Setup adfs

Getting adfs

Download from http://www.microsoft.com/en-US/download/details.aspx?id=10909\

Choose the right version (x84/x64)

Can also be done with Servermanager (see ADFS Proxy)

Install

Install the adfs on the Active Directory Server

http://support.druva.com/entries/21437659-How-to-install-and-Configure-Active-Directory-Federation-Services-for-Druva-inSync-Cloud-SAML-integr

To install the ADFS 2.0 software using the setup wizard

1. Download the ADFS 2.0 software by saving the AdfsSetup.exe setup file onto the computer. To download this file, go to Active Directory Federation Services 2.0 RTW (http://go.microsoft.com/fwlink/?LinkId=151338).

2. Locate the AdfsSetup.exe setup file that you downloaded to the computer, and then double-click it.

3. On the Welcome to the ADFS 2.0 Setup Wizard page, click Next.

4. On the End-User License Agreement page, read the license terms.

5. If you agree to the terms, select the I accept the terms in the License Agreement check box, and then click Next.

6. On the Server Role page, select one of the following options, depending on the role for which you will configure this computer.

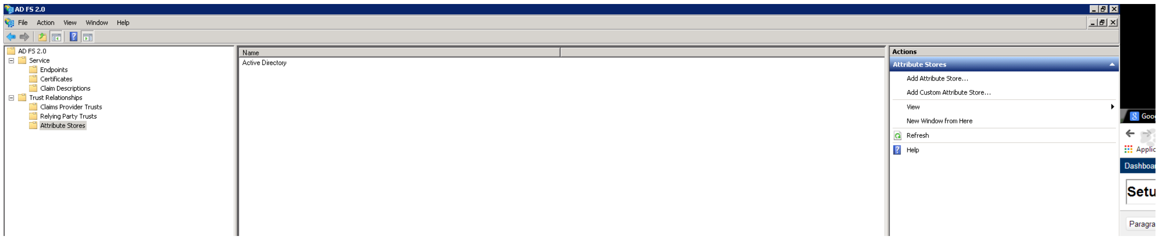
- To install ADFS 2.0 and to begin the process of configuring it for the federation server role, select **Federation server**, and then click **Next.**
- To install ADFS 2.0 and begin the process of configuring it for the federation server proxy role, select **Federation server proxy**, and then click **Next**.

7. On the Install Prerequisite Software page, click Next.
After you click Next, you see the Installing ADFS 2.0 page.
Note: The installation process can take up to 20 minutes to complete, depending on how many of the prerequisites are already installed on the computer.

8. On the Completed the ADFS 2.0 Setup Wizard page, verify that the Restart now checkbox is selected, and then click Finish to restart the computer.

After setup, open "AD FS 2.0 Management"

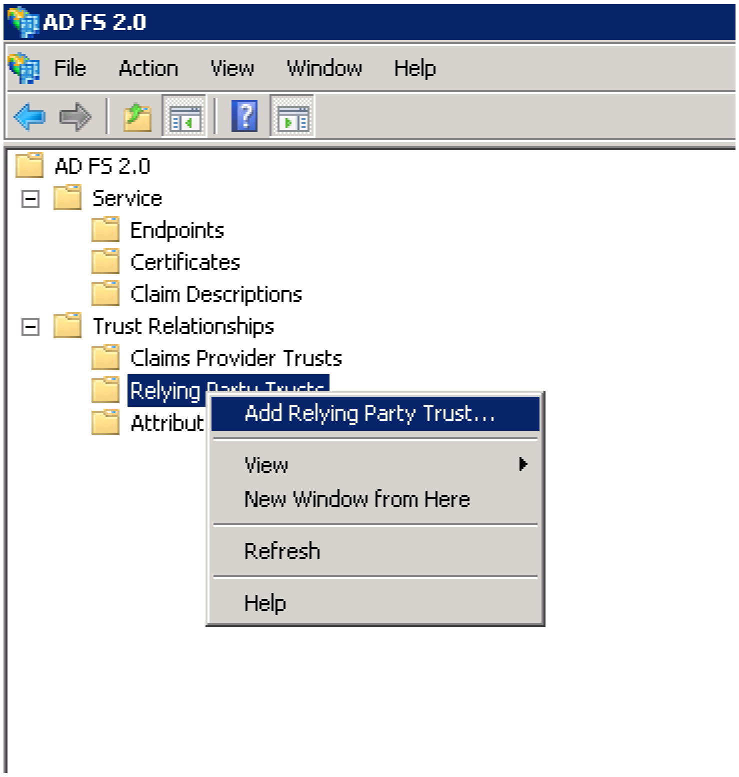
When installing adfs on the AD server it adds automaticly the AD to the atribute store, meaning that the AD is coupled to the adfs.



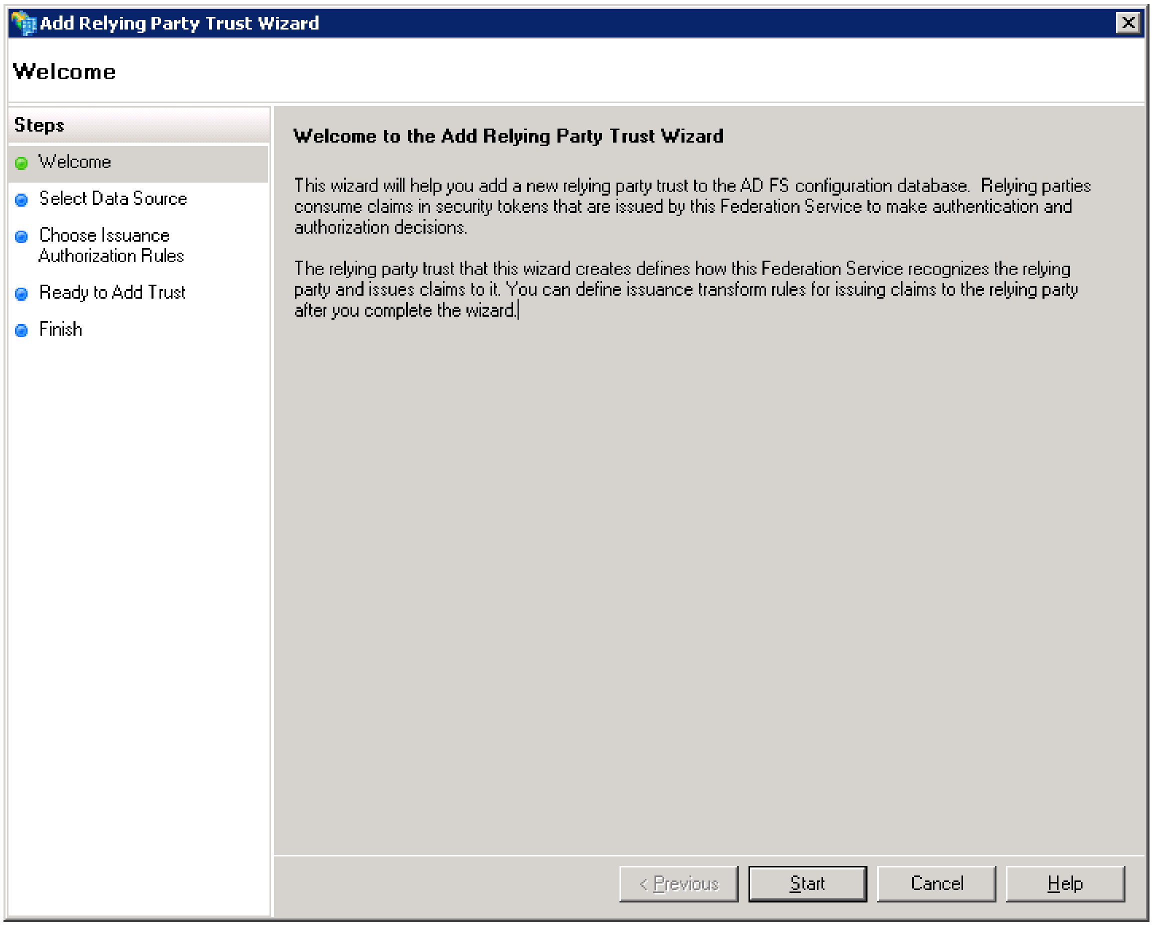
Configuring an Service provider from simple saml

Open AD FS 2.0 Manager

Right click on "Relying Party Trusts" and click "Add Relying Party Trust..."



Then the wizard start to add the service provider.

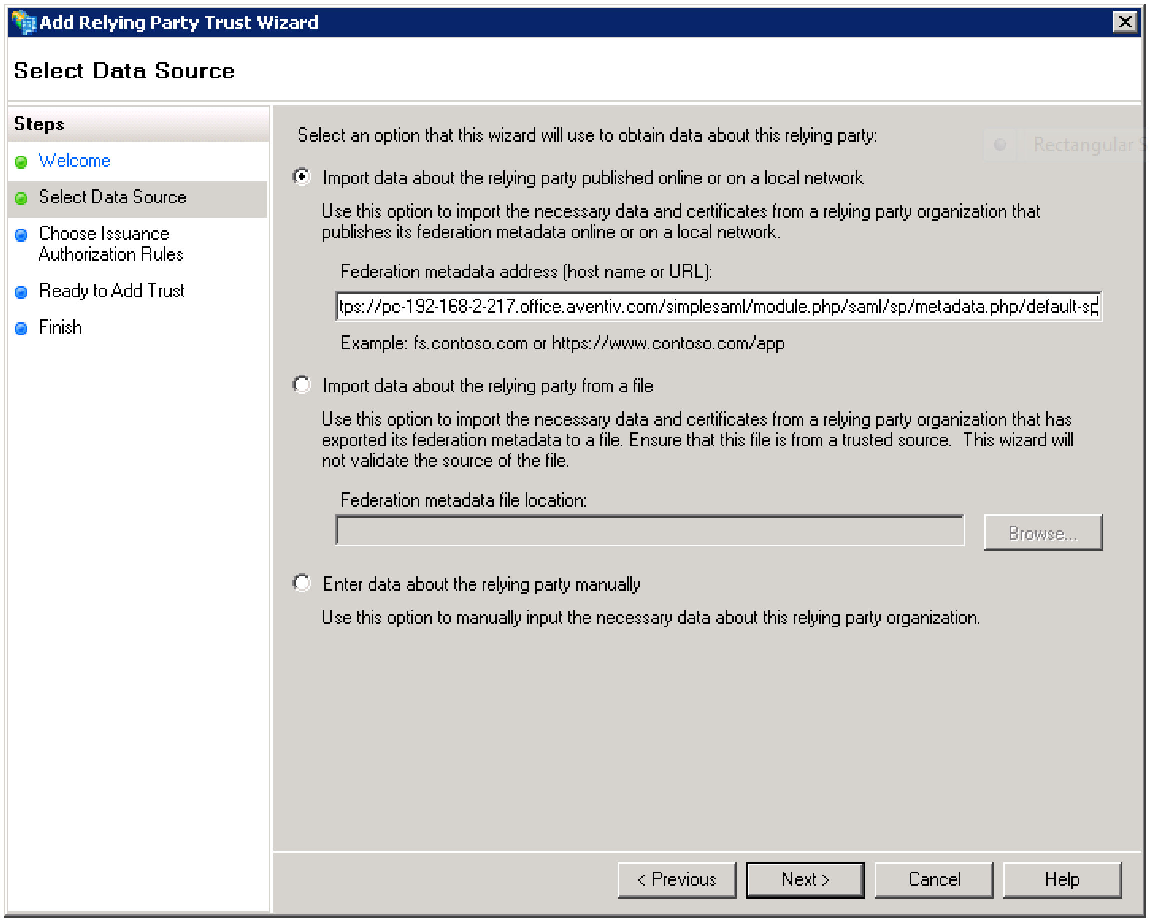


Welcome to the Add Relying Party Trust Wizard

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



Select Data Source

Steps

- Welcome
- Select Data Source
- 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):

tps://pc-192-168-2-217.office.aventiv.com/simplesaml/module.php/saml/sp/metadata.php/default-sp

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.

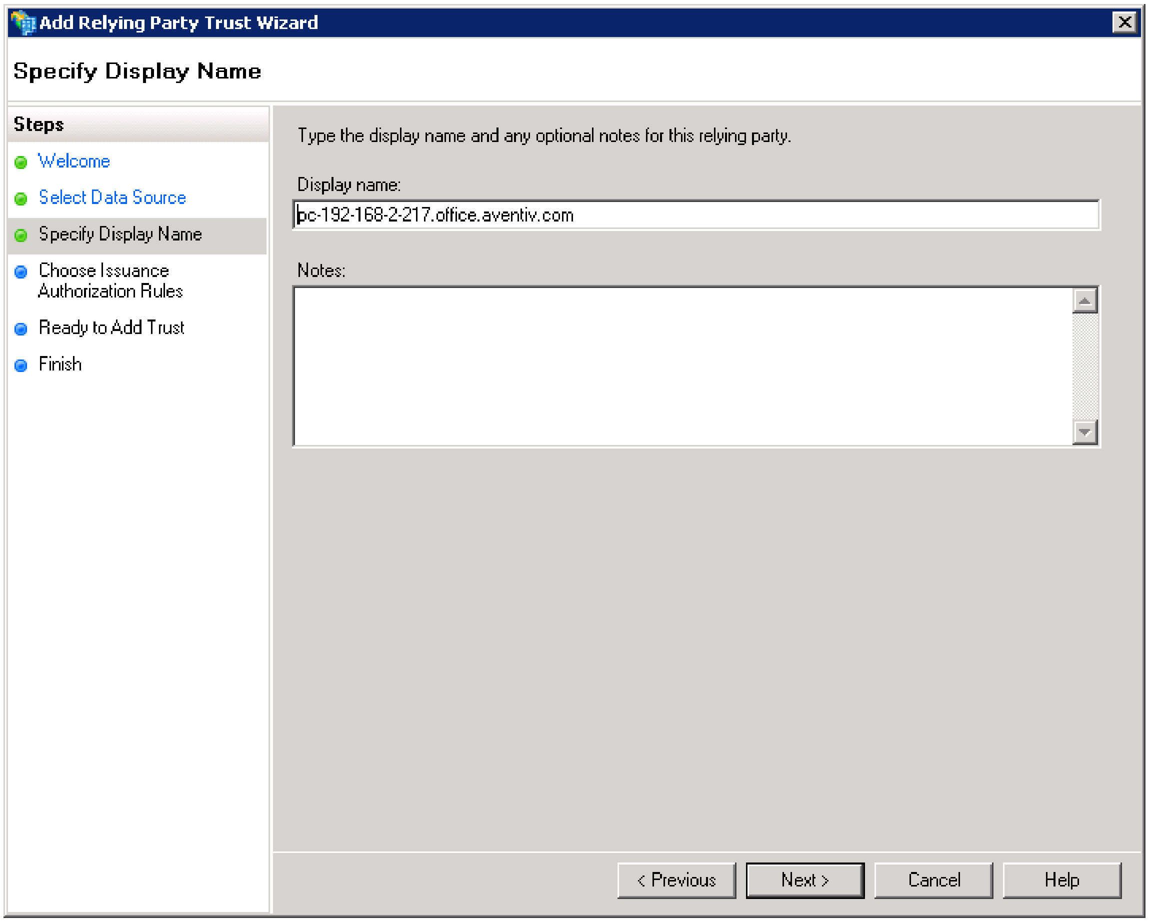
Select the first option and enter the url from the service provider

url example

https://[HOSTNAME]/simplesaml/module.php/saml/sp/metadata.php/[SERVICE]

Make sure that the certificate is accepted by the ADFS server, this can be tested by surfing to the url in a webbrowser.

Then click next and Ok in the pop up.



Specify Display Name

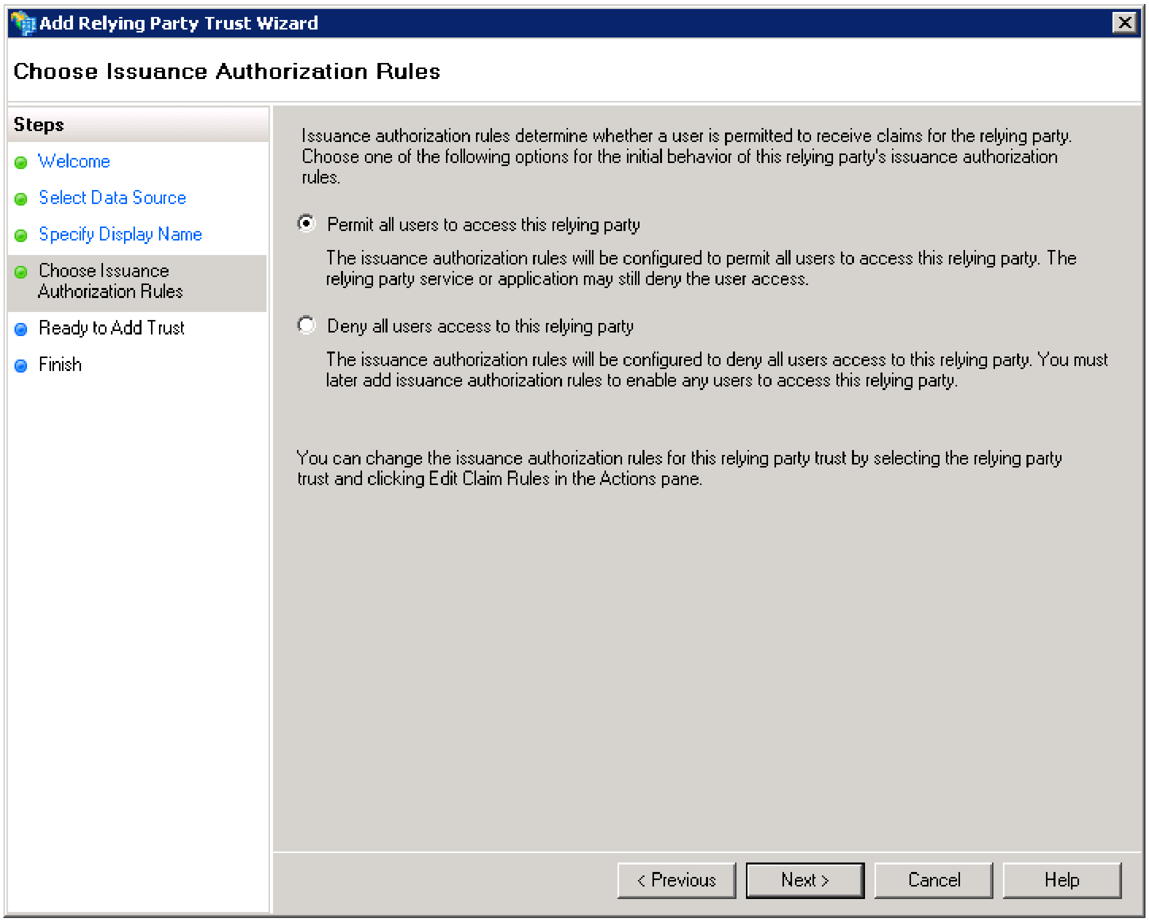
Type the display name and any optional notes for this relying party.

Display name: pc-192-168-2-217.office.aventiv.com

Notes:

Insert a Display name, or leave it at the default.

Click next.



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

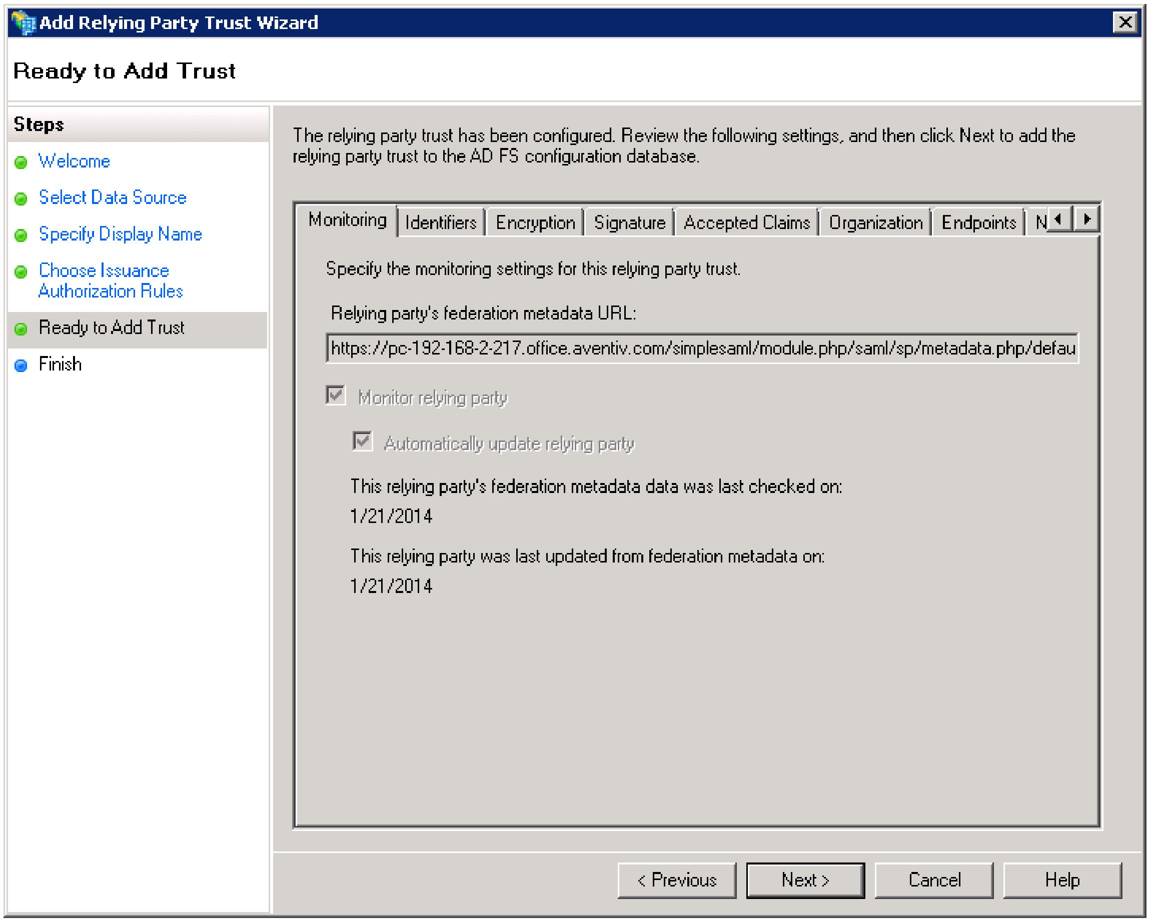
The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

○ 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.

Select the first option and click next.



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:

https://pc-192-168-2-217.office.aventiv.com/simplesaml/module.php/saml/sp/metadata.php/defau

☑ Monitor relying party

☑ Automatically update relying party

This relying party's federation metadata data was last checked on:

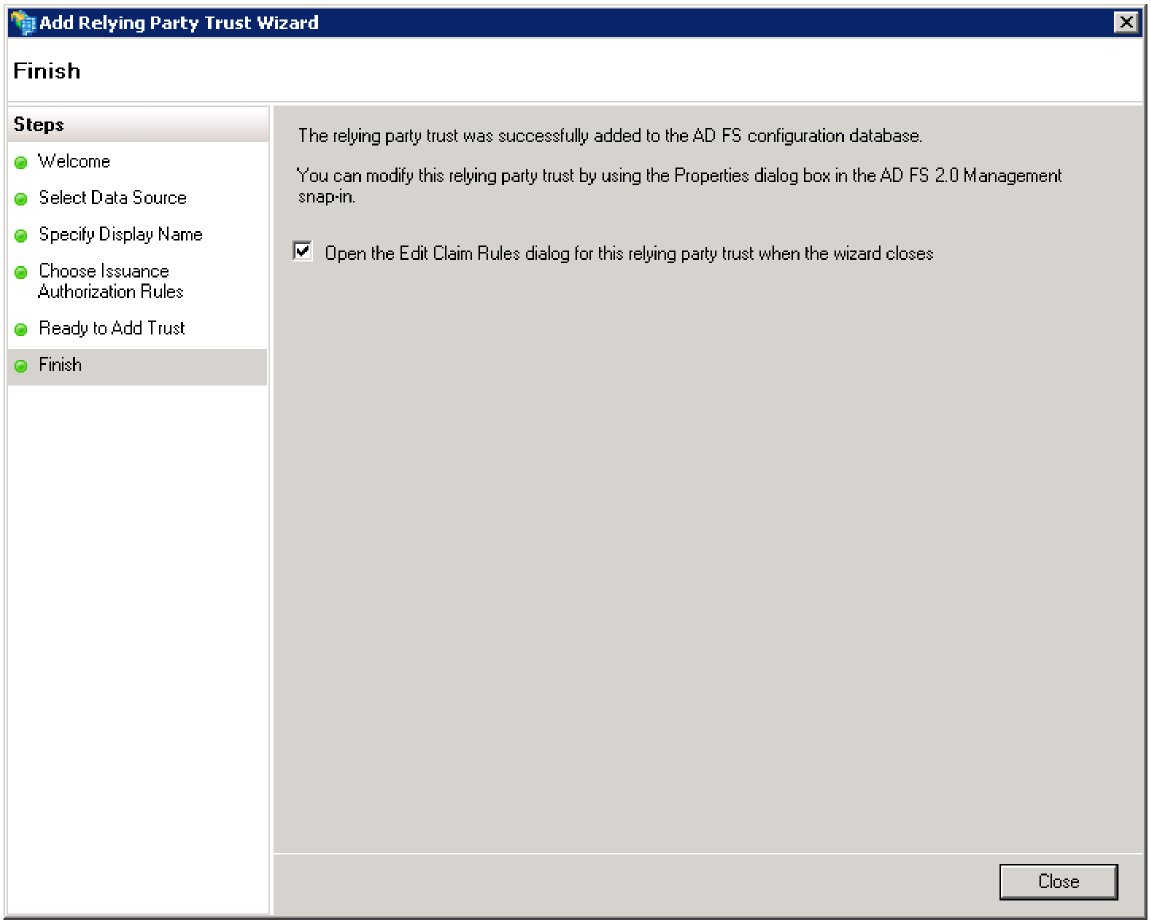
1/21/2014

This relying party was last updated from federation metadata on:

1/21/2014

This is the overview of all the settings coming from the server.

Click next



Add Relying Party Trust Wizard

Finish

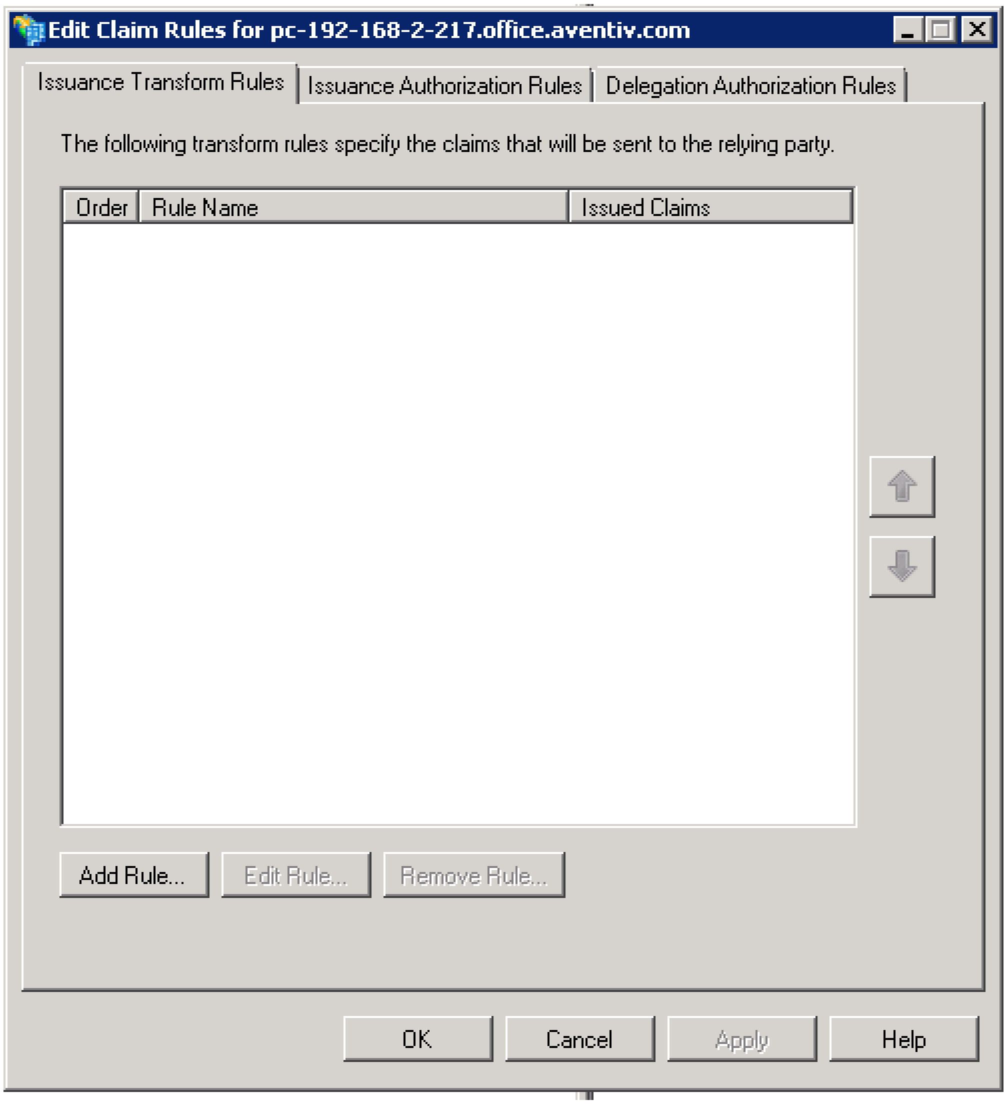
The relying party trust was successfully added to the AD FS configuration database.

You can modify this relying party trust by using the Properties dialog box in the AD FS 2.0 Management snap-in.

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

Let the checkbox checked and click close

Then a window appears to setup de SAML message.

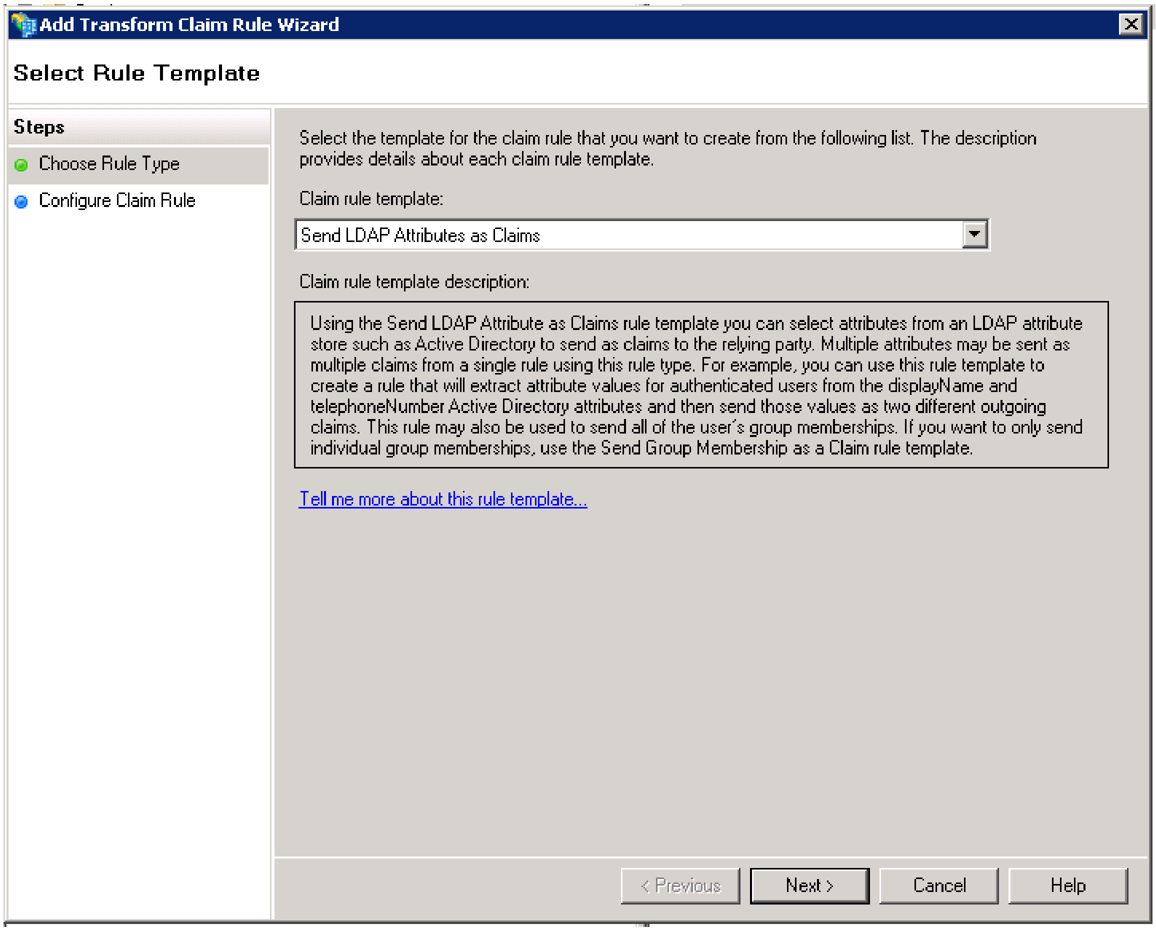


Edit Claim Rules for pc-192-168-2-217.office.aventiv.com

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

Order	Rule Name	Issued Claims

Click on Add Rule to configure the message



Add Transform Claim Rule 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

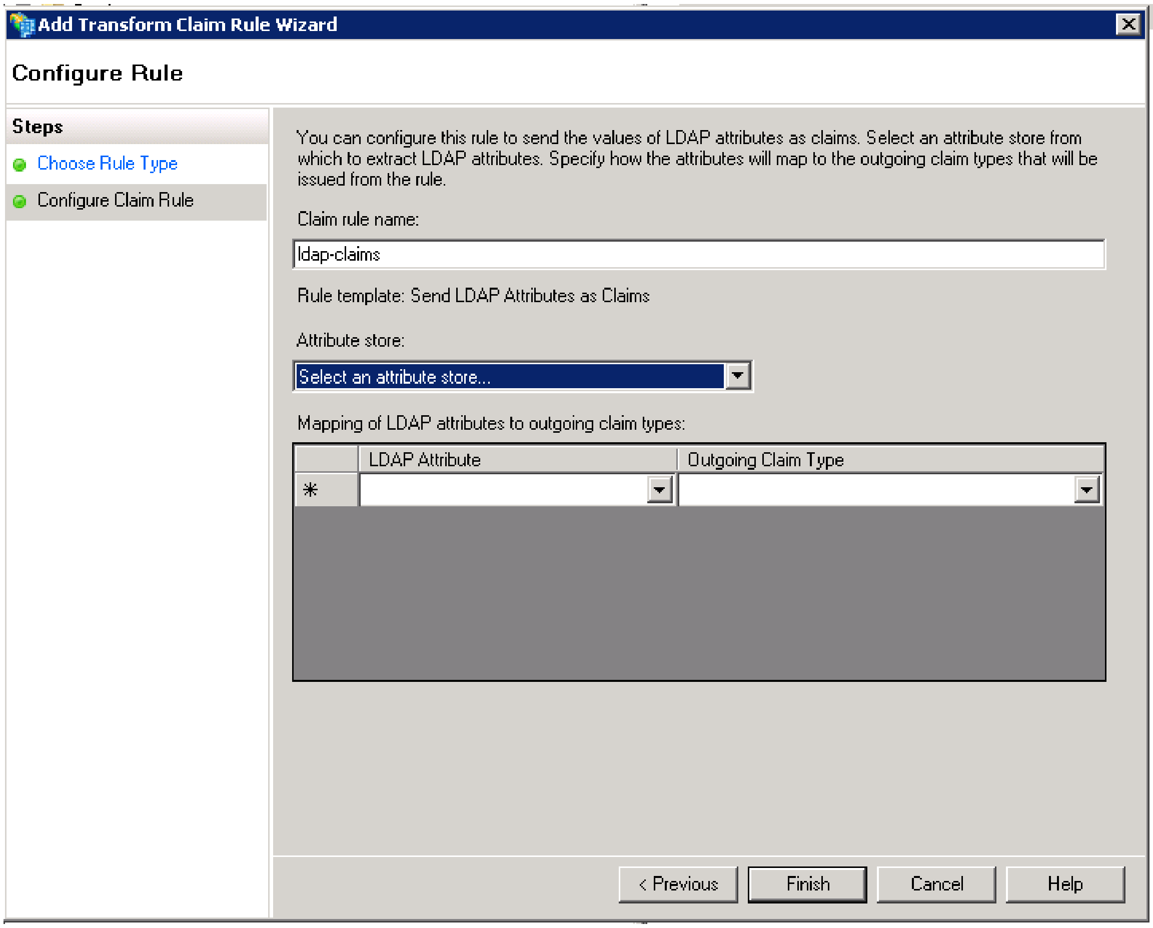
Claim rule template description:

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.

Tell me more about this rule template...

We want to send info from AD (LDAP)

Click 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: ldap-claims

Rule template: Send LDAP Attributes as Claims

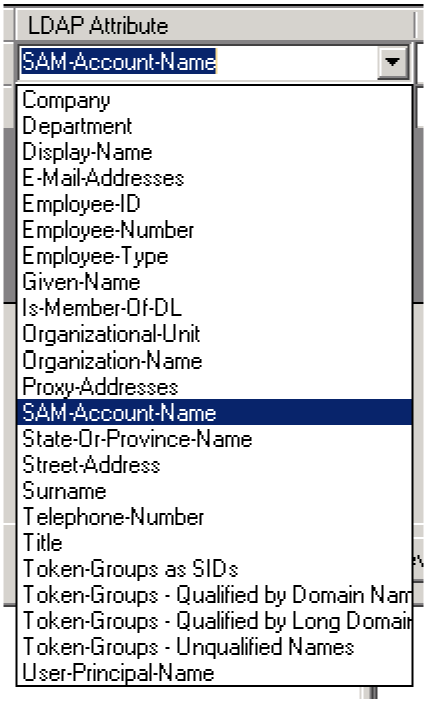
Attribute store: Select an attribute store...

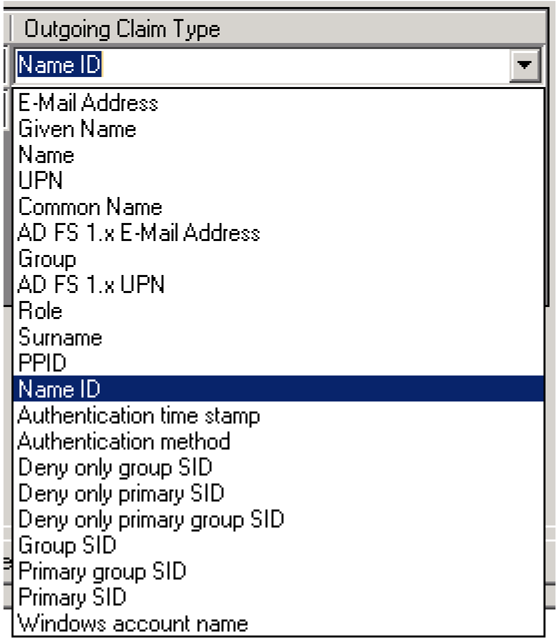
Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute	Outgoing Claim Type
*		

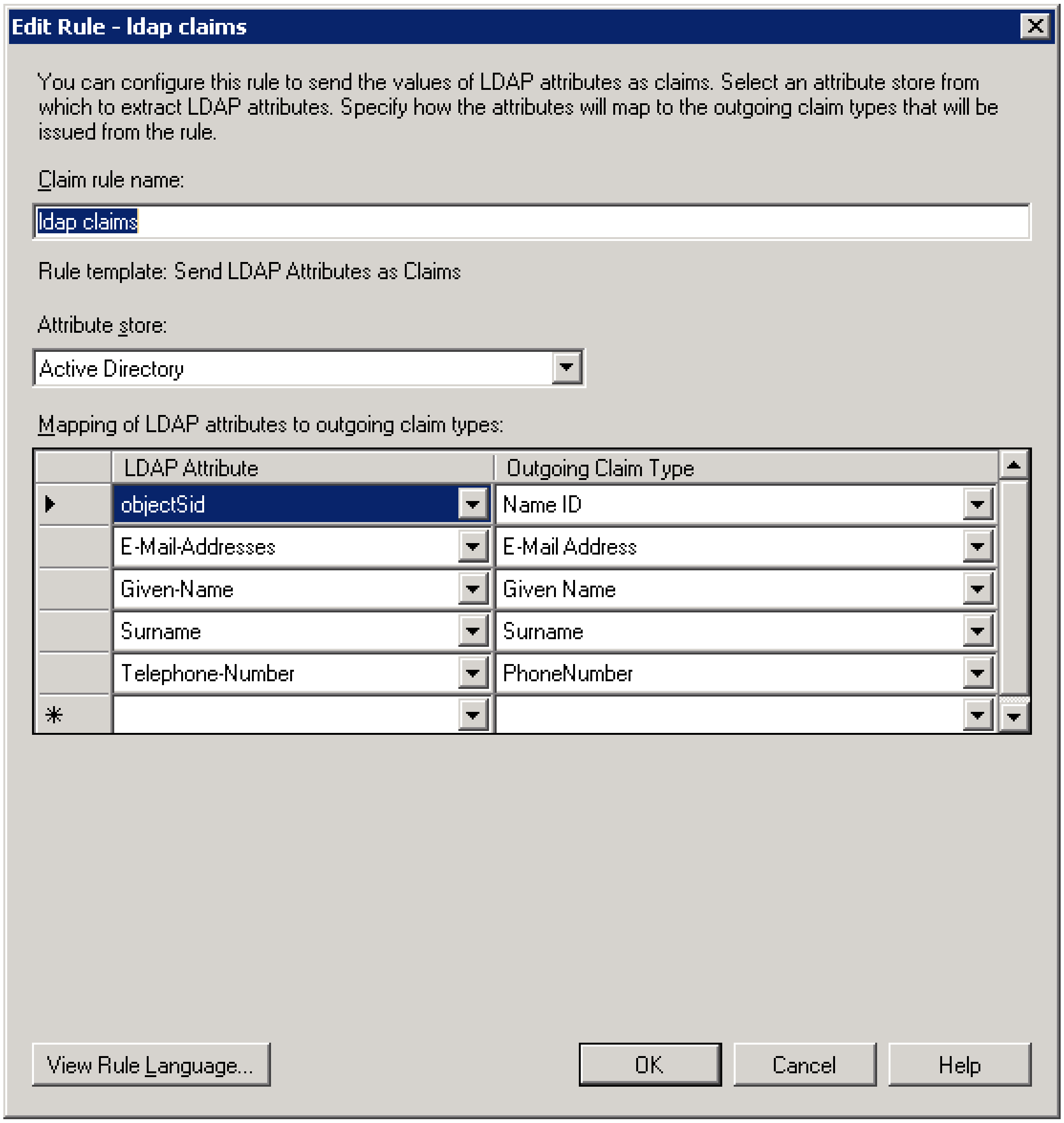
Give the rule a name, then select the attribute store (Default is Active Directory)

Then add at least one rule:





Add other attributes if neccesery then click Finish.



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:

ldap claims

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

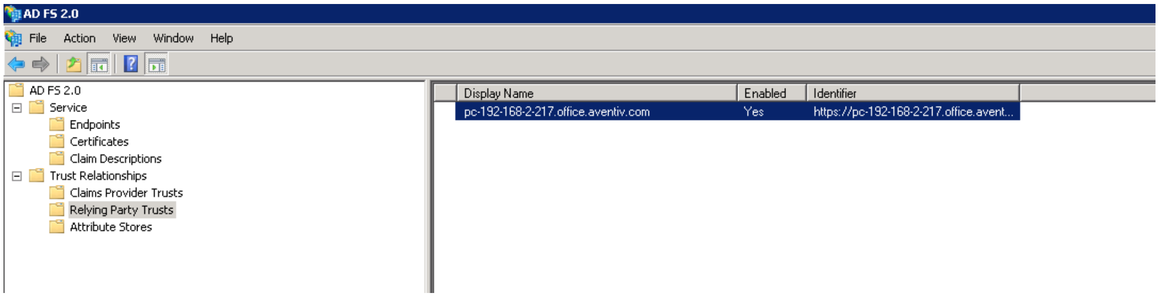
Mapping of LDAP attributes to outgoing claim types:

LDAP Attribute	Outgoing Claim Type
objectSid	Name ID
E-Mail-Addresses	E-Mail Address
Given-Name	Given Name
Surname	Surname
Telephone-Number	PhoneNumber

*Note: For Outgoing claim "Name ID", you have to manualy type "objectSid" into the LDAP Attribute list.

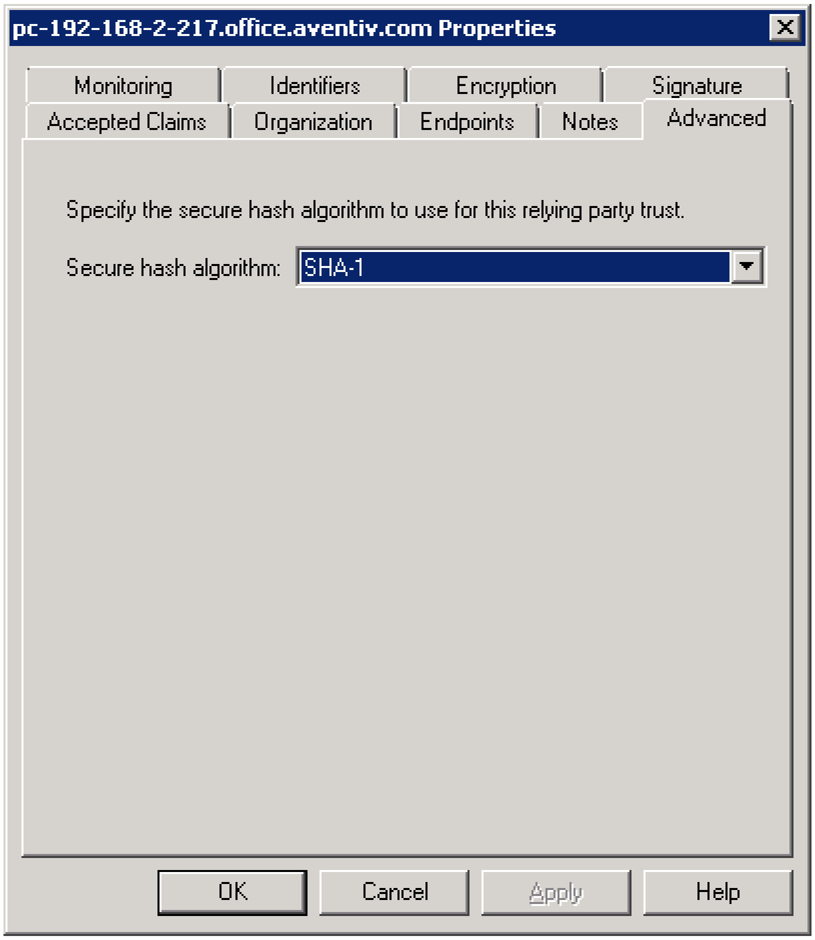
Add other rules if neccesery of click Apply - Ok to close.

Open in the AD FS 2.0 Manager the "Relying Party Trusts" folder



Display Name	Enabled	Identifier
pc-192-168-2-217.office.aventiv.com	Yes	https://pc-192-168-2-217.office.avent...

Double click on the newly added Service provider


pc-192-168-2-217.office.aventiv.com Properties

Specify the secure hash algorithm to use for this relying party trust.

Secure hash algorithm: SHA-1

Open the "Advanced" Tab and set Secure hash algorithm to SHA-1

Basic Authentication and Chrome

In the event viewer you will see an 'Audit Failure' event with "Status: 0xc000035b".

You can circumvent this problem by switching off 'Extended Protection' for the adfs/ls web application.

Some extra info about the extended protection:

> *Disabling Extended Protection does make the credential more vulnerable to man-in-the-middle attacks. But since Chrome does not support Extended Protection, you have to disable it.*
>
> *For more information about the Extended Protection in ADFS, you may refer the following links,*
>
> *Configuring Advanced Options for AD FS 2.0 and Office 365*
> *http://technet.microsoft.com/en-us/library/hh237448%28v=ws.10%29.aspx*
>
> *AD FS 2.0: Continuously Prompted for Credentials While Using Fiddler Web Debugger*
> *http://social.technet.microsoft.com/wiki/contents/articles/ad-fs-2-0-continuously-prompted-for-credentials-while-using-fiddler-web-debugger.aspx*
>
> *Extended Protection for Authentication*

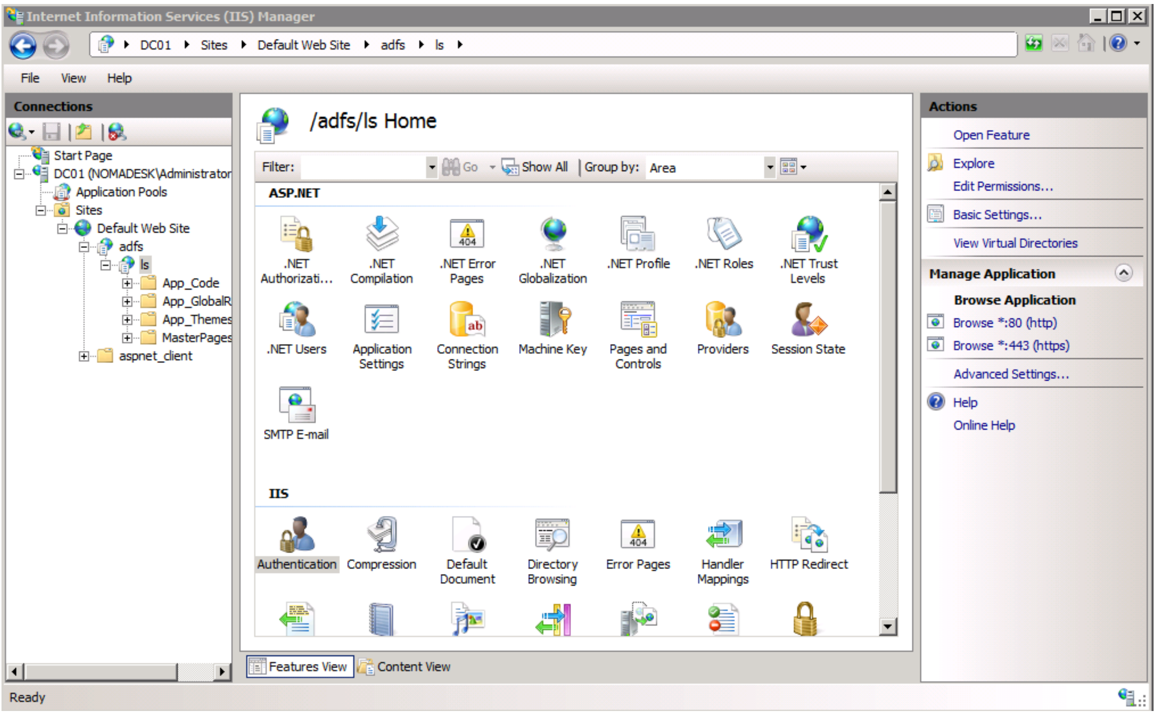
http://support.microsoft.com/kb/968389

Note that this is also for old firefox versions, it was fixed in Mozilla 11.

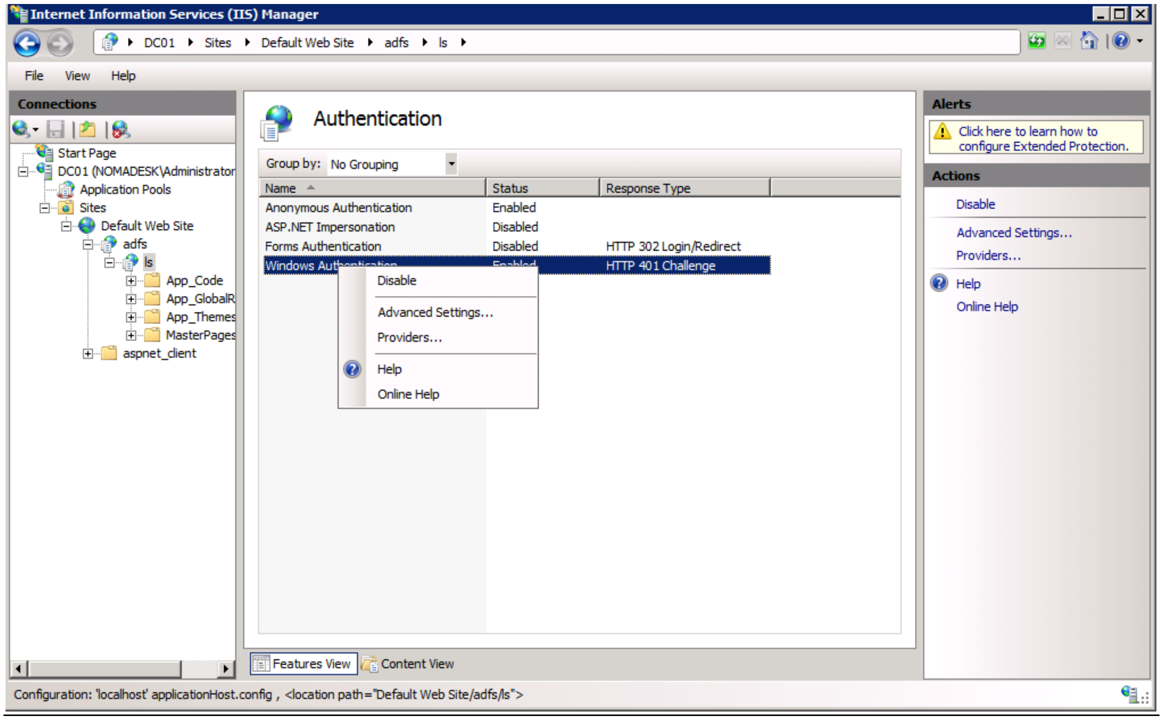
To turn Extended Protection off, on the AD FS server:

1. launch IIS Manager,
2. In the left side tree view, access Sites -> Default Web Site -> adfs -> ls.
3. Selected the "/adfs/ls" folder,
4. double-click the Authentication icon,
5. Right-click Windows Authentication and select "Advanced Settings…"
6. On the Advanced Settings dialog, choose Off for Extended Protection.
7. Restart IIS

Step 1 => 4



Step 5:



Authentication

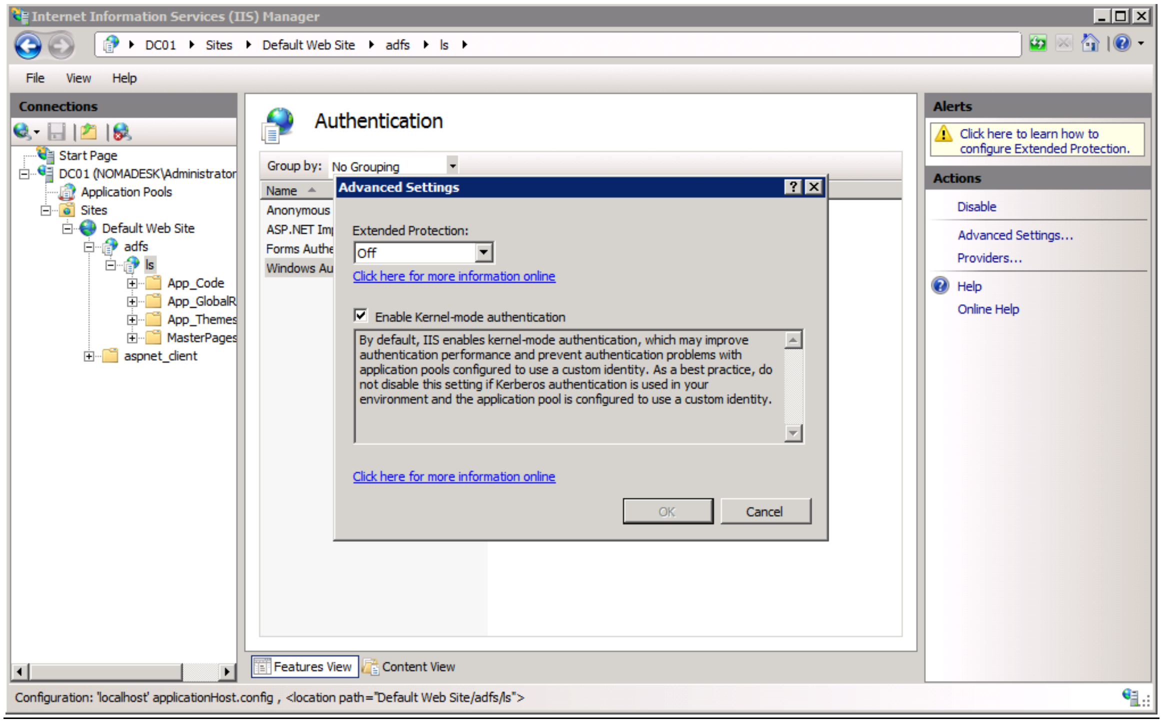
Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

Click here to learn how to configure Extended Protection.

Configuration: 'localhost' applicationHost.config , <location path="Default Web Site/adfs/ls">

<u>Step 6:</u>



Authentication

Group by: No Grouping

Advanced Settings

Extended Protection: Off

Click here for more information online

☑ Enable Kernel-mode authentication

By default, IIS enables kernel-mode authentication, which may improve authentication performance and prevent authentication problems with application pools configured to use a custom identity. As a best practice, do not disable this setting if Kerberos authentication is used in your environment and the application pool is configured to use a custom identity.

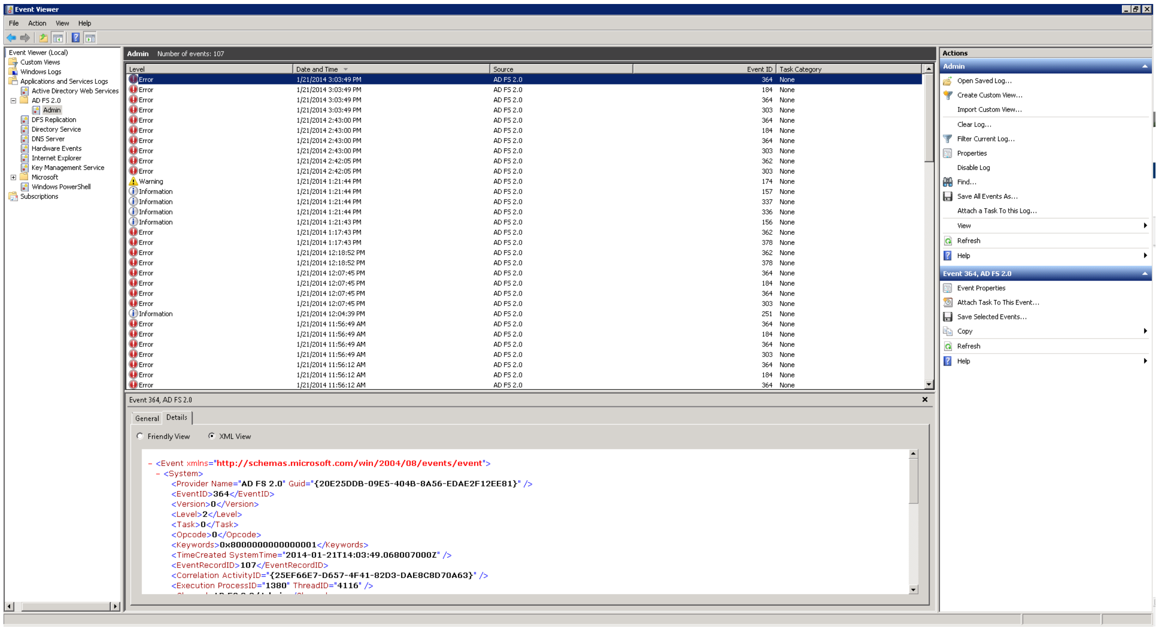
Click here for more information online

Click here to learn how to configure Extended Protection.

Configuration: 'localhost' applicationHost.config , <location path="Default Web Site/adfs/ls">

Error log

Open the Windows event viewer and go to "Applicatios and Services Logs" - "AD FS 2.0" - "Admin"



Admin Number of events: 107

Level	Date and Time	Source	Event ID	Task Category
Error	1/21/2014 3:03:49 PM	AD FS 2.0	364	None
Error	1/21/2014 3:03:49 PM	AD FS 2.0	184	None
Error	1/21/2014 3:03:49 PM	AD FS 2.0	364	None
Error	1/21/2014 3:03:49 PM	AD FS 2.0	303	None
Error	1/21/2014 2:43:00 PM	AD FS 2.0	364	None
Error	1/21/2014 2:43:00 PM	AD FS 2.0	184	None
Error	1/21/2014 2:43:00 PM	AD FS 2.0	364	None
Error	1/21/2014 2:43:00 PM	AD FS 2.0	303	None
Error	1/21/2014 2:42:05 PM	AD FS 2.0	362	None
Error	1/21/2014 2:42:05 PM	AD FS 2.0	303	None
Warning	1/21/2014 1:21:44 PM	AD FS 2.0	174	None
Information	1/21/2014 1:21:44 PM	AD FS 2.0	157	None
Information	1/21/2014 1:21:44 PM	AD FS 2.0	337	None
Information	1/21/2014 1:21:44 PM	AD FS 2.0	336	None
Information	1/21/2014 1:21:43 PM	AD FS 2.0	156	None
Error	1/21/2014 1:17:43 PM	AD FS 2.0	362	None
Error	1/21/2014 1:17:43 PM	AD FS 2.0	378	None
Error	1/21/2014 12:18:52 PM	AD FS 2.0	362	None
Error	1/21/2014 12:18:52 PM	AD FS 2.0	378	None
Error	1/21/2014 12:07:45 PM	AD FS 2.0	364	None
Error	1/21/2014 12:07:45 PM	AD FS 2.0	184	None
Error	1/21/2014 12:07:45 PM	AD FS 2.0	364	None
Error	1/21/2014 12:07:45 PM	AD FS 2.0	303	None
Information	1/21/2014 12:04:39 PM	AD FS 2.0	251	None
Error	1/21/2014 11:56:49 AM	AD FS 2.0	364	None
Error	1/21/2014 11:56:49 AM	AD FS 2.0	184	None
Error	1/21/2014 11:56:49 AM	AD FS 2.0	364	None
Error	1/21/2014 11:56:49 AM	AD FS 2.0	303	None
Error	1/21/2014 11:56:12 AM	AD FS 2.0	364	None
Error	1/21/2014 11:56:12 AM	AD FS 2.0	184	None
Error	1/21/2014 11:56:12 AM	AD FS 2.0	364	None

Event 364, AD FS 2.0

General Details

○ Friendly View ● XML View

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  - <System>
      <Provider Name="AD FS 2.0" Guid="{20E25DDB-09E5-404B-8A56-EDAE2F12EE81}" />
      <EventID>364</EventID>
      <Version>0</Version>
      <Level>2</Level>
      <Task>0</Task>
      <Opcode>0</Opcode>
      <Keywords>0x8000000000000001</Keywords>
      <TimeCreated SystemTime="2014-01-21T14:03:49.068007000Z" />
      <EventRecordID>107</EventRecordID>
      <Correlation ActivityID="{25EF66E7-D657-4F41-82D3-DAE8C8D70A63}" />
      <Execution ProcessID="1380" ThreadID="4116" />
```