ->Add/Remove Snap-in

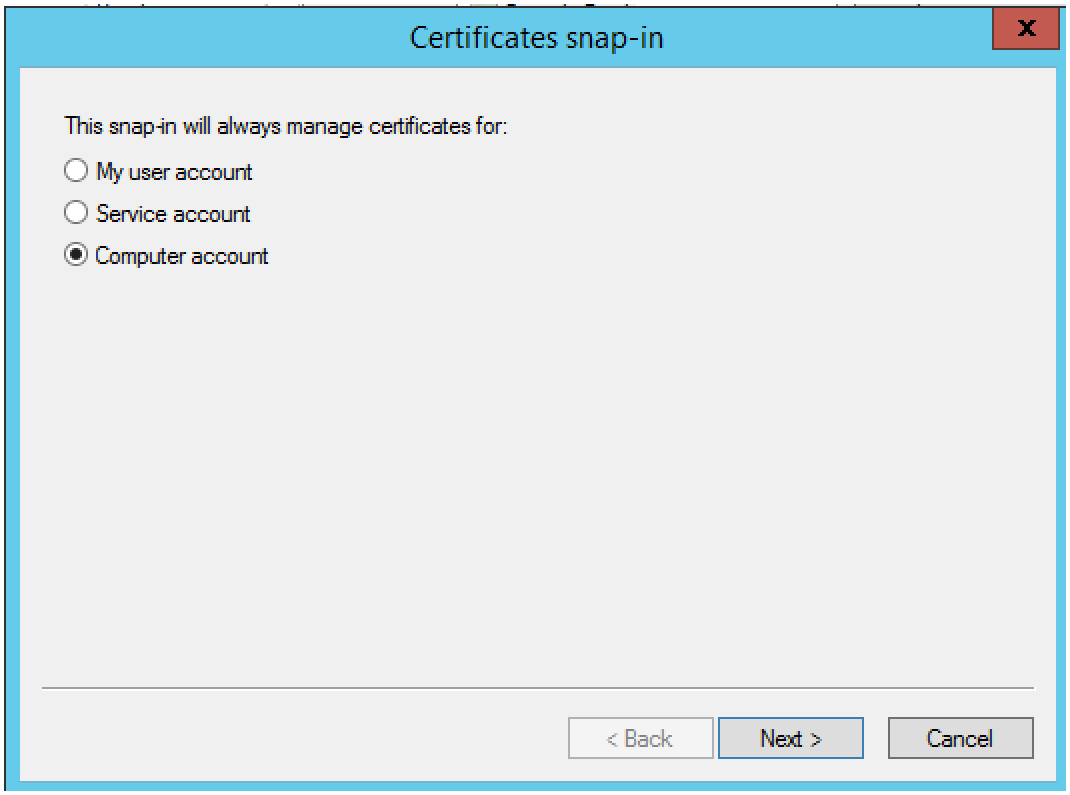


You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
AD FS Management	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Embedded Lockdow...	Copyright (c) ...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

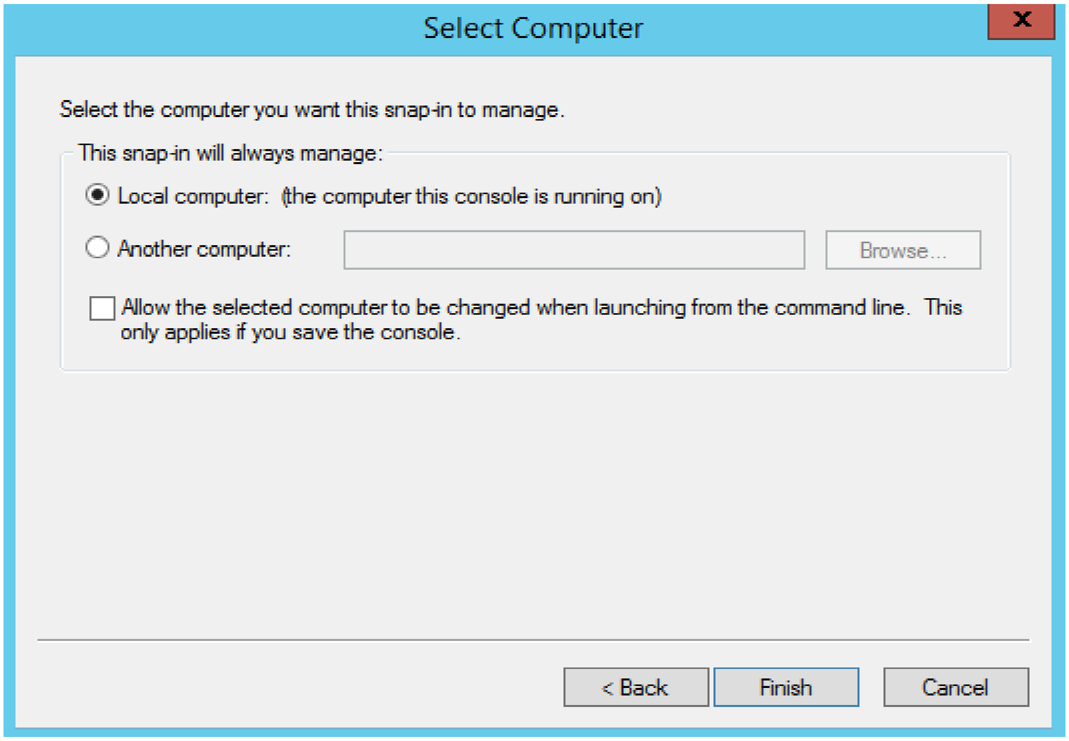
Select Certificates and click Add



This snap-in will always manage certificates for:

○ My user account
○ Service account
● Computer account

Select Computer account the click Next



Select Computer

Select the computer you want this snap-in to manage.

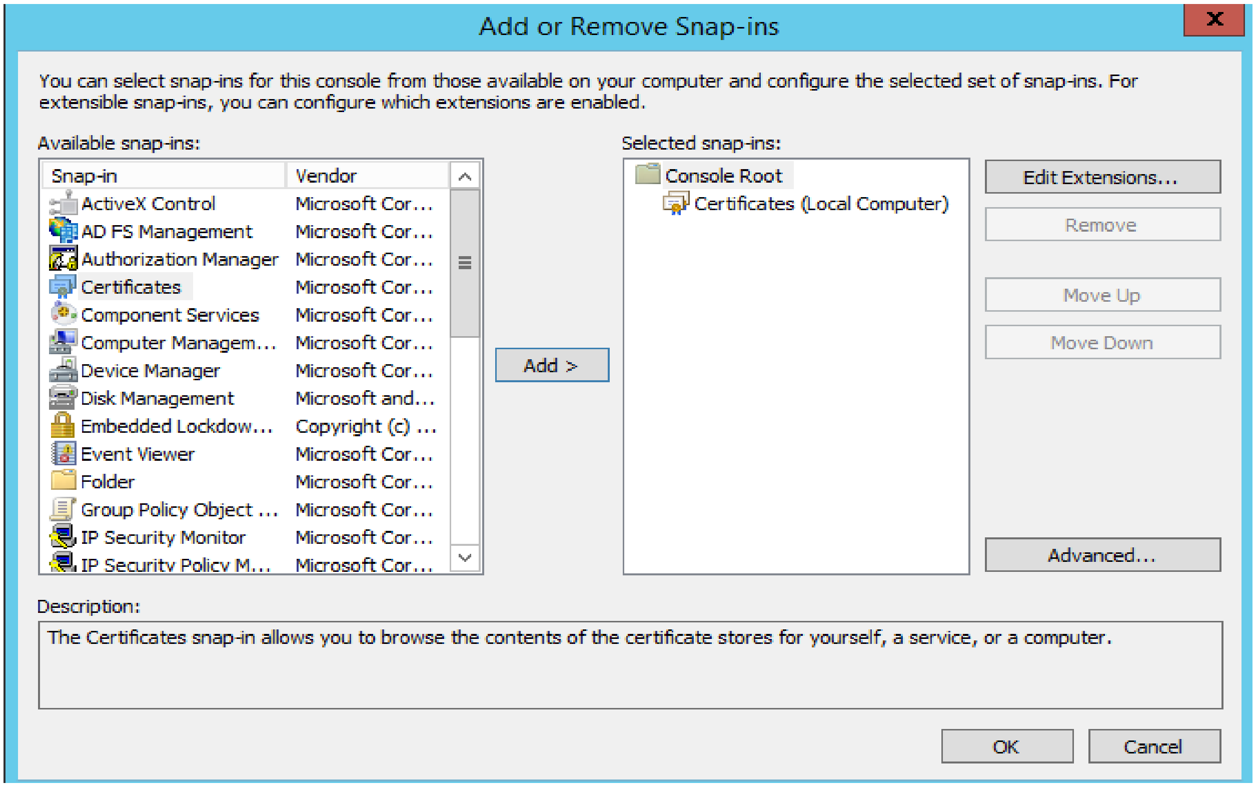
This snap-in will always manage:

● Local computer: (the computer this console is running on)

○ Another computer:

☐ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

Select Local computer then click Finish



Add or Remove Snap-ins

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

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
AD FS Management	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Embedded Lockdow...	Copyright (c) ...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...

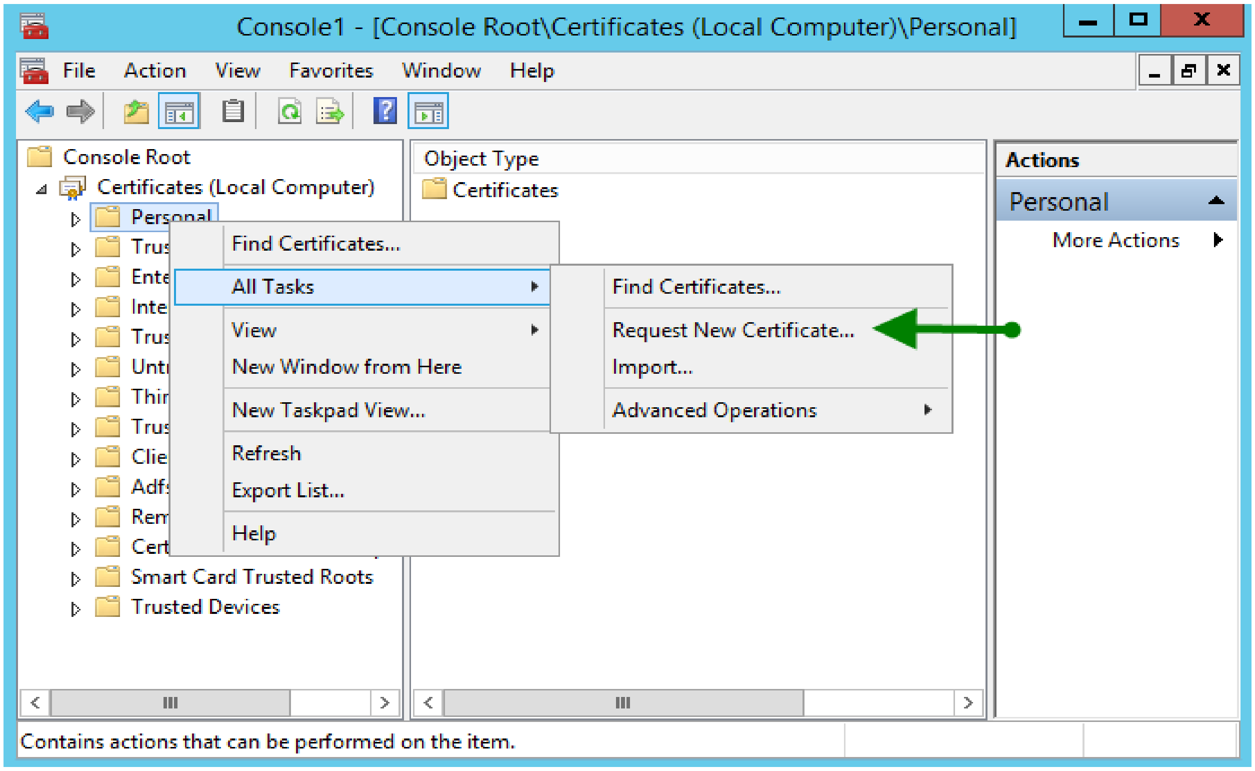
Selected snap-ins:

Console Root
Certificates (Local Computer)

Description:

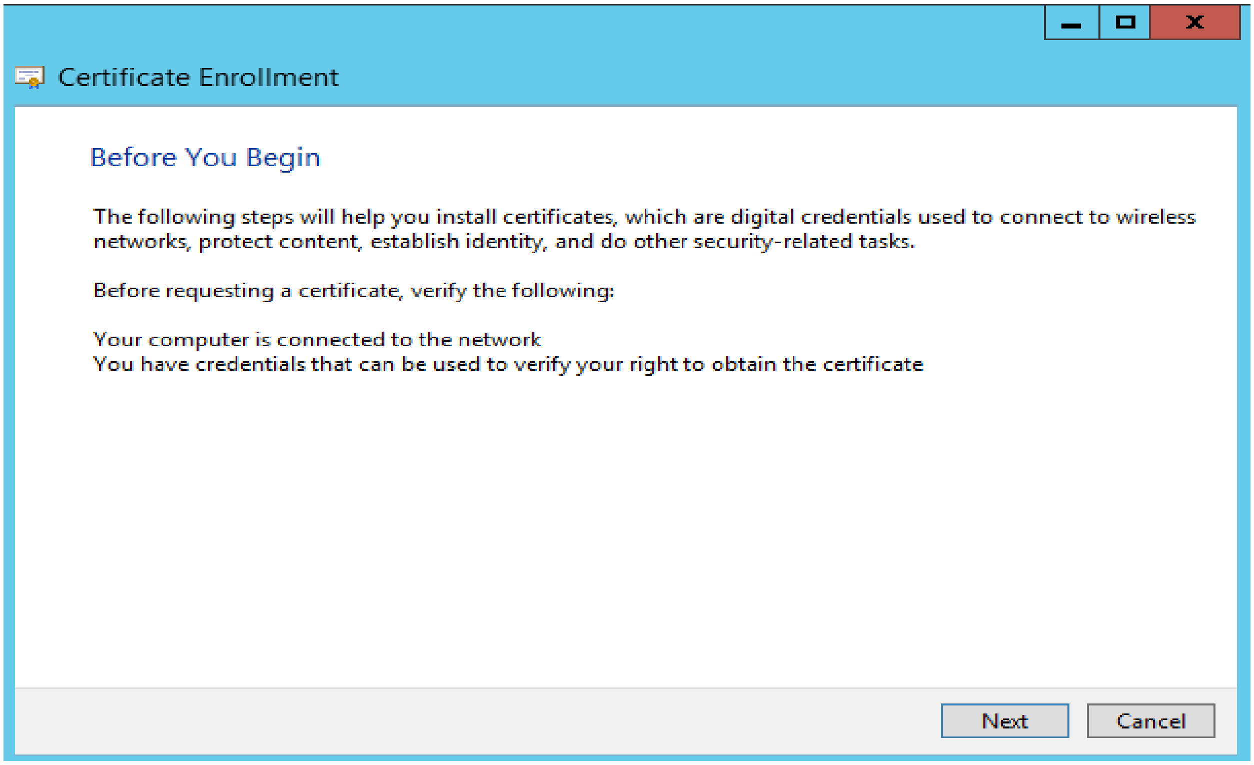
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Click OK



Contains actions that can be performed on the item.

Personal →All Tasks →Request New Certificate


Certificate Enrollment

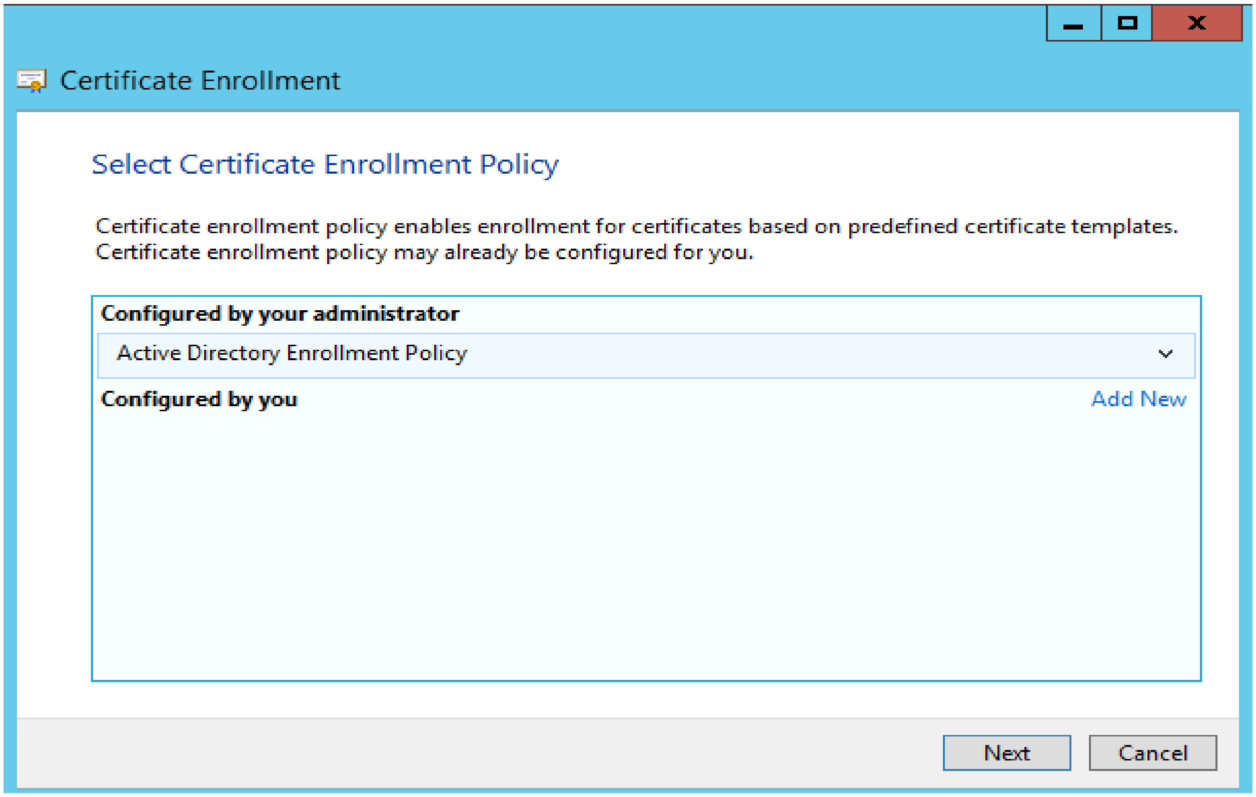
Before You Begin

The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.

Before requesting a certificate, verify the following:

Your computer is connected to the network
You have credentials that can be used to verify your right to obtain the certificate

Click Next



Certificate Enrollment

Select Certificate Enrollment Policy

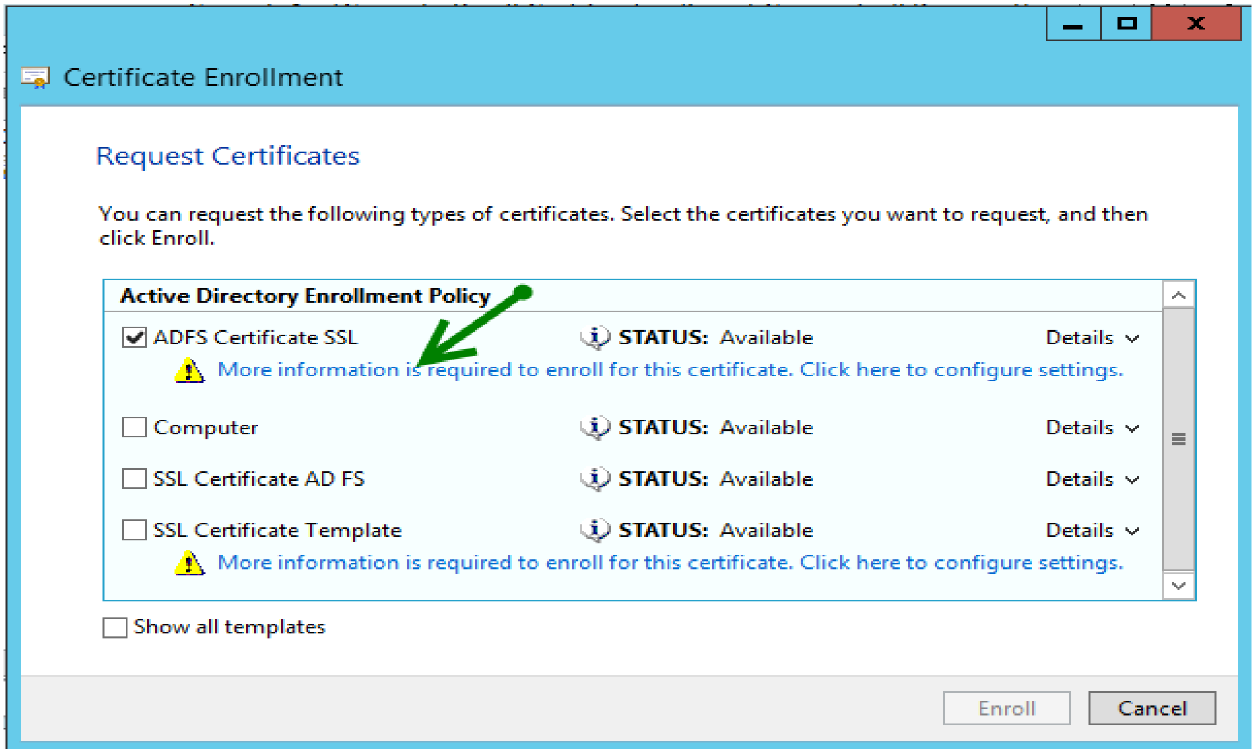
Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by your administrator

Active Directory Enrollment Policy

Configured by you

Click Next



Certificate Enrollment

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

Active Directory Enrollment Policy

☑ ADFS Certificate SSL **STATUS:** Available Details

More information is required to enroll for this certificate. Click here to configure settings.

□ Computer **STATUS:** Available Details

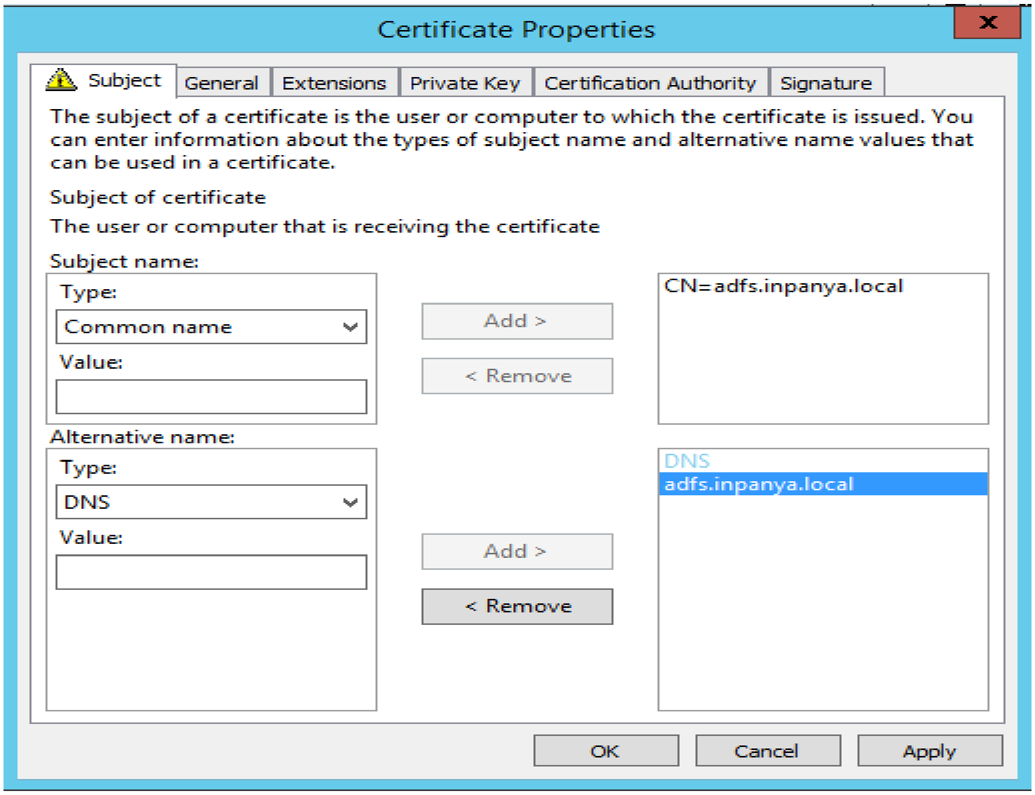
□ SSL Certificate AD FS **STATUS:** Available Details

□ SSL Certificate Template **STATUS:** Available Details

More information is required to enroll for this certificate. Click here to configure settings.

□ Show all templates

Select ADFS Certificate SSL and click link More information is required to enroll for this certificate.



The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate

The user or computer that is receiving the certificate

Subject name:

Type: Common name

Value:

CN=adfs.inpanya.local

Alternative name:

Type: DNS

Value:

DNS

adfs.inpanya.local

In Subject name section

Type: Common name

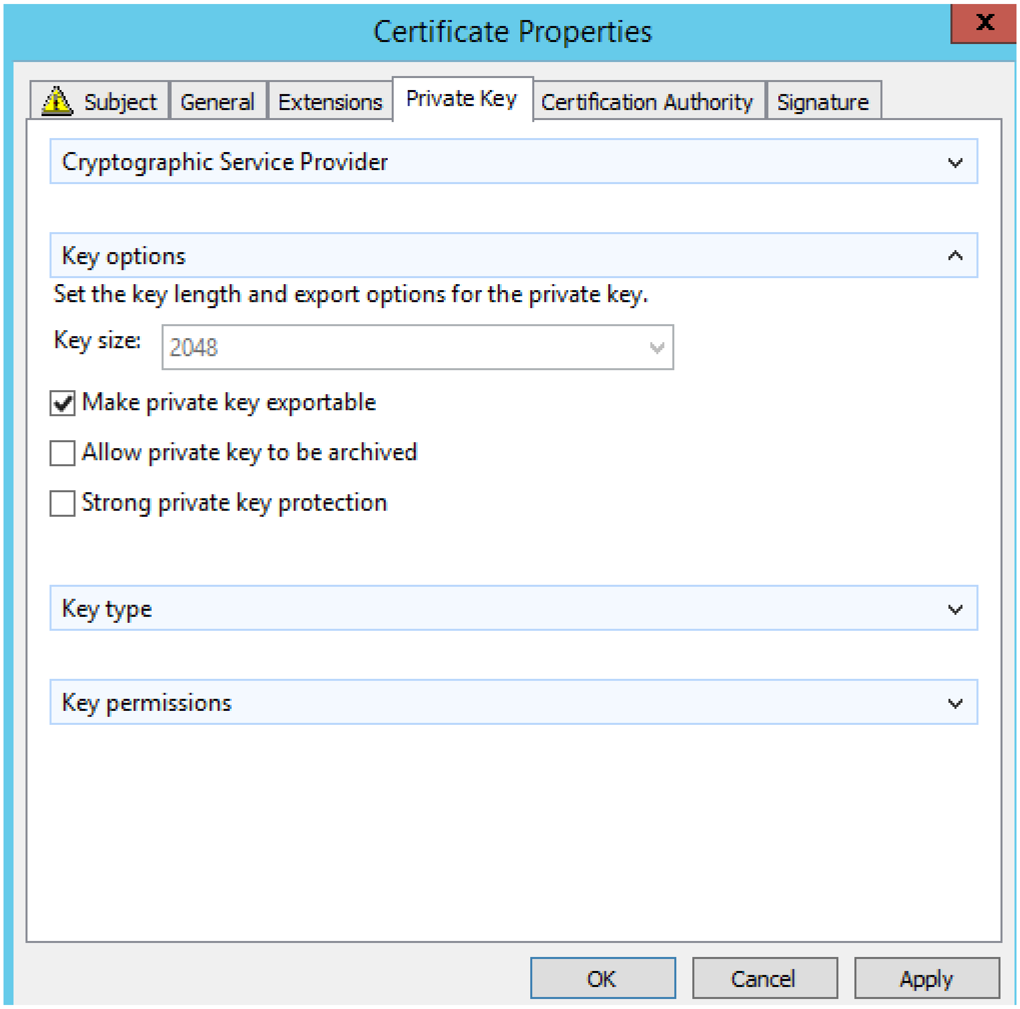
Value:adfs.inpanya.local

Click Add

In Alternative name

Type: DNS

Value:adfs.inpanya.local



Cryptographic Service Provider

Key options

Set the key length and export options for the private key.

Key size: 2048

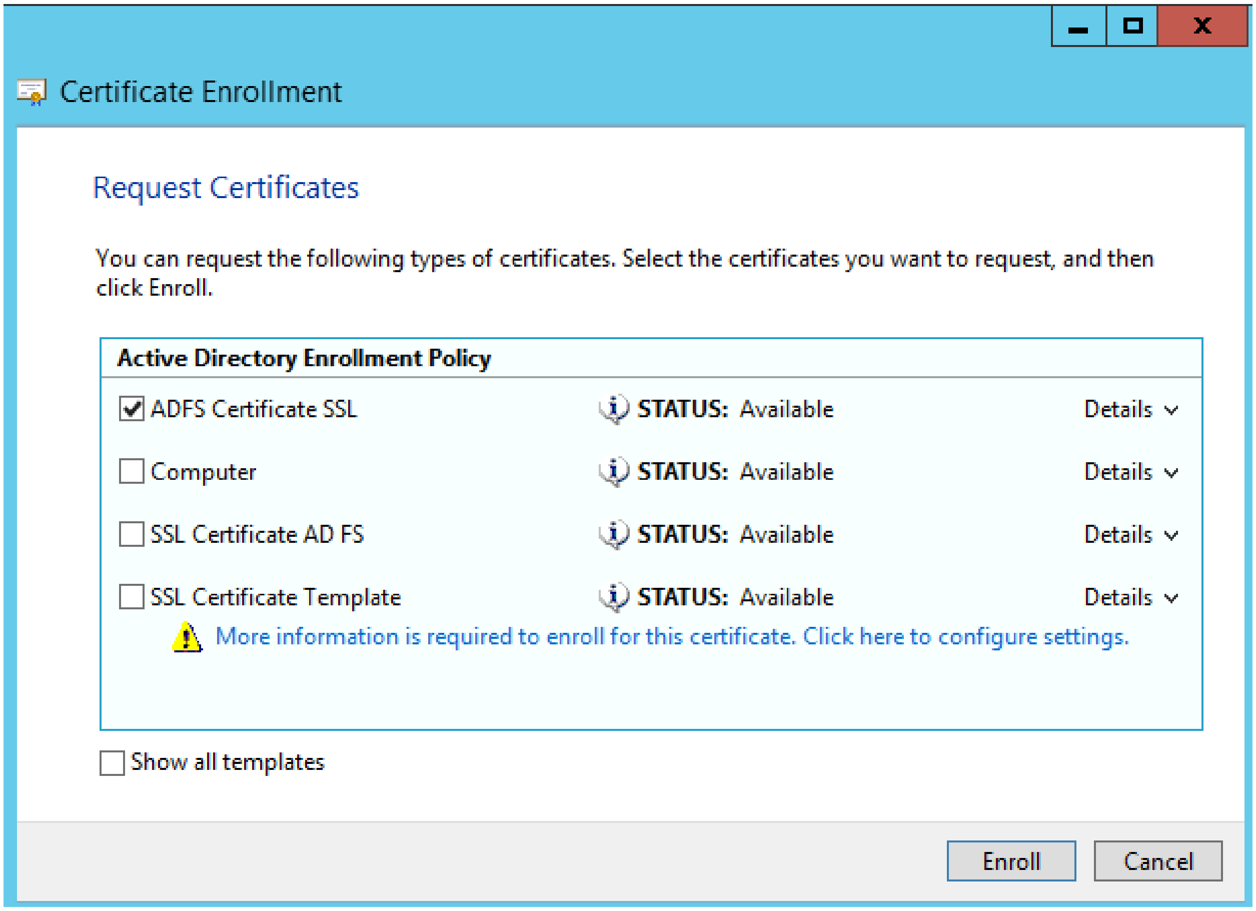
☑ Make private key exportable

□ Allow private key to be archived

□ Strong private key protection

Key type

Key permissions



Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

Active Directory Enrollment Policy

☑ ADFS Certificate SSL — **STATUS:** Available — Details

□ Computer — **STATUS:** Available — Details

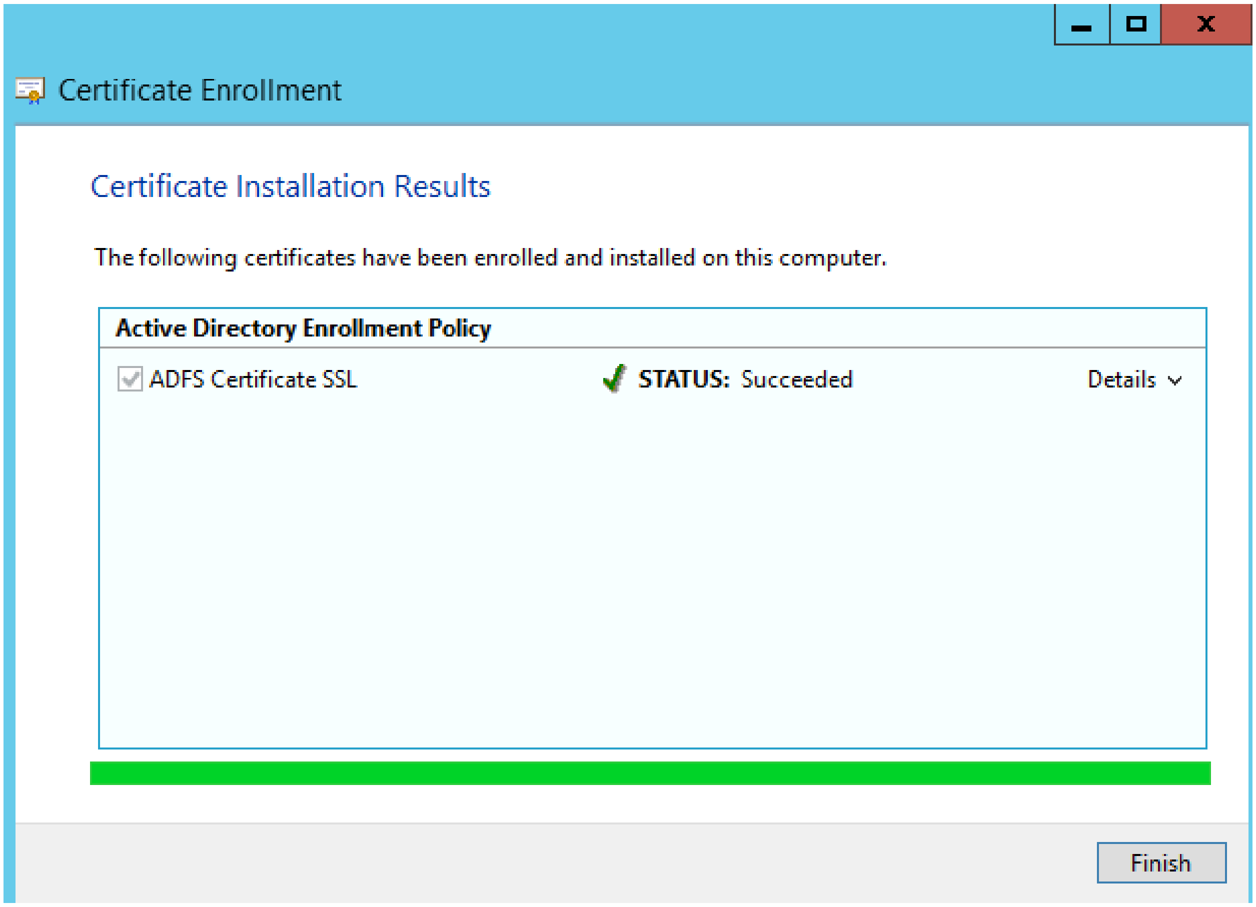
□ SSL Certificate AD FS — **STATUS:** Available — Details

□ SSL Certificate Template — **STATUS:** Available — Details

⚠ More information is required to enroll for this certificate. Click here to configure settings.

□ Show all templates

Click Enroll



Certificate Installation Results

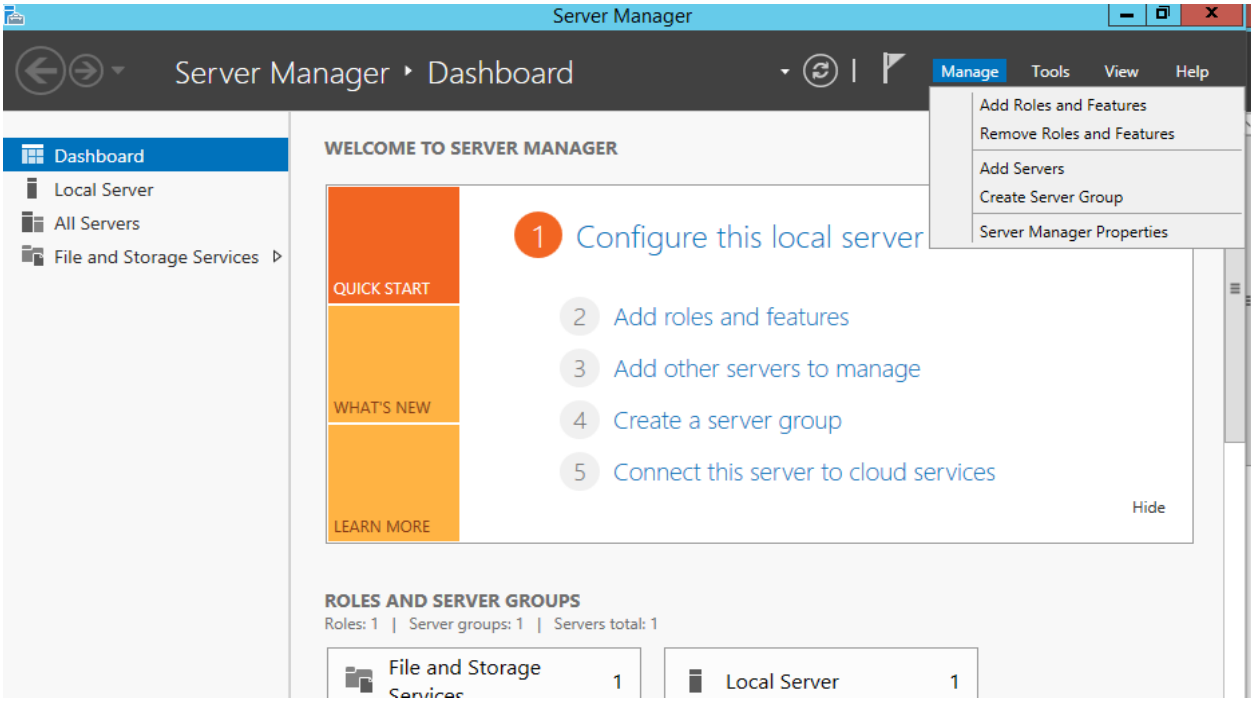
The following certificates have been enrolled and installed on this computer.

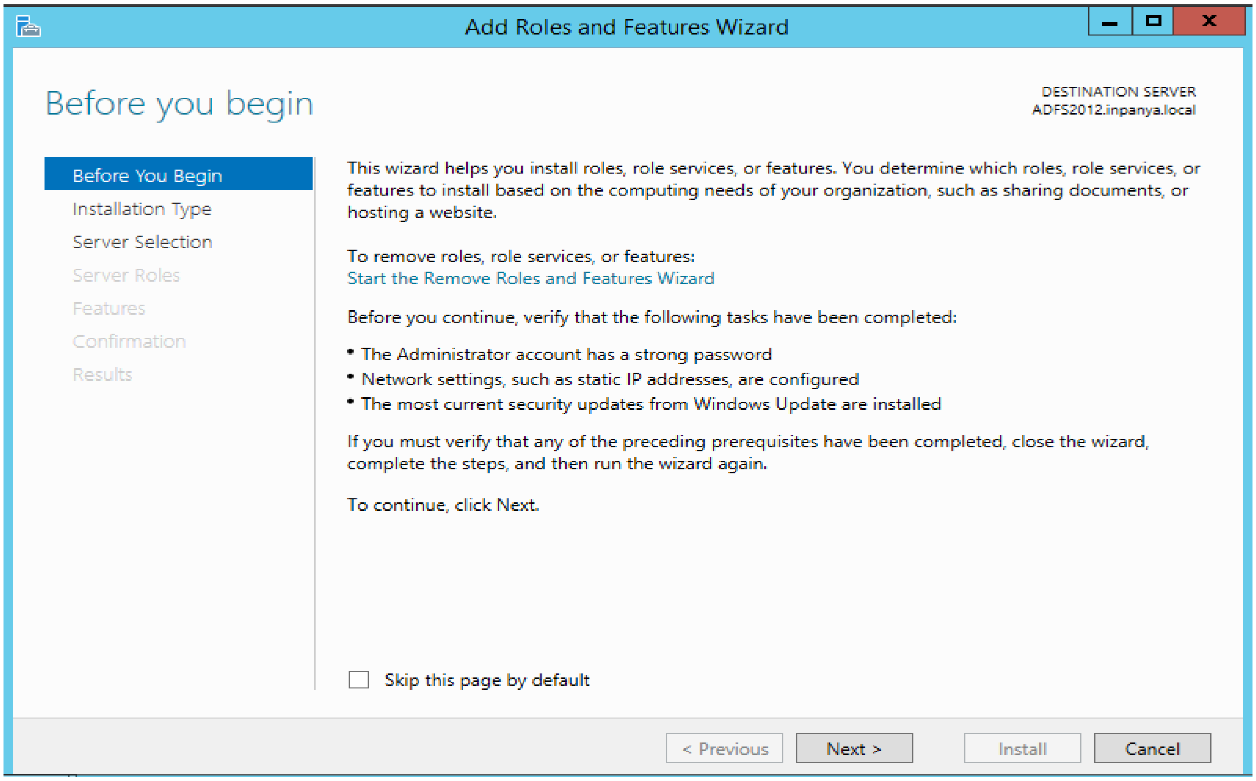
Active Directory Enrollment Policy

☑ ADFS Certificate SSL ✓ **STATUS:** Succeeded

Click Finish and close MMC

On the Server Manager click Manage ->Add Roles and Feature


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Add Roles and Features
Remove Roles and Features
Add Servers
Create Server Group
Server Manager Properties
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Local Server 1



This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

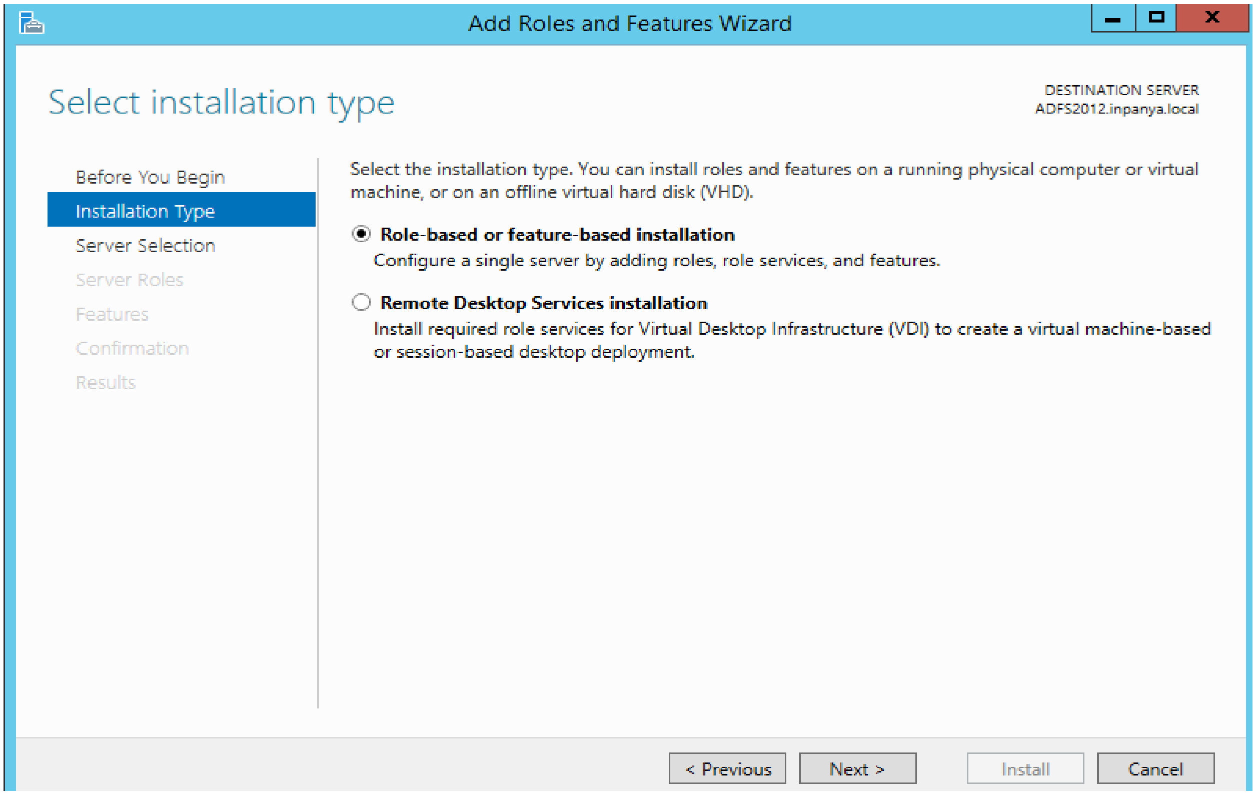
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

Click Next



Add Roles and Features Wizard

Select installation type

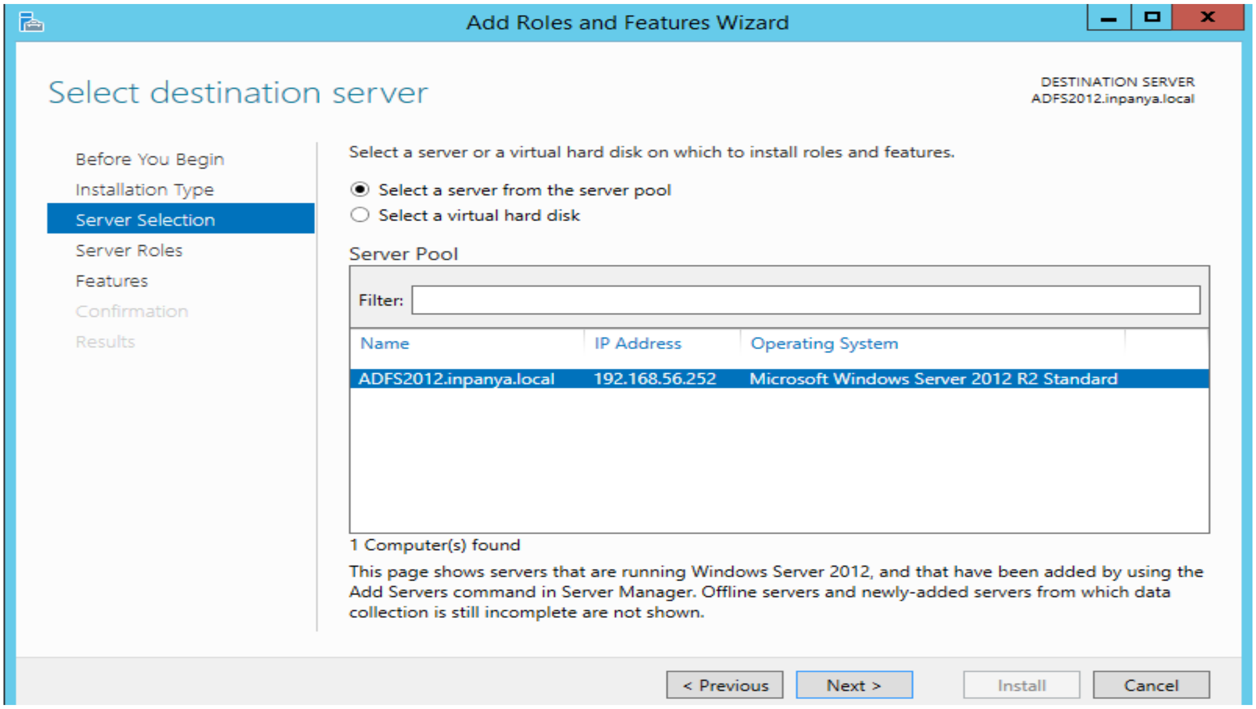
DESTINATION SERVER
ADFS2012.inpanya.local

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

Select Role-based or feature-based installation the click Next



Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
ADFS2012.inpanya.local

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

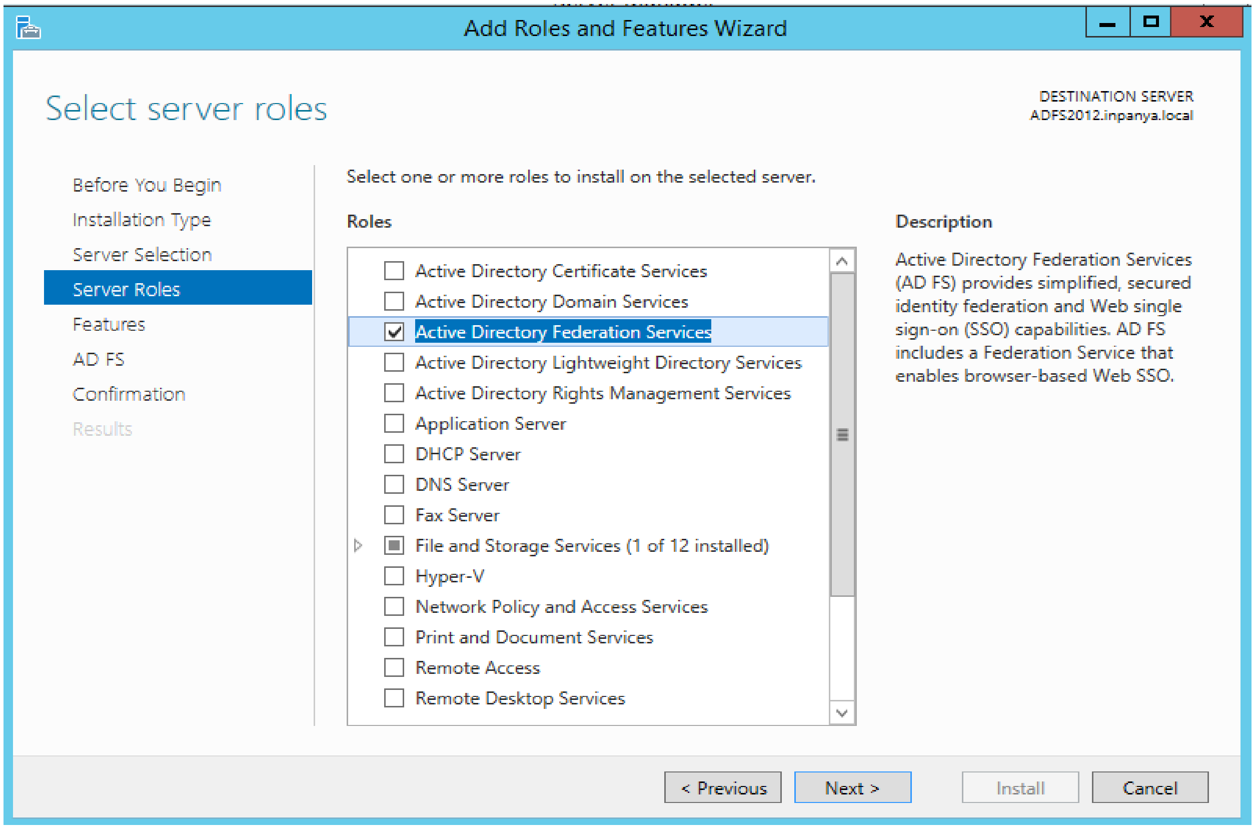
Filter:

Name	IP Address	Operating System
ADFS2012.inpanya.local	192.168.56.252	Microsoft Windows Server 2012 R2 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

Click Next



Select server roles

DESTINATION SERVER
ADFS2012.inpanya.local

Select one or more roles to install on the selected server.

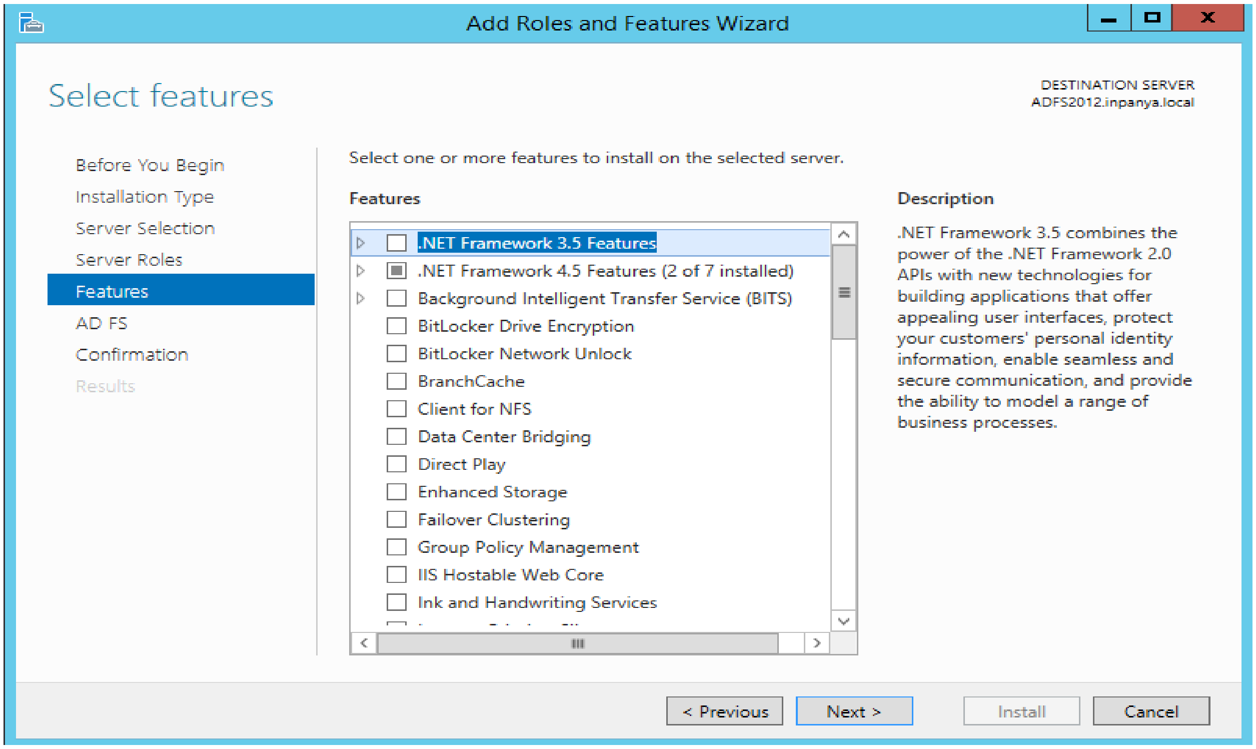
Roles

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☑ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ▣ File and Storage Services (1 of 12 installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services

Description

Active Directory Federation Services (AD FS) provides simplified, secured identity federation and Web single sign-on (SSO) capabilities. AD FS includes a Federation Service that enables browser-based Web SSO.

Checked Active Directory Federation Services then click Next



Select features

DESTINATION SERVER
ADFS2012.inpanya.local

Select one or more features to install on the selected server.

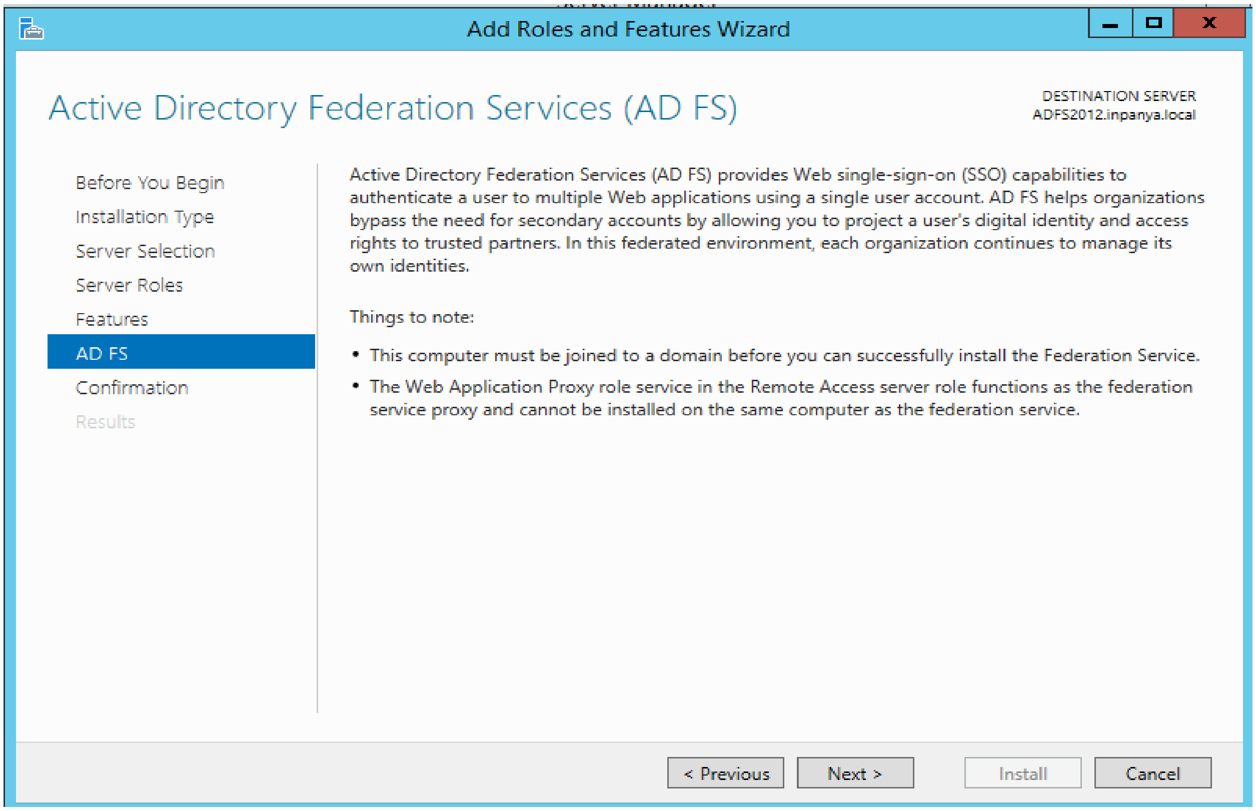
Features

- ☐ .NET Framework 3.5 Features
- ▣ .NET Framework 4.5 Features (2 of 7 installed)
- ☐ Background Intelligent Transfer Service (BITS)
- ☐ BitLocker Drive Encryption
- ☐ BitLocker Network Unlock
- ☐ BranchCache
- ☐ Client for NFS
- ☐ Data Center Bridging
- ☐ Direct Play
- ☐ Enhanced Storage
- ☐ Failover Clustering
- ☐ Group Policy Management
- ☐ IIS Hostable Web Core
- ☐ Ink and Handwriting Services

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

Click Next



Active Directory Federation Services (AD FS)

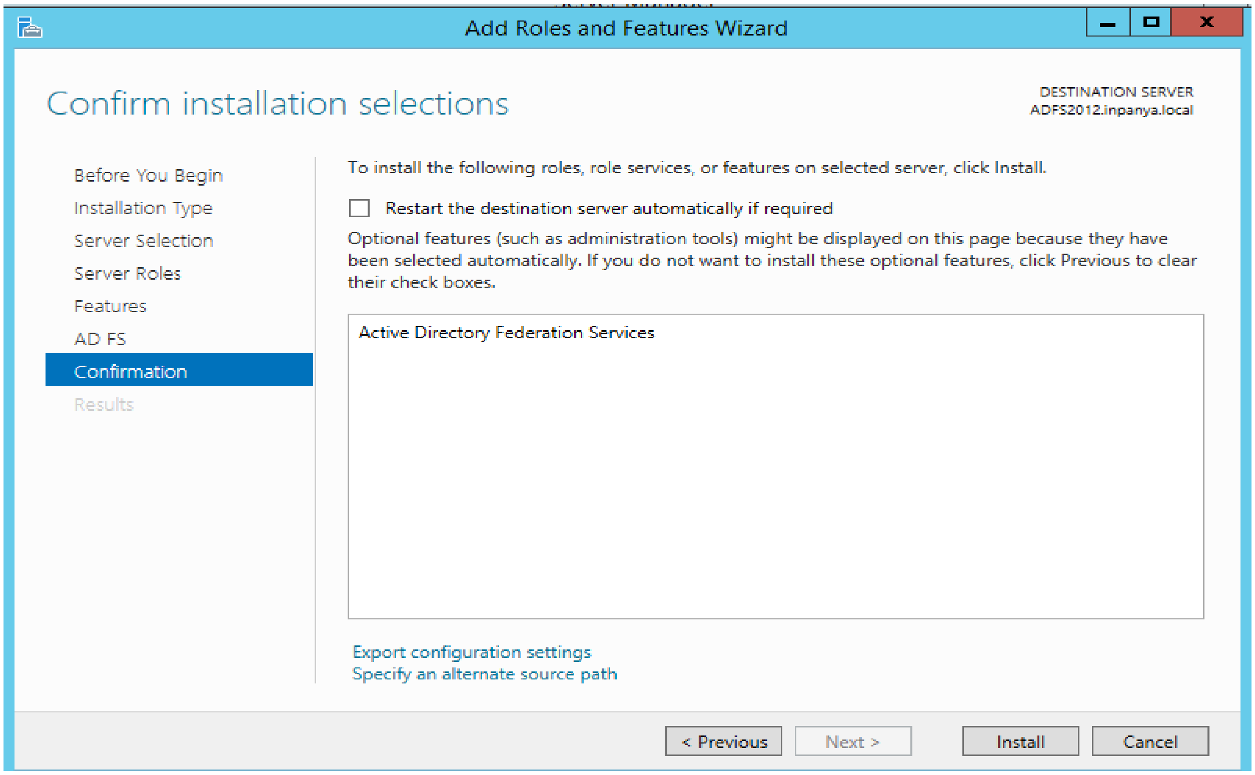
DESTINATION SERVER
ADFS2012.inpanya.local

Active Directory Federation Services (AD FS) provides Web single-sign-on (SSO) capabilities to authenticate a user to multiple Web applications using a single user account. AD FS helps organizations bypass the need for secondary accounts by allowing you to project a user's digital identity and access rights to trusted partners. In this federated environment, each organization continues to manage its own identities.

Things to note:

- This computer must be joined to a domain before you can successfully install the Federation Service.
- The Web Application Proxy role service in the Remote Access server role functions as the federation service proxy and cannot be installed on the same computer as the federation service.

Click Next



Confirm installation selections

DESTINATION SERVER
ADFS2012.inpanya.local

To install the following roles, role services, or features on selected server, click Install.

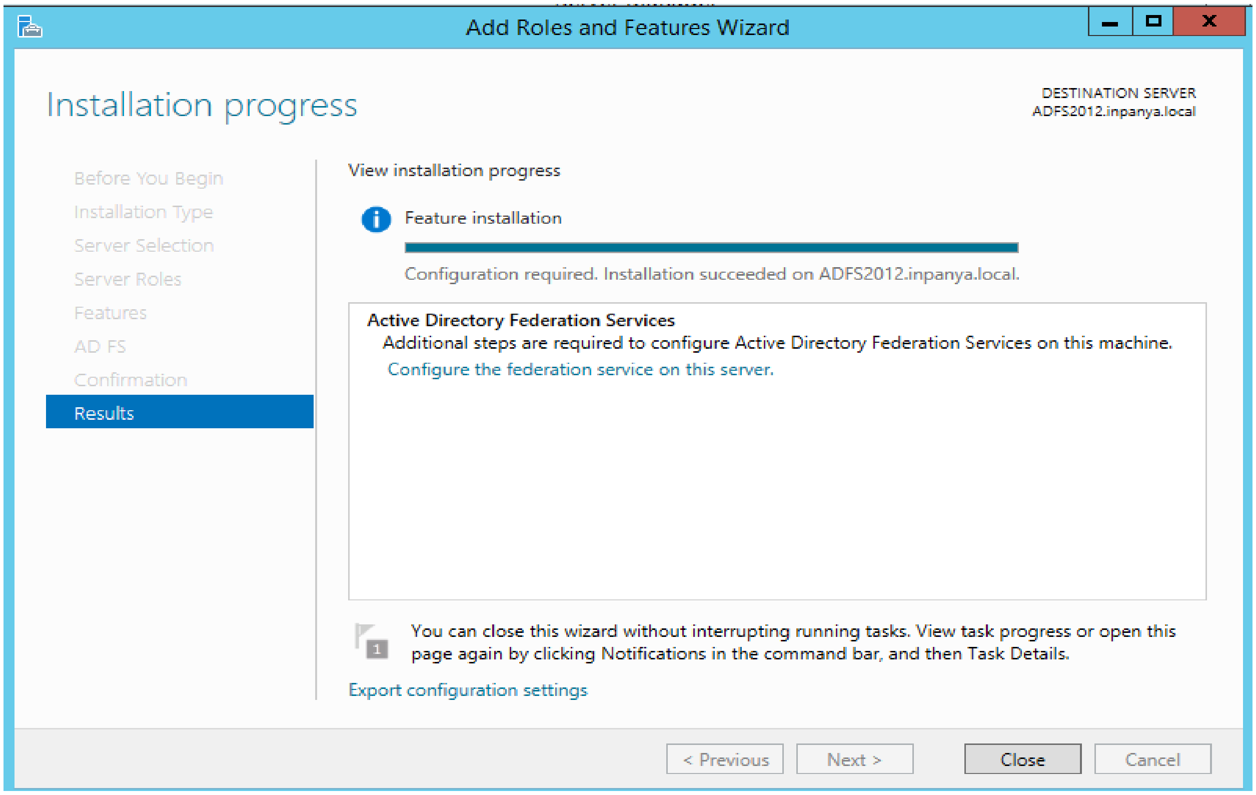
☐ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Federation Services

Export configuration settings
Specify an alternate source path

Click Install



Installation progress

DESTINATION SERVER
ADFS2012.inpanya.local

View installation progress

Feature installation

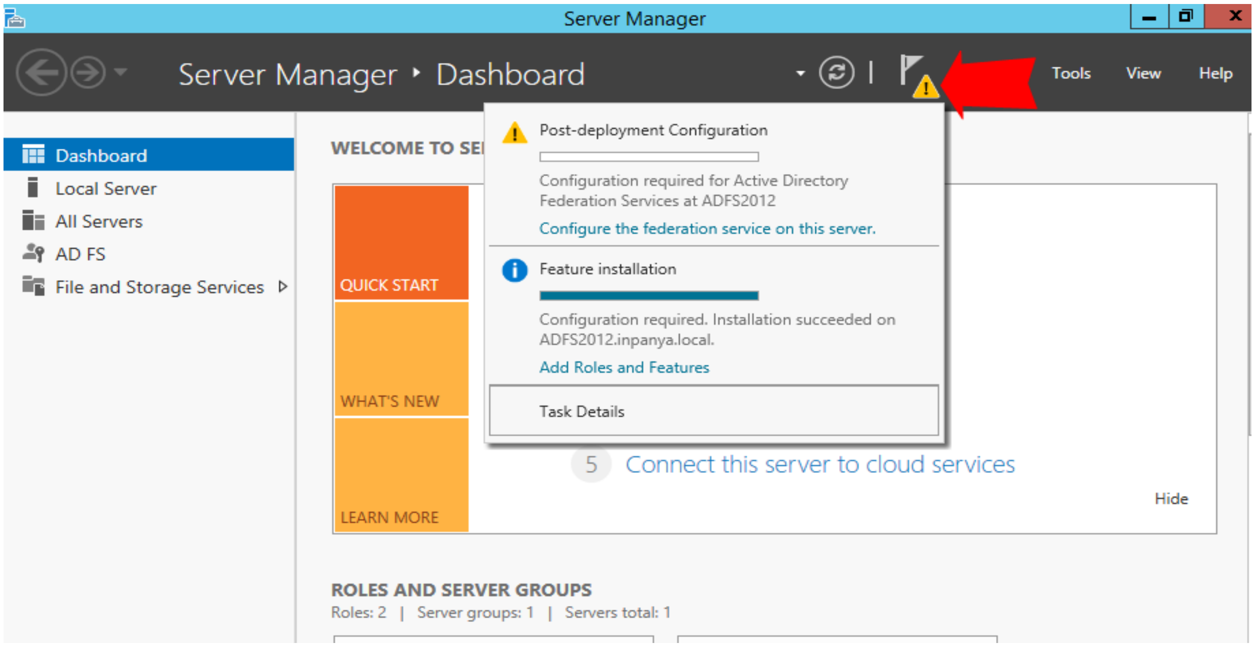
Configuration required. Installation succeeded on ADFS2012.inpanya.local.

Active Directory Federation Services
Additional steps are required to configure Active Directory Federation Services on this machine.
Configure the federation service on this server.

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

When installation succeeded click Close


Server Manager
Server Manager ‣ Dashboard
Tools
View
Help
Dashboard
Local Server
All Servers
AD FS
File and Storage Services
WELCOME TO SE
QUICK START
WHAT'S NEW
LEARN MORE
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 2 | Server groups: 1 | Servers total: 1

Post-deployment Configuration

Configuration required for Active Directory Federation Services at ADFS2012

Configure the federation service on this server.

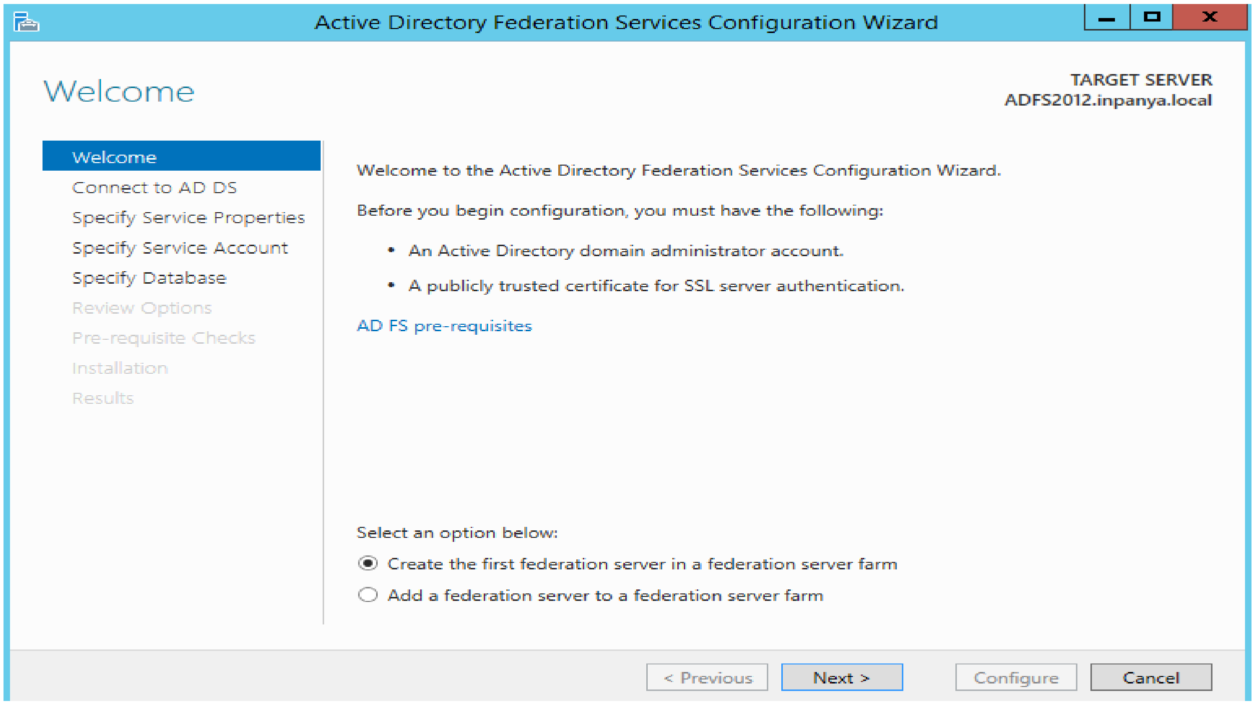
Feature installation

Configuration required. Installation succeeded on ADFS2012.inpanya.local.

Add Roles and Features

Task Details

Click “Configure the federation services on this server” link



Active Directory Federation Services Configuration Wizard

Welcome

TARGET SERVER
ADFS2012.inpanya.local

Welcome to the Active Directory Federation Services Configuration Wizard.

Before you begin configuration, you must have the following:

- An Active Directory domain administrator account.
- A publicly trusted certificate for SSL server authentication.

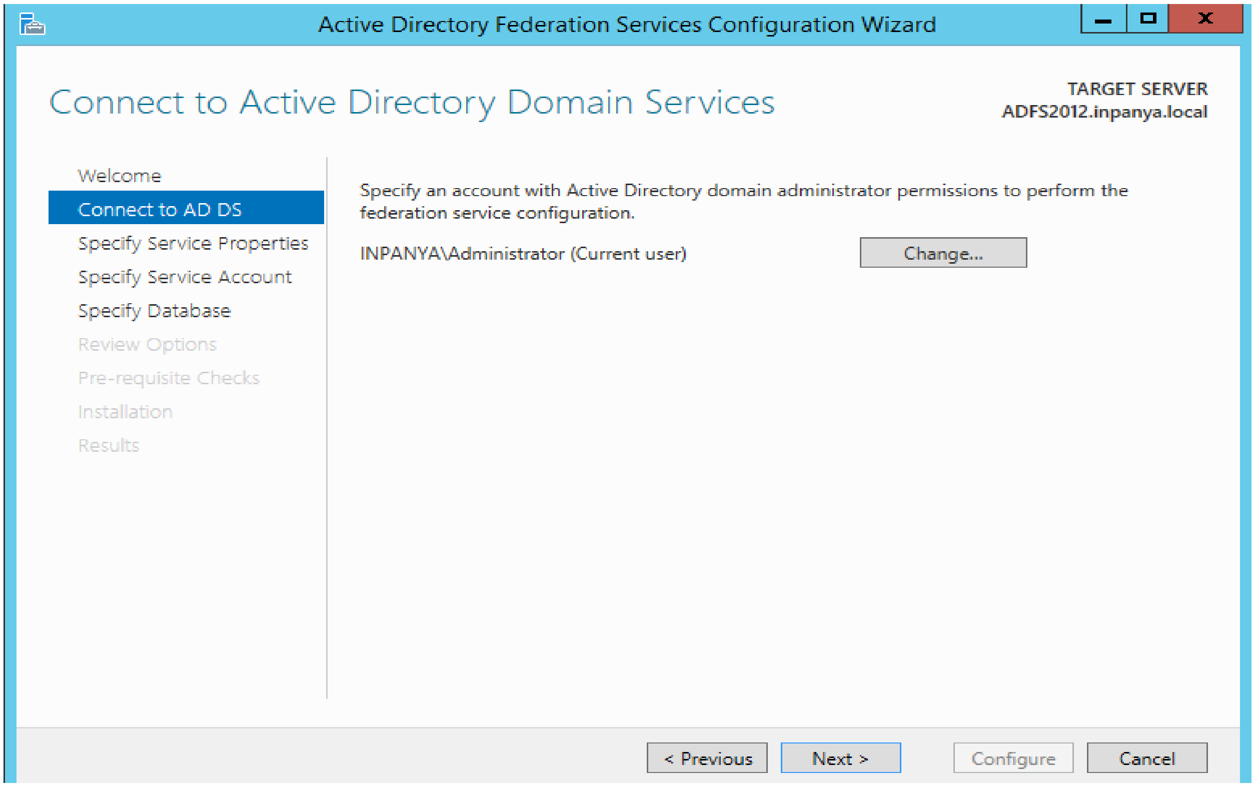
AD FS pre-requisites

Select an option below:

● Create the first federation server in a federation server farm

○ Add a federation server to a federation server farm

Selected Create the first federation server in a federation server farm   and click Next



Active Directory Federation Services Configuration Wizard

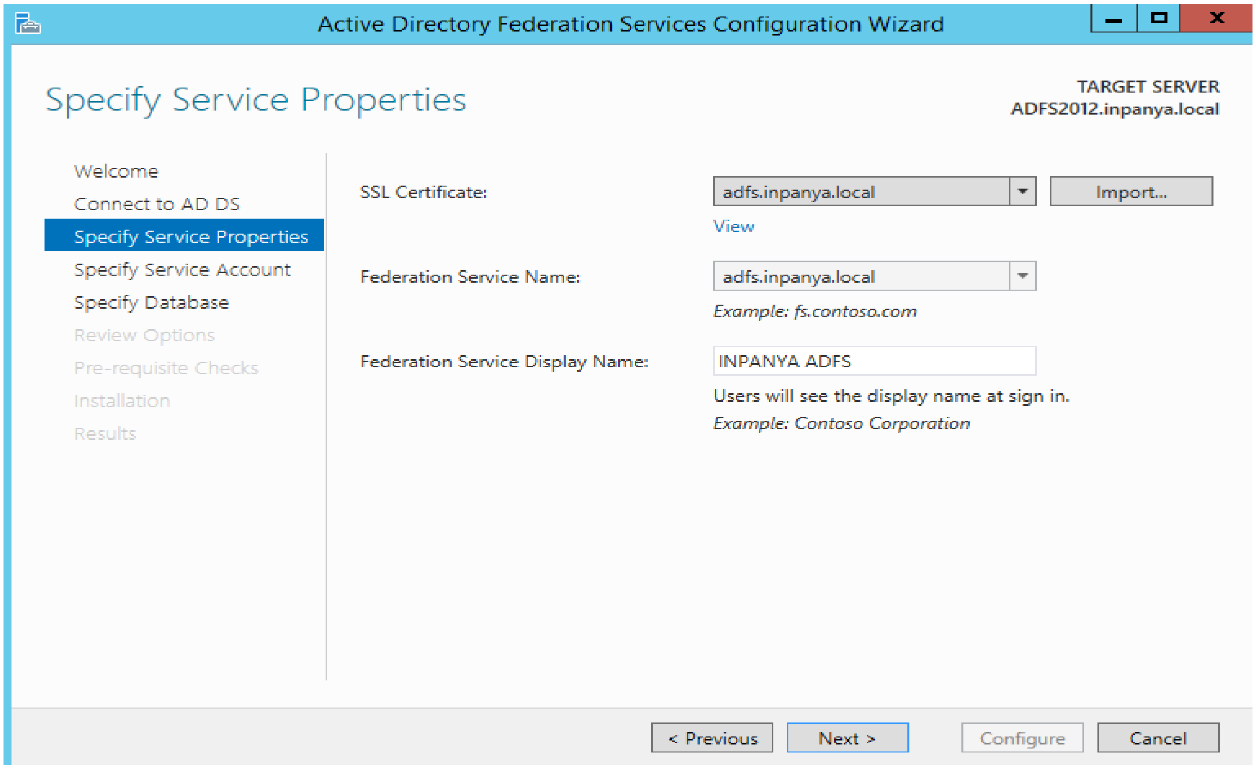
Connect to Active Directory Domain Services

TARGET SERVER
ADFS2012.inpanya.local

Specify an account with Active Directory domain administrator permissions to perform the federation service configuration.

INPANYA\Administrator (Current user)

Click Next



Specify Service Properties

TARGET SERVER
ADFS2012.inpanya.local

SSL Certificate: adfs.inpanya.local

Federation Service Name: adfs.inpanya.local

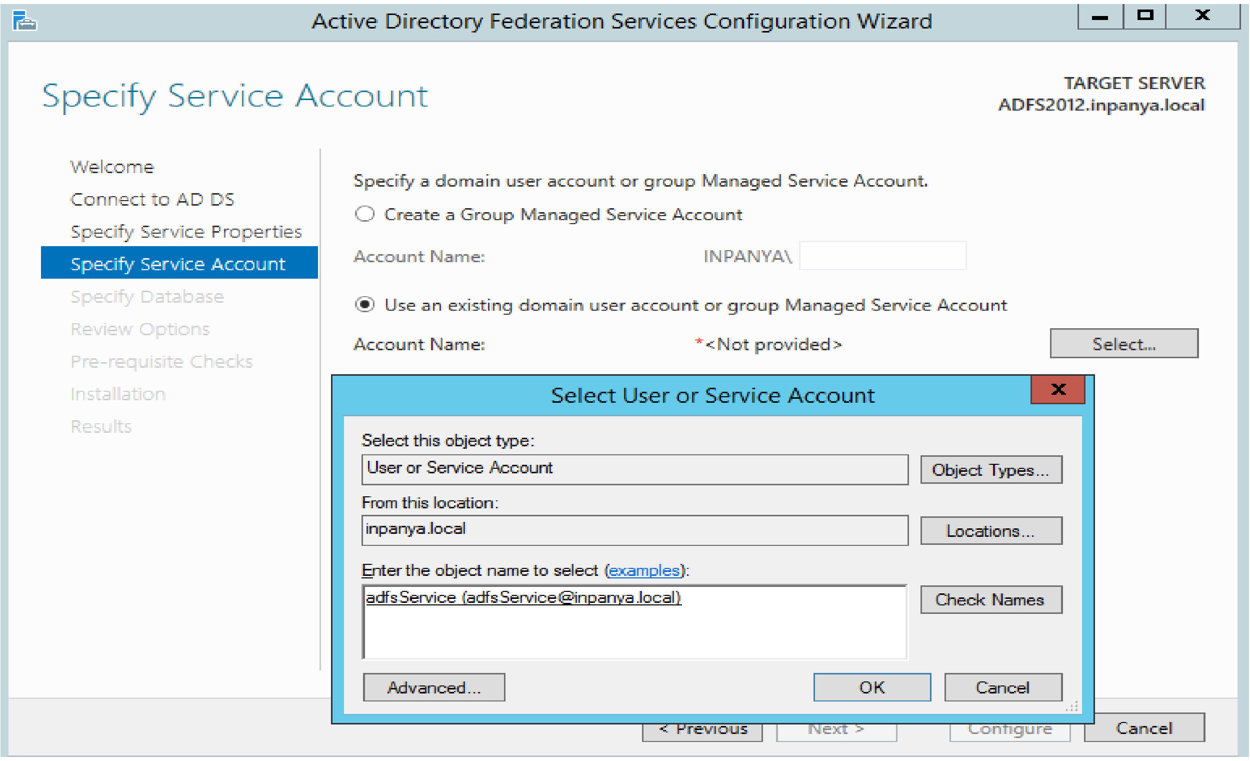
Example: fs.contoso.com

Federation Service Display Name: INPANYA ADFS

Users will see the display name at sign in.

Example: Contoso Corporation

Select SSL Certificate in list box



Specify Service Account

TARGET SERVER
ADFS2012.inpanya.local

Specify a domain user account or group Managed Service Account.

○ Create a Group Managed Service Account

Account Name: INPANYA\

● Use an existing domain user account or group Managed Service Account

Account Name: *<Not provided>

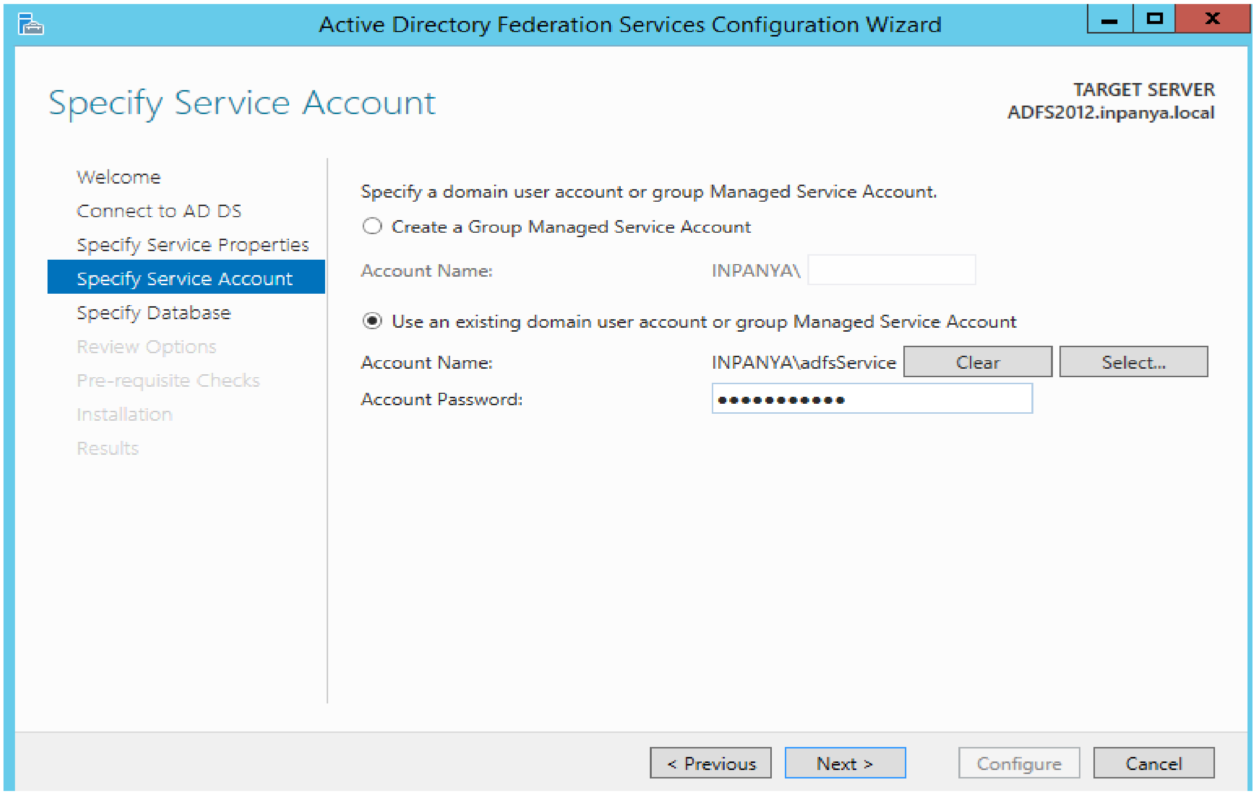
Select User or Service Account

Select this object type:
User or Service Account

From this location:
inpanya.local

Enter the object name to select (examples):
adfsService (adfsService@inpanya.local)

Select Use an existing domain user account then click Select button



Specify Service Account

TARGET SERVER
ADFS2012.inpanya.local

Specify a domain user account or group Managed Service Account.

○ Create a Group Managed Service Account

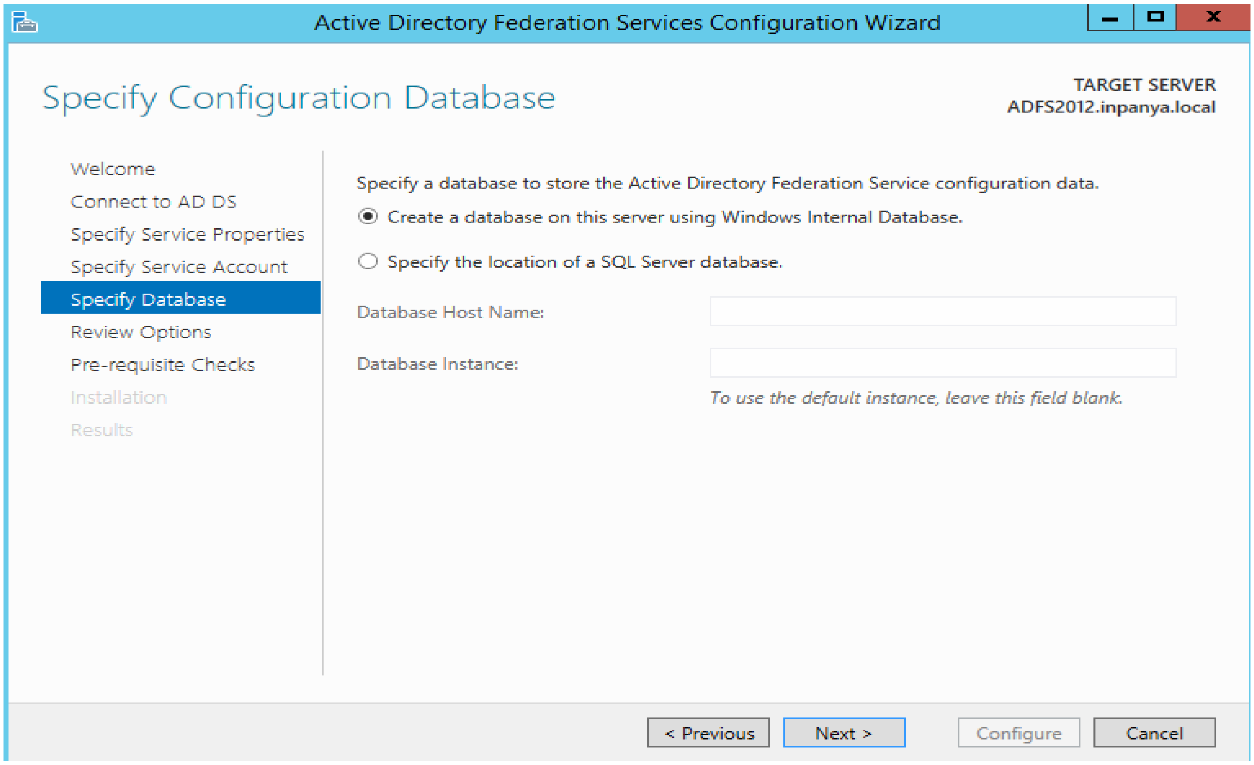
Account Name: INPANYA\

● Use an existing domain user account or group Managed Service Account

Account Name: INPANYA\adfsService

Account Password: ●●●●●●●●●●●

Enter password and click Next



Specify Configuration Database

TARGET SERVER
ADFS2012.inpanya.local

Specify a database to store the Active Directory Federation Service configuration data.

● Create a database on this server using Windows Internal Database.

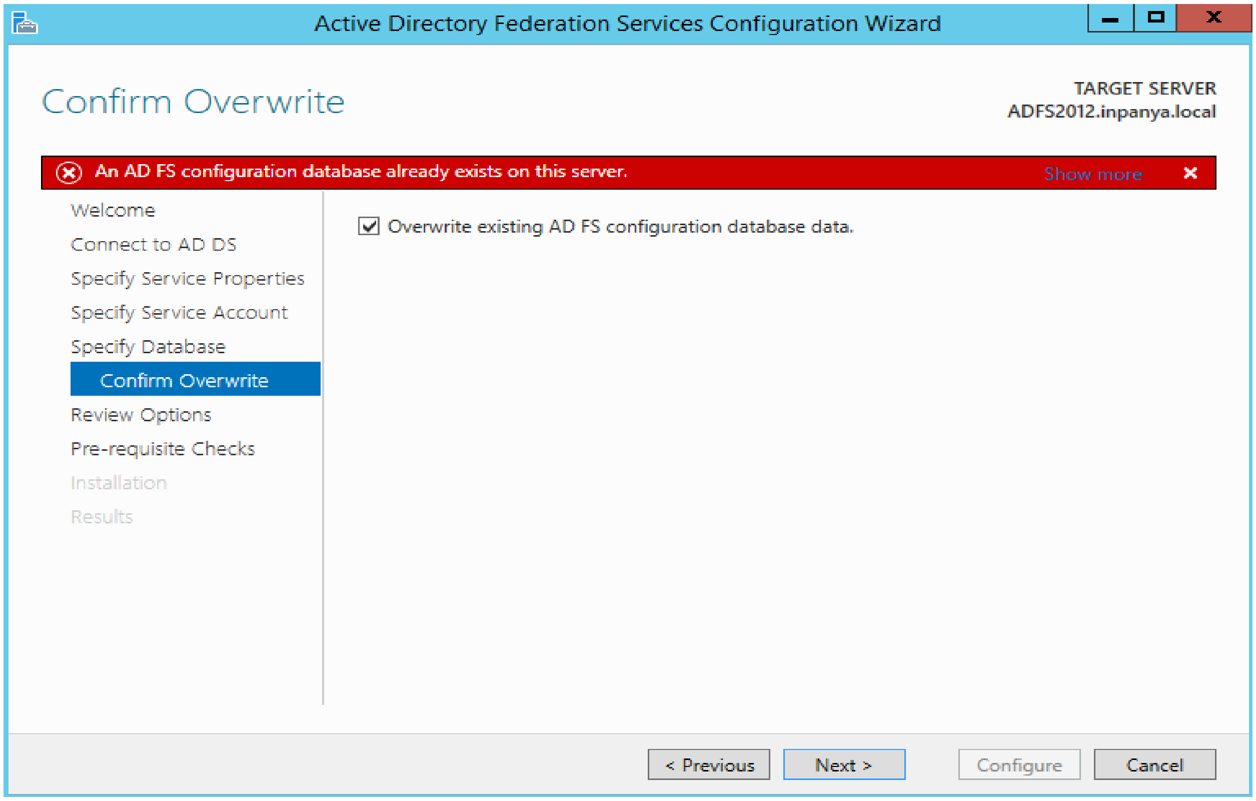
○ Specify the location of a SQL Server database.

Database Host Name:

Database Instance:

To use the default instance, leave this field blank.

Selected Create a database on this server using Windows Internal Database then click Next



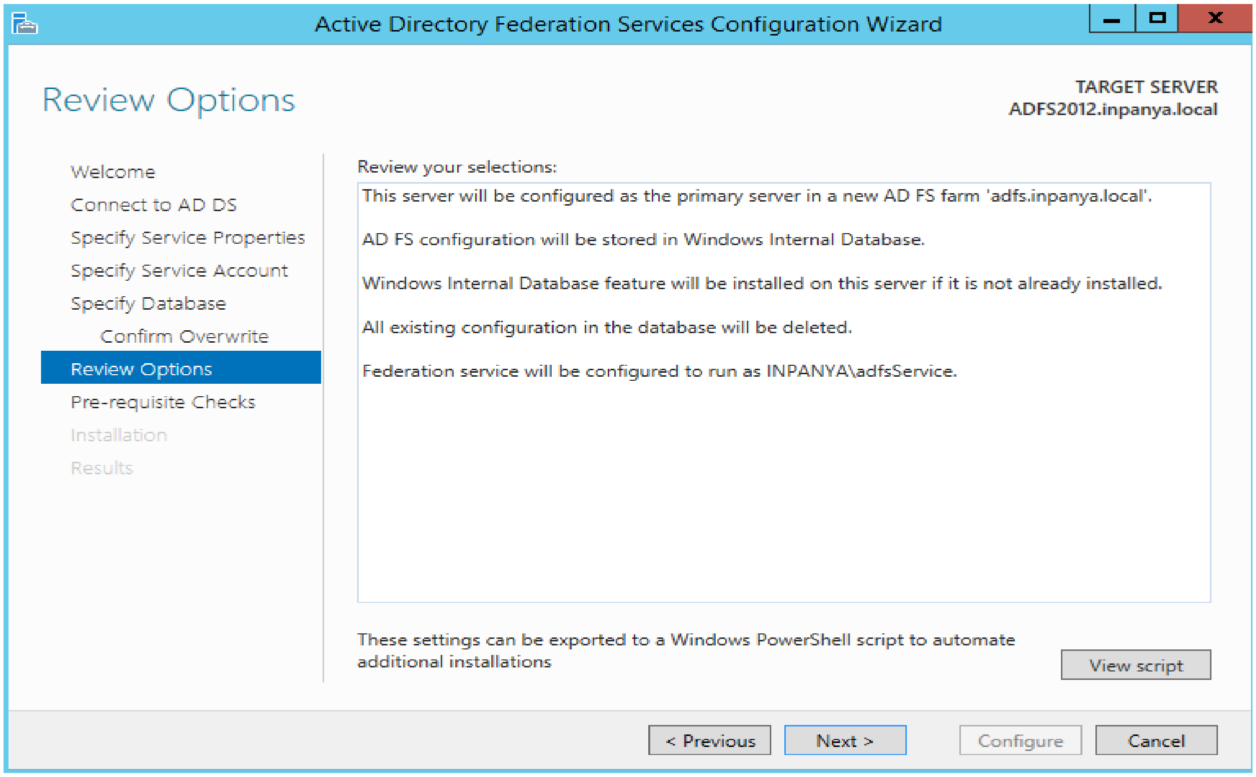
Confirm Overwrite

TARGET SERVER
ADFS2012.inpanya.local

An AD FS configuration database already exists on this server.

☑ Overwrite existing AD FS configuration database data.

Checked Overwrite existing ADFS configuration database data the click Next



Review Options

TARGET SERVER
ADFS2012.inpanya.local

Review your selections:

This server will be configured as the primary server in a new AD FS farm 'adfs.inpanya.local'.

AD FS configuration will be stored in Windows Internal Database.

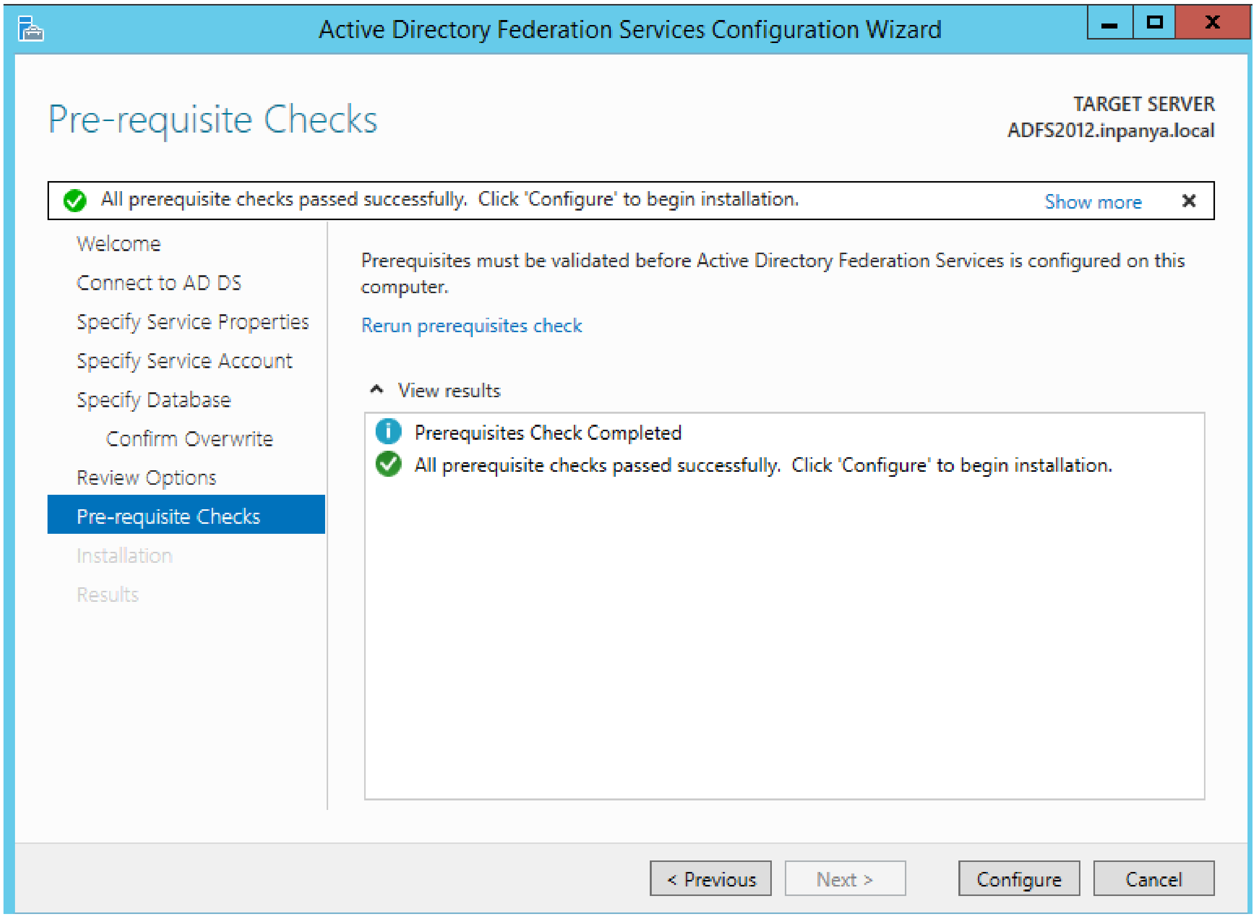
Windows Internal Database feature will be installed on this server if it is not already installed.

All existing configuration in the database will be deleted.

Federation service will be configured to run as INPANYA\adfsService.

These settings can be exported to a Windows PowerShell script to automate additional installations

Click Next



Pre-requisite Checks

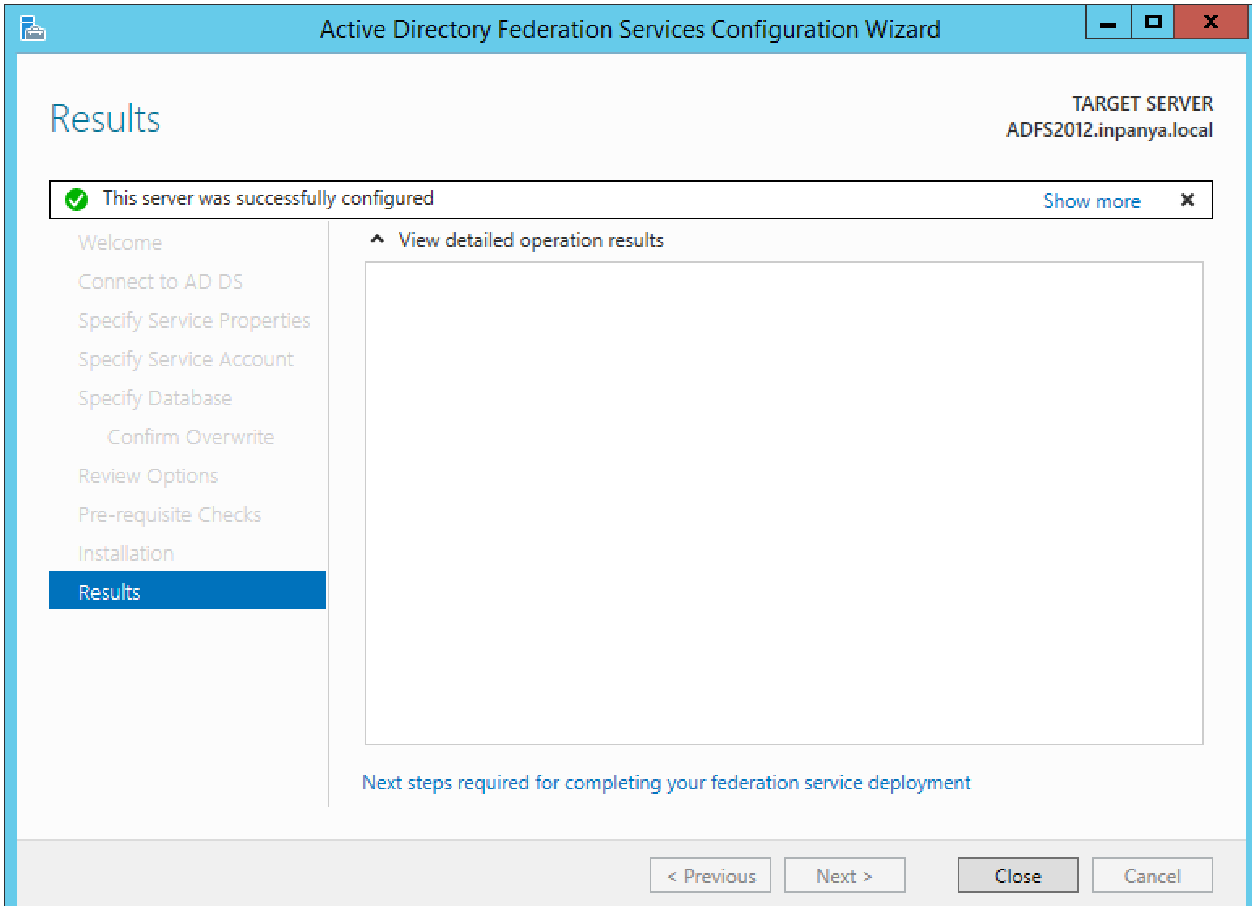
✓ All prerequisite checks passed successfully. Click 'Configure' to begin installation.

Prerequisites must be validated before Active Directory Federation Services is configured on this computer.

Prerequisites Check Completed

✓ All prerequisite checks passed successfully. Click 'Configure' to begin installation.

Click Configure



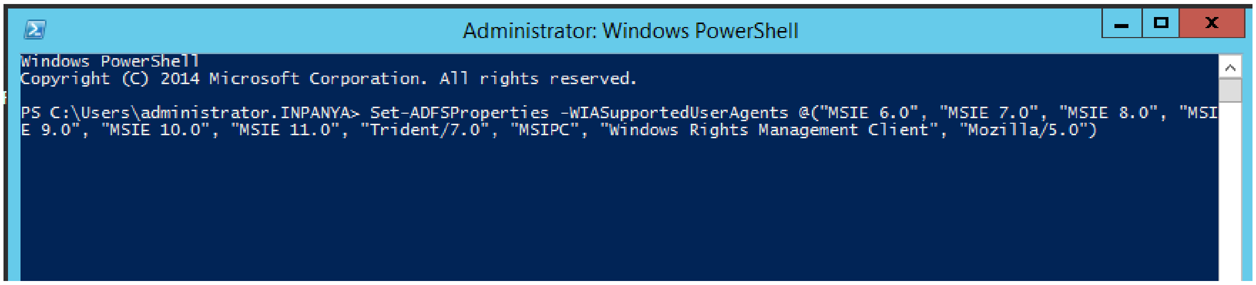
This server was successfully configured

Next steps required for completing your federation service deployment

Click Close

Execute command on Power shell for support user agent

Set-ADFSProperties -WIASupportedUserAgents @("MSIE 6.0", "MSIE 7.0", "MSIE 8.0", "MSIE 9.0", "MSIE 10.0", "MSIE 11.0", "Trident/7.0", "MSIPC", "Windows Rights Management Client", "Mozilla/5.0")

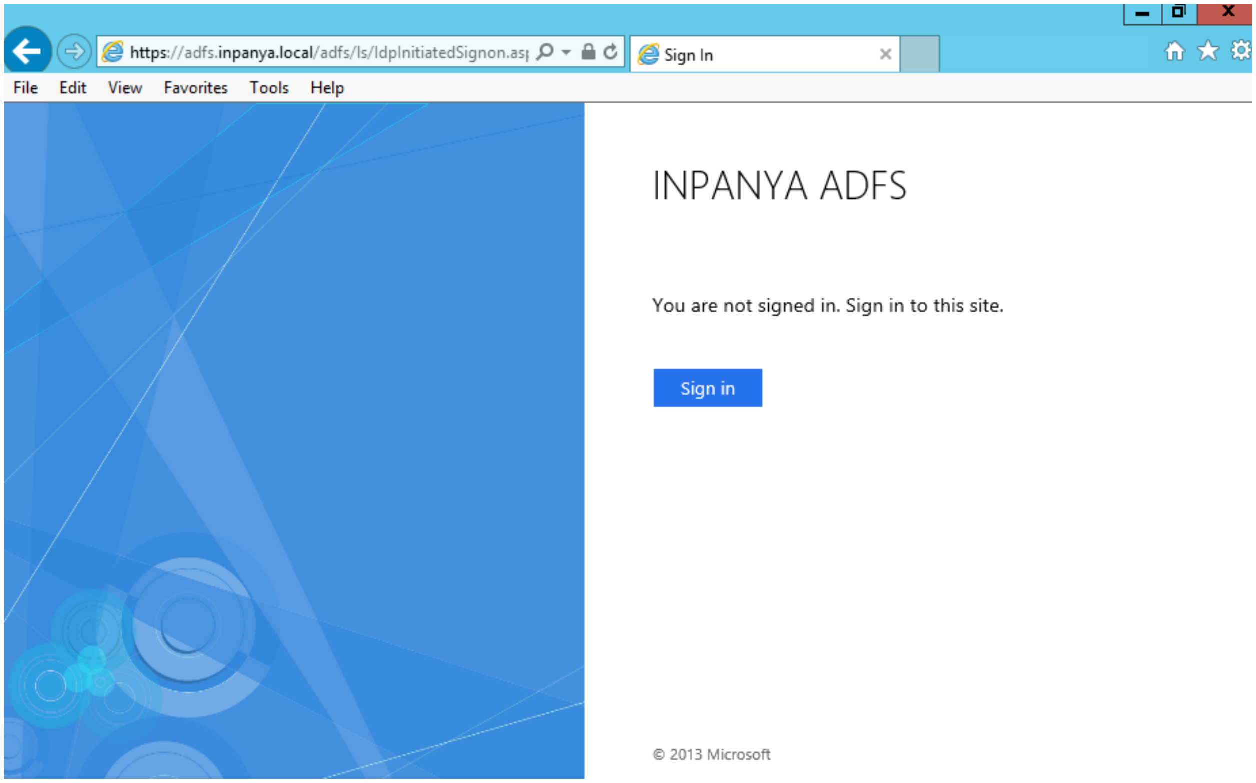


```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\administrator.INPANYA> Set-ADFSProperties -WIASupportedUserAgents @("MSIE 6.0", "MSIE 7.0", "MSIE 8.0", "MSI
E 9.0", "MSIE 10.0", "MSIE 11.0", "Trident/7.0", "MSIPC", "Windows Rights Management Client", "Mozilla/5.0")
```

Test ADFS IDP Initiated Sign on

Add trust site : https://adfs.inpanya.local

https://adfs.inpanya.local/adfs/ls/IdpInitiatedSignon.aspx



INPANYA ADFS

You are not signed in. Sign in to this site.

© 2013 Microsoft

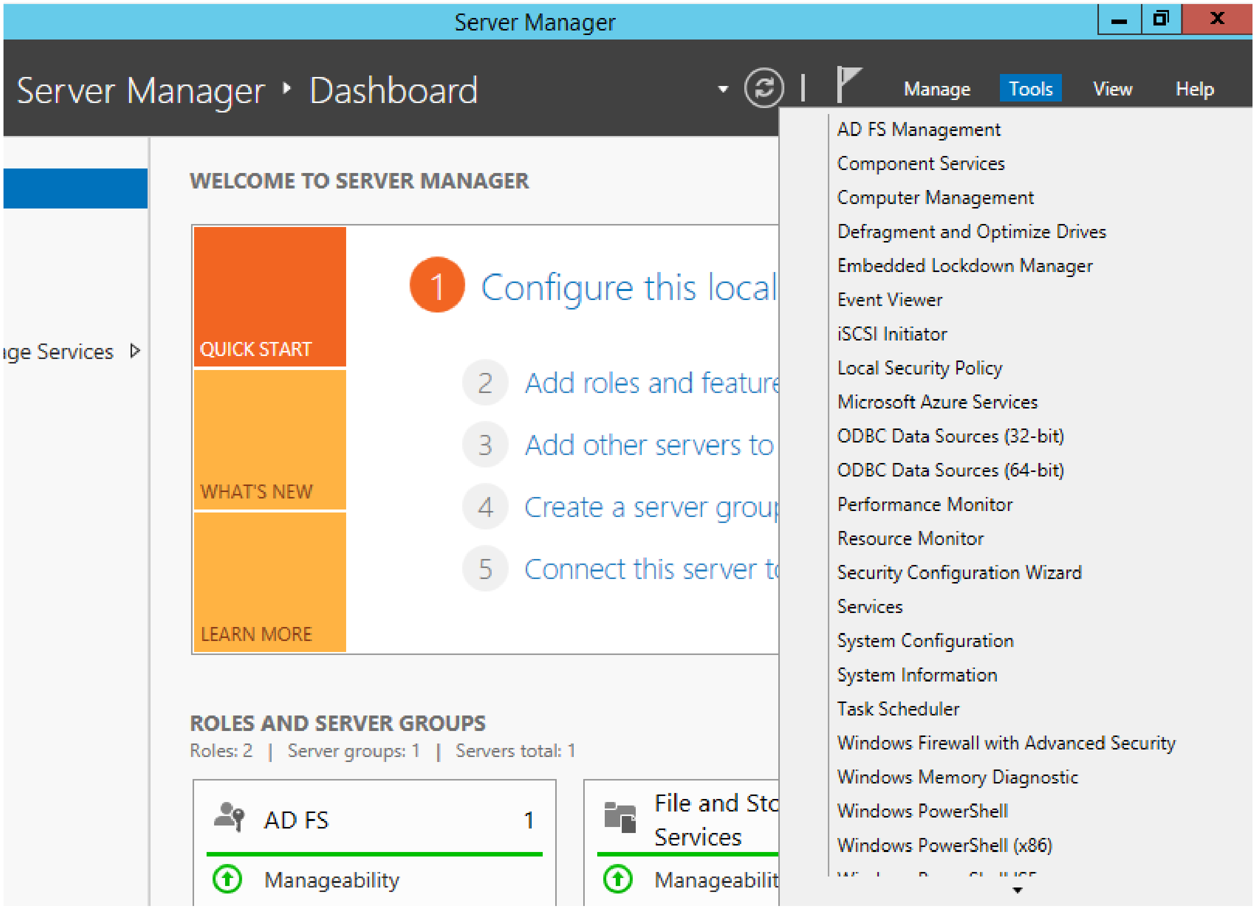
**** PS***

Add new IP in host file (All clients ‘ PC or DNS)

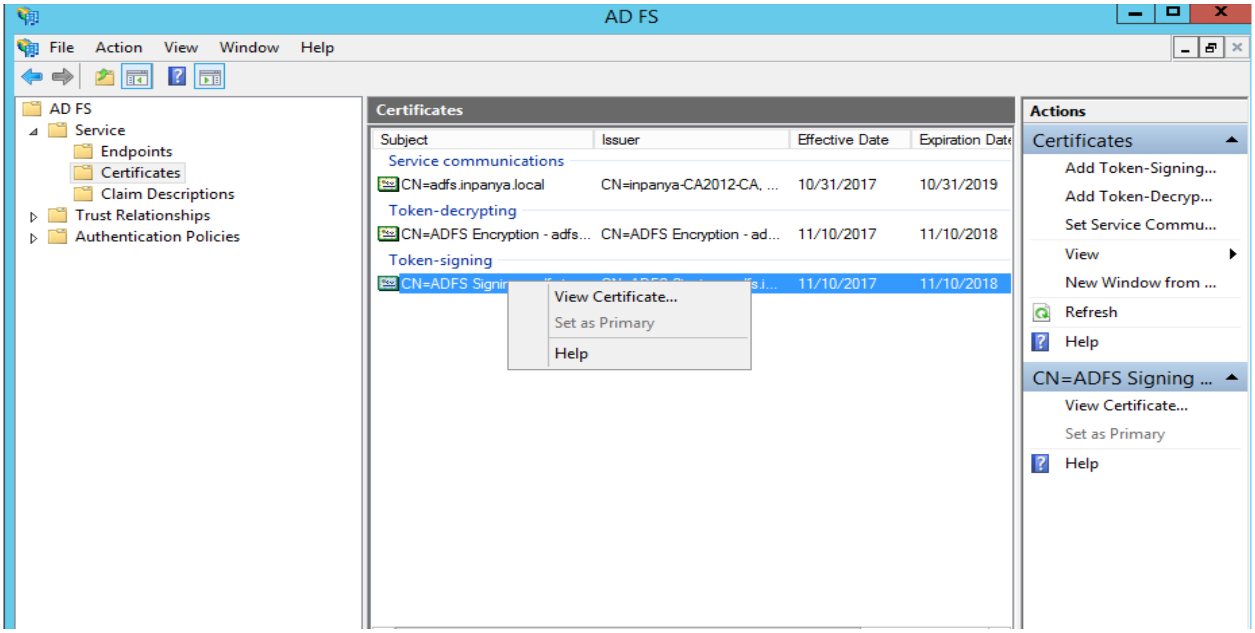
192.168.56.252   adfs.inpanya.local

Configuration Tomcat8.5.4 SSO

Export ADFS Certificate (On ADFS Server)

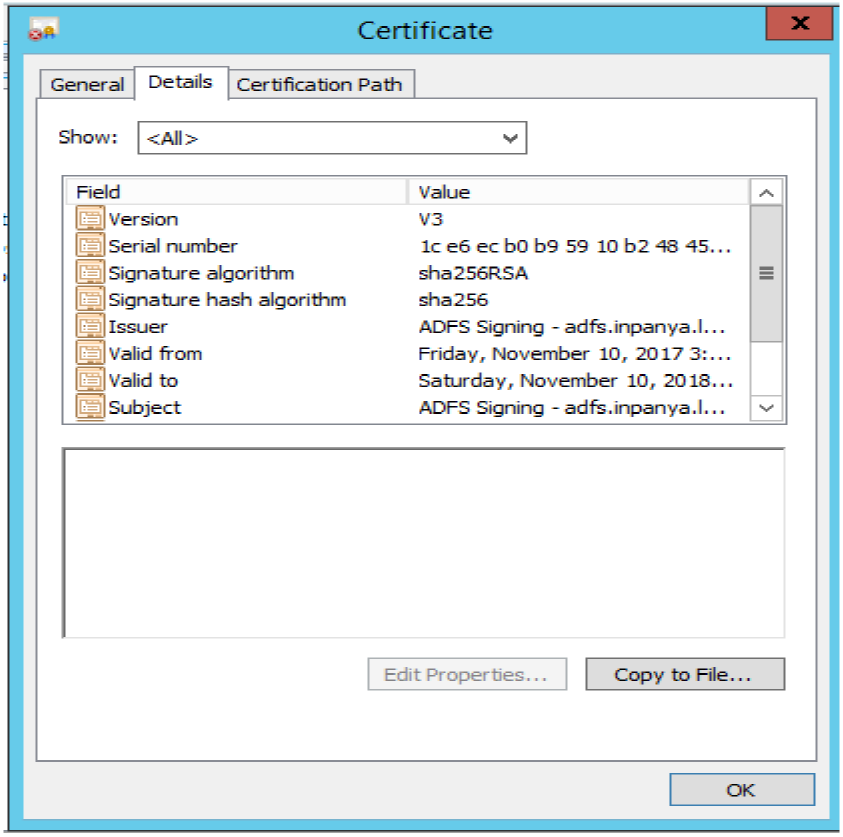


On Server Manager : click Tools->AD FS Management



Subject	Issuer	Effective Date	Expiration Date
Service communications			
CN=adfs.inpanya.local	CN=inpanya-CA2012-CA, ...	10/31/2017	10/31/2019
Token-decrypting			
CN=ADFS Encryption - adfs...	CN=ADFS Encryption - ad...	11/10/2017	11/10/2018
Token-signing			
CN=ADFS Signir		11/10/2017	11/10/2018

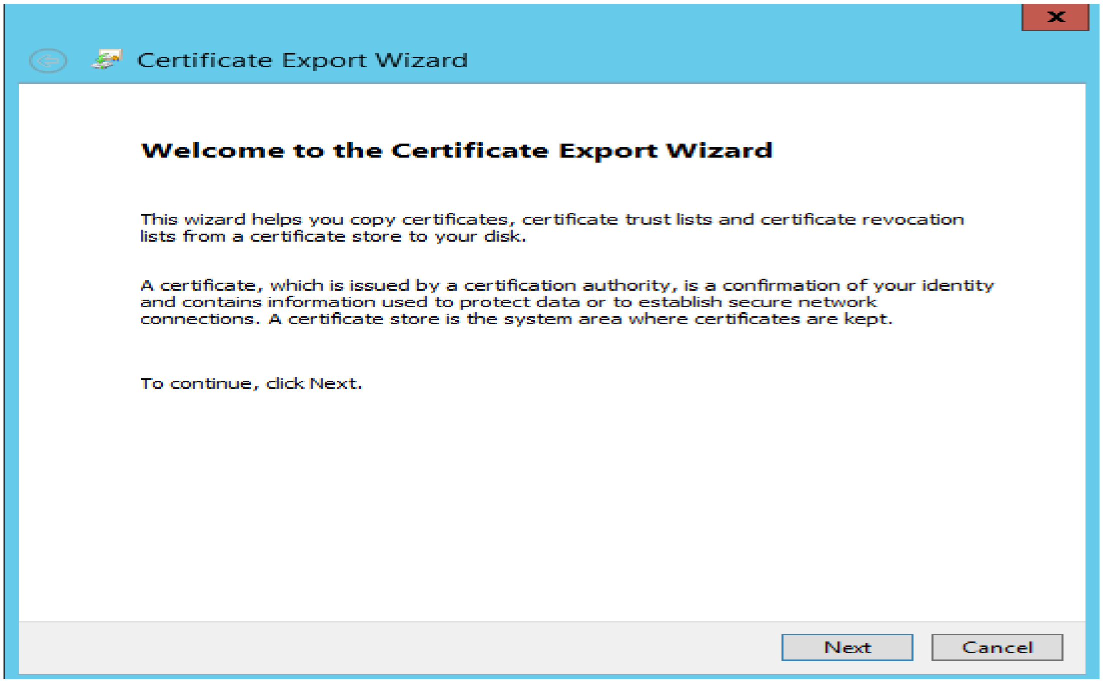
Right click Token-signing ->View Certificate



Show: <All>

Field	Value
Version	V3
Serial number	1c e6 ec b0 b9 59 10 b2 48 45...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	ADFS Signing - adfs.inpanya.l...
Valid from	Friday, November 10, 2017 3:...
Valid to	Saturday, November 10, 2018...
Subject	ADFS Signing - adfs.inpanya.l...

Click Copy to File



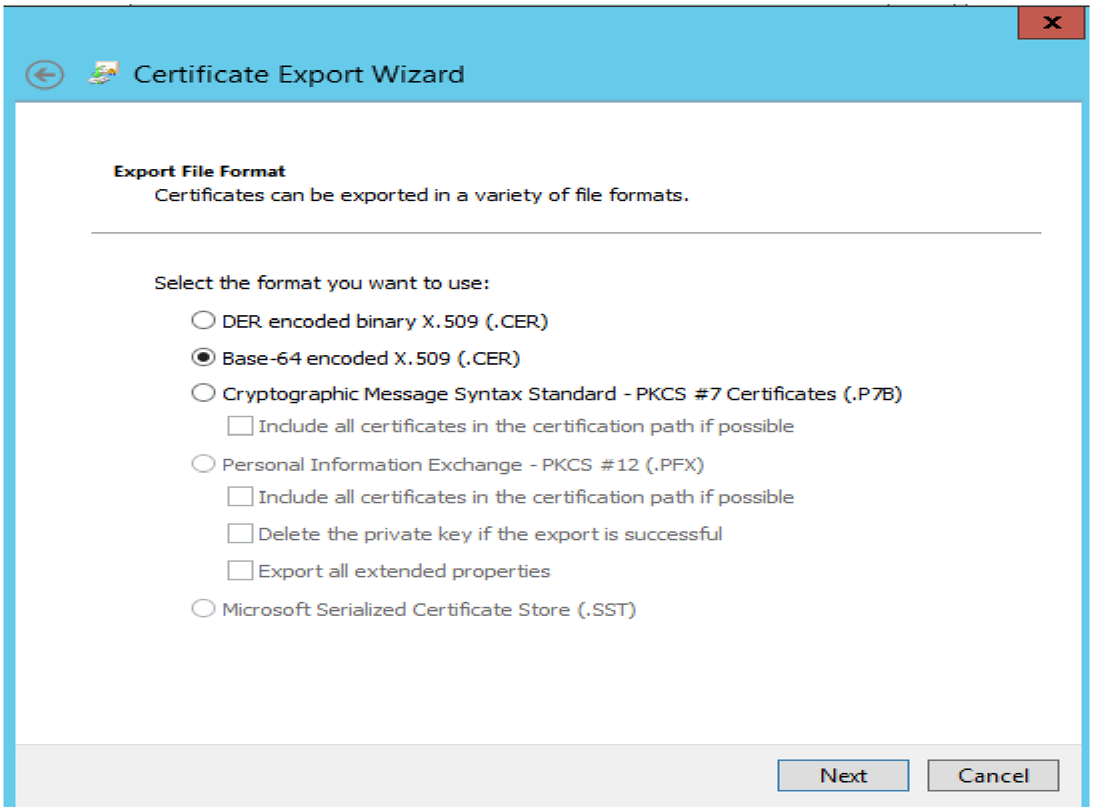
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Click Next



Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

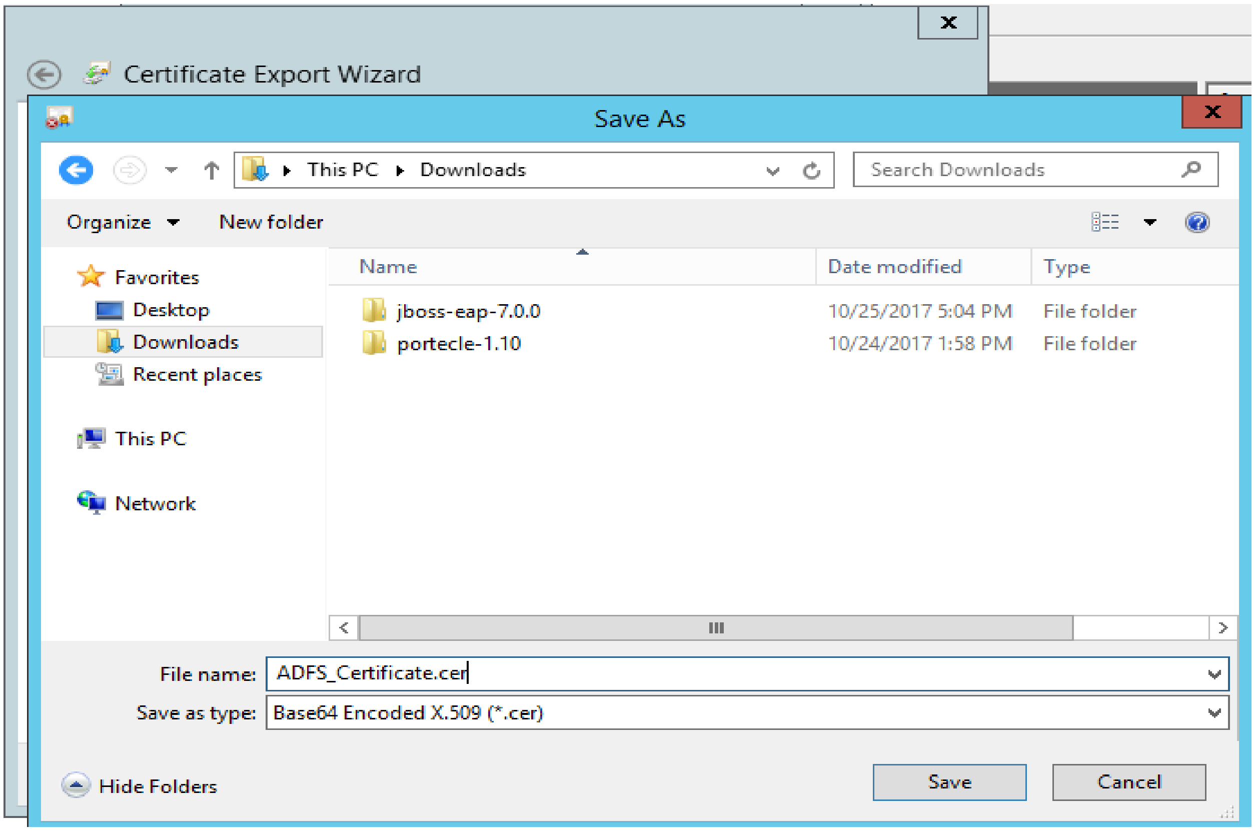
□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

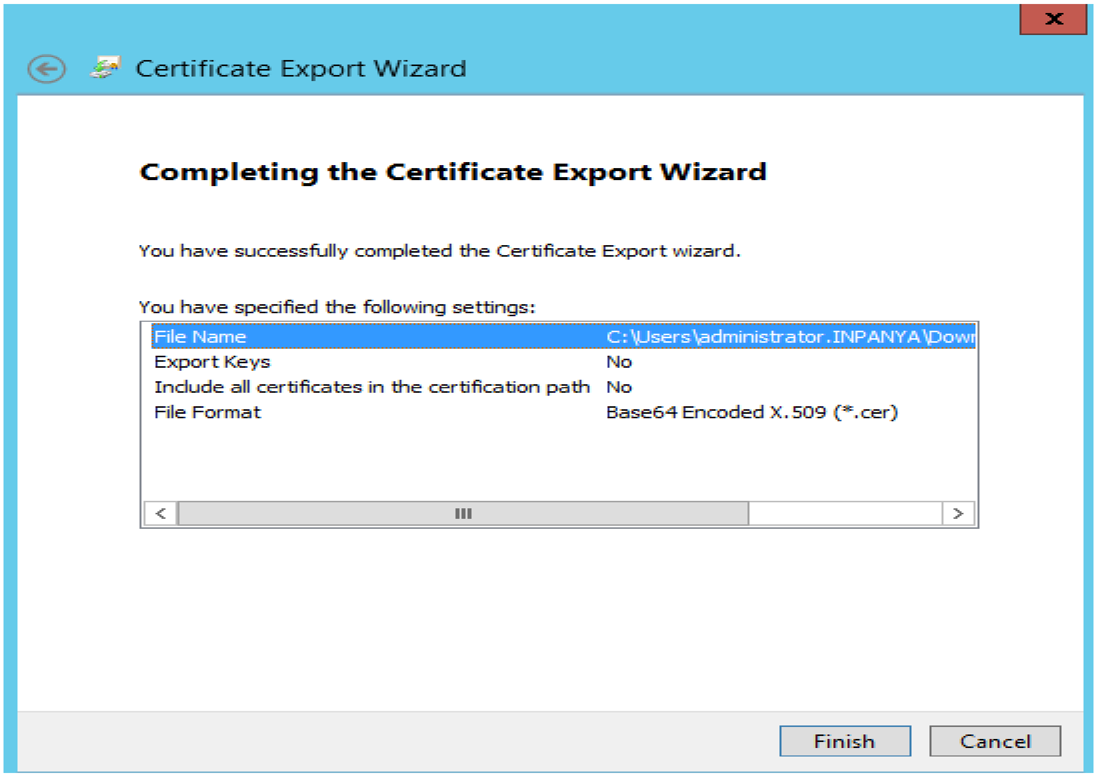
Selected Base-64 encoded x.509 then click Next



Name	Date modified	Type
jboss-eap-7.0.0	10/25/2017 5:04 PM	File folder
portecle-1.10	10/24/2017 1:58 PM	File folder

File name: ADFS_Certificate.cer

Save as type: Base64 Encoded X.509 (*.cer)



Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

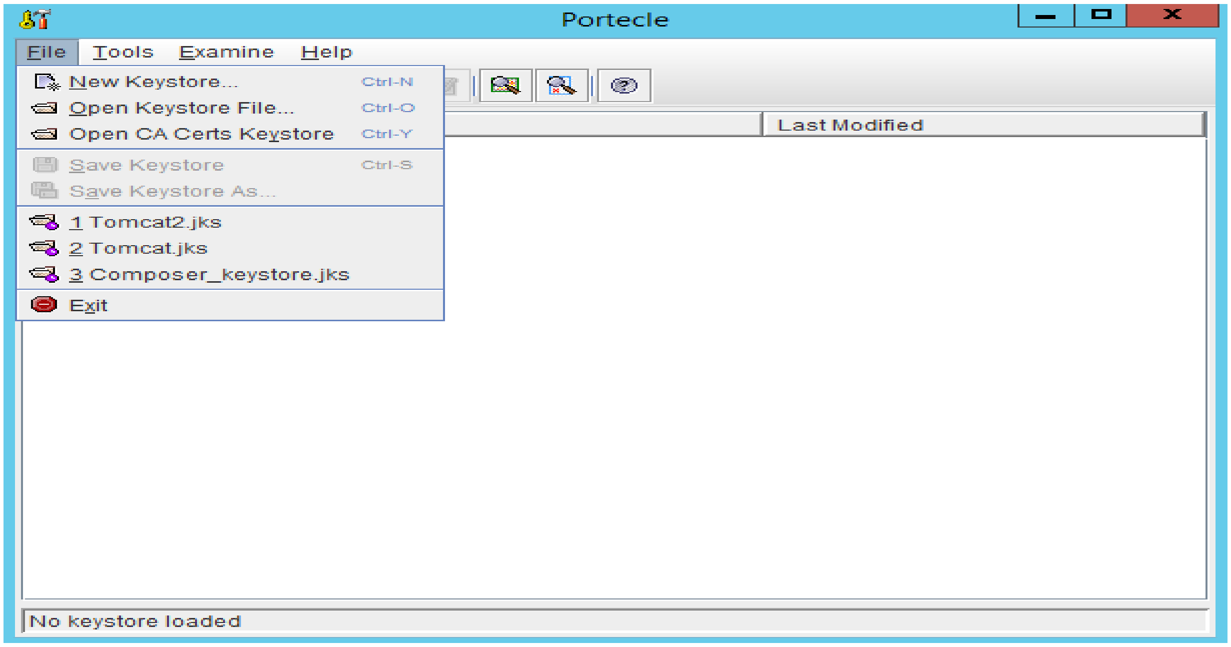
You have specified the following settings:

File Name	C:\Users\administrator.INPANYA\Dowr
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64 Encoded X.509 (*.cer)

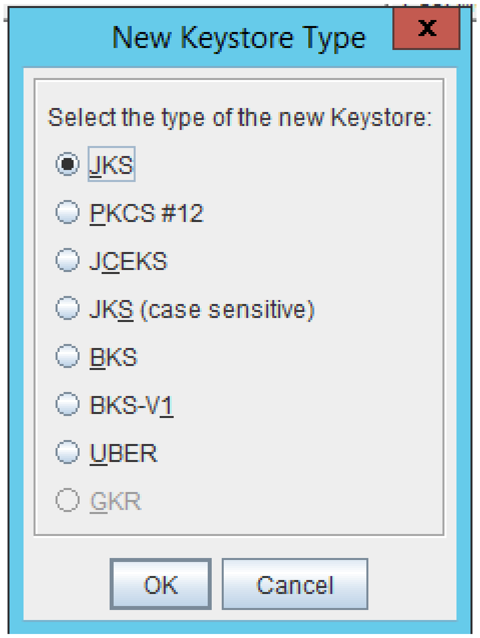
Click Finish

Generate Self sign key for tomcat server using Portecle

Download from http://sourceforge.net/projects/portecle/



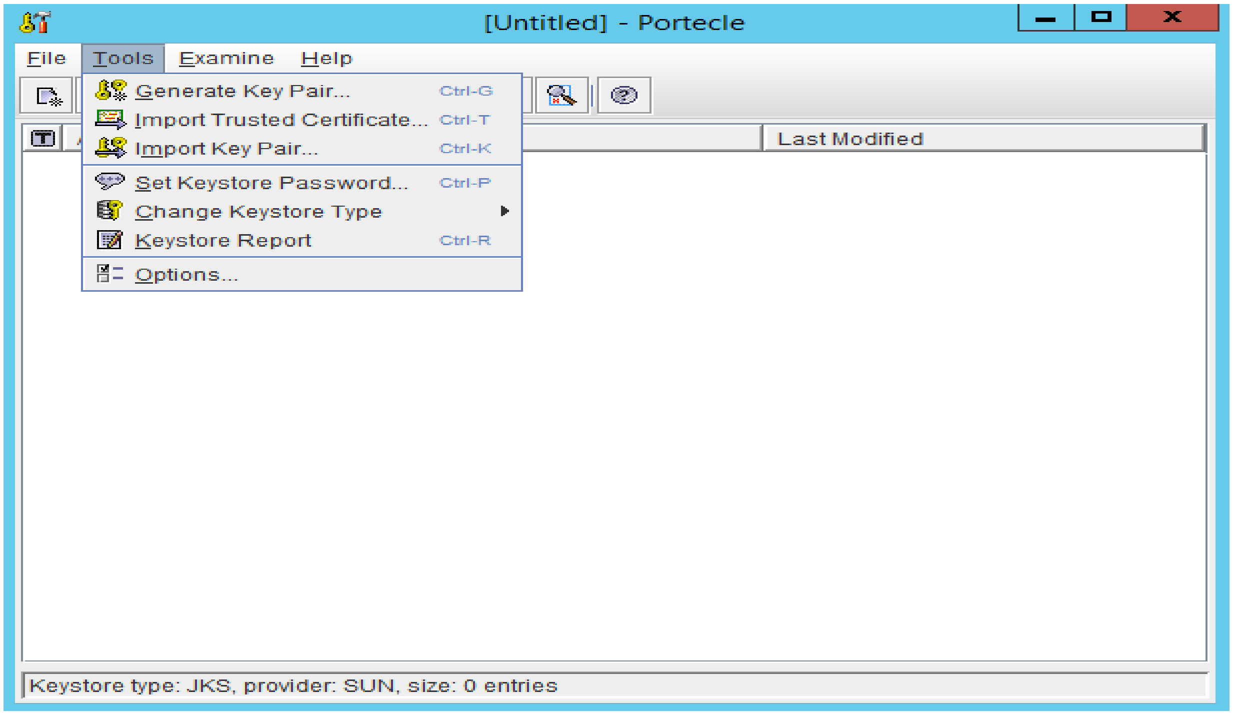
File →New Keystore



Select the type of the new Keystore:

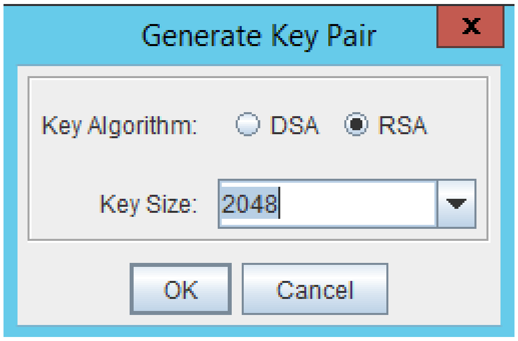
● JKS
○ PKCS #12
○ JCEKS
○ JKS (case sensitive)
○ BKS
○ BKS-V1
○ UBER
○ GKR

Select JKS then click OK


[Untitled] - Portecle
File
Tools
Examine
Help
Generate Key Pair... Ctrl-G
Import Trusted Certificate... Ctrl-T
Import Key Pair... Ctrl-K
Set Keystore Password... Ctrl-P
Change Keystore Type
Keystore Report Ctrl-R
Options...
Last Modified

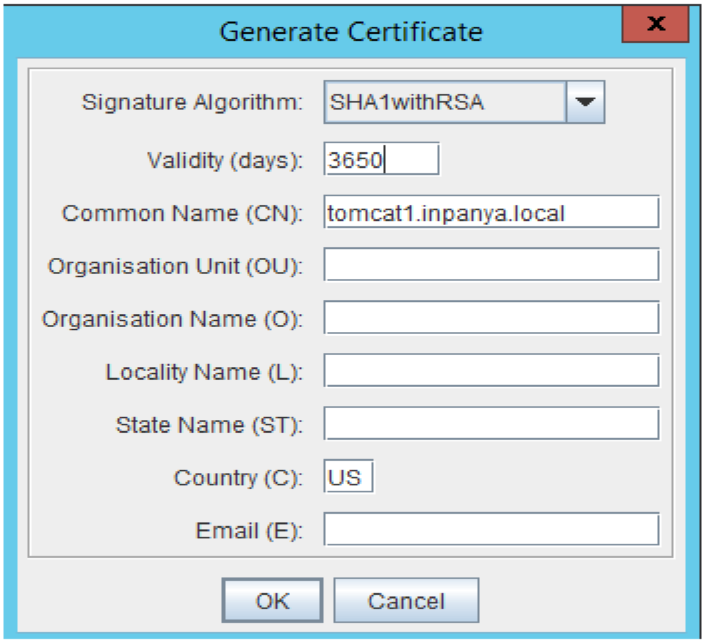
Keystore type: JKS, provider: SUN, size: 0 entries

Tools →Generate Key Pair



Key Algorithm: ○ DSA ● RSA

Key Size: 2048



Generate Certificate

Signature Algorithm: SHA1withRSA

Validity (days): 3650

Common Name (CN): tomcat1.inpanya.local

Organisation Unit (OU):

Organisation Name (O):

Locality Name (L):

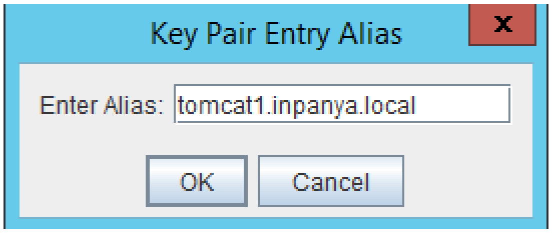
State Name (ST):

Country (C): US

Email (E):

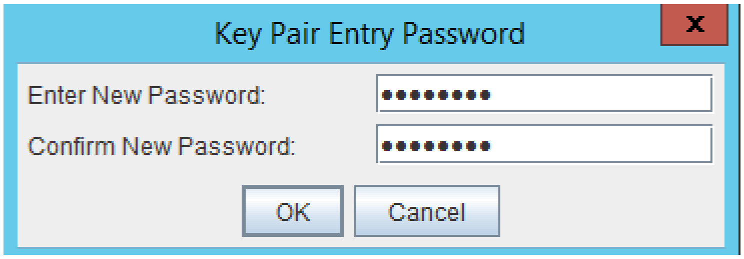
Signature Algorithm:SHA1withRSA

Common Name(CN):tomcat1.inpanya.local



Key Pair Entry Alias

Enter Alias: tomcat1.inpanya.local

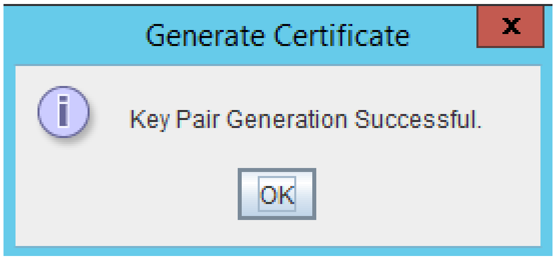


Key Pair Entry Password

Enter New Password: ●●●●●●●●

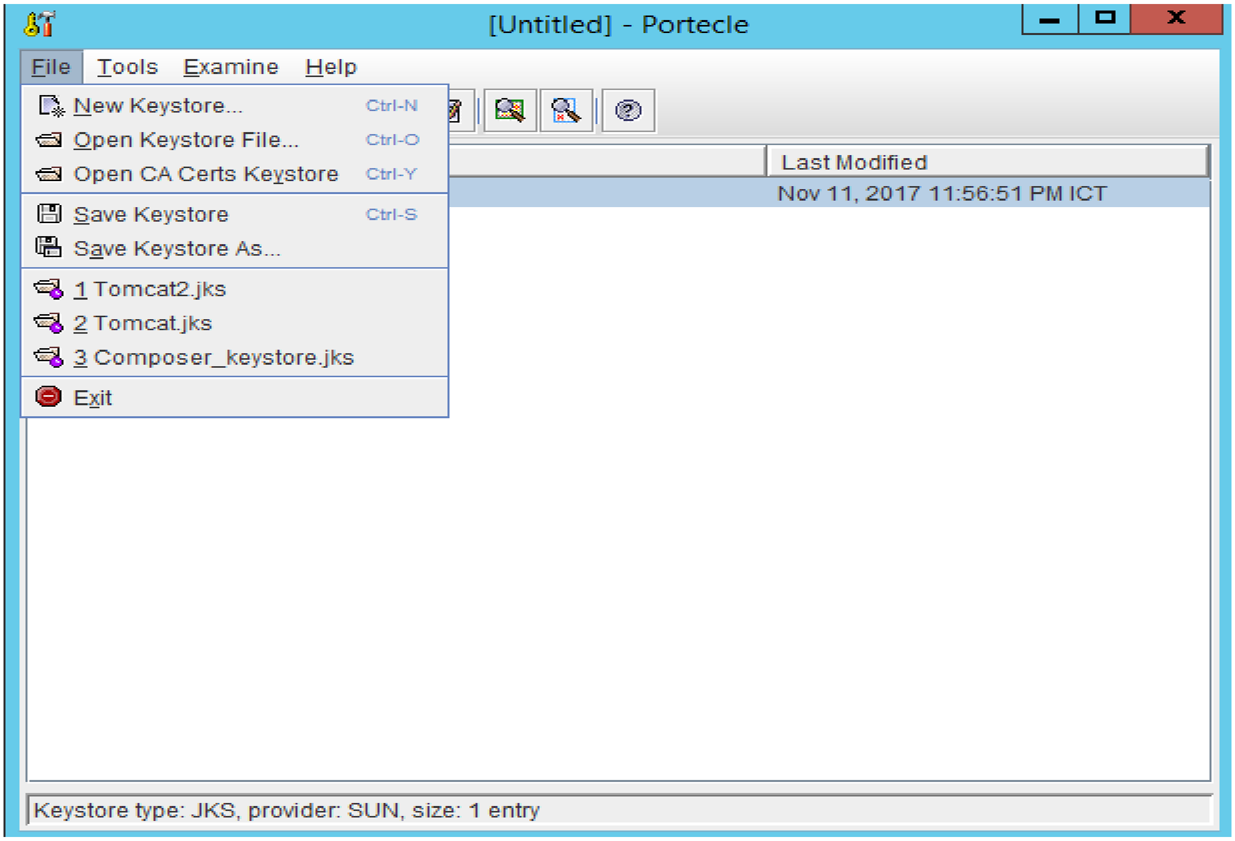
Confirm New Password: ●●●●●●●●

Enter Password:P@ssw0rd

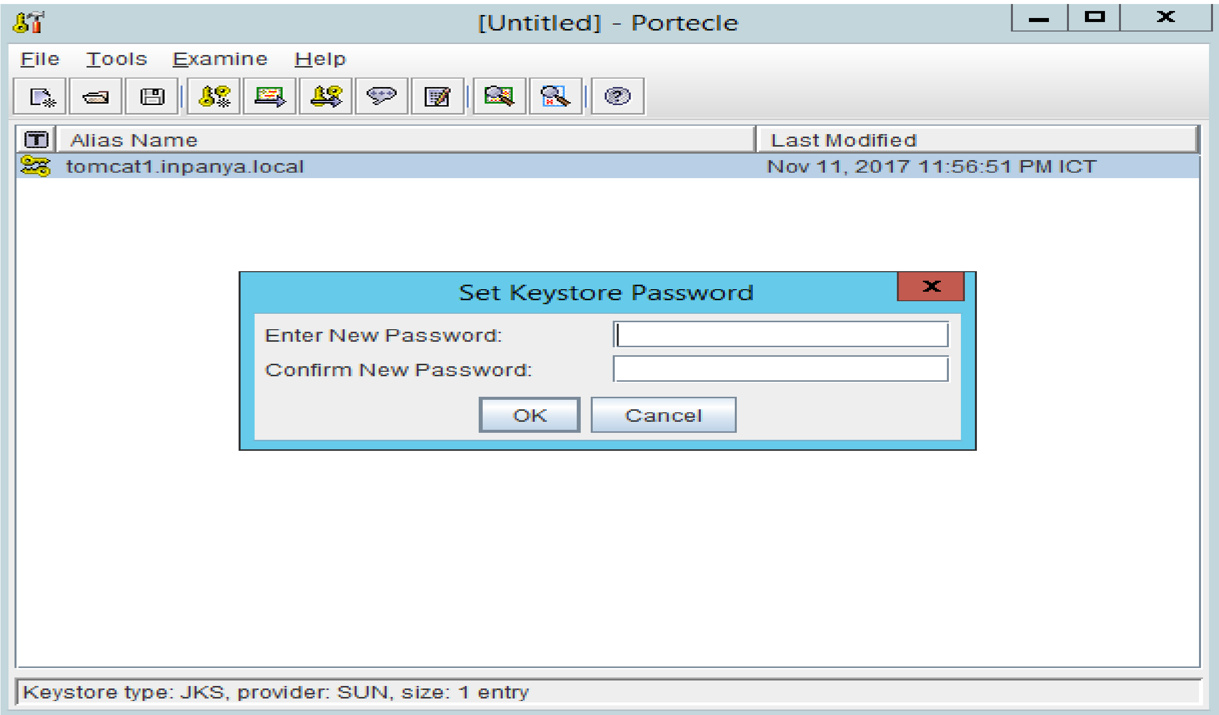


Generate Certificate

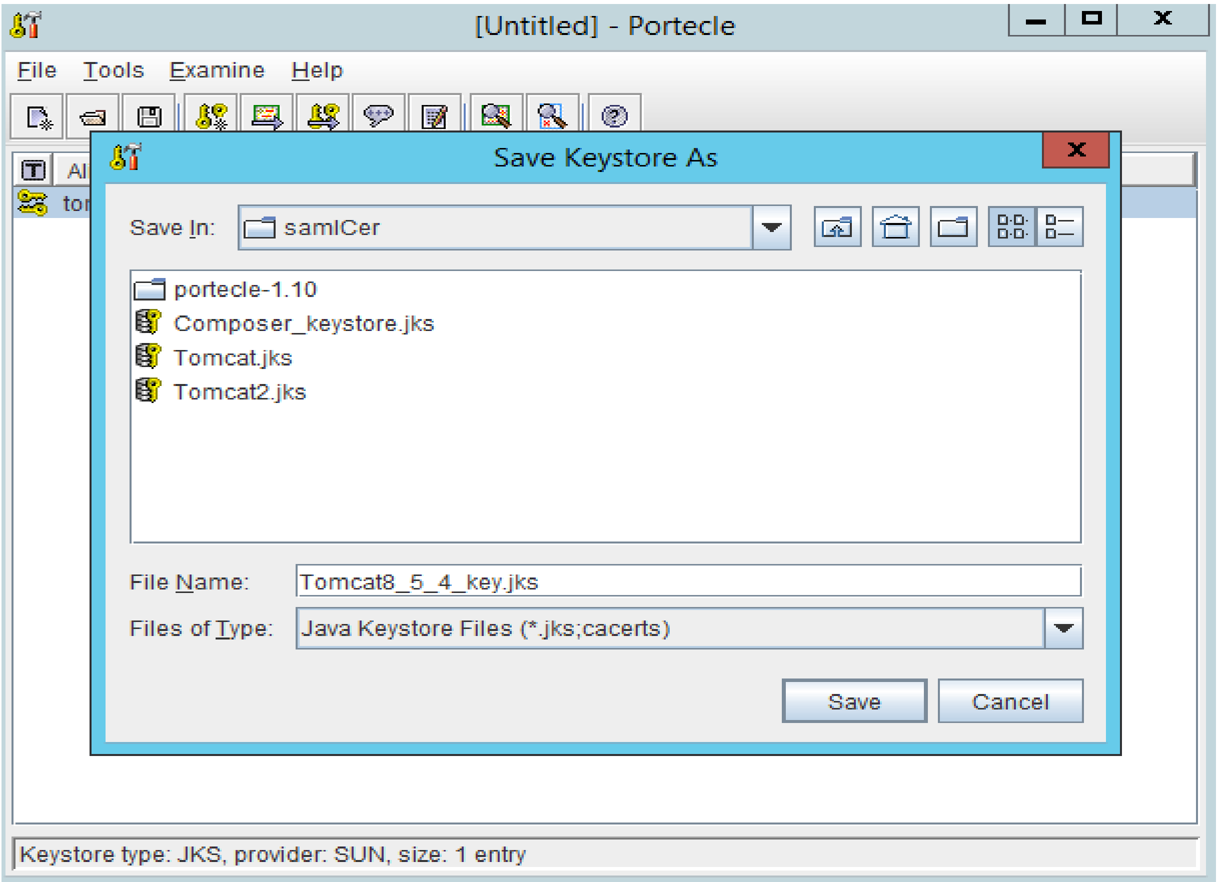
Key Pair Generation Successful.



File →Save Keystore



Enter password:P@ssw0rd



Save In: samlCer

portecle-1.10
Composer_keystore.jks
Tomcat.jks
Tomcat2.jks

File Name: Tomcat8_5_4_key.jks

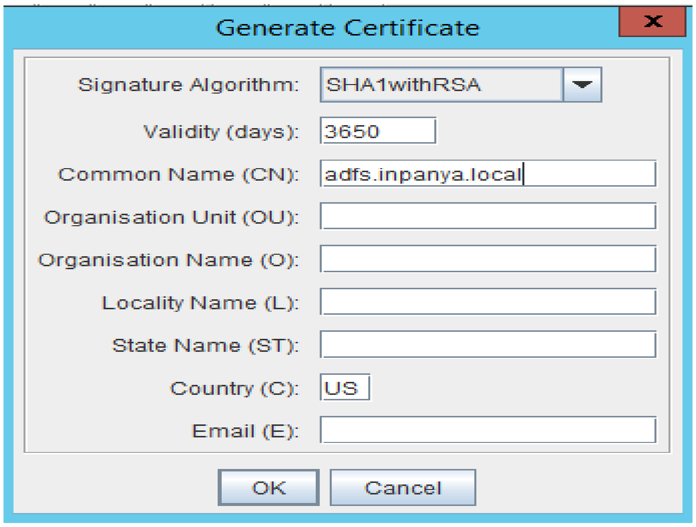
Files of Type: Java Keystore Files (*.jks;cacerts)

Keystore type: JKS, provider: SUN, size: 1 entry

Save file name:Tomcat8_5_4_key.jks

Import ADFS CA on the keystore

Create new keystore and save file name Composer_tomcat.jks



Signature Algorithm: SHA1withRSA

Validity (days): 3650

Common Name (CN): adfs.inpanya.local

Organisation Unit (OU):

Organisation Name (O):

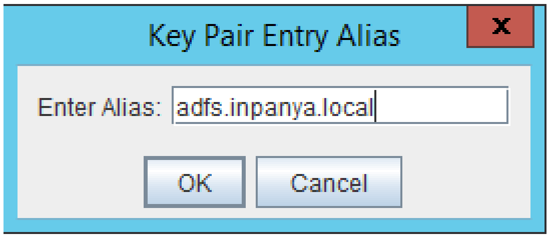
Locality Name (L):

State Name (ST):

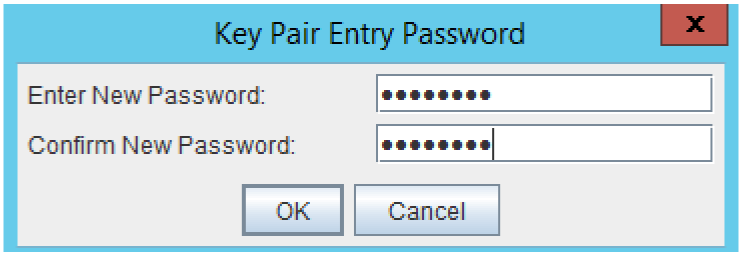
Country (C): US

Email (E):

CN:adfs.inpanya.local



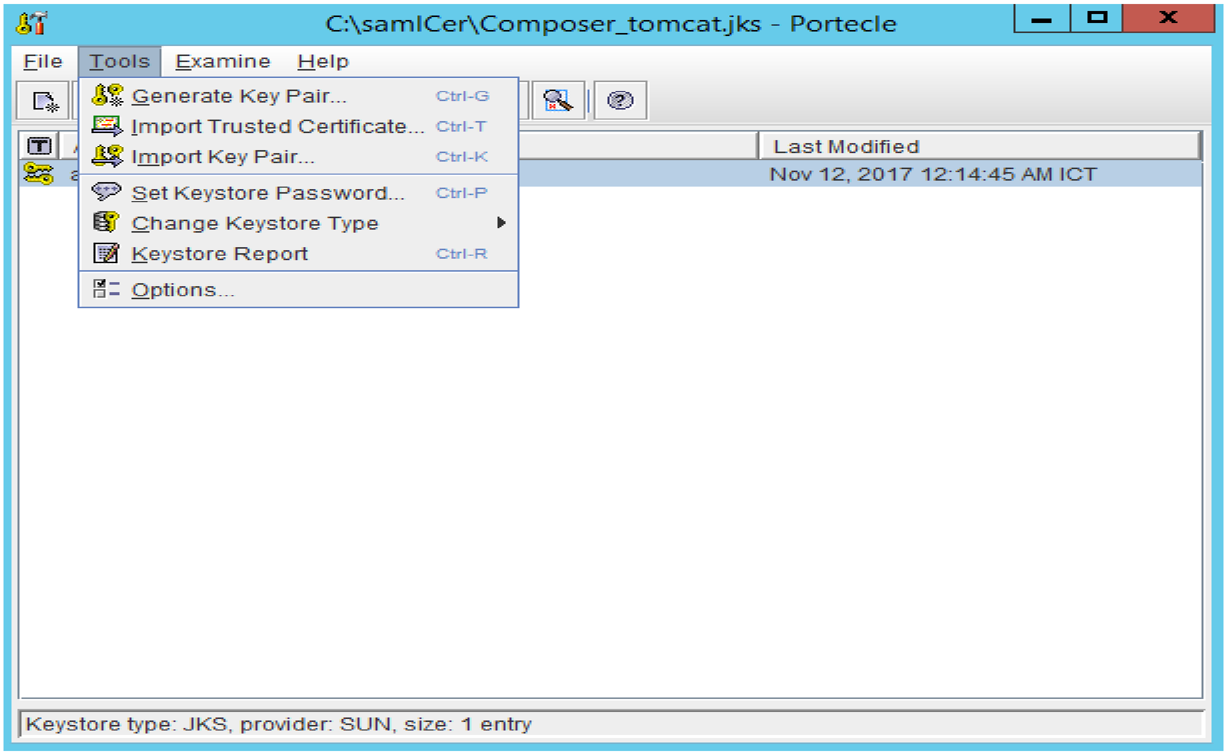
Enter Alias: adfs.inpanya.local



Enter New Password: ●●●●●●●●

Confirm New Password: ●●●●●●●●

Enter password:P@ssw0rd



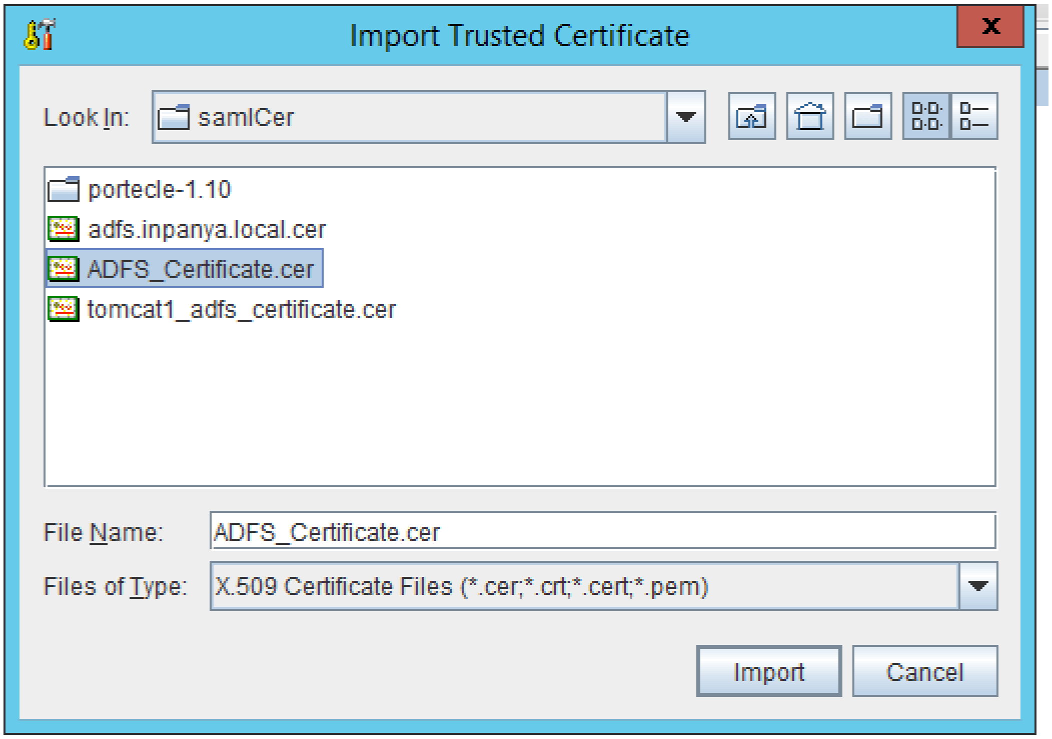
C:\samlCer\Composer_tomcat.jks - Portecle

File
Tools
Examine
Help
Generate Key Pair... Ctrl-G
Import Trusted Certificate... Ctrl-T
Import Key Pair... Ctrl-K
Set Keystore Password... Ctrl-P
Change Keystore Type
Keystore Report Ctrl-R
Options...
Last Modified

Nov 12, 2017 12:14:45 AM ICT

Keystore type: JKS, provider: SUN, size: 1 entry

Tools →Import Trusted Certificate



Import Trusted Certificate

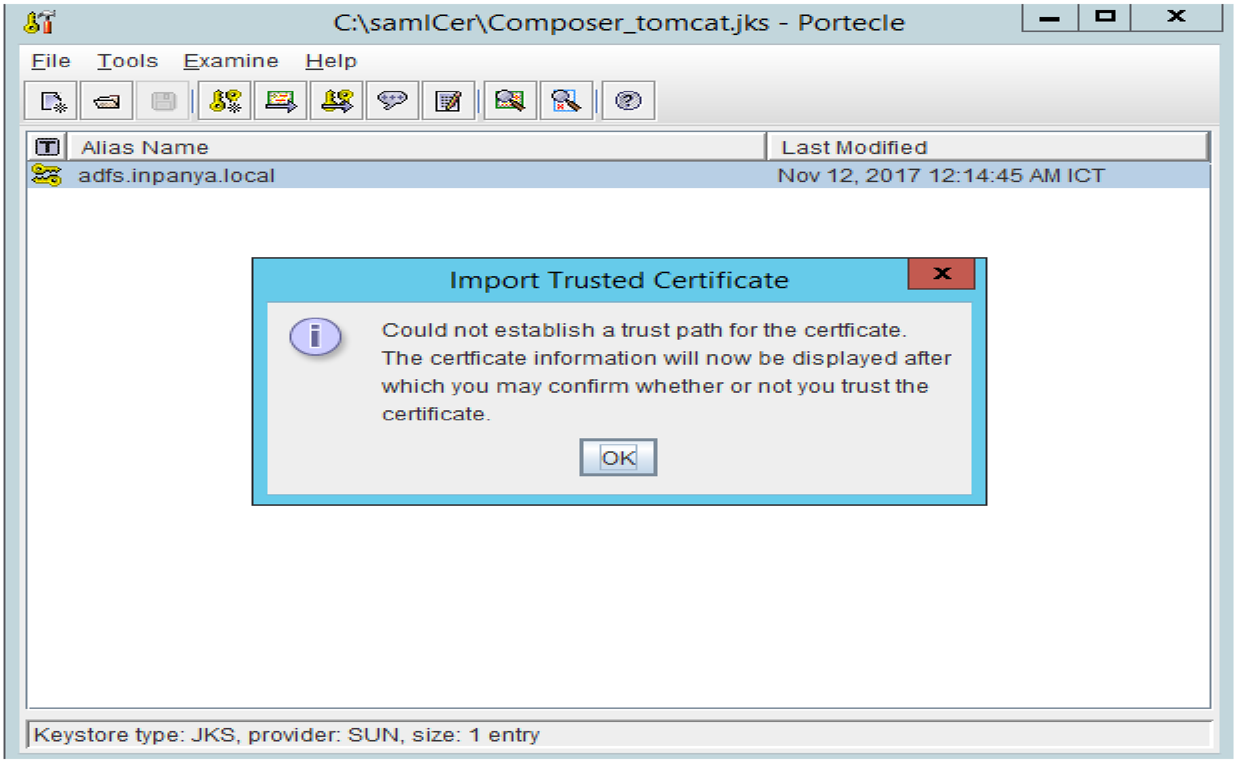
Look In: samlCer

portecle-1.10
adfs.inpanya.local.cer
ADFS_Certificate.cer
tomcat1_adfs_certificate.cer

File Name: ADFS_Certificate.cer

Files of Type: X.509 Certificate Files (*.cer;*.crt;*.cert;*.pem)

Selected ADFS_Certificate.cer (Copy this file from ADFS Server) then click Import



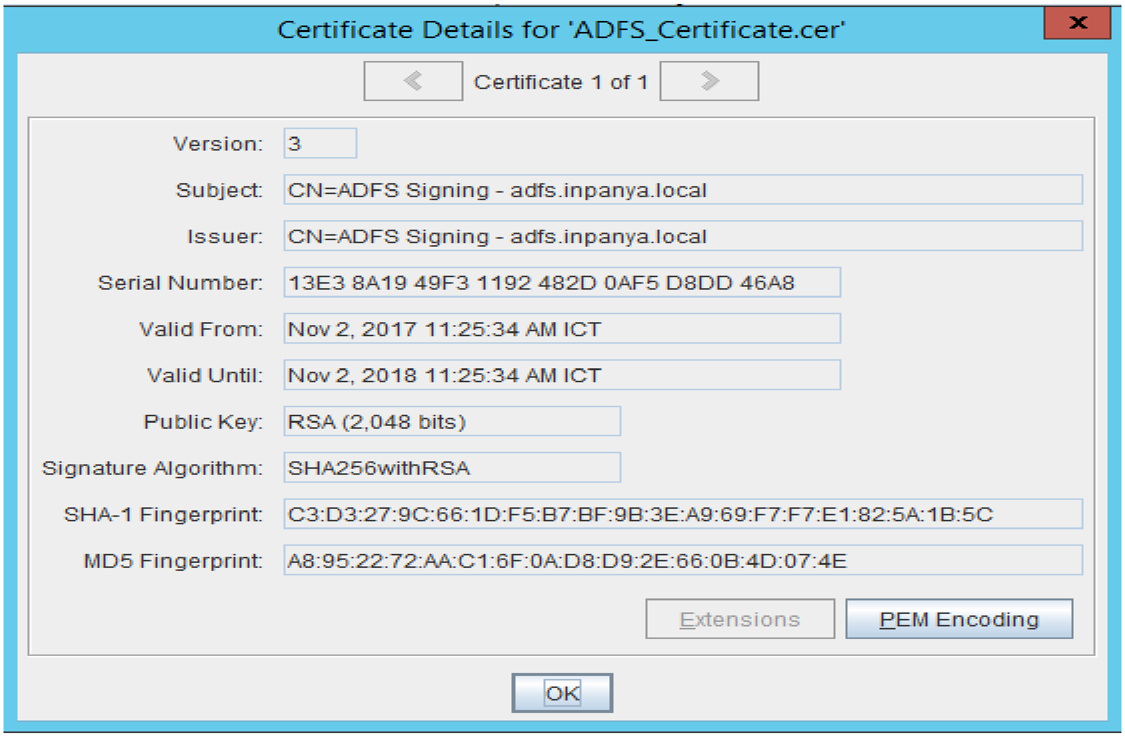
adfs.inpanya.local Nov 12, 2017 12:14:45 AM ICT

Import Trusted Certificate

Could not establish a trust path for the certficate. The certficate information will now be displayed after which you may confirm whether or not you trust the certificate.

Keystore type: JKS, provider: SUN, size: 1 entry

Click OK


Certificate Details for 'ADFS_Certificate.cer'

Certificate 1 of 1

Version: 3

Subject: CN=ADFS Signing - adfs.inpanya.local

Issuer: CN=ADFS Signing - adfs.inpanya.local

Serial Number: 13E3 8A19 49F3 1192 482D 0AF5 D8DD 46A8

Valid From: Nov 2, 2017 11:25:34 AM ICT

Valid Until: Nov 2, 2018 11:25:34 AM ICT

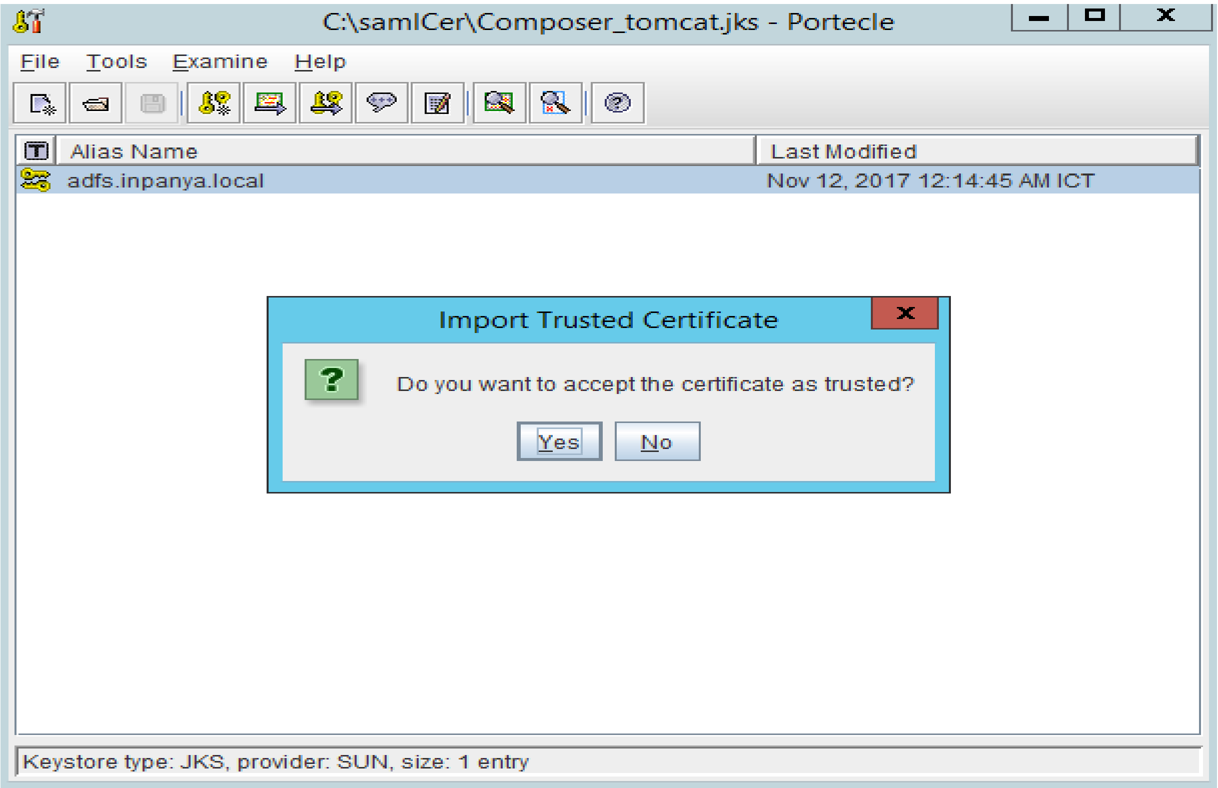
Public Key: RSA (2,048 bits)

Signature Algorithm: SHA256withRSA

SHA-1 Fingerprint: C3:D3:27:9C:66:1D:F5:B7:BF:9B:3E:A9:69:F7:F7:E1:82:5A:1B:5C

MD5 Fingerprint: A8:95:22:72:AA:C1:6F:0A:D8:D9:2E:66:0B:4D:07:4E

Click OK



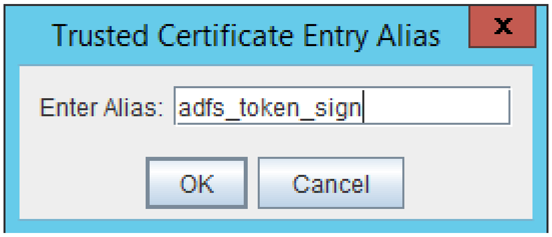
C:\samlCer\Composer_tomcat.jks - Portecle
File
Tools
Examine
Help
Alias Name
Last Modified
Import Trusted Certificate
Yes
No

adfs.inpanya.local Nov 12, 2017 12:14:45 AM ICT

Do you want to accept the certificate as trusted?

Keystore type: JKS, provider: SUN, size: 1 entry

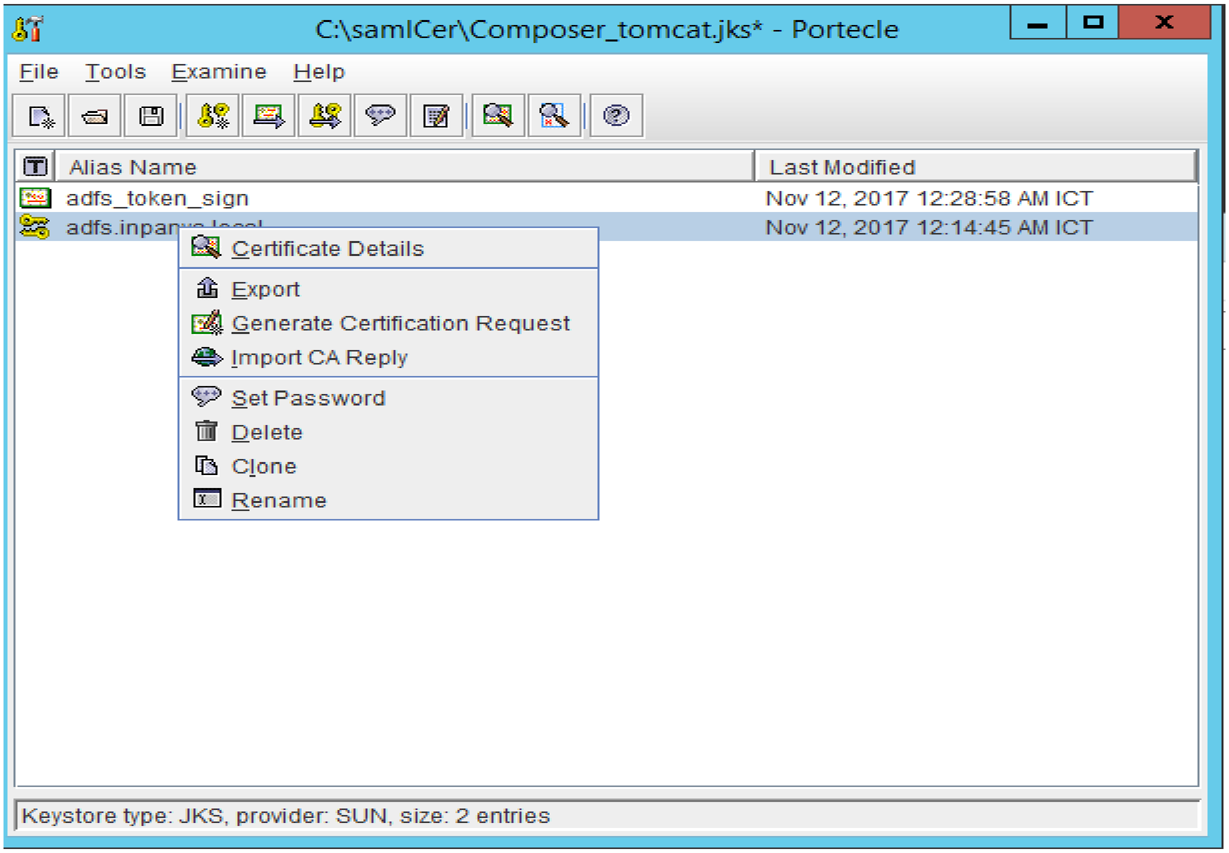
Click YES



Enter Alias: adfs_token_sign

Enter Alias:adfs_token_sign

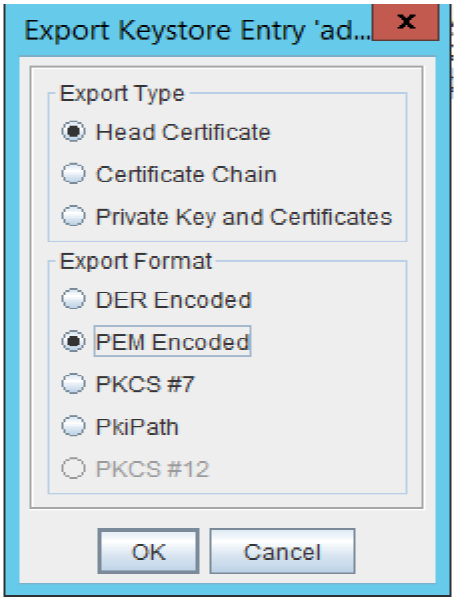
Export Certificate file



Alias Name	Last Modified
adfs_token_sign	Nov 12, 2017 12:28:58 AM ICT
adfs.inpanya.local	Nov 12, 2017 12:14:45 AM ICT

Keystore type: JKS, provider: SUN, size: 2 entries

Right click adfs.inpanya.local →Export



Export Type

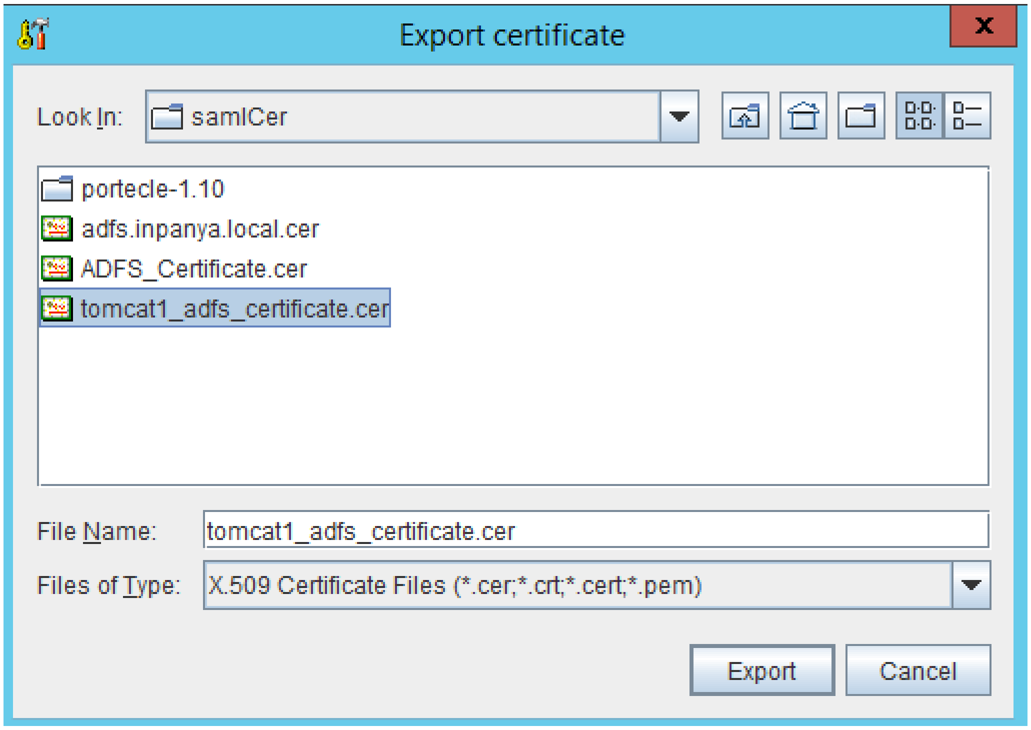
● Head Certificate
○ Certificate Chain
○ Private Key and Certificates

Export Format

○ DER Encoded
● PEM Encoded
○ PKCS #7
○ PkiPath
○ PKCS #12

Export Type:Head Certificate

Export Format:PEM Encoded



Look In: samlCer

File Name: tomcat1_adfs_certificate.cer

Files of Type: X.509 Certificate Files (*.cer;*.crt;*.cert;*.pem)

Save file name :tomcat1_adfs_certificate.cer   then click Export

Save and close Portecle

Tomcat Configuration

Add jar file to %TOMCAT_HOME%\lib

jboss-logging-3.0.0.GA.jar

jboss-security-spi-3.0.0.Final.jar

picketlink-common-2.7.1.Final.jar

picketlink-config-2.7.1.Final.jar

picketlink-federation-2.7.1.Final.jar

picketlink-tomcat7-2.7.1.Final.jar

picketlink-tomcat-common-8-2.7.1.Final.jar enable port 8443 (server.xml)

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
        maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
        enableLookups="false" disableUploadTimeout="true"
        acceptCount="100" scheme="https" secure="true"
        clientAuth="want"
        keystoreFile="C:/tomcat/security/ Tomcat8_5_4_key.jks "
        keystorePass="P@ssw0rd"
        truststoreFile=" C:/tomcat/security/ Tomcat8_5_4_key.jks "
        truststorePass="P@ssw0rd"
        sslProtocol="TLS"
        keyAlias="tomcat1.inpanya.local"
        />
```

Context.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<Context path="/samltest">
         <Valve
className="org.picketlink.identity.federation.bindings.tomcat.sp.ServiceProviderAuthenticator" />
</Context>
```

Web.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<web-app >
    <display-name>My Application</display-name>
    <description>My Web Application</description>
```

```
<servlet>
   <servlet-name>SSO</servlet-name>
   <servlet-class>com.saml.test.SSO</servlet-class>
</servlet>
<servlet-mapping>
   <servlet-name>SSO</servlet-name>
   <url-pattern>/SSO</url-pattern>
</servlet-mapping>

   <welcome-file-list>
   <welcome-file>index.jsp</welcome-file>
</welcome-file-list>

<security-constraint>
   <web-resource-collection>
      <web-resource-name>All Pages</web-resource-name>
      <url-pattern>/SSO</url-pattern>
   </web-resource-collection>
   <auth-constraint>
      <role-name>SAMLUser</role-name>
   </auth-constraint>
   <user-data-constraint>
      <transport-guarantee>CONFIDENTIAL</transport-guarantee>
   </user-data-constraint>
```

```
    </security-constraint>


       <security-role>

        <role-name>SAMLUser</role-name>

    </security-role>


</web-app>
```

Picketlink.xml

```
<?xml version="1.0" encoding="UTF-8"?>

<PicketLink xmlns="urn:picketlink:identity-federation:config:2.1">

    <PicketLinkSP xmlns="urn:picketlink:identity-federation:config:2.1"

            CanonicalizationMethod="http://www.w3.org/2001/10/xml-exc-c14n#"

            BindingType="POST"

            IDPUsesPostBindings="true"

            SupportsSignatures="true">

        <IdentityURL>https://adfs.inpanya.local/adfs/ls/</IdentityURL>

        <ServiceURL>https://tomcat1.inpanya.local:8443/samltest/SSO</ServiceURL>

        <Trust>

            <Domains>adfs.inpanya.local</Domains>

        </Trust>

                    <KeyProvider
ClassName="org.picketlink.identity.federation.core.impl.KeyStoreKeyManager">

                                   <!-- Path to keystore of certificates -->

                                   <Auth Key="KeyStoreURL" Value="C:/ tomcat/security/ Composer_tomcat.jks"
/>
```

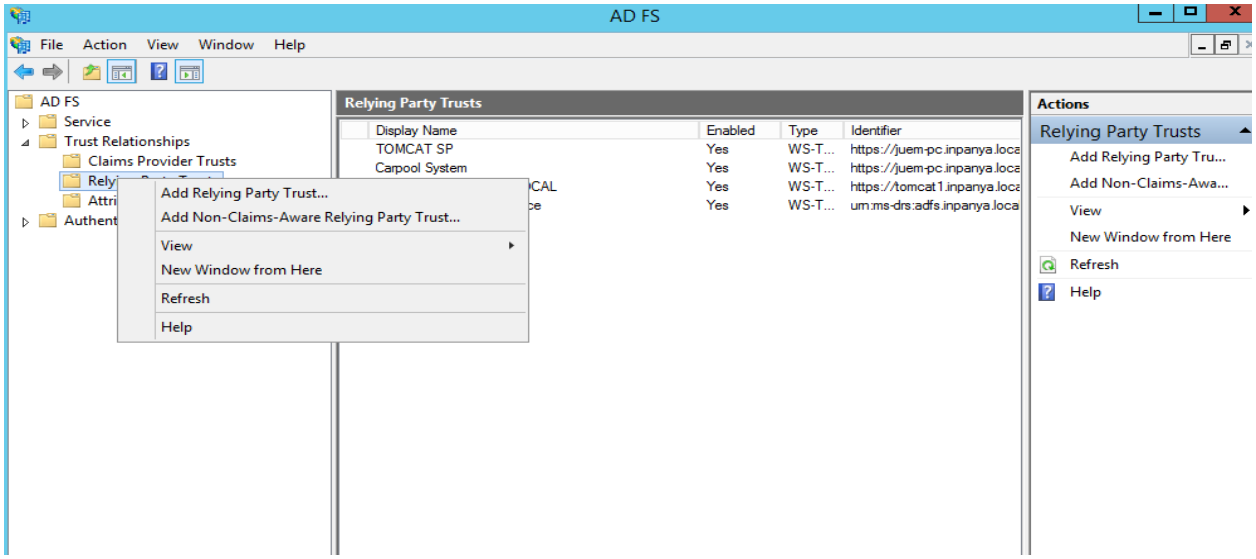
```
                  <Auth Key="KeyStorePass" Value="P@ssw0rd" />
                  <!-- Which certificate in the keystore do we use ourself for signing the SAML
AuthnRequest to the IDP? -->
                   <Auth Key="SigningKeyAlias" Value="adfs.inpanya.local" />
                  <Auth Key="SigningKeyPass" Value="P@ssw0rd" />
                  <!-- Every SAML Response from the IDP is/mustbe signed and the signing must
be checked to makeu
                  use the IDP can be trusted -->
                  <!-- Key=Domain name for which this certificate can be used to check the
signing -->
                  <!-- Value=Aliasname in keystore -->
                  <ValidatingAlias Key="adfs.inpanya.local" Value="adfs_token_sign" />
           </KeyProvider>
  </PicketLinkSP>
  <Handlers xmlns="urn:picketlink:identity-federation:handler:config:2.1">
    <Handler
class="org.picketlink.identity.federation.web.handlers.saml2.SAML2IssuerTrustHandler" />
    <Handler class="org.picketlink.identity.federation.web.handlers.saml2.SAML2LogOutHandler"
/>
    <Handler
class="org.picketlink.identity.federation.web.handlers.saml2.SAML2AuthenticationHandler">
      <Option Key="ROLE_KEY"
Value="http://schemas.microsoft.com/ws/2008/06/identity/claims/role"/>
    </Handler>
    <Handler
class="org.picketlink.identity.federation.web.handlers.saml2.RolesGenerationHandler" />
  </Handlers>
</PicketLink>
```

sso.jsp

```
<%--
    Document   : index
    Created on : Oct 19, 2017, 1:37:45 PM
    Author     : JUEM
--%>

<%@page contentType="text/html" pageEncoding="UTF-8"%>
<!DOCTYPE html>
<html>
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
        <title>SSO Page</title>
    </head>
    <body>
        <h1>Hello World!</h1>
<%
       String userId = null;
if (request.getUserPrincipal() != null){
  userId = request.getUserPrincipal().getName();
}else{
  userId = request.getRemoteUser();
}

if (userId == null){
  userId = "World";
}

String message = "Hello, " + userId;

System.out.println("UserPrincipal:"+request.getUserPrincipal());

%>
            <h2><%= message%></h2>
            <h2><%= request.getUserPrincipal()%></h2>

  </body>
</html>
```

**** Switch to ADFS Server ****

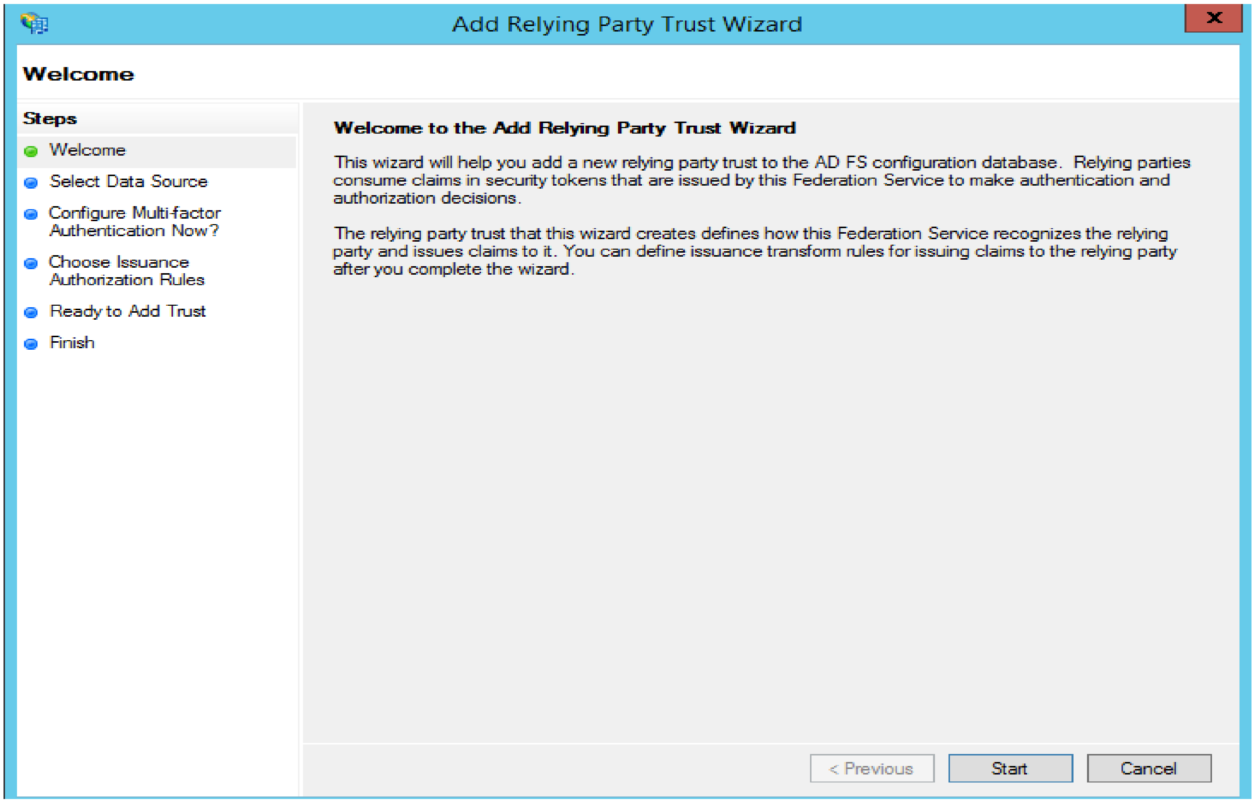
Add Relying party trust



Relying Party Trusts

Display Name	Enabled	Type	Identifier
TOMCAT SP	Yes	WS-T...	https://juem-pc.inpanya.loca
Carpool System	Yes	WS-T...	https://juem-pc.inpanya.loca
CAL	Yes	WS-T...	https://tomcat1.inpanya.loca
ce	Yes	WS-T...	urn:ms-drs:adfs.inpanya.loca

On the AD FS Management. Right click Relying Party Trust →Add Relying Party Trust



Add Relying Party Trust Wizard

Welcome

Steps

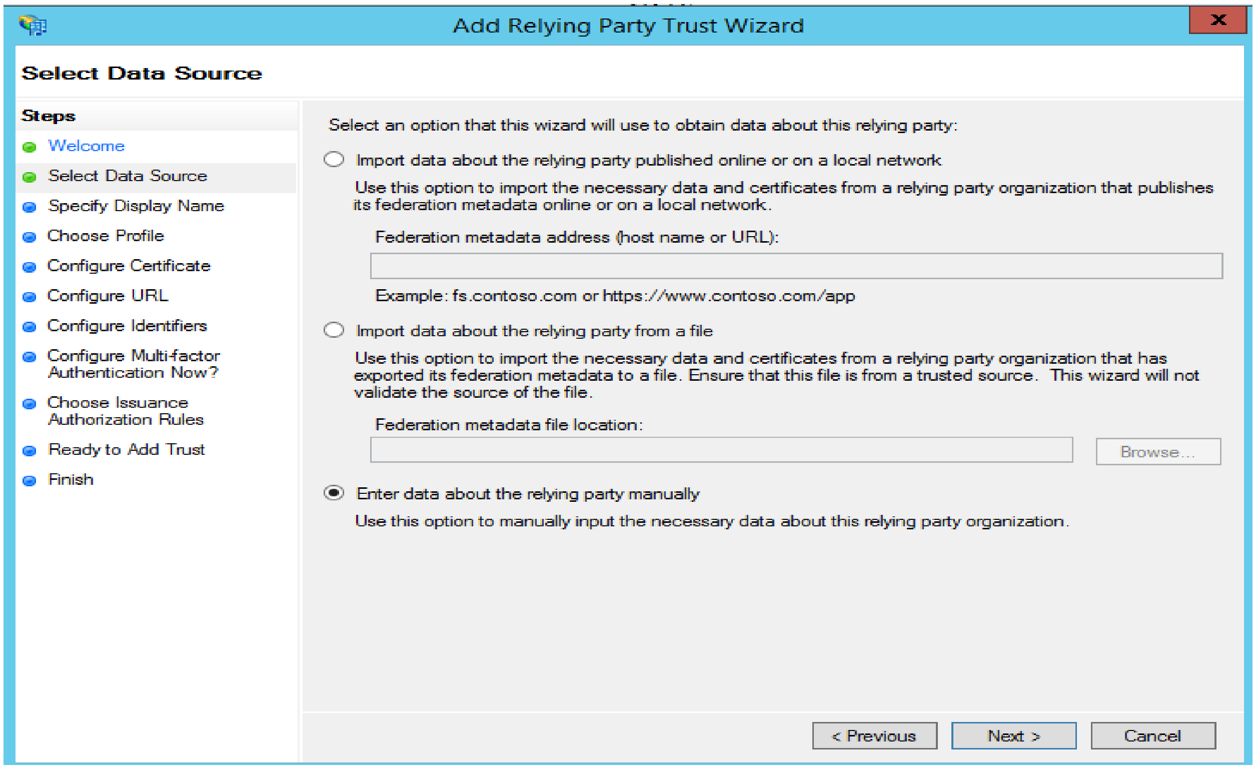
- Welcome
- Select Data Source
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Welcome to the Add Relying Party Trust Wizard

This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions.

The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.

Click Start



Add Relying Party Trust Wizard

Select Data Source

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

○ Import data about the relying party from a file

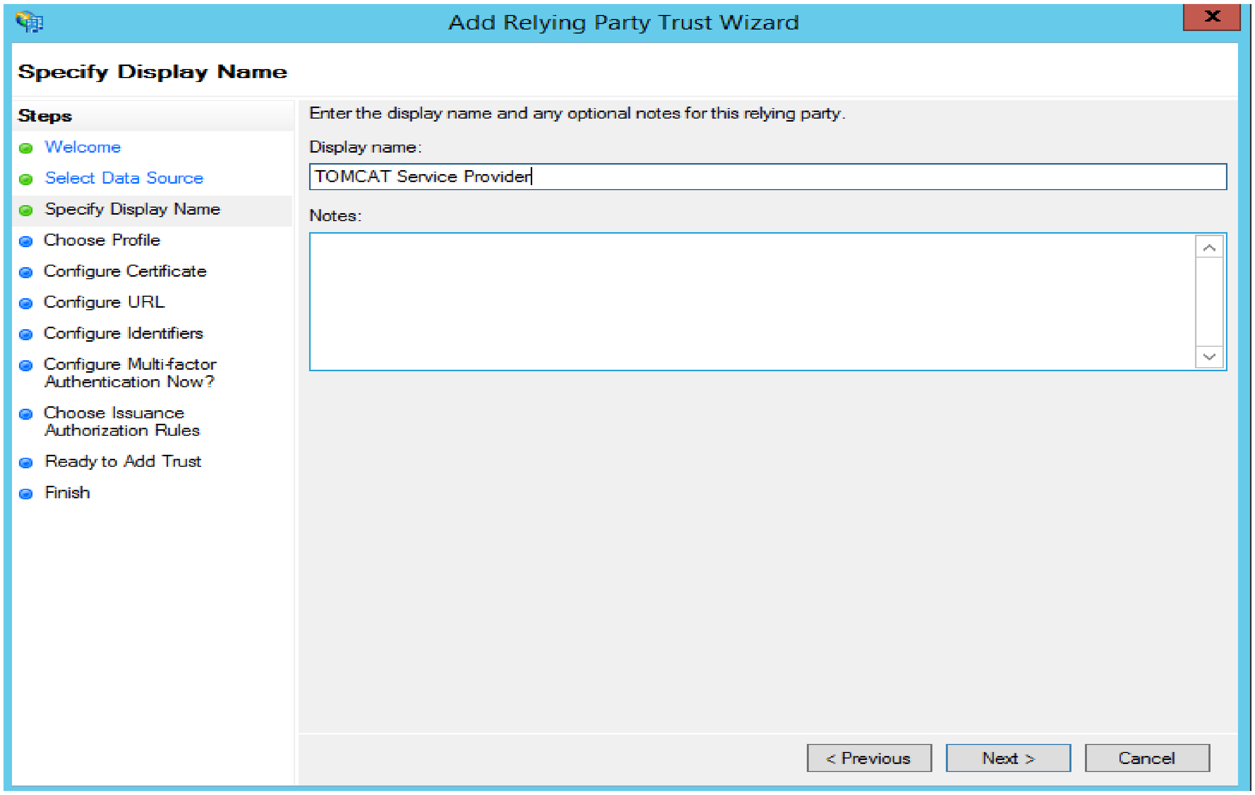
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

● Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

Selected Enter data about the relying party manually then click Next



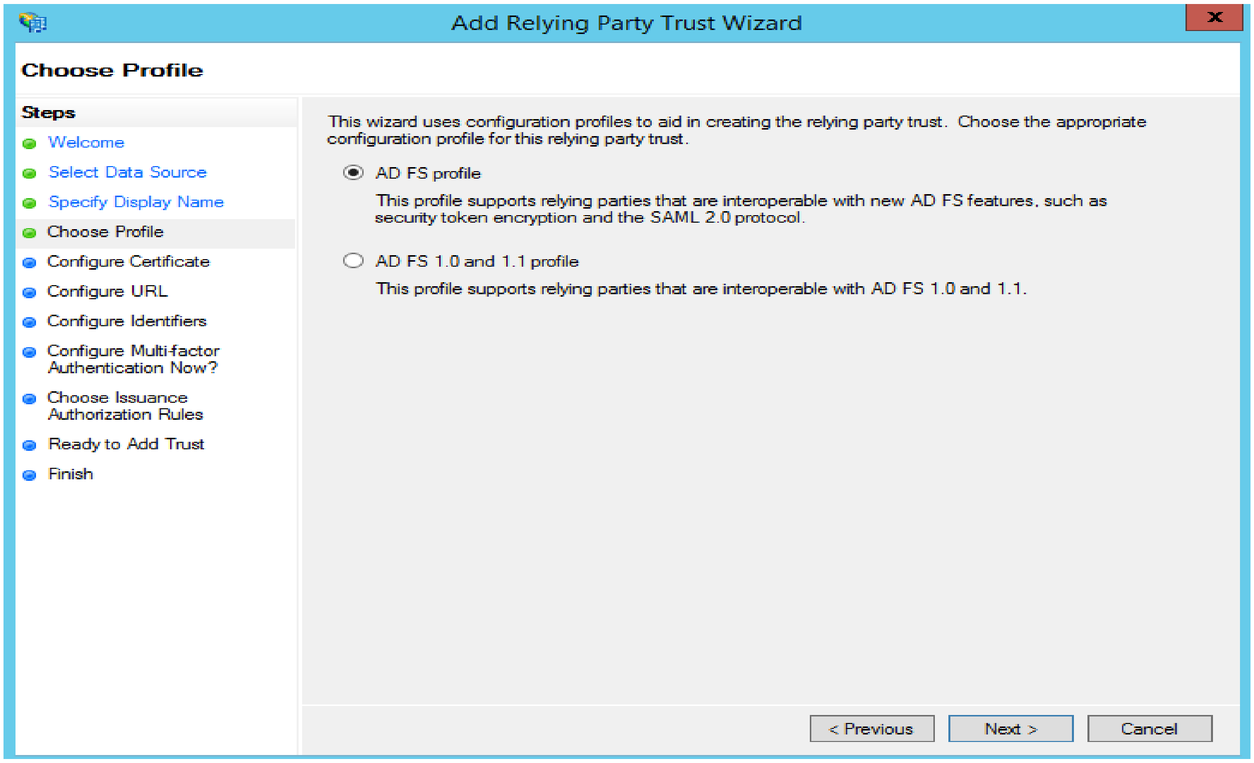
Specify Display Name

Enter the display name and any optional notes for this relying party.

Display name: TOMCAT Service Provider

Notes:

Enter display name then click Next



Choose Profile

This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust.

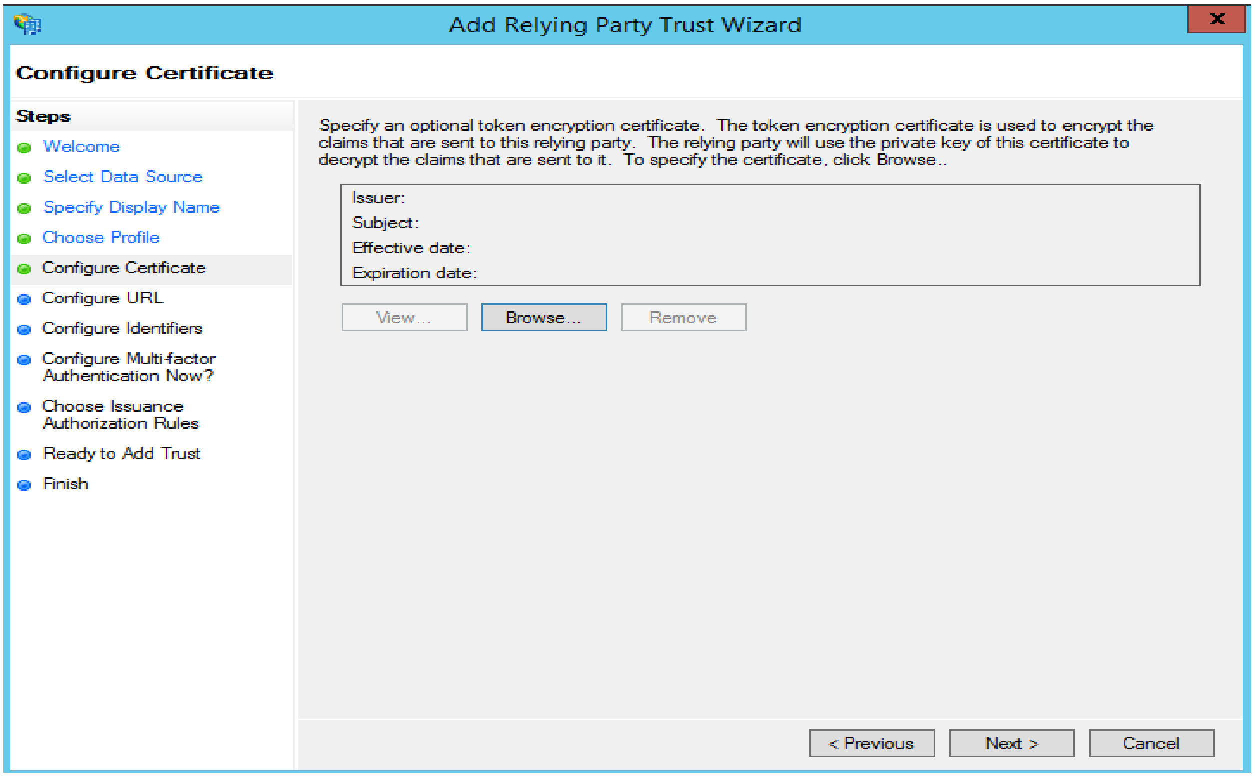
● AD FS profile

This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol.

○ AD FS 1.0 and 1.1 profile

This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.

Click Next

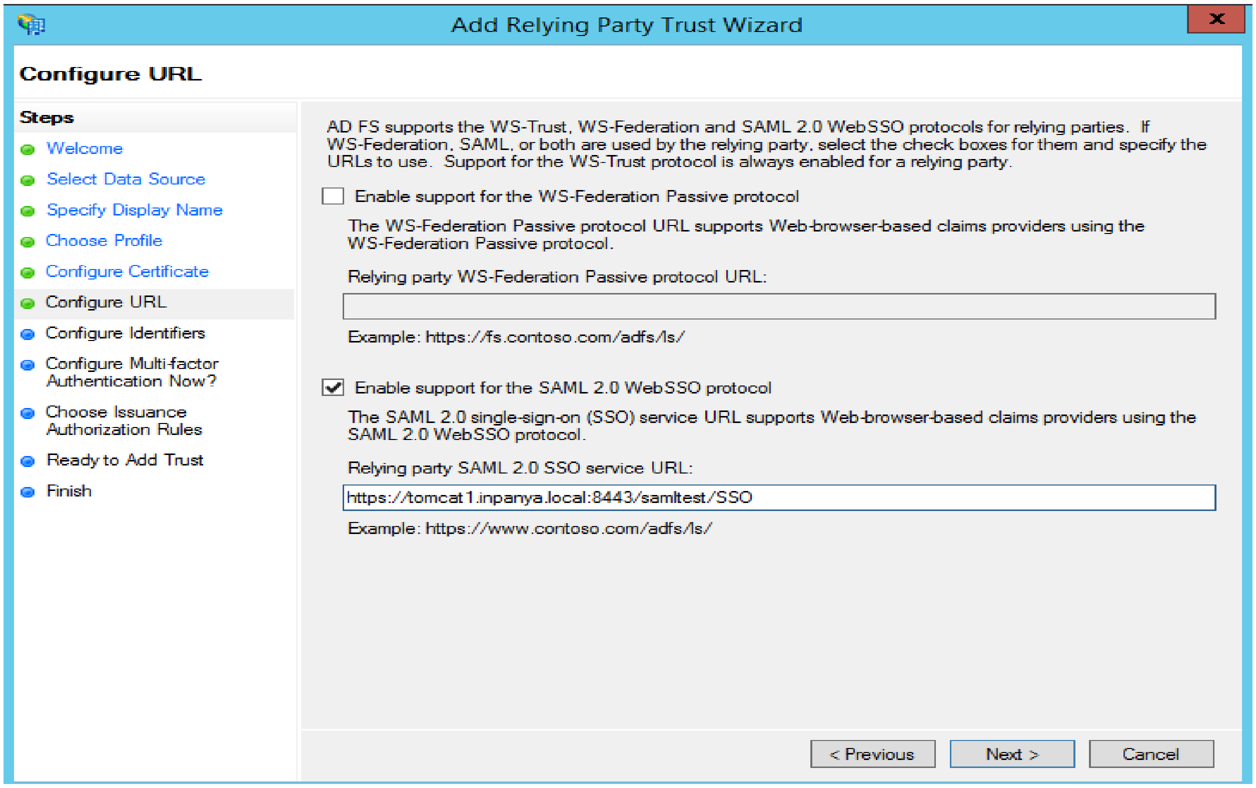


Configure Certificate

Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse..

Issuer:
Subject:
Effective date:
Expiration date:

Click Next



Configure URL

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

□ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: https://fs.contoso.com/adfs/ls/

☑ Enable support for the SAML 2.0 WebSSO protocol

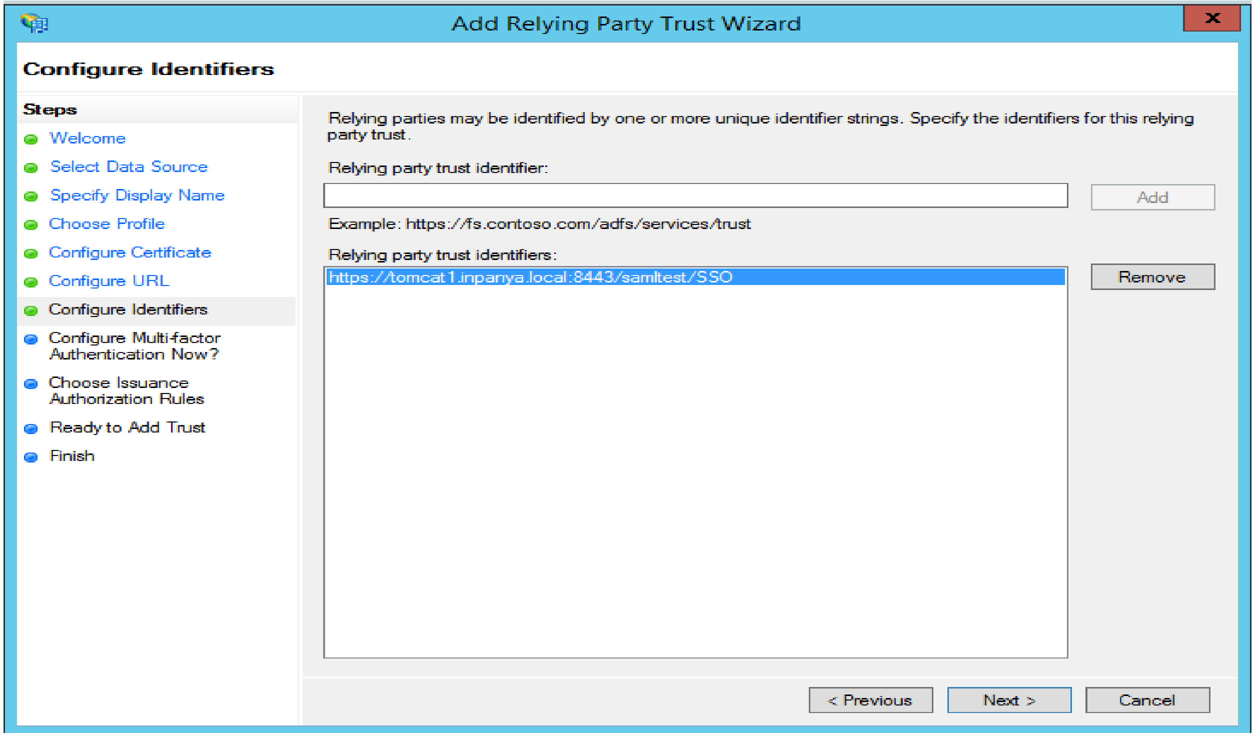
The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:

https://tomcat1.inpanya.local:8443/samltest/SSO

Example: https://www.contoso.com/adfs/ls/

Relying party SAML2.0 SSO service URL: https://tomcat1.inpanya.local:8443/samltest/SSO



Configure Identifiers

Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

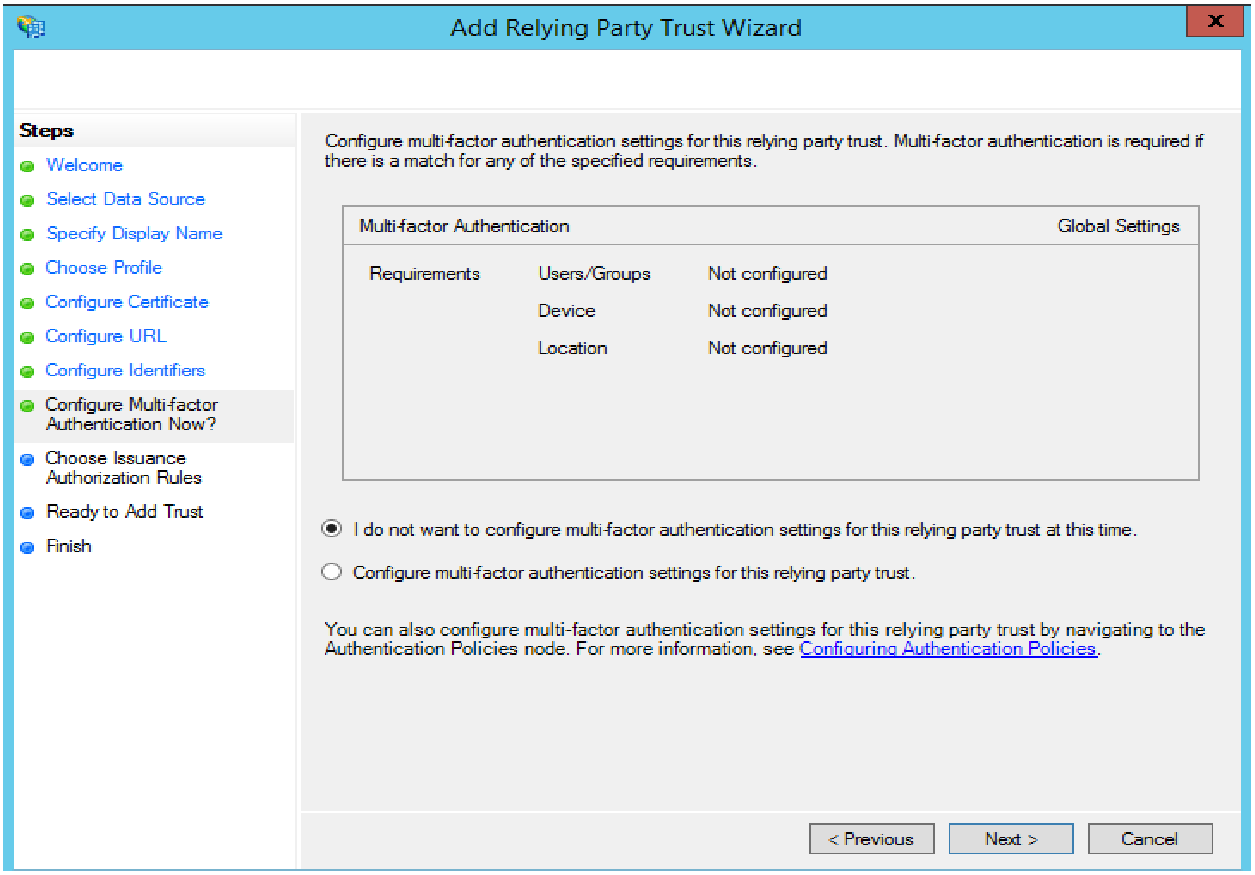
Relying party trust identifier:

Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:

https://tomcat1.inpanya.local:8443/samltest/SSO

Relying party trust identifiers: https://tomcat1.inpanya.local:8443/samltest/SSO



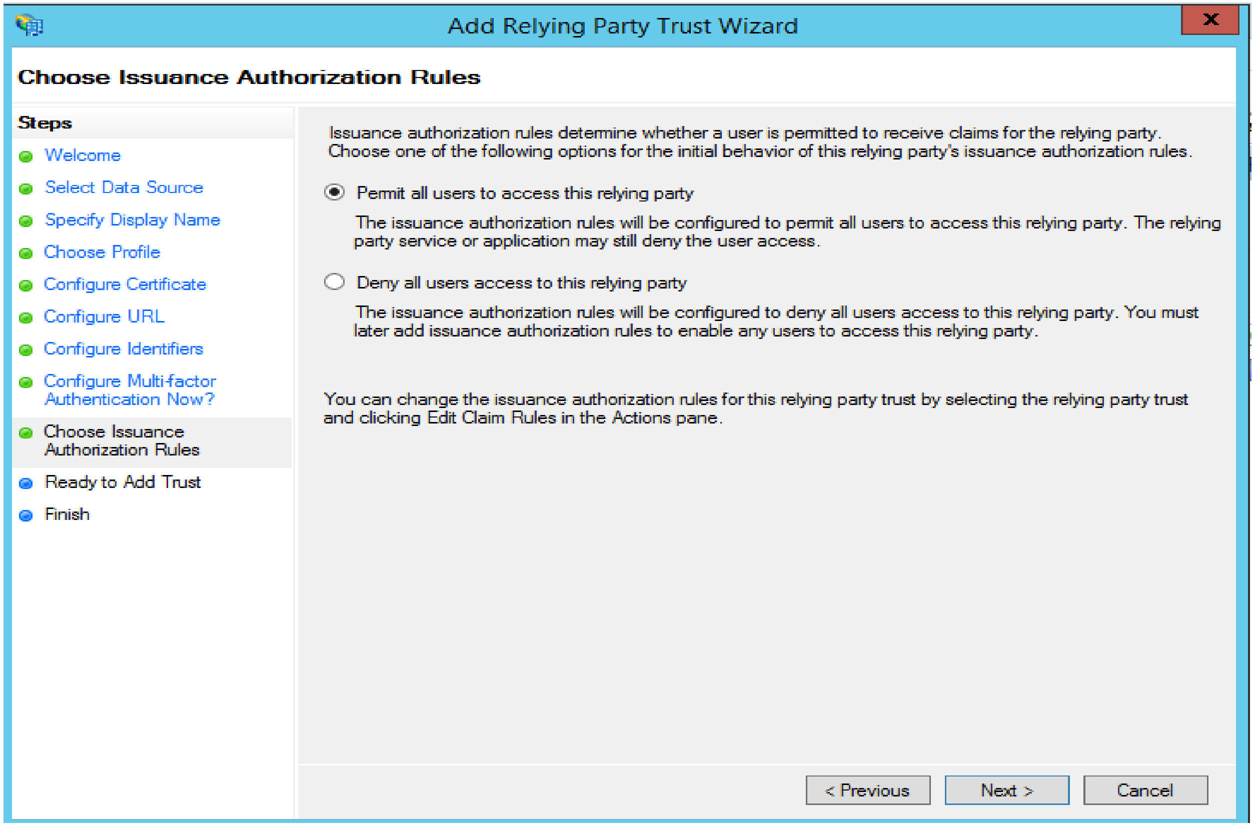
Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

Multi-factor Authentication		Global Settings
Requirements	Users/Groups	Not configured
	Device	Not configured
	Location	Not configured

● I do not want to configure multi-factor authentication settings for this relying party trust at this time.

○ Configure multi-factor authentication settings for this relying party trust.

You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see Configuring Authentication Policies.



Choose Issuance Authorization Rules

Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

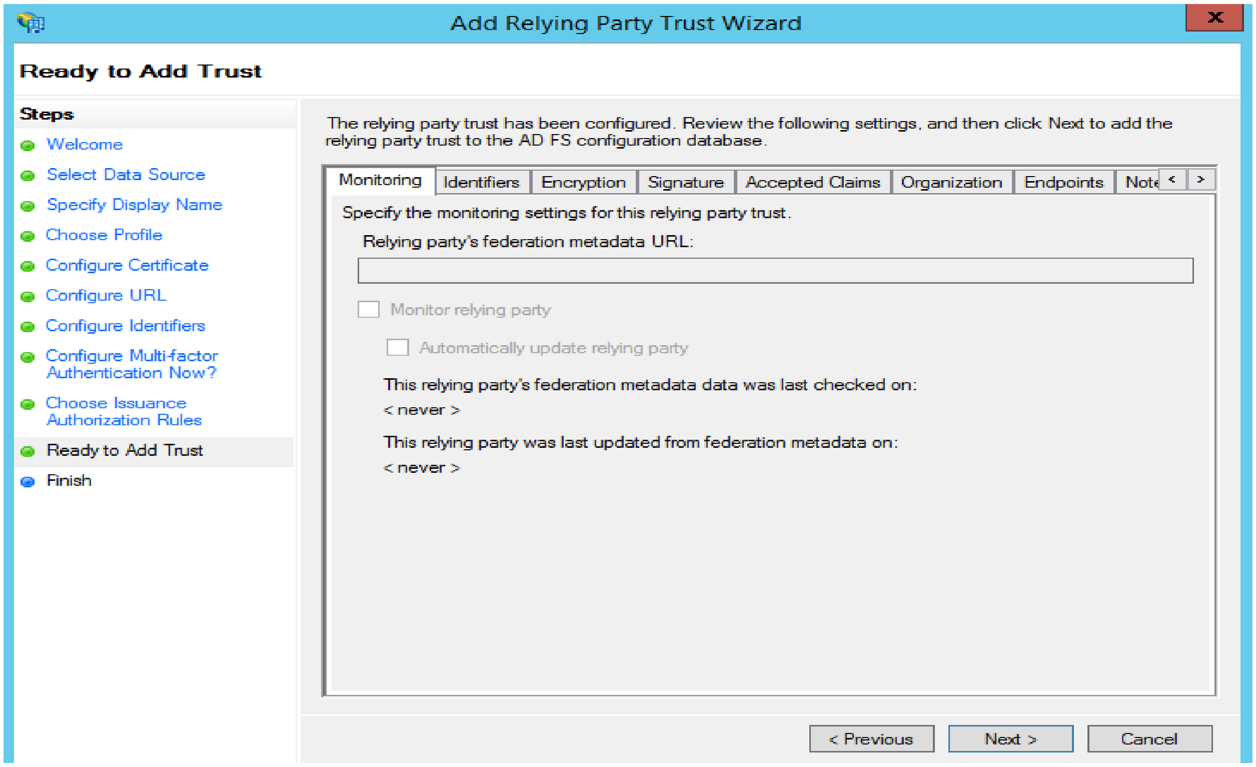
● Permit all users to access this relying party

The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

○ Deny all users access to this relying party

The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.



Ready to Add Trust

The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

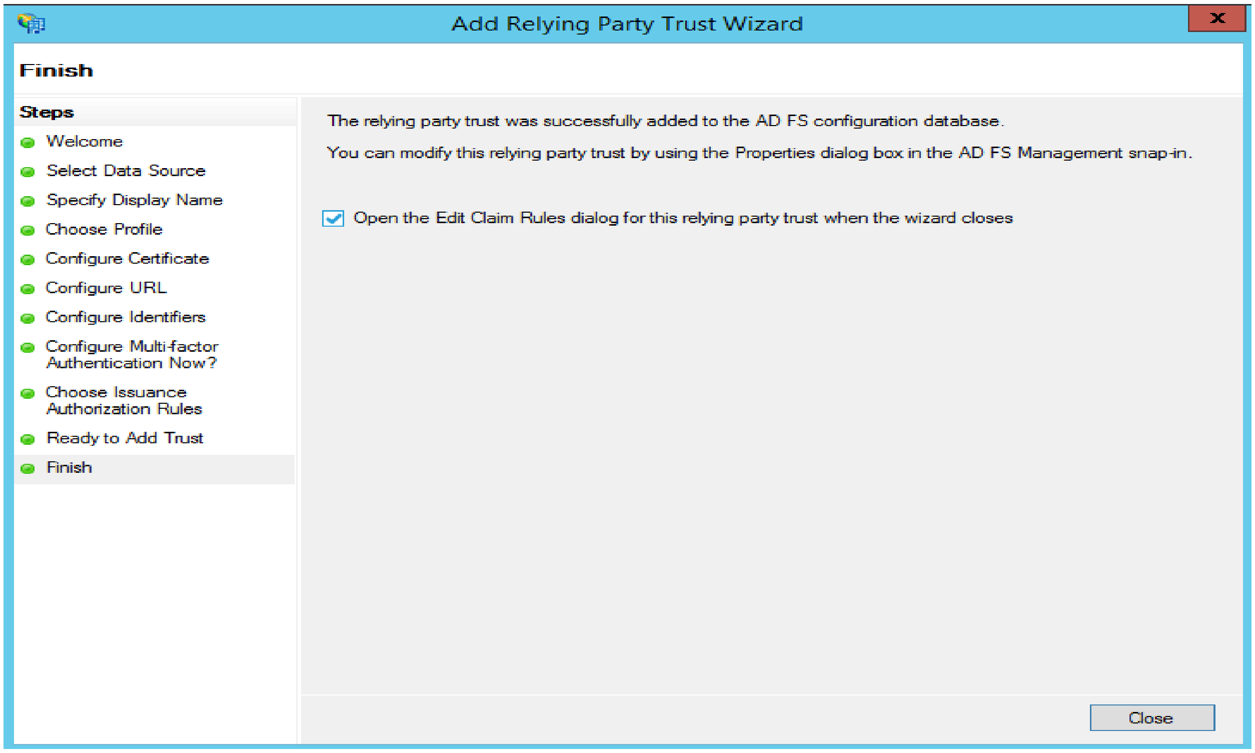
□ Monitor relying party

□ Automatically update relying party

This relying party's federation metadata data was last checked on:
< never >

This relying party was last updated from federation metadata on:
< never >

Click Next

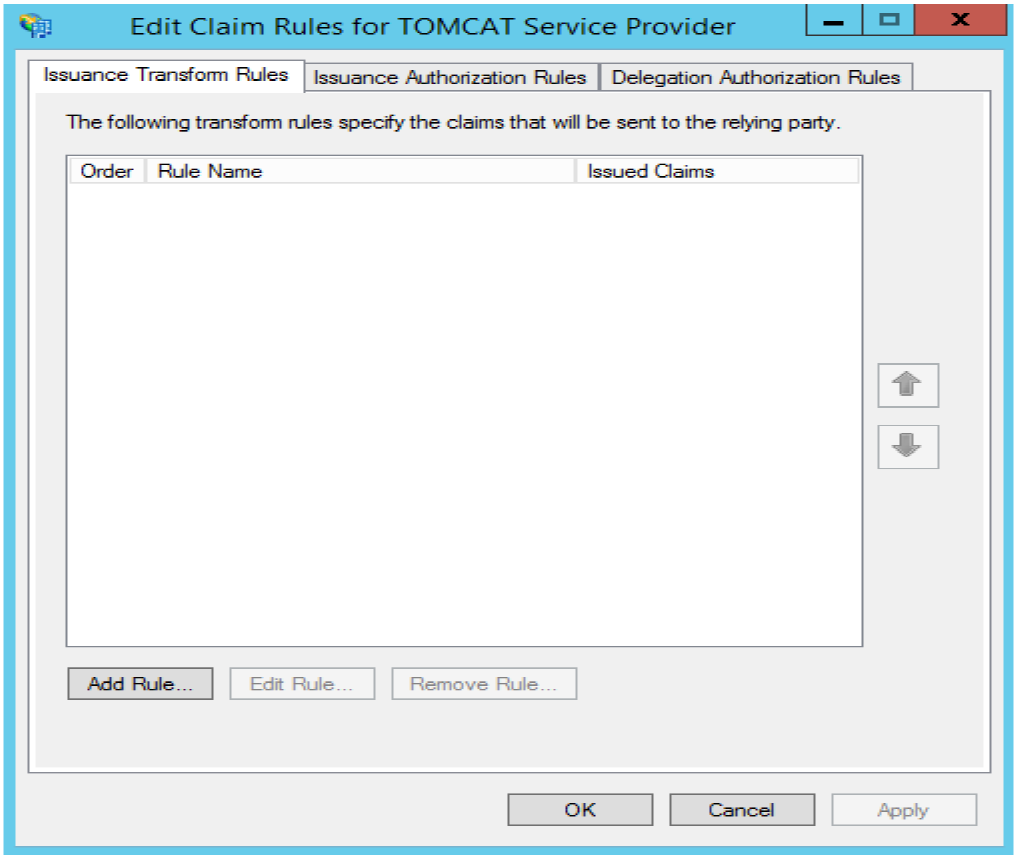


The relying party trust was successfully added to the AD FS configuration database.

You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in.

☑ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes

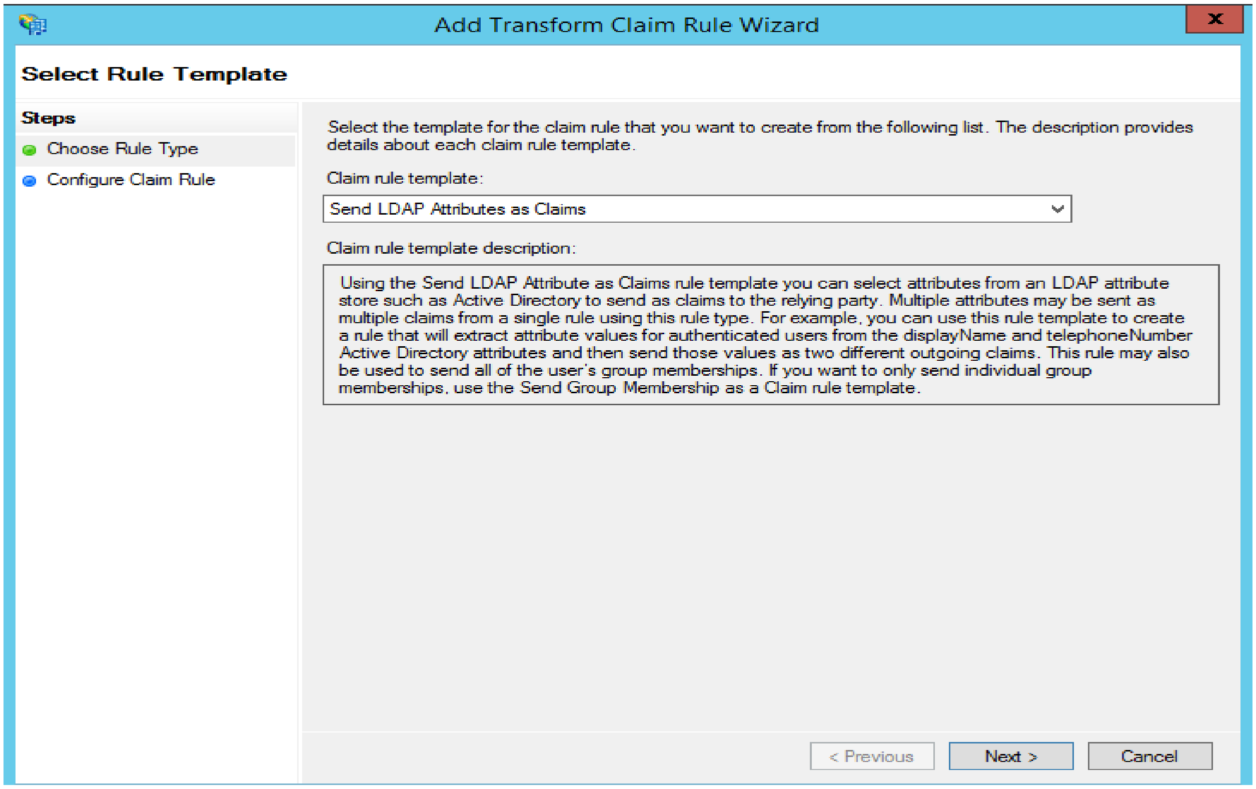
Click Close


Edit Claim Rules for TOMCAT Service Provider
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims

Click Add Rule



Select Rule Template

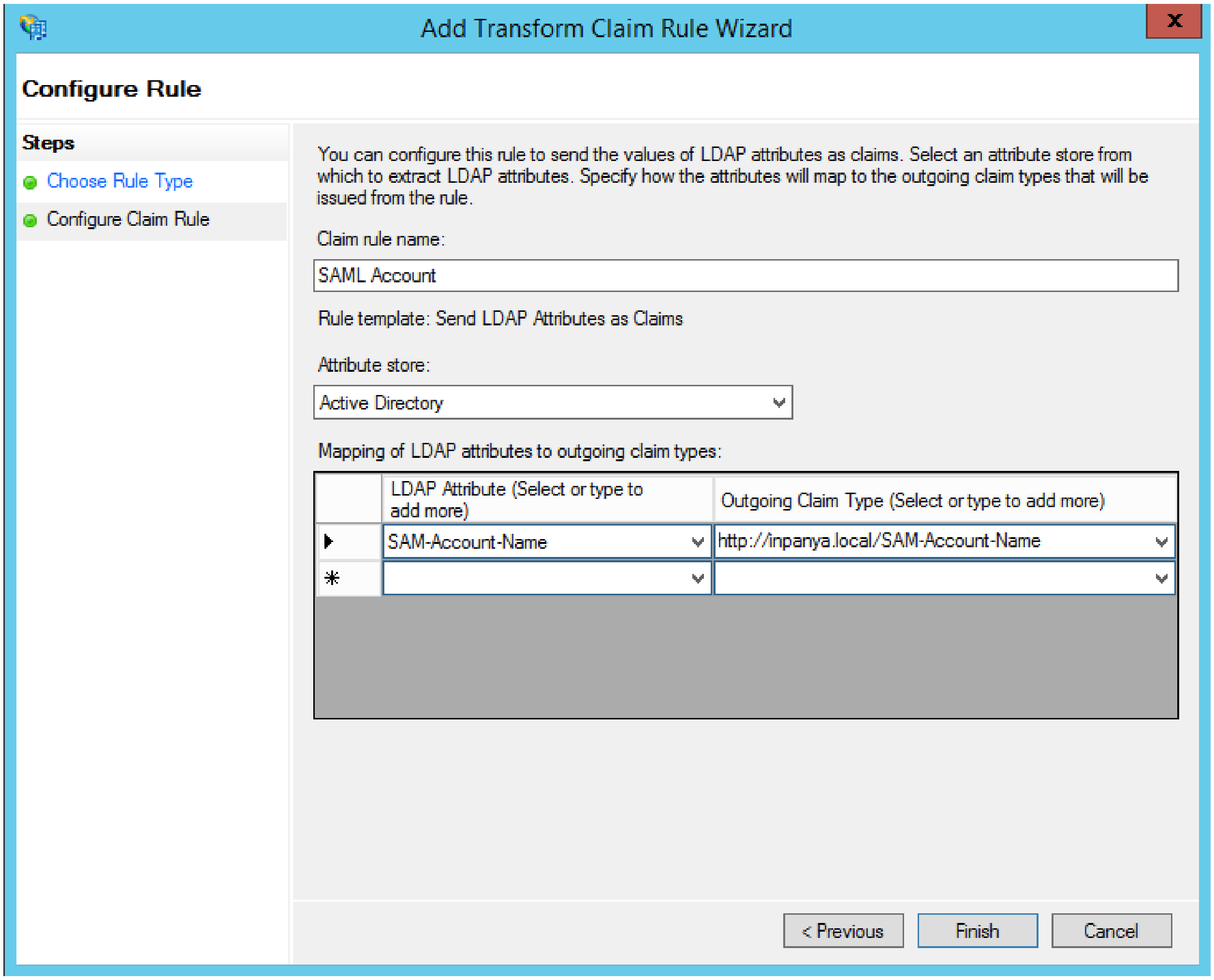
Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

Claim rule template:Send LDAP Attributes as Claims



You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: SAML Account

Rule template: Send LDAP Attributes as Claims

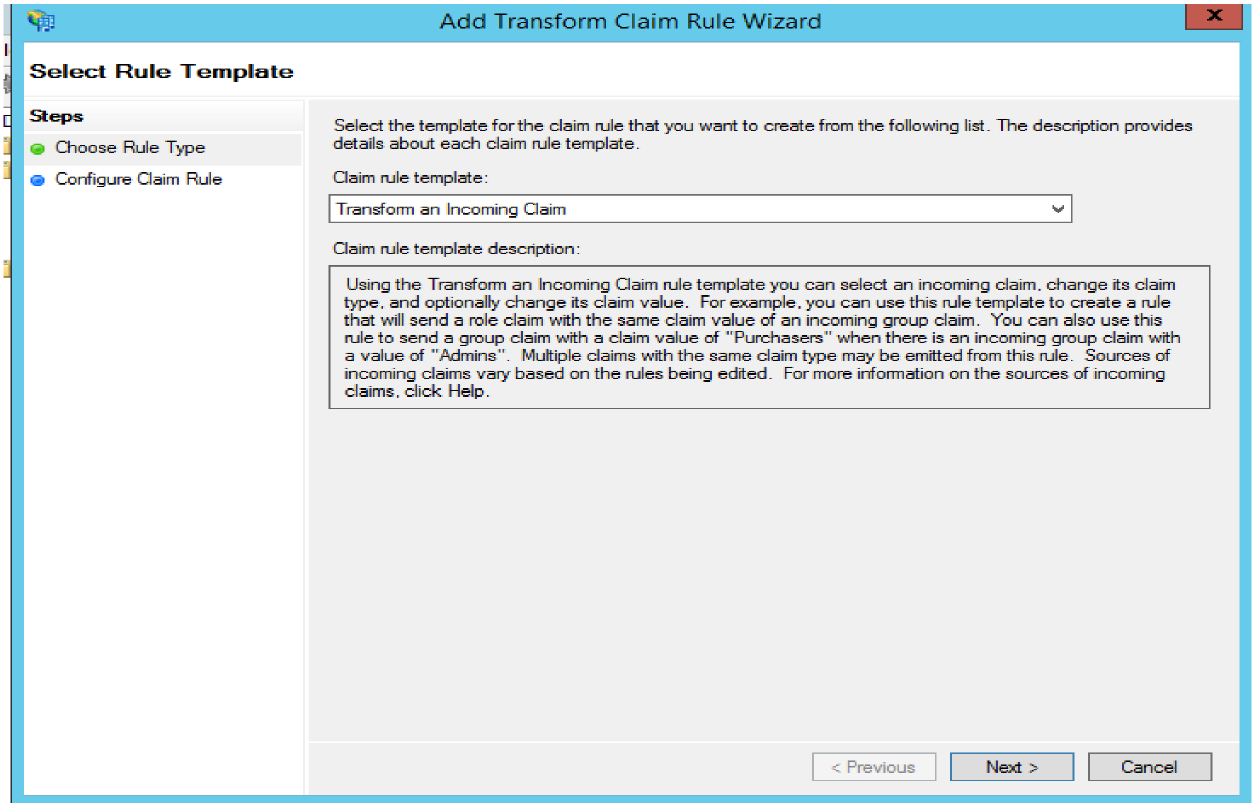
Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	SAM-Account-Name	http://inpanya.local/SAM-Account-Name
*		

Click Finish

Add new Rule



Select Rule Template

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

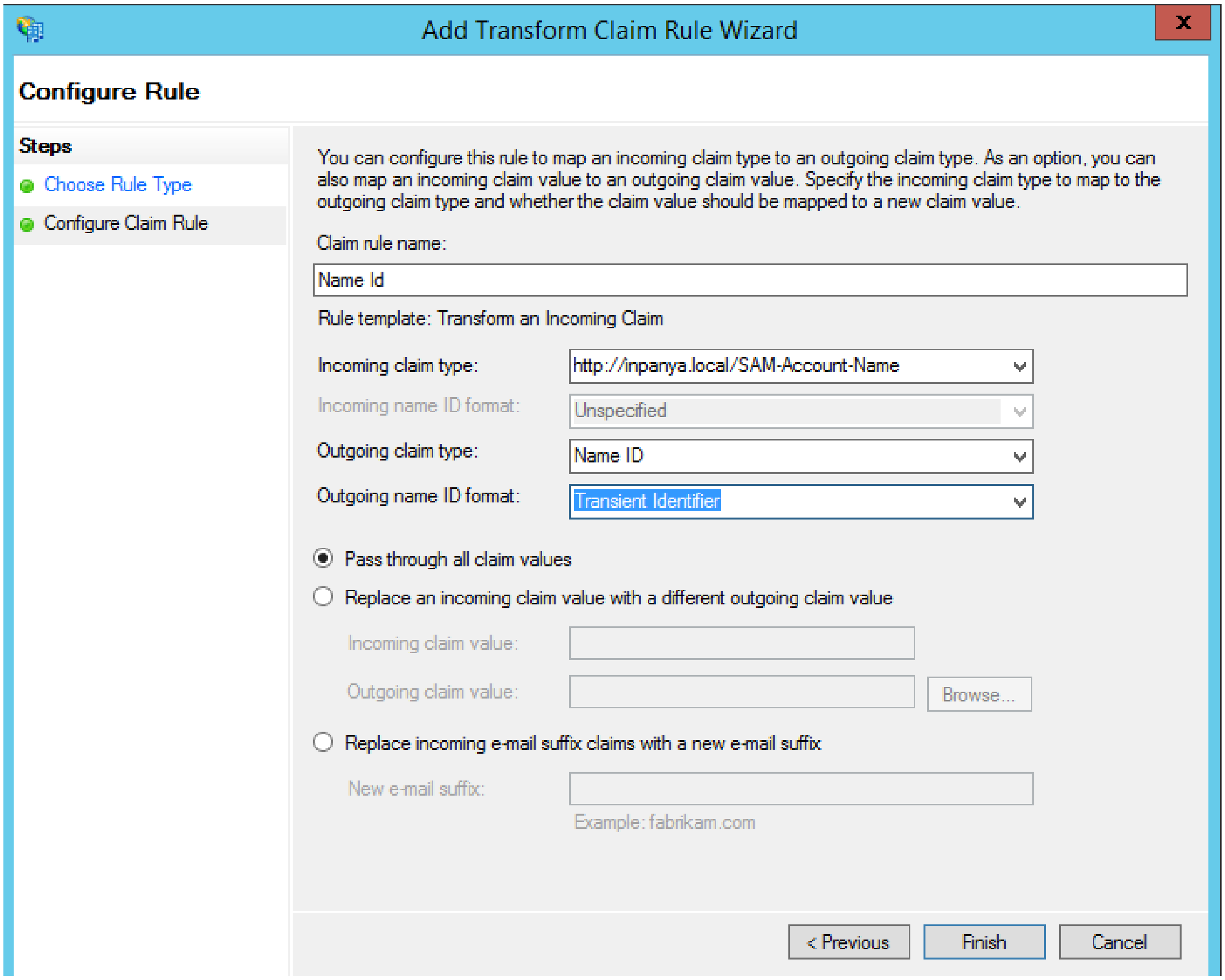
Claim rule template:

Transform an Incoming Claim

Claim rule template description:

Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited. For more information on the sources of incoming claims, click Help.

Claim rule template:Transform an Incoming Claim



Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Name Id

Rule template: Transform an Incoming Claim

Incoming claim type: http://inpanya.local/SAM-Account-Name

Incoming name ID format: Unspecified

Outgoing claim type: Name ID

Outgoing name ID format: Transient Identifier

● Pass through all claim values

○ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

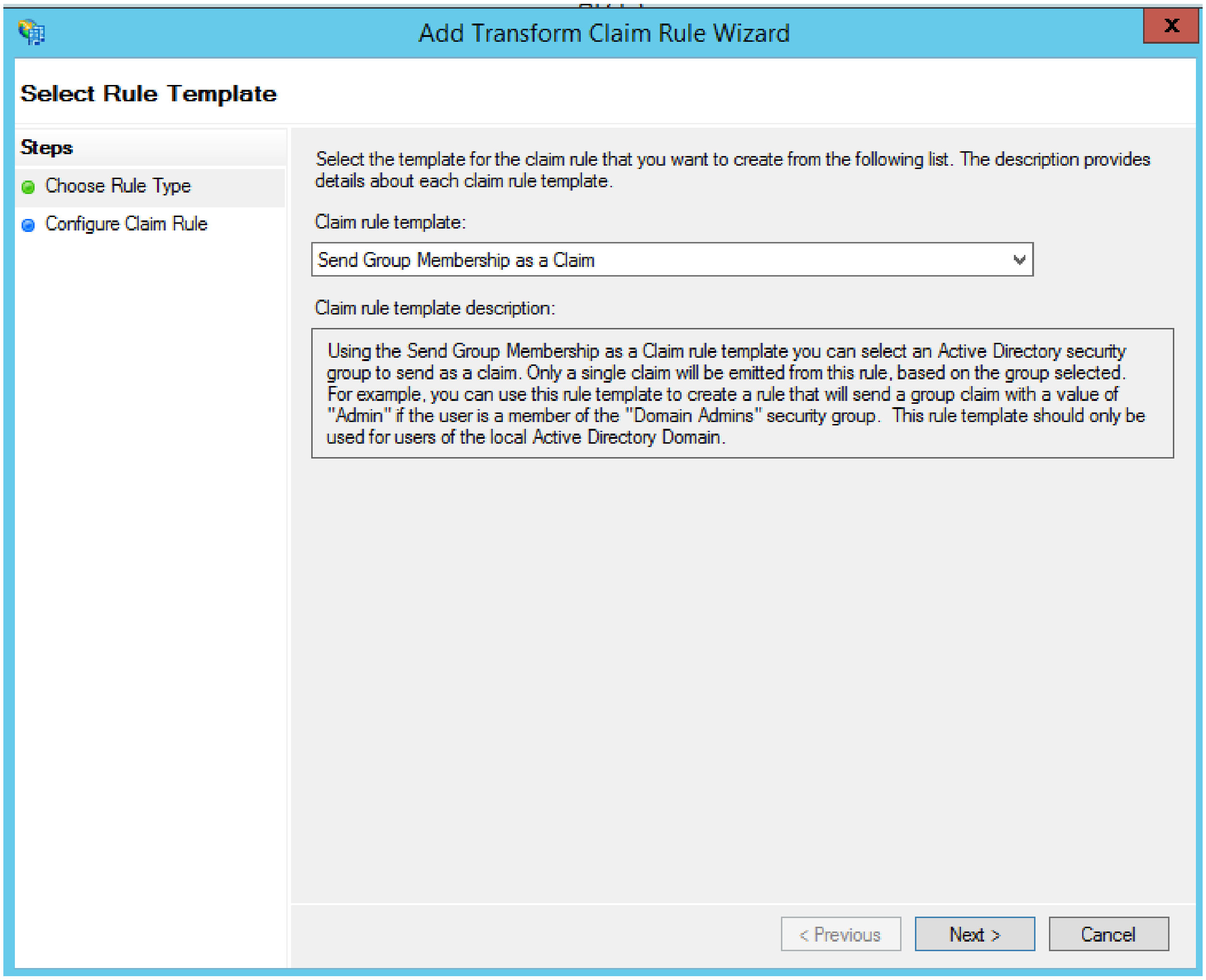
○ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

Click Finish

Add new Rule



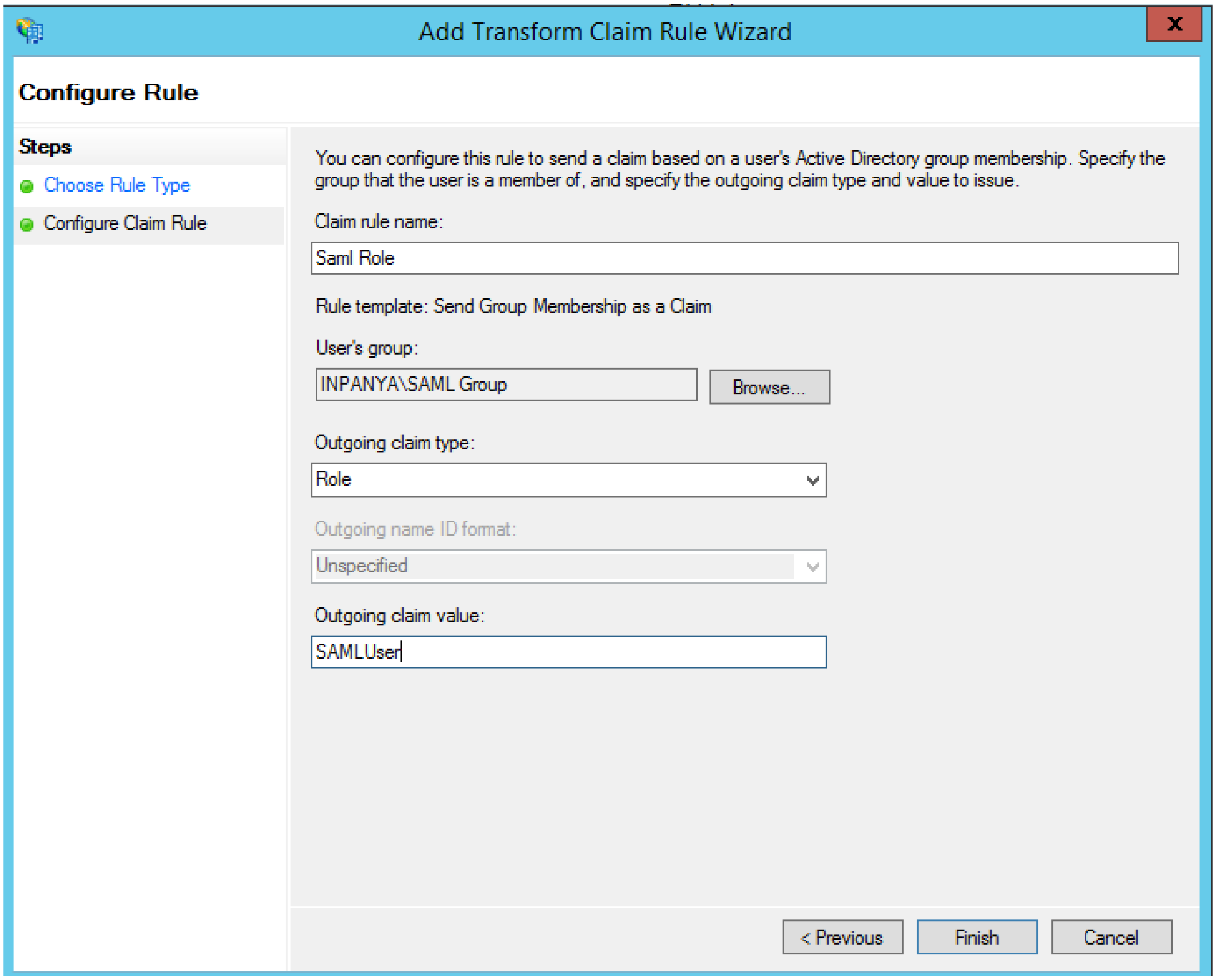
Select Rule Template

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Send Group Membership as a Claim

Claim rule template description:

Using the Send Group Membership as a Claim rule template you can select an Active Directory security group to send as a claim. Only a single claim will be emitted from this rule, based on the group selected. For example, you can use this rule template to create a rule that will send a group claim with a value of "Admin" if the user is a member of the "Domain Admins" security group. This rule template should only be used for users of the local Active Directory Domain.



You can configure this rule to send a claim based on a user's Active Directory group membership. Specify the group that the user is a member of, and specify the outgoing claim type and value to issue.

Claim rule name: Saml Role

Rule template: Send Group Membership as a Claim

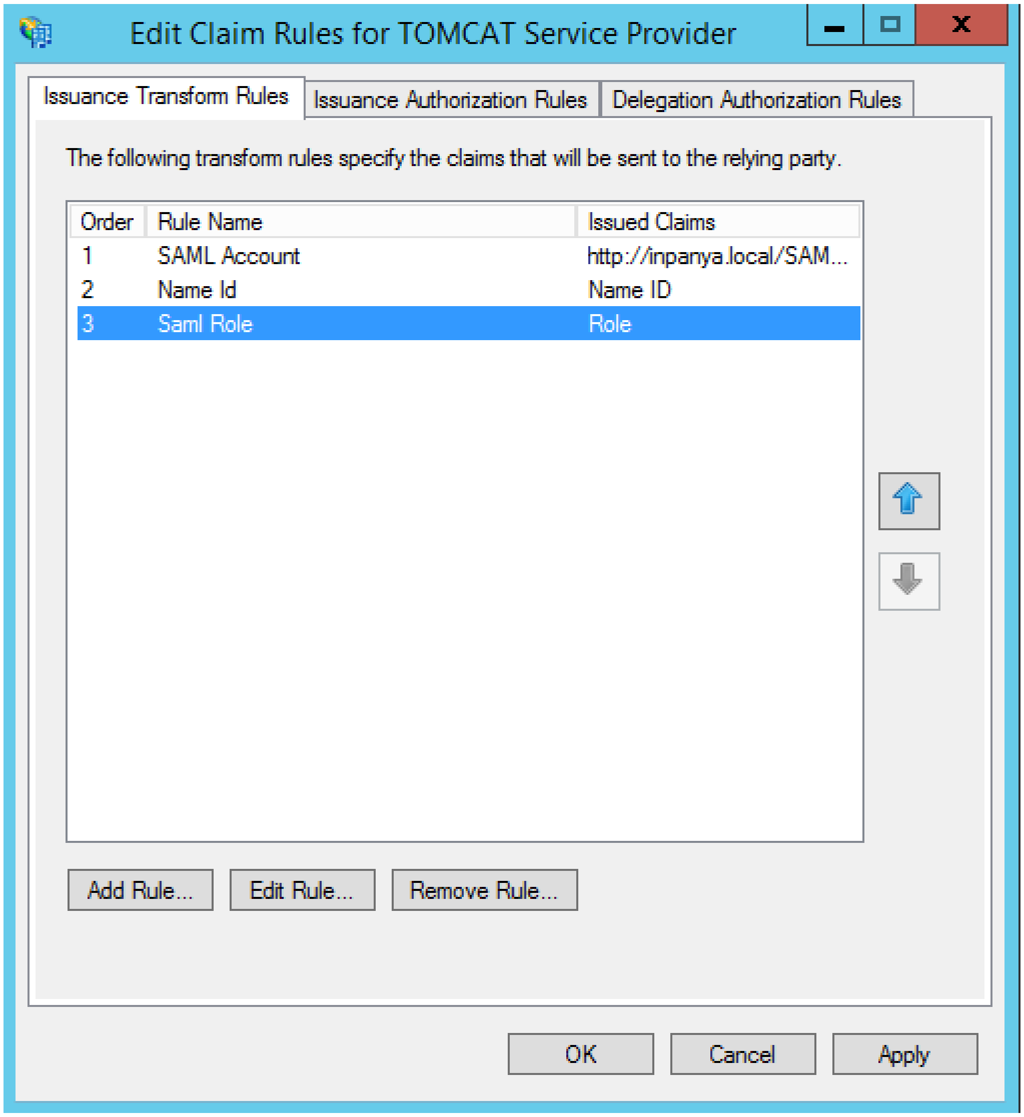
User's group: INPANYA\SAML Group

Outgoing claim type: Role

Outgoing name ID format: Unspecified

Outgoing claim value: SAMLUser

*** Create User Group in Active Directory server :SAML Group****



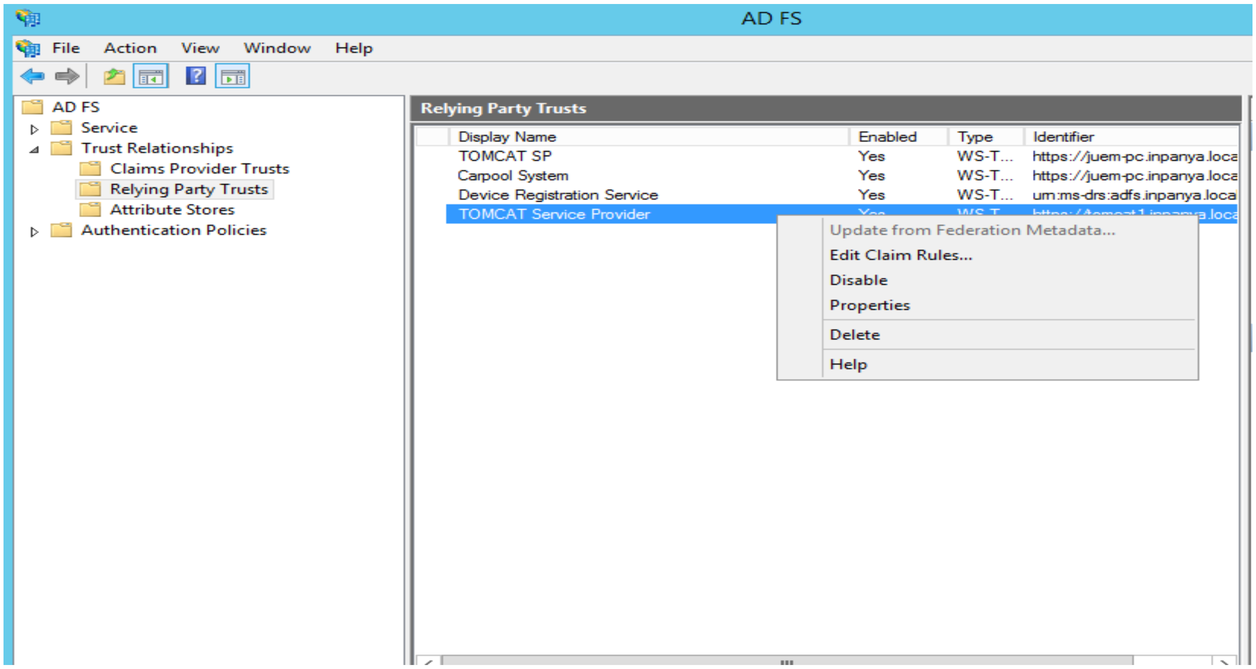
Edit Claim Rules for TOMCAT Service Provider
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	SAML Account	http://inpanya.local/SAM...
2	Name Id	Name ID
3	Saml Role	Role

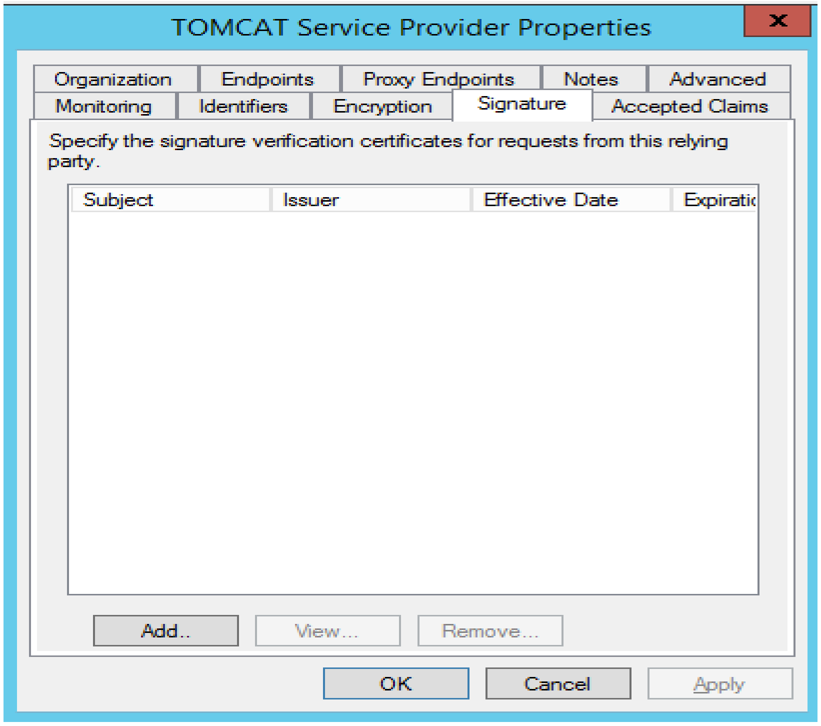
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply

Add Signature certificate to Relying party Trust



Display Name	Enabled	Type	Identifier
TOMCAT SP	Yes	WS-T...	https://juem-pc.inpanya.loca
Carpool System	Yes	WS-T...	https://juem-pc.inpanya.loca
Device Registration Service	Yes	WS-T...	urn:ms-drs:adfs.inpanya.loca
TOMCAT Service Provider	Yes	WS-T...	https://tomcat1.inpanya.loca

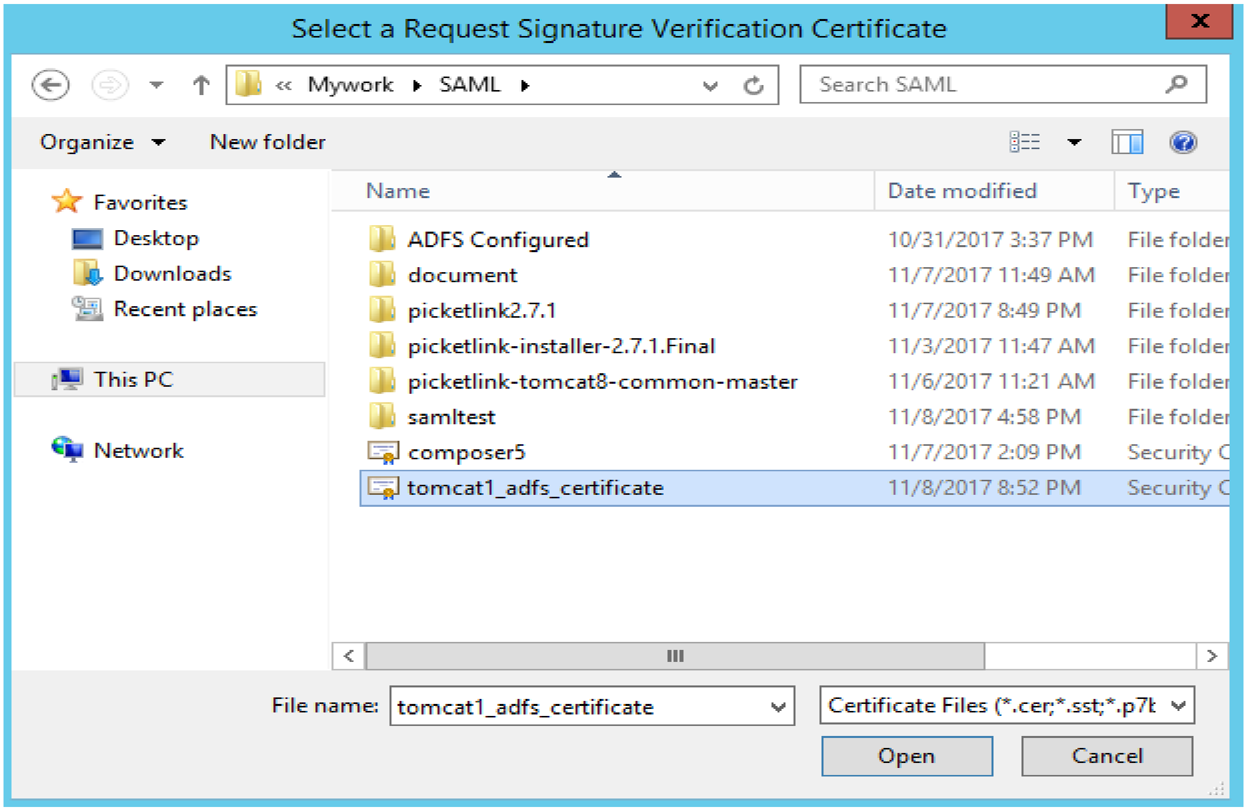
Right click on TOMCAT Service Provider →Properties



Specify the signature verification certificates for requests from this relying party.

Subject	Issuer	Effective Date	Expiratic

On Signature tab click Add

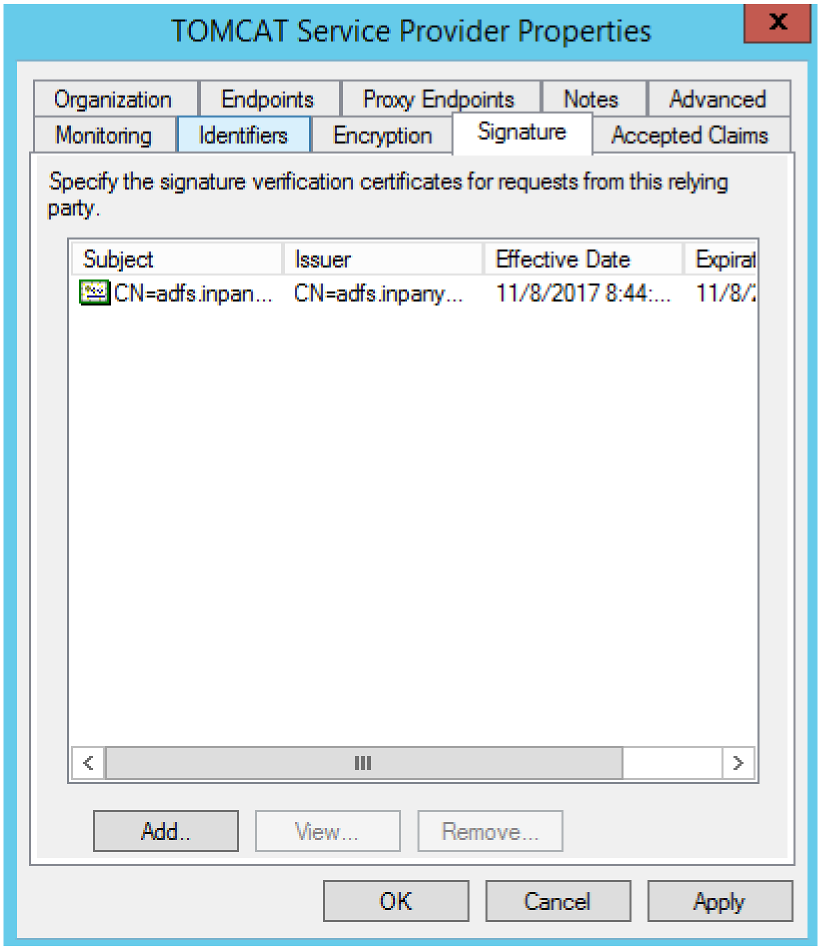


Name	Date modified	Type
ADFS Configured	10/31/2017 3:37 PM	File folder
document	11/7/2017 11:49 AM	File folder
picketlink2.7.1	11/7/2017 8:49 PM	File folder
picketlink-installer-2.7.1.Final	11/3/2017 11:47 AM	File folder
picketlink-tomcat8-common-master	11/6/2017 11:21 AM	File folder
samltest	11/8/2017 4:58 PM	File folder
composer5	11/7/2017 2:09 PM	Security C
tomcat1_adfs_certificate	11/8/2017 8:52 PM	Security C

File name: tomcat1_adfs_certificate

Certificate Files (*.cer;*.sst;*.p7b

Browse to tomcat1_adfs_certificate.cer

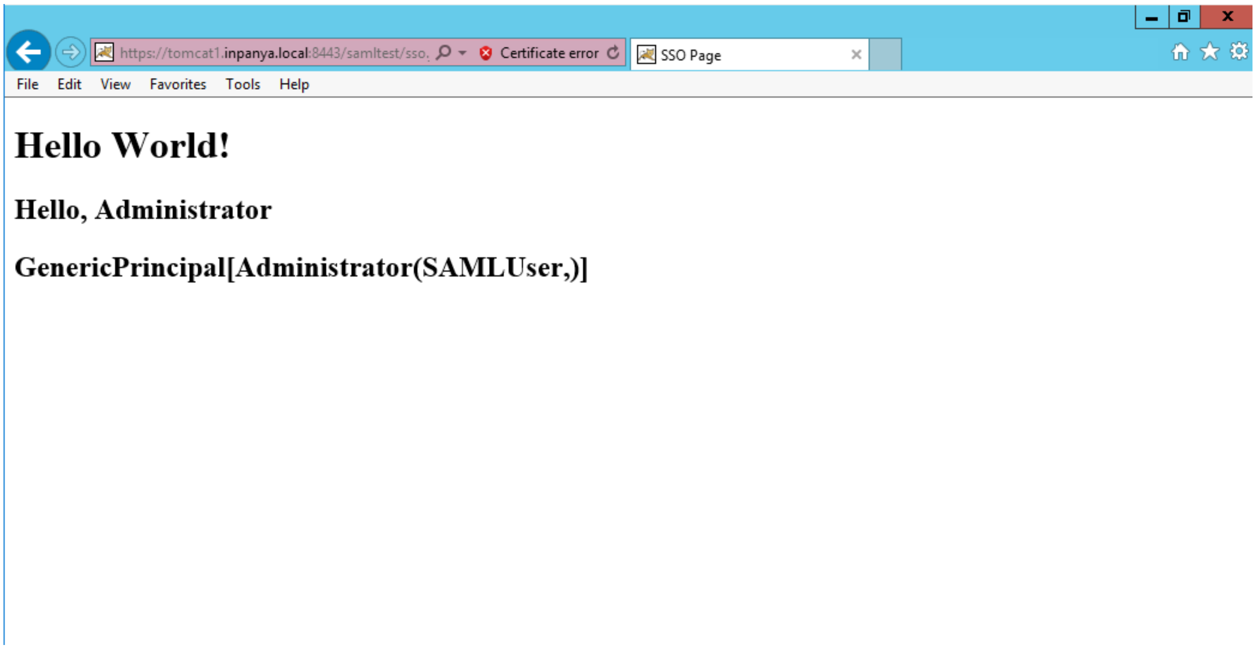


Specify the signature verification certificates for requests from this relying party.

Subject	Issuer	Effective Date	Expirat
CN=adfs.inpan...	CN=adfs.inpany...	11/8/2017 8:44:...	11/8/:

Test Result

http://tomcat1.inpanya.local:8080/samltest/SSO

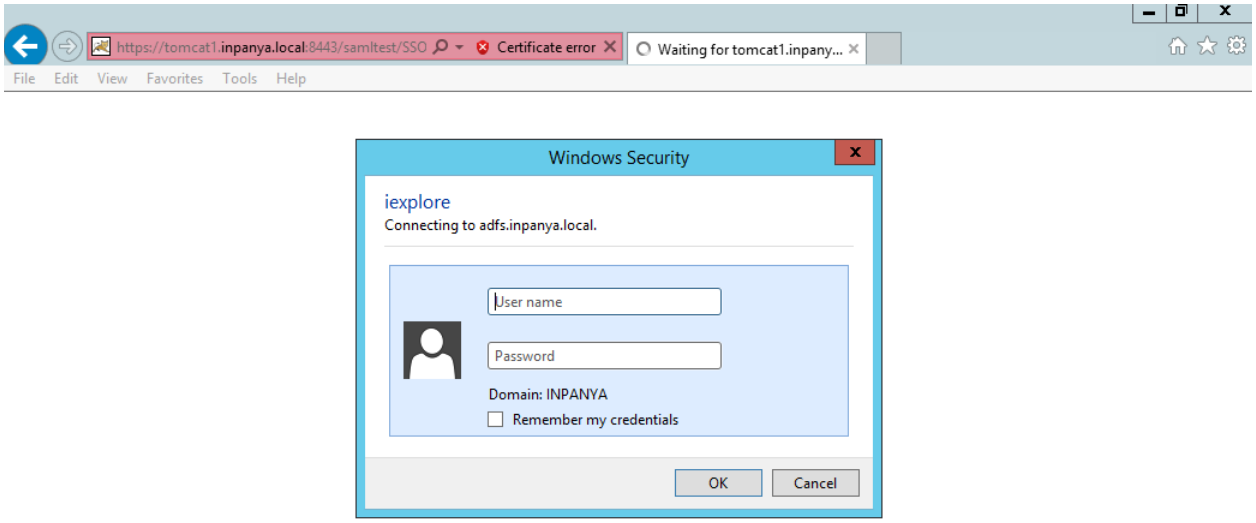


Hello World!

Hello, Administrator

GenericPrincipal[Administrator(SAMLUser,)]

If Single Sign on popup windows security .You need to add adfs.inpanya.local   in to intranet Zone



https://tomcat1.inpanya.local:8443/samltest/SSO
Certificate error
Waiting for tomcat1.inpany...
File
Edit
View
Favorites
Tools
Help

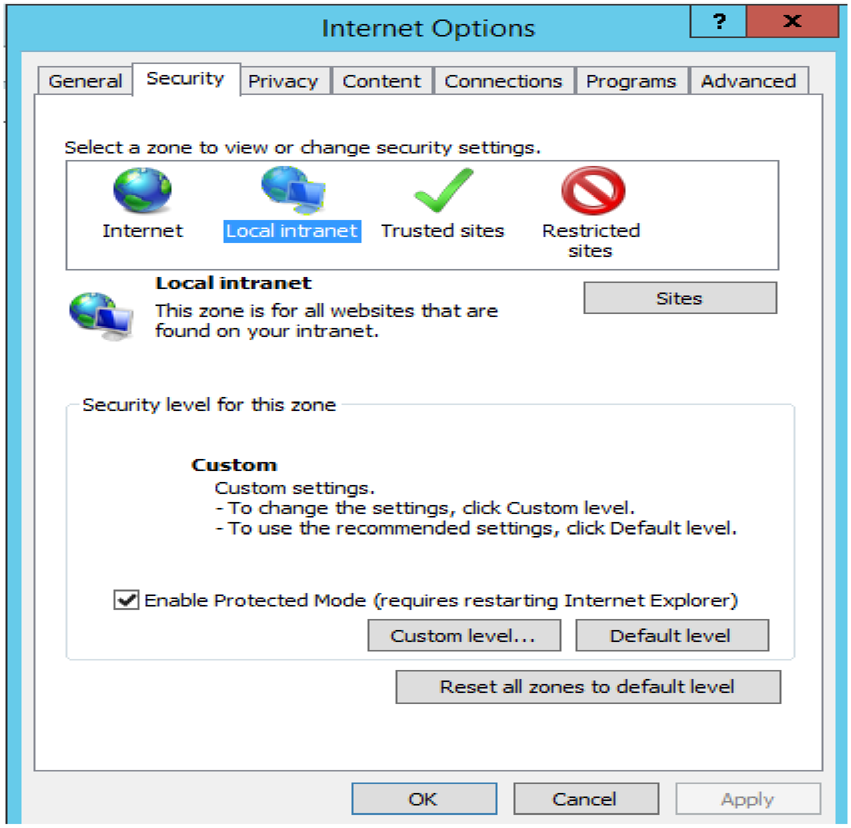
Windows Security

iexplore

Connecting to adfs.inpanya.local.

Domain: INPANYA

□ Remember my credentials



Select a zone to view or change security settings.

Local intranet

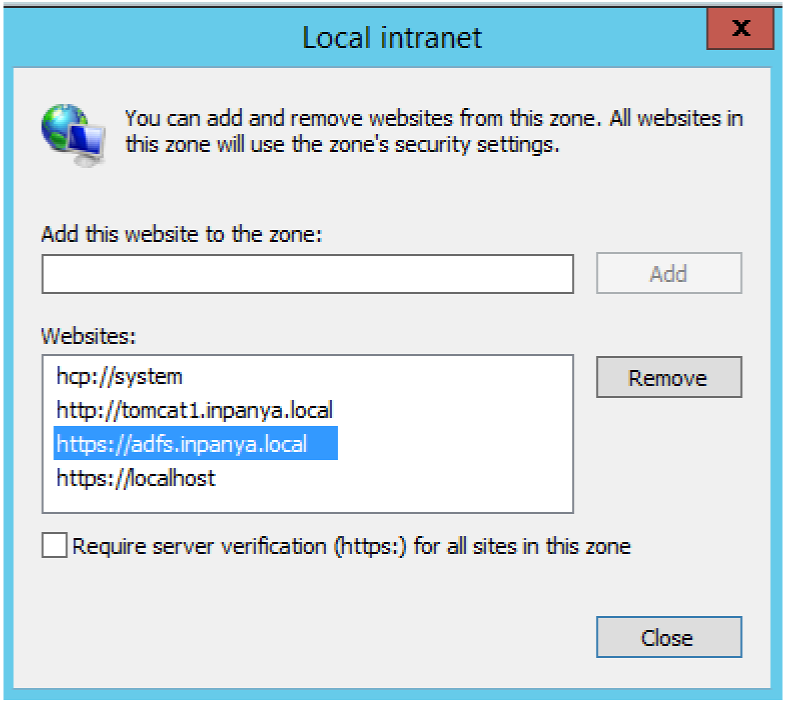
This zone is for all websites that are found on your intranet.

Security level for this zone

Custom

Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

☑ Enable Protected Mode (requires restarting Internet Explorer)



You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

Websites:

hcp://system
http://tomcat1.inpanya.local
https://adfs.inpanya.local
https://localhost

□ Require server verification (https:) for all sites in this zone