AD FS Relying Party Trust

Server 2012R2

COMPANY A – Accounts Partner

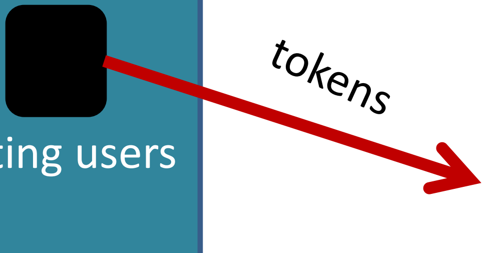
Enterprise CA

DC

AD FS

Federation Accounts Server

- Collecting and authenticating users credentials
- Building up claims for that user and packaging the claims into security tokens
- Presenting the tokens across a Federated Trust to enable access to Web-based resources that are located in the resource partner organization



COMPANY B – Resource Partner

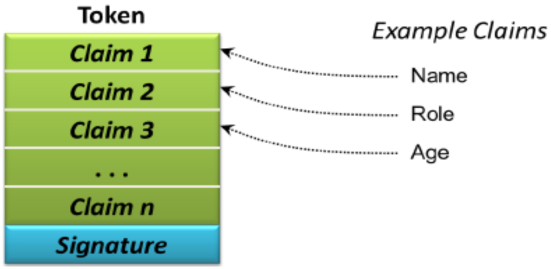
ADFS enabled Web Server (Web based Applications)

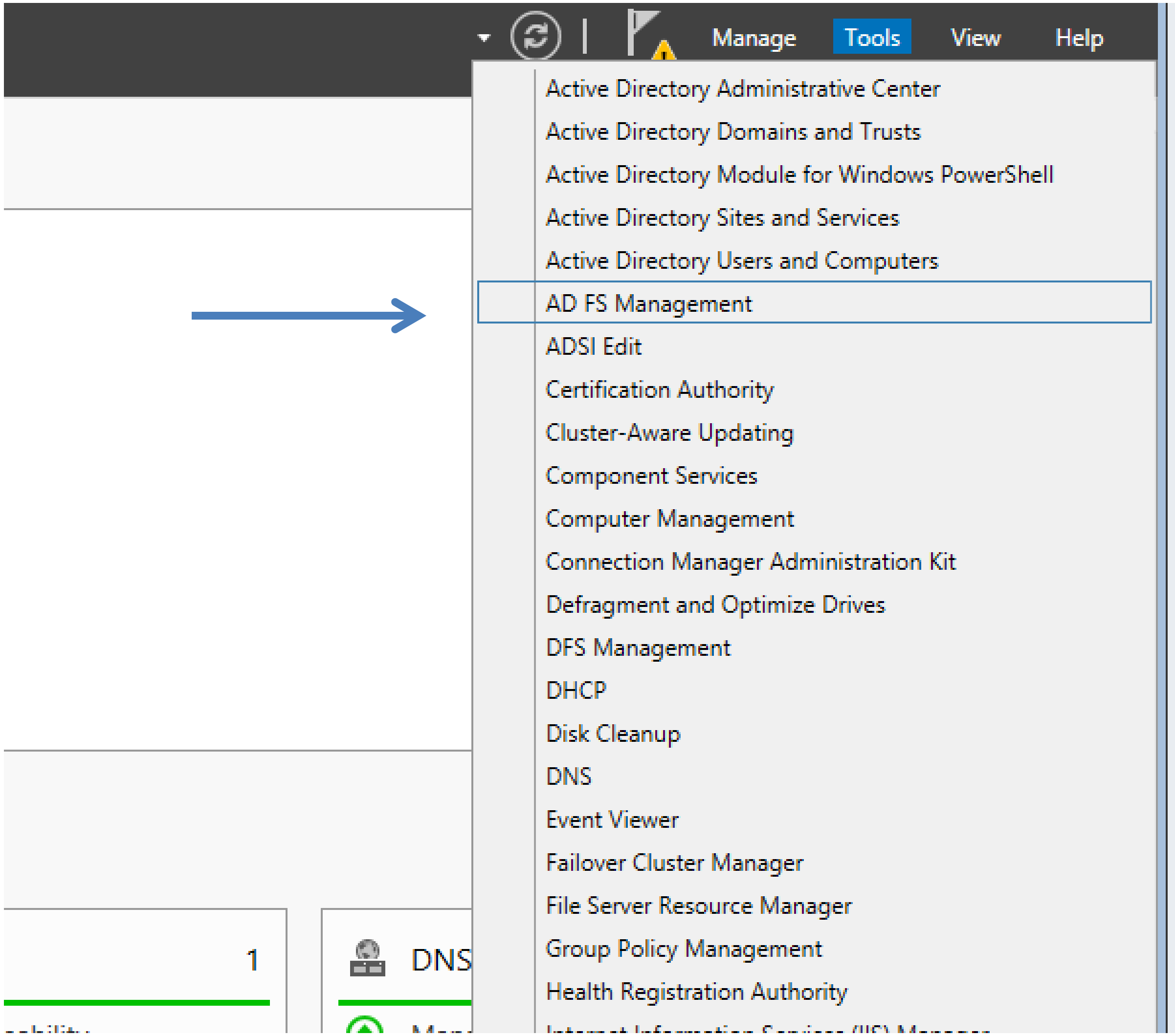
AD FS

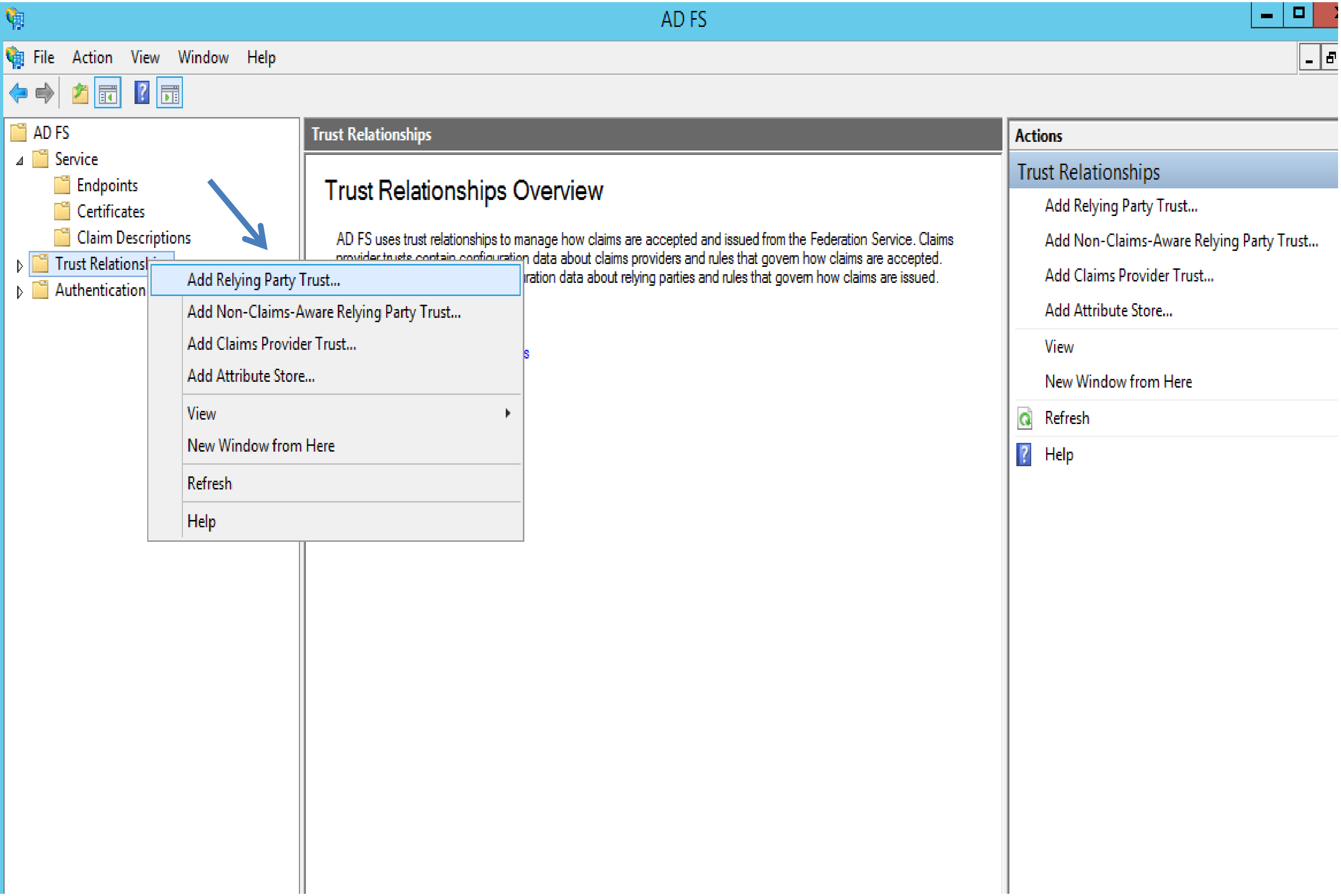
Federation Resource Server

- uses the security tokens to make authorization decisions for its Web servers
- To function as an ADFS resource, Web servers must either have Windows Identity Foundation (WIF) installed or have the Active Directory Federation Services Claims-Aware Web Agent role services installed.

In a claims-based world, a token contains one or more *claims*, each of which carries some piece of information about the user it identifies.

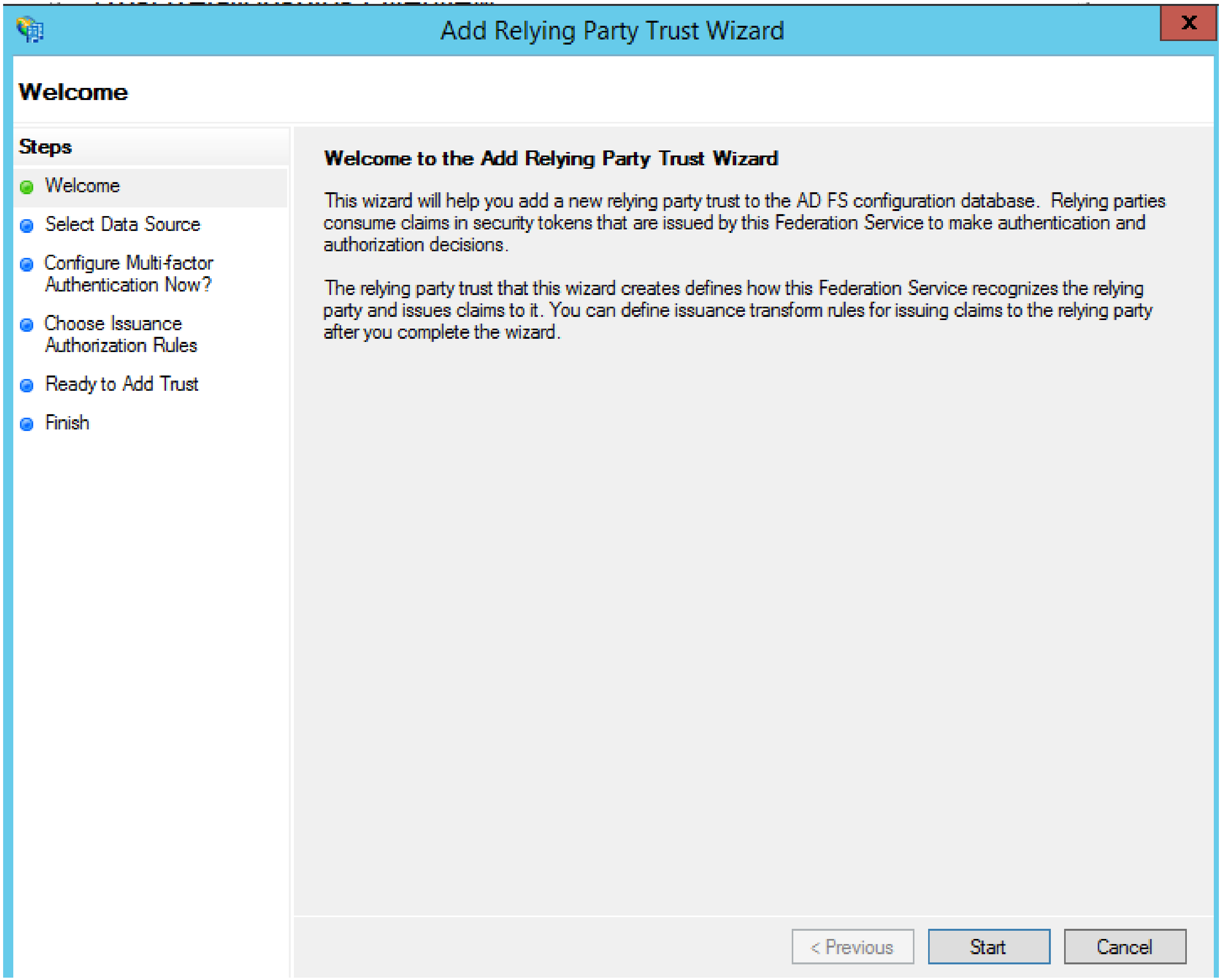



Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
AD FS Management
ADSI Edit
Certification Authority
Cluster-Aware Updating
Component Services
Computer Management
Connection Manager Administration Kit
Defragment and Optimize Drives
DFS Management
DHCP
Disk Cleanup
DNS
Event Viewer
Failover Cluster Manager
File Server Resource Manager
Group Policy Management
Health Registration Authority
Internet Information Services (IIS) Manager
1
DNS



Trust Relationships Overview

AD FS uses trust relationships to manage how claims are accepted and issued from the Federation Service. Claims provider trusts contain configuration data about claims providers and rules that govern how claims are accepted. ration data about relying parties and rules that govern how claims are issued.



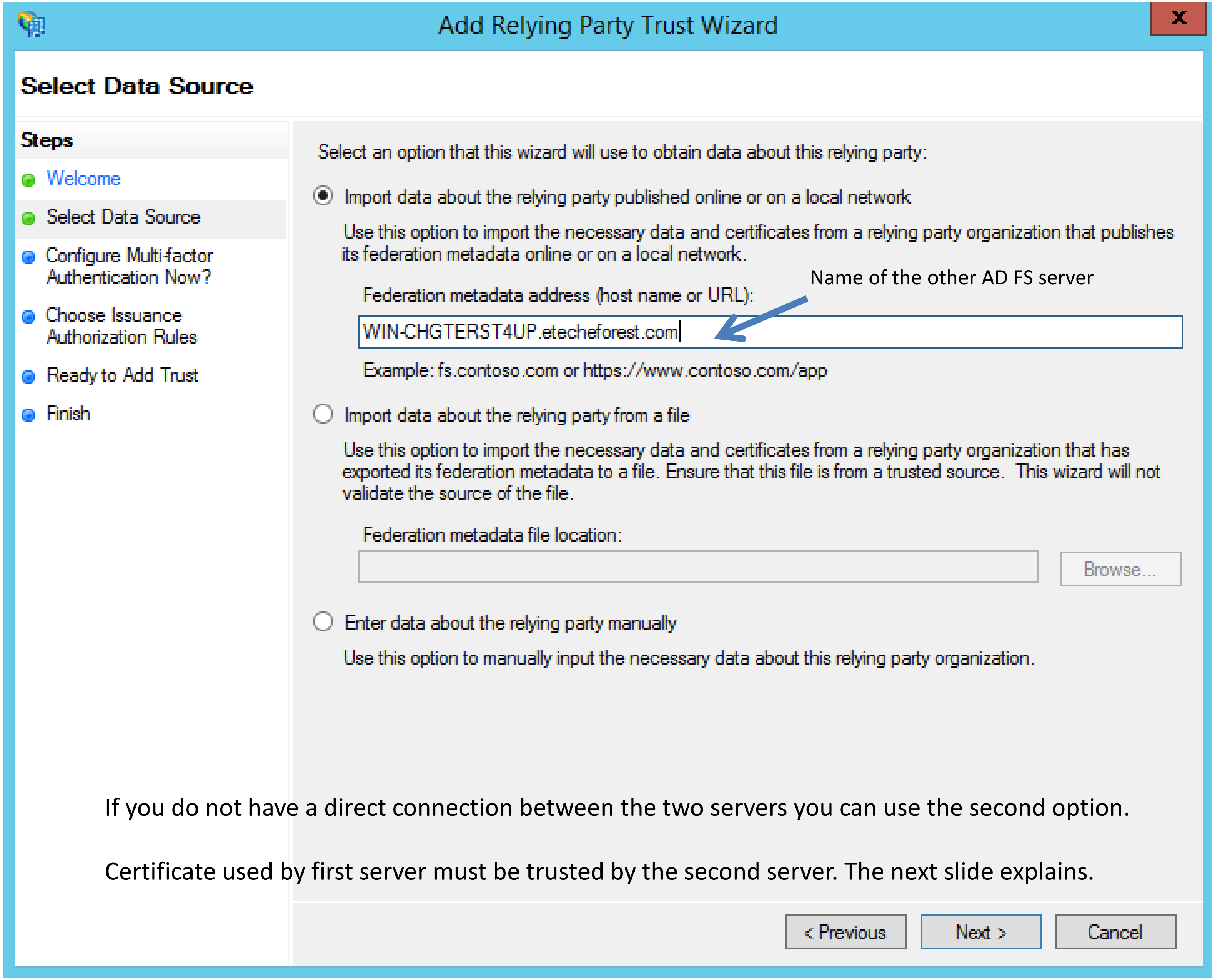
Add Relying Party Trust Wizard

● 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.



Add Relying Party Trust Wizard
x

Select Data Source

Steps
● Welcome
● Select Data Source
● 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):

WIN-CHGTERST4UP.etecheforest.com

Name of the other AD FS server

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.

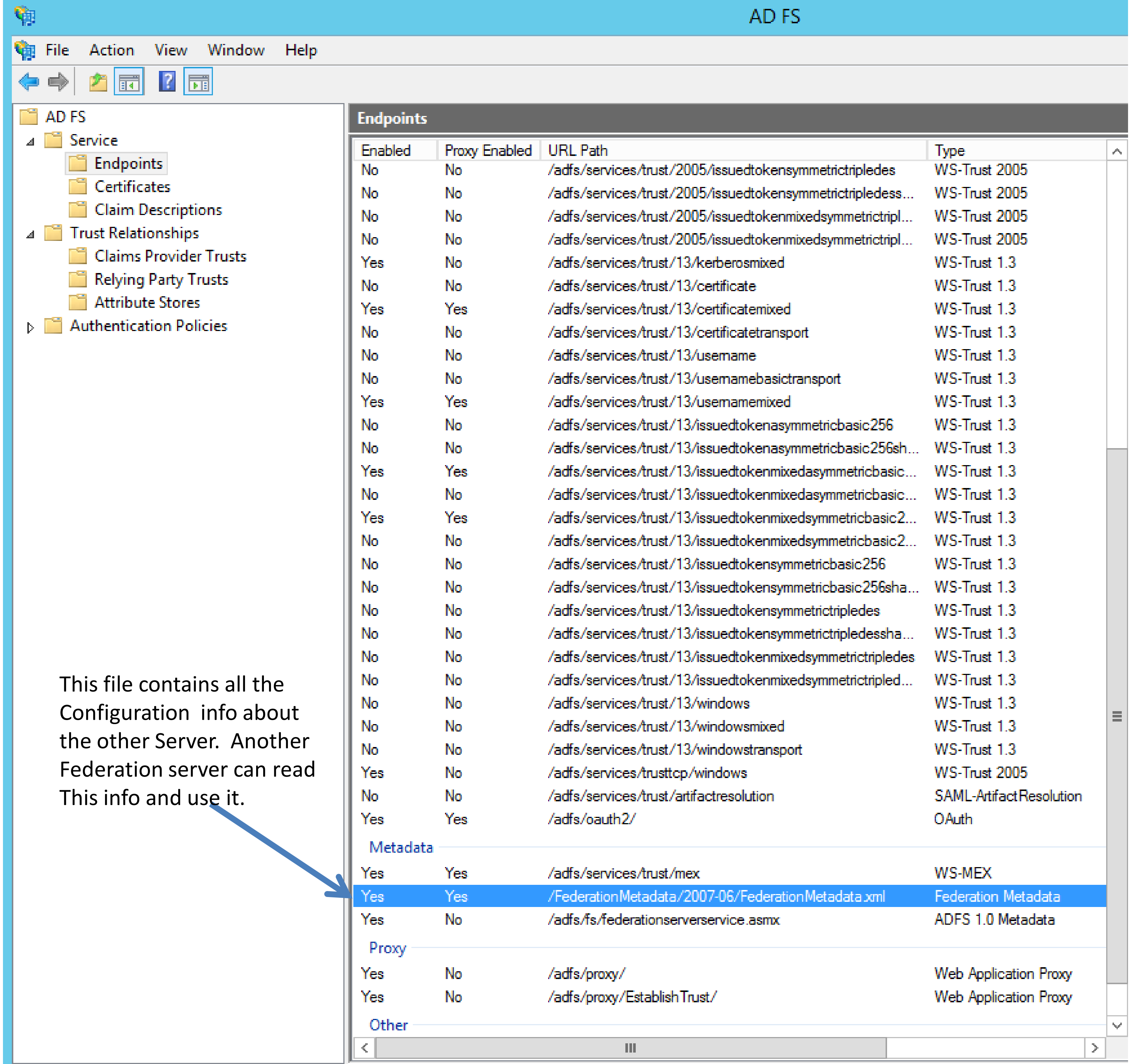
Federation metadata file location:

○ Enter data about the relying party manually

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

If you do not have a direct connection between the two servers you can use the second option.

Certificate used by first server must be trusted by the second server. The next slide explains.

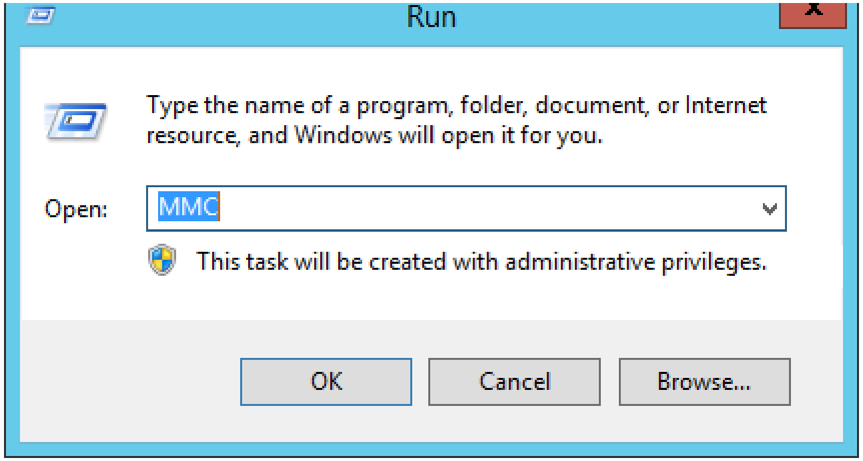


Endpoints

Enabled	Proxy Enabled	URL Path	Type
No	No	/adfs/services/trust/2005/issuedtokensymmetrictripledes	WS-Trust 2005
No	No	/adfs/services/trust/2005/issuedtokensymmetrictripledess...	WS-Trust 2005
No	No	/adfs/services/trust/2005/issuedtokenmixedsymmetrictripl...	WS-Trust 2005
No	No	/adfs/services/trust/2005/issuedtokenmixedsymmetrictripl...	WS-Trust 2005
Yes	No	/adfs/services/trust/13/kerberosmixed	WS-Trust 1.3
No	No	/adfs/services/trust/13/certificate	WS-Trust 1.3
Yes	Yes	/adfs/services/trust/13/certificatemixed	WS-Trust 1.3
No	No	/adfs/services/trust/13/certificatetransport	WS-Trust 1.3
No	No	/adfs/services/trust/13/username	WS-Trust 1.3
No	No	/adfs/services/trust/13/usernamebasictransport	WS-Trust 1.3
Yes	Yes	/adfs/services/trust/13/usernamemixed	WS-Trust 1.3
No	No	/adfs/services/trust/13/issuedtokenasymmetricbasic256	WS-Trust 1.3
No	No	/adfs/services/trust/13/issuedtokenasymmetricbasic256sh...	WS-Trust 1.3
Yes	Yes	/adfs/services/trust/13/issuedtokenmixedasymmetricbasic...	WS-Trust 1.3
No	No	/adfs/services/trust/13/issuedtokenmixedasymmetricbasic...	WS-Trust 1.3
Yes	Yes	/adfs/services/trust/13/issuedtokenmixedsymmetricbasic2...	WS-Trust 1.3
No	No	/adfs/services/trust/13/issuedtokenmixedsymmetricbasic2...	WS-Trust 1.3
No	No	/adfs/services/trust/13/issuedtokensymmetricbasic256	WS-Trust 1.3
No	No	/adfs/services/trust/13/issuedtokensymmetricbasic256sha...	WS-Trust 1.3
No	No	/adfs/services/trust/13/issuedtokensymmetrictripledes	WS-Trust 1.3
No	No	/adfs/services/trust/13/issuedtokensymmetrictripledessha...	WS-Trust 1.3
No	No	/adfs/services/trust/13/issuedtokenmixedsymmetrictripledes	WS-Trust 1.3
No	No	/adfs/services/trust/13/issuedtokenmixedsymmetrictripled...	WS-Trust 1.3
No	No	/adfs/services/trust/13/windows	WS-Trust 1.3
No	No	/adfs/services/trust/13/windowsmixed	WS-Trust 1.3
No	No	/adfs/services/trust/13/windowstransport	WS-Trust 1.3
Yes	No	/adfs/services/trusttcp/windows	WS-Trust 2005
No	No	/adfs/services/trust/artifactresolution	SAML-ArtifactResolution
Yes	Yes	/adfs/oauth2/	OAuth
Metadata			
Yes	Yes	/adfs/services/trust/mex	WS-MEX
Yes	Yes	/FederationMetadata/2007-06/FederationMetadata.xml	Federation Metadata
Yes	No	/adfs/fs/federationserverservice.asmx	ADFS 1.0 Metadata
Proxy			
Yes	No	/adfs/proxy/	Web Application Proxy
Yes	No	/adfs/proxy/EstablishTrust/	Web Application Proxy
Other			

This file contains all the Configuration info about the other Server. Another Federation server can read This info and use it.

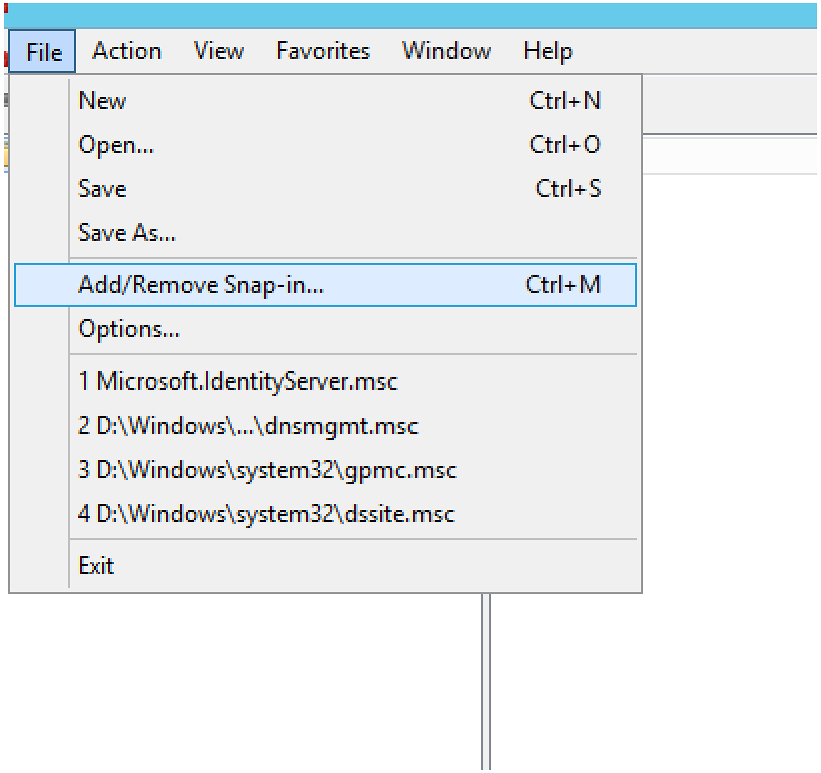
Transfering the certificate to the second AD FS Server



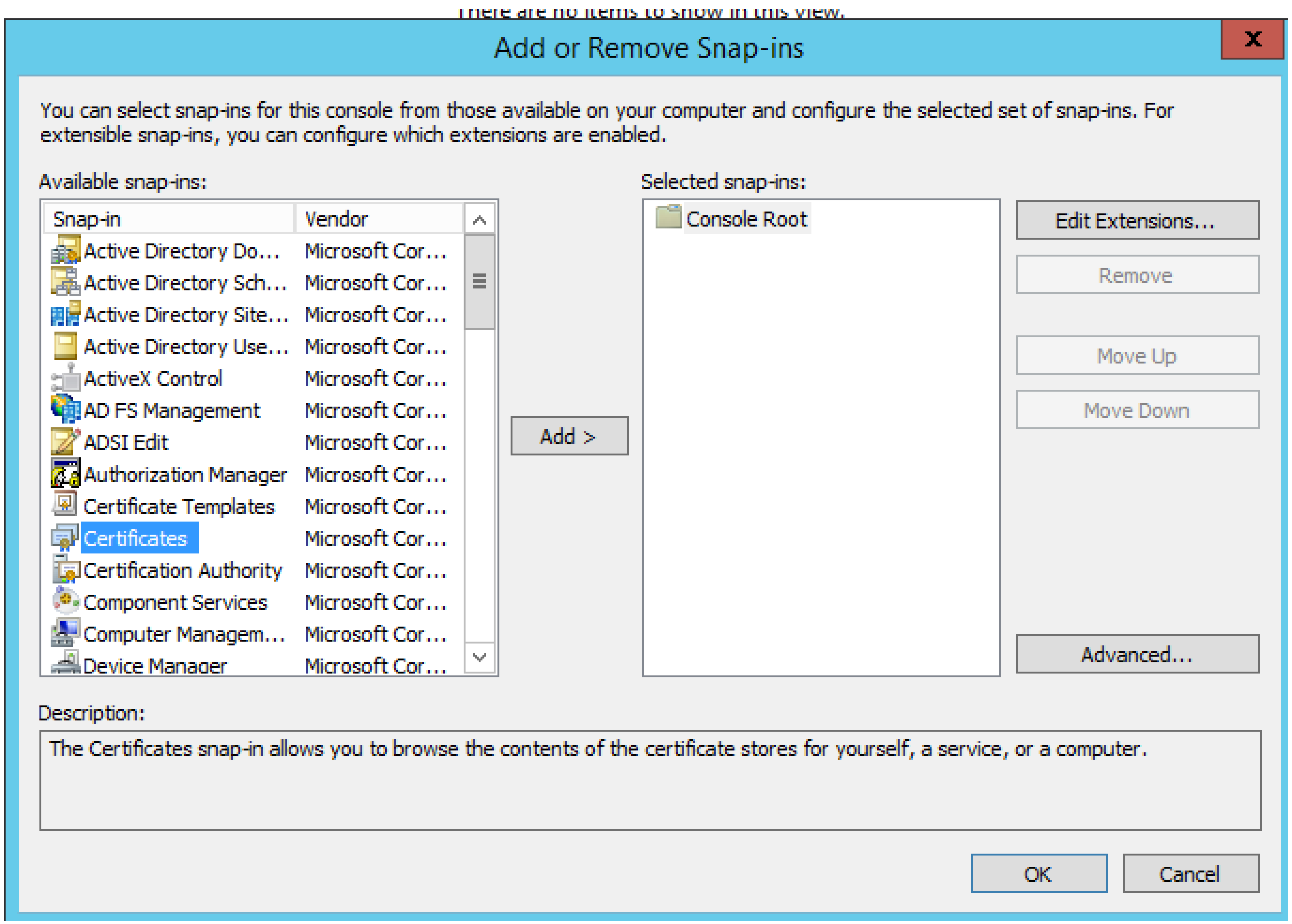
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: MMC

This task will be created with administrative privileges.


File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 Microsoft.IdentityServer.msc
2 D:\Windows\...\dnsmgmt.msc
3 D:\Windows\system32\gpmc.msc
4 D:\Windows\system32\dssite.msc
Exit

- From the run type mmc and click on ok
- In the mmc console click on Add/Remove Snap-in



There are no items to show in this view.

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
Active Directory Do...	Microsoft Cor...
Active Directory Sch...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
AD FS Management	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...

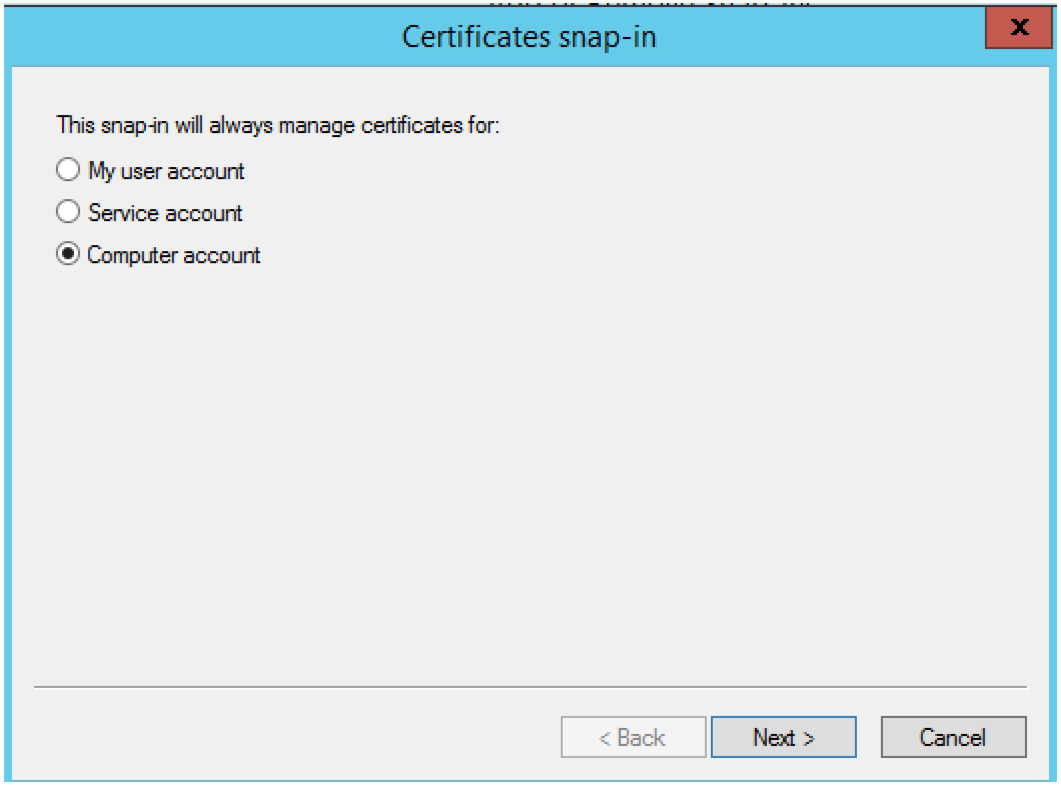
Selected snap-ins:

Console Root

Description:

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

Select certificates then click on Add



Certificates snap-in

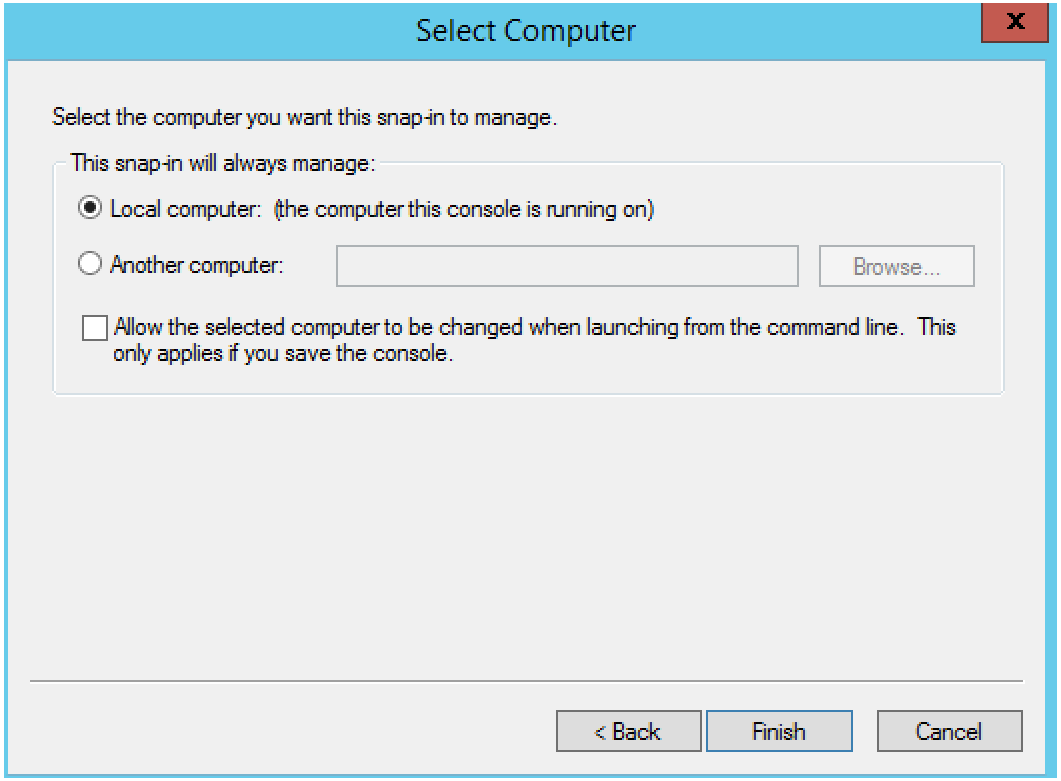
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

Select computer account and click next



Select Computer

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

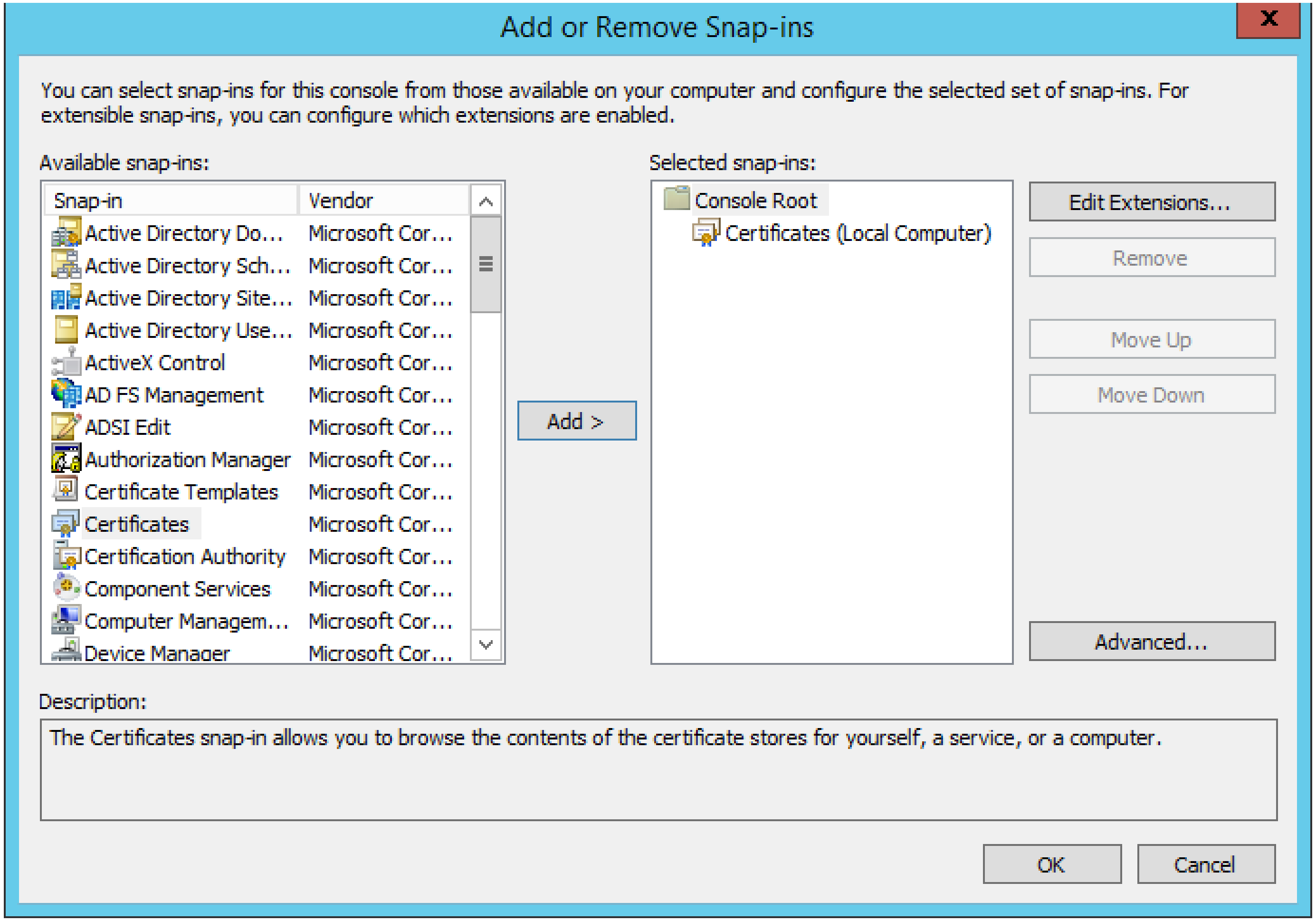
This snap-in will always manage:

● 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
Active Directory Do...	Microsoft Cor...
Active Directory Sch...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
AD FS Management	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...

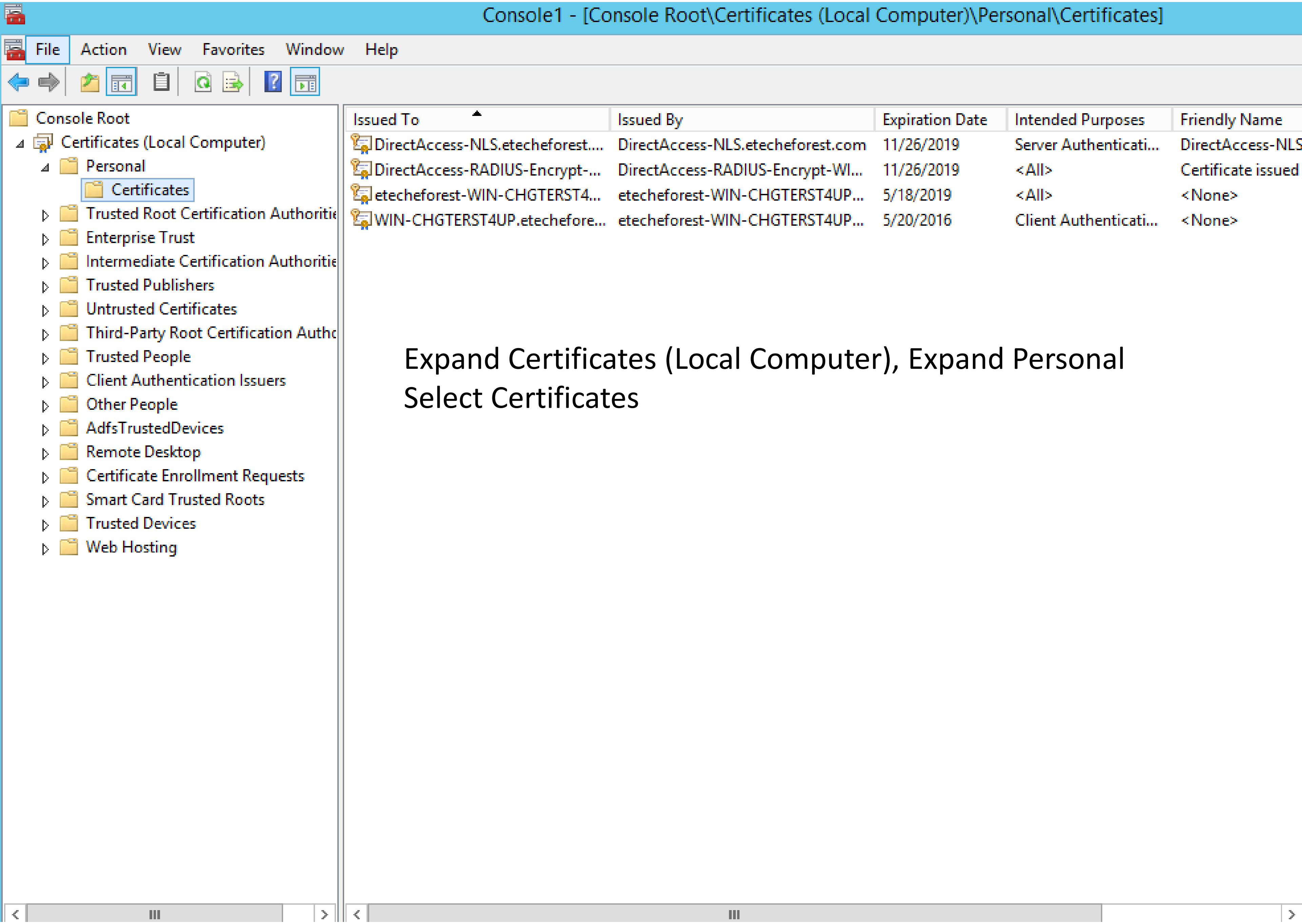
Selected snap-ins:

- 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 on OK.

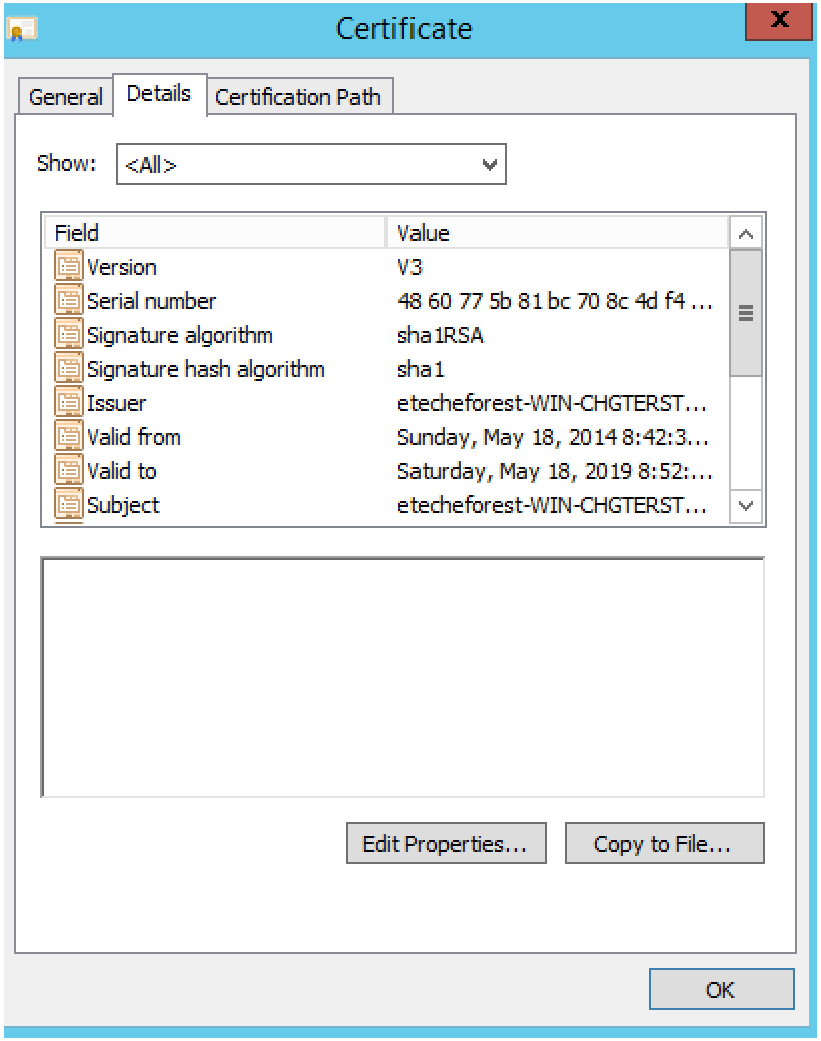


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File
Action
View
Favorites
Window
Help

- Console Root
  - Certificates (Local Computer)
    - Personal
      - Certificates
    - Trusted Root Certification Authoritie
    - Enterprise Trust
    - Intermediate Certification Authoritie
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Autho
    - Trusted People
    - Client Authentication Issuers
    - Other People
    - AdfsTrustedDevices
    - Remote Desktop
    - Certificate Enrollment Requests
    - Smart Card Trusted Roots
    - Trusted Devices
    - Web Hosting

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
DirectAccess-NLS.etecheforest....	DirectAccess-NLS.etecheforest.com	11/26/2019	Server Authenticati...	DirectAccess-NLS
DirectAccess-RADIUS-Encrypt-...	DirectAccess-RADIUS-Encrypt-WI...	11/26/2019	<All>	Certificate issued
etecheforest-WIN-CHGTERST4...	etecheforest-WIN-CHGTERST4UP...	5/18/2019	<All>	<None>
WIN-CHGTERST4UP.etechefore...	etecheforest-WIN-CHGTERST4UP...	5/20/2016	Client Authenticati...	<None>

Expand Certificates (Local Computer), Expand Personal
Select Certificates

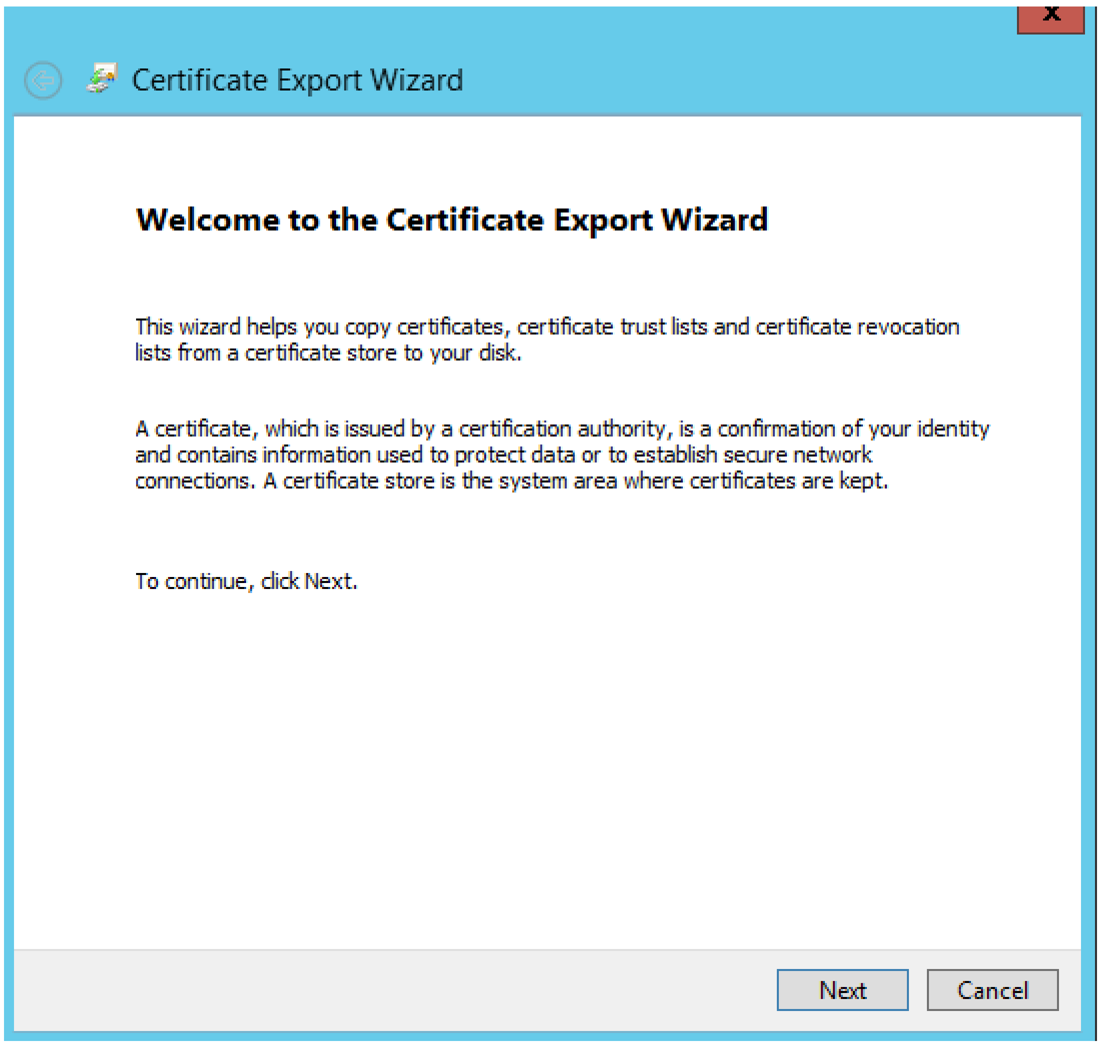


Show: <All>

Field	Value
Version	V3
Serial number	48 60 77 5b 81 bc 70 8c 4d f4 ...
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	etecheforest-WIN-CHGTERST...
Valid from	Sunday, May 18, 2014 8:42:3...
Valid to	Saturday, May 18, 2019 8:52:...
Subject	etecheforest-WIN-CHGTERST...

Double click the certificate and click on the details tab

Click on copy to file



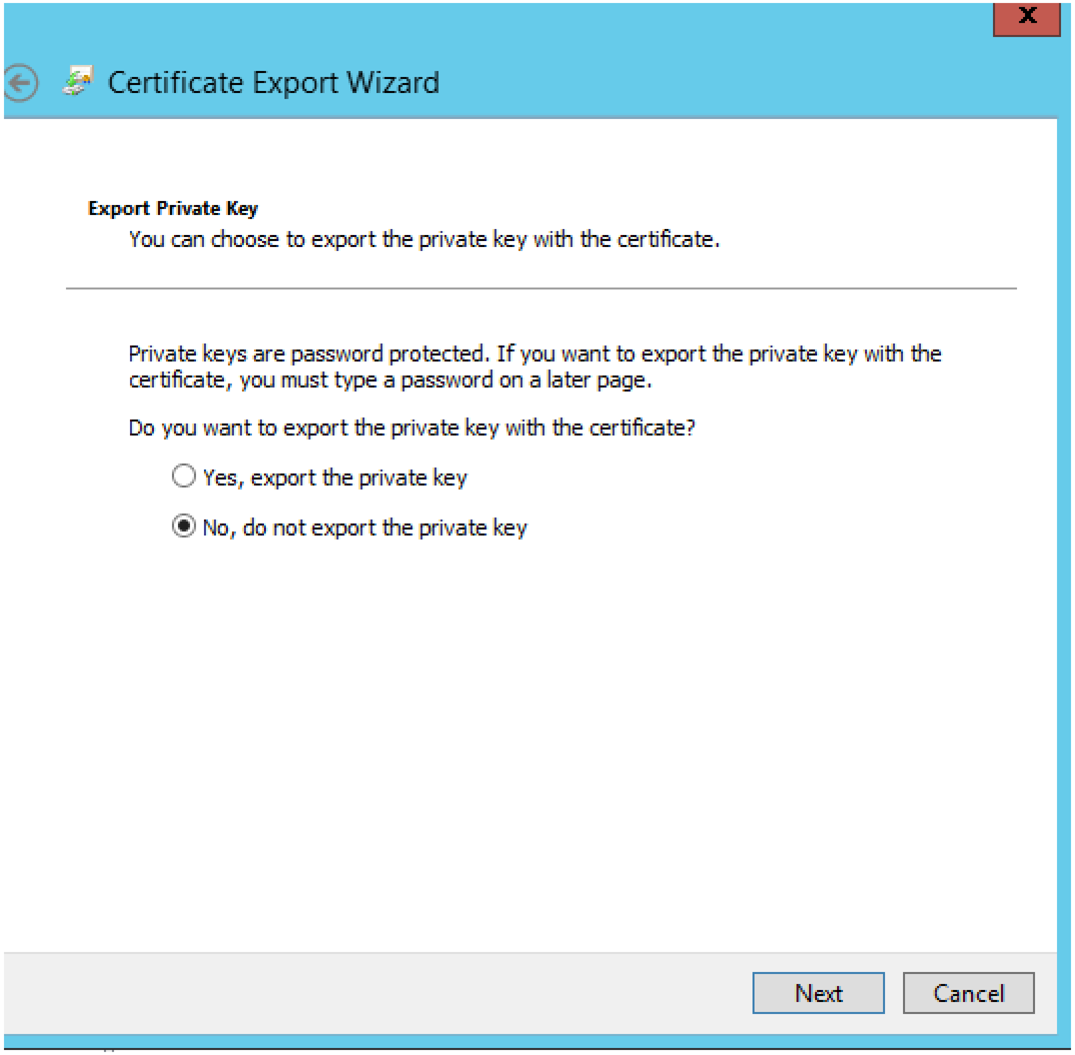
Welcome to the Certificate Export Wizard

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 Private Key

You can choose to export the private key with the certificate.

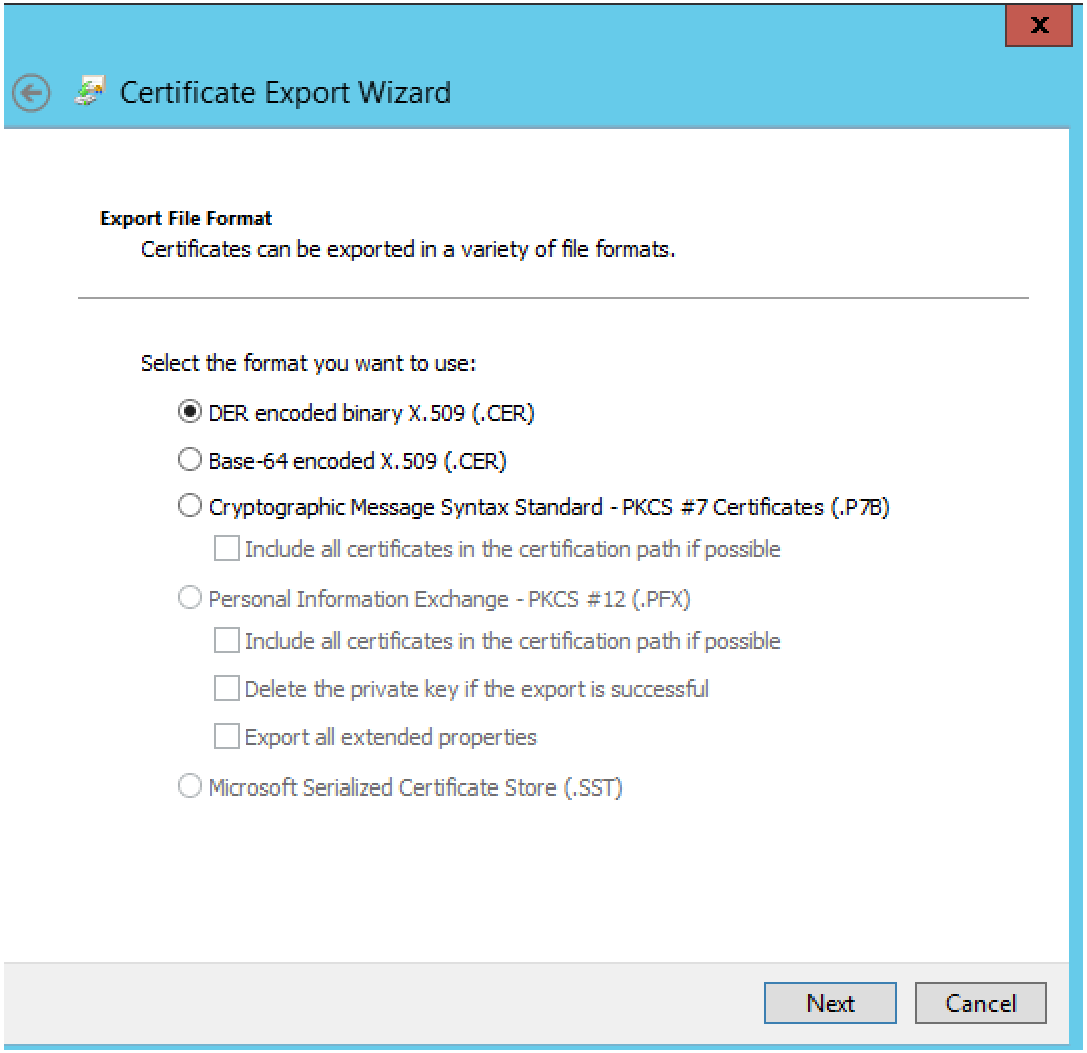
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

○ Yes, export the private key

● No, do not export the private key

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

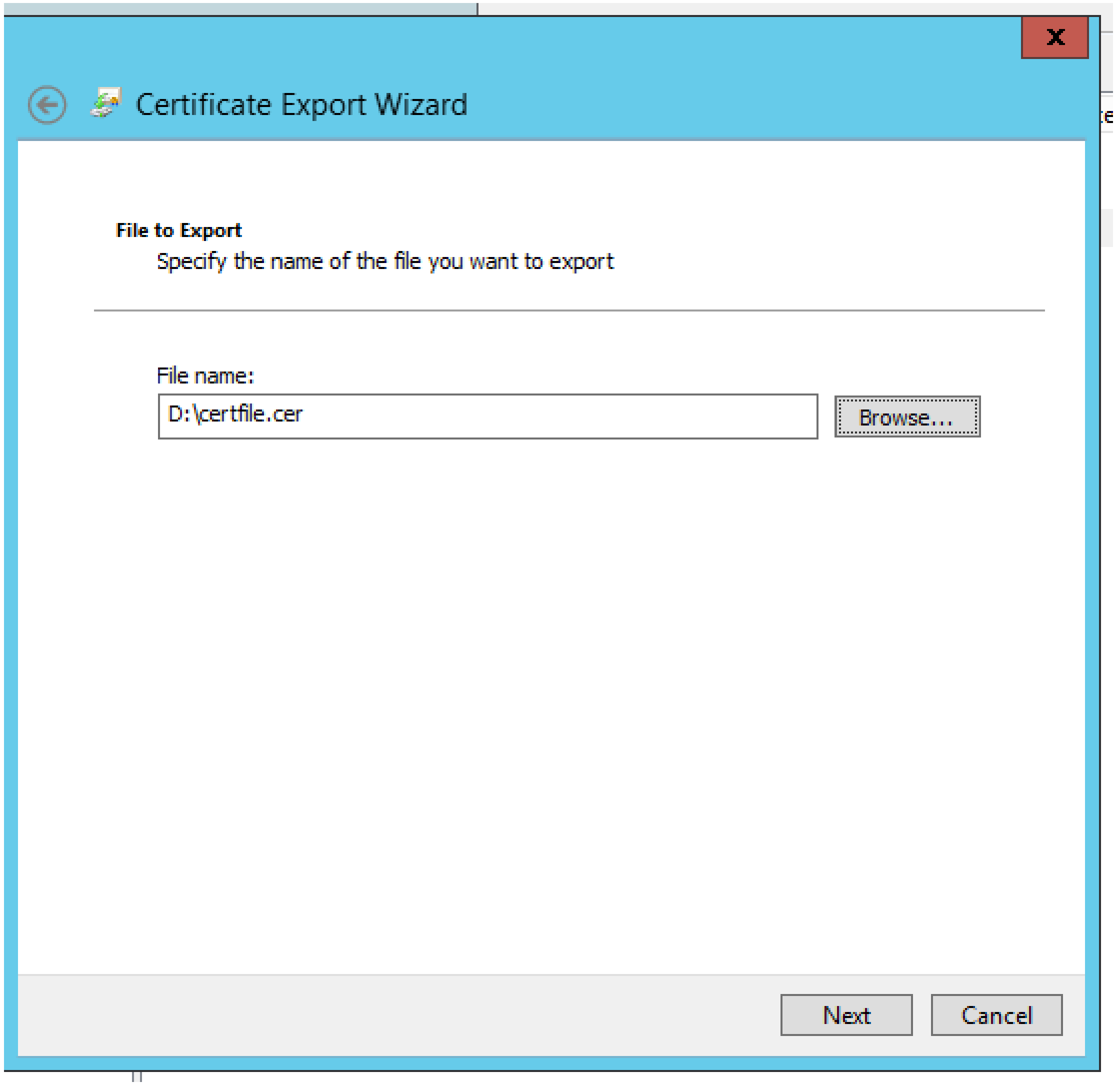
○ Personal Information Exchange - PKCS #12 (.PFX)

□ 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)



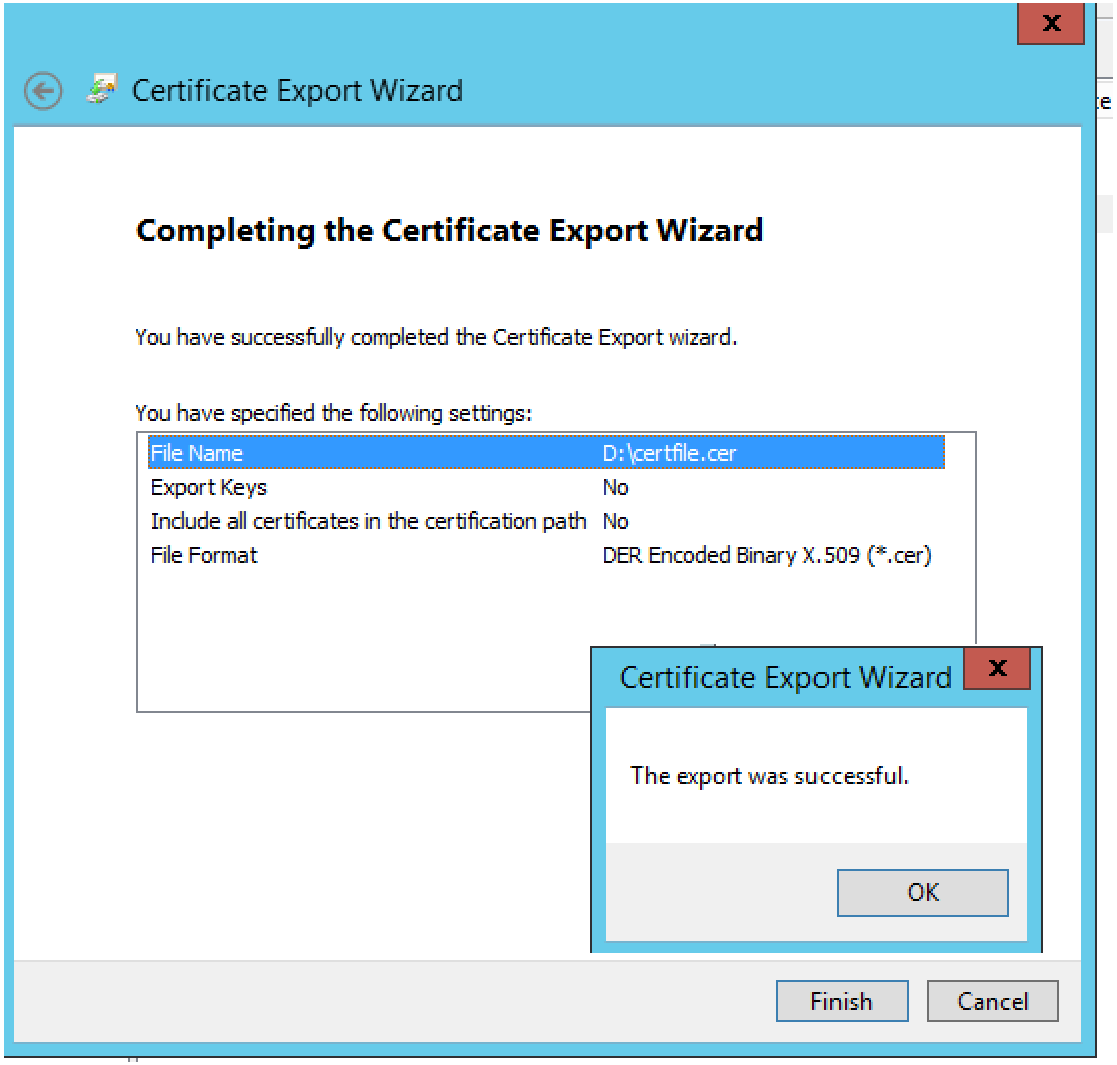
File to Export

Specify the name of the file you want to export

File name:

D:\certfile.cer

Tyne the name of file and choose your saving location using the browse button



Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

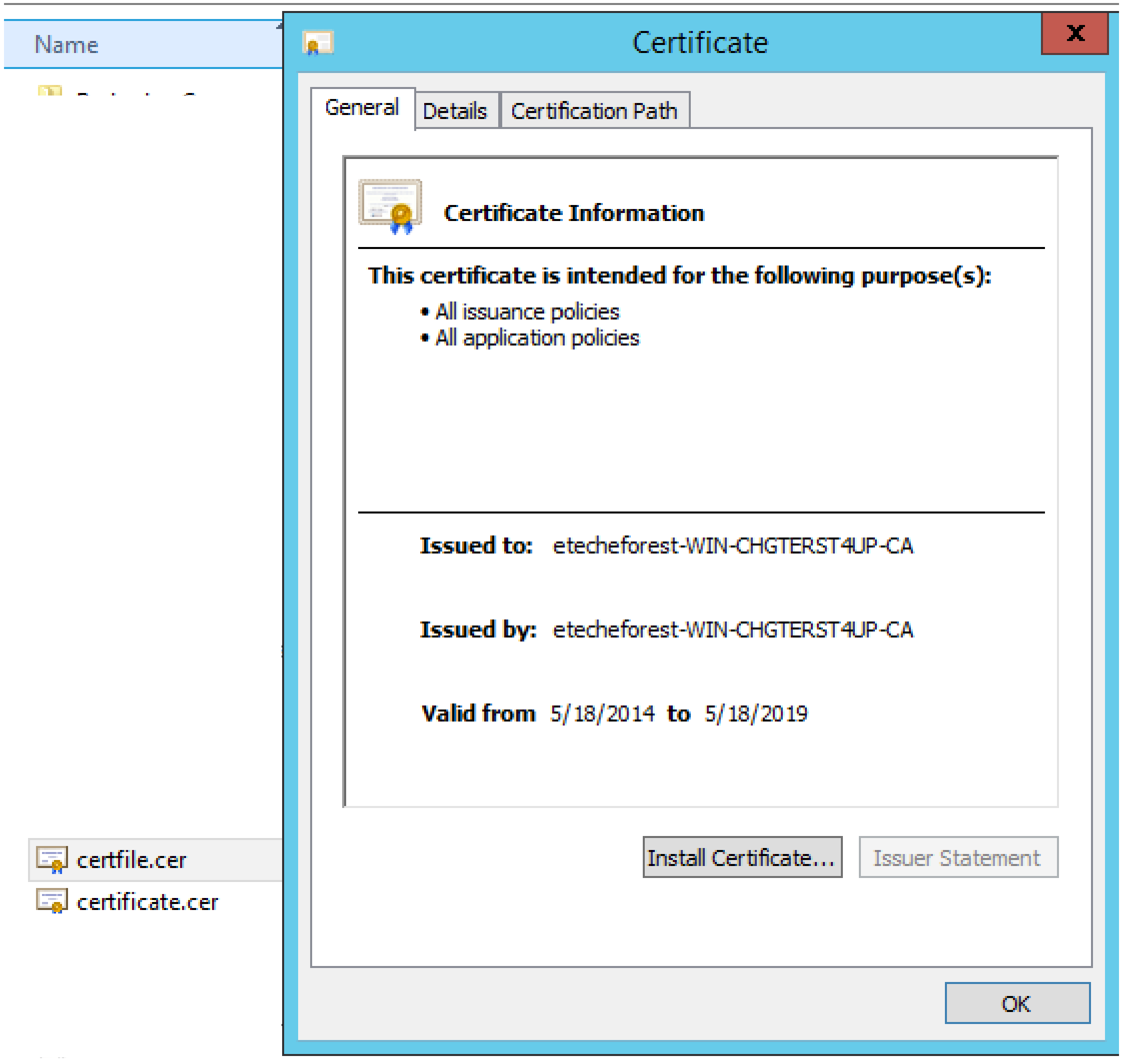
You have specified the following settings:

File Name	D:\certfile.cer
Export Keys	No
Include all certificates in the certification path	No
File Format	DER Encoded Binary X.509 (*.cer)

The export was successful.

Go the the second server

Using Windows explorer navigate the exported certificate and double click to open it



Certificate

General | Details | Certification Path

Certificate Information

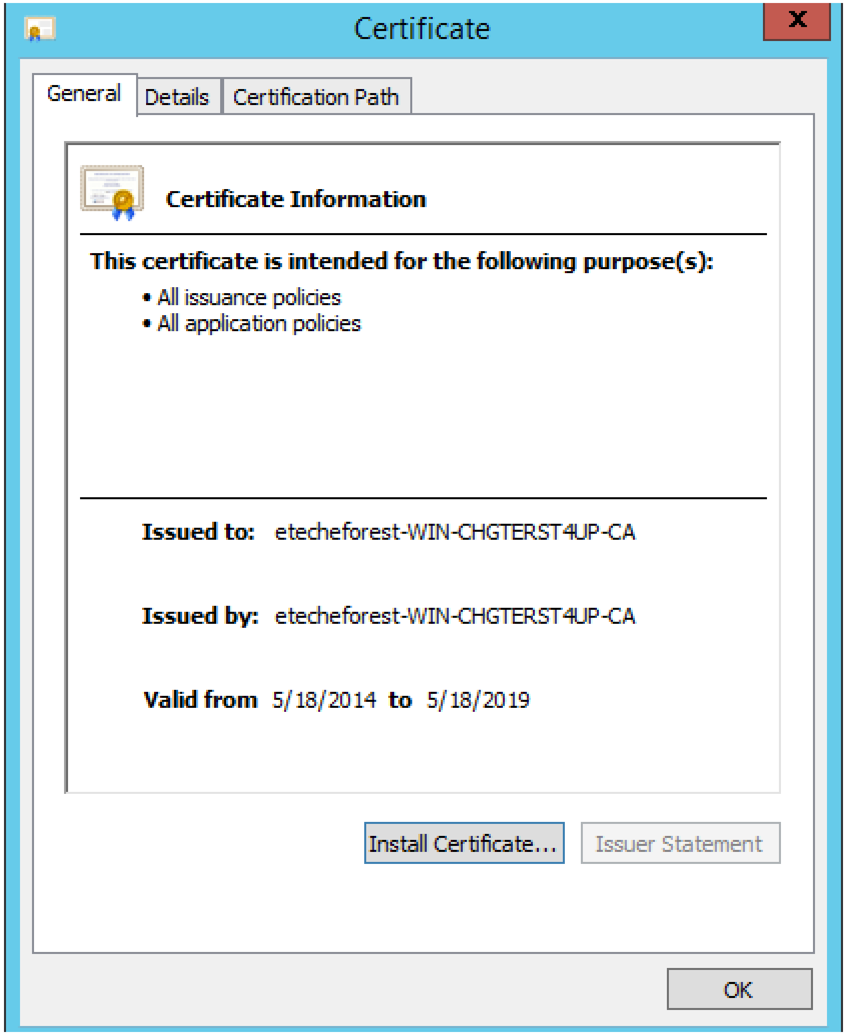
This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: etecheforest-WIN-CHGTERST4UP-CA

Issued by: etecheforest-WIN-CHGTERST4UP-CA

Valid from 5/18/2014 to 5/18/2019



Certificate Information

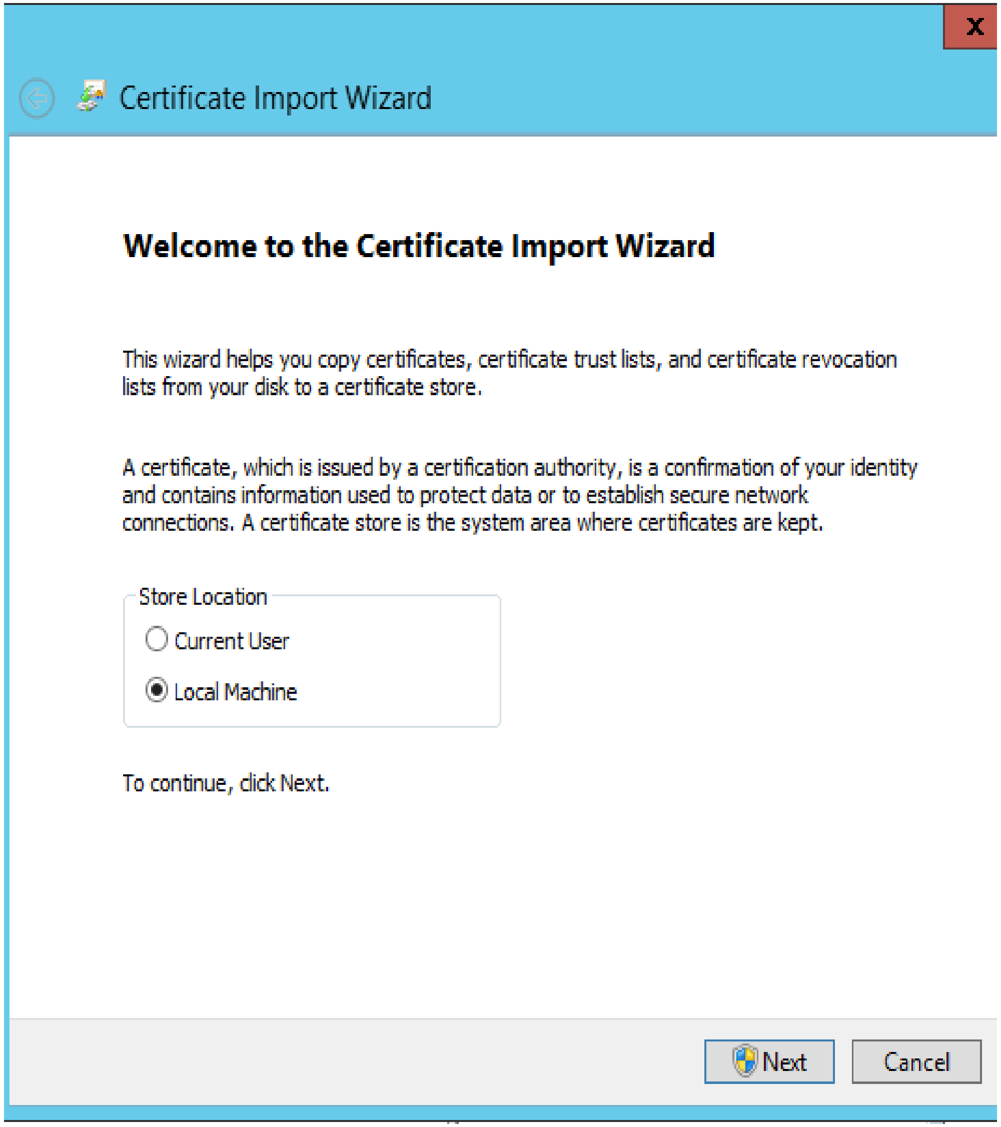
This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: etecheforest-WIN-CHGTERST4UP-CA

Issued by: etecheforest-WIN-CHGTERST4UP-CA

Valid from 5/18/2014 **to** 5/18/2019



Welcome to the Certificate Import Wizard

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

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.

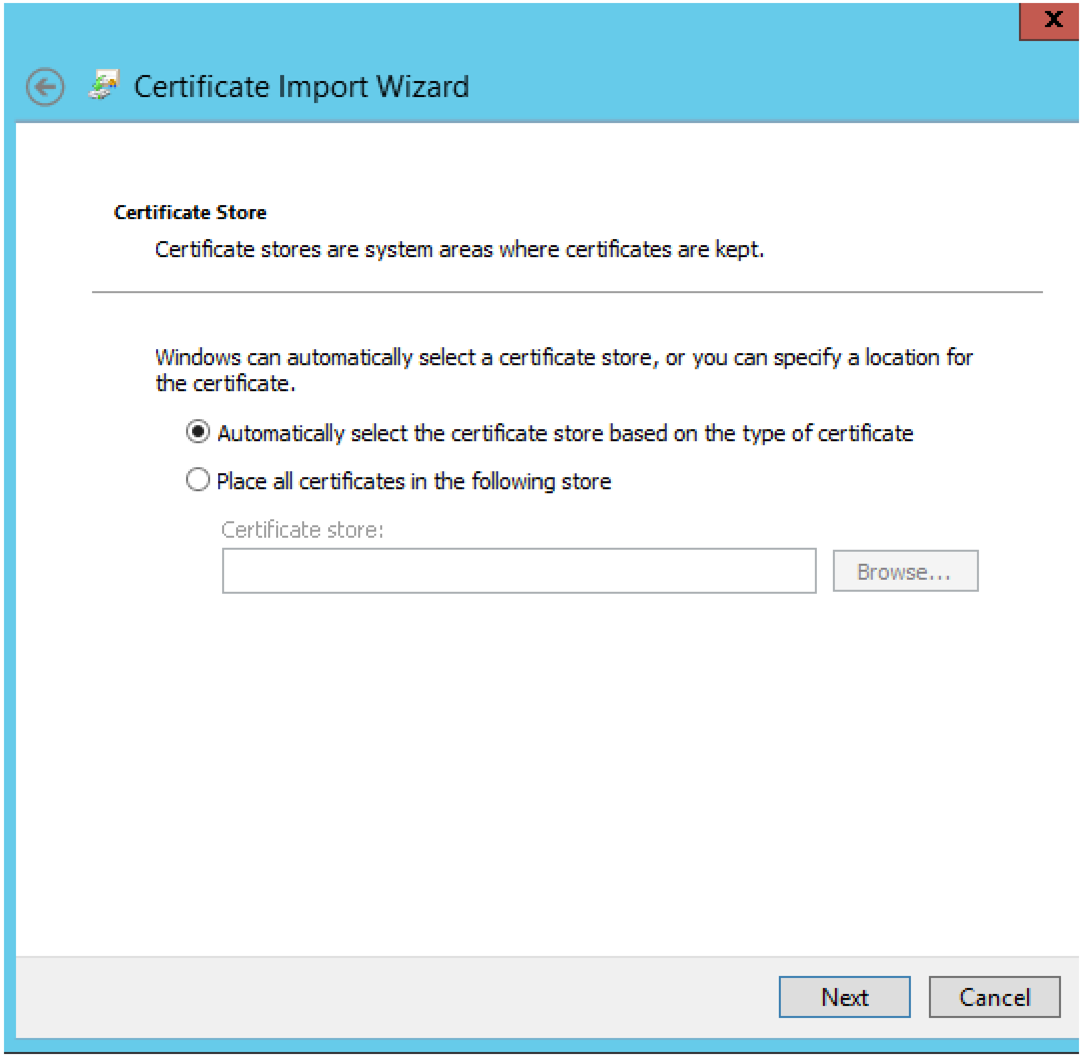
Store Location

○ Current User

● Local Machine

To continue, click Next.

Click on install then select local machine



Certificate Import Wizard

Certificate Store

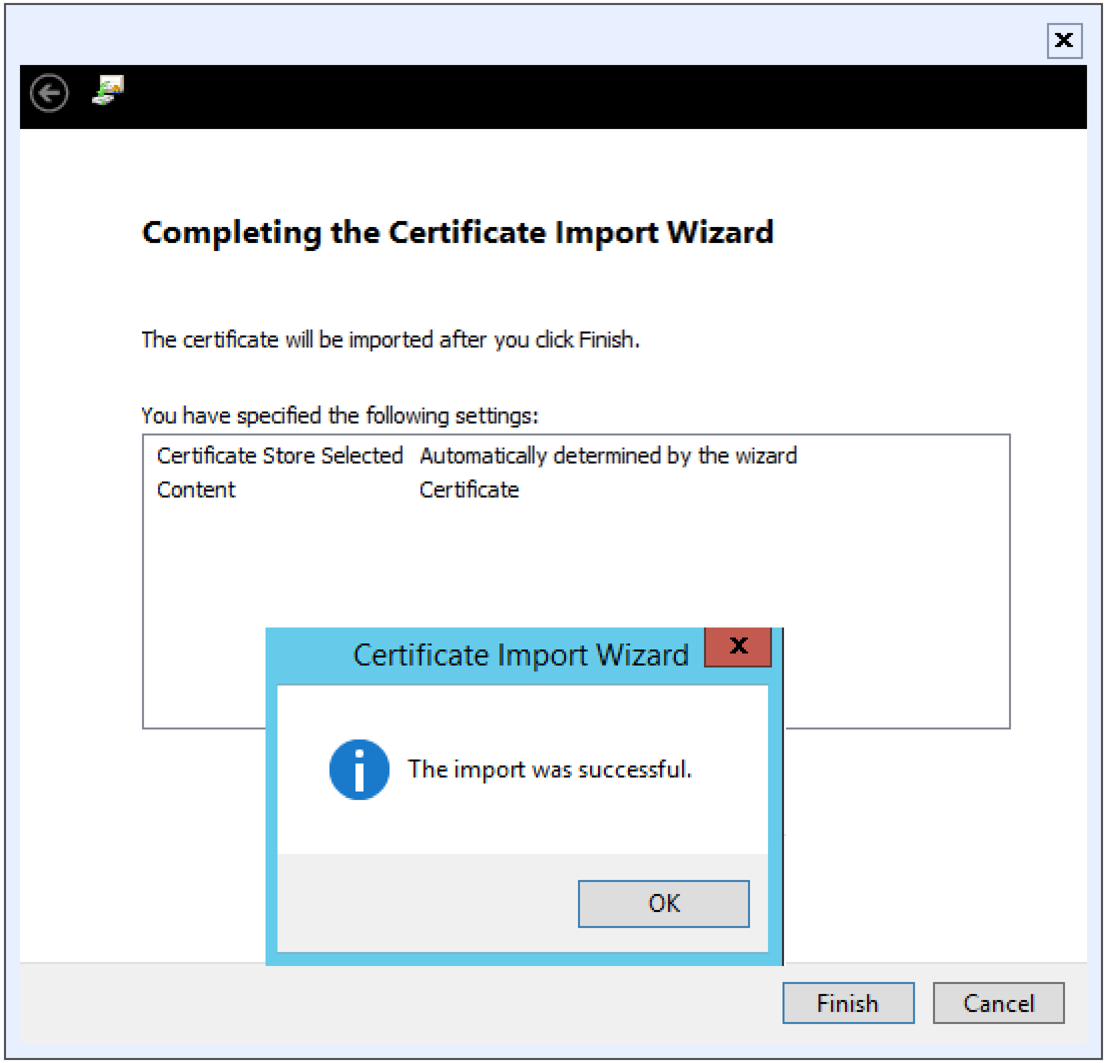
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:



Completing the Certificate Import Wizard

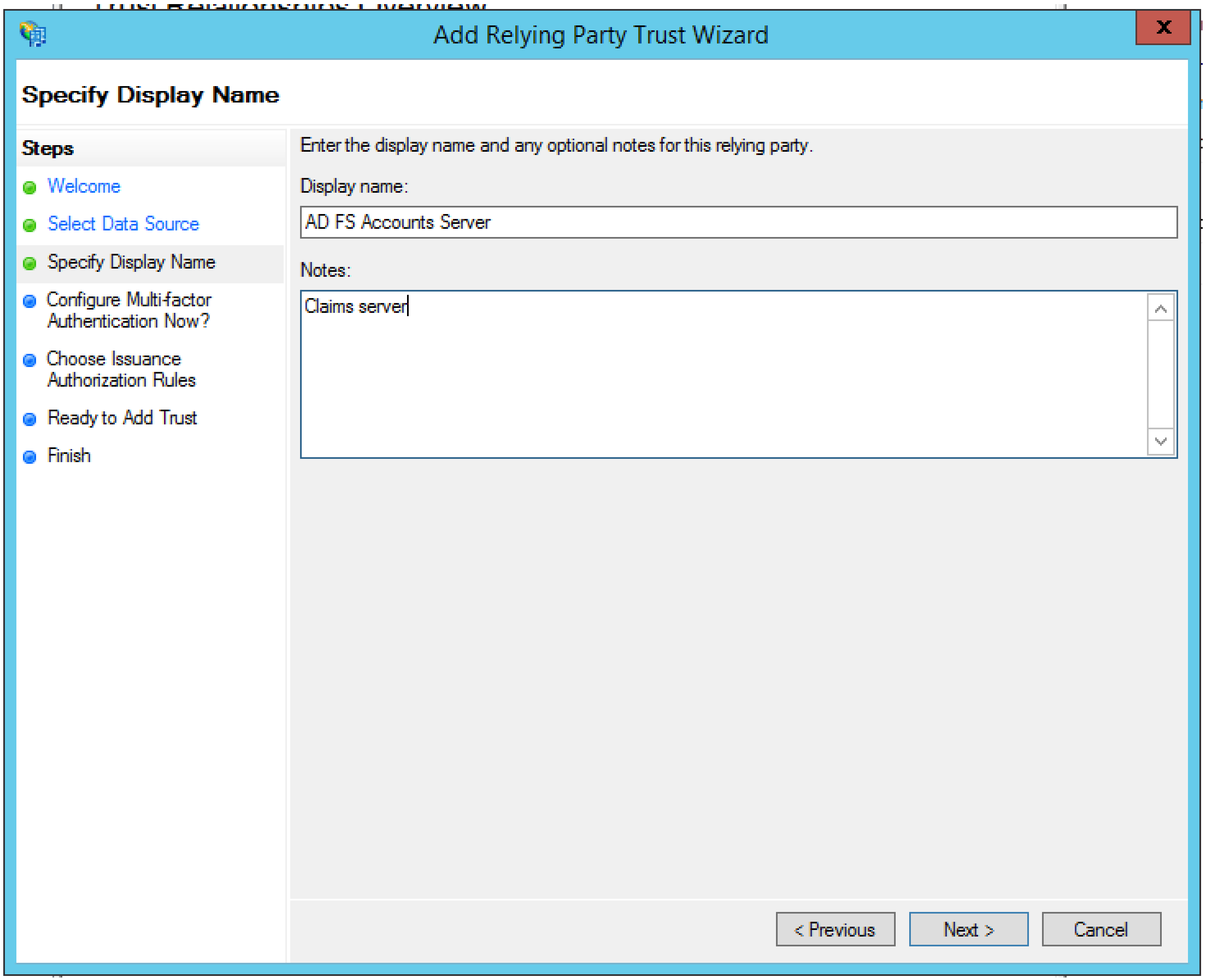
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected	Automatically determined by the wizard
Content	Certificate

Certificate Import Wizard

The import was successful.



Add Relying Party Trust Wizard
x

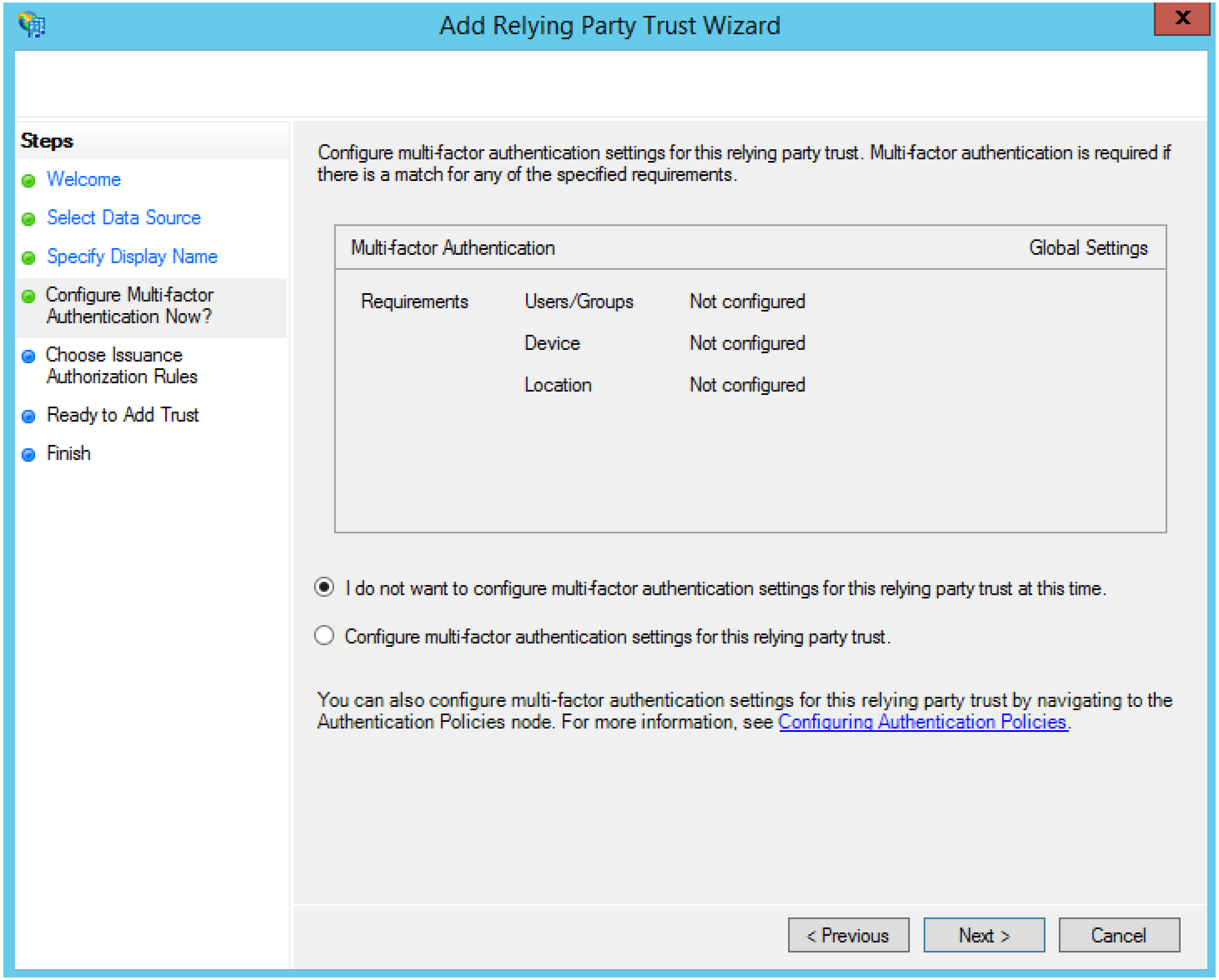
Specify Display Name

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

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

Display name: AD FS Accounts Server

Notes: Claims server



Steps

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

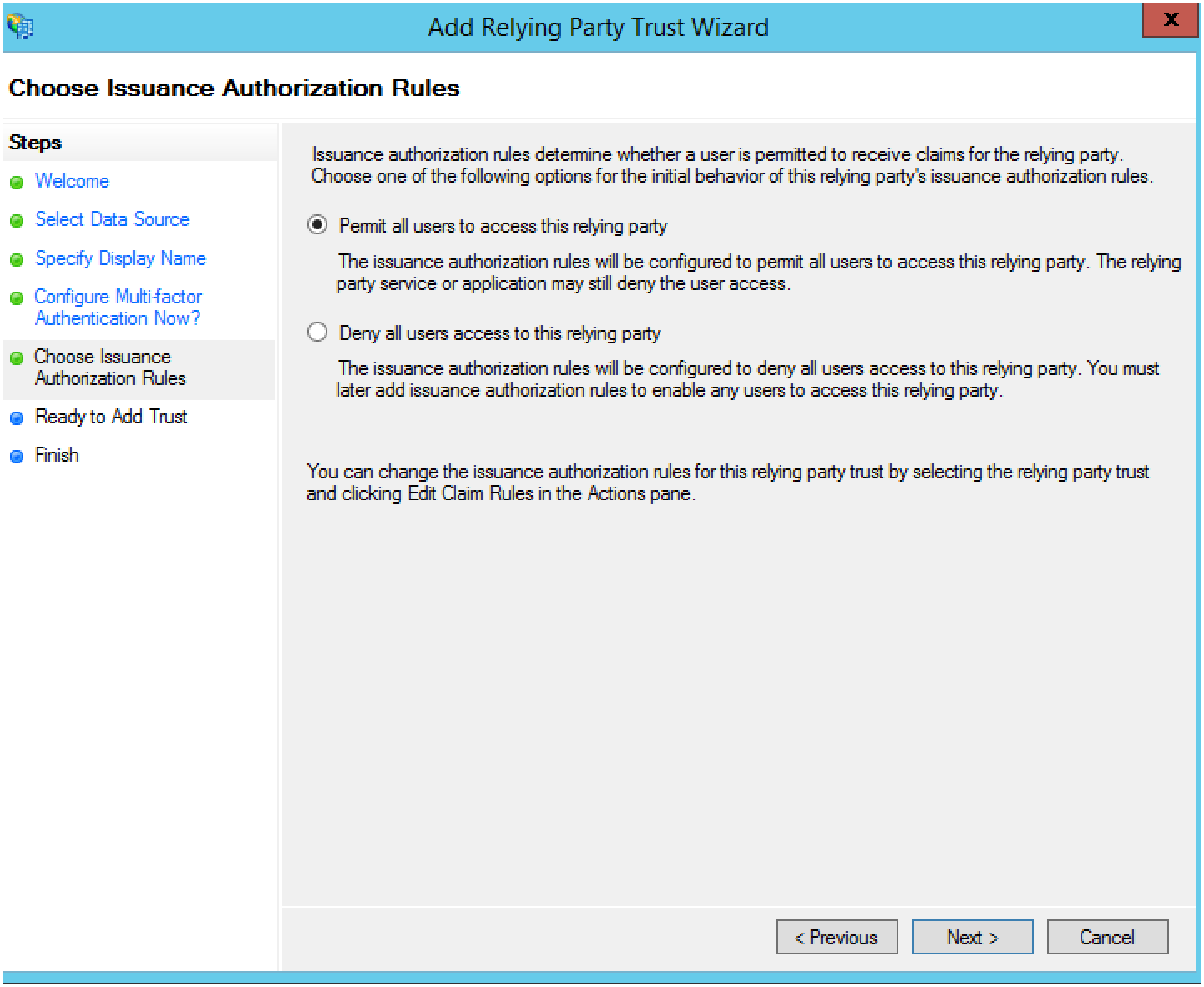
Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

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.



Add Relying Party Trust Wizard

Choose Issuance Authorization Rules

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

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.

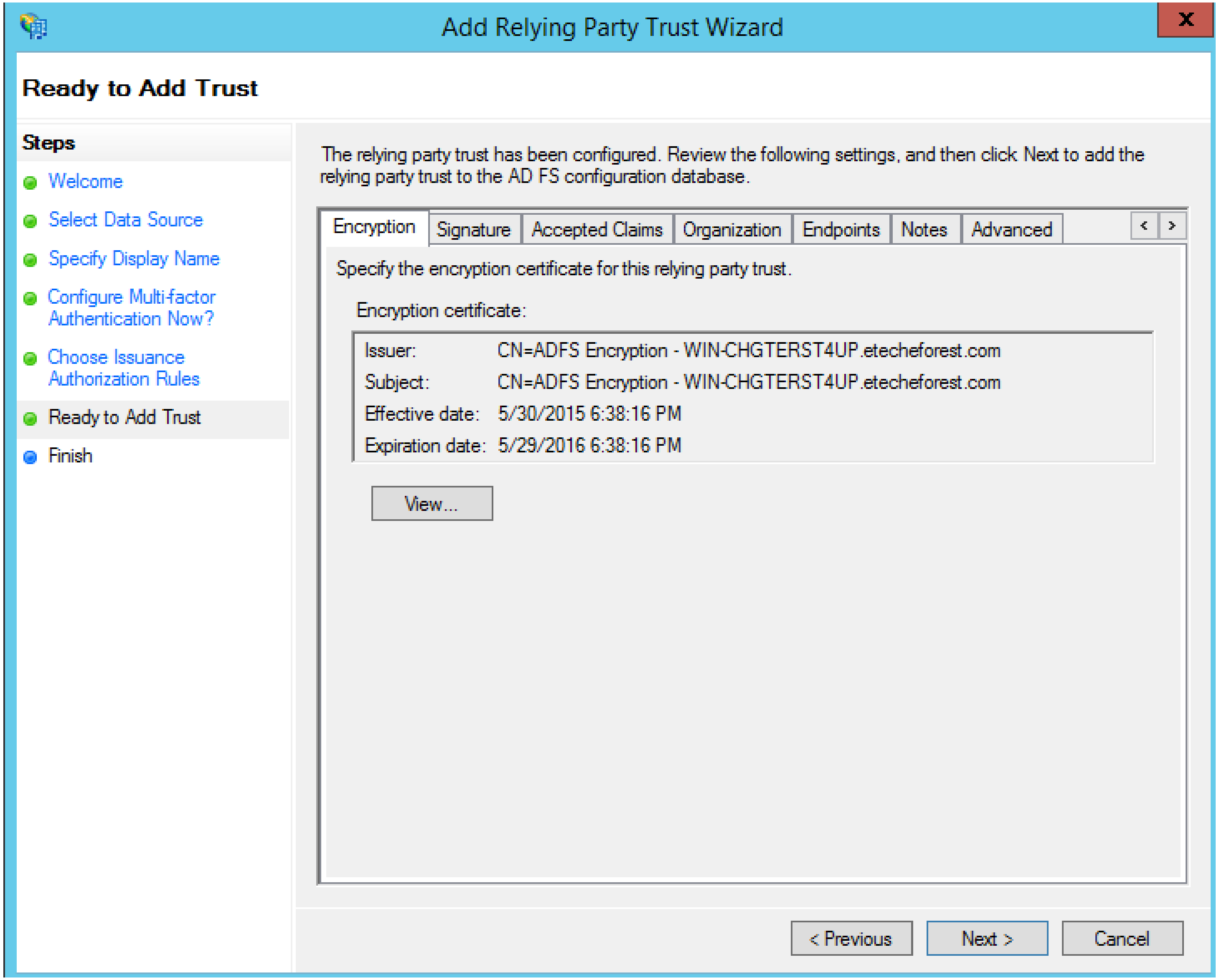
● Permit all users to access this relying party

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

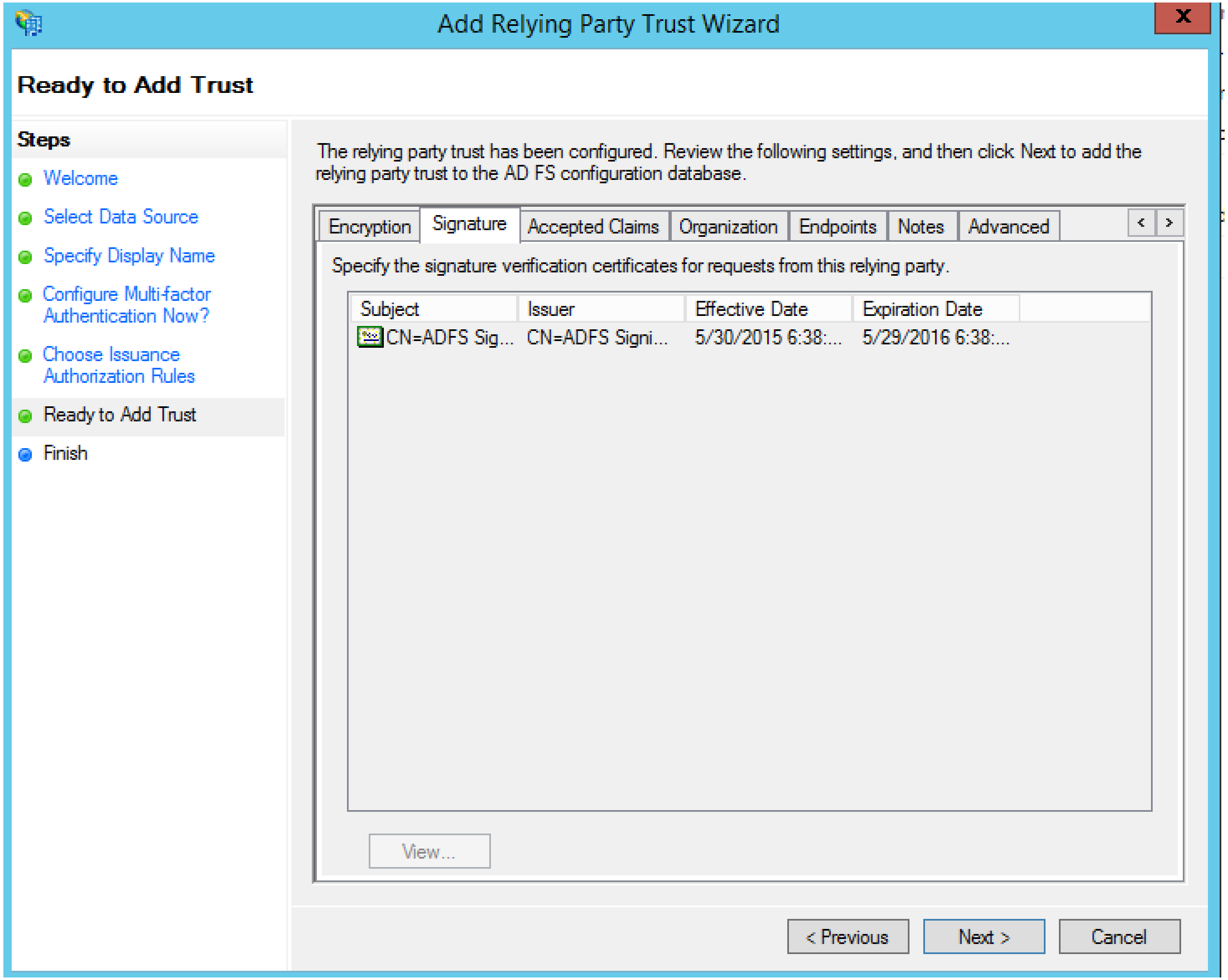
Steps
Welcome
Select Data Source
Specify Display Name
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish

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 encryption certificate for this relying party trust.

Encryption certificate:

Issuer:	CN=ADFS Encryption - WIN-CHGTERST4UP.etecheforest.com
Subject:	CN=ADFS Encryption - WIN-CHGTERST4UP.etecheforest.com
Effective date:	5/30/2015 6:38:16 PM
Expiration date:	5/29/2016 6:38:16 PM



Add Relying Party Trust Wizard

Ready to Add Trust

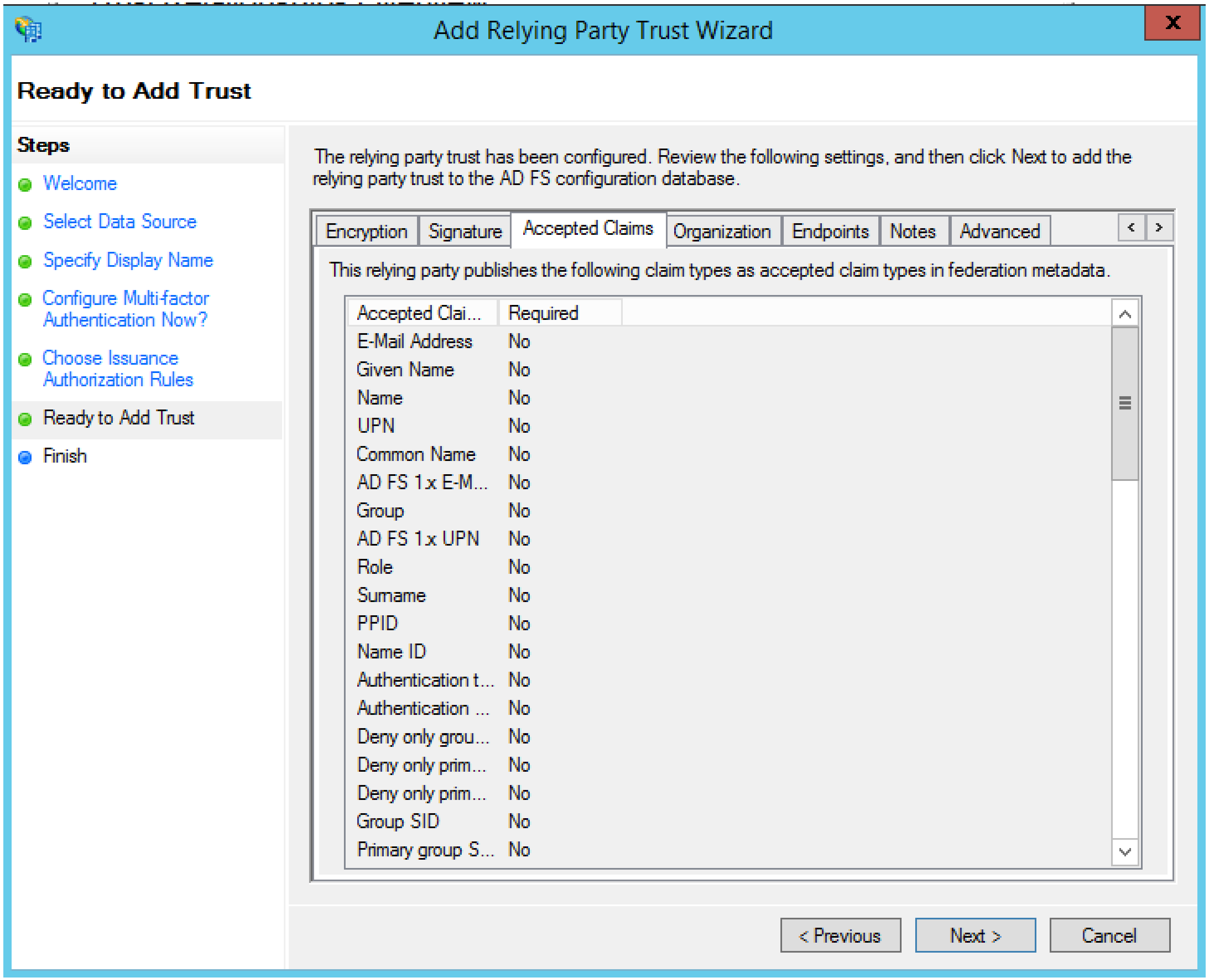
Steps

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

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 signature verification certificates for requests from this relying party.

Subject	Issuer	Effective Date	Expiration Date
CN=ADFS Sig...	CN=ADFS Signi...	5/30/2015 6:38:...	5/29/2016 6:38:...

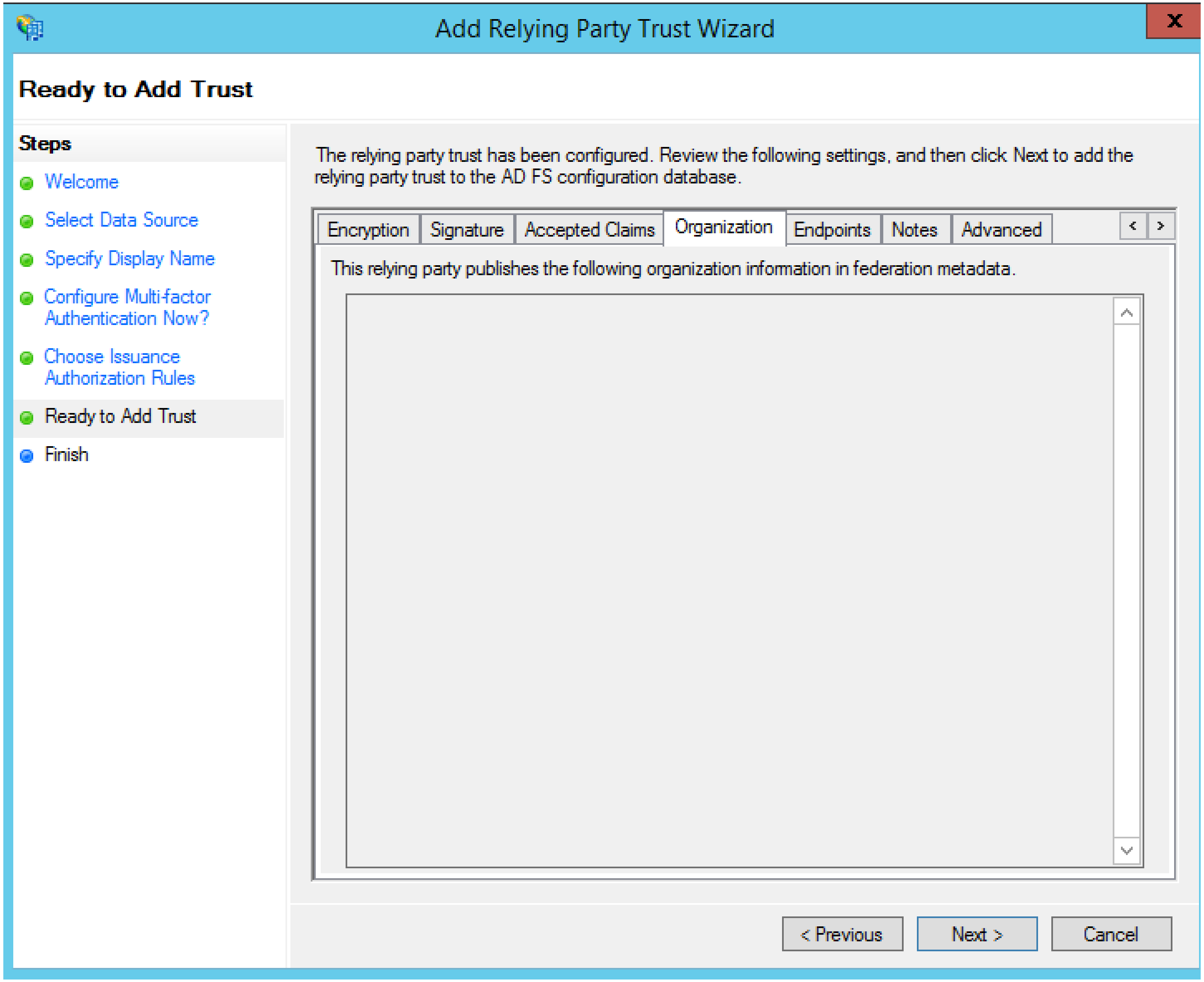


Ready to Add Trust

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.

This relying party publishes the following claim types as accepted claim types in federation metadata.

Accepted Clai...	Required
E-Mail Address	No
Given Name	No
Name	No
UPN	No
Common Name	No
AD FS 1.x E-M...	No
Group	No
AD FS 1.x UPN	No
Role	No
Surname	No
PPID	No
Name ID	No
Authentication t...	No
Authentication ...	No
Deny only grou...	No
Deny only prim...	No
Deny only prim...	No
Group SID	No
Primary group S...	No



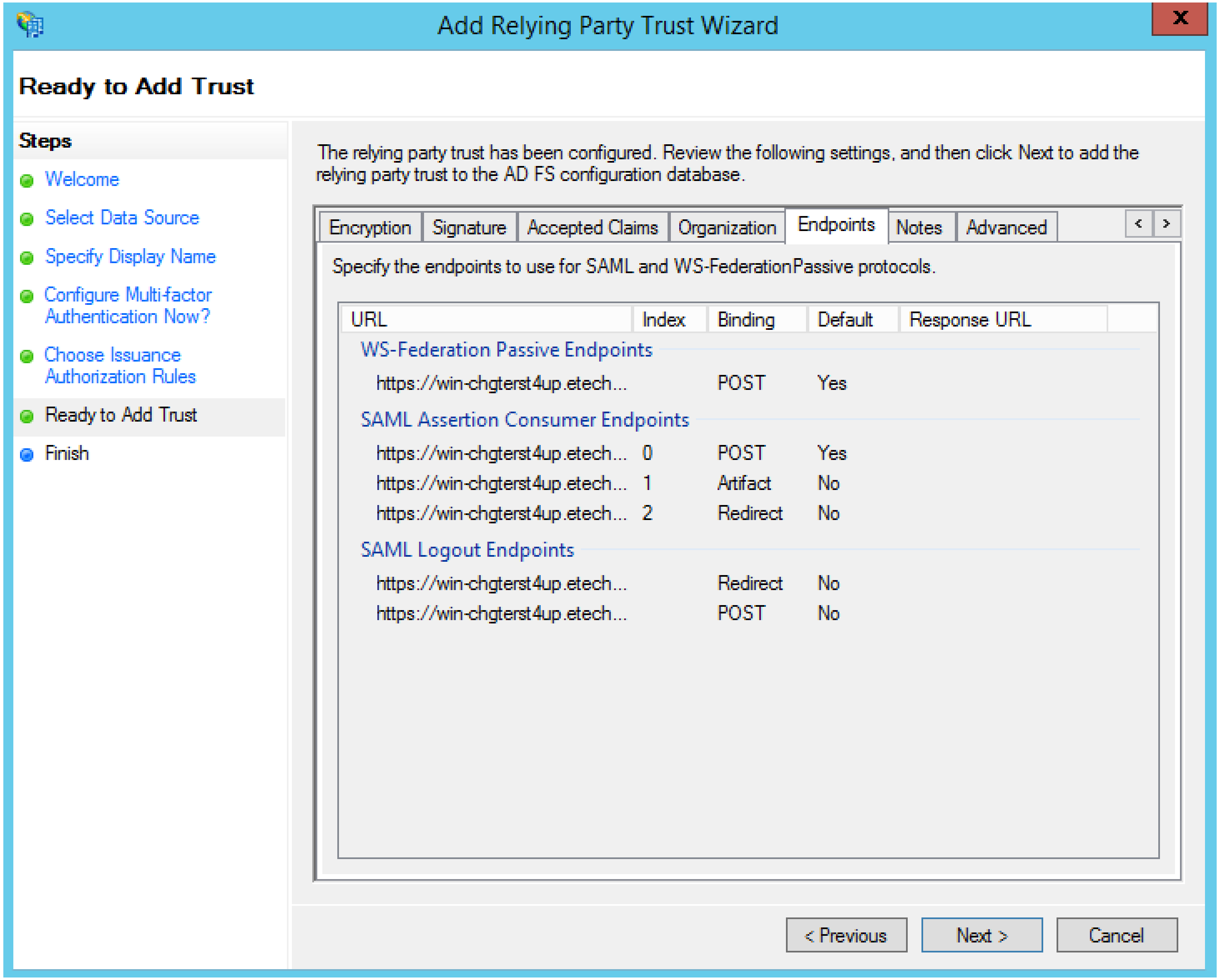
Add Relying Party Trust Wizard

Ready to Add Trust

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

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.

This relying party publishes the following organization information in federation metadata.



Ready to Add Trust

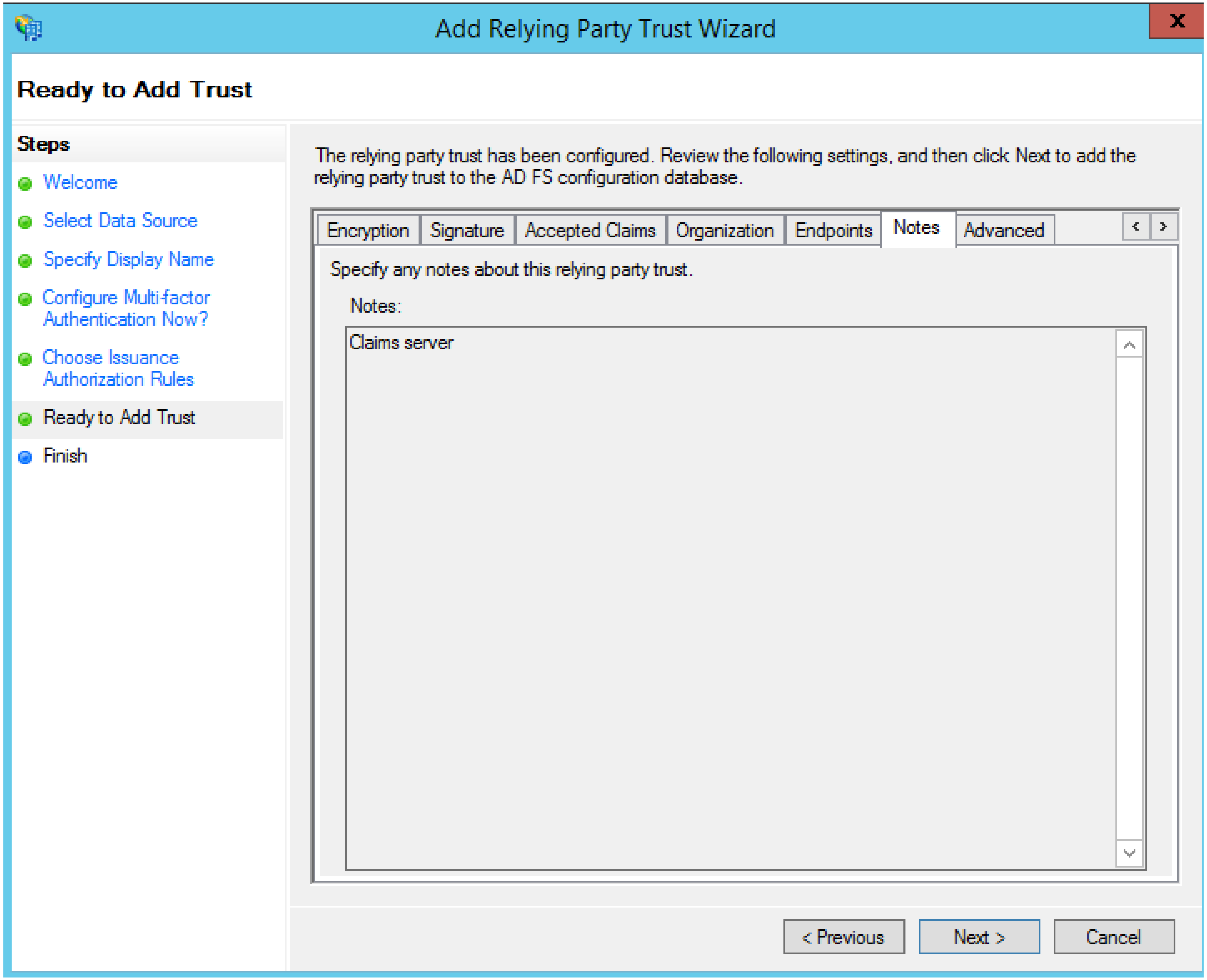
Steps

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

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 endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	Binding	Default	Response URL
WS-Federation Passive Endpoints				
https://win-chgterst4up.etech...		POST	Yes	
SAML Assertion Consumer Endpoints				
https://win-chgterst4up.etech...	0	POST	Yes	
https://win-chgterst4up.etech...	1	Artifact	No	
https://win-chgterst4up.etech...	2	Redirect	No	
SAML Logout Endpoints				
https://win-chgterst4up.etech...		Redirect	No	
https://win-chgterst4up.etech...		POST	No	



Add Relying Party Trust Wizard

Ready to Add Trust

Steps

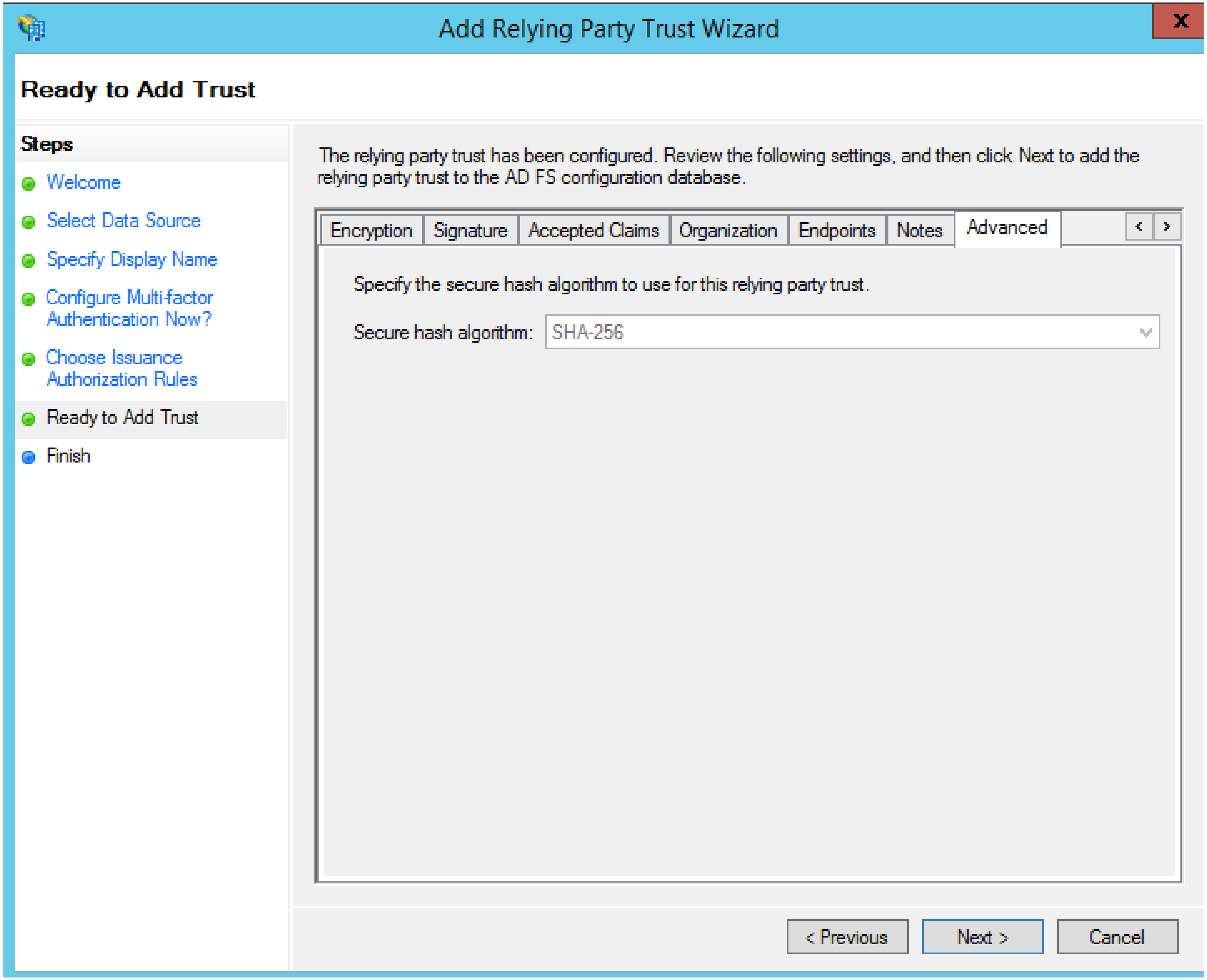
- ● Welcome
- ● Select Data Source
- ● Specify Display Name
- ● Configure Multi-factor Authentication Now?
- ● Choose Issuance Authorization Rules
- ● Ready to Add Trust
- ● Finish

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 any notes about this relying party trust.

Notes:

Claims server



Ready to Add Trust

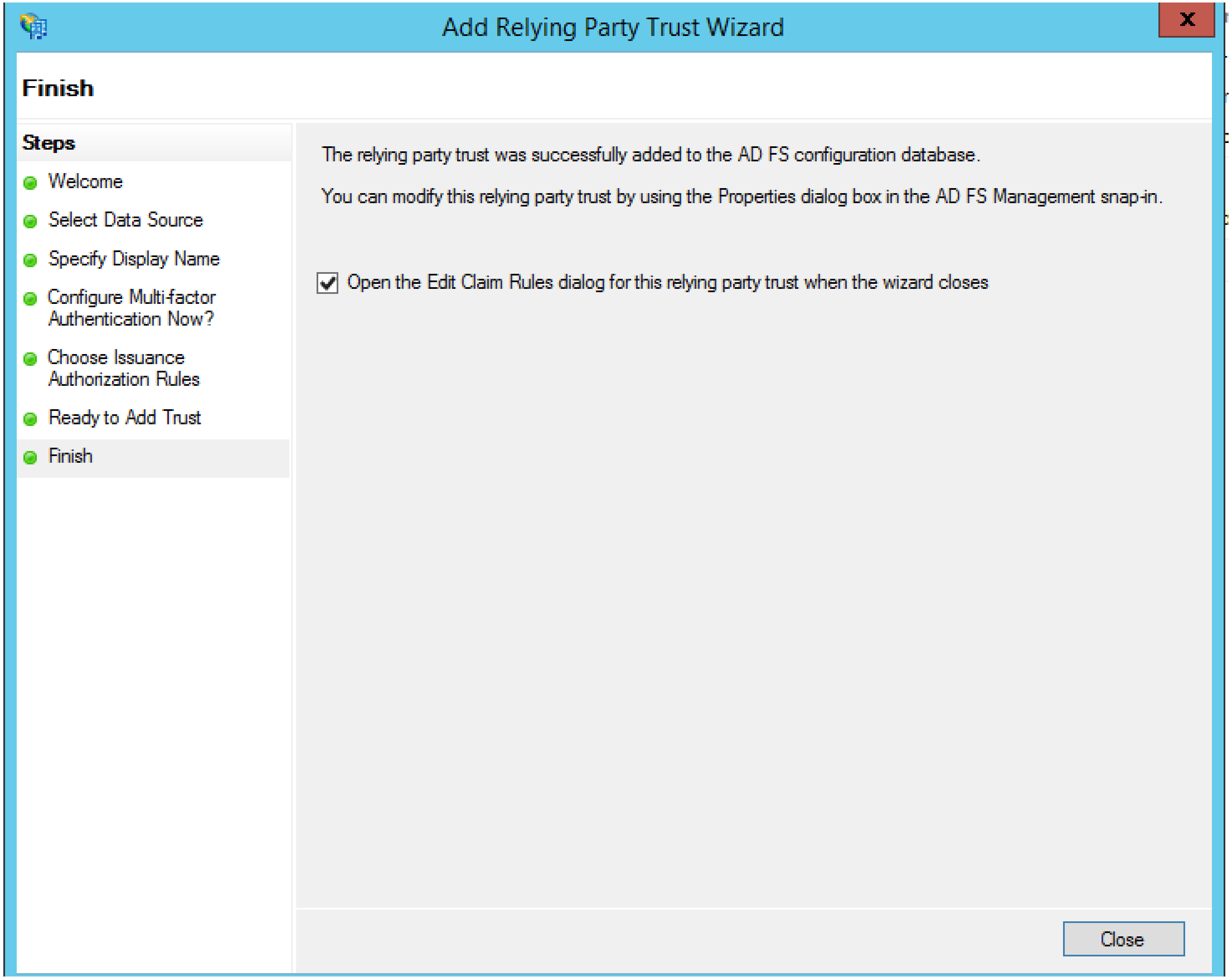
Steps

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

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 secure hash algorithm to use for this relying party trust.

Secure hash algorithm: SHA-256



Finish

Steps

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

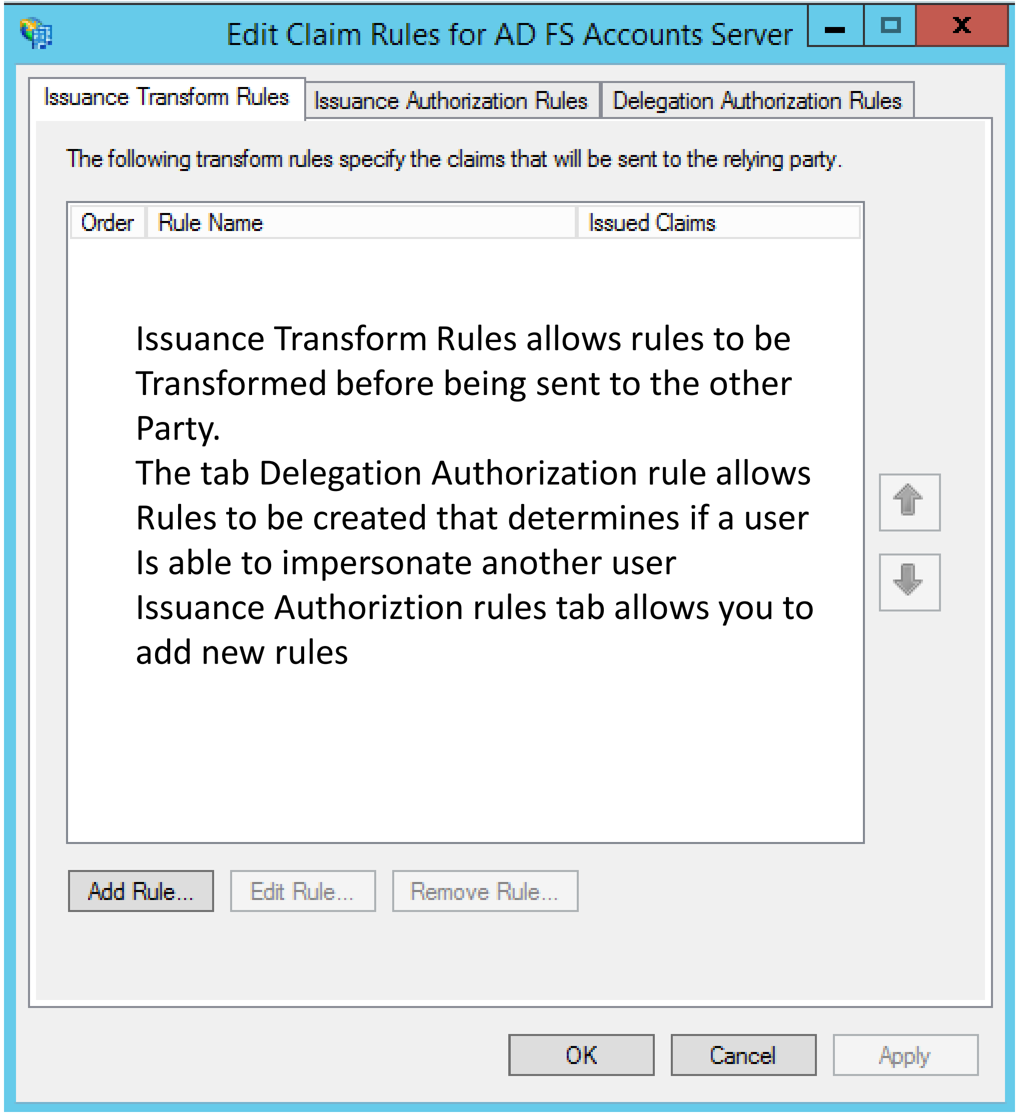
The relying party trust was successfully added to the AD FS configuration database.

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

Editing claims

Right click the Relying Trust and click on Edit claims rules



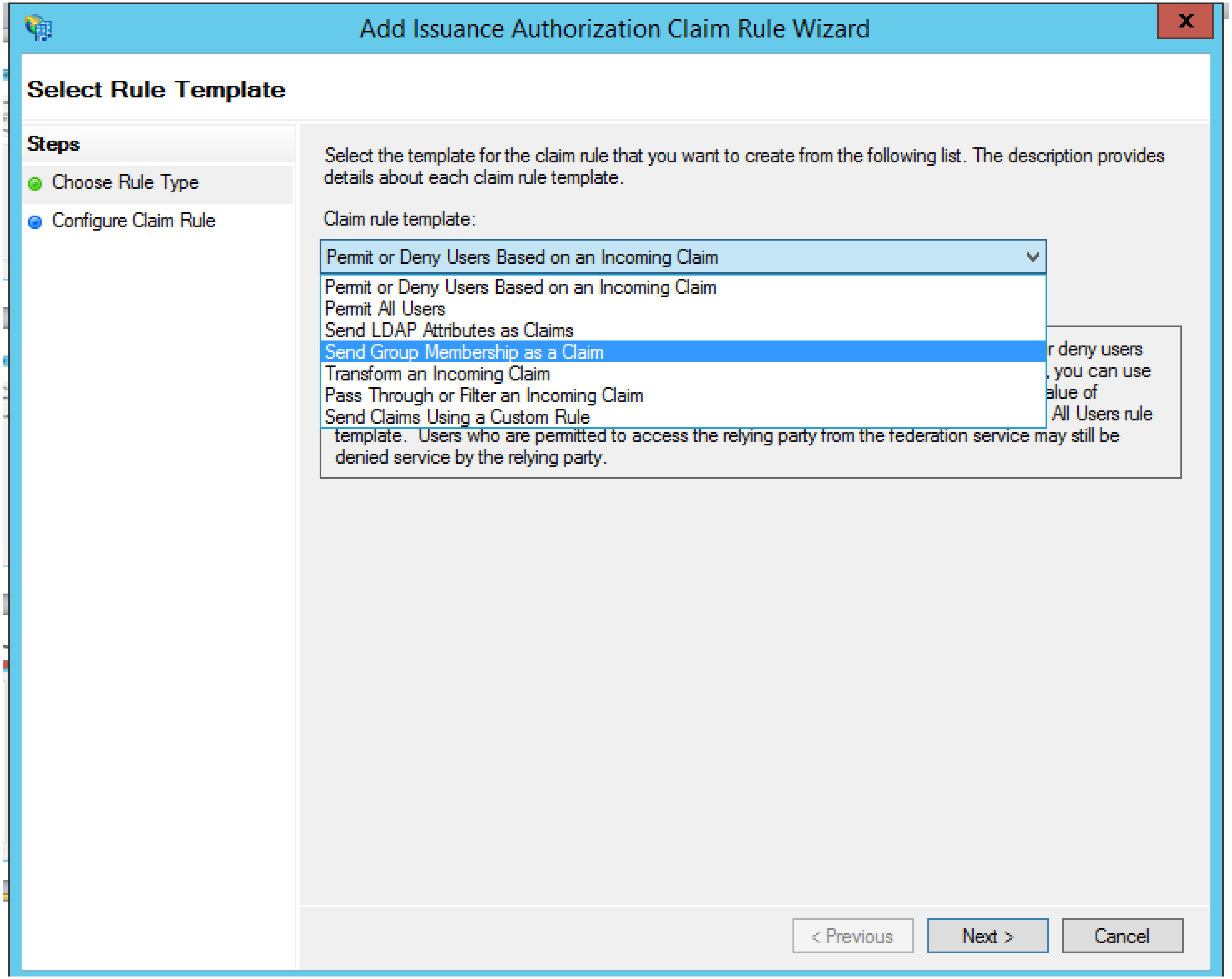
Edit Claim Rules for AD FS Accounts Server
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules

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

Order	Rule Name	Issued Claims

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

Issuance Transform Rules allows rules to be Transformed before being sent to the other Party.
The tab Delegation Authorization rule allows Rules to be created that determines if a user Is able to impersonate another user
Issuance Authoriztion rules tab allows you to add new rules



Add Issuance Authorization Claim Rule Wizard

Select Rule Template

Steps

- Choose Rule Type
- Configure Claim Rule

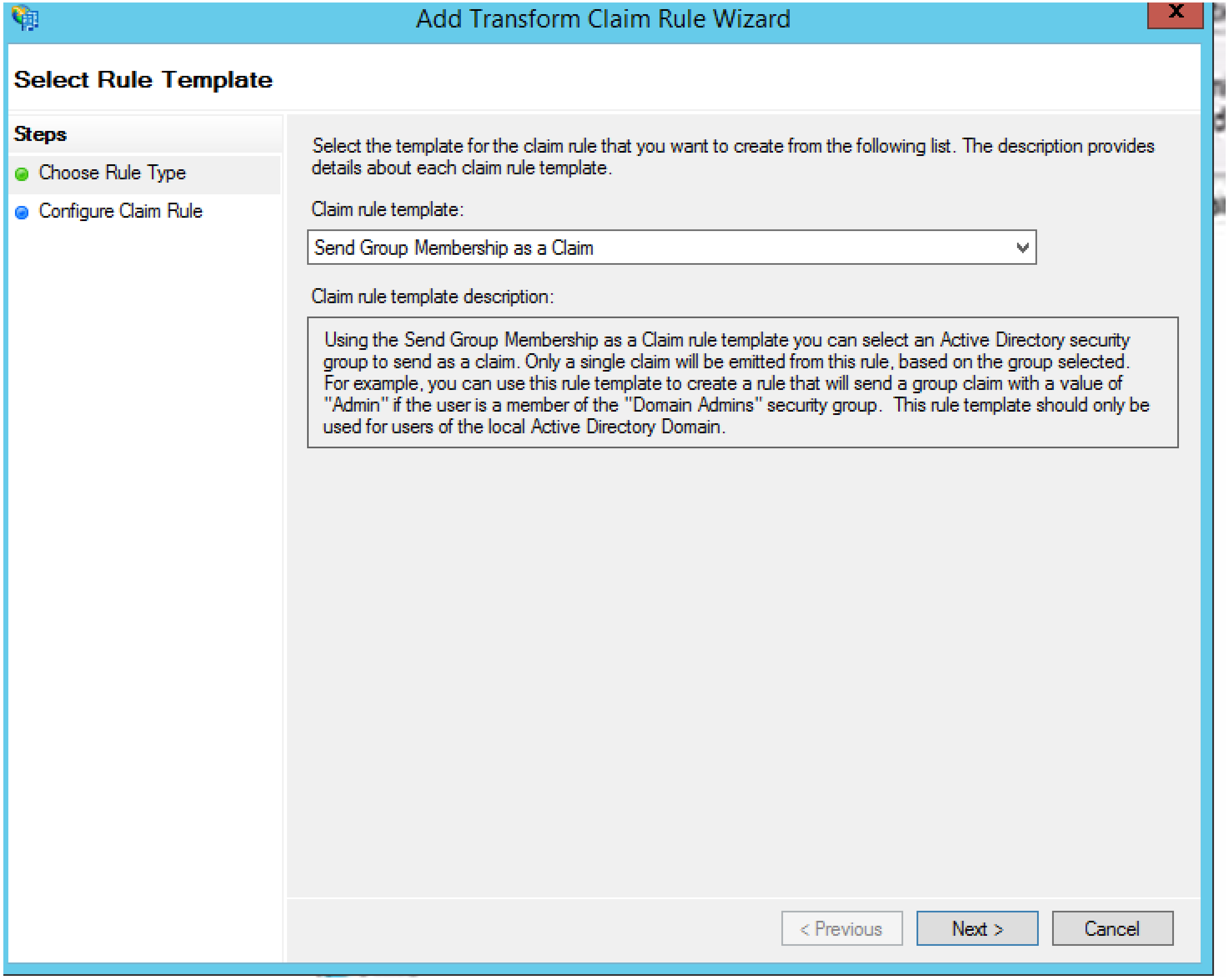
Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Permit or Deny Users Based on an Incoming Claim

- Permit or Deny Users Based on an Incoming Claim
- Permit All Users
- Send LDAP Attributes as Claims
- Send Group Membership as a Claim
- Transform an Incoming Claim
- Pass Through or Filter an Incoming Claim
- Send Claims Using a Custom Rule

r deny users
, you can use
alue of
All Users rule
template. Users who are permitted to access the relying party from the federation service may still be denied service by the relying party.



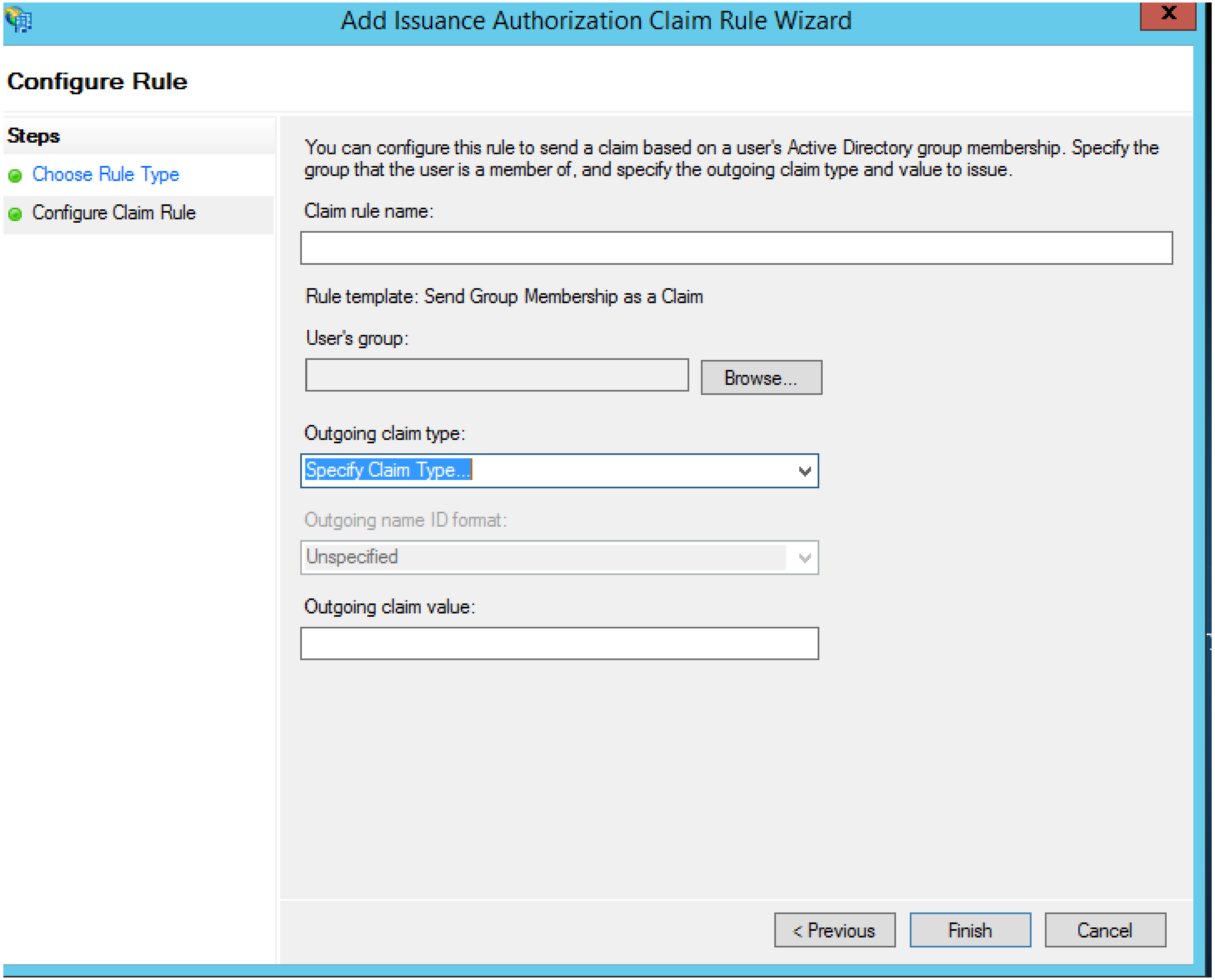
Select Rule Template

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.



Add Issuance Authorization Claim Rule Wizard

Configure Rule

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:

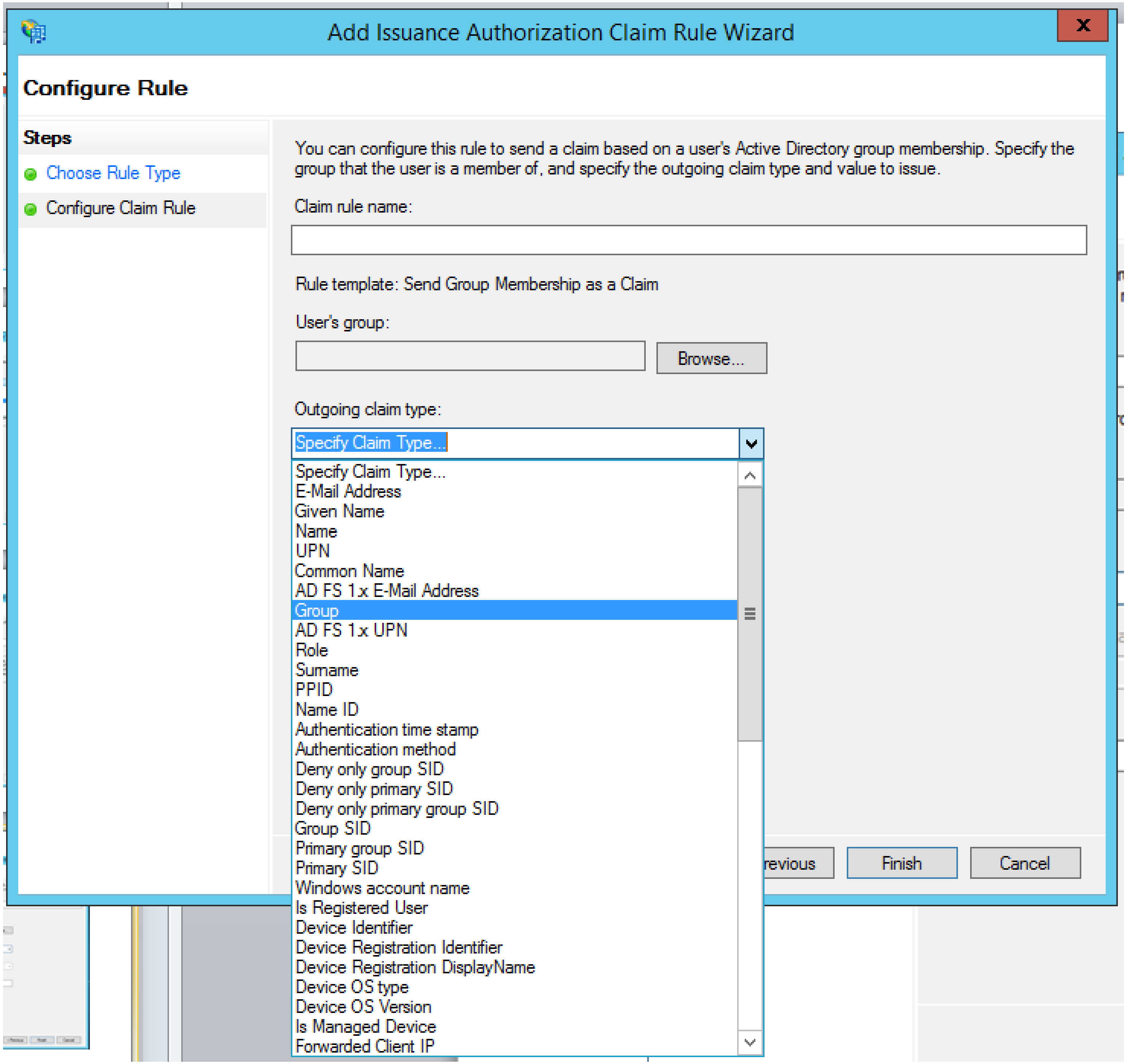
Rule template: Send Group Membership as a Claim

User's group:

Outgoing claim type: Specify Claim Type...

Outgoing name ID format: Unspecified

Outgoing claim value:



Add Issuance Authorization Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

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:

Rule template: Send Group Membership as a Claim

User's group:

Outgoing claim type:

Specify Claim Type...