

Collaborate Single Sign-on Configuration

Integration with Active Directory Federation Services (ADFS)

by **Shahid Munir**

November 2013

COMMERCIAL IN CONFIDENCE

1. Setting up and Configuring ADFS for SSO to work with HighQHub

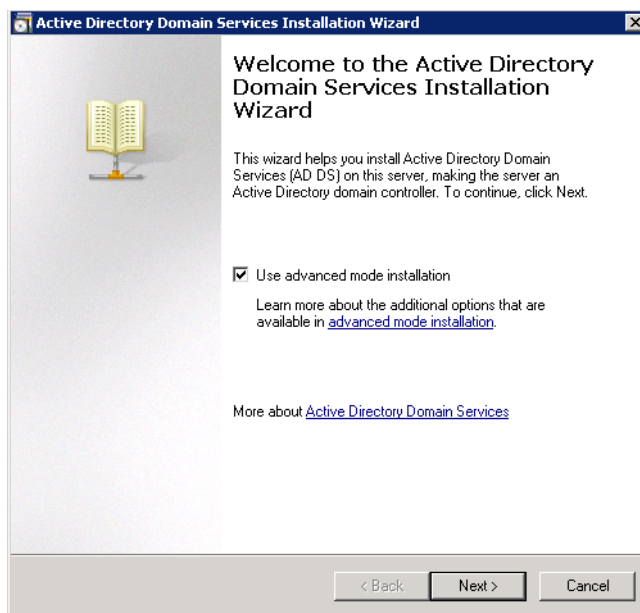
If you already have a Domain Controller setup in your network you can skip first part and start from

First of all an Active Directory Domain must be installed.

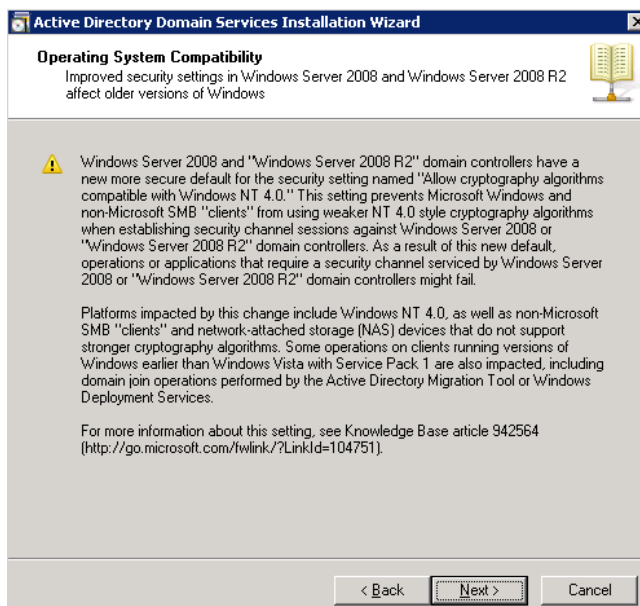
Here is a step-by-step guide how to setup new Active Directory Domain if you don't already have one. In this example, we setup an AD Domain highq.com.

This document is based on a Windows Server 2008 R2.

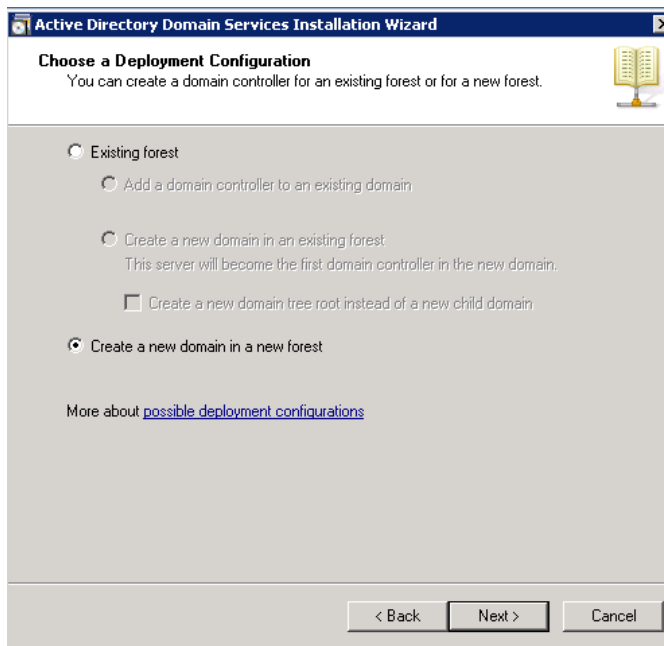
From run prompt, run "dcpromo" to setup domain and follow the setup Wizard.



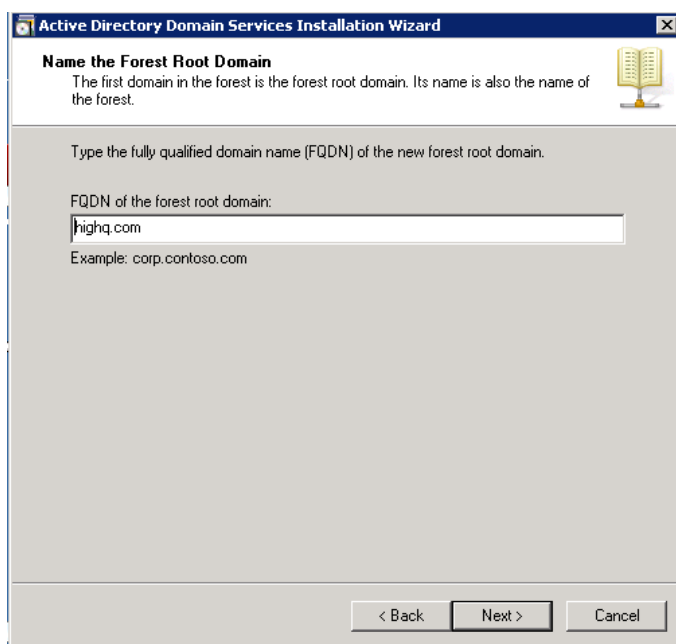
Select advanced mode installation.



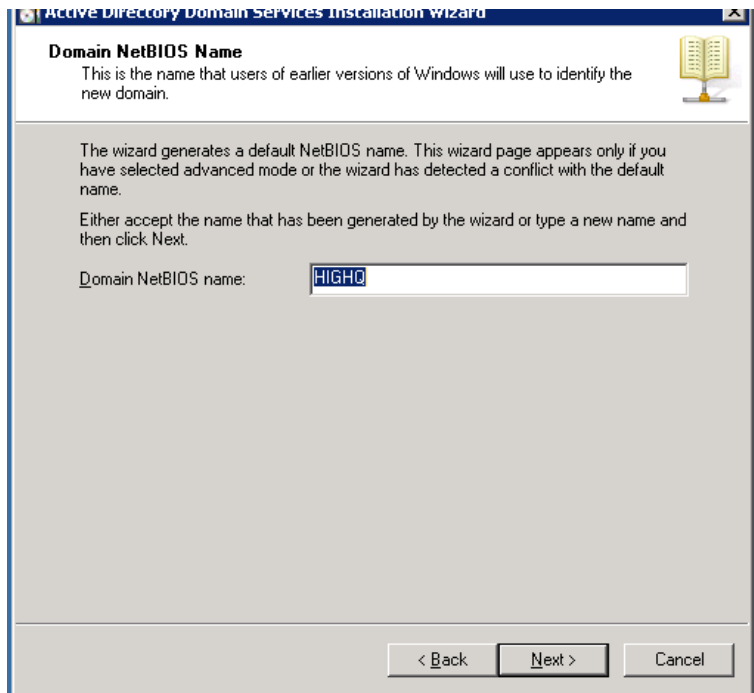
Click Next.



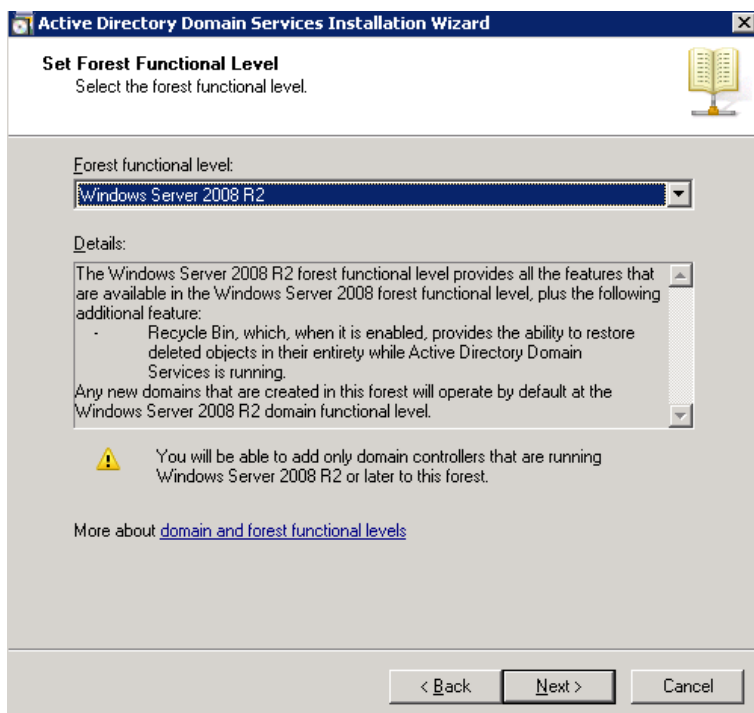
In this example we are creating a new domain, so “Create a new domain in a new forest” is selected.



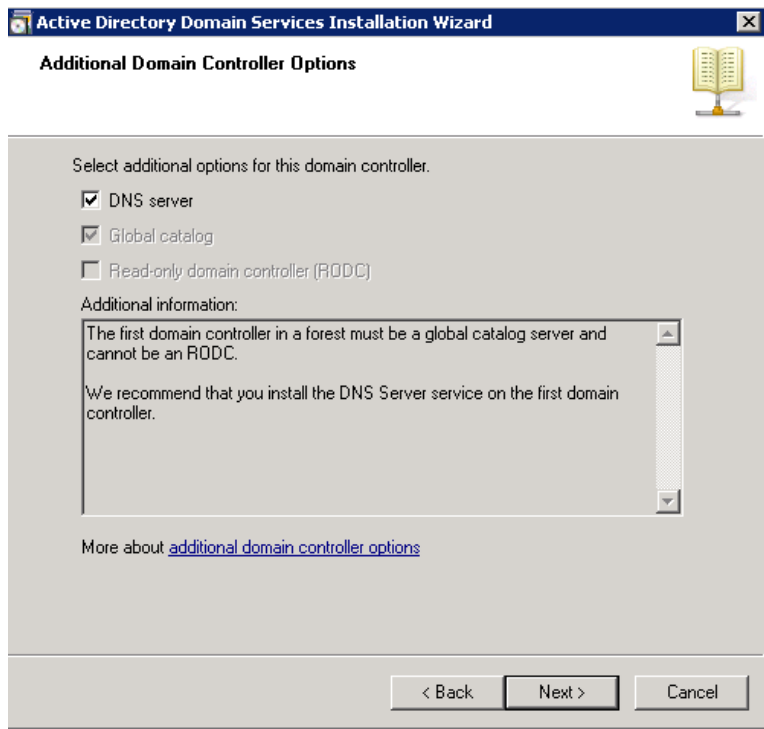
Enter the Fully Qualified Domain Name of the forest root domain; here it is “highq.com”



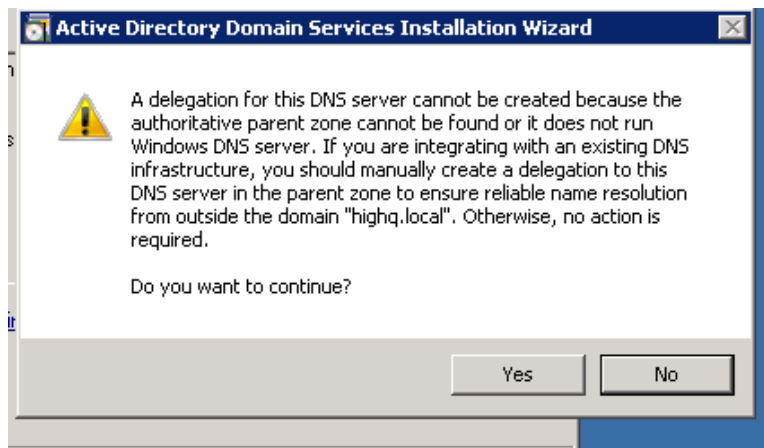
Leave as default "HIGHQ".



Forest functional level selected as "Windows Server 2008 R2"



Select DNS Server to install DNS on same machine.



If you see warning above, ignore it.

Finish and restart server.

2. ADFS Installation

Download ADFS 2.0 from link below.

<http://www.microsoft.com/en-au/download/details.aspx?id=10909>

Active Directory Federation Services 2.0 RTW

Quick links

- Overview
- System requirements
- Instructions
- Additional information

Microsoft Store

Find quality products from people you trust >

Active Directory Federation Services 2.0 helps IT enable users to collaborate across organizational boundaries and easily access applications on-premises and in the cloud, while maintaining application security.

Registration Suggested

Registration takes only a few moments and allows Microsoft to provide you with the latest resources relevant to your interests, including service packs, security notices, and training. Please click the **Continue** button. Registration is suggested for this download.

Quick details

Version: RTW Date Published: 18/04/2011

Change Language: English

Files in this download

The links in this section correspond to files available for this download. Download the files appropriate for you.

File Name	Size	
RTW\W2K8\amd64\AdfsSetup.exe	42.5 MB	CONTINUE
RTW\W2K8\x86\AdfsSetup.exe	38.6 MB	
RTW\W2K8R2\amd64\AdfsSetup.exe	23.9 MB	

For Win2k8 R2 64bit download direct link is,

<http://download.microsoft.com/download/F/3/D/F3D66A7E-C974-4A60-B7A5-382A61EB7BC6/RTW/W2K8R2/amd64/AdfsSetup.exe>

Proceed to Download

Though you have declined to register now, please consider registering in the future. Your registration information allows Microsoft to provide you with the latest resources relevant to your interests, including service packs, security notices, and training. Please click the **Download** button or **Download Files Below** link to start the download.

Quick details

Version: RTW Date Published: 18/04/2011

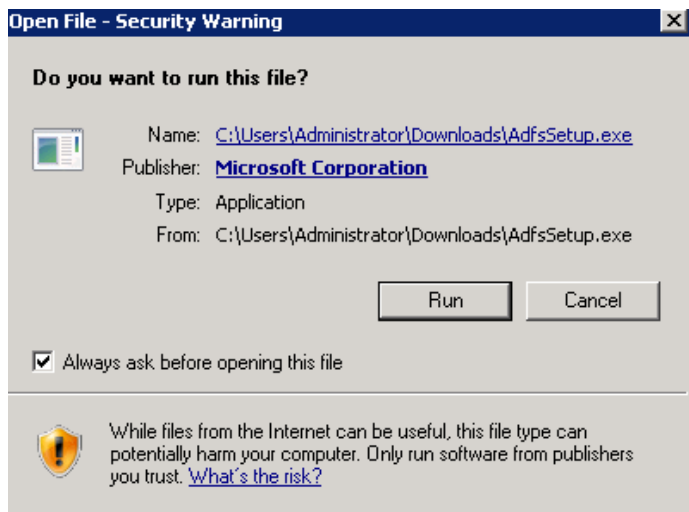
Change Language: English

Files in this download

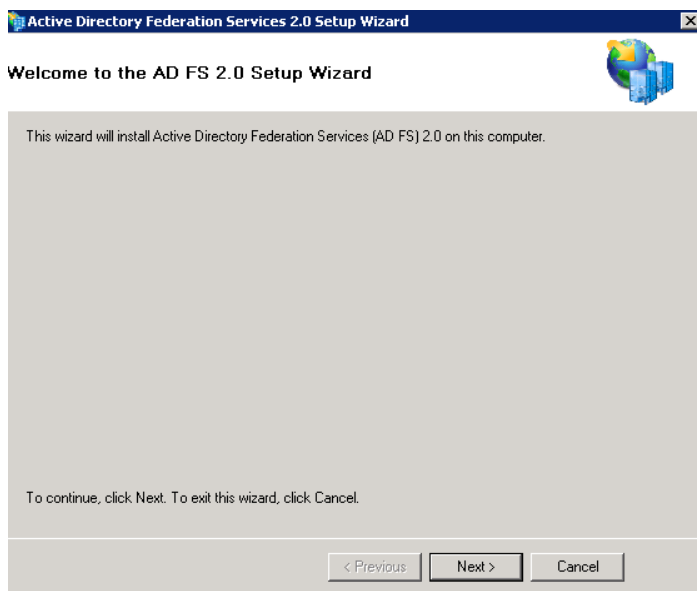
The links in this section correspond to files available for this download. Download the files appropriate for you.

File Name	Size	
RTW\W2K8\amd64\AdfsSetup.exe	42.5 MB	DOWNLOAD
RTW\W2K8\x86\AdfsSetup.exe	38.6 MB	DOWNLOAD
RTW\W2K8R2\amd64\AdfsSetup.exe	23.9 MB	DOWNLOAD

Run the setup “AdfsSetup.exe”



Follow the step-by-step wizard to Setup AD DS 2.0

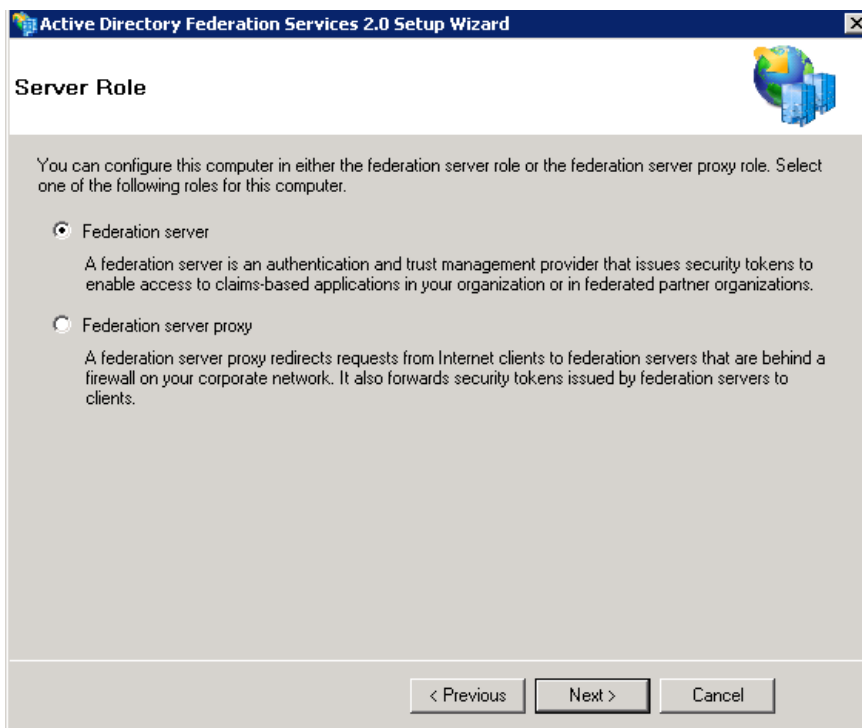


Click Next.

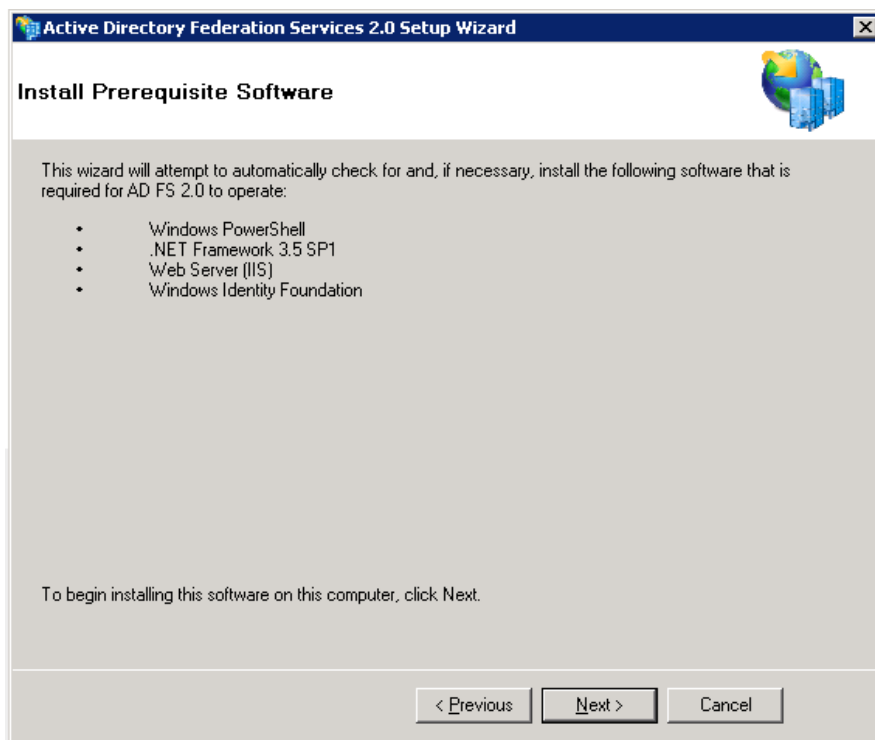
Accept Ts&Cs,



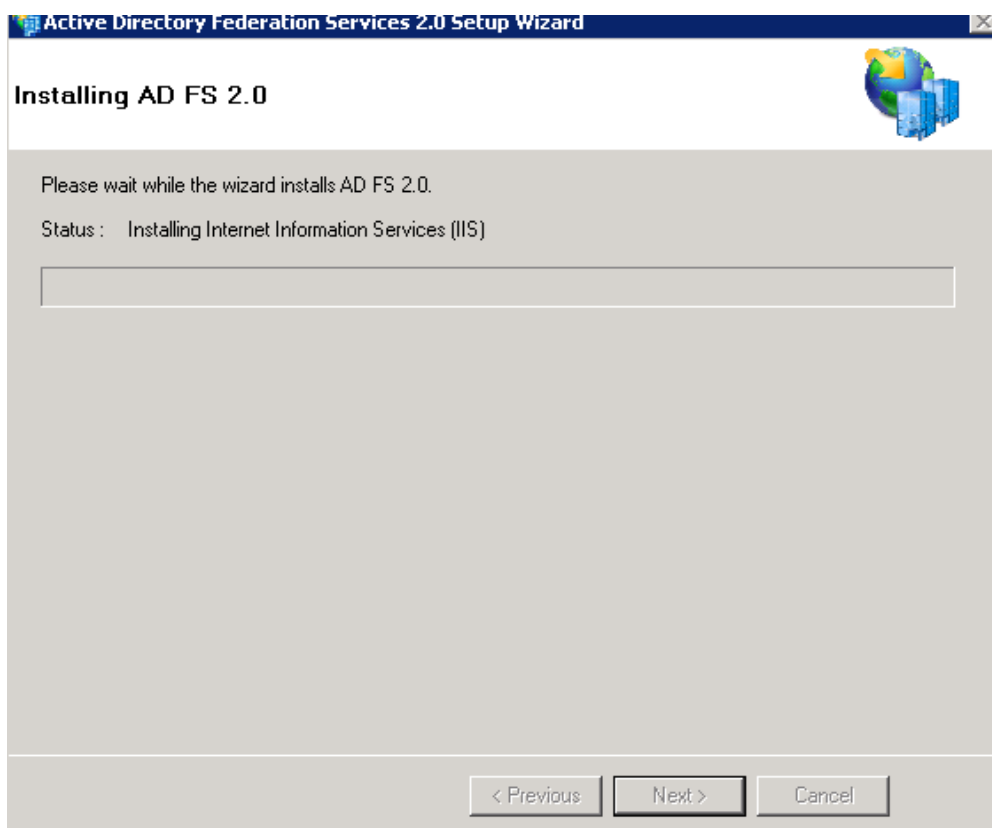
Select Federation server as below.



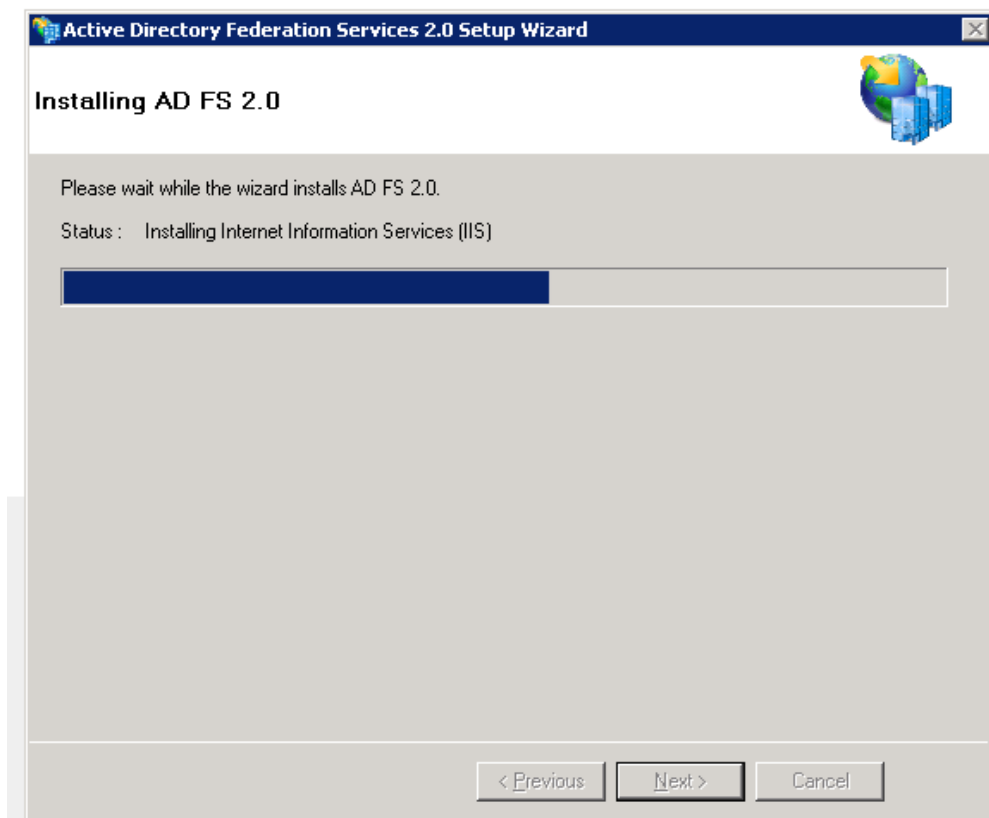
Setup will install all pre-requisites automatically, click Next.



AD FS installation will begin.



Wait for installation to finish.

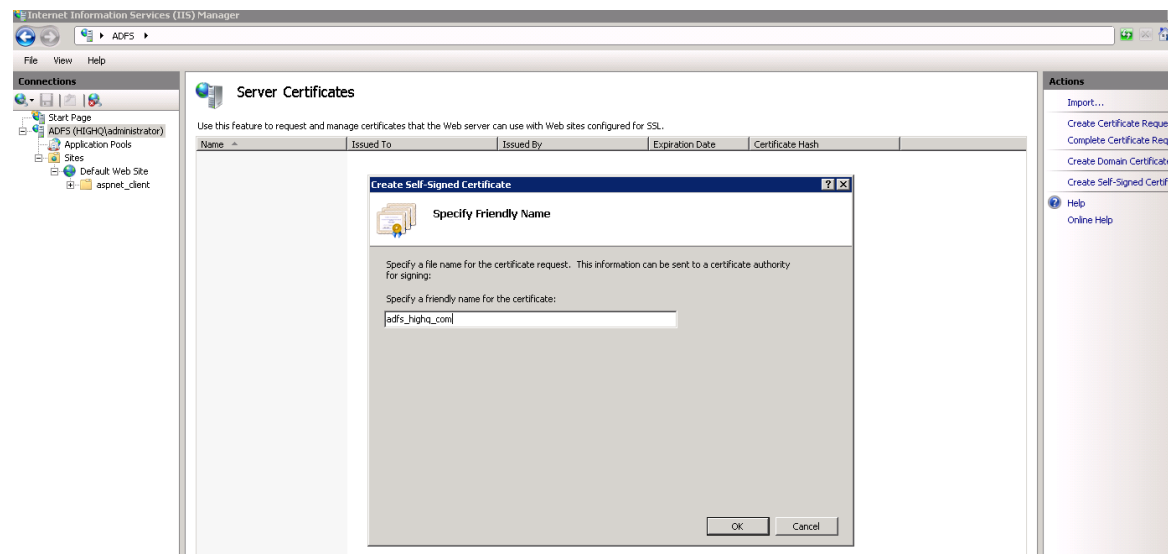


When setup is finished, click on Finish.



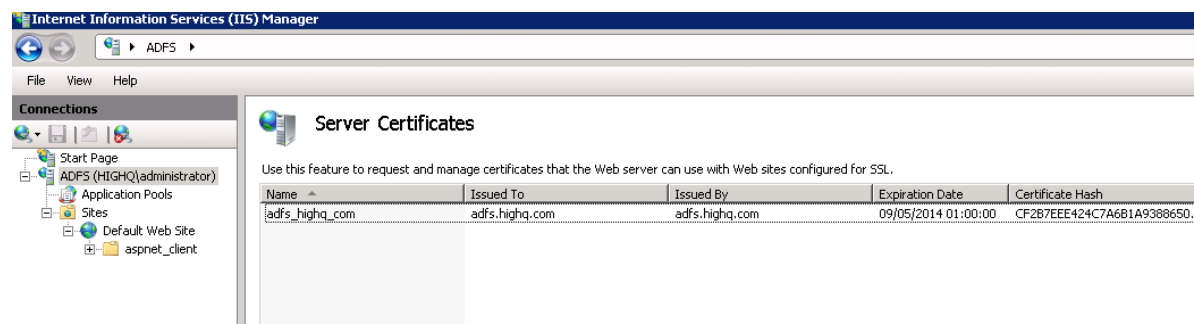
3. Configuring Relying Party on ADFS server

Open IIS Manager. Select “ADFS” in left pane and click on “Create Self-Signed Certificate” in Actions on right.

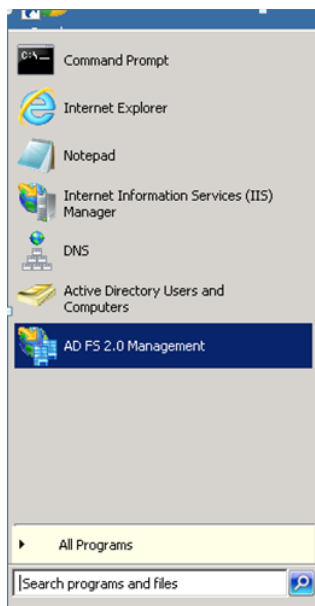


If you have purchased an SSL certificate, you can Import it from Actions in right pane.

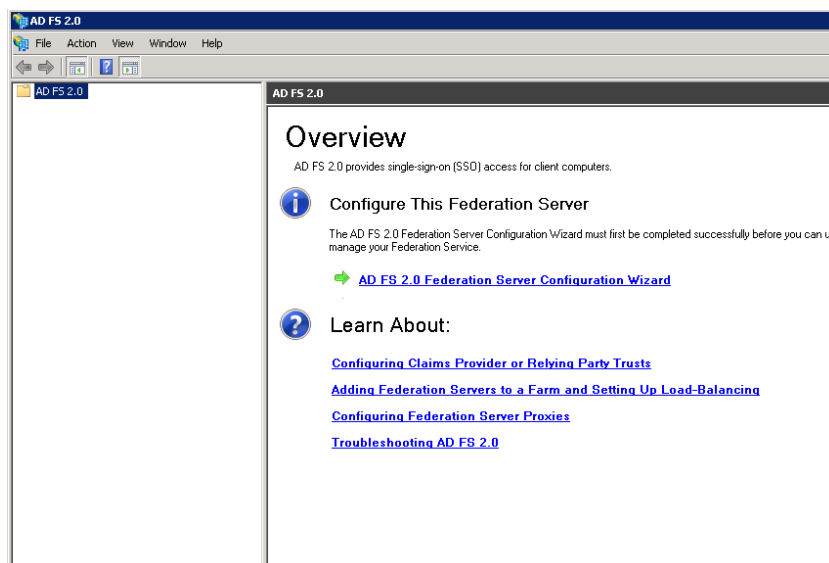
Your SSL certificate will show in Server Certificates.



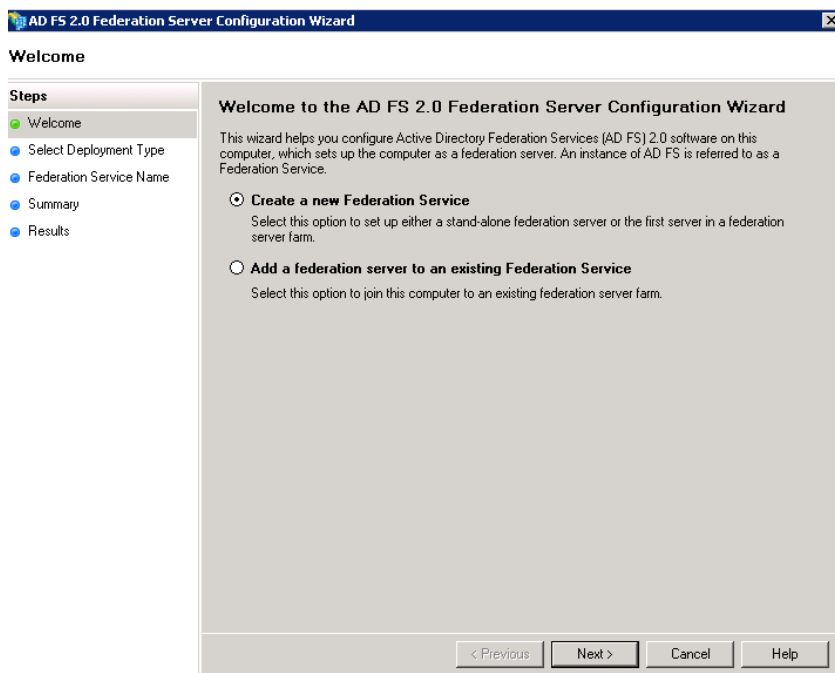
Start AD FS 2.0 Management



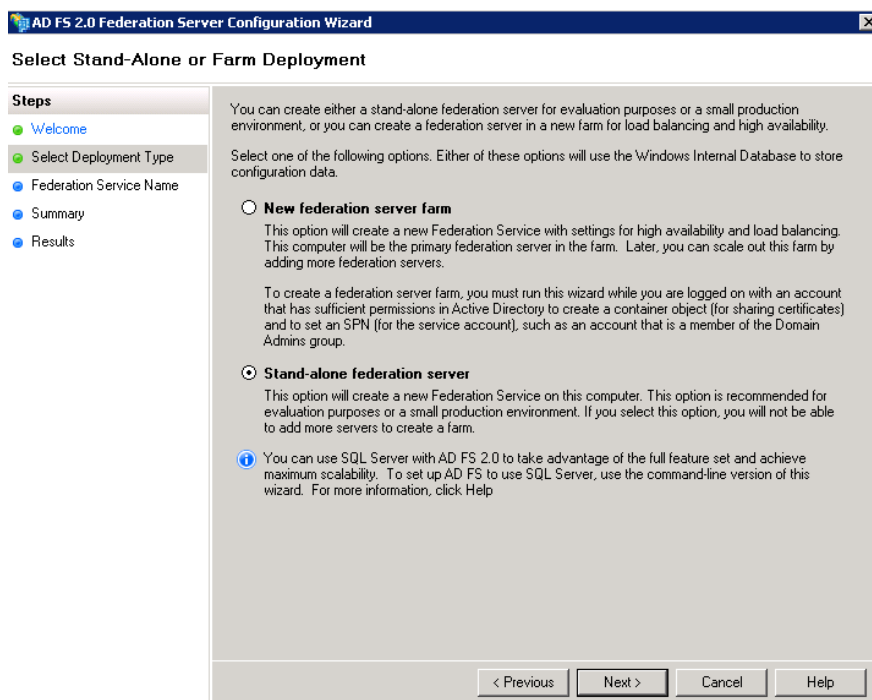
, and click on “AD FS 2.0 Federation Server Configuration Wizard”.



Select “Create a new Federation Service” and click Next.



Select “Stand-alone federation server” and click Next.



Your SSL Certificate will be selected on next screen. If you have multiple certificates setup you can select the appropriate for your ADFS FQDN. Click Next.

AD FS 2.0 Federation Server Configuration Wizard

Specify the Federation Service Name

Steps

- Welcome
- Select Deployment Type
- Federation Service Name
- Summary
- Results

This wizard determines the Federation Service name from the Subject field of the SSL certificate for the Default Web Site. If the wizard cannot determine the Federation Service name from the SSL settings, you must select a certificate.

Select the certificate and/or port, and then click Next.

SSL certificate: Port:

Federation Service name:

[What kind of certificate do I need?](#)

< Previous Next > Cancel Help

Click Next.

AD FS 2.0 Federation Server Configuration Wizard

Ready to Apply Settings

Steps

- Welcome
- Select Deployment Type
- Federation Service Name
- Summary
- Results

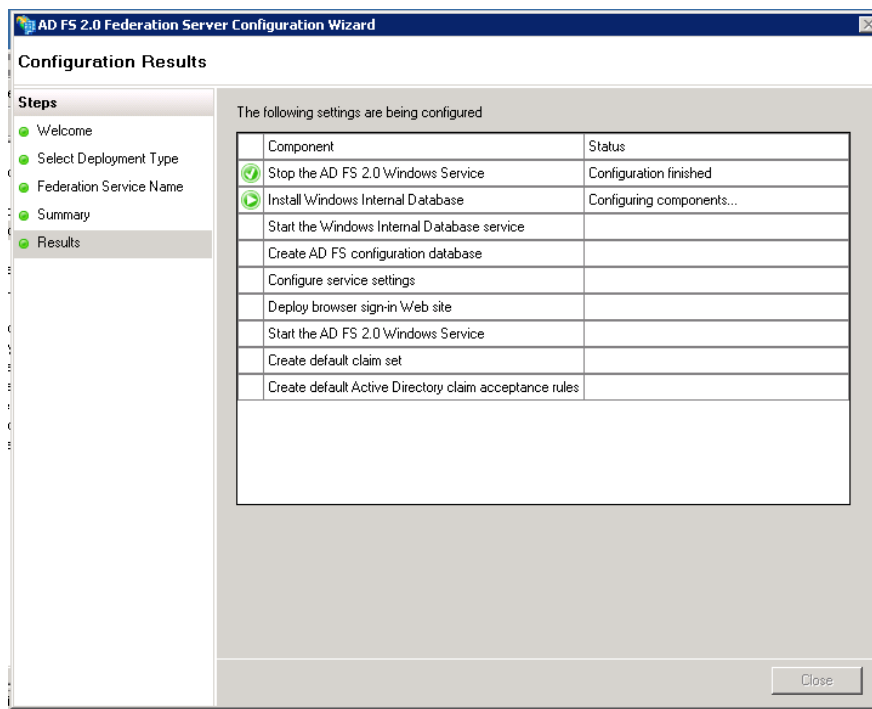
The following settings will be configured for AD FS 2.0:

- Stop AD FS server.
- Windows Internal Database service will be started and set to automatic startup.
- Signing and token-encryption certificates will be generated and set to automatic roll over.
- Selected SSL certificate will be used for securing service communication.
- Network Service account will be given access to the database, to the certificate private keys and endpoints, and the service will run under this account.
- Default set of endpoints will be enabled.
- Browser sign-in web site will be deployed to the 'adfs/ls' virtual directory under the Default Web Site in IIS.
- Federation Service name is dns2hq.highq.com
- Start AD FS server.

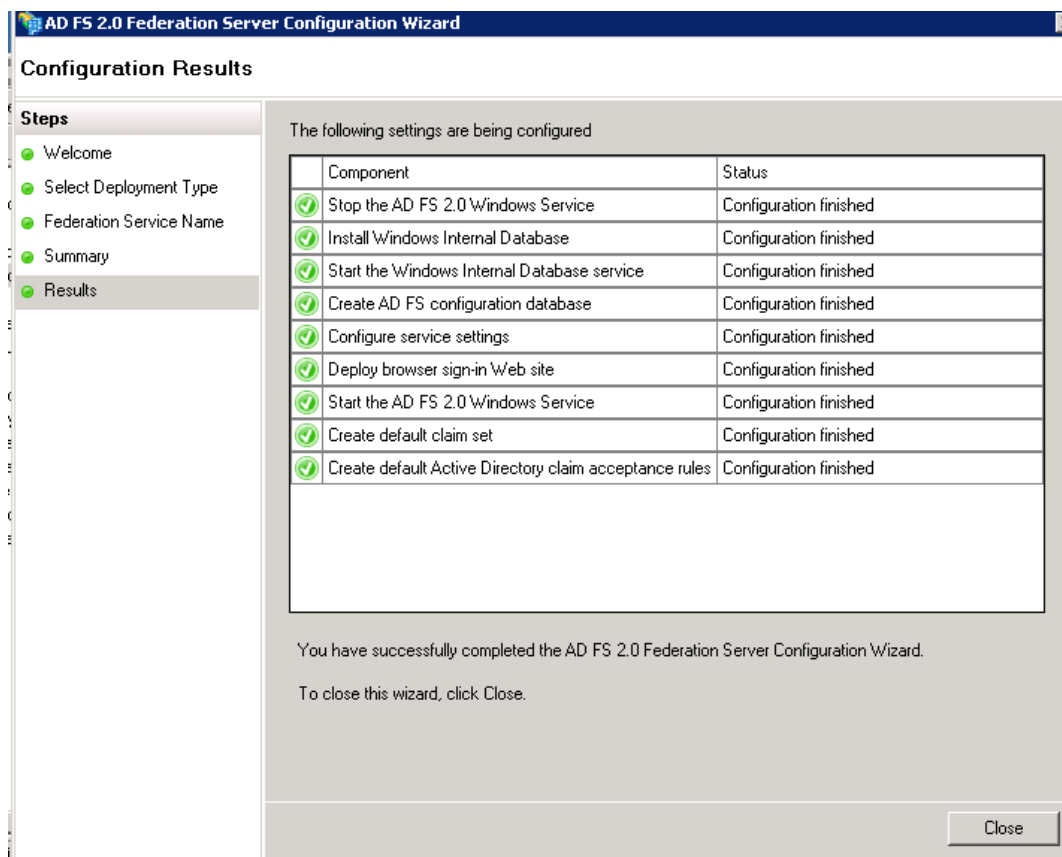
To begin configuring this computer with these settings, click Next.

< Previous Next > Cancel Help

Configuration will begin.



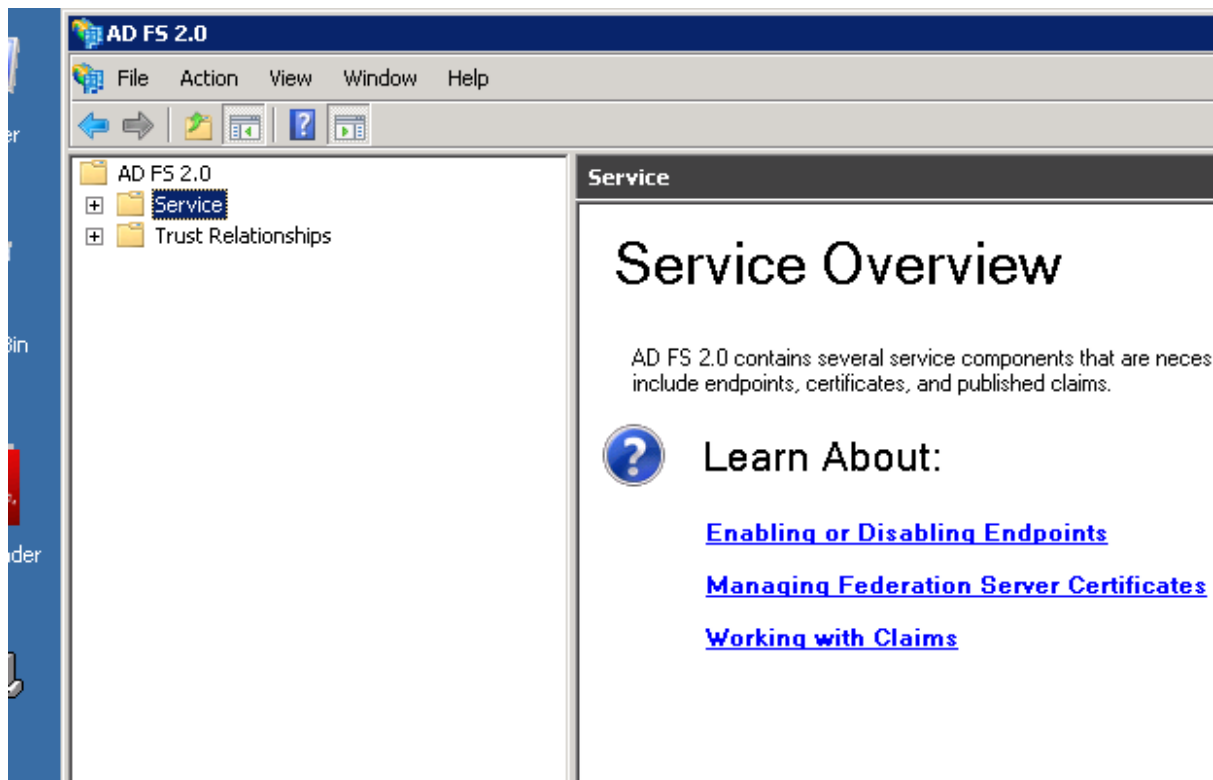
Wait for Configuration to finish.



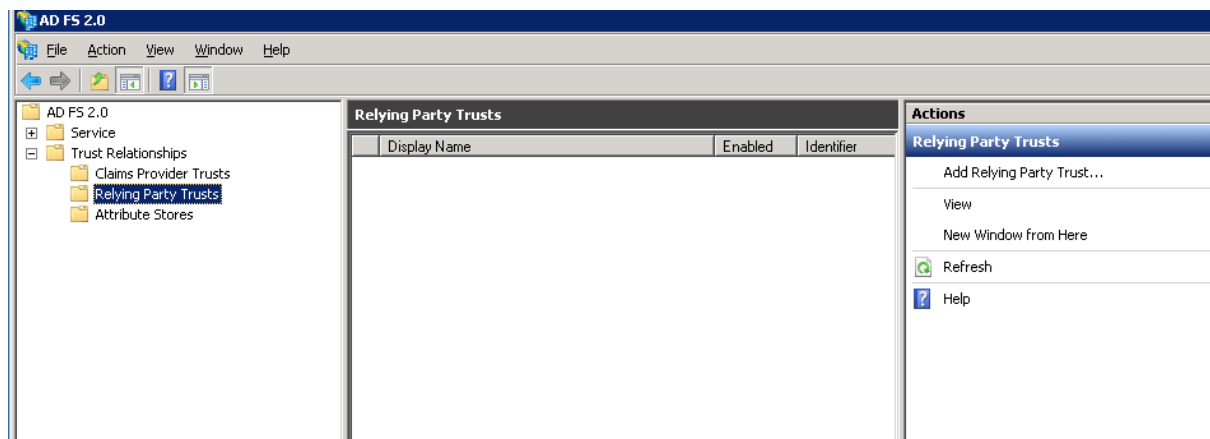
Click Close to finish ADFS installation.

4. ADFS Configuration for SSO

Open AD FS 2.0 Management.

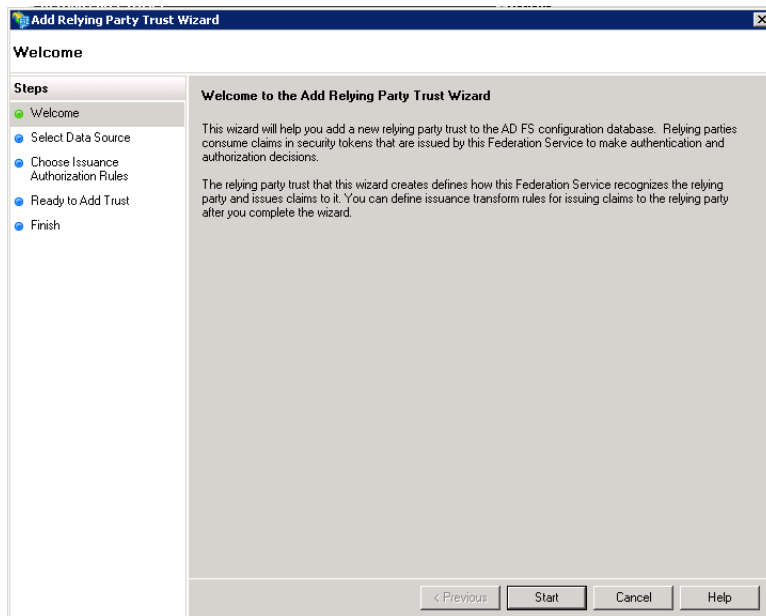


Go to Trust Relationships>>Relying Party Trusts



Click on Add Replying Party Trust in Actions on right.

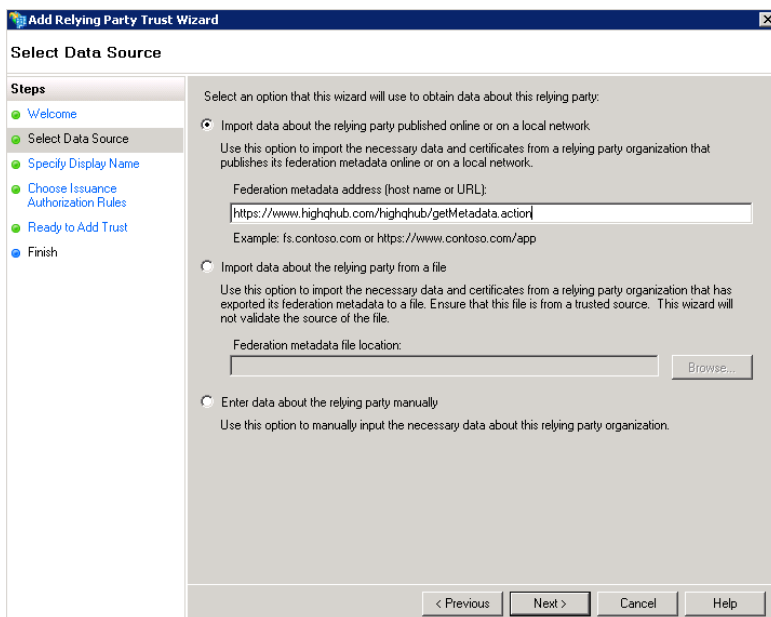
Click Next to continue



On next screen, select first option, "Import data about the relying party....."

Give URL to "Federation metadata address"

<https://highqhub.com/highqhub/getMetadata.action>



Click Next.

Enter Display name “www.highqhub.com”

The screenshot shows the 'Add Relying Party Trust Wizard' window, specifically the 'Specify Display Name' step. The 'Steps' pane on the left lists: Welcome, Select Data Source, Specify Display Name (current), Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains a text box for 'Display name:' with 'www.highqhub.com' entered. Below it is a 'Notes:' text area. At the bottom are buttons for '< Previous', 'Next >', 'Cancel', and 'Help'.

On next screen select “Permit all users to access this relying party”.

The screenshot shows the 'Add Relying Party Trust Wizard' window, specifically the 'Choose Issuance Authorization Rules' step. The 'Steps' pane on the left lists: Welcome, Select Data Source, Specify Display Name, Choose Issuance Authorization Rules (current), Ready to Add Trust, and Finish. The main area has a heading 'Choose Issuance Authorization Rules' and explains that these rules determine whether a user is permitted to receive claims. It offers two options: 'Permit all users to access this relying party' (selected) and 'Deny all users access to this relying party'. Below the options is a note: '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.' At the bottom are buttons for '< Previous', 'Next >', 'Cancel', and 'Help'.

Click Next.

Add Relying Party Trust Wizard

Ready to Add Trust

Steps

- Welcome
- Select Data Source
- Specify Display Name
- 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.

Monitoring | Identifiers | Encryption | Signature | Accepted Claims | Organization | Endpoints | **N** | >

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:
 08/05/2013

This relying party was last updated from federation metadata on:
 08/05/2013

< Previous **Next >** Cancel Help

Click on close.

Add Relying Party Trust Wizard

Finish

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish**

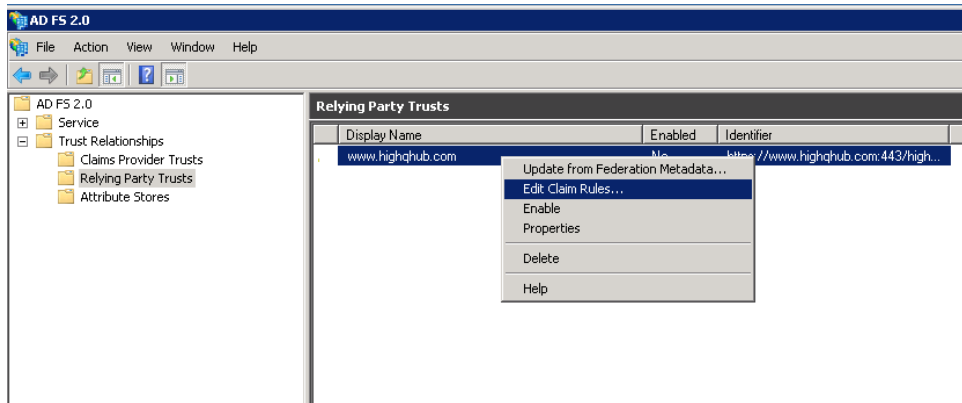
The relying party trust was successfully added to the AD FS configuration database.

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

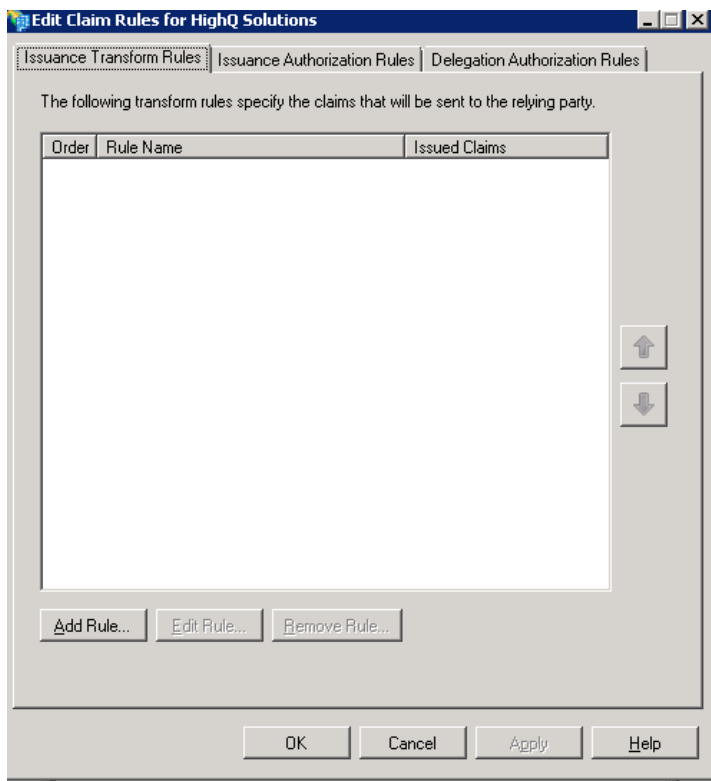
☒ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes

Close

Go to Relying Party Trusts, right click on Display Name www.highqhub.com and Edit Claim Rules



Click "Add Rule" button, will get Select Rule Template window.



Select "Send LDAP Attributes as Claims" from "Claim rule template" drop down, and click Next.

Add Transform 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:

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...](#)

< Previous Next > Cancel Help

On next screen,

- give claim rule name in "Claim rule name:" textbox.
- select "Active directory" from "Attribute store:" dropdown.
- select the value for "Mapping of LDAP attributes to outgoing claim types:"
- select "E-mail-addresses" from "LDAP Attribute" and write "mail" in "Outgoing Claim Type".
- click Finish and Apply.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

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:

Rule1

Rule template: Send LDAP Attributes as Claims

Attribute store:

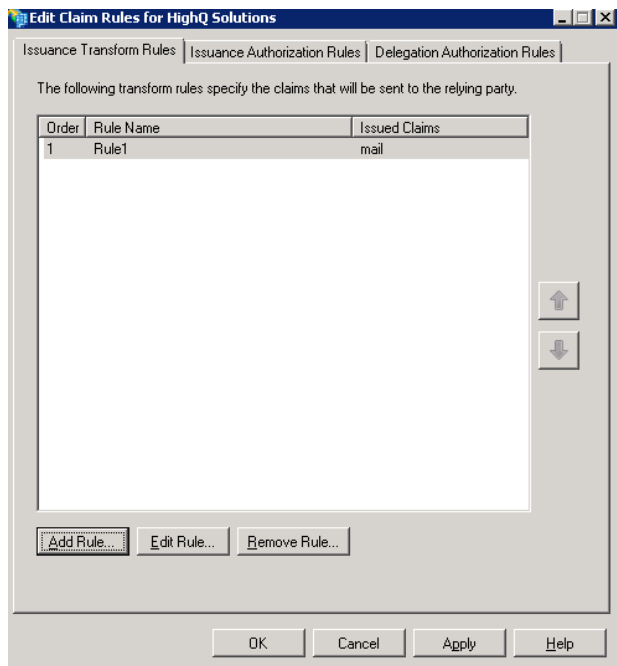
Active Directory

Mapping of LDAP attributes to outgoing claim types:

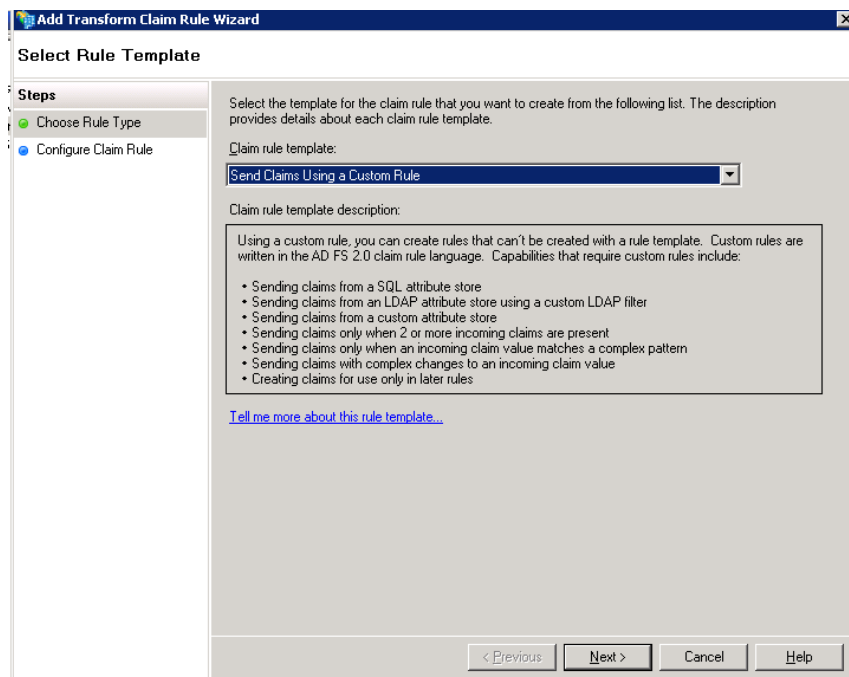
LDAP Attribute	Outgoing Claim Type
E-Mail-Addresses	mail
▶*	

< Previous Finish Cancel Help

Again click on “Add Rule”



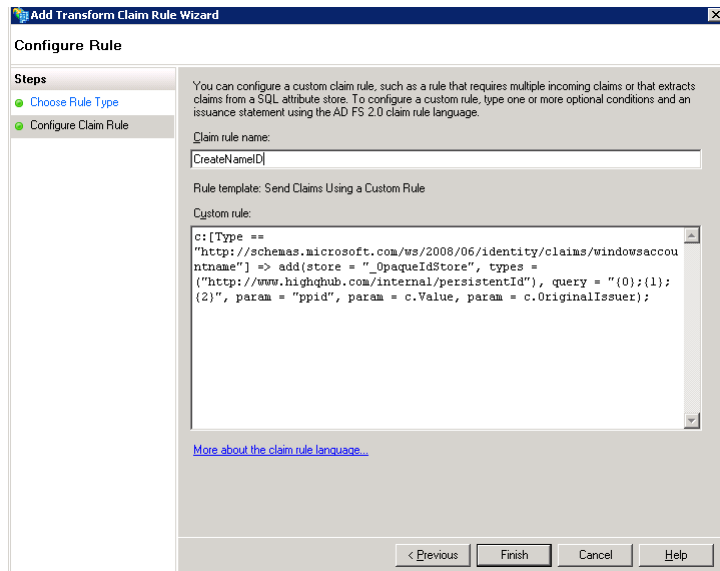
Select "Send Claims Using a Custom Rule" from "Claim rule template" drop down. and click Next.



-- give claim rule name as "CreateNameID" in "Claim rule name:" textbox.
 -- copy and add below code in Custom rule box:

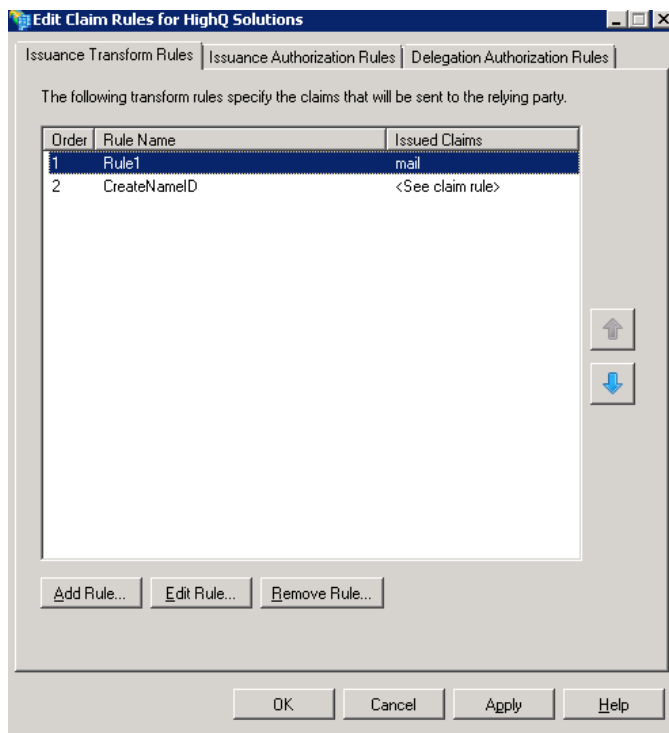
```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
=> add(store = "_OpaqueIdStore", types = ("http://www.highqhub.com/internal/persistentId"), query =
"{0};{1};{2}", param = "ppid", param = c.Value, param = c.OriginalIssuer);
```

-- Please note that the spacing is very important and has to be exactly right otherwise it will simply not work. The below image is what it should look like exactly.

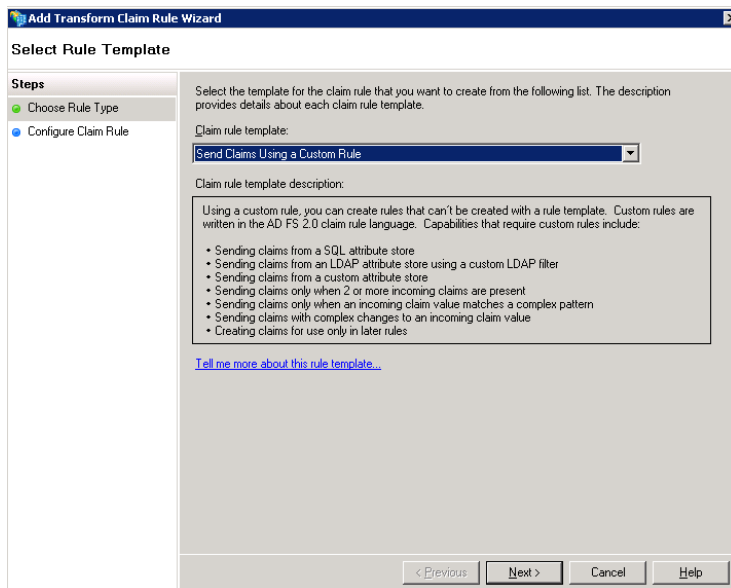


Click on Finish.

For third rule, click "Add Rule" button.



-- select "Send Claims Using a Custom Rule" from "Claim rule template" drop down. and click Next.



-- give claim rule name as "Issue Name ID" in "Claim rule name:" textbox.
 -- copy and add below code in Custom rule box:

```
c:[Type == "http://www.highqhub.com/internal/persistentId"]
```

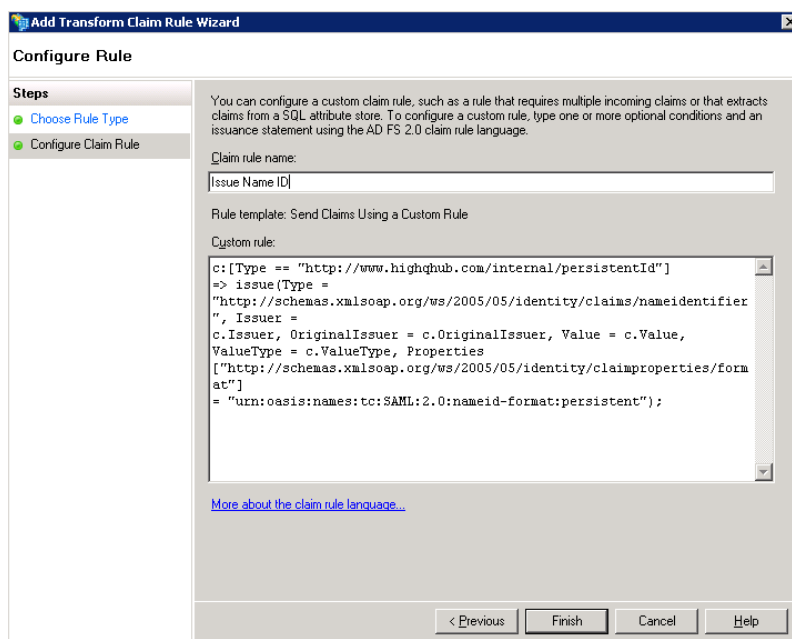
```
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer =  

c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,  

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =  

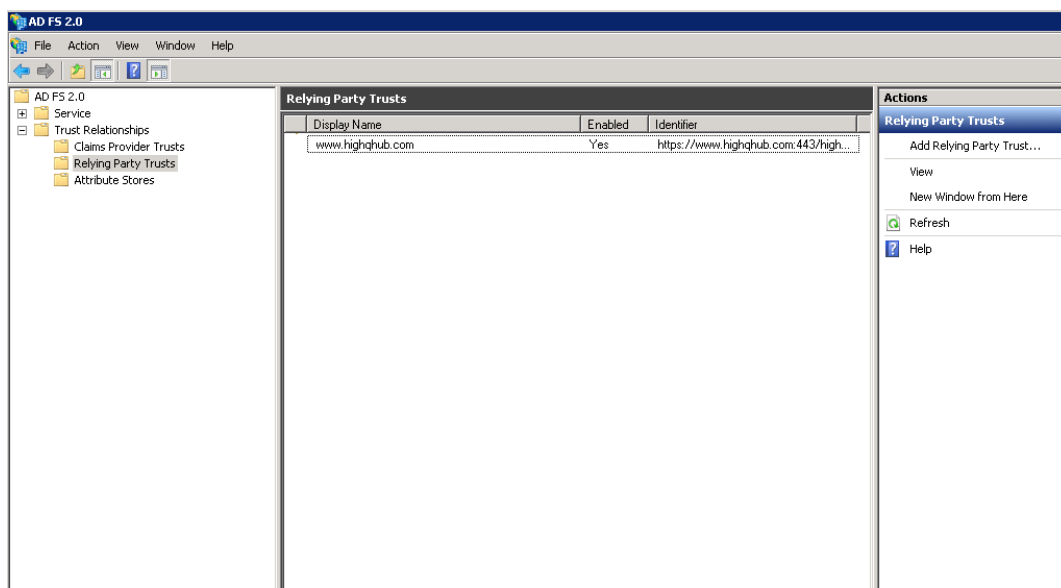
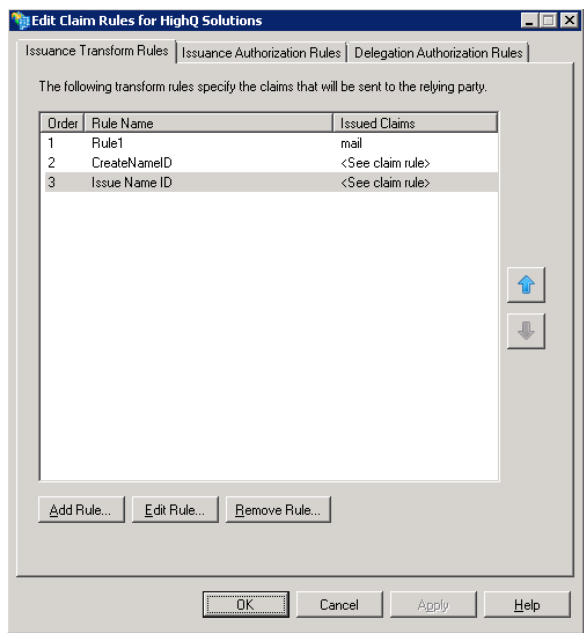
"urn:oasis:names:tc:SAML:2.0:nameid-format:persistent");
```

-- Please note that the spacing is very important and has to be exactly right otherwise it will simply not work. The below image is what it should look like exactly.



Click Finish.

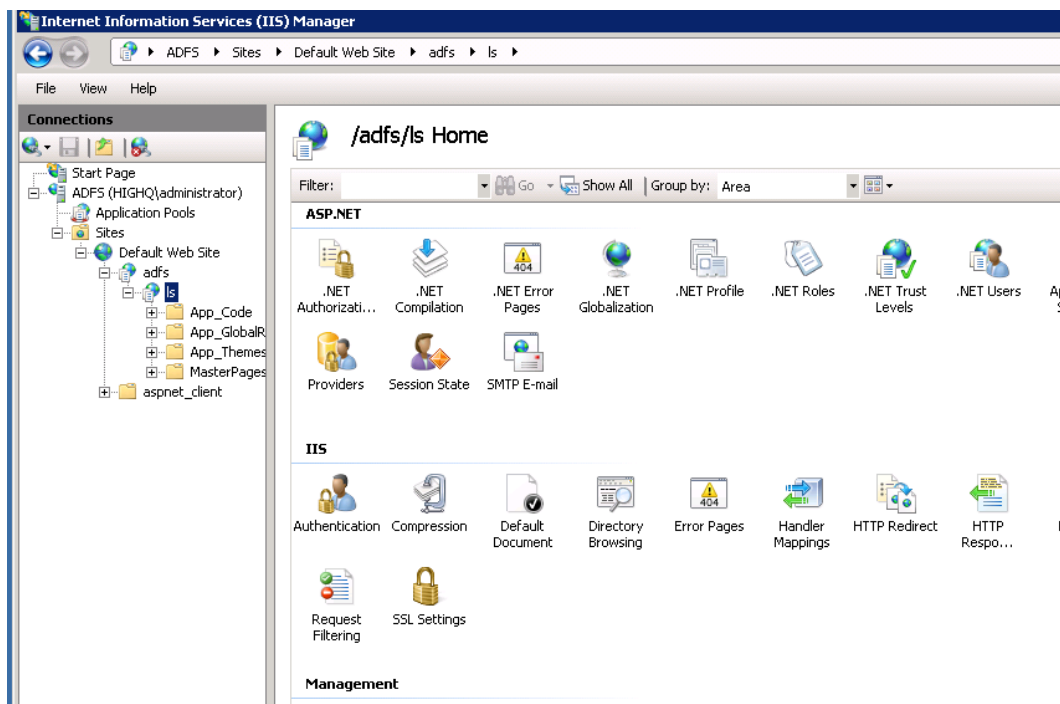
Apply and Click OK.



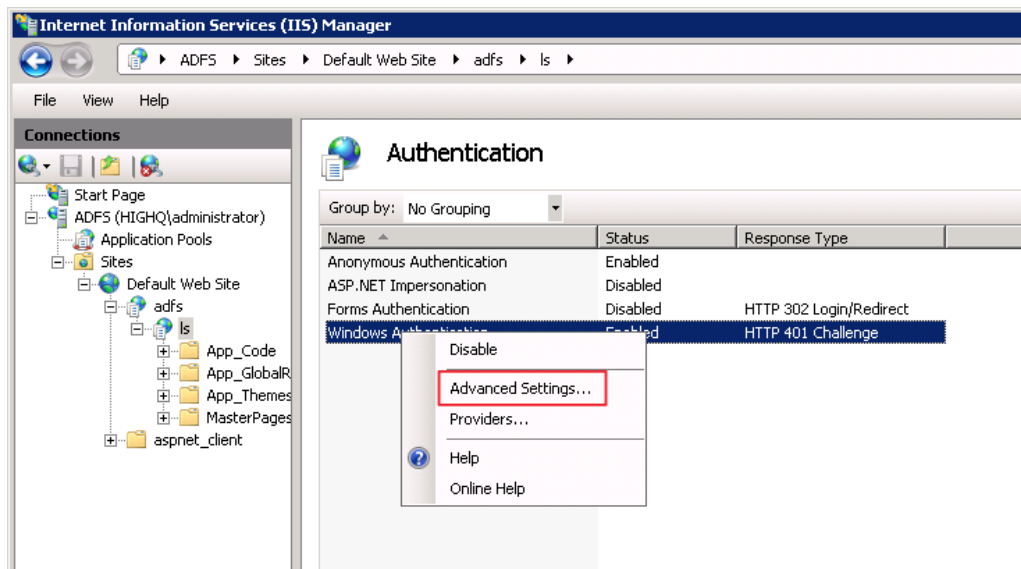
5. Other info

5.1 To get the SSO working with non-IE browsers, following must be done in IIS on ADFS server.

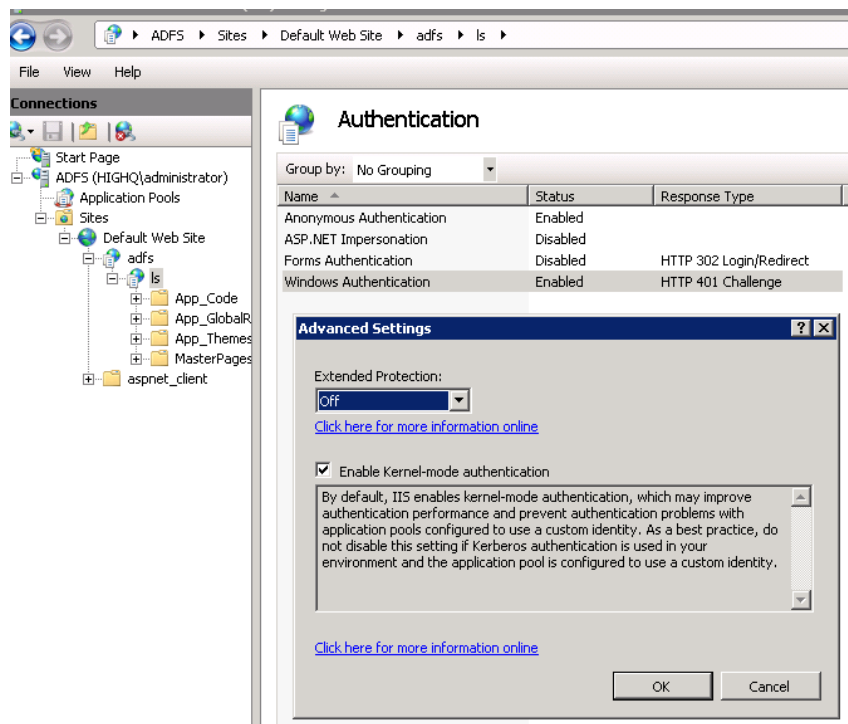
Go to IIS Manager>>Default Web Site>>adfs>>ls - double click on "Authentication under IIS heading.



Right click on Windows Authentication and click on "Advanced Settings".



Set “Extended Protection” to **Off**.



Click OK.

5.2 Firewall

Inbound HTTPS access should be open for AD FS server so that HighQ hub can access the AD FS server Meta data using URL above.

5.3 Send meta detail to HighQ for Integration:

HighQ will need to know the FQDN of AD FS server e.g. in this example it is “adfs.highq.com”.

The URL below must be accessible over HTTPS from our HighQ Hub’s IP addresses 213.212.88.196 and 213.212.110.80. Please configure your Firewall to allow this access.

<https://adfs.highq.com/FederationMetadata/2007-06/FederationMetadata.xml>

Replace the “adfs.highq.com” highlighted in red with the DNS address of your AD FS Server and Send this URL to HighQ to configure in HighQ hub for SSO integration.

5.4 Local DNS address of AD FS Server

Make sure “adfs.highq.com” (the DNS address of your AD FS Server) points to local IP address of you AD FS server on you network.

5.5 Domain Controller and AD FS Server on separate machines.

You can have Domain Controller and AD FS on two different server machines.

5.6 Firewall access between Domain Controller and ADFS Servers.

If your Domain Controller is in Inside zone and AD FS Server in DMZ, then between these two servers you will need to allow everything to flow in both directions.

5.7 SSL Certificate

You can either issue a self-signed SSL certificate yourself or purchase it, your choice.

5.8 Certification Authority Access

ADFS server required HTTP (TCP 80) access outbound to SSL provider's certification revocation servers.

All outbound HTTP access from ADFS server to Internet should be opened on firewall.

6. Information to send to HighQ

Send the following information to send to HighQ.

- 1) **Complete list of your Internet facing IP addresses.** We need to add these to relevant IDP discovery rule in HighQ Hub. It may be the IP addresses of your internet Gateway(s) or proxy server(s) which internal users use to access the internet. Please provide list of all outbound fixed public IP addresses which you use to access internet.
- 2) **FQDN of AD FS server.** It will be like "adfs.highq.com". Please ensure external DNS and your Firewall are configured for this URL to be accessible from outside internet using HTTPS.
- 3) **Email domain which can perform SSO.**