PACIFIC
TIMESHEET.

Configuring Active Directory Federation Services for SSO using SAML 2.0 with Pacific Timesheet

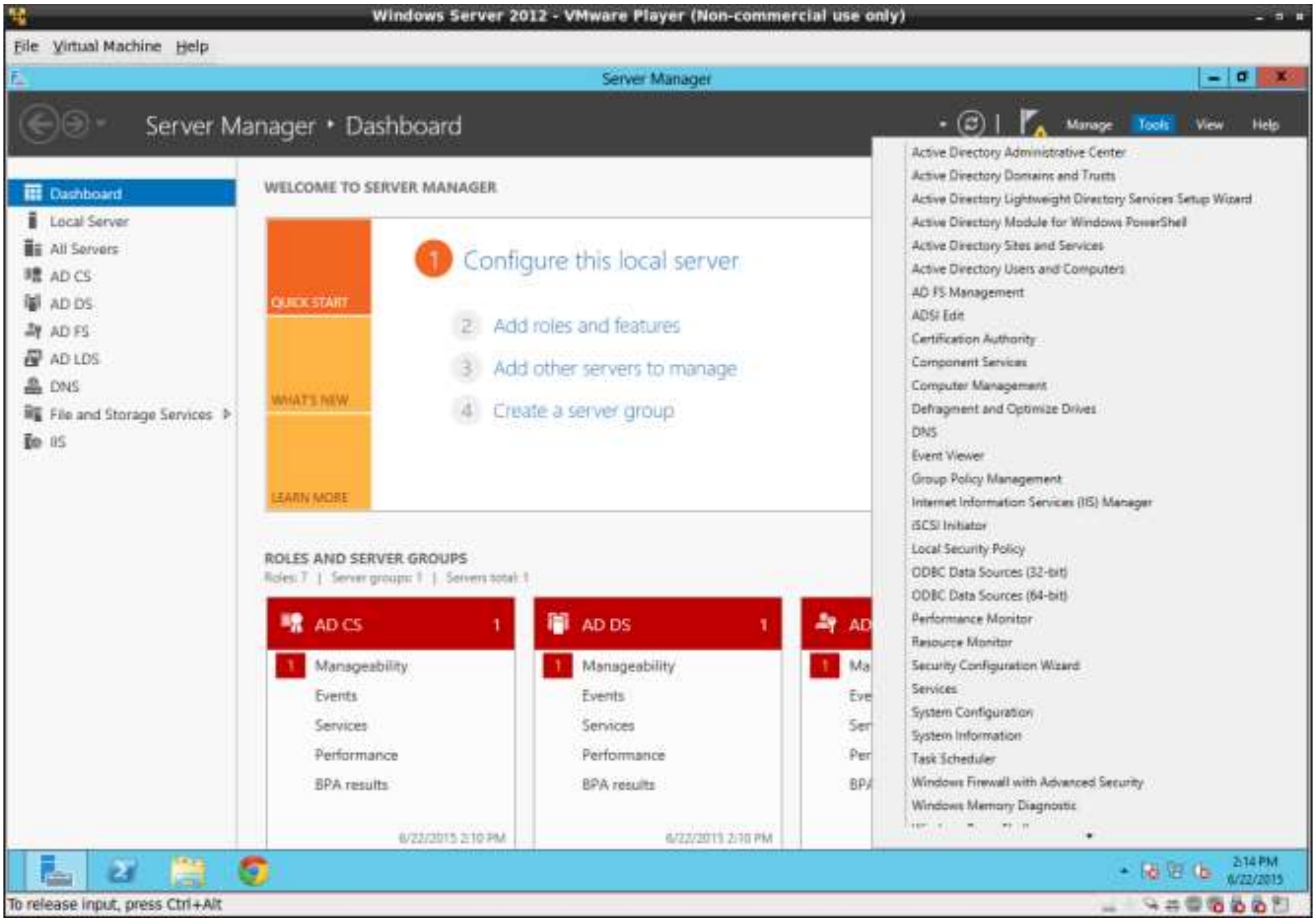
Last Update: October 15, 2015

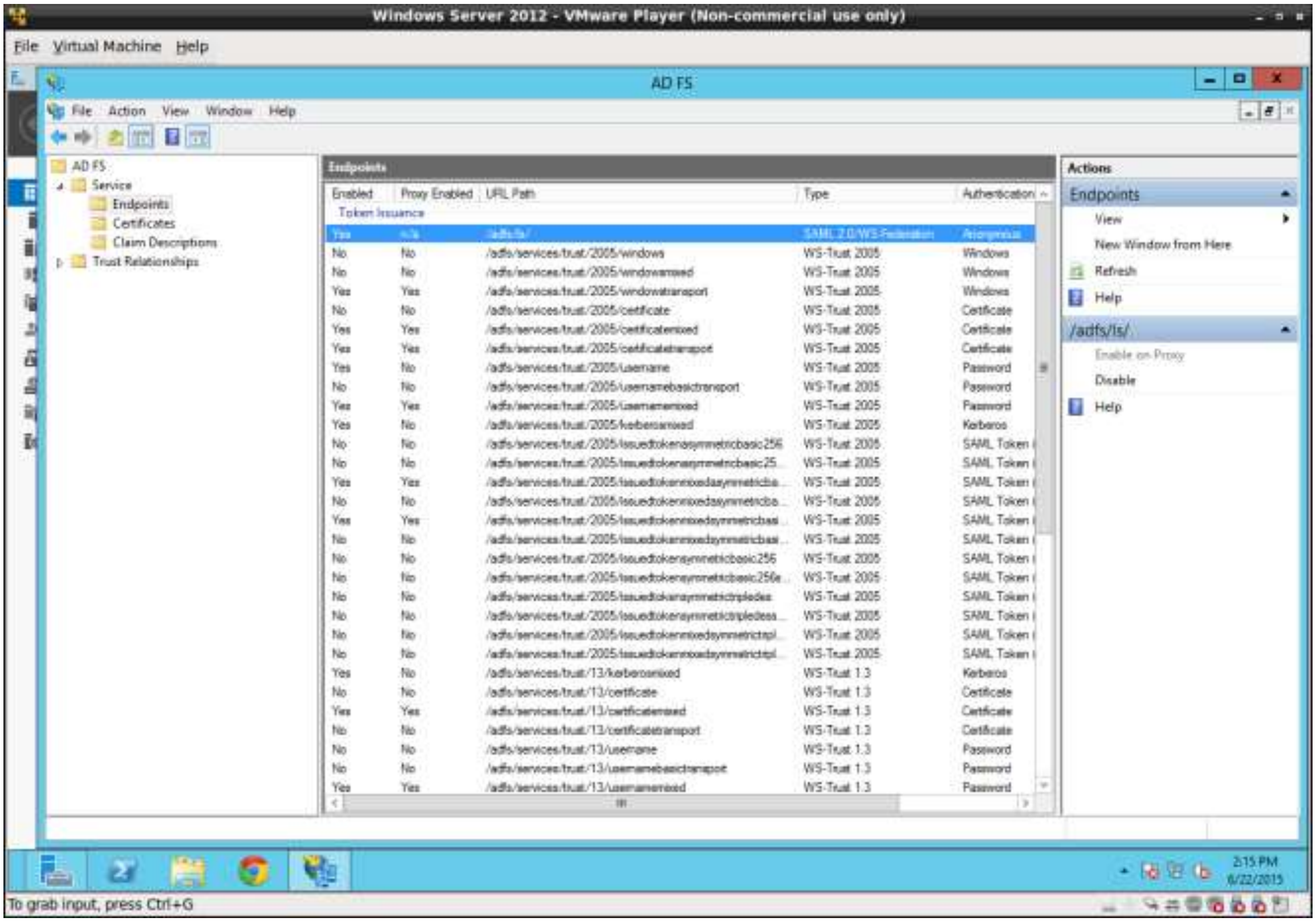
Background

You can connect Active Directory Federation Services (AD FS) Single Sign-On (SSO), as an identity provider, with Pacific Timesheet as a cloud-based application. The steps to configure AD FS SSO to connect with Pacific Timesheet first must be completed within AD FS SSO configuration tools, then certain SSO settings must be completed in Pacific Timesheet's AD FS SSO SAML 2.0 settings under system>security>authentication. AD FS does not currently have a cloud applications catalog like Azure Active Directory. If you have an Azure Active Directory account and you want to connect your SSO with Pacific Timesheet proceed to the Azure Active Directory cloud application catalog, search for Pacific Timesheet and follow the instructions there. Whether you are using Pacific Timesheet on-premise or in the cloud, the procedure is the same as here, requiring that you to manually setup a Pacific Timesheet application in AD FS, then complete the setup of your AD FS SSO SAML 2.0 connection within Pacific Timesheet.

This thirty-one-page guide provides detailed step-by-step instructions on how to setup AD FS SSO and then Pacific Timesheet to enable Single Sign-On for your users.

Startup AD FS Management and go to the Server Manager Dashboard.

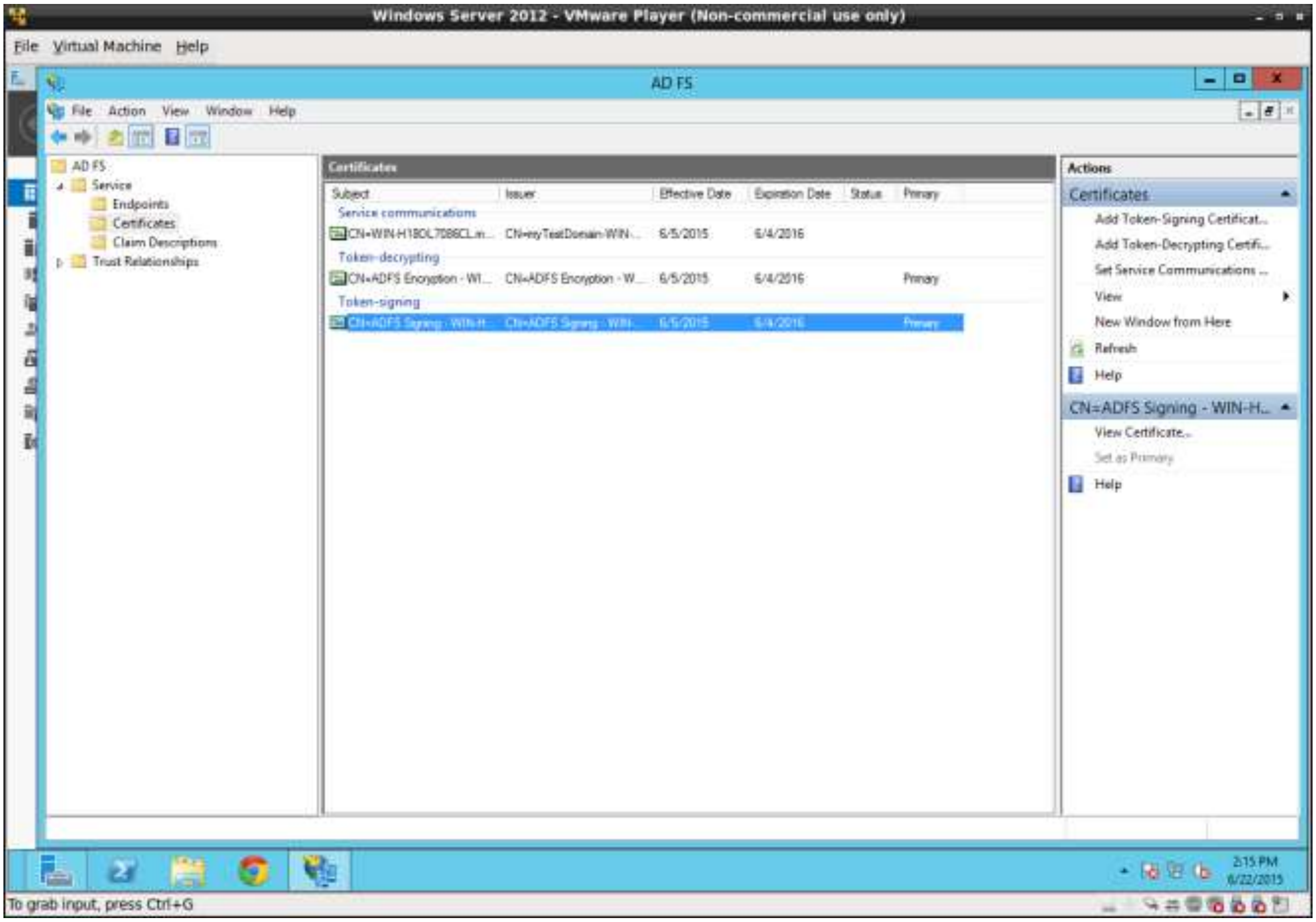

Windows Server 2012 - VMware Player (Non-commercial use only)
File Virtual Machine Help
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD CS
AD DS
AD FS
AD LDS
DNS
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
ROLES AND SERVER GROUPS
Roles: 7 | Server groups: 1 | Servers total: 1
AD CS 1
1 Manageability
Events
Services
Performance
BPA results
6/22/2015 2:10 PM
AD DS 1
1 Manageability
Events
Services
Performance
BPA results
6/22/2015 2:10 PM
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Lightweight Directory Services Setup Wizard
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
AD FS Management
ADSI Edit
Certification Authority
Component Services
Computer Management
Defragment and Optimize Drives
DNS
Event Viewer
Group Policy Management
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Resource Monitor
Security Configuration Wizard
Services
System Configuration
System Information
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic
2:14 PM
6/22/2015
To release input, press Ctrl+Alt



Enabled	Proxy Enabled	URL Path	Type	Authentication
Token Issuance				
Yes	n/a	/adfs/ls/	SAML 2.0/WS-Federation	Anonymous
No	No	/adfs/services/trust/2005/windows	WS-Trust 2005	Windows
No	No	/adfs/services/trust/2005/windowsmixed	WS-Trust 2005	Windows
Yes	Yes	/adfs/services/trust/2005/windowstransport	WS-Trust 2005	Windows
No	No	/adfs/services/trust/2005/certificate	WS-Trust 2005	Certificate
Yes	Yes	/adfs/services/trust/2005/certificatemixed	WS-Trust 2005	Certificate
Yes	Yes	/adfs/services/trust/2005/certificatetransport	WS-Trust 2005	Certificate
Yes	No	/adfs/services/trust/2005/username	WS-Trust 2005	Password
No	No	/adfs/services/trust/2005/usernamebasictransport	WS-Trust 2005	Password
Yes	Yes	/adfs/services/trust/2005/usernamemixed	WS-Trust 2005	Password
Yes	No	/adfs/services/trust/2005/kerberosmixed	WS-Trust 2005	Kerberos
No	No	/adfs/services/trust/2005/issuedtokenasymmetricbasic256	WS-Trust 2005	SAML Token (
No	No	/adfs/services/trust/2005/issuedtokenasymmetricbasic25...	WS-Trust 2005	SAML Token (
Yes	Yes	/adfs/services/trust/2005/issuedtokenmixedasymmetricba...	WS-Trust 2005	SAML Token (
No	No	/adfs/services/trust/2005/issuedtokenmixedasymmetricba...	WS-Trust 2005	SAML Token (
Yes	Yes	/adfs/services/trust/2005/issuedtokenmixedsymmetricbasi...	WS-Trust 2005	SAML Token (
No	No	/adfs/services/trust/2005/issuedtokenmixedsymmetricbasi...	WS-Trust 2005	SAML Token (
No	No	/adfs/services/trust/2005/issuedtokensymmetricbasic256	WS-Trust 2005	SAML Token (
No	No	/adfs/services/trust/2005/issuedtokensymmetricbasic256s...	WS-Trust 2005	SAML Token (
No	No	/adfs/services/trust/2005/issuedtokensymmetrictripledes	WS-Trust 2005	SAML Token (
No	No	/adfs/services/trust/2005/issuedtokensymmetrictripledess...	WS-Trust 2005	SAML Token (
No	No	/adfs/services/trust/2005/issuedtokenmixedsymmetrictripl...	WS-Trust 2005	SAML Token (
No	No	/adfs/services/trust/2005/issuedtokenmixedsymmetrictripl...	WS-Trust 2005	SAML Token (
Yes	No	/adfs/services/trust/13/kerberosmixed	WS-Trust 1.3	Kerberos
No	No	/adfs/services/trust/13/certificate	WS-Trust 1.3	Certificate
Yes	Yes	/adfs/services/trust/13/certificatemixed	WS-Trust 1.3	Certificate
No	No	/adfs/services/trust/13/certificatetransport	WS-Trust 1.3	Certificate
No	No	/adfs/services/trust/13/username	WS-Trust 1.3	Password
No	No	/adfs/services/trust/13/usernamebasictransport	WS-Trust 1.3	Password
Yes	Yes	/adfs/services/trust/13/usernamemixed	WS-Trust 1.3	Password

Check Your End Service Endpoints

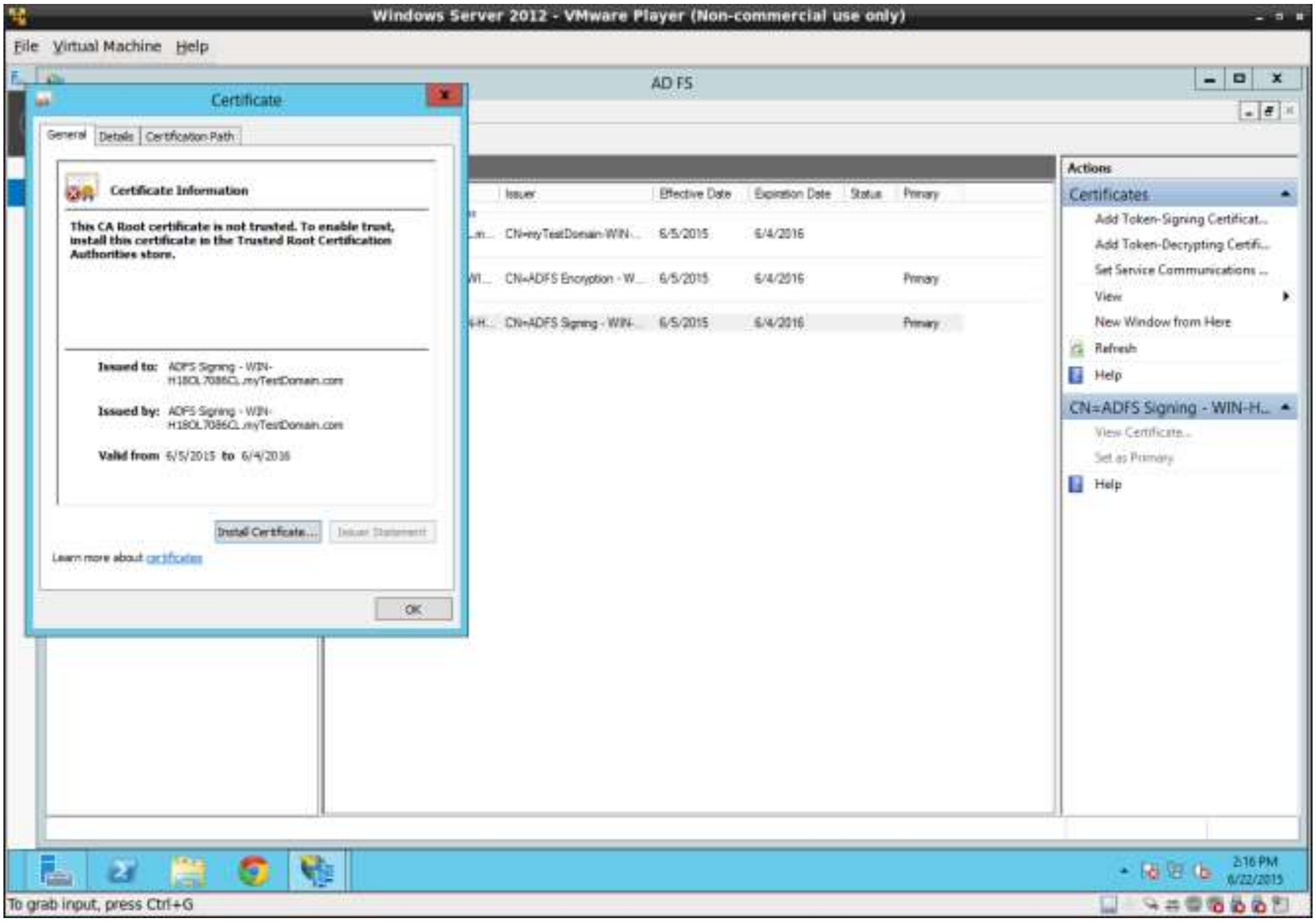
Make sure that you have an endpoint for SAML requests. You will need this URL to configure Pacific Timesheet later.


Windows Server 2012 - VMware Player (Non-commercial use only)
File Virtual Machine Help
AD FS
File Action View Window Help
AD FS
Service
Endpoints
Certificates
Claim Descriptions
Trust Relationships
Certificates
Actions
Certificates
Add Token-Signing Certificat...
Add Token-Decrypting Certifi...
Set Service Communications ...
View
New Window from Here
Refresh
Help
CN=ADFS Signing - WIN-H...
View Certificate...
Set as Primary
Help
2:15 PM
6/22/2015
To grab input, press Ctrl+G

Subject	Issuer	Effective Date	Expiration Date	Status	Primary
Service communications					
CN=WIN-H18OL7086CL.m...	CN=myTestDomain-WIN-...	6/5/2015	6/4/2016		
Token-decrypting					
CN=ADFS Encryption - WI...	CN=ADFS Encryption - W...	6/5/2015	6/4/2016		Primary
Token-signing					
CN=ADFS Signing - WIN-H...	CN=ADFS Signing - WIN...	6/5/2015	6/4/2016		Primary

Export Certificate

Export your certificate to configure Pacific Timesheet. To do so, select the certificates folder and select the signing certificate. Right mouse click and select properties.



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: ADFS Signing - WIN-H18OL7086CL.myTestDomain.com

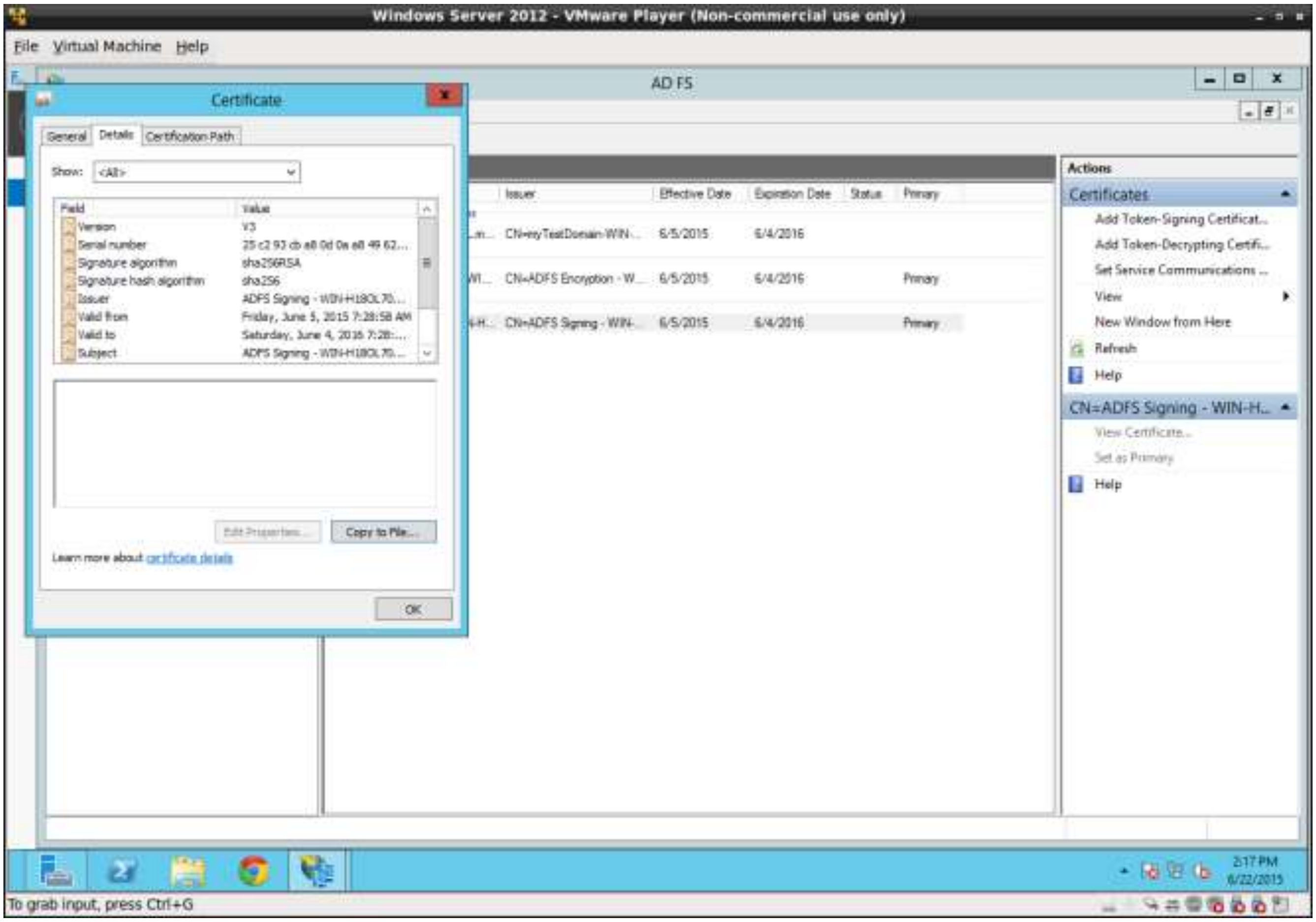
Issued by: ADFS Signing - WIN-H18OL7086CL.myTestDomain.com

Valid from 6/5/2015 to 6/4/2016

Learn more about certificates

	Issuer	Effective Date	Expiration Date	Status	Primary
...m...	CN=myTestDomain-WIN-...	6/5/2015	6/4/2016		
WI...	CN=ADFS Encryption - W...	6/5/2015	6/4/2016		Primary
-H...	CN=ADFS Signing - WIN-...	6/5/2015	6/4/2016		Primary

Certificate Dialog
The certificated dialog will display as shown above.


Windows Server 2012 - VMware Player (Non-commercial use only)
File Virtual Machine Help
AD FS
Certificate
General Details Certification Path
Edit Properties...
Copy to File...
OK
Actions
Certificates
Add Token-Signing Certificat...
Add Token-Decrypting Certifi...
Set Service Communications ...
View
New Window from Here
Refresh
Help
CN=ADFS Signing - WIN-H...
View Certificate...
Set as Primary
Help
2:17 PM
6/22/2015
To grab input, press Ctrl+G

Show: <All>

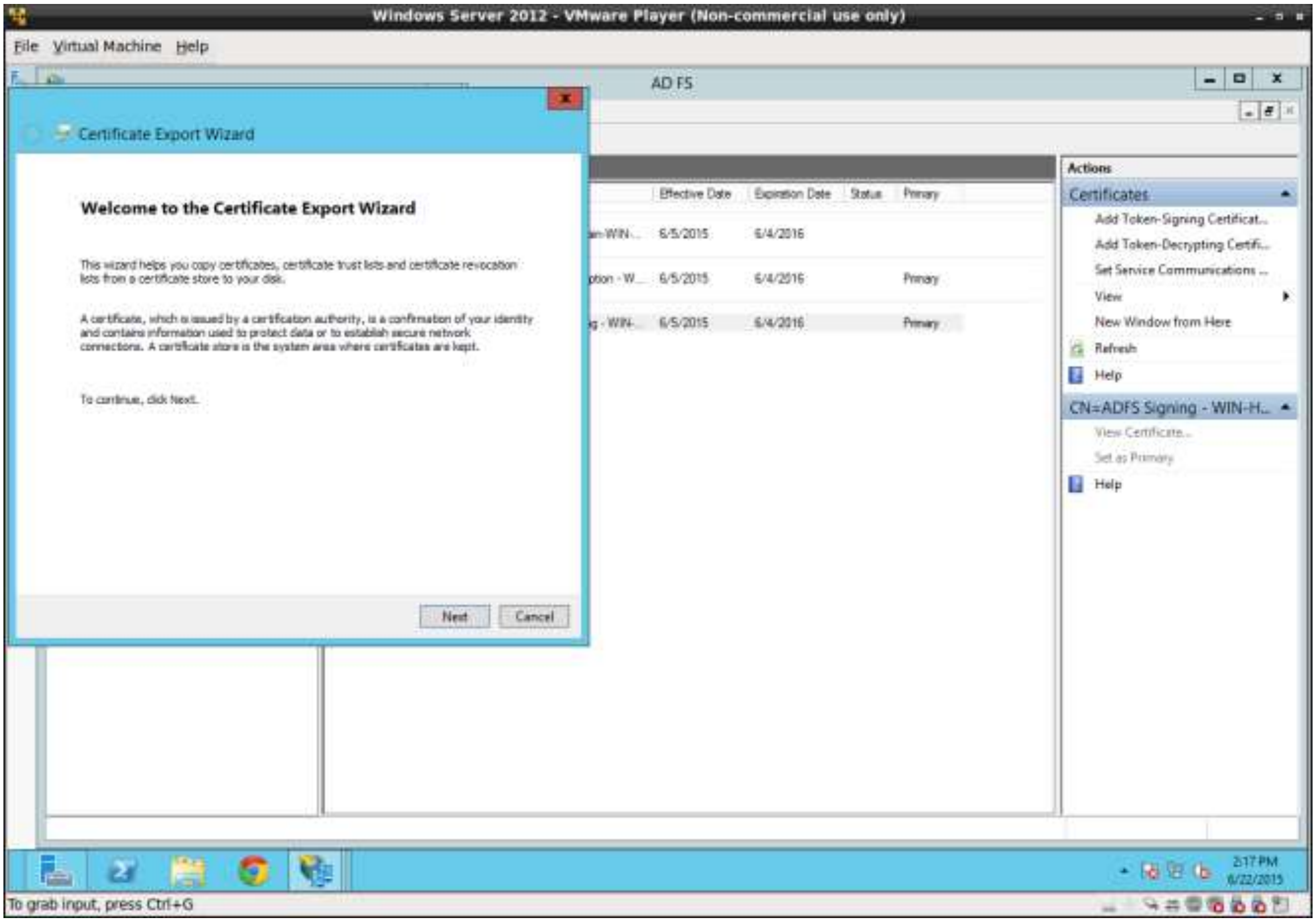
Field	Value
Version	V3
Serial number	25 c2 93 cb a8 0d 0a a8 49 62...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	ADFS Signing - WIN-H18OL70...
Valid from	Friday, June 5, 2015 7:28:58 AM
Valid to	Saturday, June 4, 2016 7:28:...
Subject	ADFS Signing - WIN-H18OL70...

Learn more about certificate details

Issuer	Effective Date	Expiration Date	Status	Primary
CN=myTestDomain-WIN-...	6/5/2015	6/4/2016		
CN=ADFS Encryption - W...	6/5/2015	6/4/2016		Primary
CN=ADFS Signing - WIN-...	6/5/2015	6/4/2016		Primary

Select the details tab

Press the “copy to file” button.


Windows Server 2012 - VMware Player (Non-commercial use only)
File Virtual Machine Help
AD FS
Certificate Export Wizard
Effective Date Expiration Date Status Primary
Actions
Certificates
Add Token-Signing Certificat...
Add Token-Decrypting Certifi...
Set Service Communications ...
View
New Window from Here
Refresh
Help
CN=ADFS Signing - WIN-H...
View Certificate...
Set as Primary
Help
Next
Cancel
2:17 PM
6/22/2015
To grab input, press Ctrl+G

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.

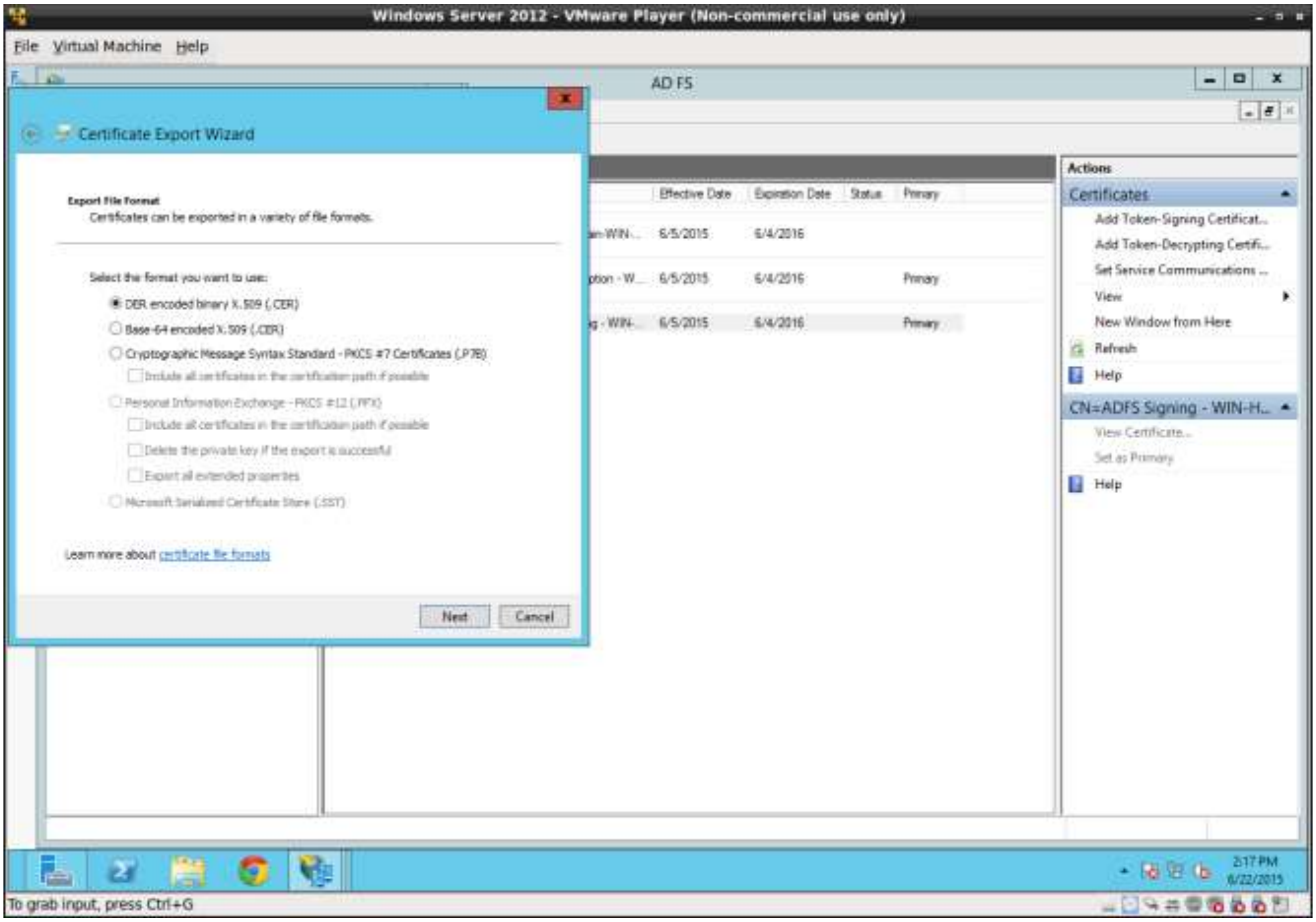
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

	Effective Date	Expiration Date	Status	Primary
...an-WIN-...	6/5/2015	6/4/2016		
...ption - W...	6/5/2015	6/4/2016		Primary
...g - WIN-...	6/5/2015	6/4/2016		Primary

Export Wizard

An export wizard will appear to guide you through the export steps. Press next to continue.


Windows Server 2012 - VMware Player (Non-commercial use only)
File
Virtual Machine
Help
AD FS
Actions
Certificates
Add Token-Signing Certificat...
Add Token-Decrypting Certifi...
Set Service Communications ...
View
New Window from Here
Refresh
Help
CN=ADFS Signing - WIN-H...
View Certificate...
Set as Primary
Help
Next
Cancel
2:17 PM
6/22/2015
To grab input, press Ctrl+G

	Effective Date	Expiration Date	Status	Primary
n-WIN-...	6/5/2015	6/4/2016		
ption - W...	6/5/2015	6/4/2016		Primary
g - WIN-...	6/5/2015	6/4/2016		Primary

Certificate Export Wizard

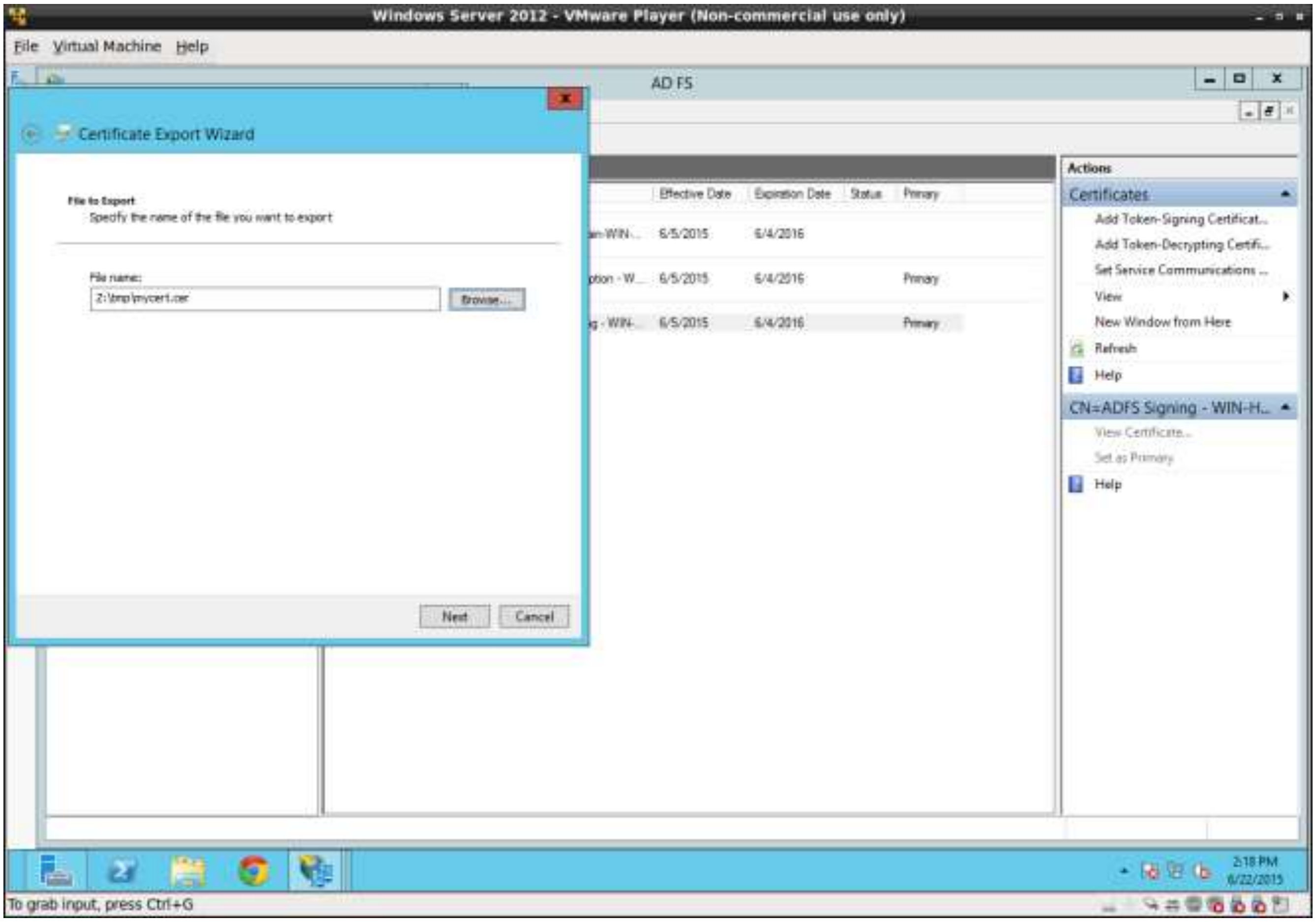
Export File Format
Certificates can be exported in a variety of file formats.

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)

Learn more about certificate file formats

Select DER Format
Select the DER format and press next.



Windows Server 2012 - VMware Player (Non-commercial use only)
File Virtual Machine Help
AD FS
Certificate Export Wizard
Next
Cancel
Actions
Certificates
Add Token-Signing Certificat...
Add Token-Decrypting Certifi...
Set Service Communications ...
View
New Window from Here
Refresh
Help
CN=ADFS Signing - WIN-H...
View Certificate...
Set as Primary
Help
2:18 PM
6/22/2015
To grab input, press Ctrl+G

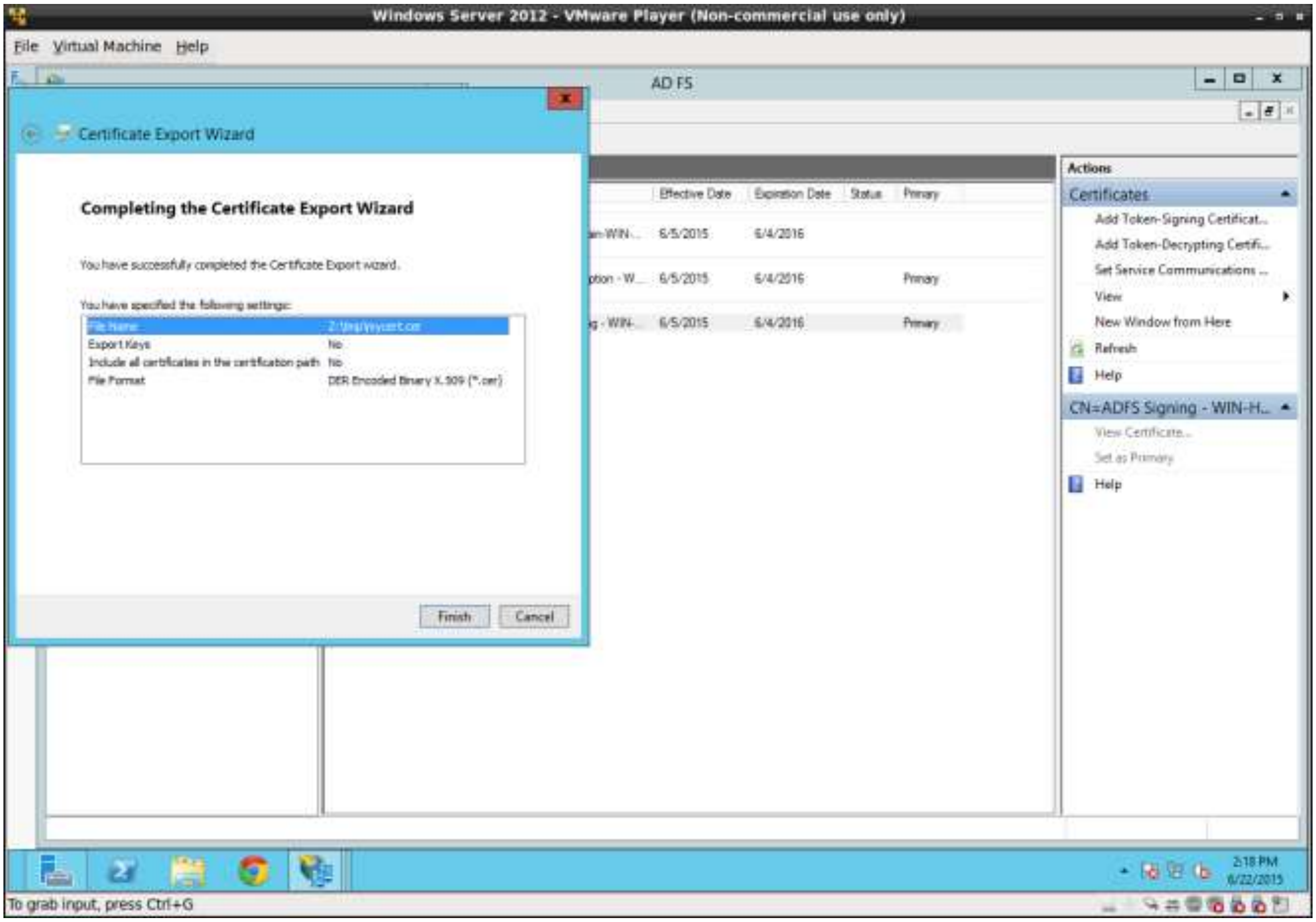
File to Export
Specify the name of the file you want to export

File name: Z:\tmp\mycert.cer

Browse...

	Effective Date	Expiration Date	Status	Primary
...n-WIN-...	6/5/2015	6/4/2016		
...ption - W...	6/5/2015	6/4/2016		Primary
...g - WIN-...	6/5/2015	6/4/2016		Primary

Set File Name
Provide a file name and press next.


Windows Server 2012 - VMware Player (Non-commercial use only)
File
Virtual Machine
Help
AD FS
Certificate Export Wizard
Effective Date
Expiration Date
Status
Primary
Actions
Certificates
Add Token-Signing Certificat...
Add Token-Decrypting Certifi...
Set Service Communications ...
View
New Window from Here
Refresh
Help
CN=ADFS Signing - WIN-H...
View Certificate...
Set as Primary
Help
Finish
Cancel
2:18 PM
6/22/2015
To grab input, press Ctrl+G

...an-WIN-...	6/5/2015	6/4/2016	
...ption - W...	6/5/2015	6/4/2016	Primary
...g - WIN-...	6/5/2015	6/4/2016	Primary

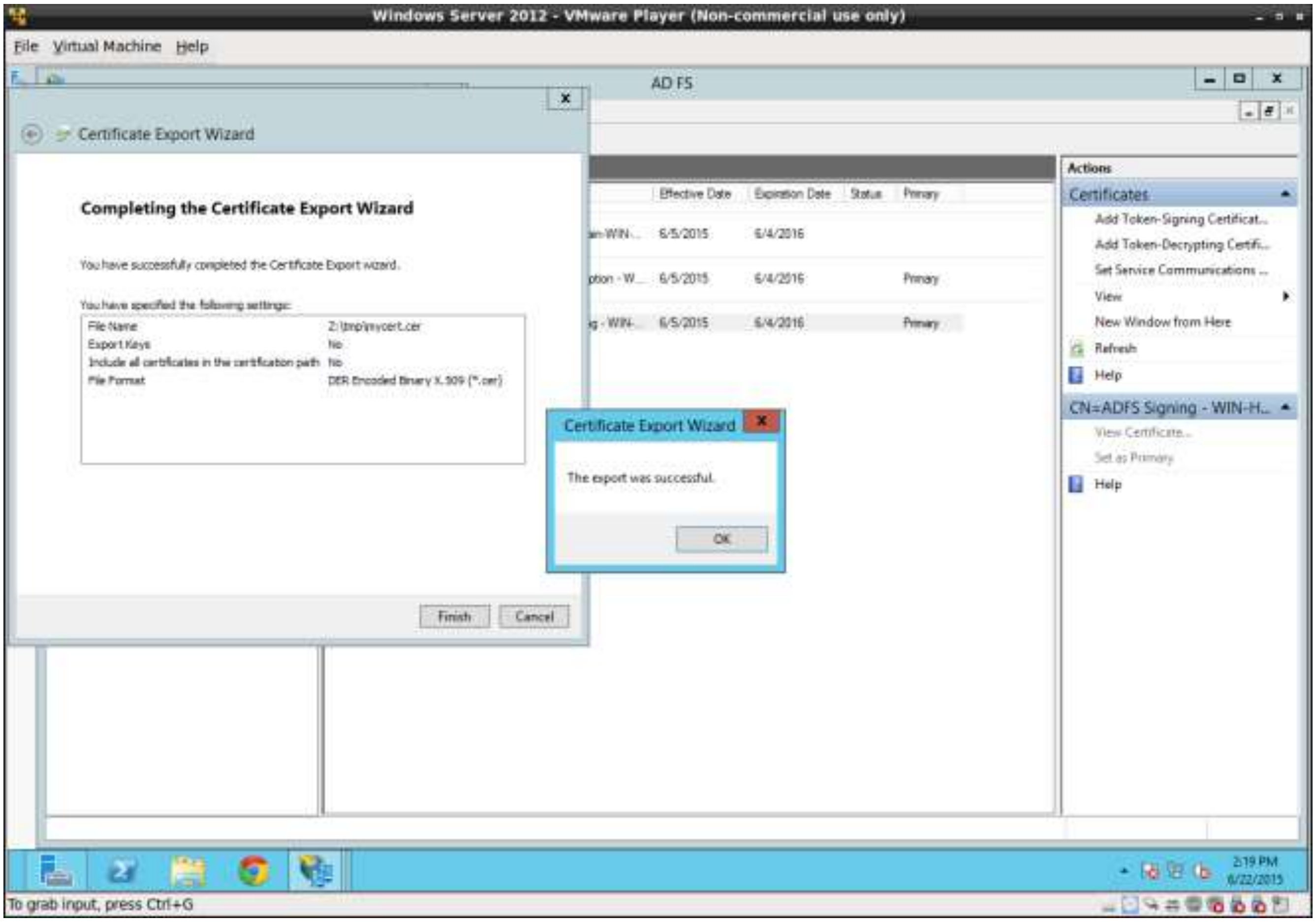
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

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

Finish
Press the finish button.


Windows Server 2012 - VMware Player (Non-commercial use only)
File
Virtual Machine
Help
AD FS
Certificate Export Wizard
Actions
Certificates
Add Token-Signing Certificat...
Add Token-Decrypting Certifi...
Set Service Communications ...
View
New Window from Here
Refresh
Help
CN=ADFS Signing - WIN-H...
View Certificate...
Set as Primary
Help
Finish
Cancel
OK
2:19 PM
6/22/2015
To grab input, press Ctrl+G

	Effective Date	Expiration Date	Status	Primary
...n-WIN-...	6/5/2015	6/4/2016		
...ption - W...	6/5/2015	6/4/2016		Primary
...g - WIN-...	6/5/2015	6/4/2016		Primary

Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

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

Certificate Export Wizard

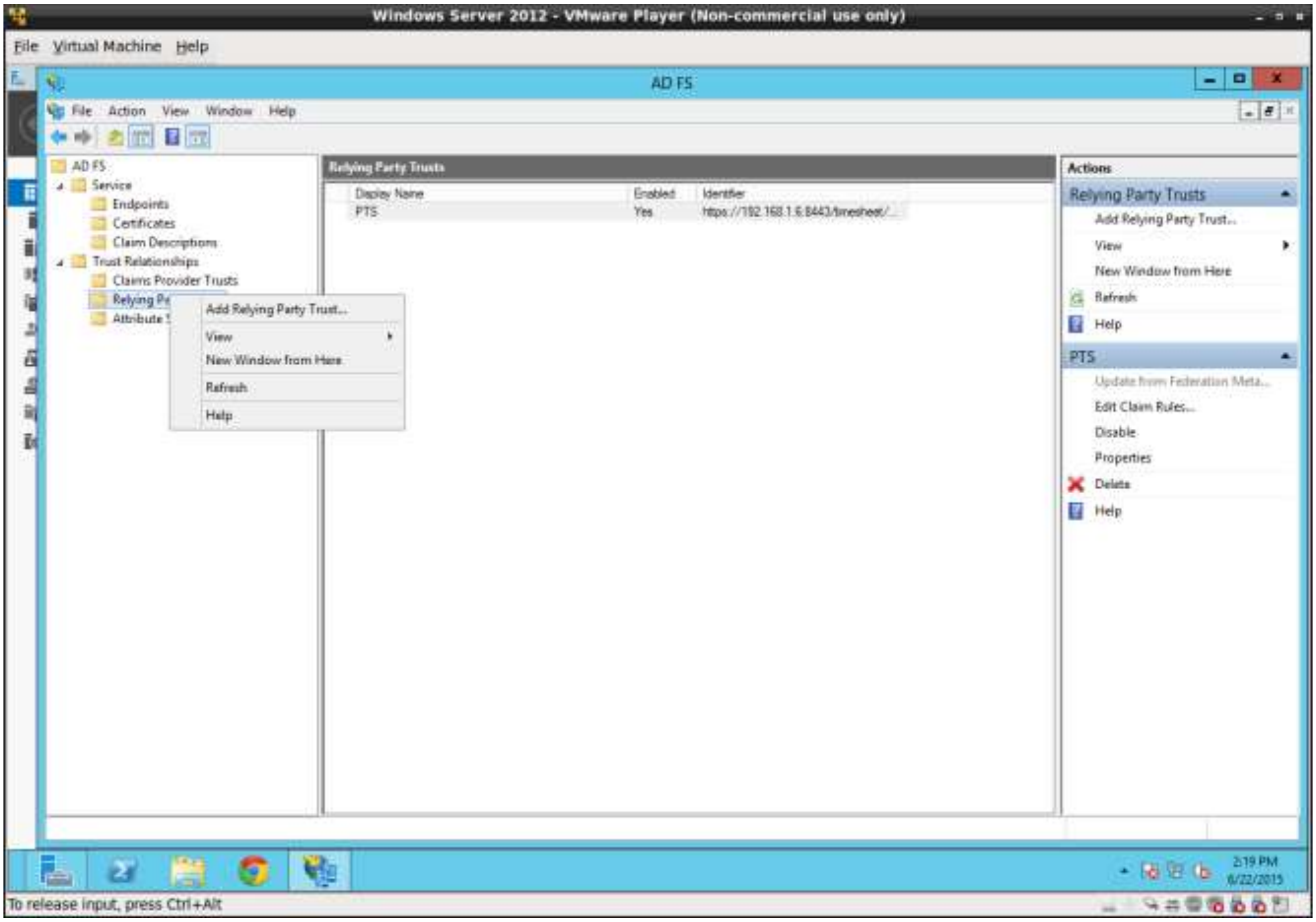
The export was successful.

Success

The dialog “The export was successful” means you have successfully exported your certificate.

Convert Certificate to PEM Format

Your next step will be to convert the certificate into the PEM format by using an online conversion tool. Here is a one example available from SSL Shopper https://www.sslshopper.com/ssl-converter.html .



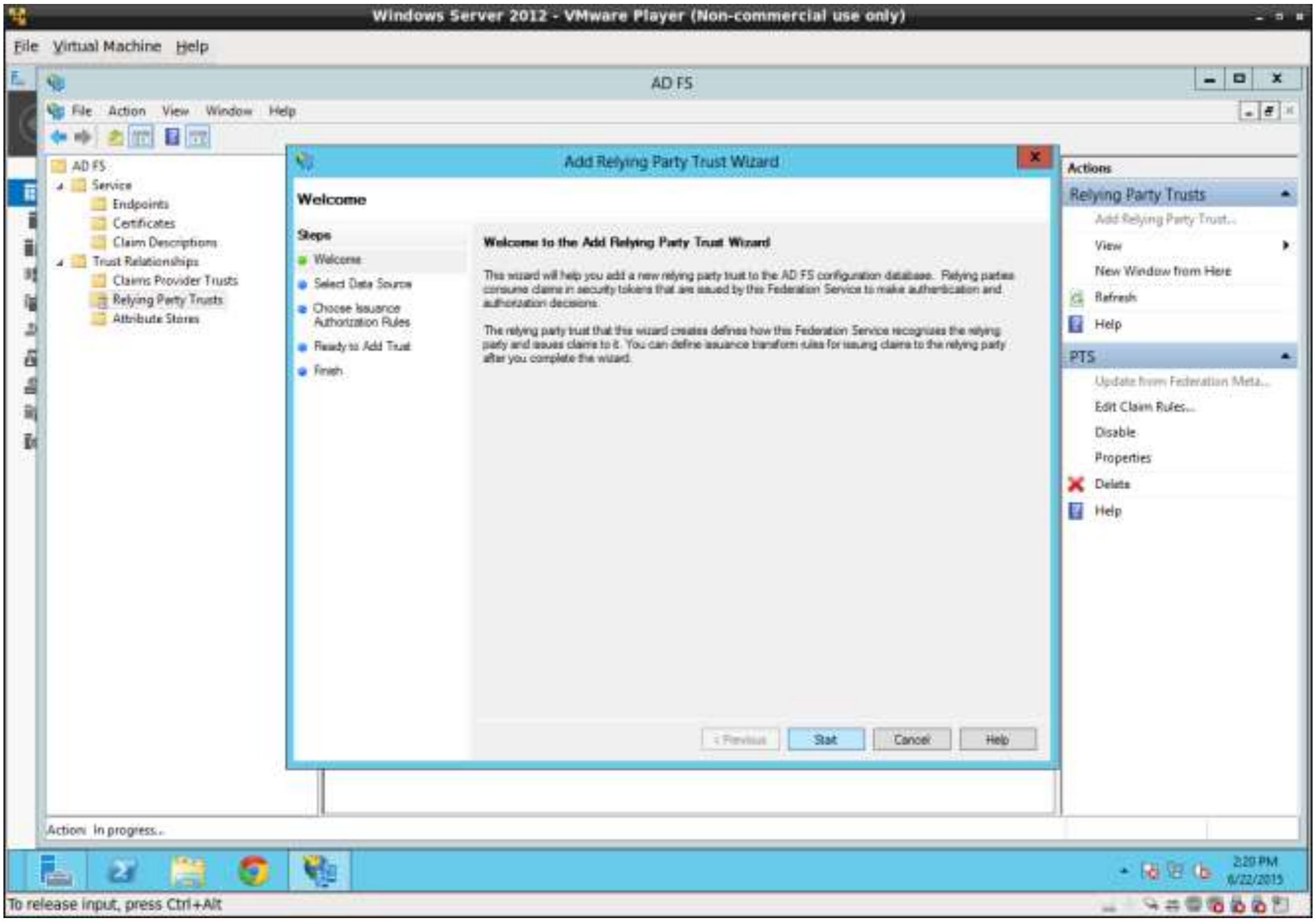
Display Name	Enabled	Identifier
PTS	Yes	https://192.168.1.6:8443/timesheet/...

Create Relying Party

Once the conversion to the PEM format is done, the next step is to create the Relying Party in AD FS.

Add Relying Party

From the AD FS management tool right mouse click on the “Relying Parties” folder and select “Add a relying party”.

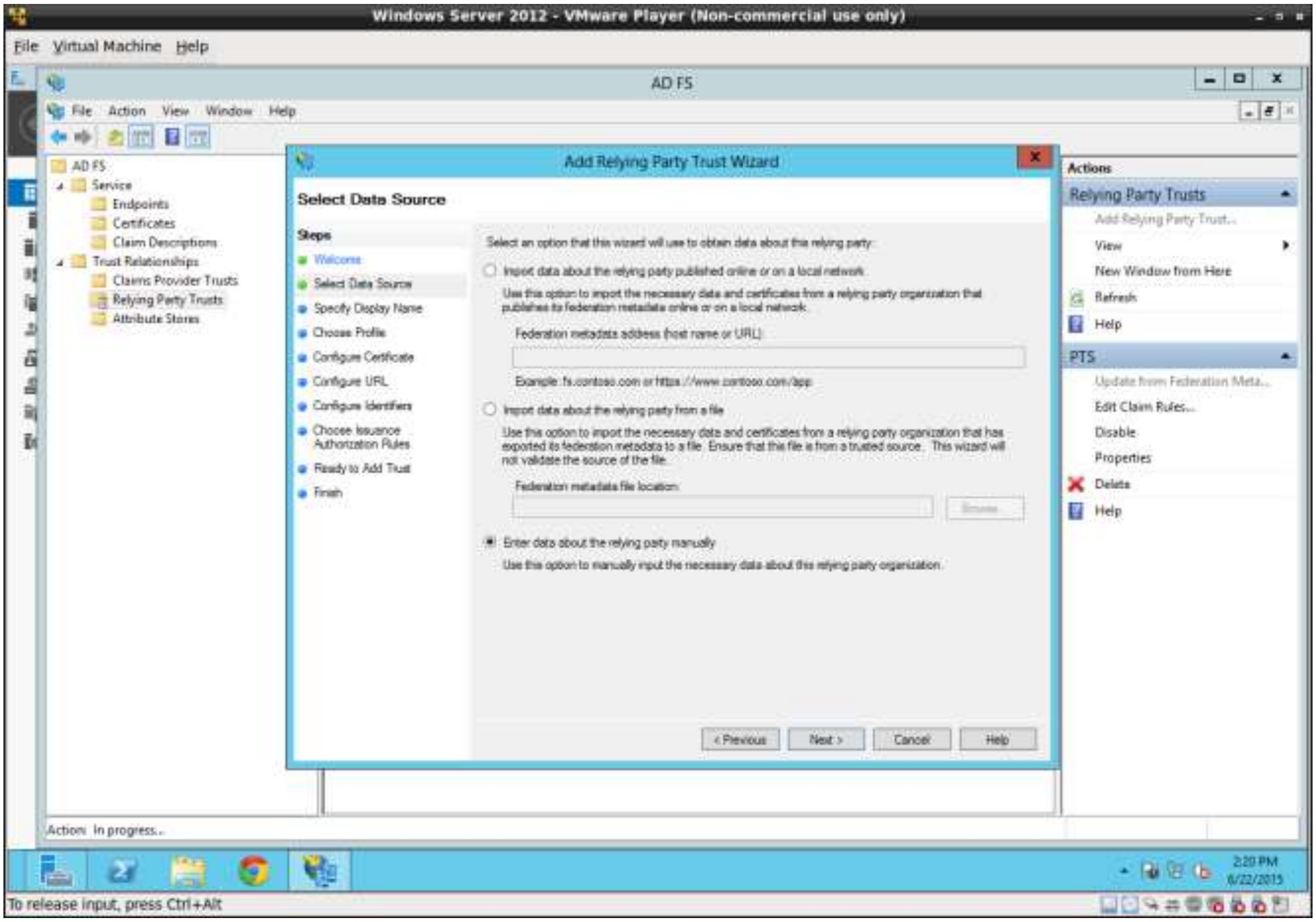


Welcome to the Add Relying Party Trust Wizard

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
The Add Relying Party Trust Wizard will display. Press next.



Add Relying Party Trust Wizard

Select Data Source

Steps
- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- 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:

Browse...

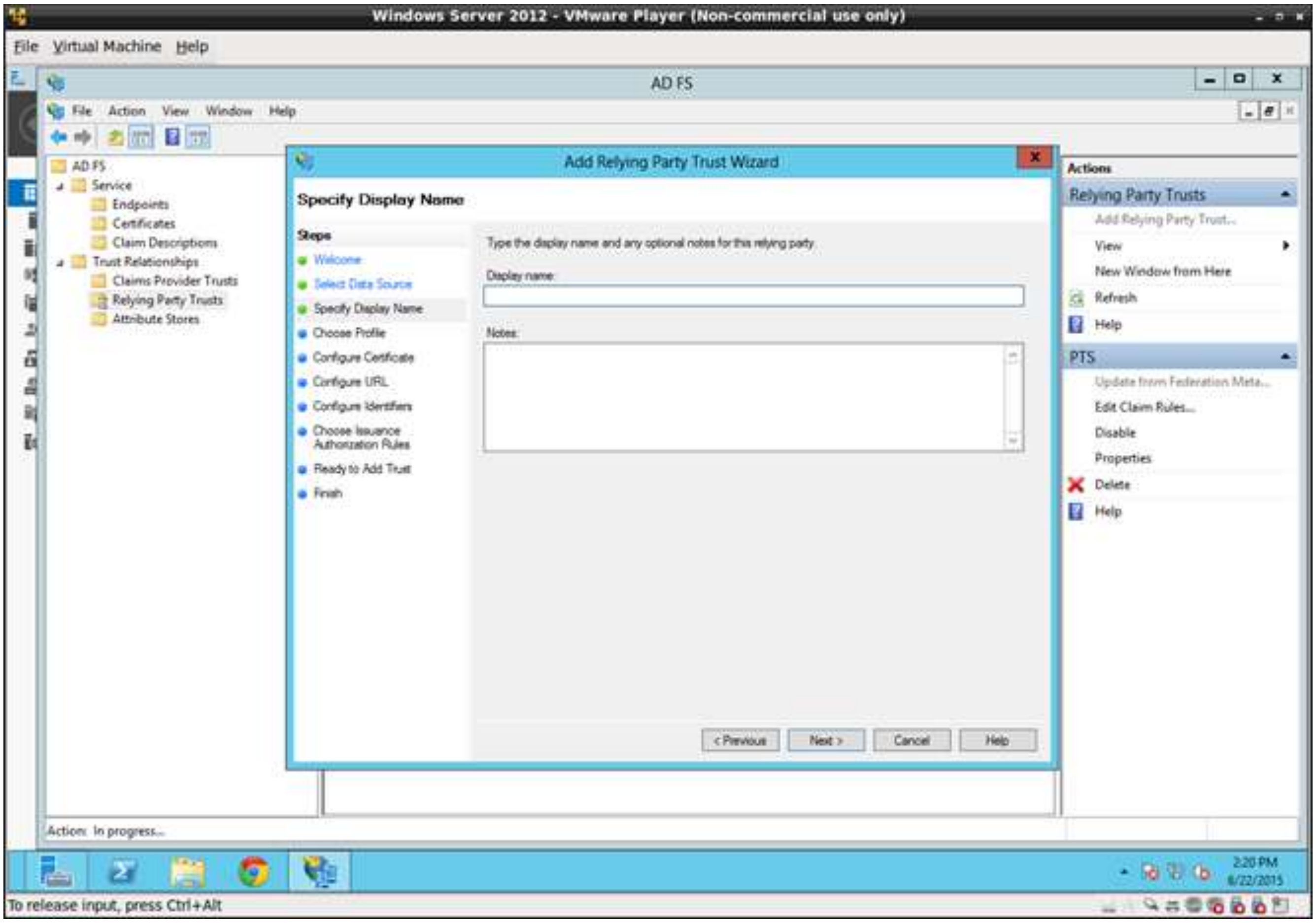
● Enter data about the relying party manually

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

< Previous | Next > | Cancel | Help

Select Enter Manually

Select the “Enter manually” radio button and press next.



Specify Display Name

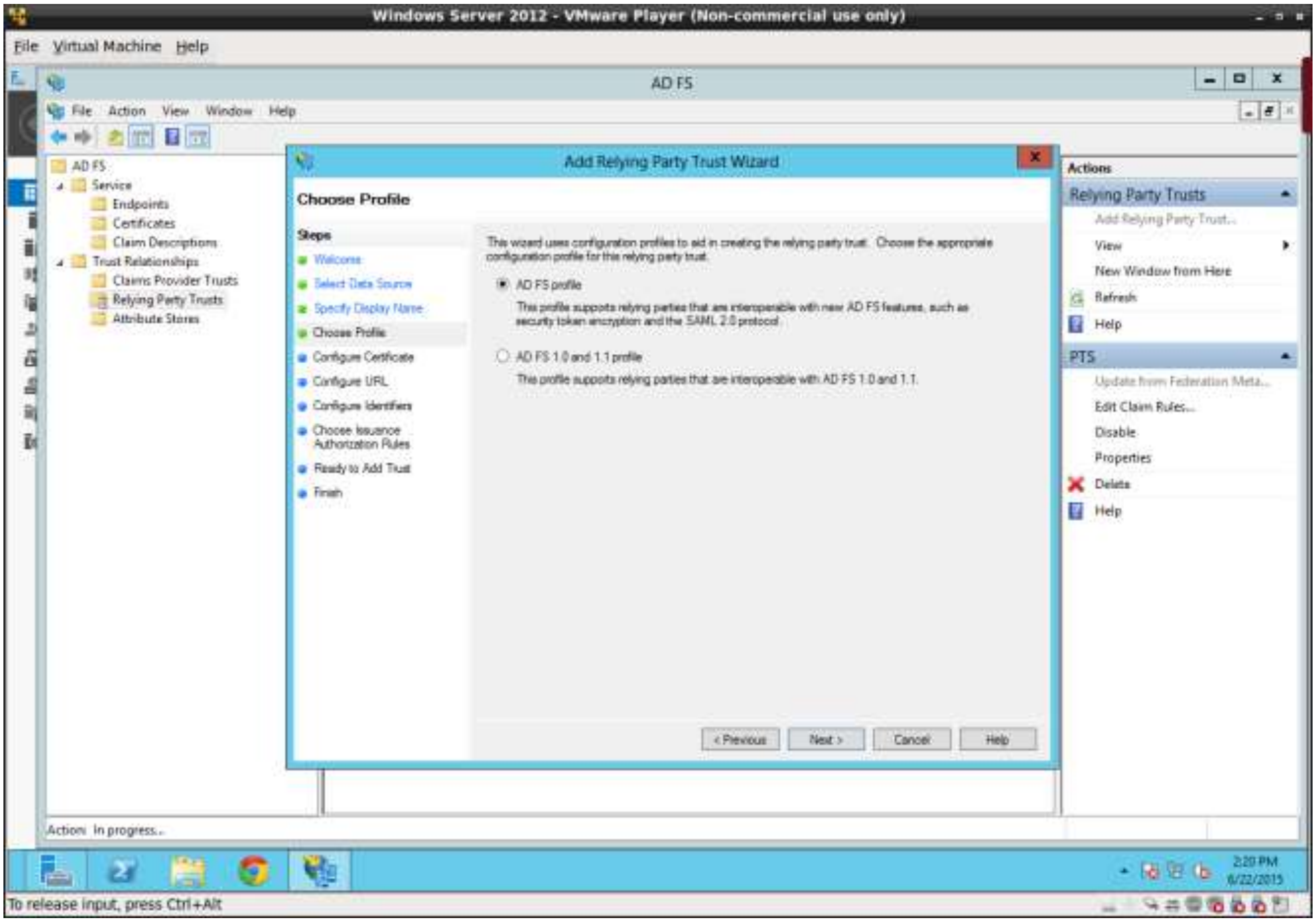
Type the display name and any optional notes for this relying party.

Display name:

Notes:

Set Pacific Timesheet Name

Enter Pacific Timesheet as the name of the relying party and press 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

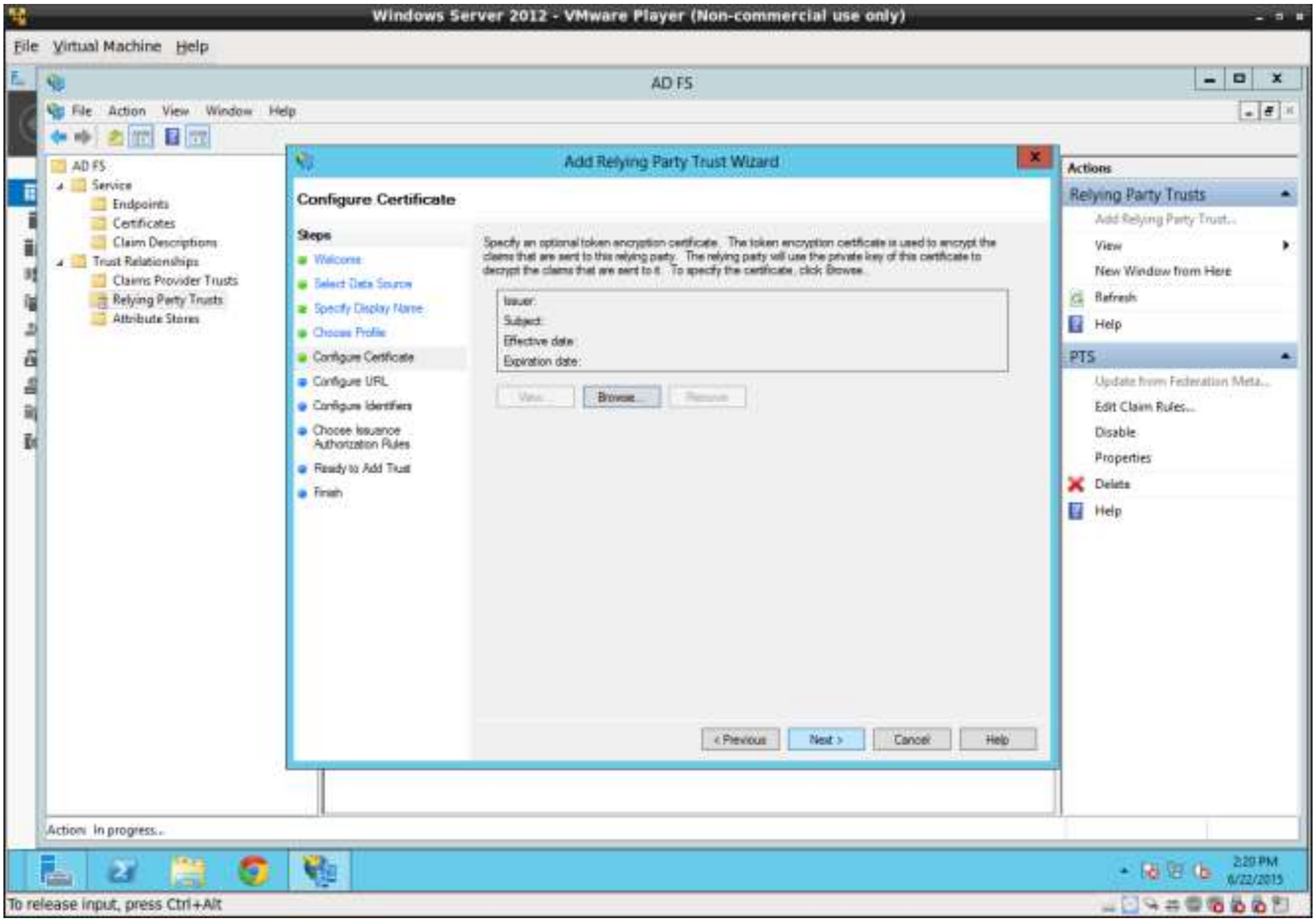
This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol.

○ AD FS 1.0 and 1.1 profile

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

Select AD FS Profile

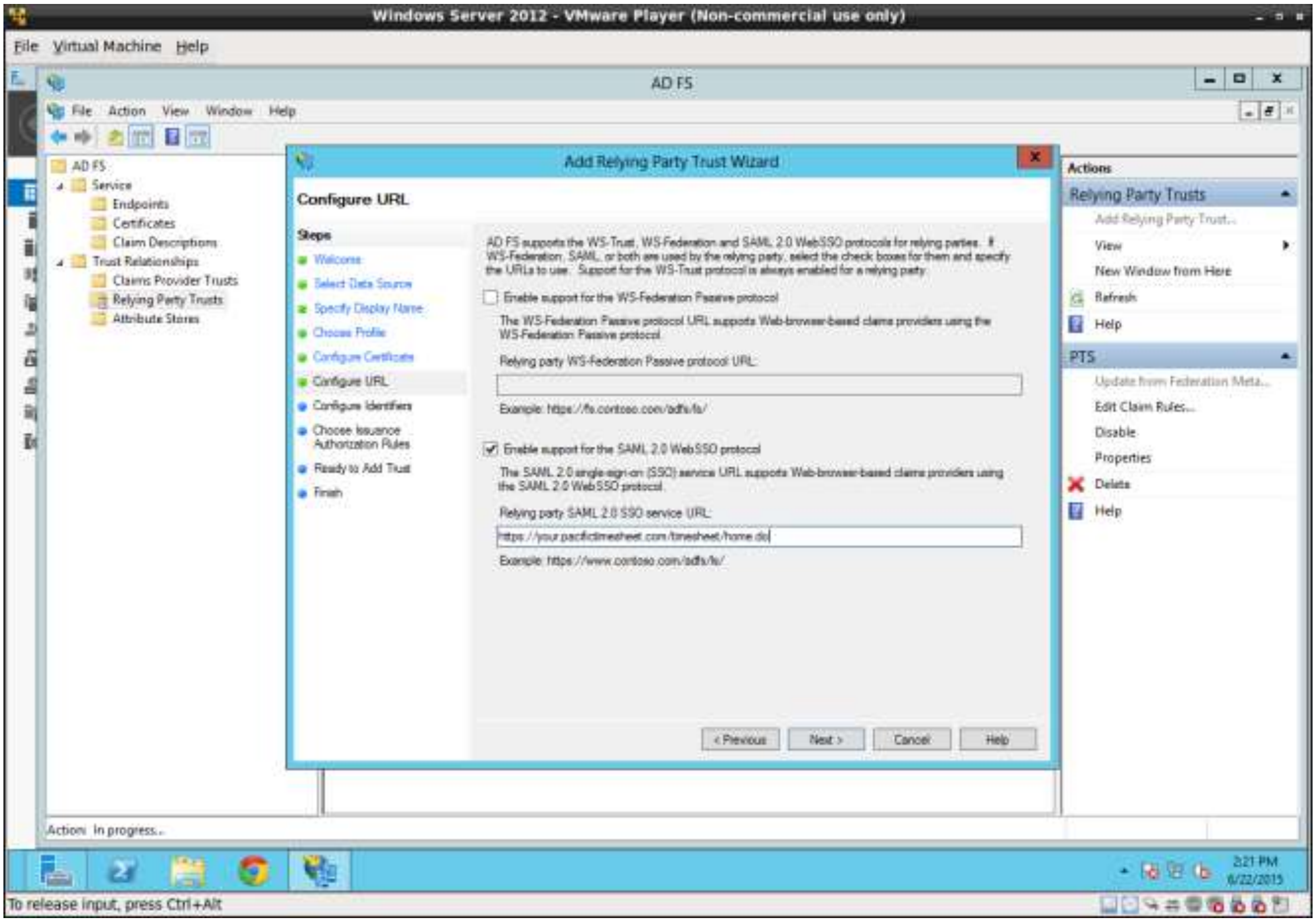
Select AD FS profile and press next.



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:

Press next.



Add Relying Party Trust Wizard

Configure URL

Steps
- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

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://your.pacifictimesheet.com/timesheet/home.do

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

< Previous | Next > | Cancel | Help

Enable SAML 2.0 Support

Select “Enable support for the SAML 2.0 WebSSO protocol”. Enter the service name for your Pacific Timesheet service end point and press next. In your case, you should enter the full end point URL assigned by Pacific Timesheet.

Cloud Service end point URL format

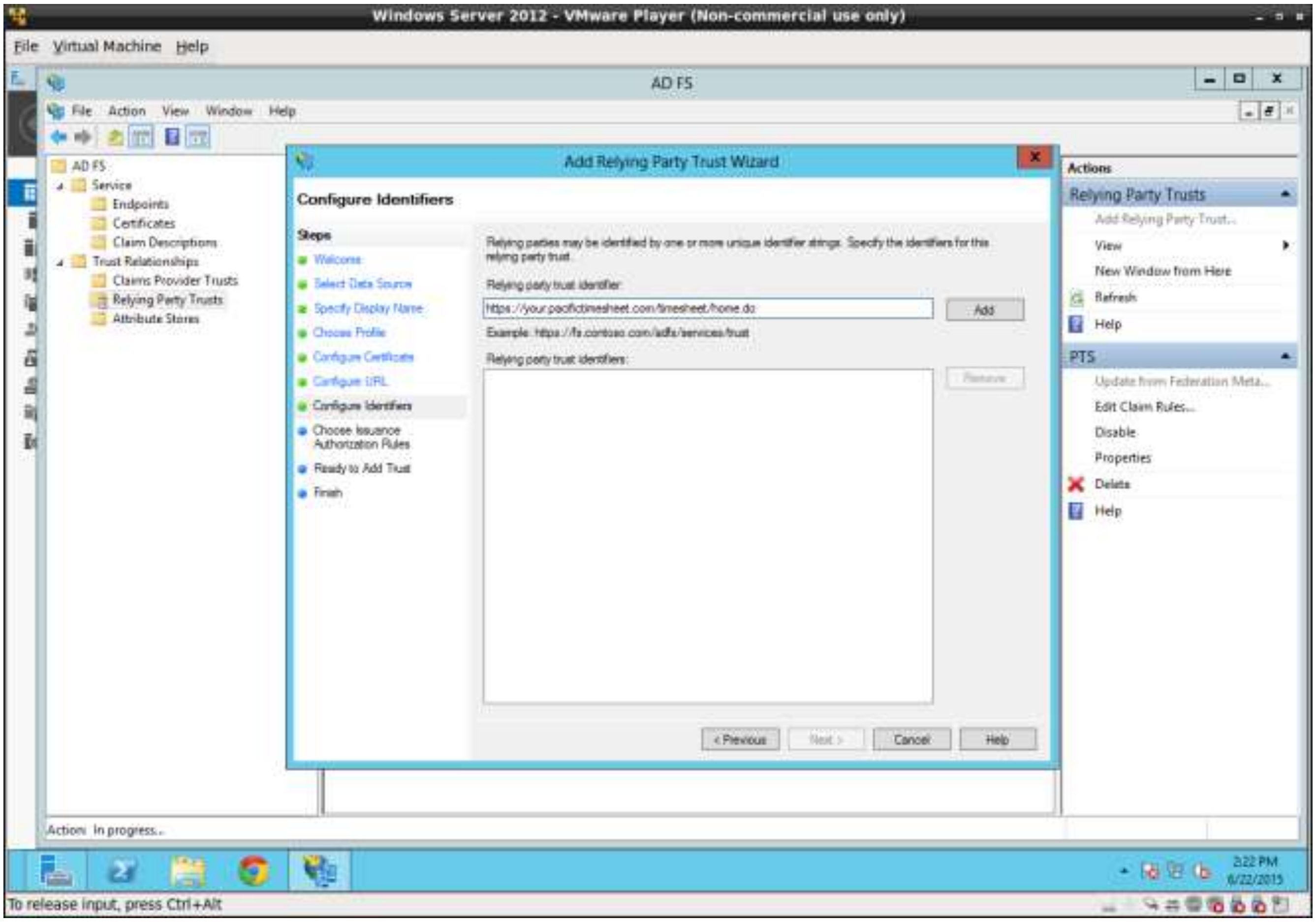
When using the Pacific Timesheet Cloud Service, this URL should have the format:

https://(subdomain).pacifictimesheet.com/timesheet/home.do

Where the subdomain is the full or shortened name of your company assigned by Pacific Timesheet.

On-Premise end point URL format

This URL format is setup by your IT department which is hosting the Pacific Timesheet on-premise application. However, it should always end with: “/timesheet/home.do”



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:

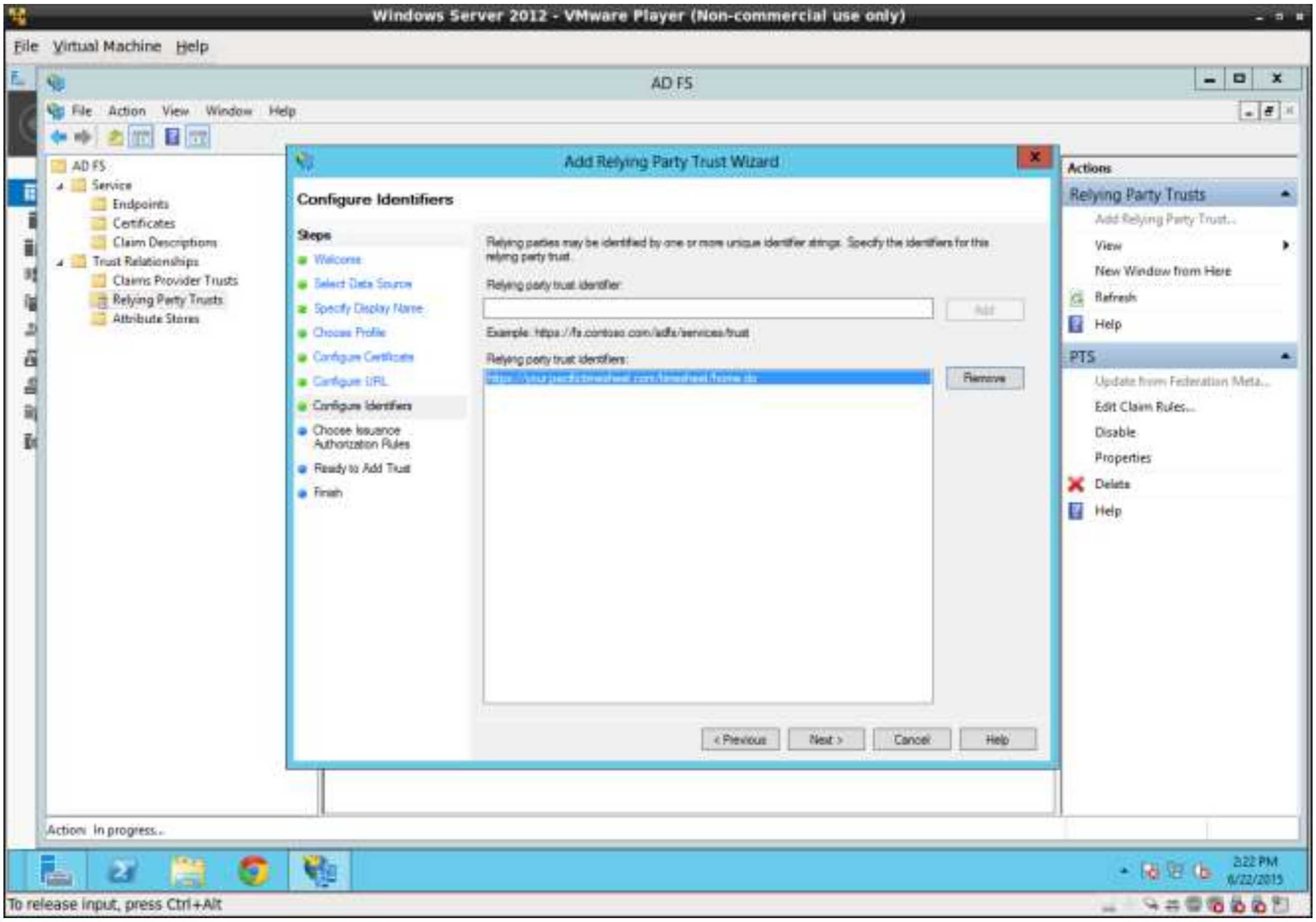
https://your.pacifictimesheet.com/timesheet/home.do

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

Relying party trust identifiers:

Enter Pacific Timesheet Service End Point

Enter the URL for the service (the Pacific Timesheet Service End Point) again and press the add button.



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

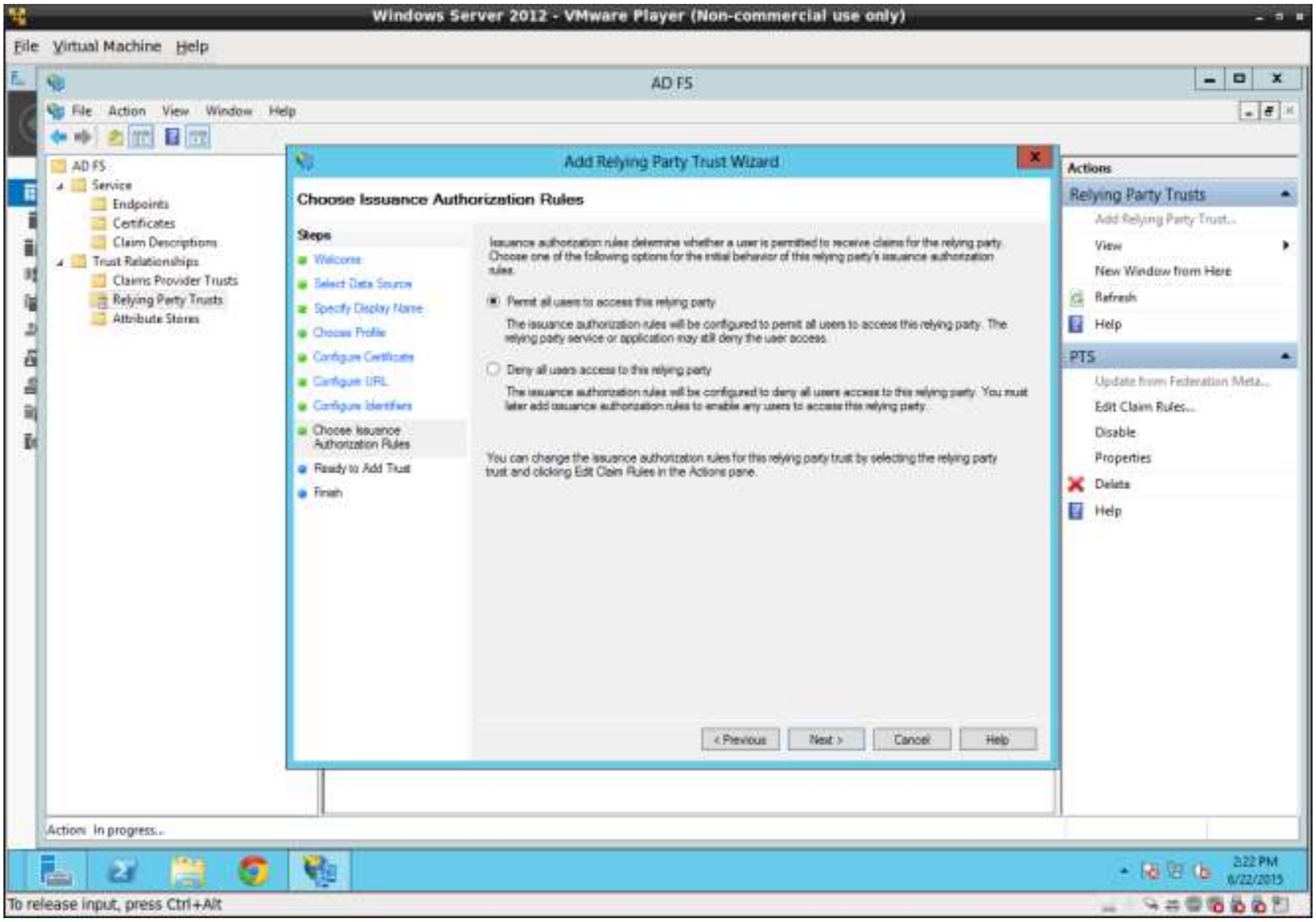
Relying party trust identifiers:

https://yourpacifictimesheet.com/timesheet/home.do

Action: In progress...

Next

Press the next button.



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.

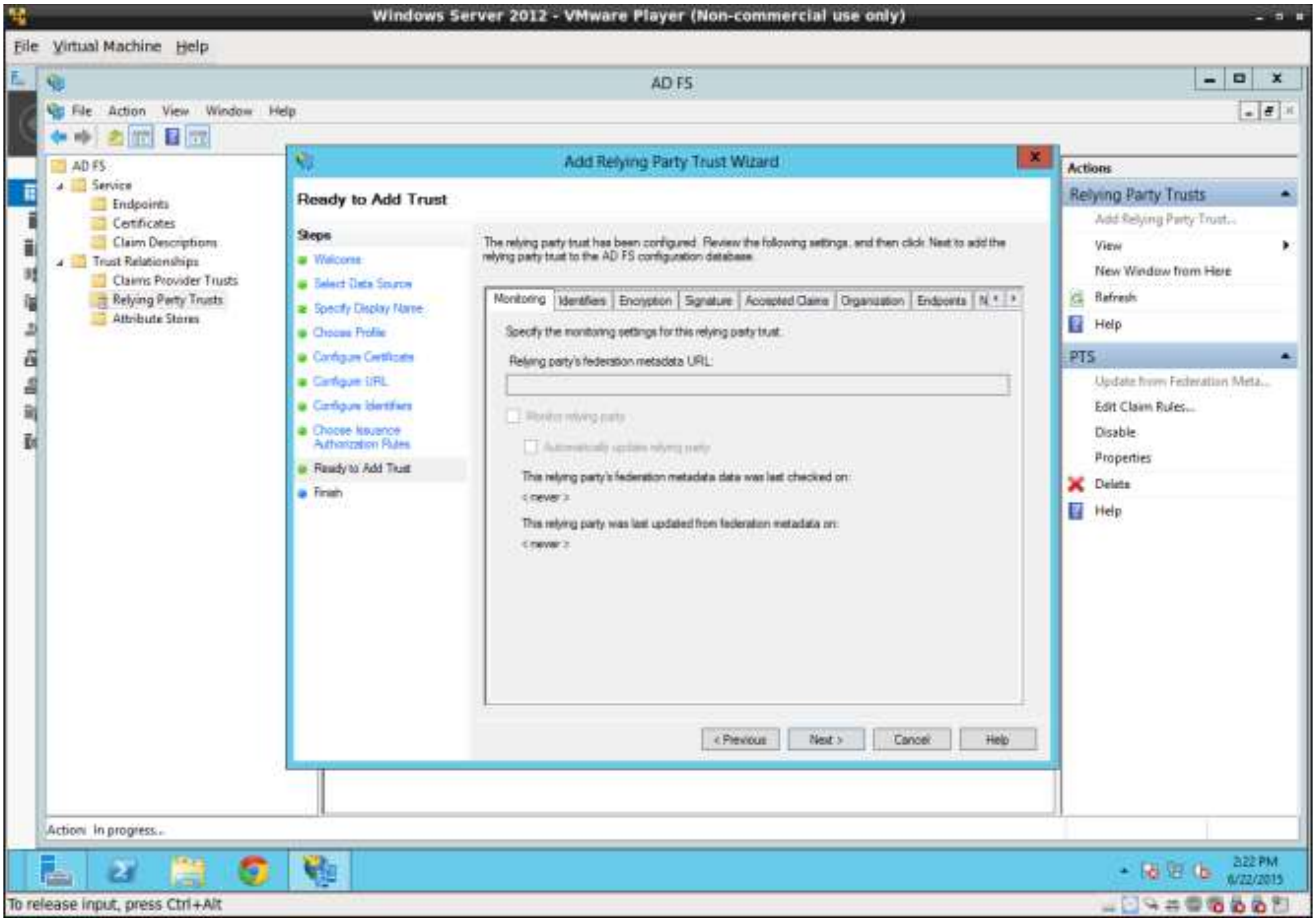
○ Deny all users access to this relying party

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.

Set Permissions

Set the permissions and press next. This should be set to “Permit all users to access the relying party.”



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

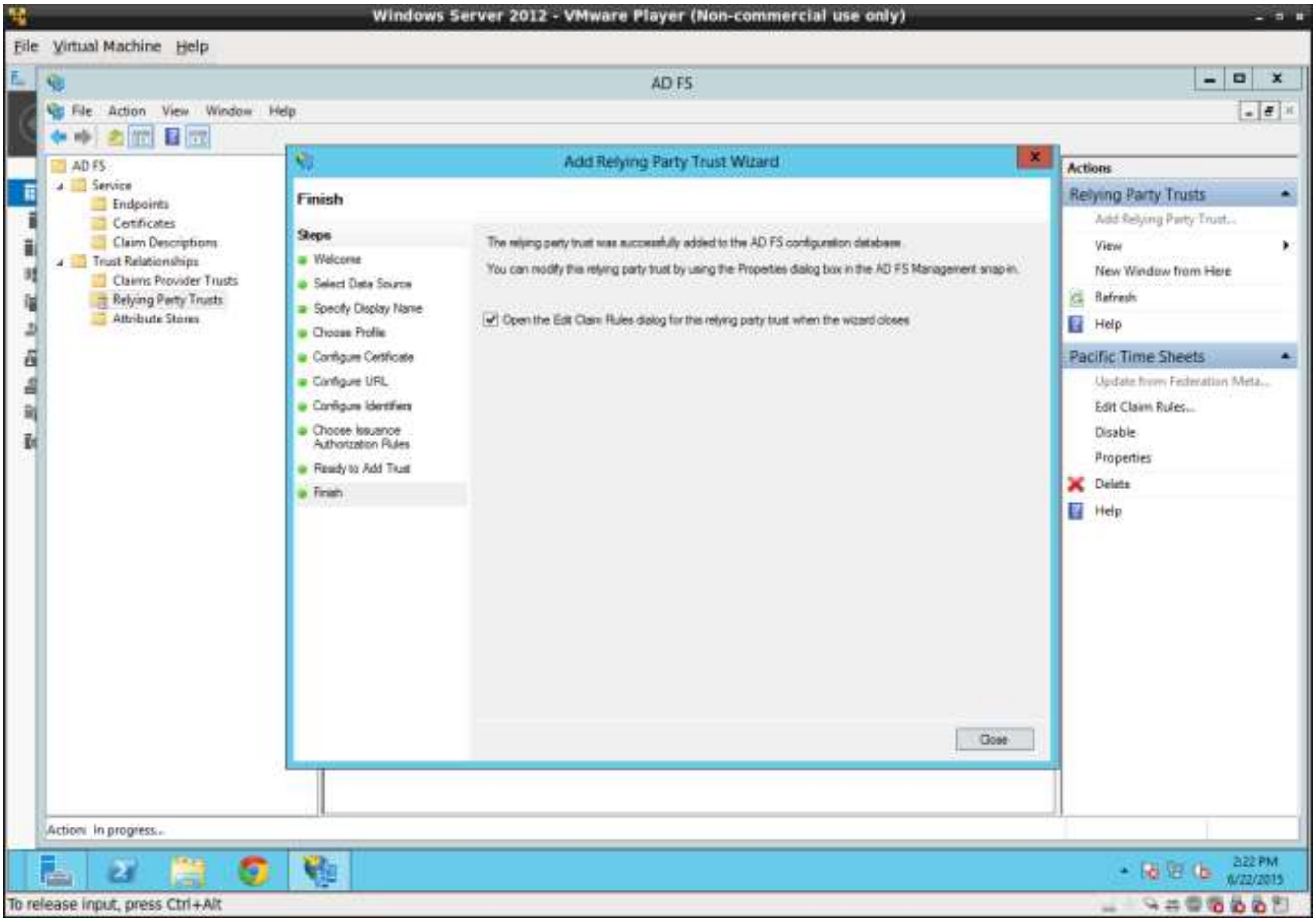
☐ Automatically update relying party

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

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

Review Settings and Press Next

Review the settings you have so far and press next.



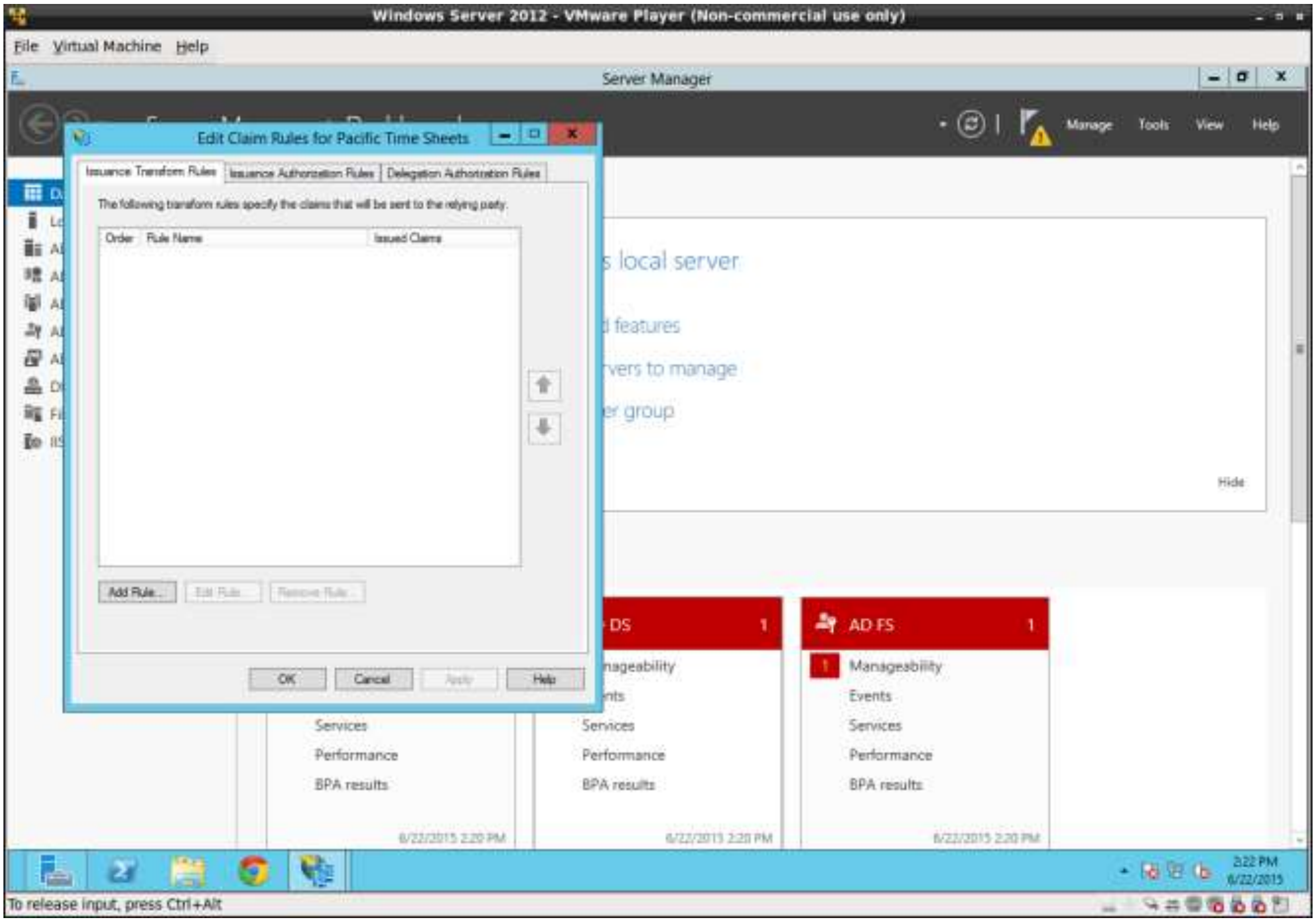
The relying party trust was successfully added to the AD FS configuration database.

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

Close to Reach Edit Claims Rules Dialog

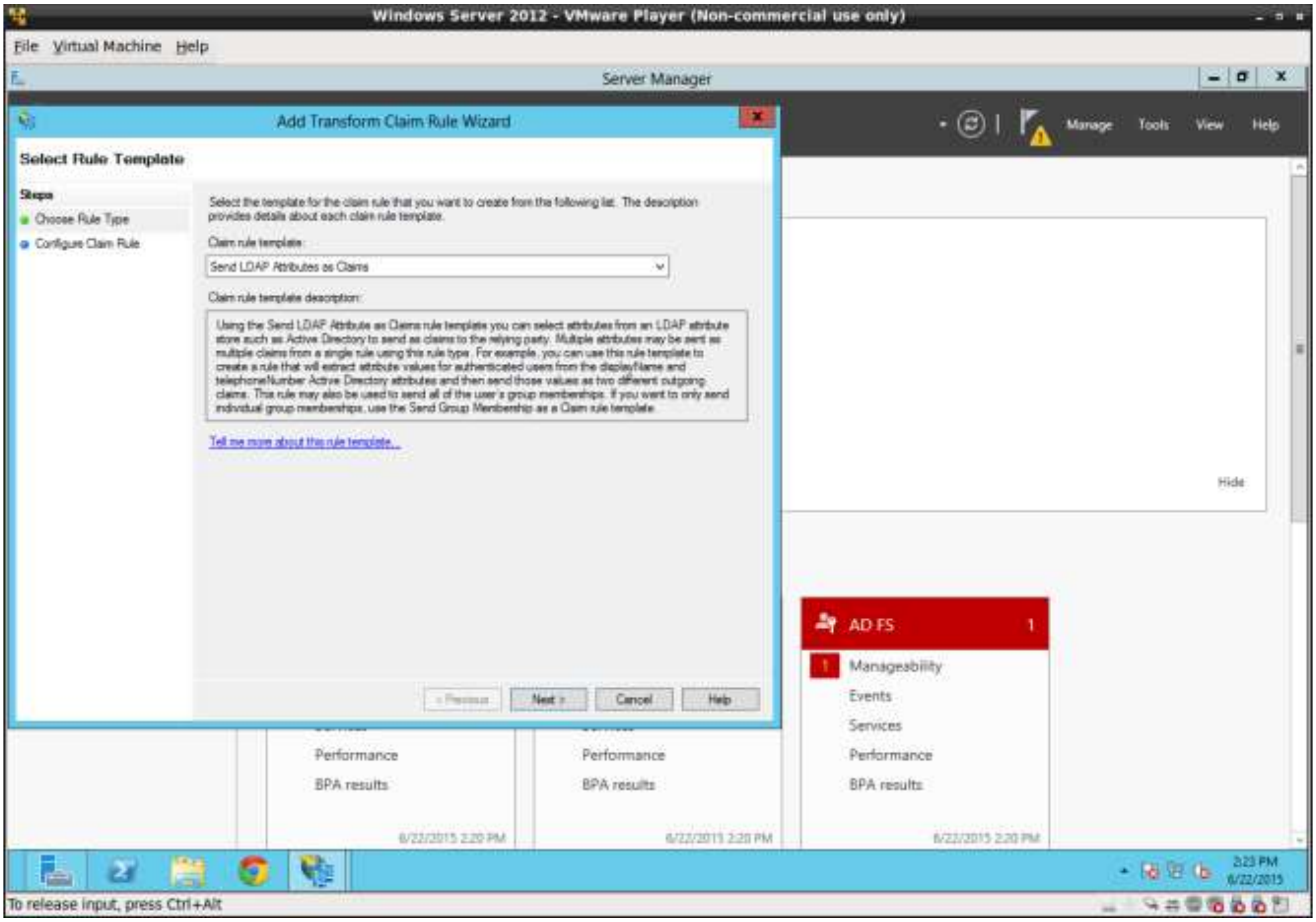
Press close. The edit claims rules dialog will then display.



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

Add Rule

Press “Add Rule” to start claims wizard.



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.

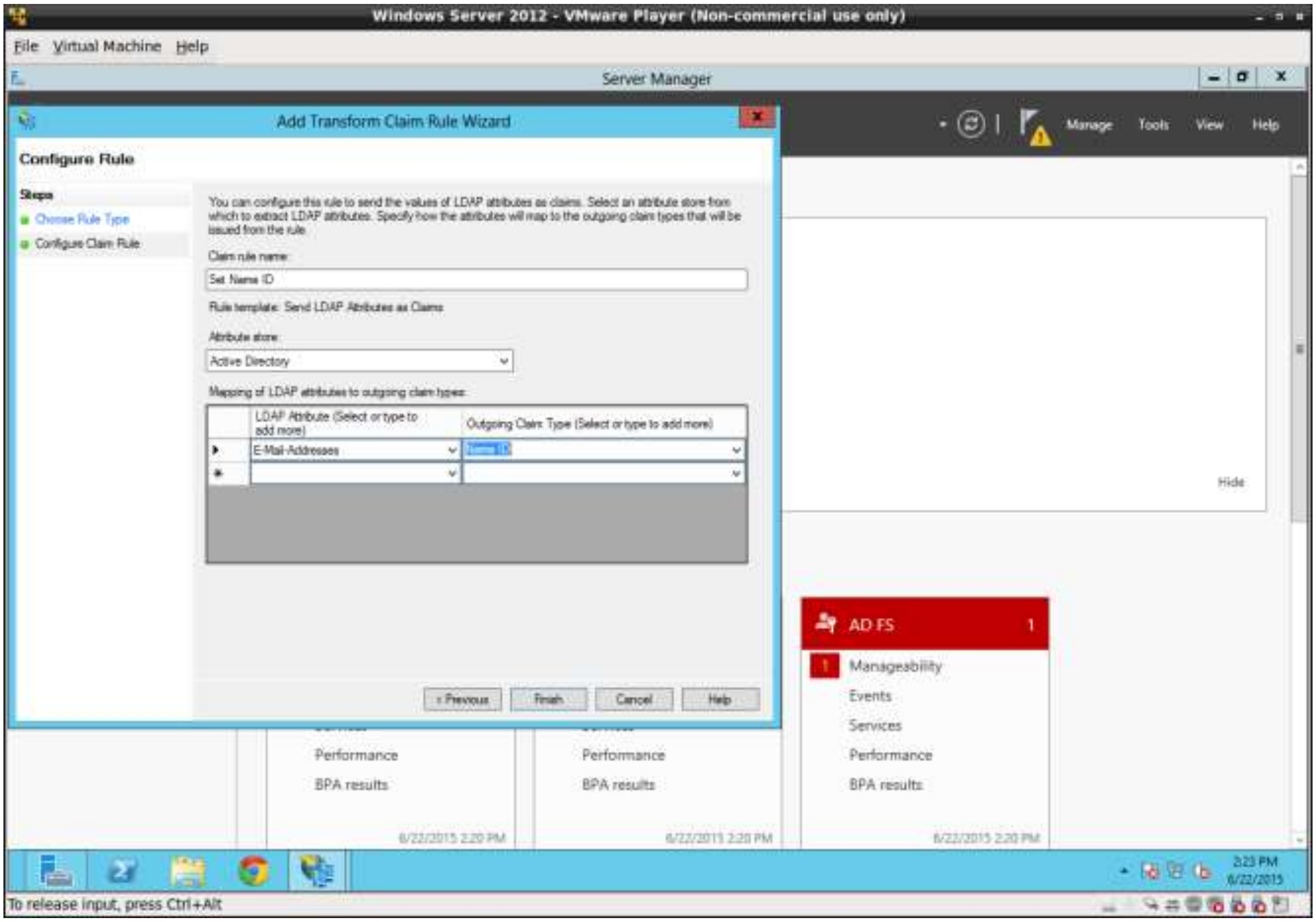
Claim rule template: Send LDAP Attributes as Claims

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.

Next

This is will set the system to the claim rule template “Send LDAP Attributes as Claims.” Then press next.



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: Set Name ID

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

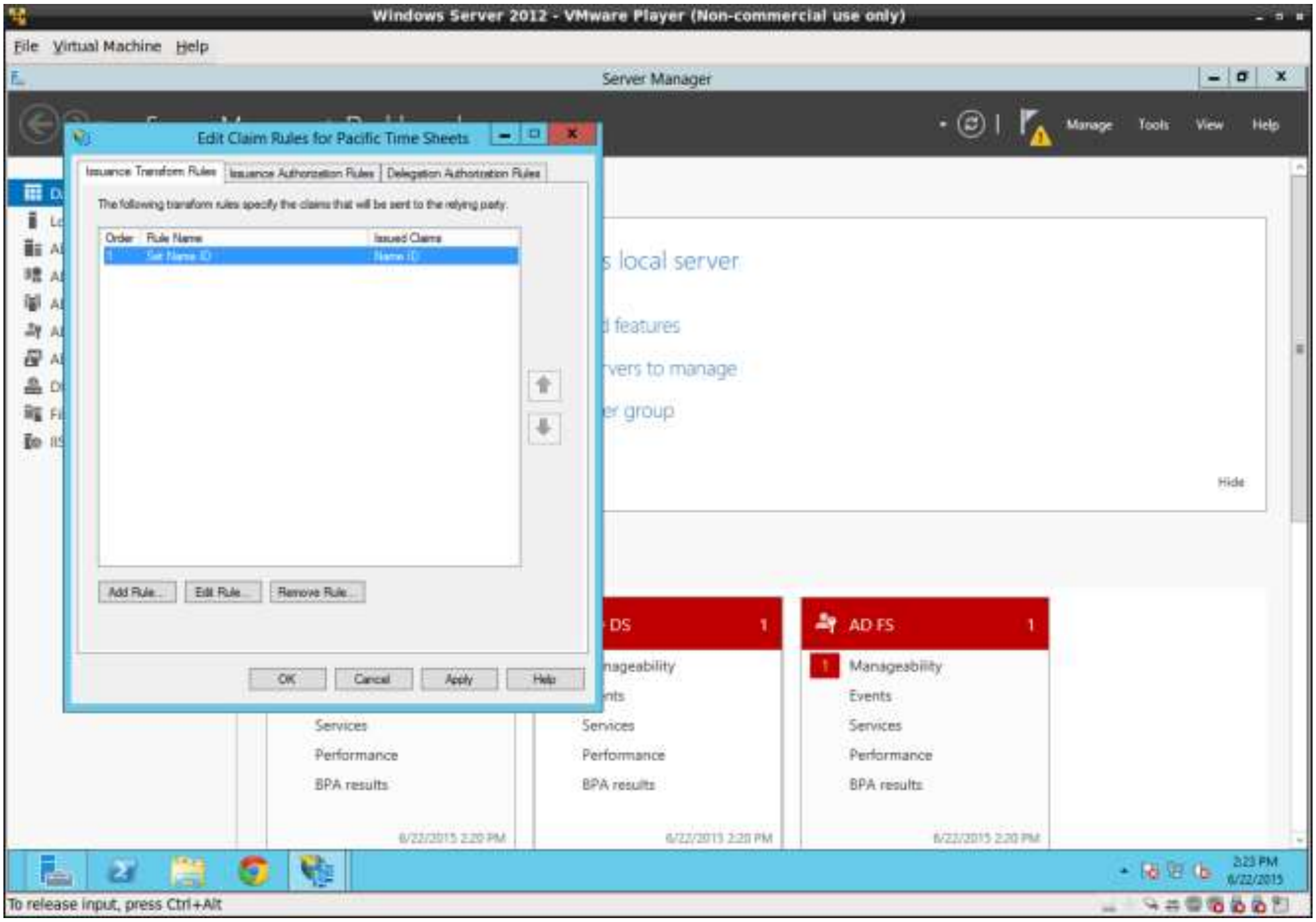
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	E-Mail-Addresses	Name ID
*		

Enter Claim Rule Name

Enter in claim rule name.

Set LDAP Attribute

Set LDAP attribute to E-Mail-Address and Outgoing Claim Type to “Name ID” and press finish.

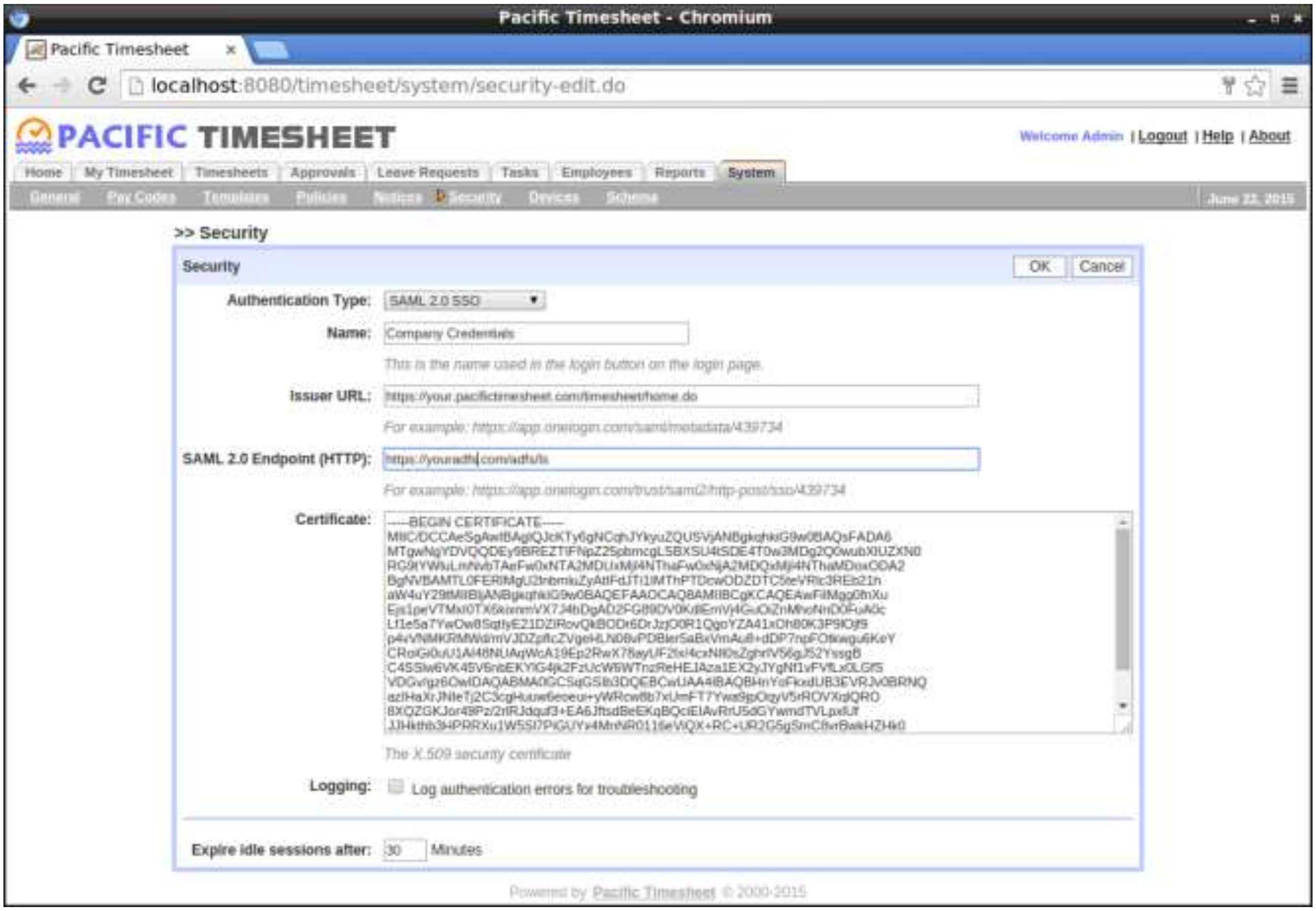

Windows Server 2012 - VMware Player (Non-commercial use only)
File Virtual Machine Help
Server Manager
Manage Tools View Help
Edit Claim Rules for Pacific Time Sheets
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply
Help
AD FS
Manageability
Events
Services
Performance
BPA results
To release input, press Ctrl+Alt

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

Order	Rule Name	Issued Claims
1	Set Name ID	Name ID

Okay

Press OK.



>> Security

Security

Authentication Type: SAML 2.0 SSO

Name: Company Credentials

This is the name used in the login button on the login page.

Issuer URL: https://your.pacifictimesheet.com/timesheet/home.do

For example: https://app.onelogin.com/saml/metadata/439734

SAML 2.0 Endpoint (HTTP): https://youradfs.com/adfs/ls

For example: https://app.onelogin.com/trust/saml2/http-post/sso/439734

Certificate:

```
-----BEGIN CERTIFICATE-----
MIIC/DCCAeSgAwIBAgIQJcKTy6gNCqhJYkyuZQUSVjANBgkqhkiG9w0BAQsFADA6
MTgwNgYDVQQDEy9BREZTIFNpZ25pbmcgLSBXSU4tSDE4T0w3MDg2Q0wubXlUZXN0
RG9tYWluLmNvbTAeFw0xNTA2MDUxMjI4NThaFw0xNjA2MDQxMjI4NThaMDoxODA2
BgNVBAMTL0FERlMgU2lnbmluZyAtIFdJTi1IMThPTDcwODZDTC5teVRlc3REb21h
aW4uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwFilMgg0fnXu
Ejs1peVTMxl0TX6kxnmVX7J4bDgAD2FG89DV0KdlEmVj4GuOiZnMhoNnD0FuA0c
Lf1e5a7YwOw8SqtIyE21DZlRovQkBODr6DrJzjO0R1QgoYZA41xOh80K3P9lOjf9
p4vVNMKRMWdimVJDZpflcZVgeHLN08vPDBlerSaBxVmAu8+dDP7npFOtkwgu6KeY
CRoiGi0uU1A/48NUAqWcA19Ep2RwX78ayUF2lxl4cxNl0sZghrlV56gJ52YssgB
C4SSiw6VK45V6nbEKYlG4jk2FzUcW6WTnzReHEJAza1EX2yJYgNf1vFVfLx0LGf5
VDGvlgz6OwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBHnYoFkxdUB3EVRJv0BRNQ
azlHaXrJNIeTj2C3cgHuuw6eoeu+yWRcw8b7xUmFT7Ywa9jpOqyV5rROVXqlQRO
8XQZGKJor49Pz/2rlRJdquf3+EA6JftsdBeEKqBQciEIAvRrU5dGYwmdTVLpxlUf
JJHkthb34PRRXu1W5Sl7PiGUYx4MnNR011eViQX+RC+UR2G5g5mC8vrBwkHZHk0
```

The X.509 security certificate

Logging: □ Log authentication errors for troubleshooting

Expire idle sessions after: 30 Minutes

Setup Pacific Timesheet SAML 2.0 Security Page

Log into Pacific Timesheet and navigate to system>security>authentication>SAML 2.0.

Now taking the information you gathered earlier along with the converted certificate, enter those values into the Pacific Timesheet security dialog.

Testing

You can now test AD FS SSO with Pacific Timesheet. Any active user with AD FS credentials will be able to connect with and use Pacific Timesheet.