ADFS Configuration for Arctera Desktop and Laptop Option 10.0

Contents

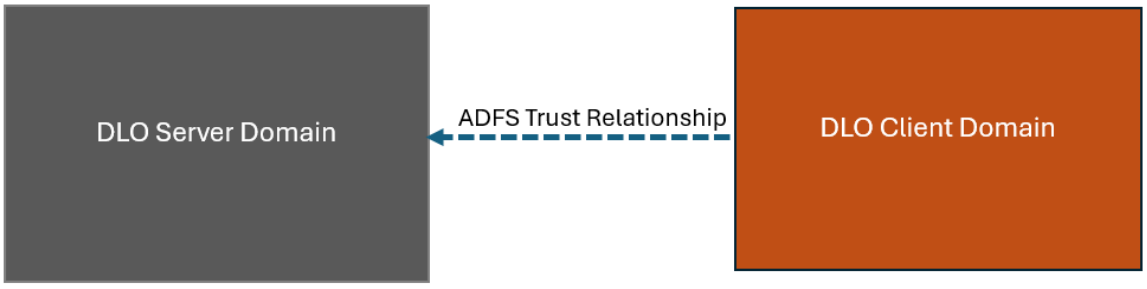
1. Introduction

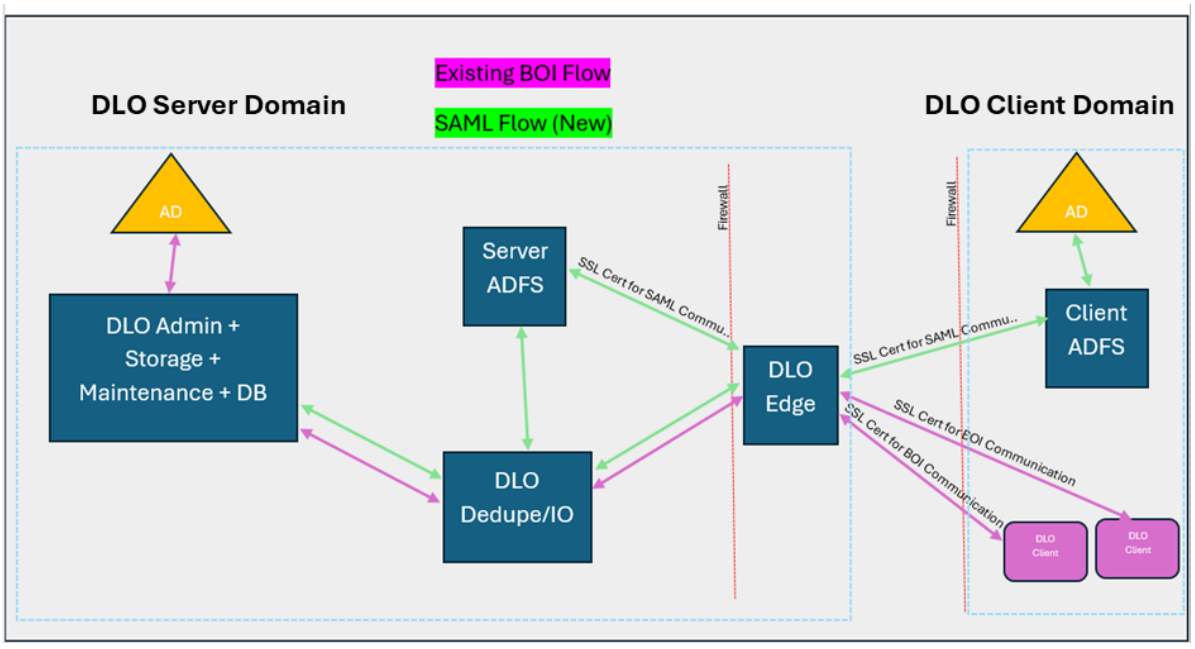
Arctera Desktop and Laptop Option can now protect endpoints in different isolated domains through federated trust between ADFS Servers. The domains can be in the same or different location and within the same, or different organizations.

Establishing a domain trust relationship between two domains is no longer mandatory for DLO to function in a multi-domain environment. In such cases, the DLO ADFS solution can be utilized. With this change, DLO ADFS solution enhances security by excluding the need for a direct Client AD connection.

This document details the steps for an administrator to Install and Configure ADFS for the Desktop and Laptop Option.

2. Architecture Overview for ADFS





3. Steps and Configuration settings

3.1 DLO ADFS Solution Deployment Overview

Domain 1 is referred as **DLO Server Domain** and **Domain 2** is referred as **DLO Client Domain**. Windows ADFS is running in Domain 1 and Domain 2. DLO Server component is deployed in Domain 1 and DLO Client resides in Domain 2. Domain 1 and Domain 2 can be an isolated domain present in two different locations, organizations. There should be a federation trust between ADFS of respective domains.

Domain 1 (DLO Server Domain): Components present in Domain 1 are:

- DLO Administration Service
- DLO Administration Console
- DLO Maintenance Service
- DLO Dedupe Server
- DLO Database Server
- DLO Storage Server
- DLO IO Server
- DLO Edge Server*
- Windows ADFS Server (Server ADFS)
- Active Directory Domain Services (Server Domain User Identity provider)

  **- DLO Edge Server can be installed in demilitarized zone.*

Domain 2 (DLO Client Domain): Components present in Domain 2 are:

- DLO Agent on endpoints
- Windows ADFS Server (Client ADFS)
- Active Directory Domain Services (Client Domain User Identity provider)

For the **System requirement** of the individual DLO components please refer DLO Administrator Guide.

3.2 Port Requirements

Source	Destination	Source Port	Destination Port	Protocol
DLO Edge Server	**Client Domain ADFS Server**	Dynamic Port (49152 to 65535)	443	TLS
DLO IO Server	**Server Domain ADFS Server**	Dynamic Port (49152 to 65535)	443	TLS
Client Domain ADFS Server	**Client Domain AD**	Multiple Port based on AD Configuration (389, 139, 445, 445, 88)	Multiple Port based on deployment	CLDAP, NBS, TCP, LSARPC, KRB5
DLO Edge Server	**DLO Client**	443	Dynamic Port (49152 to 65535)	TLS

Note: The Source and Destination components mentioned in the table have two-way communication, so both inbound and outbound rules need to be defined in the firewall for the specified port.

For port specification for other DLO components, please refer -*Port Requirements for Arctera Desktop and Laptop Option.*

3.3 Usage of Different SSL Certificates

1. **Certificate used for DLO Edge Server**: This is a certificate used by DLO Edge Server. DLO Client will trust this certificate for BOI connection and for accessing DLO Web Restore URL.
2. **Server ADFS certificate**: This is a Server ADFS certificate, which DLO IO Server and DLO Edge Server will trust, to establish a secure communication channel (DLO-IO <--> Server-ADFS, Server-ADFS <--> DLO-Edge).
3. **Client ADFS certificate:** This is a client ADFS certificate, which DLO Edge Server will trust to establish a trusted communication channel (DLO Edge<->Client ADFS).
4. **Server ADFS Token-decryption certificate:** This is a certificate used by Server ADFS to encrypt and decrypt the SAML request.
    - The SAML string is formed in DLO-IO Server and reaches to Server ADFS in plain string form. The Server ADFS encrypts the SAML string using this certificate and passes to Client ADFS via DLO-Edge Server.
    - The Client ADFS will process the request by decrypting and will send the response by encrypting again via DLO Edge Server.
    - The Server ADFS on receiving the encrypted response, decrypts it using the certificate.
5. **Server ADFS Token Signing certificate:** This is a certificate used to sign the response received from Client ADFS.
   This certificate can be obtained from DLO Server Domain's ADFS machine. Launch ADFS Management console and go to Services and then to Certificate. In Certificate section, select and right-click Token Signing certificate and export it as .cer file.
6. **Certificate used to access DLO Web Restore SAML endpoint(optional):** The signed response which Server ADFS created is sent to DLO Web Restore SAML API Endpoint by encrypting using this certificate. Then internally, corresponding .key file is used to decrypt this encrypted information. At the end, the signature in token is verified to confirm the response is occurring from right ADFS.

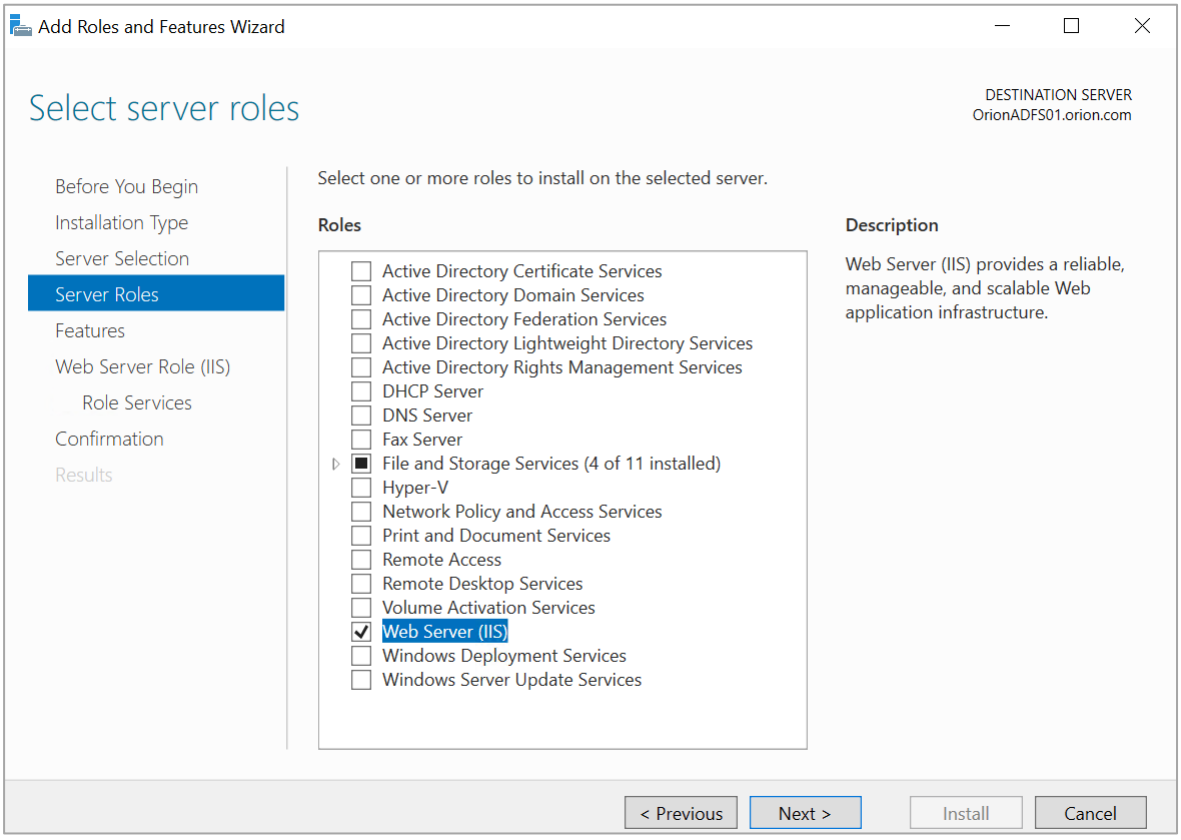
3.4 Windows ADFS Installation and Configuration

Steps -

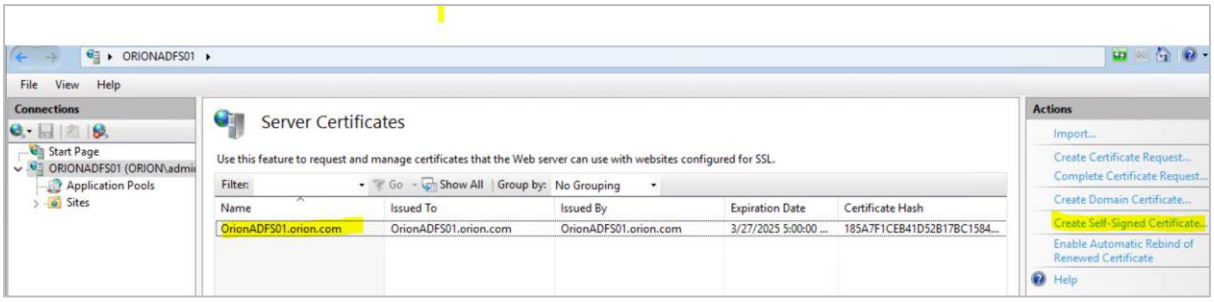
1. **Domain creation**: Skip this step if domain is already configured.
   Install an ADDS (Active Directory Domain Service) in a Windows Server machine. DC, DNS, LDAP all component of ADDS should be configured.

2. **Rename hostname and add to the domain**: Take another Windows Server machine. Here ADFS (Active Directory Federation Service) will be installed. Rename the hostname of the machine to something which can be remembered. Then add this machine to the domain created in Step 1 and restart it.

3. **Add Web Server role**: In Windows Server machine, install Microsoft IIS Web Server.

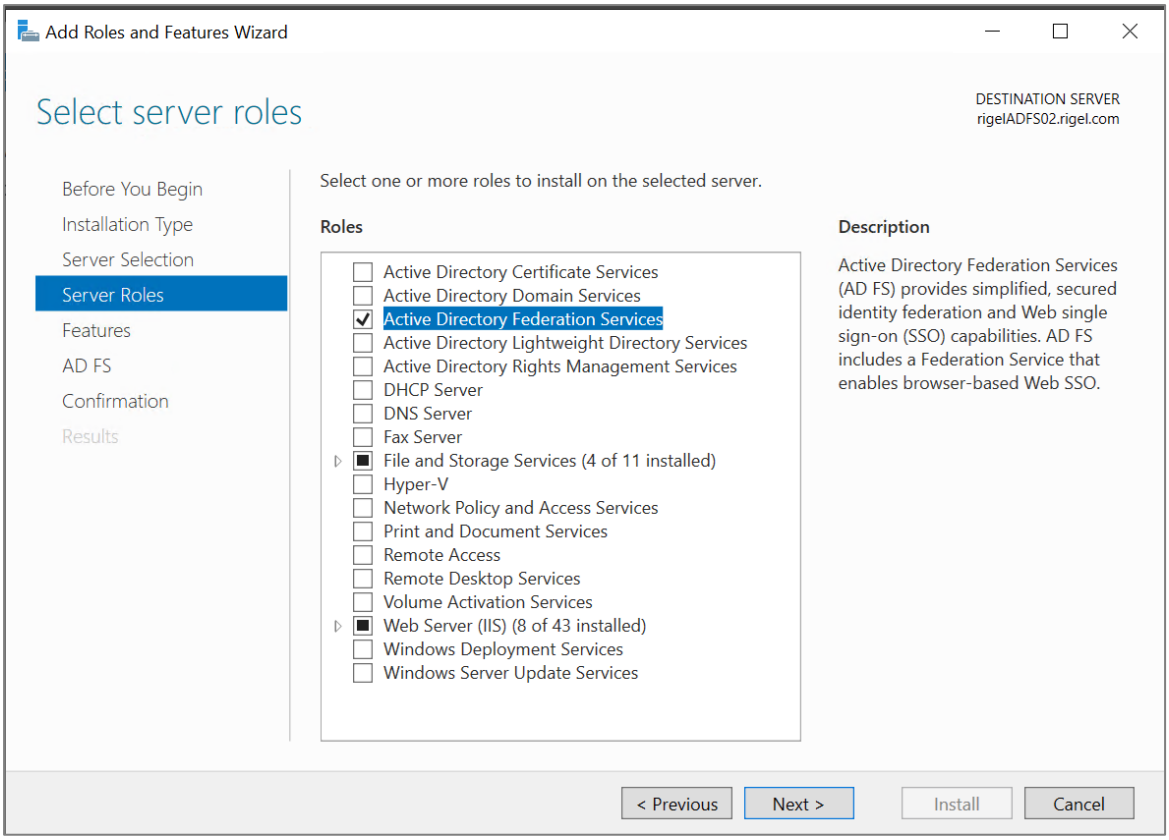


4. **Generate Self-signed certificate for ADFS authentication:** Skip this step if valid CA Signed certificate is used.
   Once the IIS web server is installed. Open IIS Manager. Go to 'Server Certificate' and create a self-signing certificate by the machine name in .pfx form.



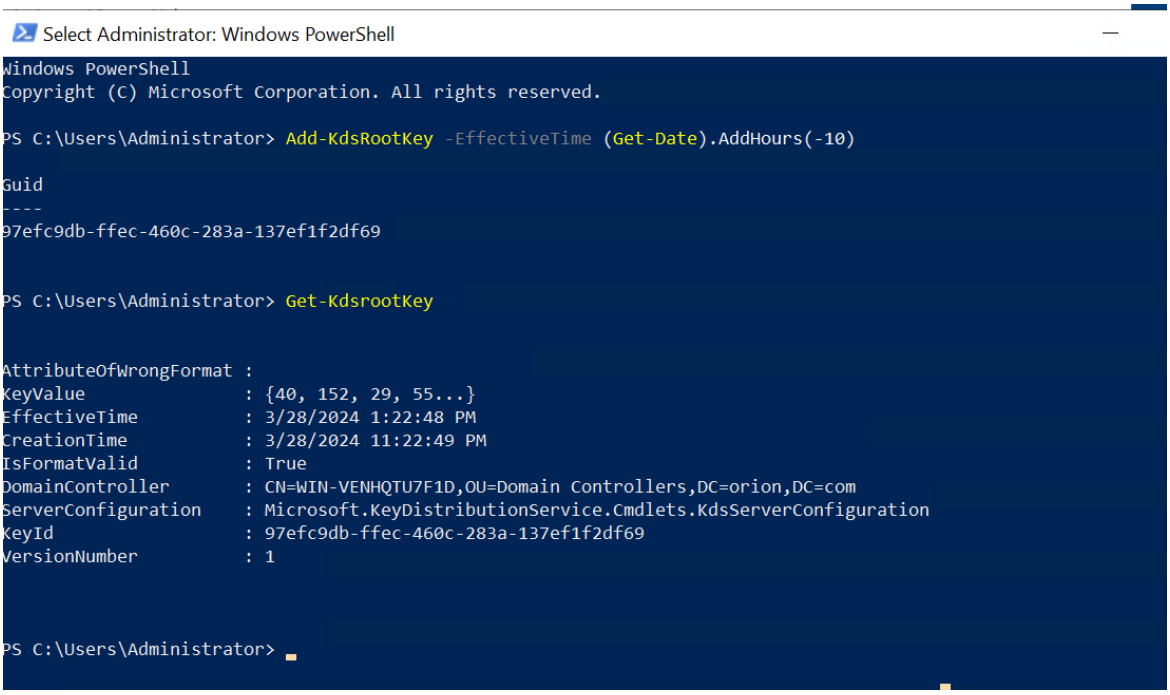
5. **Import of certificate to local cert-store**: Skip this step if legitimate CA Signed is used. Once the certificate is created, import the certificate into the local user certificate store. Open 'certlm.msc' and import the self-signed certificate created in previous step to 'Personal' and 'Trusted Root Certificate Authority'.

6. **Add ADFS Server Role**: In same machine, add ADFS Server Role.

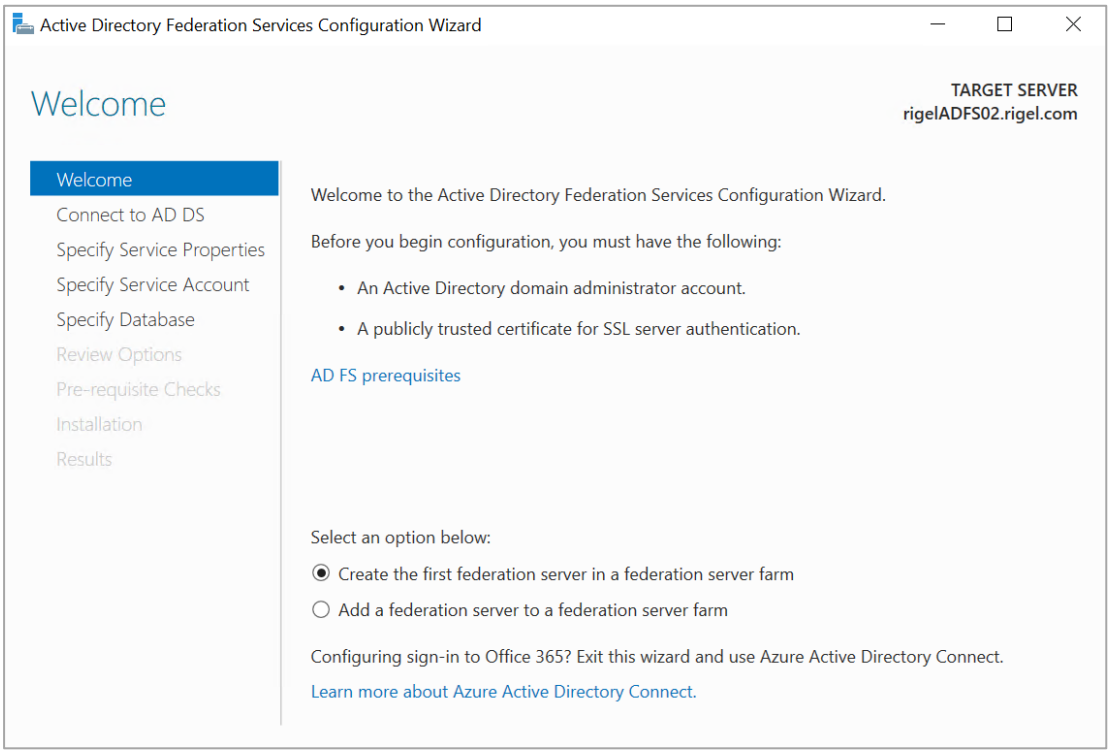


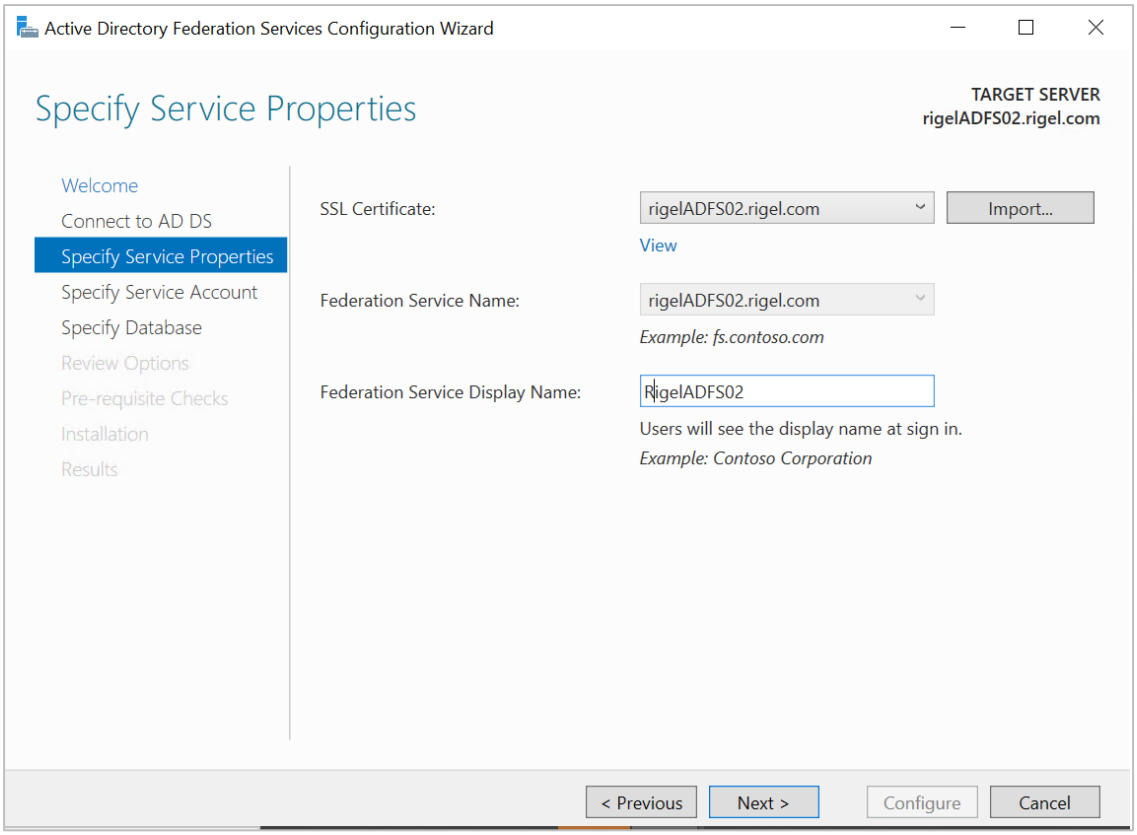
7. **Add KDS Root key in Domain Controller**: For Group Managed Service Account (gMSA), domain controller needs Key distribution Service (KDS) root key to be enabled to generate gMSA password.
Go to domain machine and open PowerShell to run following command –

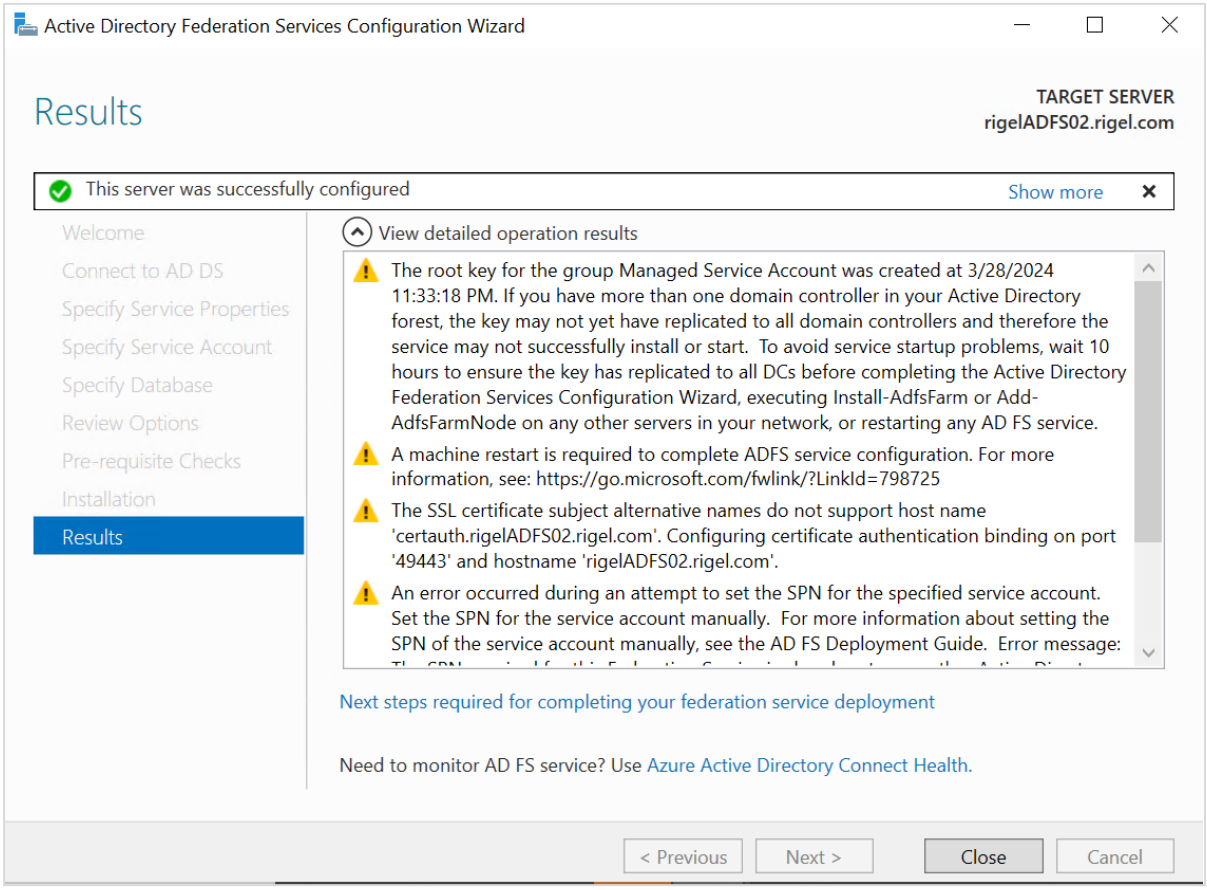
Add-KdsRootKey –EffectiveTime (Get-Date).AddHours(-10)



8. **Configure ADFS**: After adding the ADFS role, configure ADFS.
   Choose certificate, service account, federation display name appropriately to finish the configuration.







9. **Create Domain 2 (DLO Client Domain)**: Skip this step if domain is already configured.

Create another domain machine. Install an ADDS (Active Directory Domain Service) in a Windows Server machine. DC, DNS, LDAP all component of ADFS should be configured.

10. **Create ADFS Setup 2**: Now, create another server machine and repeat the above Steps from 1 to 8.

11. **Import self-signed certificate**: Skip this step if legitimate CA Signed is used.

    Import self-signed certificate of ADFS Setup 1 to Personal and Trusted CA directory of ADFS Setup 2.
    And
    Import self-signed certificate of ADFS Setup 2 to Personal and Trusted CA directory of ADFS Setup 1.

12. **Add 'Relying Party Trust in Client Domain ADFS**: In Client ADFS (i.e. ADFS Setup 2), launch ADFS Management console to add DLO Server ADFS as 'Relying Party Trust'.

    While adding Relying Party Trust: -
    a) Choose 'Claims aware'
    b) In 'Select Data Source', select "Import data from the relying party published online or on a local network" option and add federation metadata xml URL of ADFS Setup 1 (i.e. DLO Server Domain's ADFS Server) and finish adding the trust provider.

    Here DLO Server Domain's ADFS URL can be provided, or complete Federation Metadata
    URL can be provided in following manner -
    https://<adfs_setup1_server_name>
    (OR)
    https://<adfs_setup1_server_name>/FederationMetadata/2007-06/FederationMetadata.xml

    c) Choose rule as per requirement in access control policy.

13. **Add Claim rule**: Select and right click the recently added relying party and choose edit claim issuance policy.
    a) Add Rule – 'Send LDAP Attribute as claims.
    b) Choose attribute UPN (Universal Principal Number) and click finish.

14. **Add 'Claim Provider Trust' in ADFS Setup 1** (DLO Server Domain's ADFS):
    a) Login to ADFS Setup 1 (i.e. DLO Server Domain's ADFS) and add 'Claim Provider Trust'.
    b) In 'Select Data Source', select 'Import data from the claim provider published online or on a local network' option and add federation metadata xml URL of ADFS Setup 2 (i.e. DLO Client Domain's ADFS) and finish adding the claim provider.

https://<adfs_setup1_server_name>/FederationMetadata/2007-06/FederationMetadata.xml

15. **Enable SSO (Single-Sign on)**: In DLO Client Domain ADFS, open PowerShell as administrator and run following command –

    Set-AdfsProperties -EnableIdPInitiatedSignonPage $true

```
PS C:\Users\administrator.ORION> Set-AdfsProperties -EnableIdPInitiatedSignonPage $true
PS C:\Users\administrator.ORION> Get-AdfsProperties


AcceptableIdentifiers                   : {}
AddProxyAuthorizationRules              : exists([Type ==
                                          "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", Value
```

16. **Install Browser**: Install chrome browser in DLO Domain's ADFS Setup.

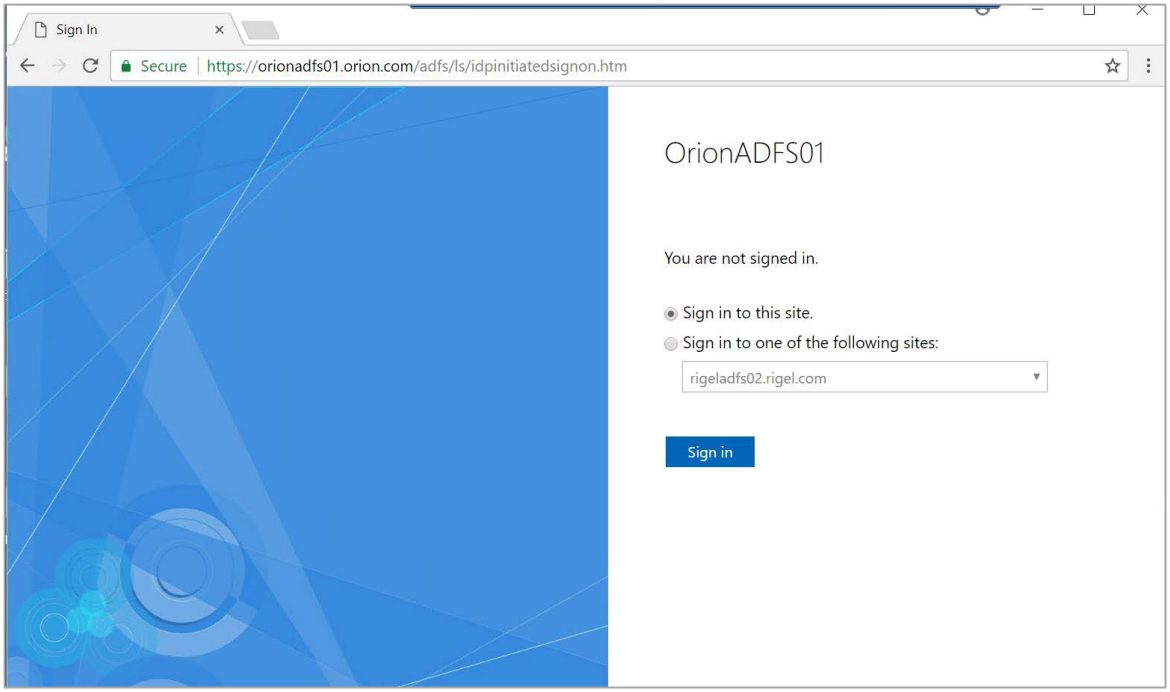
17. **Test ADFS Connection**:

    Access resource of Domain 1 (DLO Server Domain) using credential of Domain 2 (DLO Client Domain).

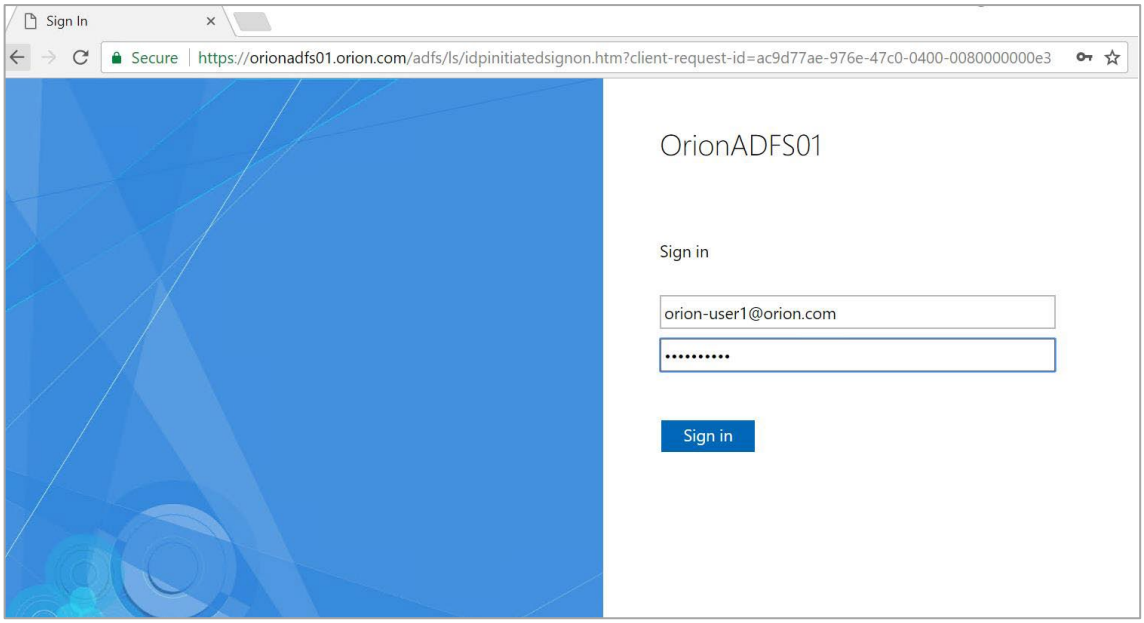
    In DLO Client ADFS Server machine, launch chrome and access SSO link of ADFS 1 –

    https://<adfs1.domain.com>/adfs/ls/idpinitiatedsignon.htm

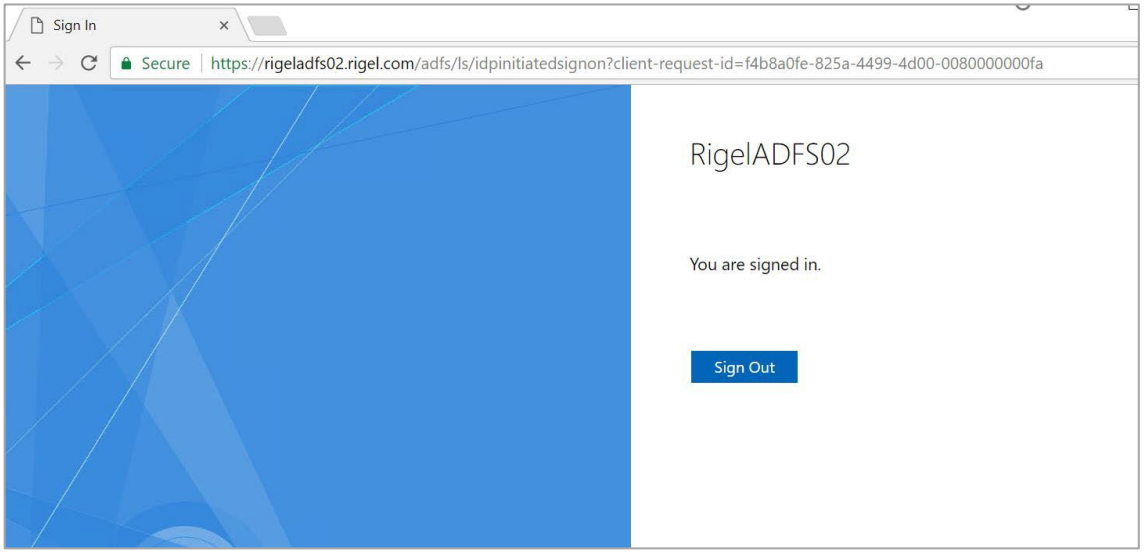
    Once SSO page is loaded, select domain 1 URL from the drop down and click **Sign in.**



Use credential of Domain 2 to sign-in.



Successful login



3.5 Configure ADFS in DLO

Import Certificate for IO Server:

1. Login to the machine where DLO IO Server is installed.
2. Open CMD and Navigate to “C:\Program Files\Veritas\Veritas DLO\IOServer\Jre\bin”.
3. Import DLO Server Domain’s ADFS Machine certificate in **.der** form to DLO IO Server Keystore.
   Syntax: Keytool -importcert -file “<%CertificatePath%>” -alias <Certificate_Name> -keystore "C:\Program Files\Veritas\Veritas DLO\IOServer\Jre\lib\security\cacerts"

   Example:
   Keytool -importcert -file “C:\Users\administrator.Sydney\Downloads\ServerSydneyADFS.der” -alias ServerSydneyADFS -keystore "C:\Program Files\Veritas\Veritas DLO\IOServer\Jre\lib\security\cacerts"
4. Enter password: “**changeit**” when prompted.
5. Enter **Yes** for confirmation.

```
C:\Users\administrator.SYDNEY>cd C:\Program Files\Veritas\Veritas DLO\IOServer\Jre\bin

C:\Program Files\Veritas\Veritas DLO\IOServer\Jre\bin>Keytool -importcert -file "C:\syd-adfs-lab01.sydney.der" -alias ServerSydneyADFS -keystore "C:\Program Files\Veritas
eritas DLO\IOServer\Jre\lib\security\cacerts"
Warning: use -cacerts option to access cacerts keystore
Enter keystore password:
Owner: CN=syd-adfs-lab01.sydney.com
Issuer: CN=syd-adfs-lab01.sydney.com
Serial number: 52e6d3d4edf16ea048afa62e2e5f4069
Valid from: Wed Dec 18 07:25:05 PST 2024 until: Wed Dec 17 16:00:00 PST 2025
Certificate fingerprints:
         SHA1: DD:BE:2A:FB:F2:AE:7A:CE:AB:DC:5F:19:4E:06:EE:1B:40:85:FC:70
         SHA256: 97:DF:3C:92:8A:FB:99:D2:F0:2F:02:C3:B8:98:D1:36:CE:47:0F:98:3F:8B:78:1E:6F:88:CD:DE:62:0B:8F:EC
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
]

#2: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  Key_Encipherment
  Data_Encipherment
]

#3: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
  DNSName: syd-adfs-lab01.sydney.com
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
```

6. Repeat the Steps 2 to 4, to import other DLO Edge Server certificate as well. Replace the certificate name and alias named accordingly for DLO Edge Server certificate.
7. After successfully importing DLO Server Domain’s ADFS Machine certificate, open ‘**Services.msc**’ and restart ‘**Veritas DLO Edge Server**’ and ‘**Veritas DLO Web Server**’ services.

Import Certificate for Dedupe Server:

1. **Login to the machine where DLO Dedupe Server is installed.**
2. Open CMD and Navigate to “C:\Program Files\Veritas\Veritas DLO\Dedupe\Jre\bin” .
3. Import DLO Server Domain’s ADFS Machine certificate in **.der** form to DLOIO Server Keystore.

   Syntax: Keytool -importcert -file “<%CertificatePath%>” -alias <Certificate_Name> -keystore " C:\Program Files\Veritas\Veritas DLO\Dedupe\Jre\lib\security\cacerts"

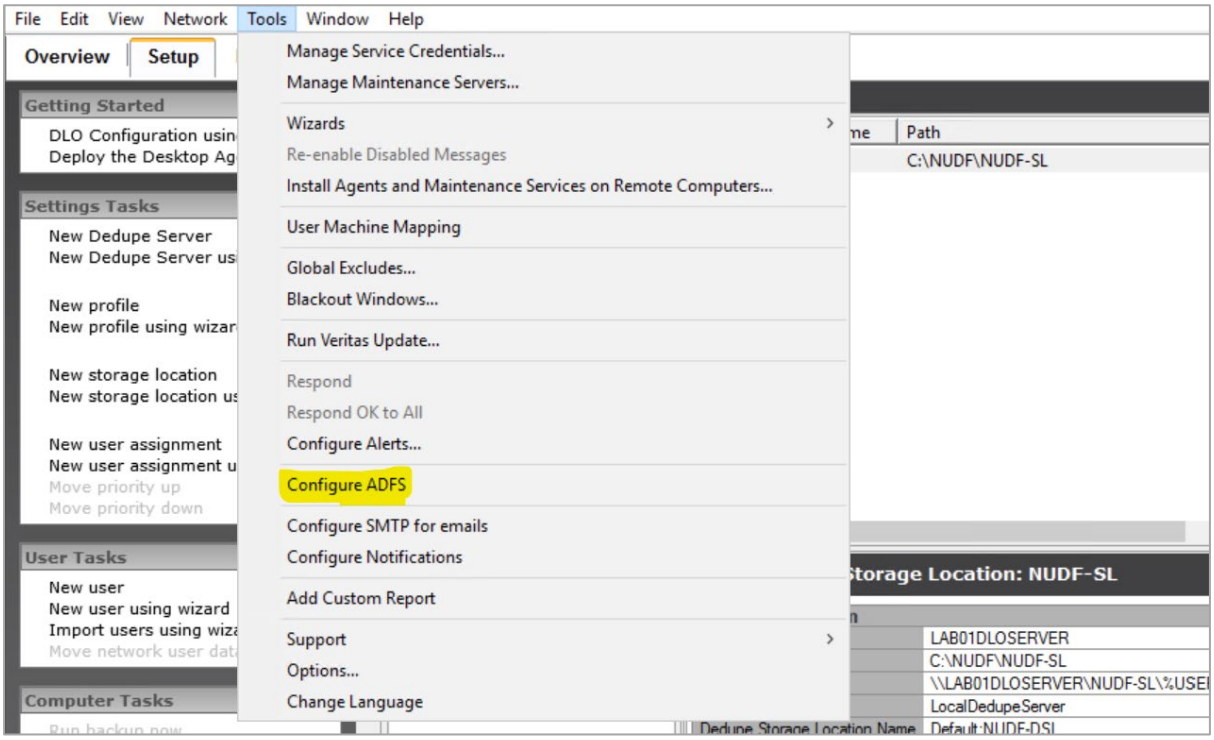
   Example:

Keytool -importcert -file "C:\Users\administrator.Sydney\Downloads\ServerSydneyADFS.der" -alias ServerSydneyADFS -keystore "C:\Program Files\Veritas\Veritas DLO\Dedupe\Jre\lib\security\cacerts"

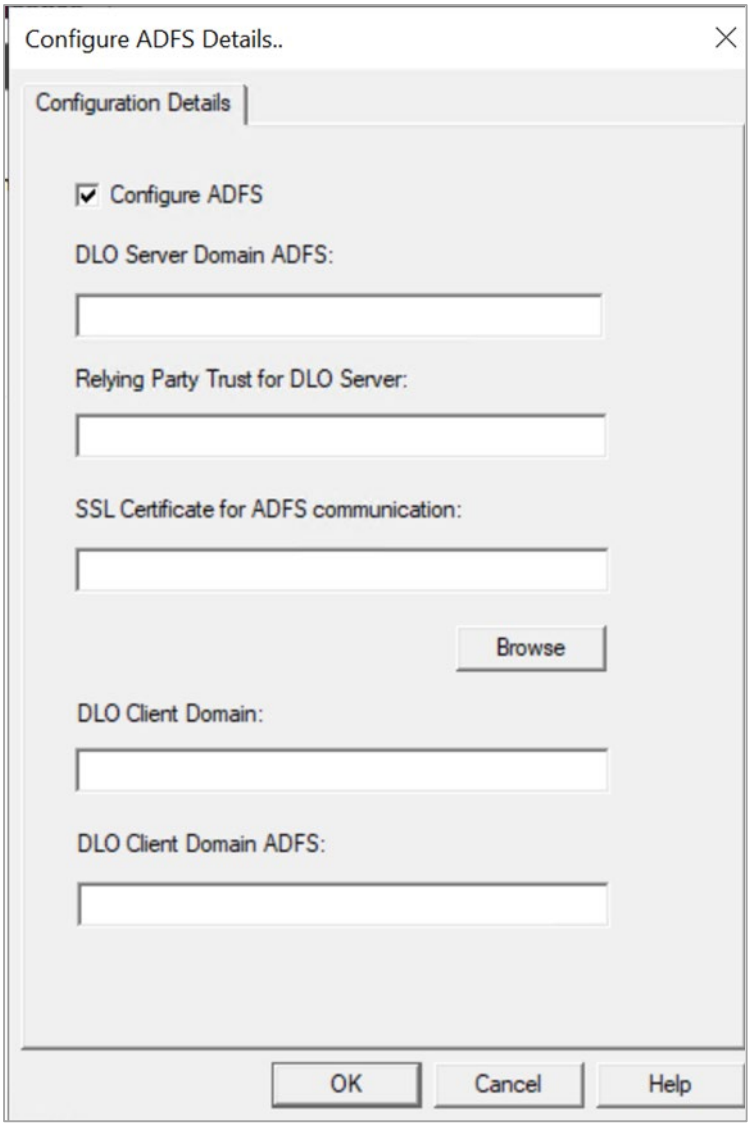
4. Enter password: "**changeit**" when prompted.
5. Enter **Yes** for confirmation.
6. Repeat the Steps 2 to 4, to import other DLO Edge Server certificate as well. Replace the certificate name and alias named accordingly for DLO Edge Server certificate.
7. After successfully importing DLO Server Domain's ADFS Machine certificate, open '**Services.msc**' and restart '**Mindtree StoreSmart Dedupe Server**' services.

<u>To configure ADFS in DLO, follow the below steps:</u>

1. On DLO, click **Tools** tab, and select **Configure ADFS**.



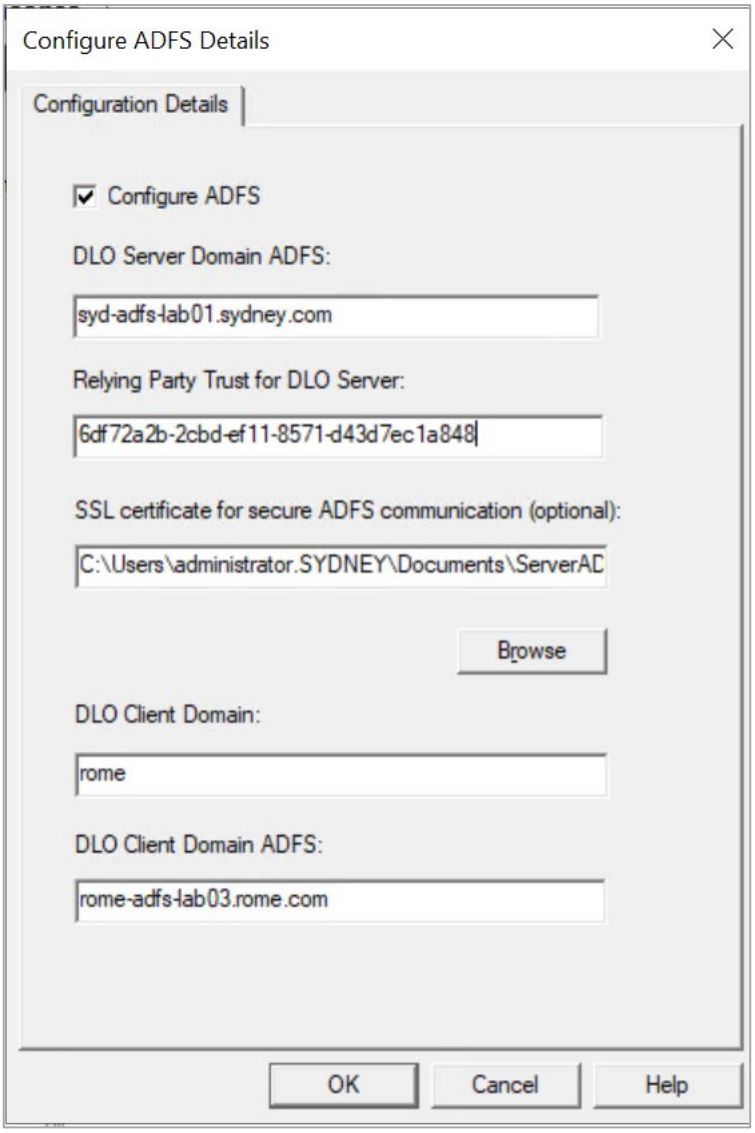
2. In the **Configure ADFS Details** Window, enable checkbox **Configure ADFS**.



3. Enter **DLO Server Domain ADFS** in FQDN (Fully Qualified Domain Name) format.
4. Enter **Relying Party Trust (RPT) Object Identifier** for DLO Edge Server.
5. To get this value, go to ADFS Server where DLO_Webrestore RPT was added and check DLO Edge Server RPT Object Identifier. Launch PowerShell as Administrator and run command: *Get-AdfsRelyingPartyTrust | where-object -Property Name -EQ "<RPT Name>" select ObjectIdentifier*

```
PS C:\Users\Administrator.SYDNEY> Get-AdfsRelyingPartyTrust | Where-Object -Property Name -EQ "DLO_Webrestore" | Select ObjectIdentifier

ObjectIdentifier
----------------
6df72a2b-2cbd-ef11-8571-d43d7ec1a848
```

6. For SSL certificate, click **Browse** and select DLO Server Domain ADFS token signing certificate. [Refer certificate section]
7. Enter **DLO Client domain** name.
8. **DLO Client Domain ADFS** in FQDN (Fully Qualified Domain Name) format.
9. Click **OK**.



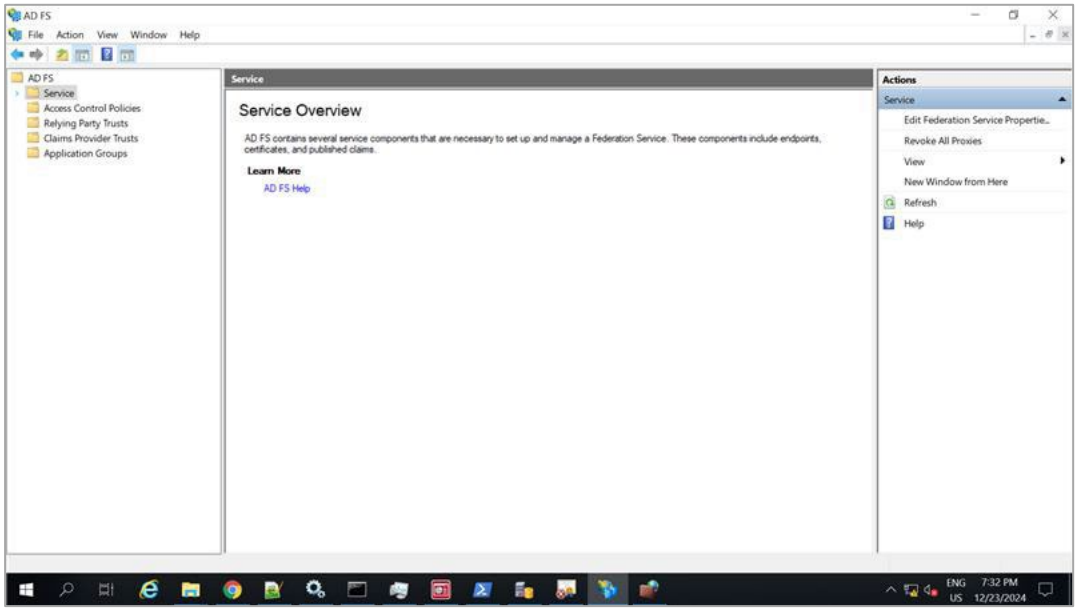
10. Verify **config_adfs.properties** file is created in below path:
    - *"C:\Program Files\Veritas\Veritas DLO"*
    - *"C:\Program Files\Veritas\Veritas DLO\Dedupe\Tomcat\webapps\DedupeServer\WEB-INF\classes\resource"*
    - *"C:\Program Files\Veritas\Veritas DLO\IOServer\Tomcat\webapps\DLOServer\WEB-INF\classes\resource"*
11. Verify ADFS token signing certificate **.cer** file are placed at "C:\Program Files\Veritas\Veritas DLO\IOServer\Tomcat\webapps\DLOServer\WEB-INF\classes\resource" path.

Note: If Self signed certificate is used, then Windows host file should have the necessary entries to resolve the network address.

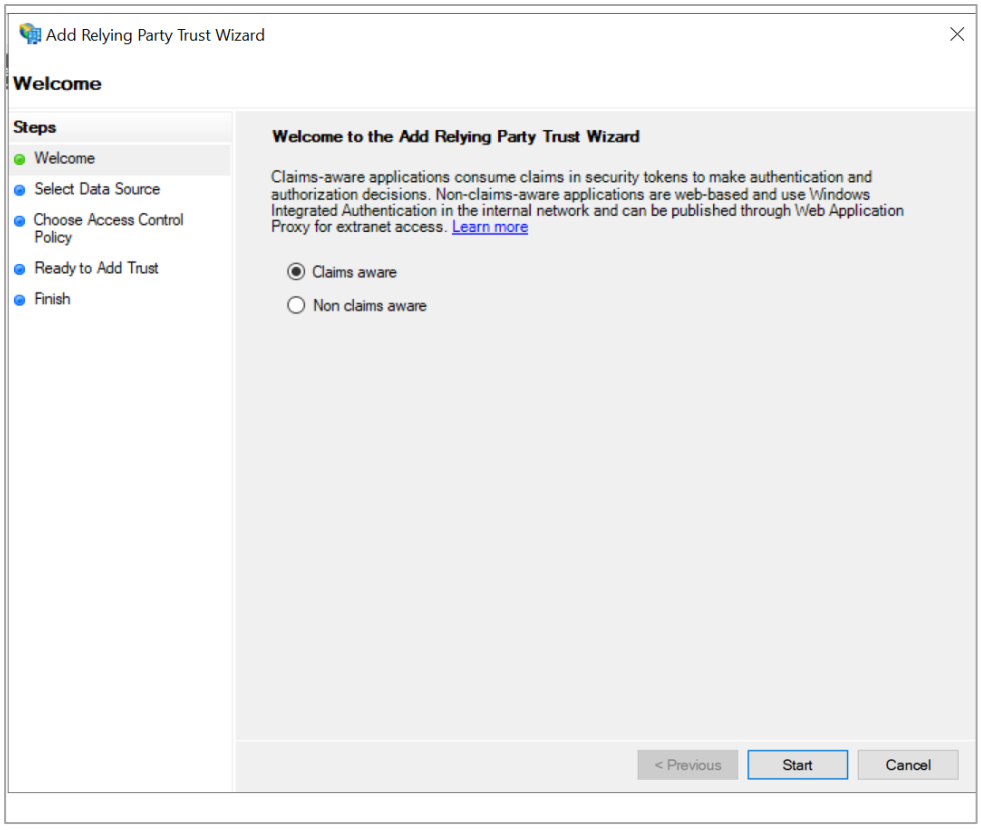
3.6 Configuring Windows ADFS with DLO

In DLO Server Domain's ADFS machine, launch ADFS Manager and perform following steps –

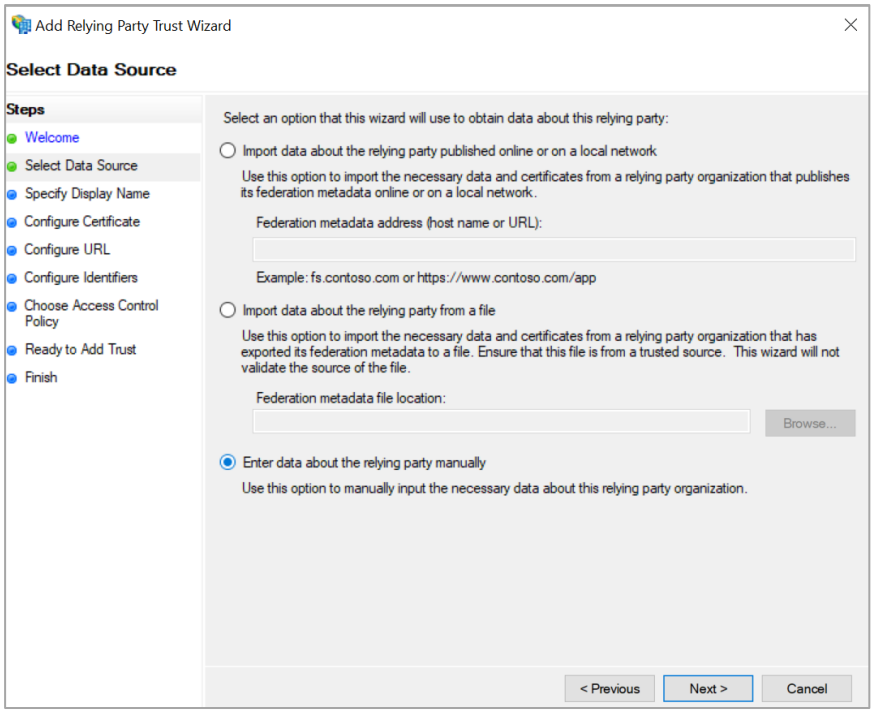
1. Open Server ADFS.



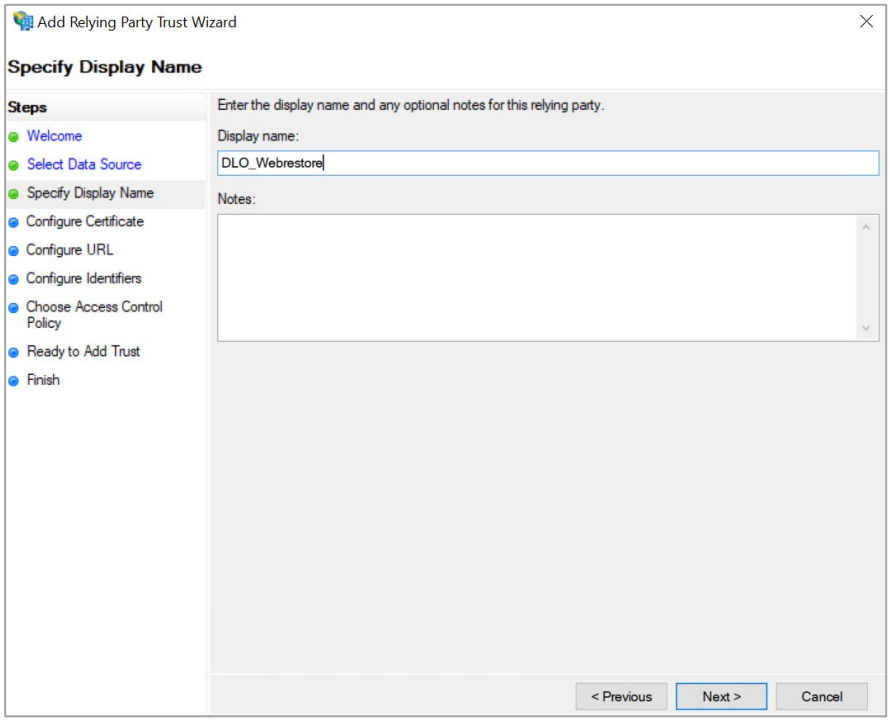
2. Navigate to **Relying Party Trusts**.
3. Click **Add** new relying party trust.
4. Select **Claims aware** and click **Start**.



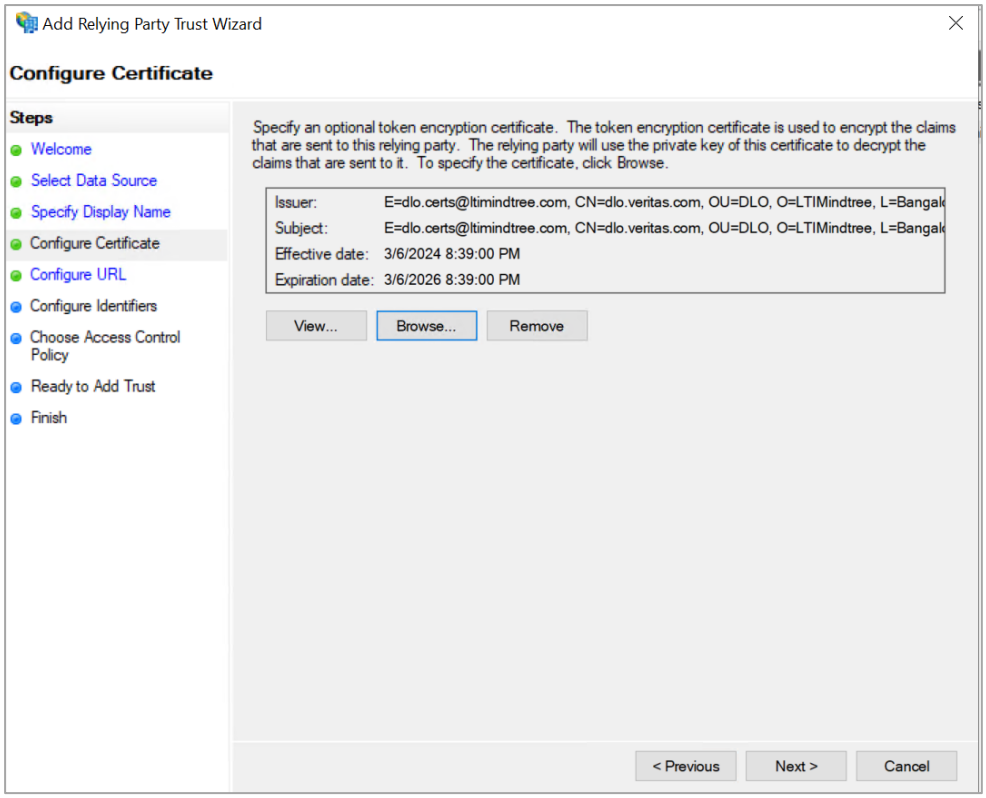
5. Select **Enter data about the relying party manually** and click **Next.**



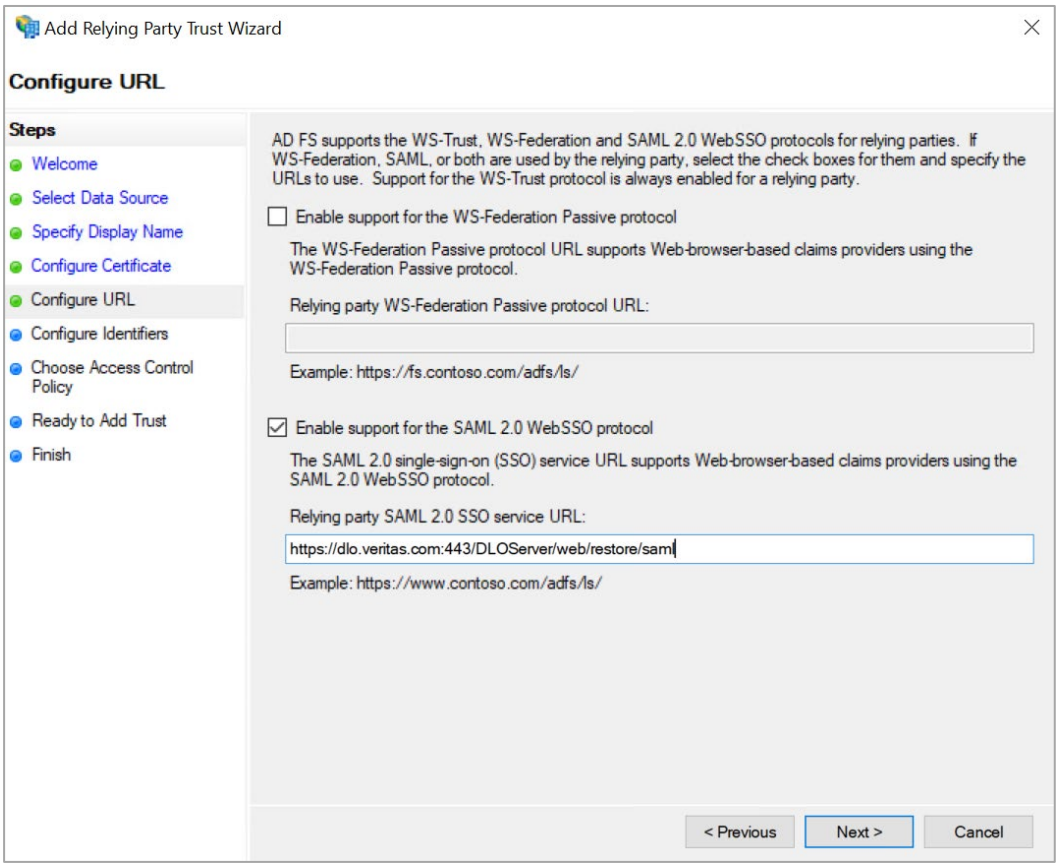
6. In **Display name** box, enter the name and click **Next**



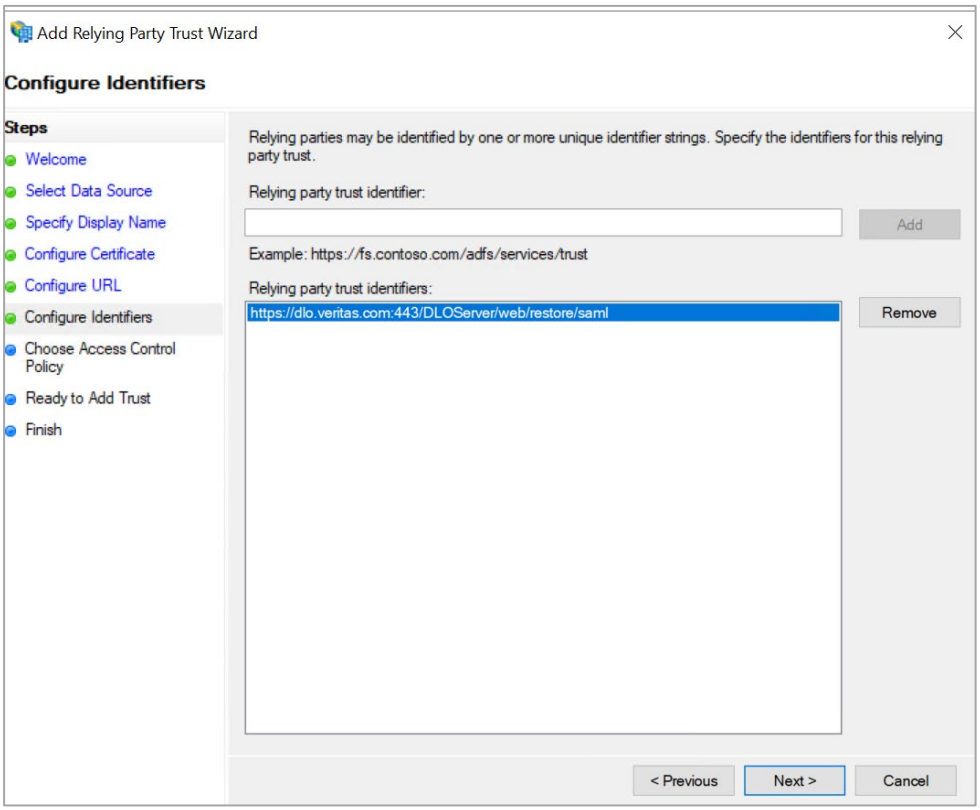
7. [Optional Step] Click **Configure Certificate**.
8. [Optional Step] Click **Browse** and select the certificate. Here, self-signed certificate or valid CA signed certificate can be used.
   Kindly note, if certificate is used in this step, then corresponding .key file should be placed at path “C:\Program Files\Veritas\Veritas DLO\IOServer\Tomcat\webapps\DLOServer\WEB-INF\classes\resource” path.



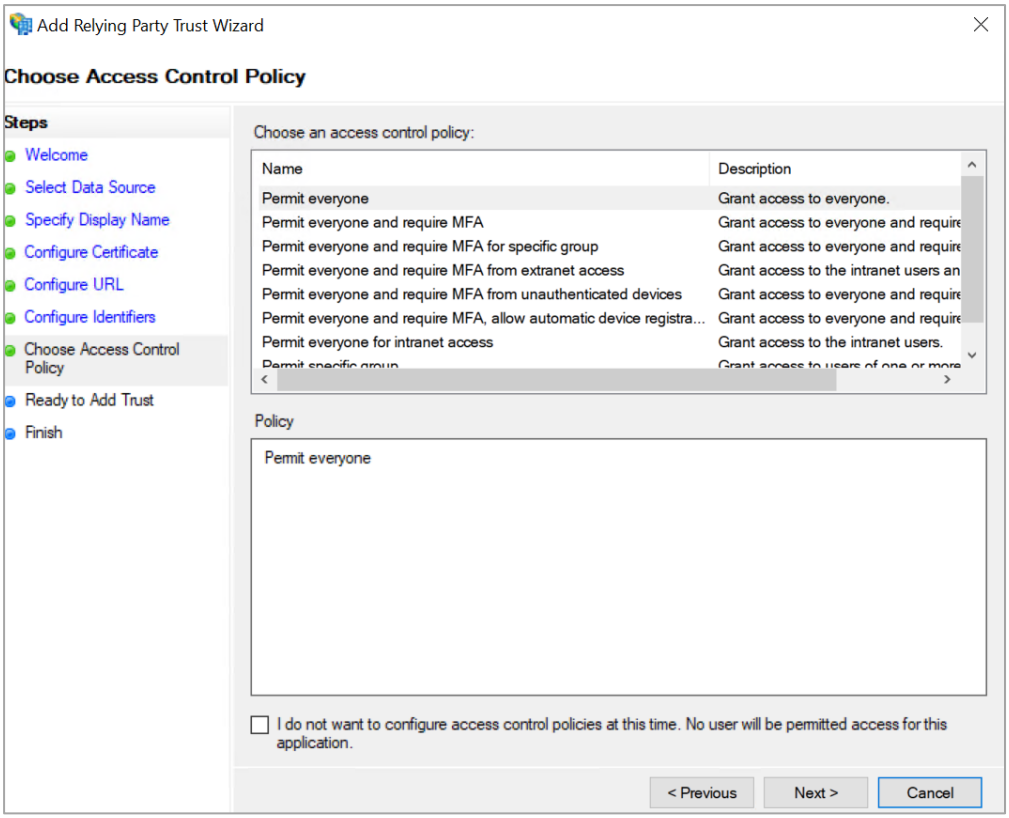
9. Click **Next.**
10. Select **Enable support for the SAML 2.0 WebSSO protocol** and enter the URL *“https://<DLO Edge Server:PortNumber>/DLOServer/web/restore/saml”* and select **Next**.



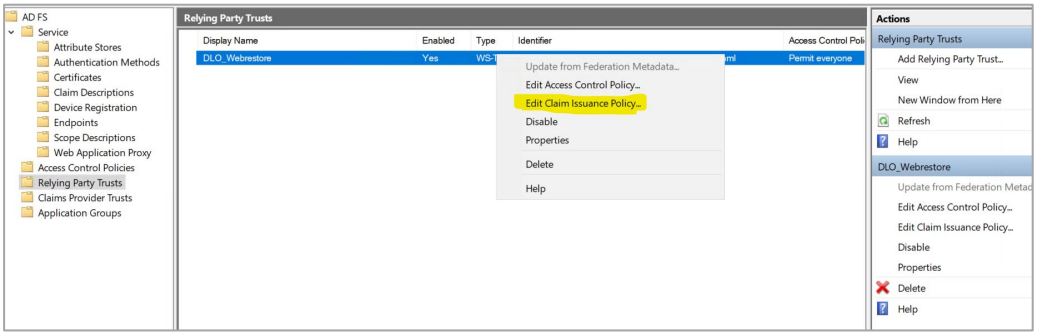
11. Click **Configure Identifiers** and enter the URL - *"https://<DLO Edge Server:PortNumber>/DLOServer/web/restore/saml"* and click **Next.**



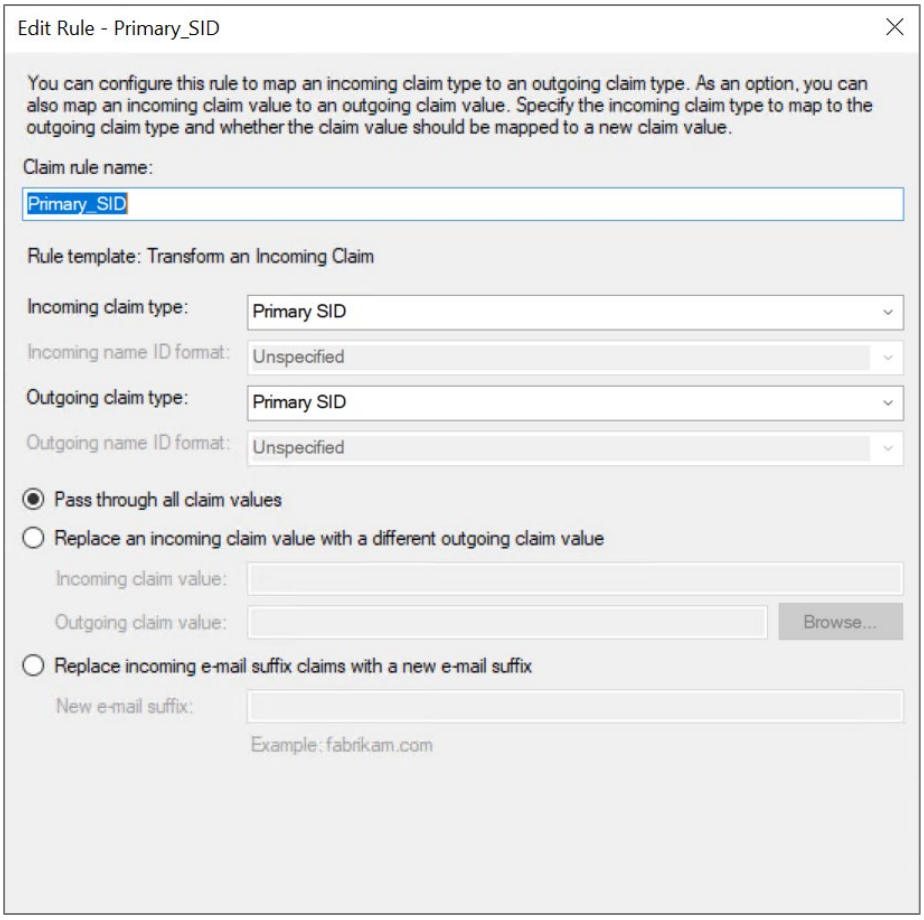
12. **Choose Access Control Policy** as per requirements and click **Next**. Note: MFA is not supported by DLO.



13. Click **Next** in '**Ready to Add Trust**' page and **Finish**.
14. Once finished, select the recently added RPT and right click to select **Edit Claim Issuance Policy.**



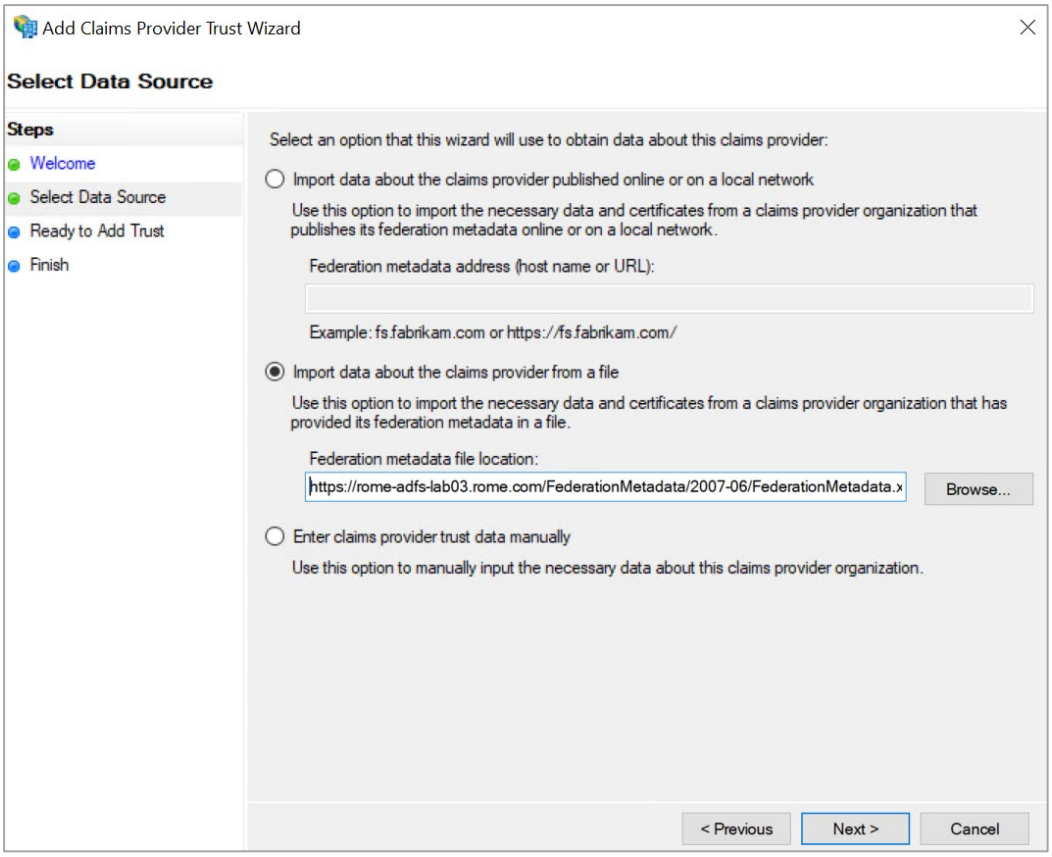
15. Click on **Edit Rule** and add a claim rule
    - Give a **Claim rule name**
    - Select "**Primary SID**" in **Incoming claim type**
    - Select "**Primary SID**" in **Outgoing claim type**



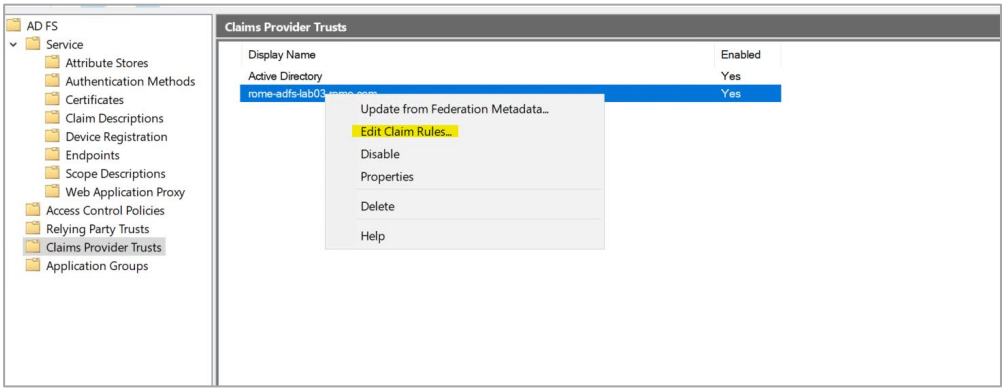
and click **OK** and **OK** to finish adding claim.

16. Now, add a Claim Provider Trusts. Select and right click the **Claim Provider Trusts** and select **Add Claim Provider Trusts**.
17. In **Claim Provider Trust Wizard**, on the welcome page click **Start.**
18. In **Select Data Source** page, select **Import data about the claims provider from a file** option and enter Client domain's ADFS metadata endpoint URL.

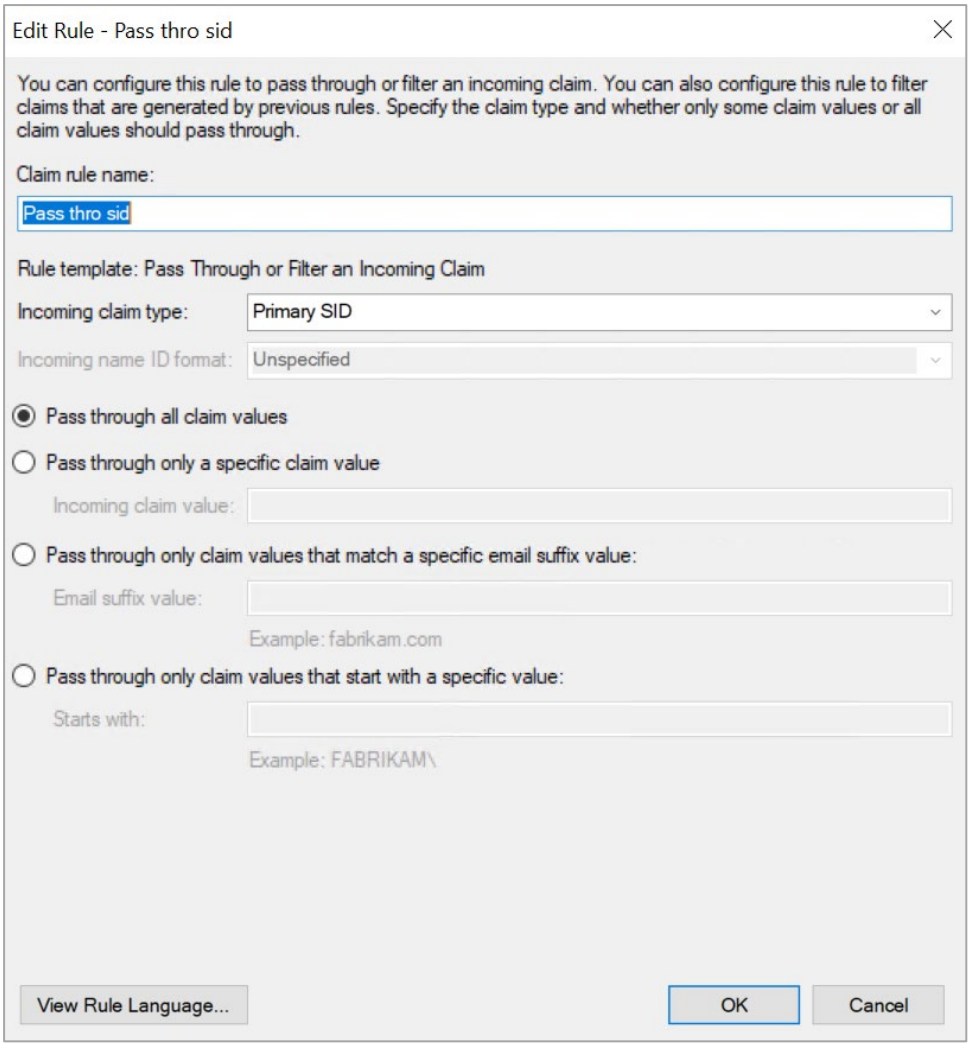
    To get Client domain's ADFS metadata endpoint URL, go to Client ADFS Server machine and launch ADFS Manager, expand Service -> Endpoint and pick URL extension from Metadata section – *https://<Client ADFS Server>/ederationMetadata/2007-06/FederationMetadata.xml*



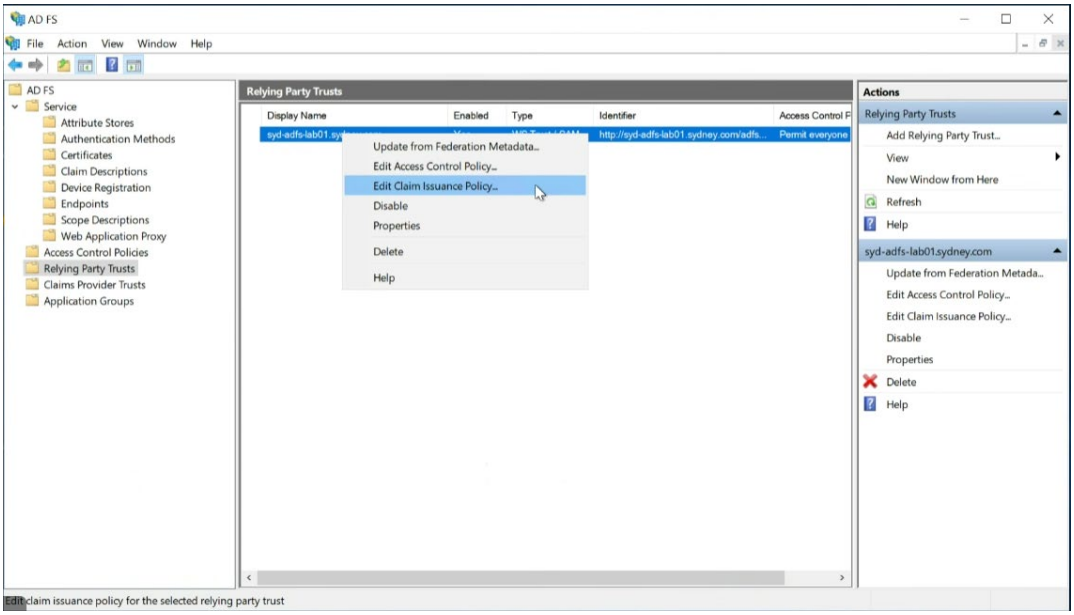
19. Click **Next** and in **Ready to Add Trust** Page click **Next** to finish adding the claim trust provider.
20. Once claim trust provider is added, then select it and right click to select **Edit Claim Rules**.



21. Select **Edit Rule** button. In **Edit Rule** Page select **Pass through all claim values** radio button and select **Primary SID** in **Incoming claim type** drop down and provide some name in **Claim rule name** field and click **OK** and **OK** again to save.

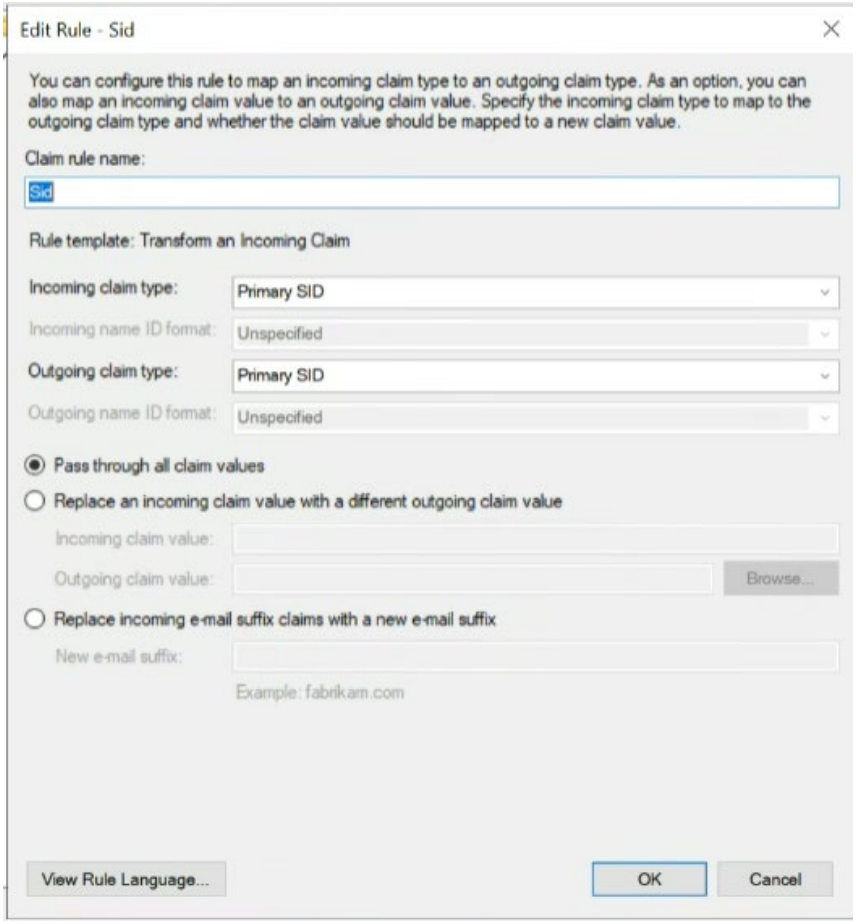


22. Login to **Client ADFS machine**, launch ADFS Management Console.
23. Navigate to **Relying Party Trust**. Select and Right click Server ADFS entry and select **Edit Claim Issuance Policy**.

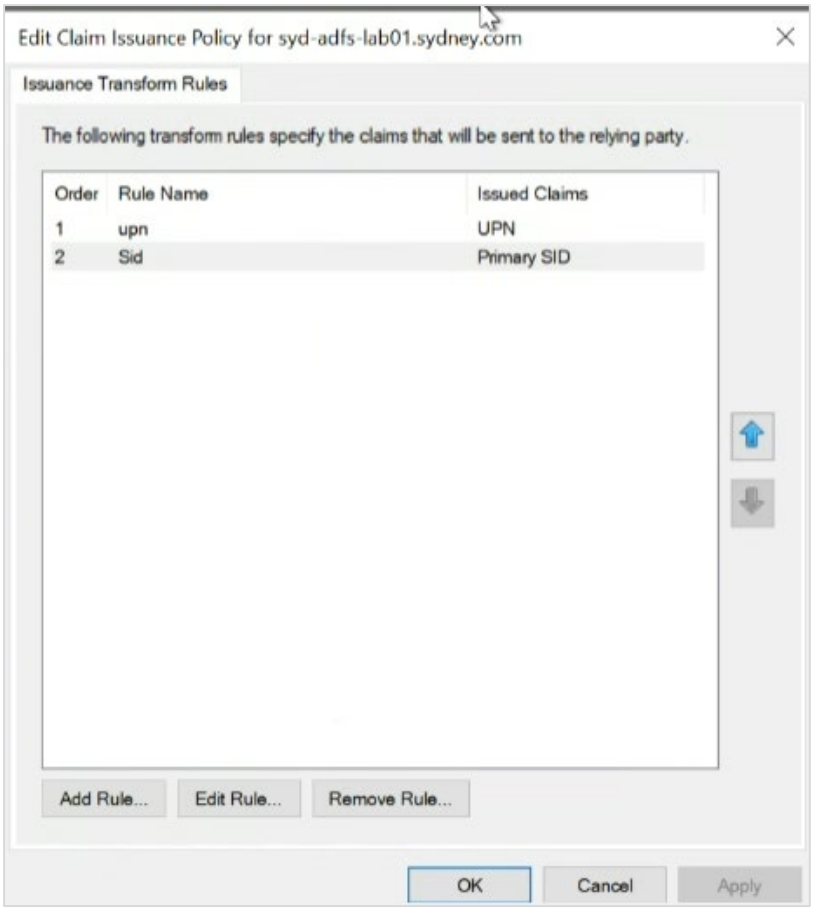


24. Click on **Edit Rule** and add a claim rule

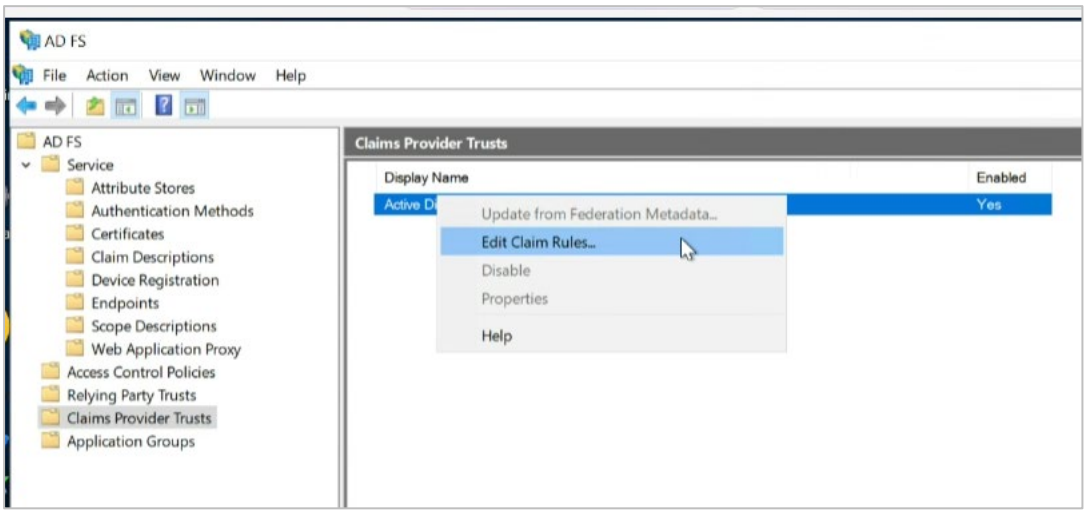
- Give a **Claim rule name**
- Select “**Primary SID**” in **Incoming claim type**
- Select “**Primary SID**” in **Outgoing claim type**



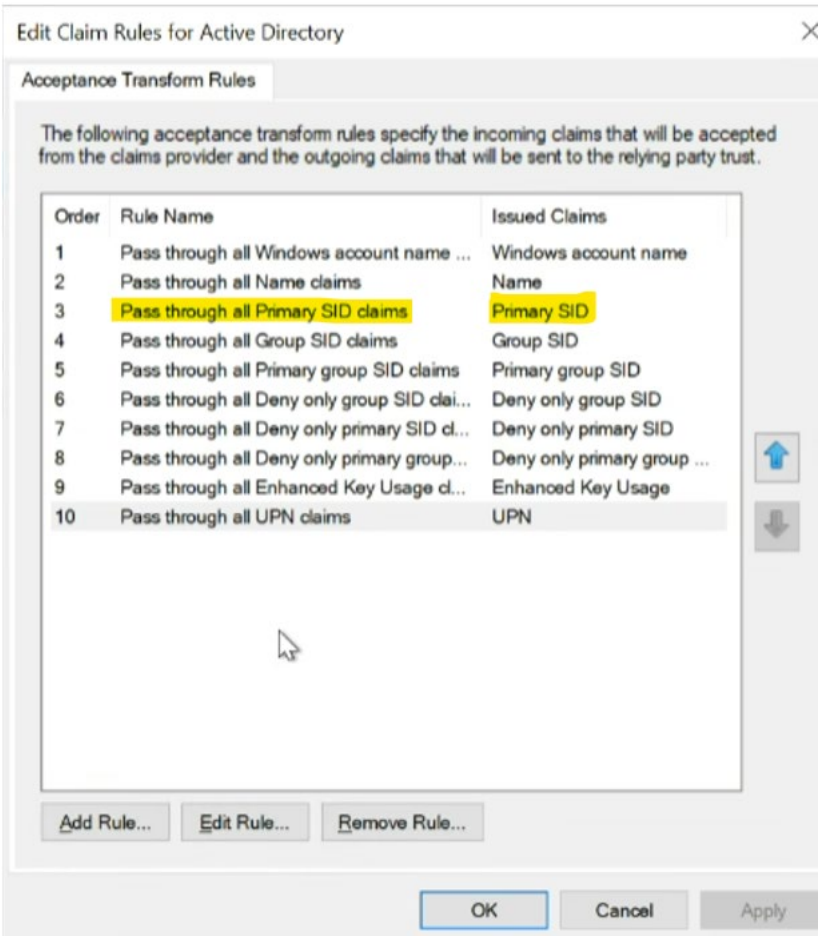
and click **OK** and **OK** again to finish adding the claim.



25. Now, go to **Claim Provider Trusts** and make sure **Active Directory** is enabled. Select **Active Directory** and right click to select **Edit Claim Rules**.



26. In **Edit Claim Rules** page, make sure **Pass through all Primary SID claims** is present.


Edit Claim Rules for Active Directory
Acceptance Transform Rules
The following acceptance transform rules specify the incoming claims that will be accepted from the claims provider and the outgoing claims that will be sent to the relying party trust.
Order
Rule Name
Issued Claims
1 Pass through all Windows account name ... Windows account name
2 Pass through all Name claims Name
3 Pass through all Primary SID claims Primary SID
4 Pass through all Group SID claims Group SID
5 Pass through all Primary group SID claims Primary group SID
6 Pass through all Deny only group SID clai... Deny only group SID
7 Pass through all Deny only primary SID cl... Deny only primary SID
8 Pass through all Deny only primary group... Deny only primary group ...
9 Pass through all Enhanced Key Usage cl... Enhanced Key Usage
10 Pass through all UPN claims UPN
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply

3.7 Adding AUA and Launching DLO Agent

1. Login to DLO Server machine and launch DLO Administration Console.
2. Navigate to **Setup** page, select **Automated User Assignment** and right click to select **New User Assignment**.
3. In New Automated User Assignment window, make sure in **Domain** drop down default value '**All Domain**' is selected and in **Group** drop down default value **'All group in this domain'** is selected.
4. Go to '**DLO->Profiles**' from settings tree list and make sure the profile is 'BOI Enabled'.
5. If profile has 'Enable Dedupe' selected then ensure the dedupe storage location is configured for deduplication file storage.
6. In '**Settings -> DLO -> Storage Location'**, ensure the storage location is configured, and Edge-IO Server is tagged.
7. Once Edge-IO Server is tagged to storage location then ensure in the DLO Edge Server **Apache httpd.conf file** below 2 lines are present.

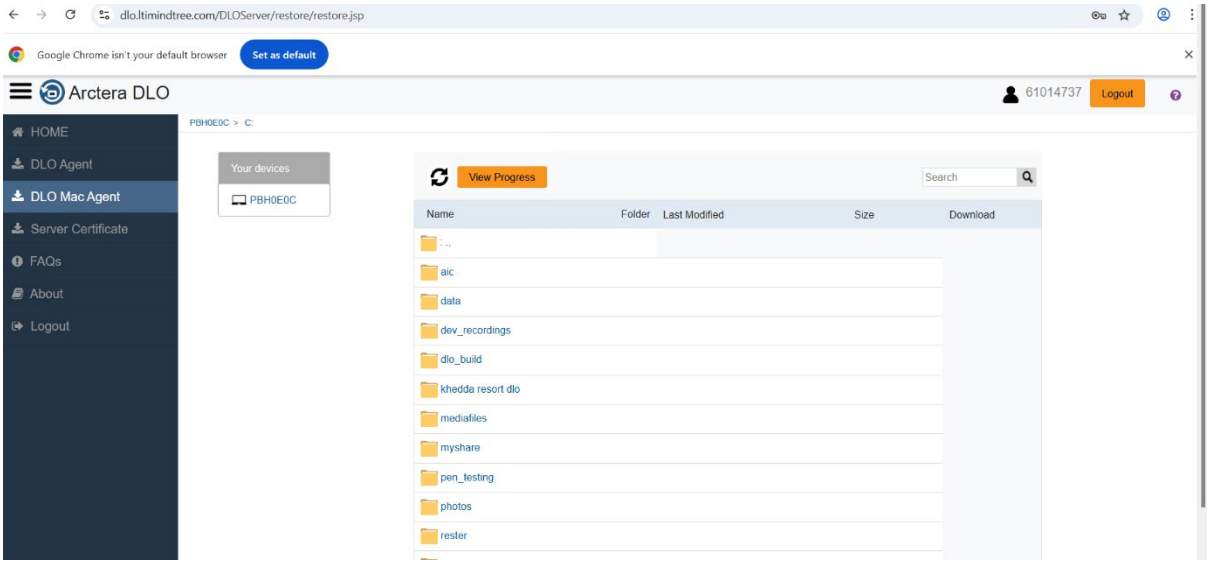
   ProxyRequests On
   AllowCONNECT 443

   Path in DLO Edge Server Machine: *C:\Program Files\Apache Software Foundation\Apache24\Conf\httpd.conf*

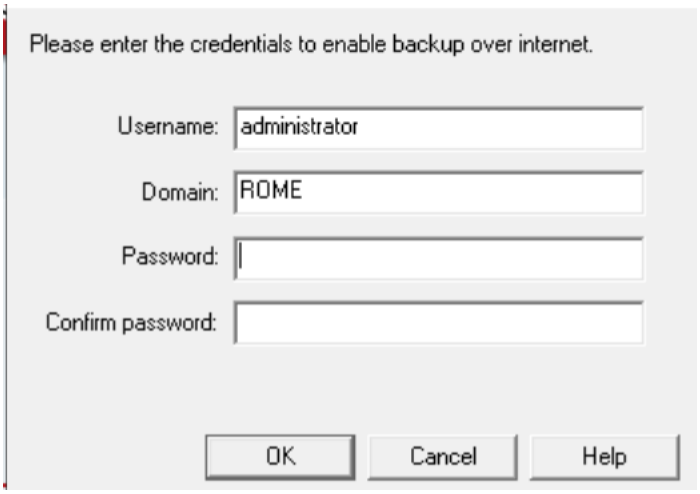
```
<VirtualHost 10.60.138.91:443>
SSLEngine On
KeepAlive On
KeepAliveTimeout 300
MaxKeepAliveRequests 0
#JkWorkersFile "C:/Program Files/apache-http/conf/worker.properties"
#JkLogFile logs/mod_jk.log
#JkLogLevel info
JkMount /DLOServer/restore/* WebRestoreLoadBalancer
JkMount /DLOServer/web/* WebRestoreLoadBalancer
JkMount /DLOServer/rest1/ioserver/getIOServerName/ DLOLoadBalancer
JkMount /DLOServer/rest1/ioserver/getEdgeServerDetails/ DLOLoadBalancer
JkMount /DLOServer/rest1/DefaultIOServer/* DefaultIOServer
JkMount /DedupeServer/rest/LocalDedupe/* LocalDedupe
JkMount /DedupeServer/rest/dedupeManager/* LocalDedupe

SSLCertificateFile "conf\\\SSL\\\SERVER.CRT"
SSLCertificateKeyFile "conf\\\SSL\\\SERVER.KEY"

ProxyRequests On
AllowCONNECT 443
</VirtualHost>
```

*Here, port 443 is used as static port for DLO Edge Server to communicate with DLO Client Domain's ADFS Server. This port can be changed if the user desires to use a different port.

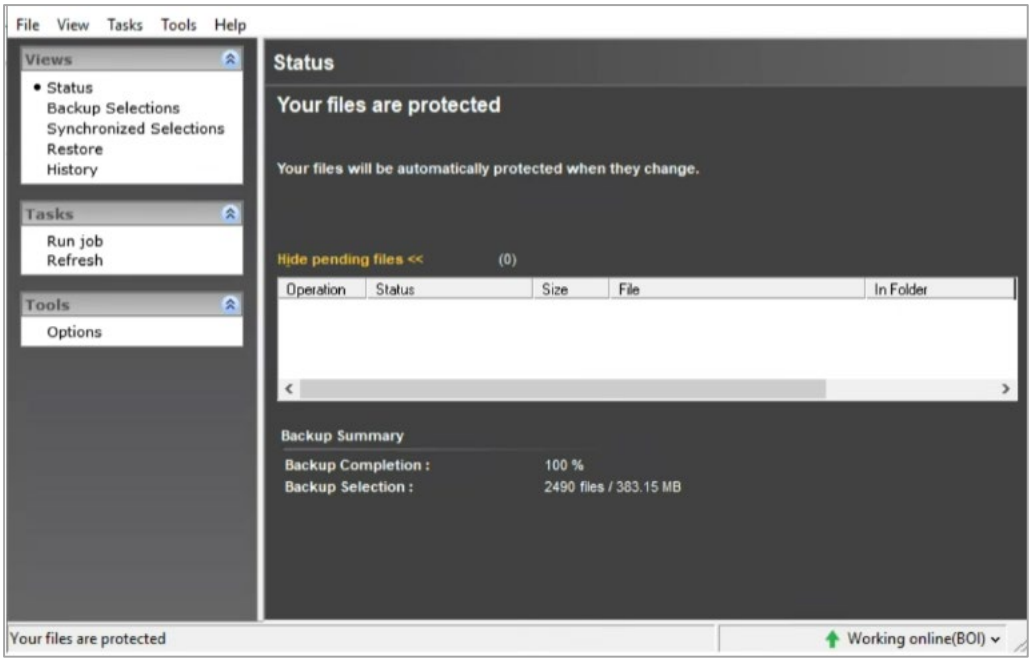
8. Now, go to the desktop machine present in DLO Client domain and access DLO Web Restore URL from browser.
   DLO Web restore URL: *https://<DLO Edge Server:443>/DLOServer/restore/login.jsp*



9. Login to a valid desktop machine with logged-in profile user and click **Download DLO Agent** present in left menu option.
10. Once **DLOAgent.zip** file is downloaded, then unzip the downloaded bundle and run **setup.exe** file to install DLO Agent.
11. Once DLO Agent is installed, launch it from Windows Start menu option.
12. A DLO BOI (Backup Over Internet) window will appear prompting for login credential. Provide login credentials to start the DLO Agent.



13. Now, DLO Agent will be launched, and backup will be automatically initiated.


File View Tasks Tools Help
Views
Status
Backup Selections
Synchronized Selections
Restore
History
Tasks
Run job
Refresh
Tools
Options
Status
Your files are protected
Your files will be automatically protected when they change.
Hide pending files <<
(0)
Operation
Status
Size
File
In Folder
Backup Summary
Backup Completion :
100 %
Backup Selection :
2490 files / 383.15 MB
Your files are protected
Working online(BOI)

4. Supportability

- DLO ADFS solution supports only one isolated client domain.
- DLO ADFS solution supports only SAML 2.0 protocol.

5. Limitations

- MFA (Multi Factor Authentication) for ADFS is not supported by DLO.
- DLO ADFS solution will not support direct adding of Client domain user.
- DLO ADFS solution will not support adding of Client Domain and Client Domain Group under AUA (Automated User Assignment). Here, ‘All Domain’ and ‘All Group’ should be added as AUA entry.
- DLO ADFS solution will not support AD object adding in AUA using LDAP protocol.