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

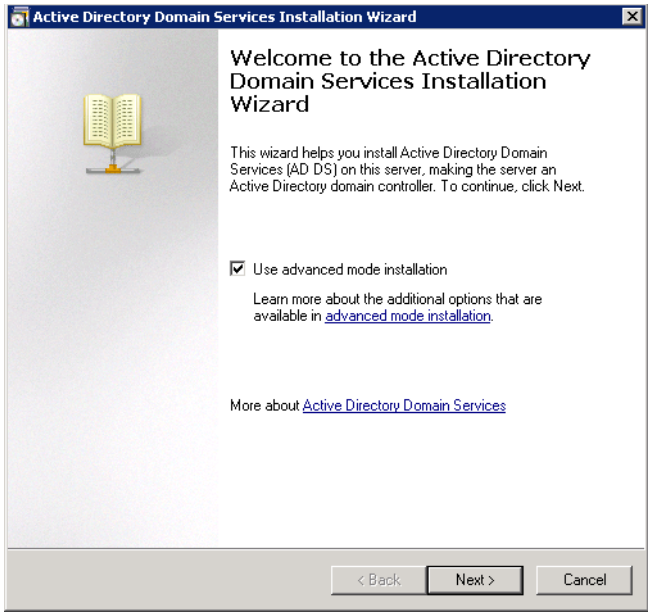
If you already have a Domain Controller setup in your network you can skip first part and start from

First of all an Active Directory Domain must be installed.

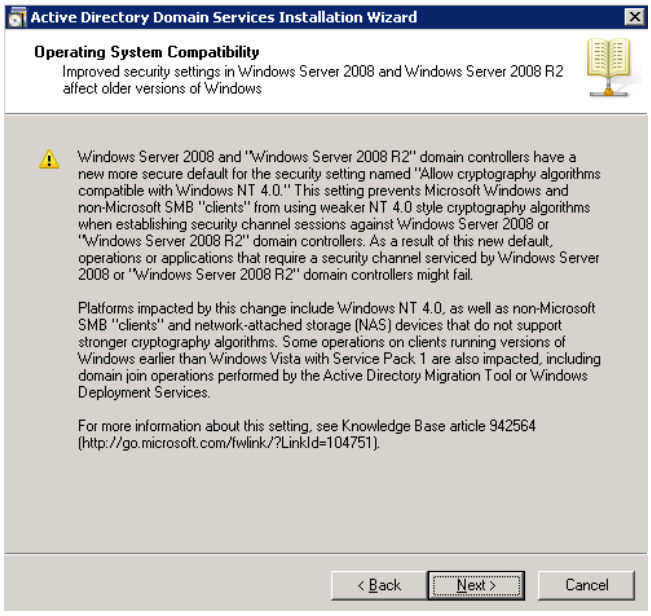
Here is a step-by-step guide how to setup new Active Directory Domain if you don't already have one. In this example, we setup an AD Domain highq.com.

This document is based on a Windows Server 2008 R2.

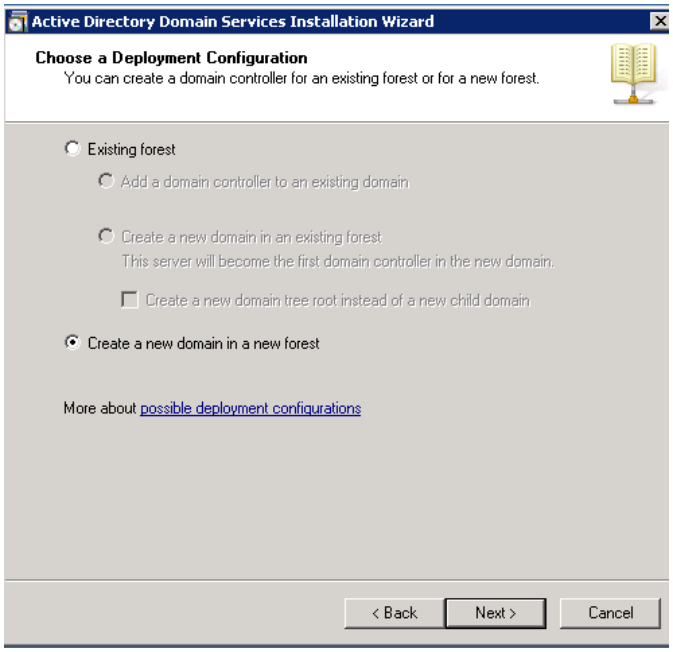
From run prompt, run "dcpromo" to setup domain and follow the setup Wizard.



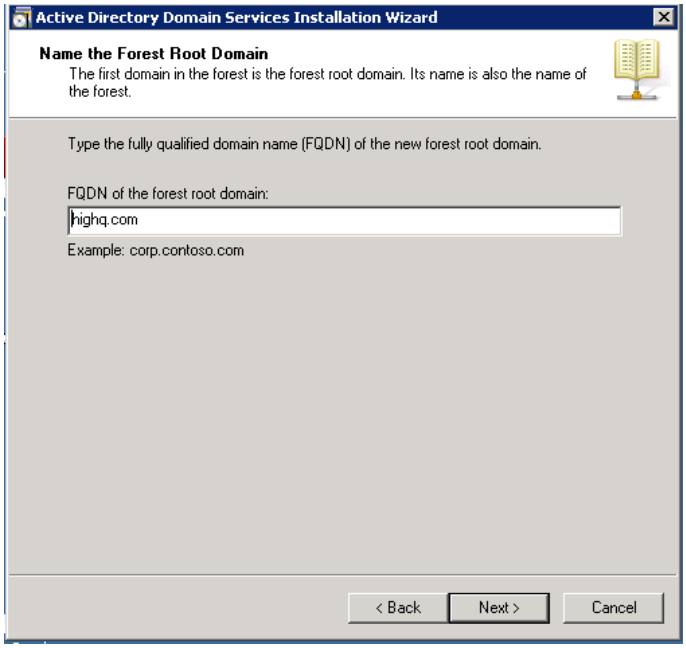
Select advanced mode installation.



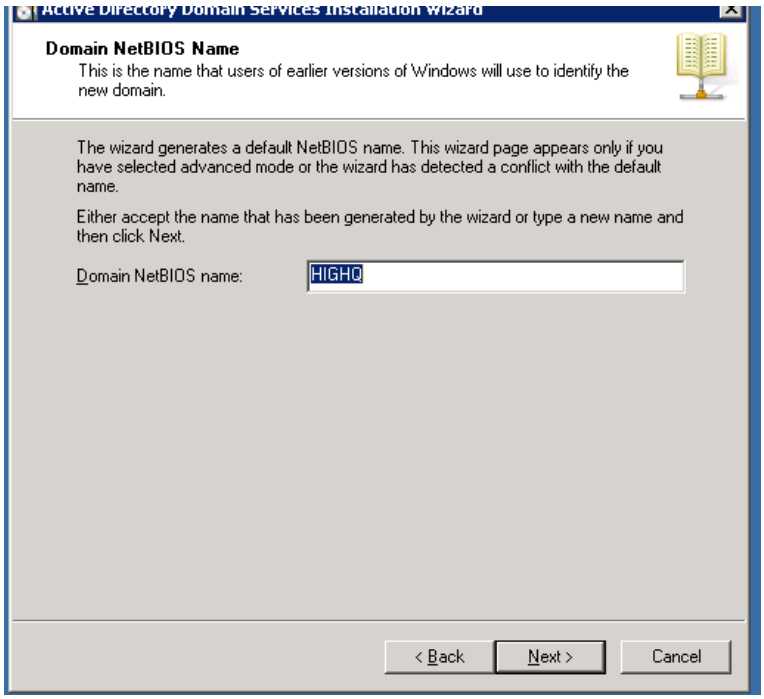
Click Next.



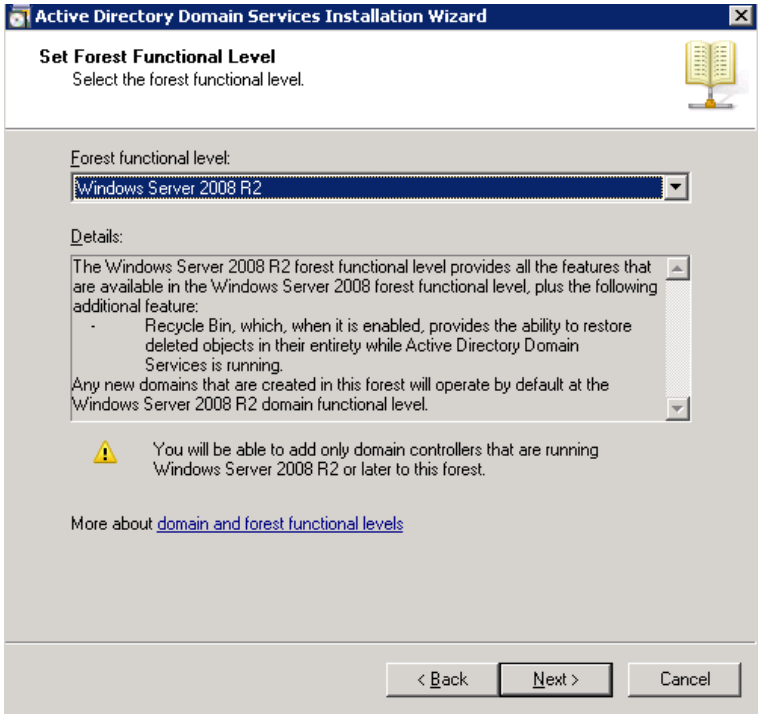
In this example we are creating a new domain, so “Create a new domain in a new forest” is selected.



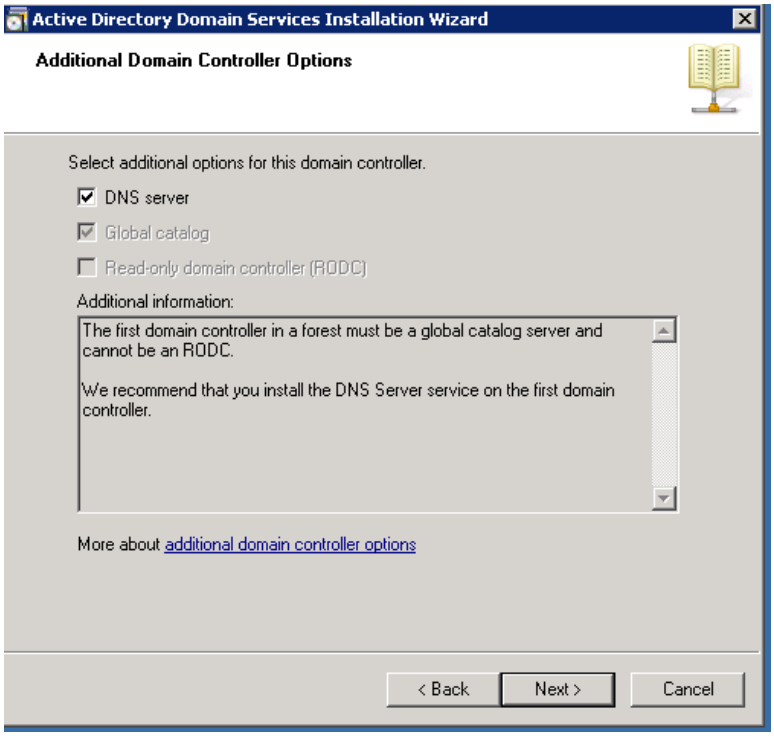
Enter the Fully Qualified Domain Name of the forest root domain; here it is “highq.com”



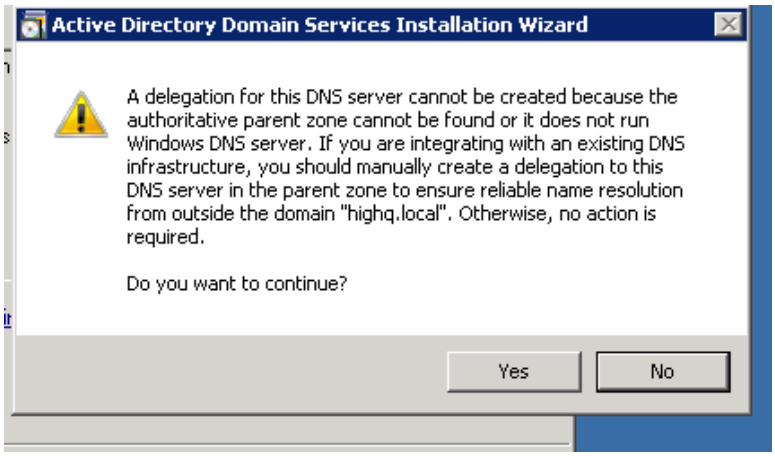
Leave as default “HIGHQ”.



Forest functional level selected as “Windows Server 2008 R2”



Select DNS Server to install DNS on same machine.

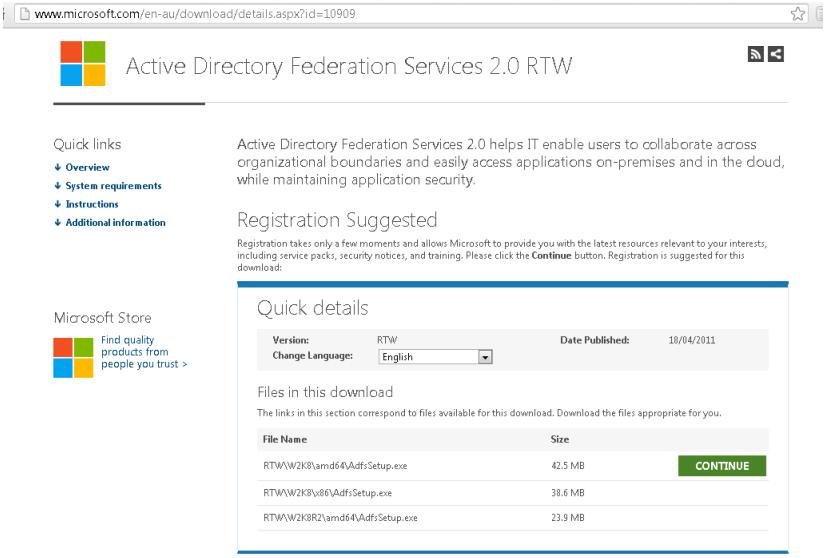


If you see warning above, ignore it.

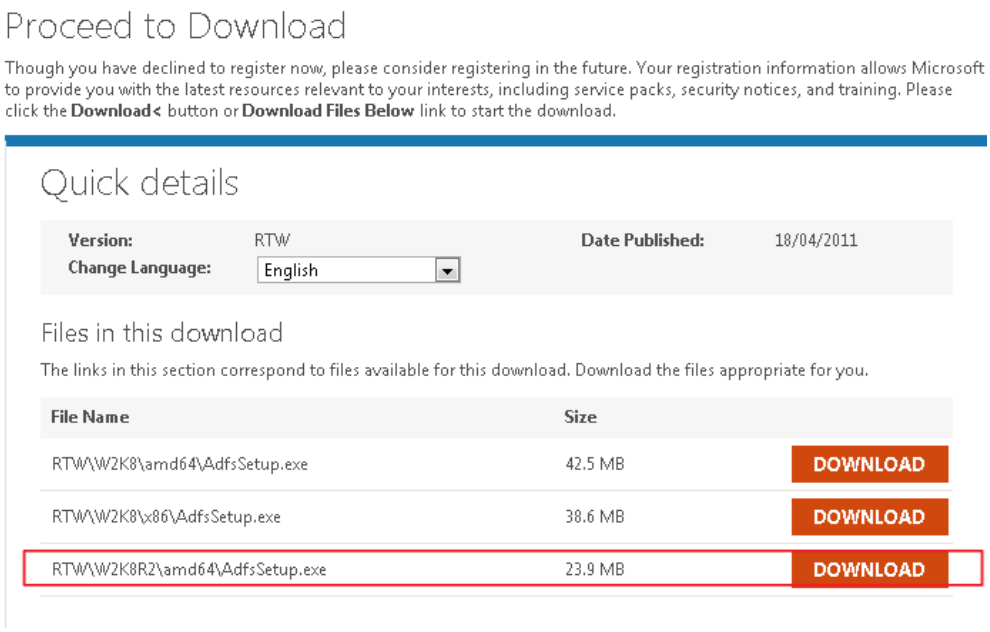
Finish and restart server.

2. ADFS Installation

Download ADFS 2.0 from link below.
http://www.microsoft.com/en-au/download/details.aspx?id=10909

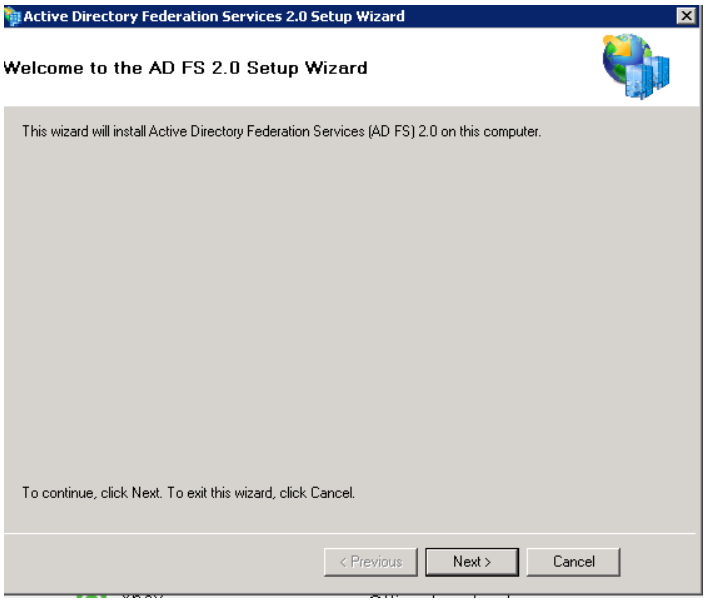


For Win2k8 R2 64bit download direct link is,
http://download.microsoft.com/download/F/3/D/F3D66A7E-C974-4A60-B7A5-382A61EB7BC6/RTW/W2K8R2/amd64/AdfsSetup.exe



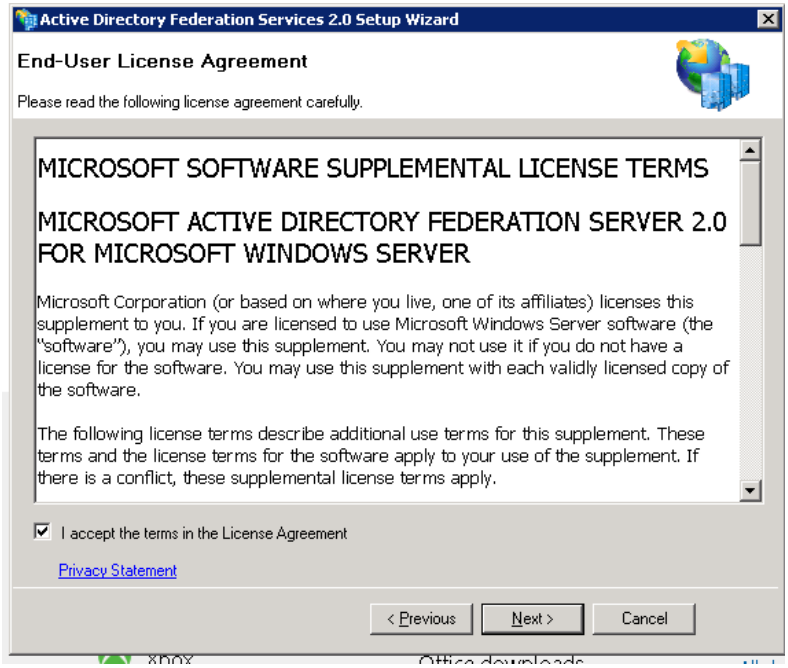
Run the setup "**AdfsSetup.exe**"

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

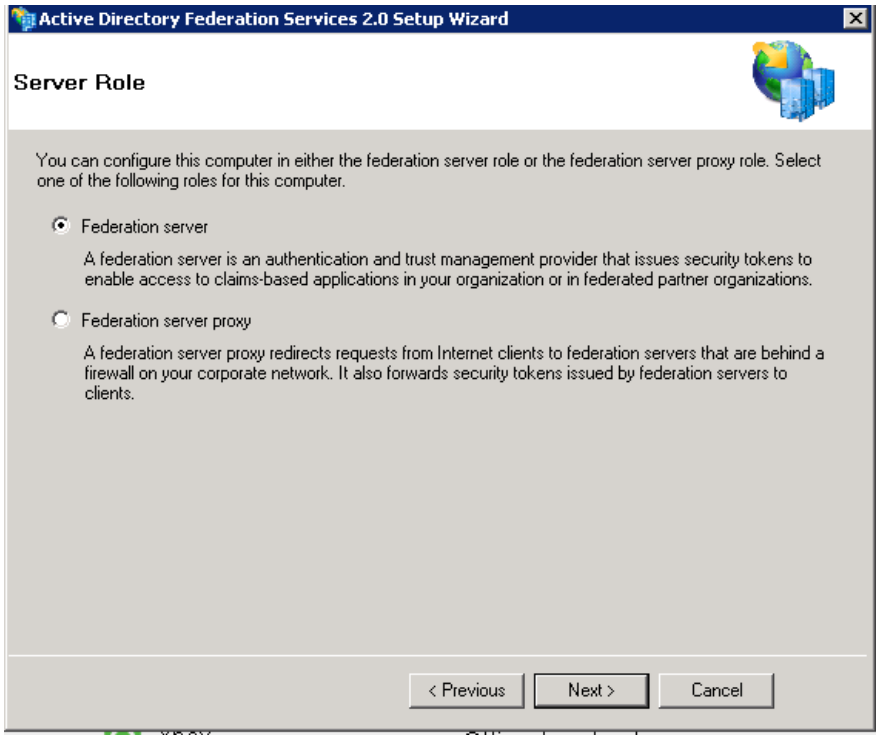


Click Next.

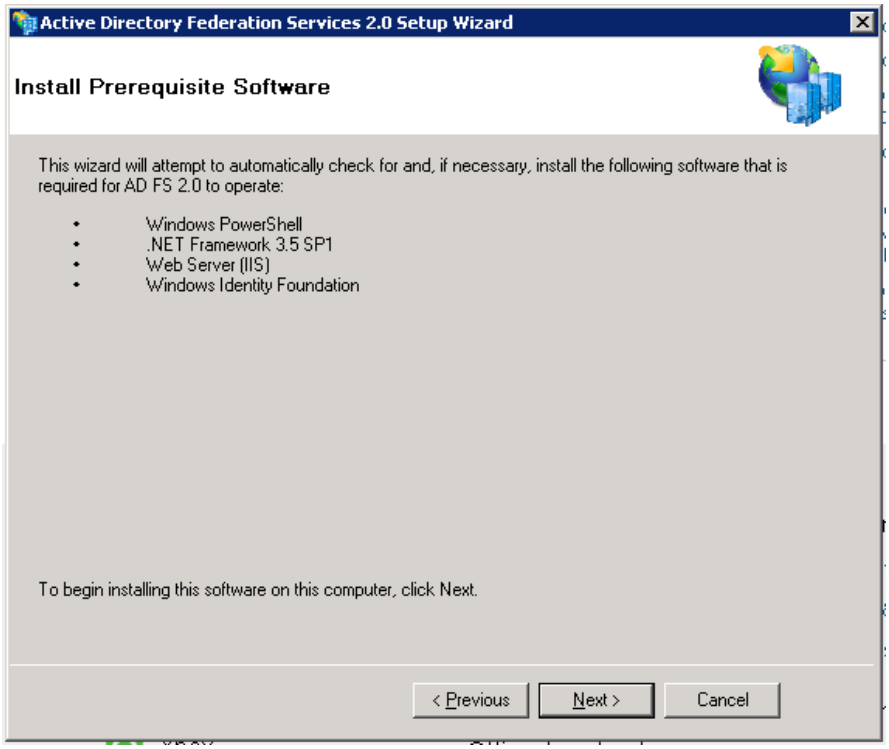
Accept Ts&Cs,



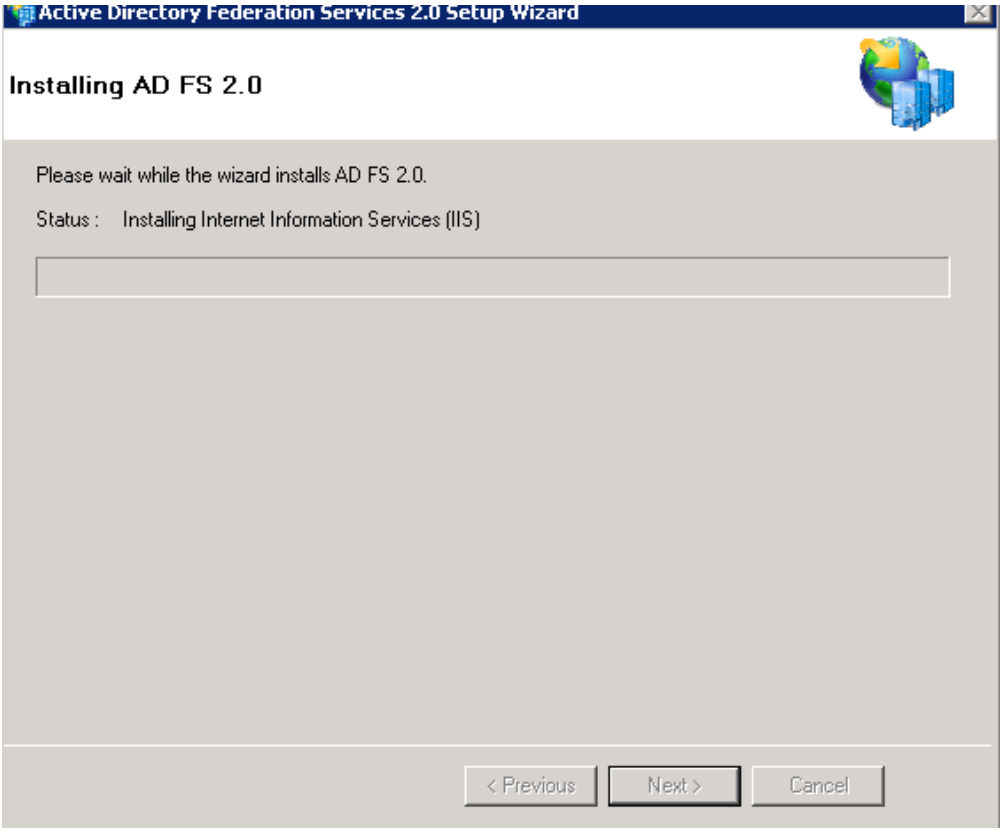
Select Federation server as below.



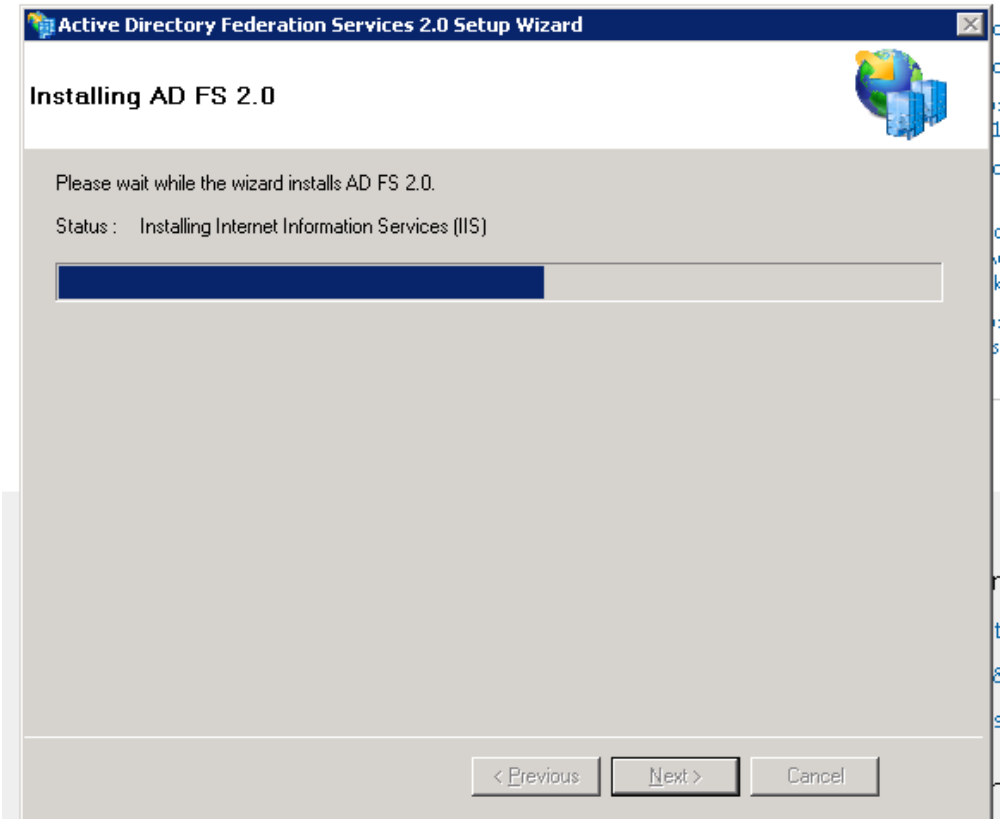
Setup will install all pre-requisites automatically, click Next.



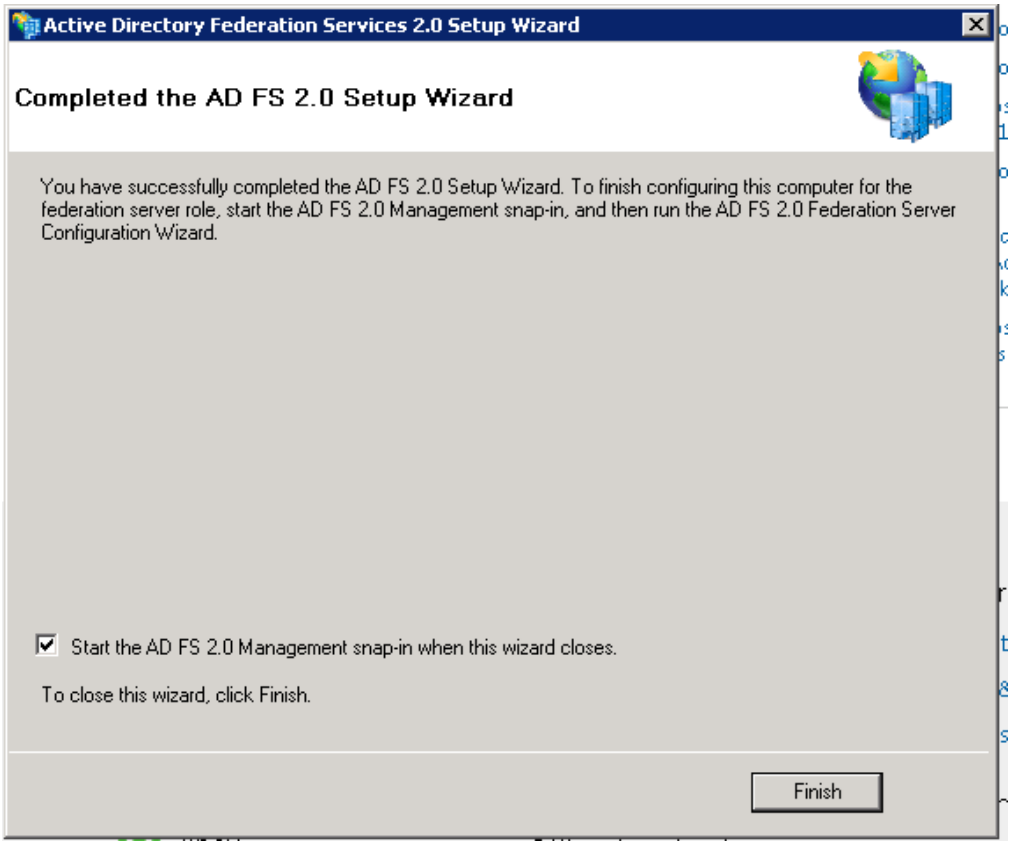
AD FS installation will begin.



Wait for installation to finish.

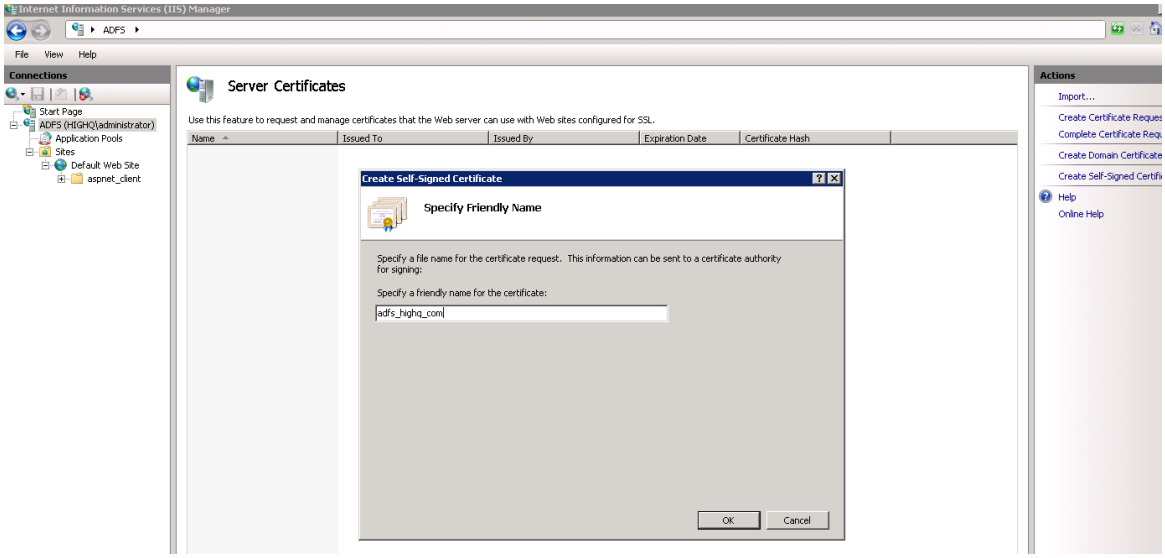


When setup is finished, click on Finish.



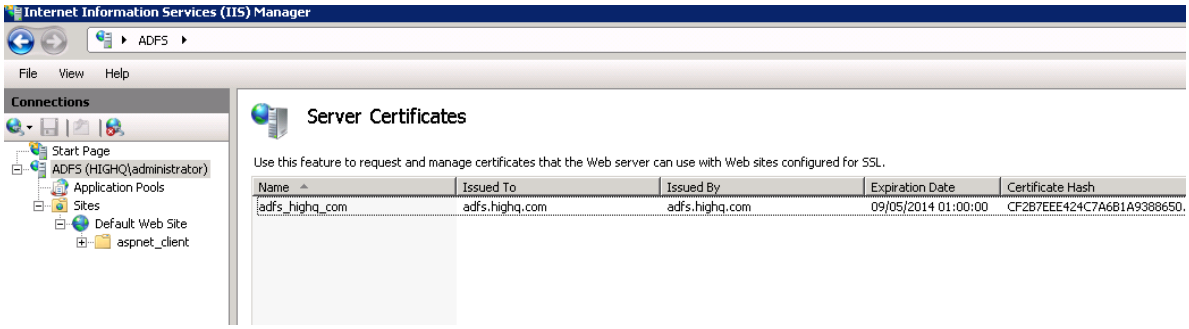
3. Configuring Relying Party on ADFS server

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

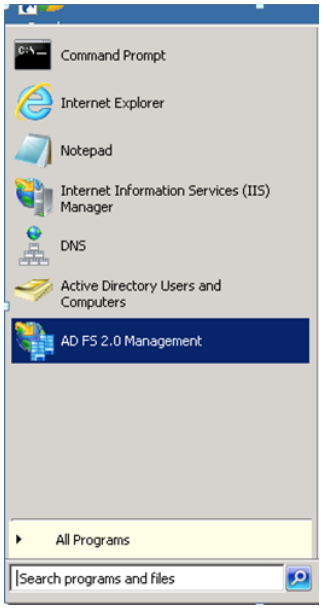


If you have purchased an SSL certificate, you can Import it from Actions in right pane.

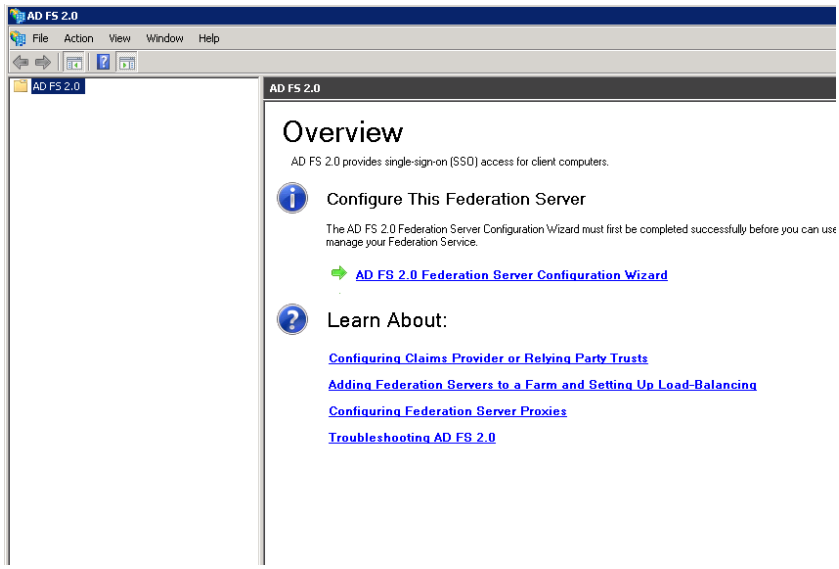
Your SSL certificate will show in Server Certificates.



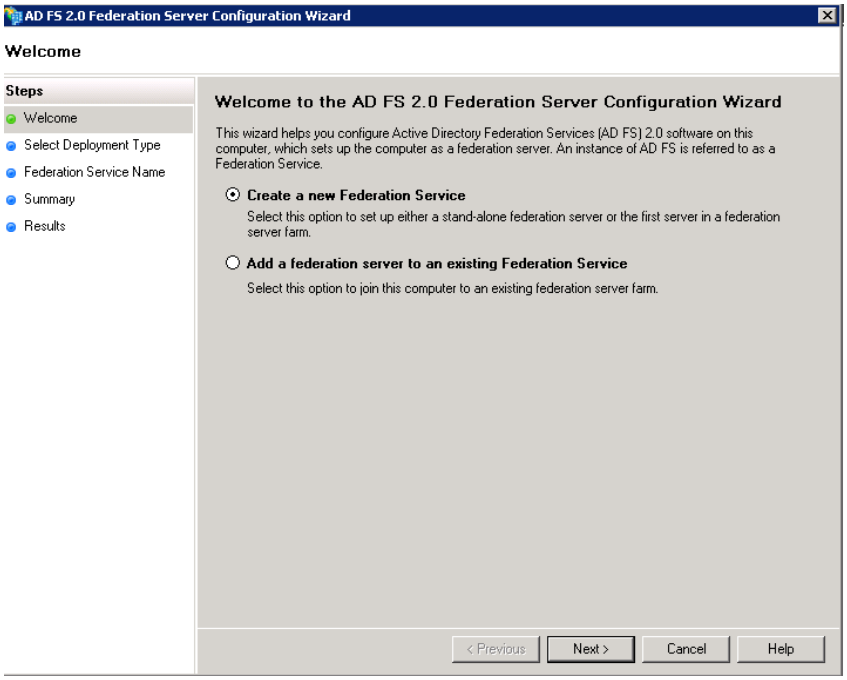
Start AD FS 2.0 Management



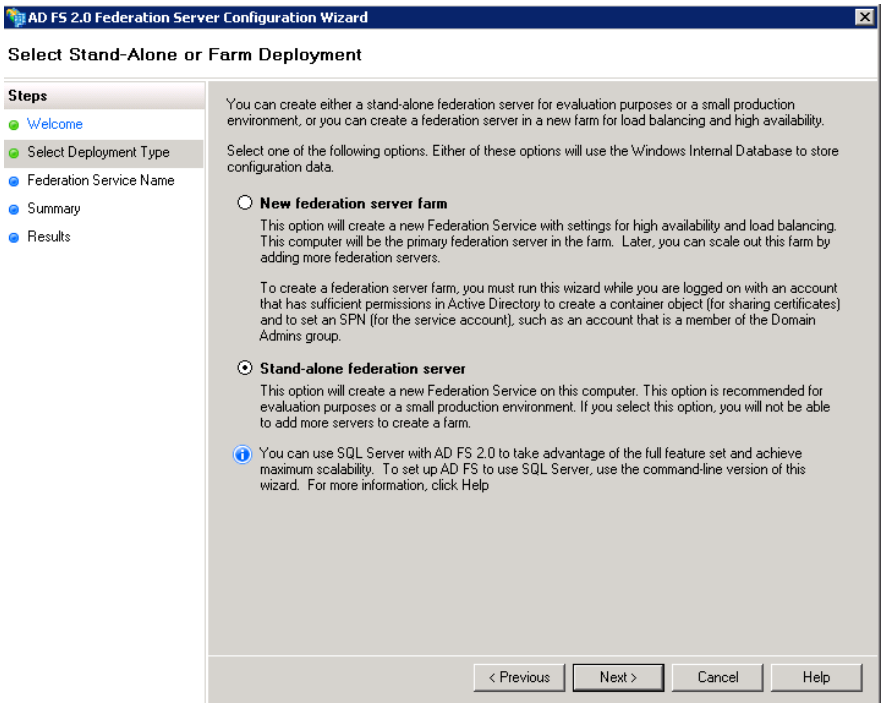
, and click on “AD FS 2.0 Federation Server Configuration Wizard”.



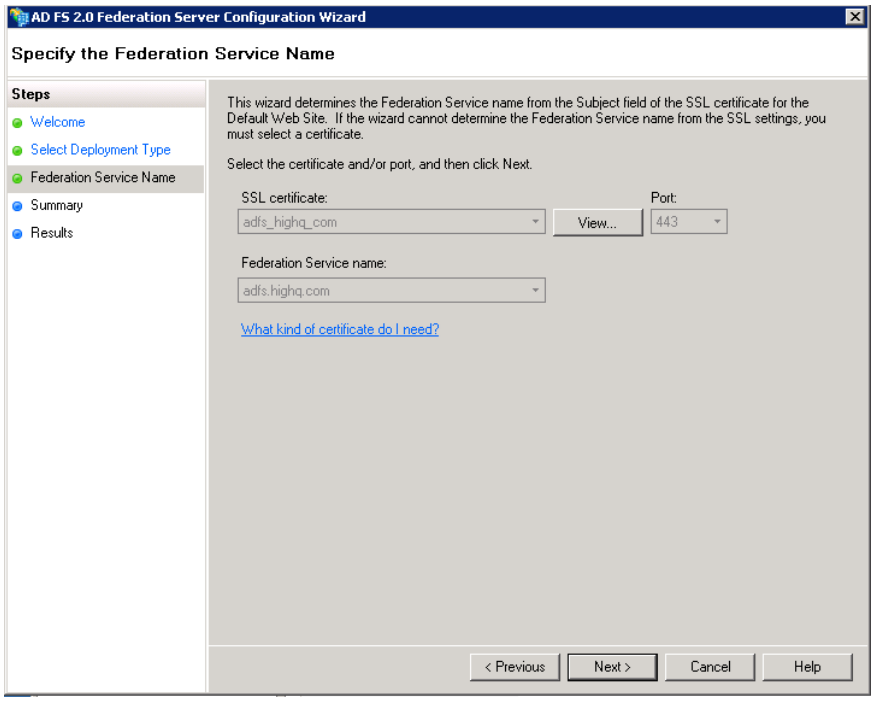
Select “Create a new Federation Service” and click Next.



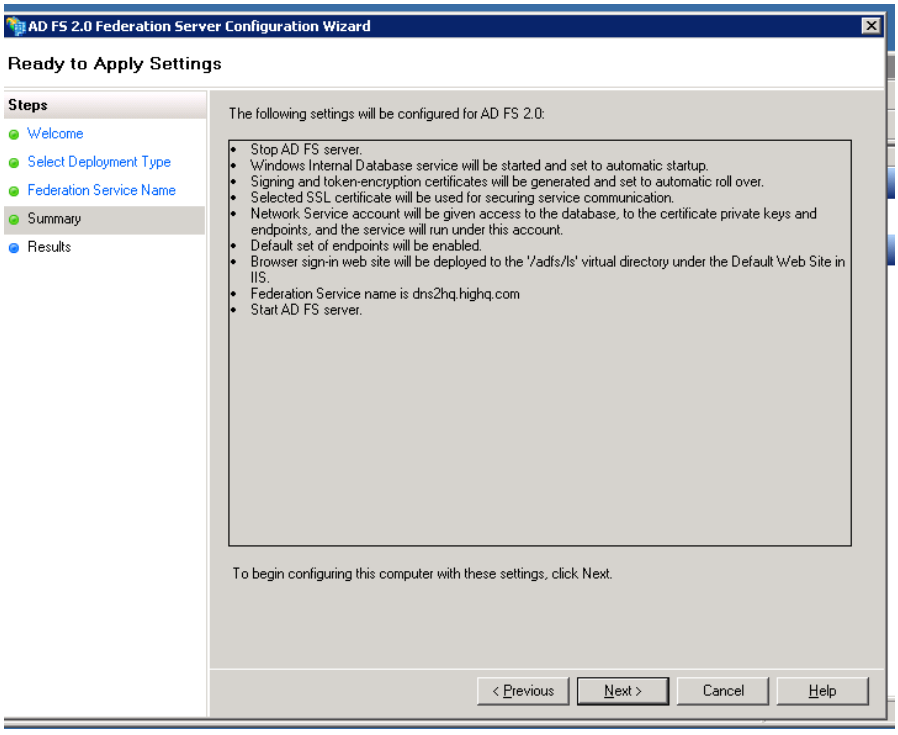
Select “Stand-alone federation server” and click Next.



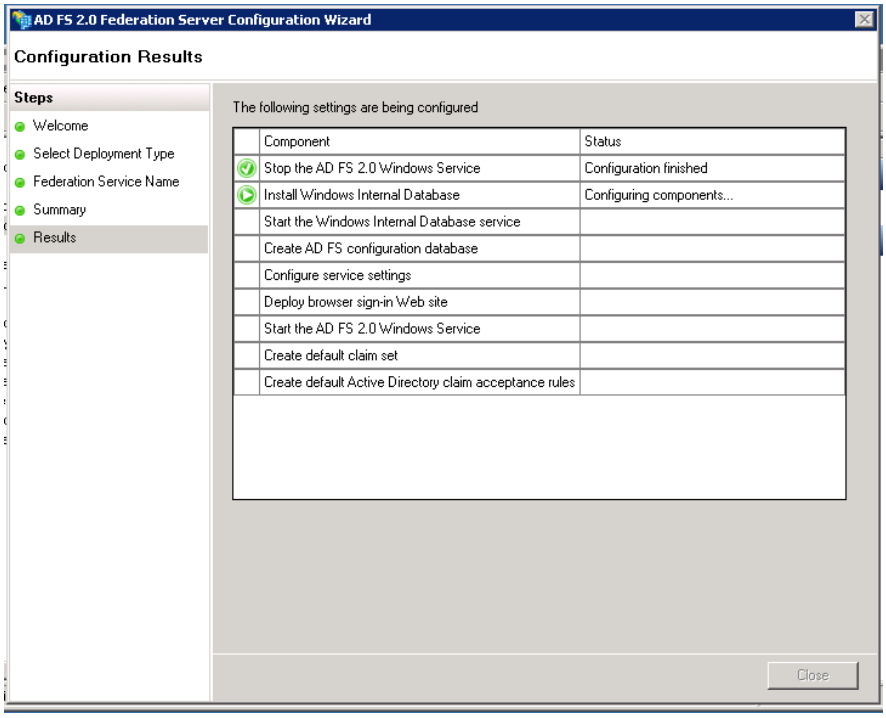
Your SSL Certificate will be selected on next screen. If you have multiple certificates setup you can select the appropriate for your ADFS FQDN. Click Next.



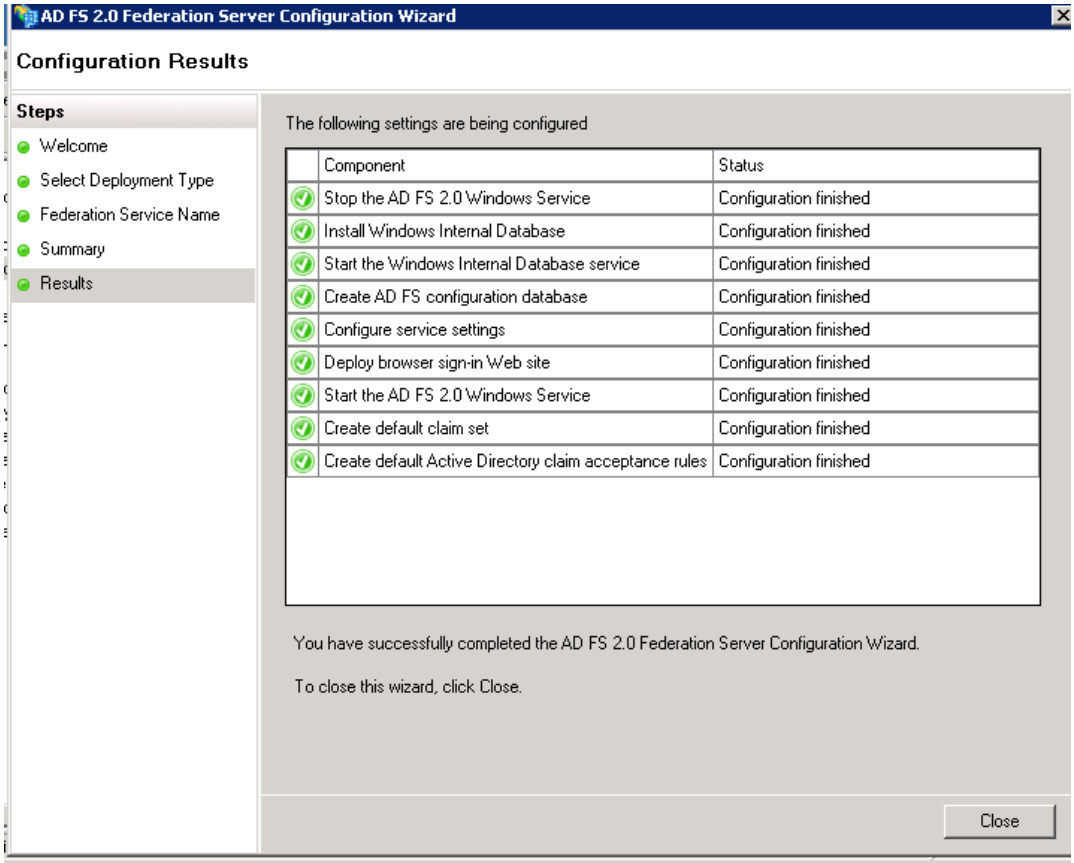
Click Next.



Configuration will begin.



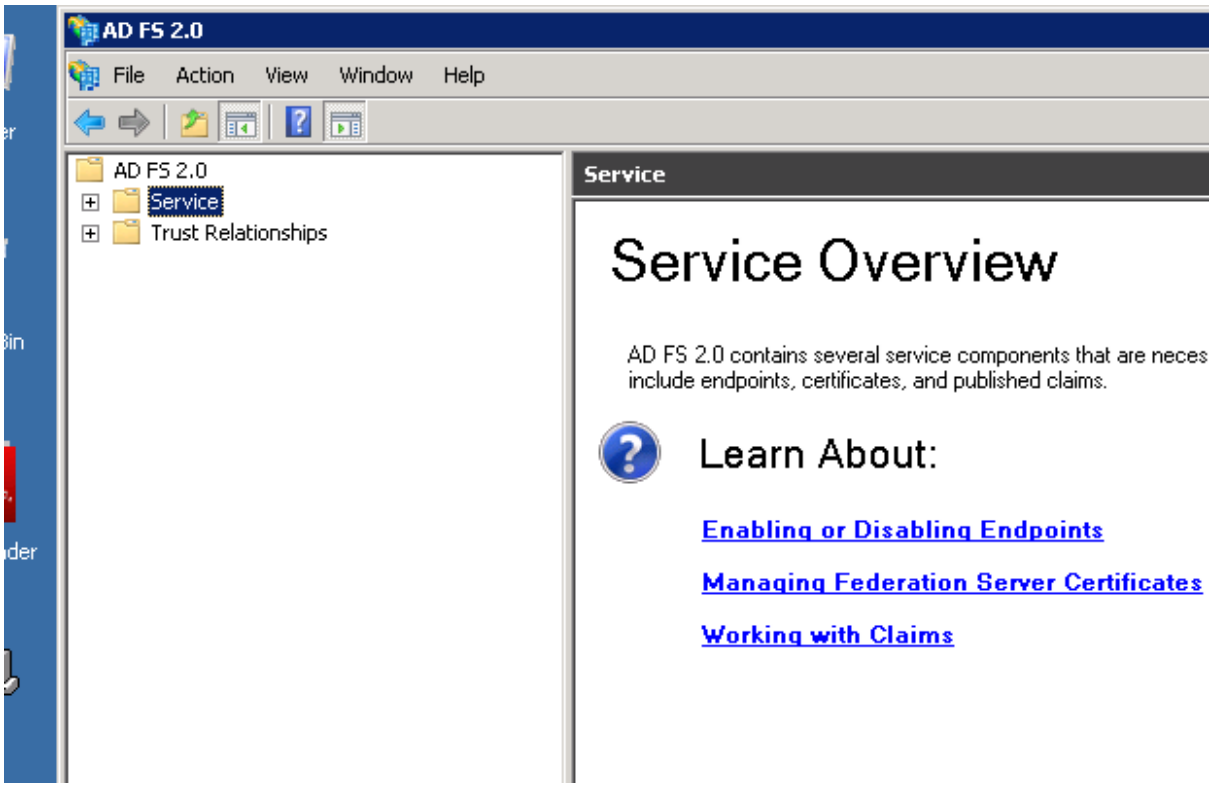
Wait for Configuration to finish.



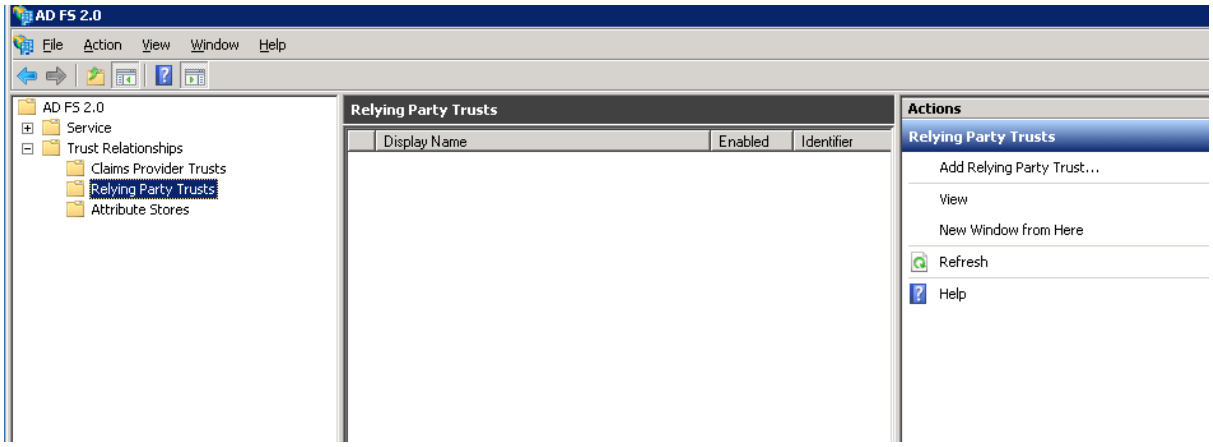
Click Close to finish ADFS installation.

4. ADFS Configuration for SSO

Open AD FS 2.0 Management.

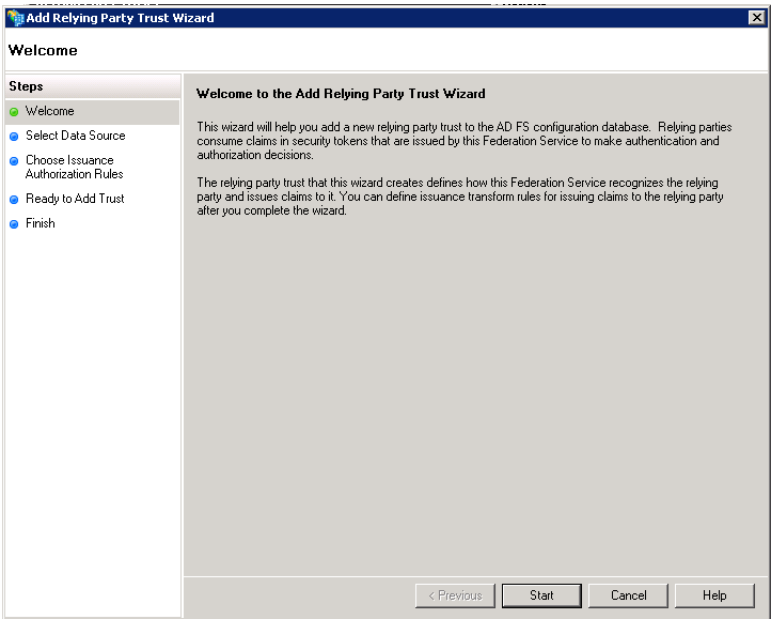


Go to Trust Relationships>>Relying Party Trusts



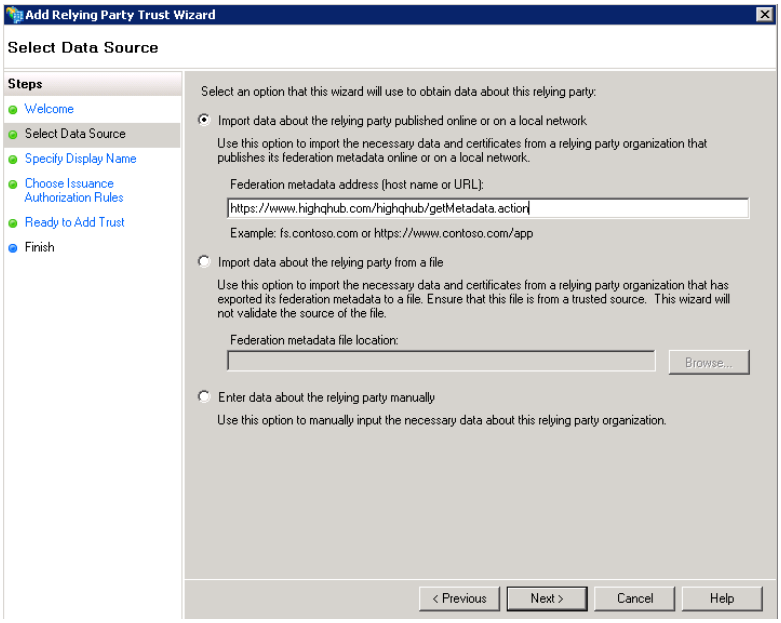
Click on Add Replying Party Trust in Actions on right.

Click Next to continue



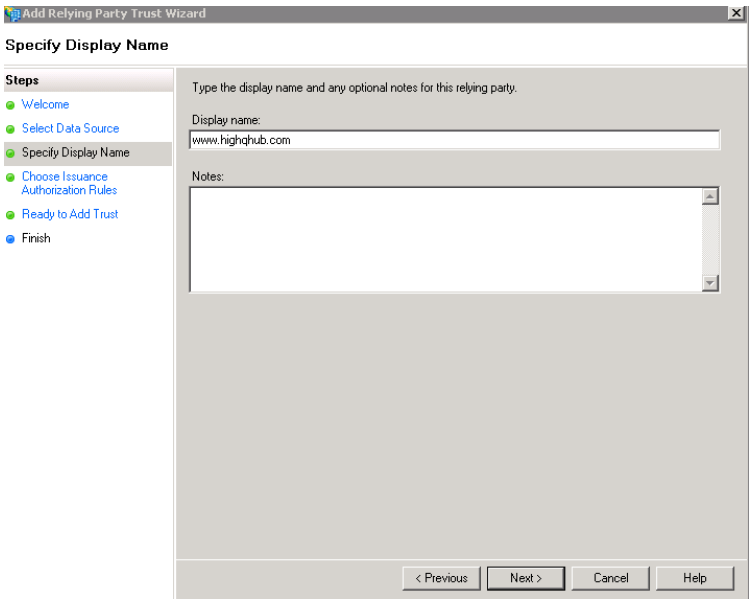
On next screen, select first option, “Import data about the relying party…….”

Give URL to "Federation metadata address"
https://highqhub.com/highqhub/getMetadata.action

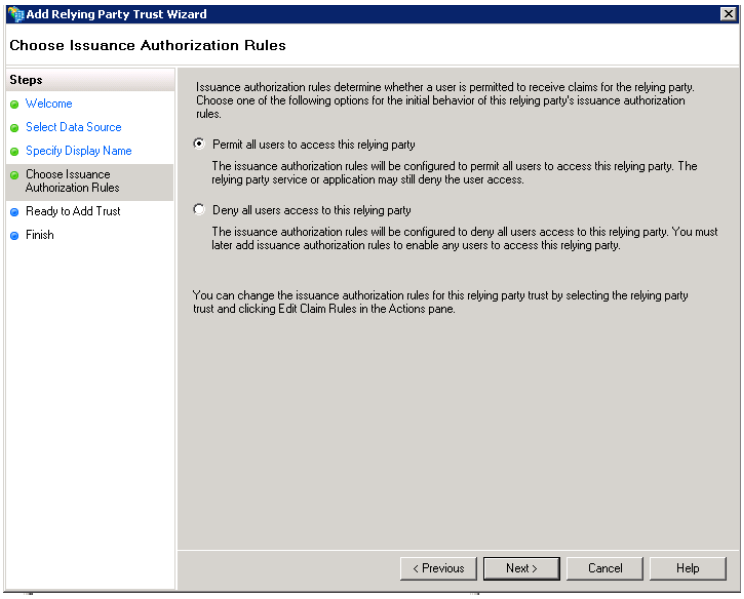


Click Next.

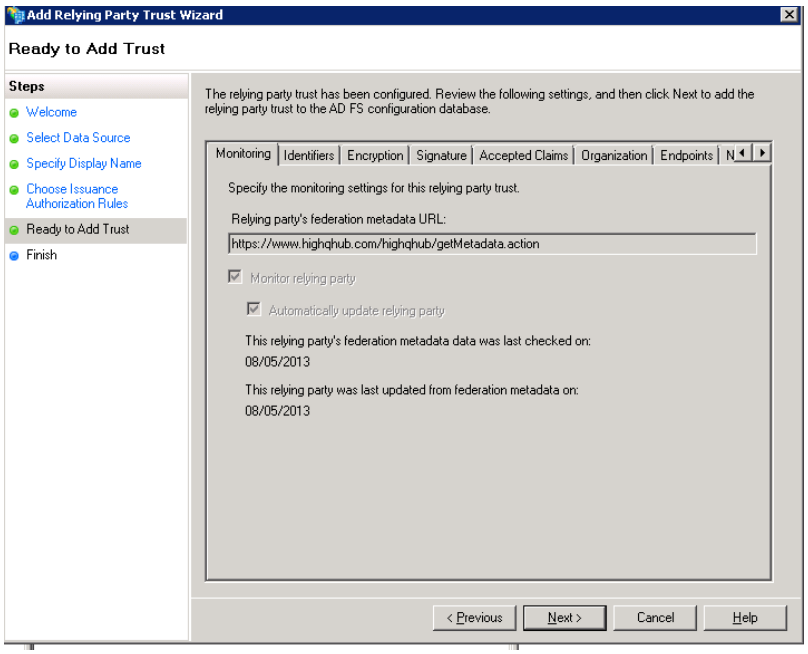
Enter Display name “www.highqhub.com”



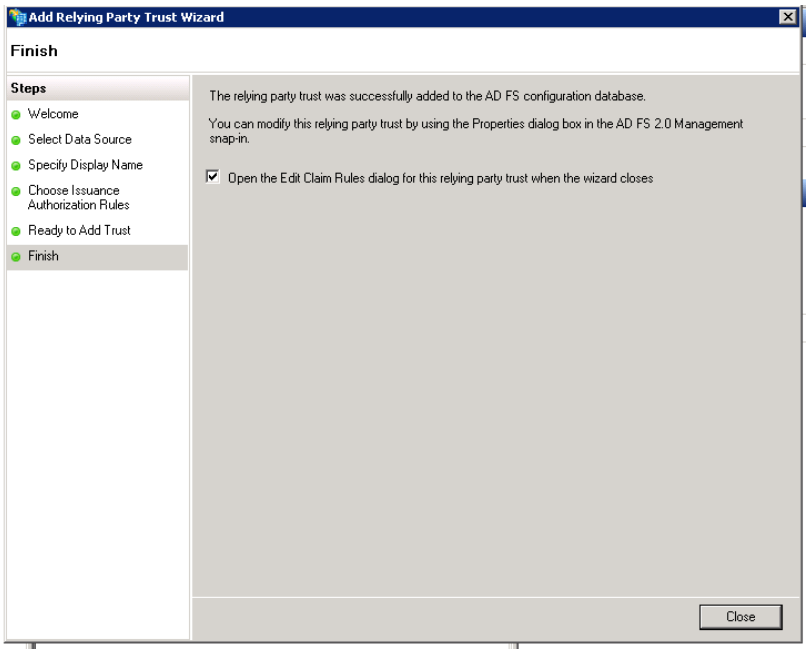
On next screen select “Permit all users to access this relying party”.



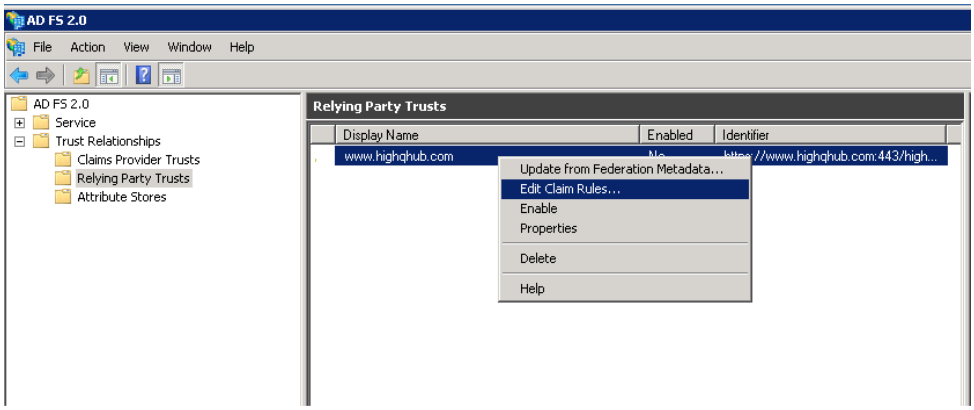
Click Next.



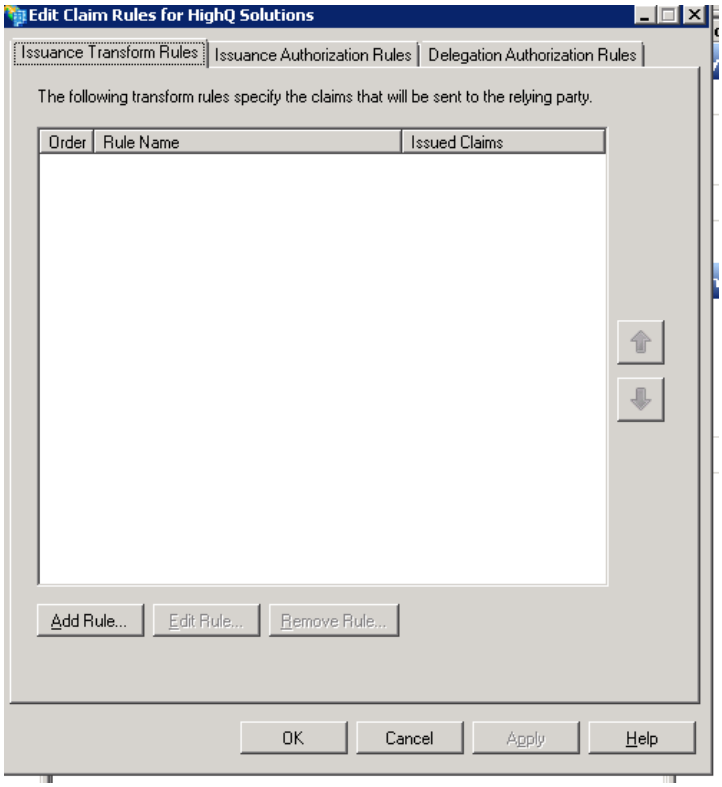
Click on close.



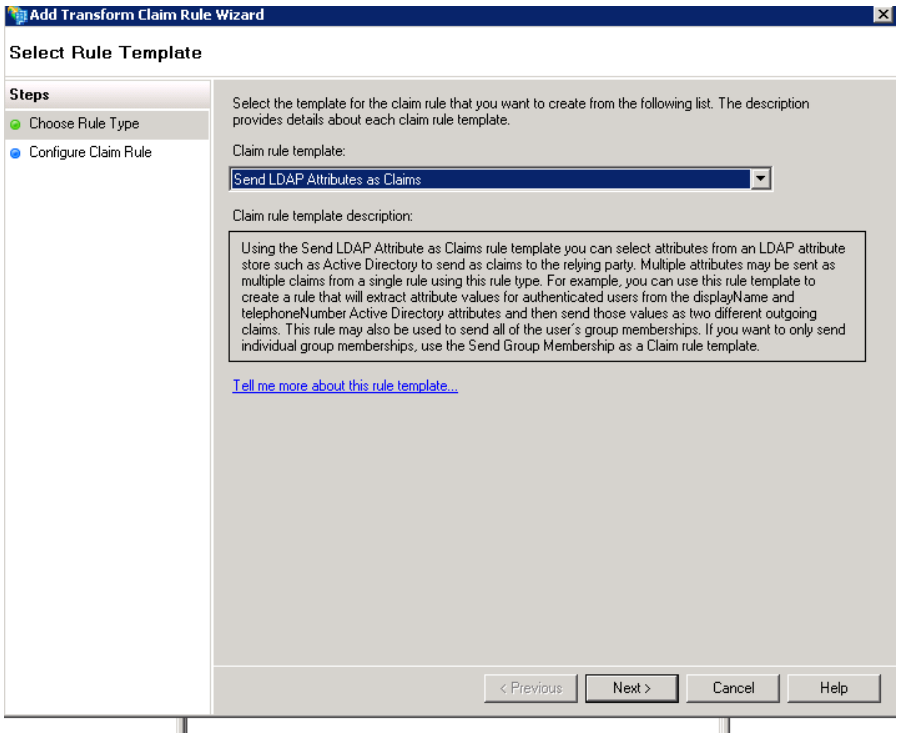
Go to Relying Party Trusts, right click on Display Name www.highqhub.com and Edit Claim Rules



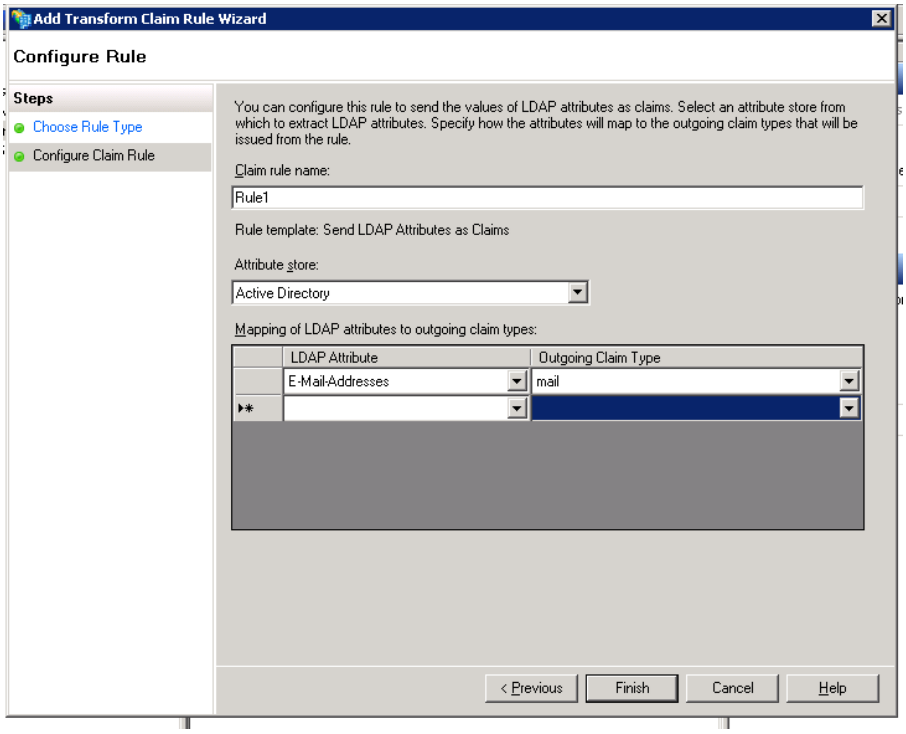
Click "Add Rule" button, will get Select Rule Template window.



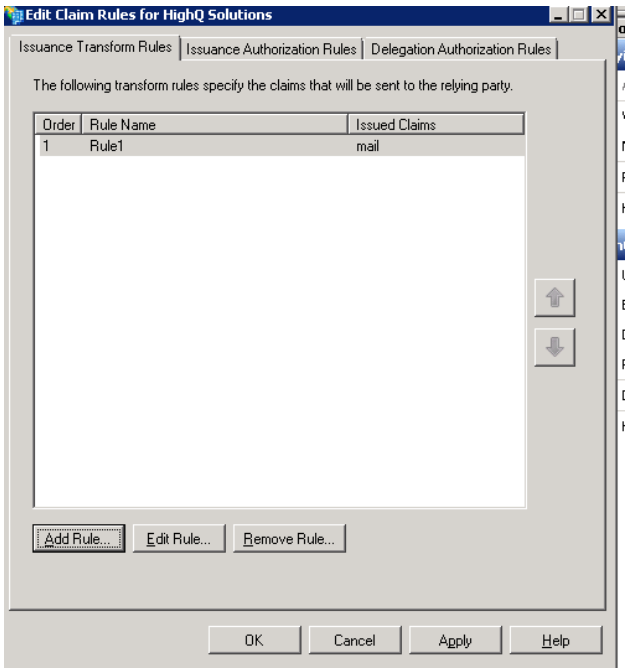
Select "Send LDAP Attributes as Claims" from "Claim rule template" drop down, and click Next.



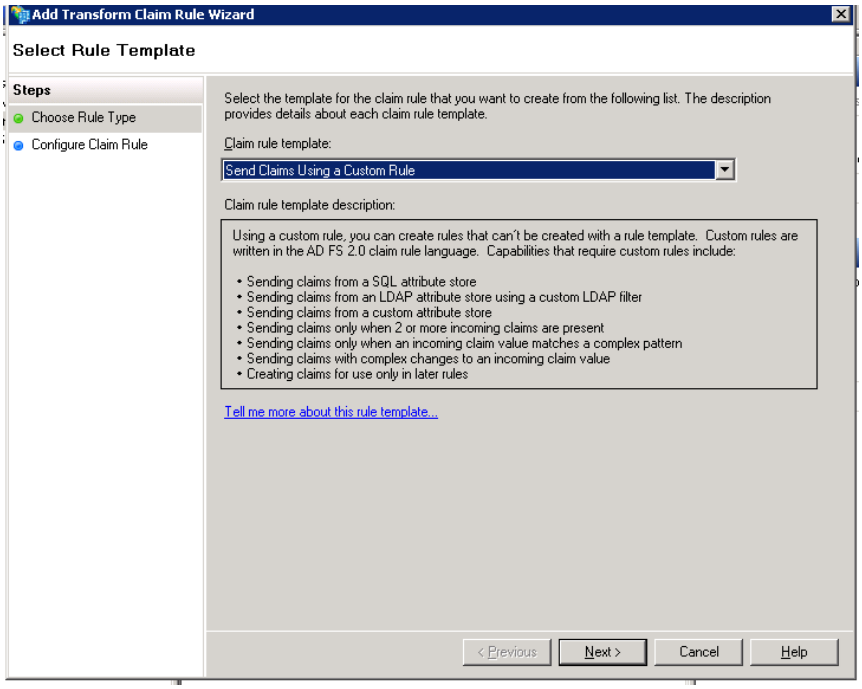
On next screen,
-- give claim rule name in "Claim rule name:" textbox.
-- select "Active directory" from "Attribute store:" dropdown.
-- select the value for "Mapping of LDAP attributes to outgoing claim types:"
-- select "E-mail-addresses" from "LDAP Attribute" and write "mail" in "Outgoing Claim Type".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



Again click on “Add Rule”



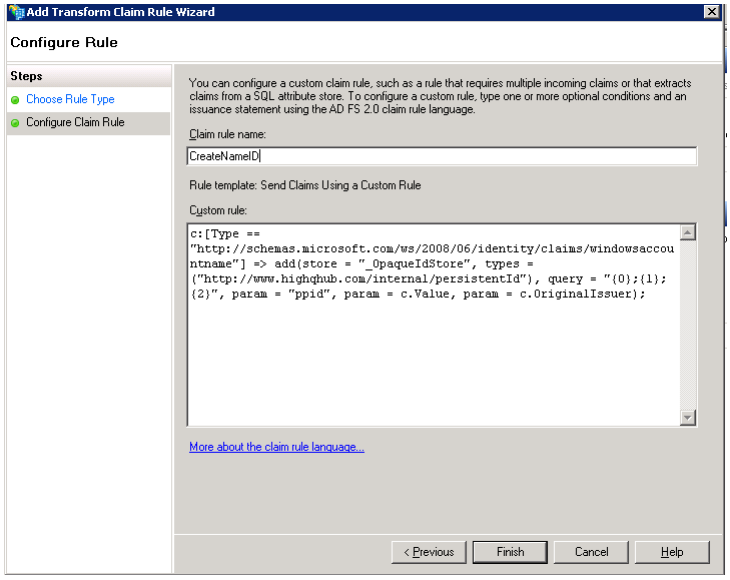
Select "Send Claims Using a Custom Rule" from "Claim rule template" drop down. and click Next.



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

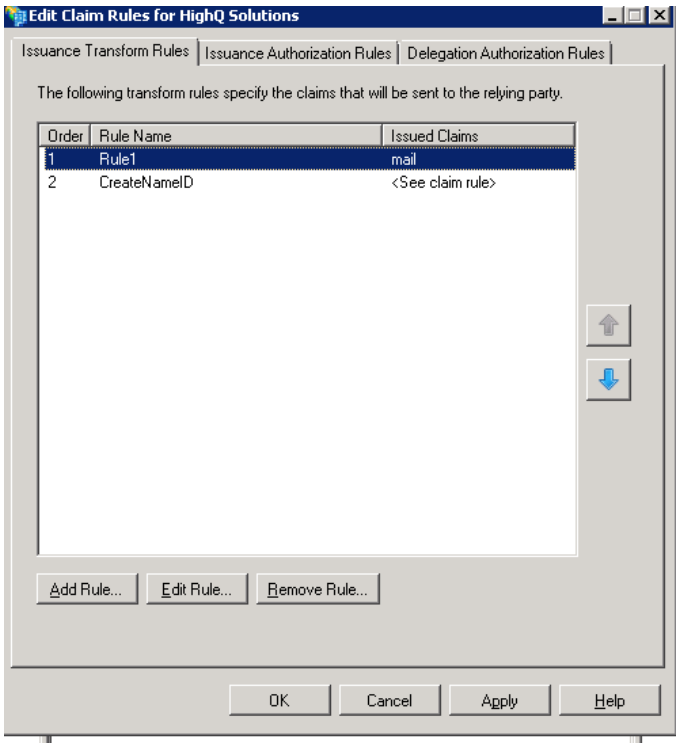
```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
 => add(store = "_OpaqueIdStore", types = ("http://www.highqhub.com/internal/persistentId"), query =
"{0};{1};{2}", param = "ppid", param = c.Value, param = c.OriginalIssuer);
```

-- 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.

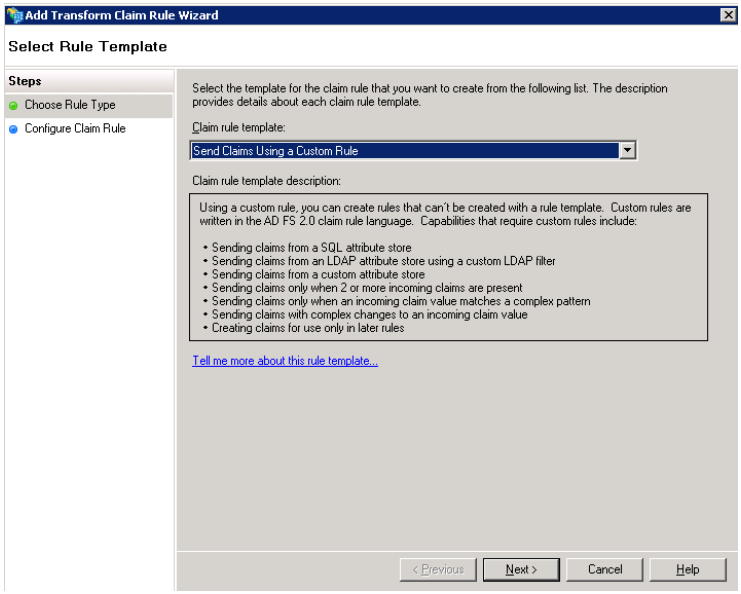


Click on Finish.

For third rule, click “Add Rule” button.



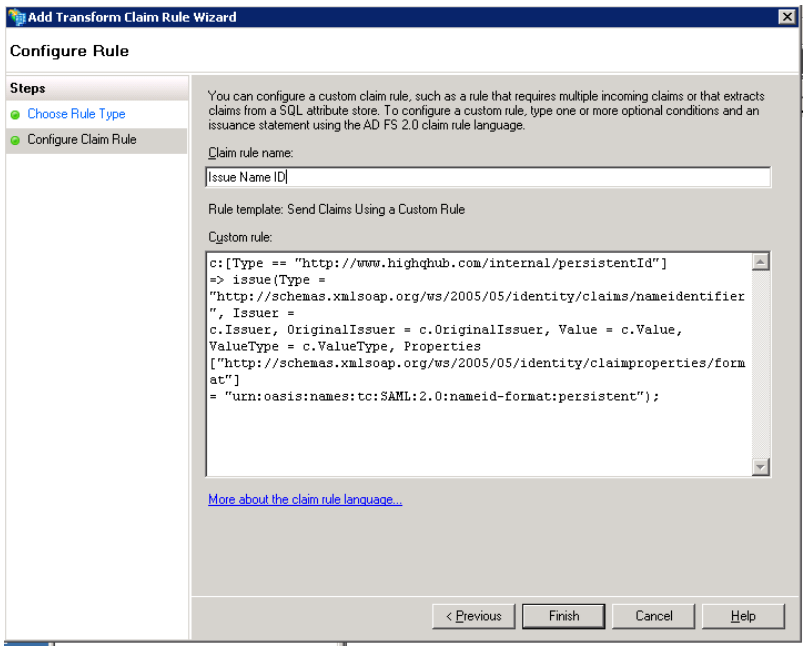
-- select "Send Claims Using a Custom Rule" from "Claim rule template" drop down. and click Next.



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

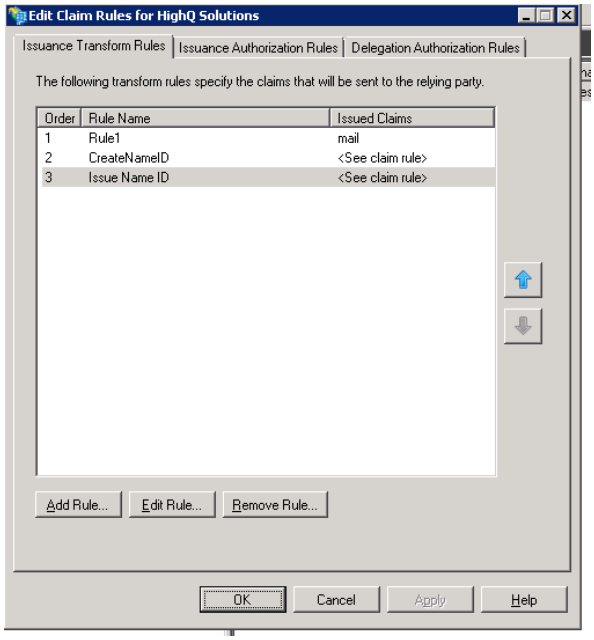
```
c:[Type == "http://www.highqhub.com/internal/persistentId"]

 => 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");
```

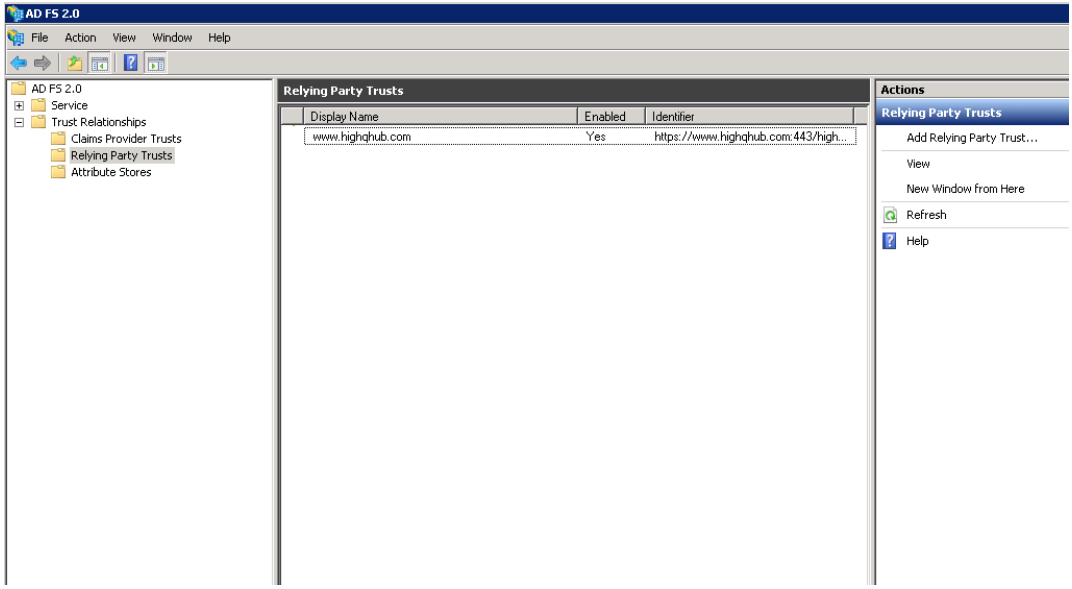
-- Please note that the spacing is very important and has to be exactly right otherwise it will simply not work. The below image is what it should look like exactly.



Click Finish.

Apply and Click OK.

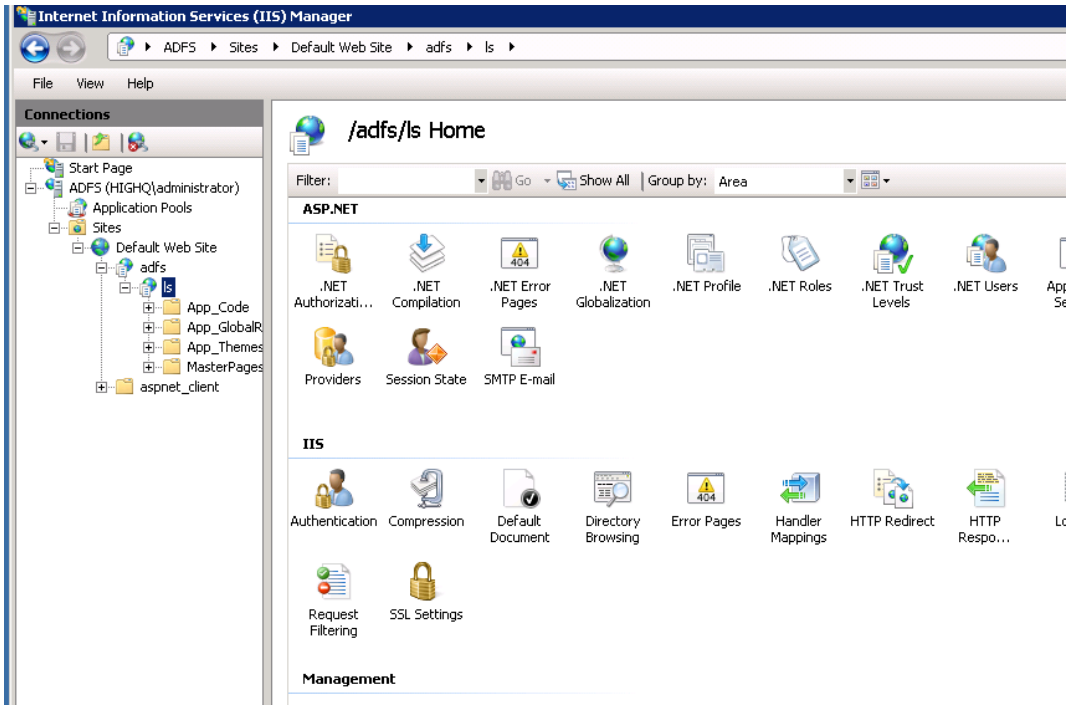




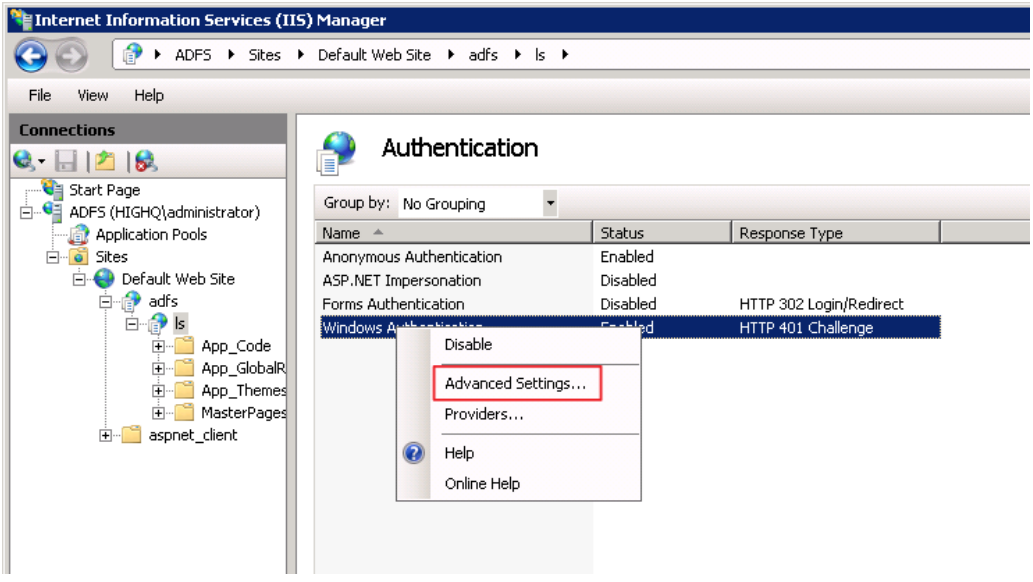
5. Other info

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

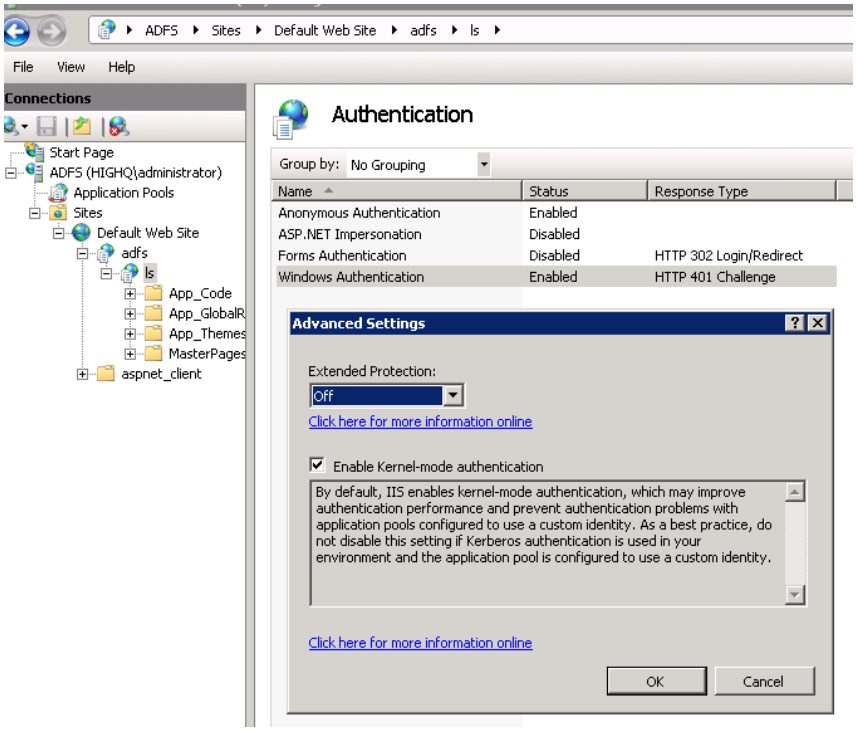
Go to IIS Manager>>Default Web Site>>adfs>>ls - double click on "Authentication under IIS heading.



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**.