Report: Active Directory Federation (ADFS & SSO)

1. Introduction

Active Directory Federation Services (ADFS) is a robust identity federation solution that enables organizations to provide secure, seamless Single Sign-On (SSO) access to both internal and external applications. ADFS leverages standard protocols such as SAML, OAuth, and WS-Federation to authenticate users across security boundaries without requiring multiple logins. This capability enhances user experience, reduces password fatigue, and improves security by centralizing authentication. Setting up ADFS with a test SSO application allows organizations to validate their federation infrastructure and ensure interoperability with various service providers. Furthermore, continuous monitoring of federation trust relationships is critical to detect misconfigurations, unauthorized changes, or suspicious activities that could compromise trust and expose the network to attacks.

2. Objective

The primary objective of this task is to install and configure Active Directory Federation Services to enable Single Sign-On for a sample application, demonstrating the functionality and benefits of federated identity management. This includes establishing secure trust relationships between the ADFS server and the test application, configuring claim rules, and validating user authentication flows. Additionally, the task seeks to implement monitoring mechanisms to track the health and security of federation trust relationships, promptly identifying anomalies such as unexpected changes, expired certificates, or failed authentications, thereby ensuring continuous trustworthiness and resilience of the federation infrastructure.

Key goals include:

- **Deploy a Fully Functional ADFS Environment**
  Set up and configure Active Directory Federation Services properly to establish a secure federation server that can handle authentication requests reliably.

- **Configure a Test SSO Application for Seamless Access**
  Integrate a sample application with ADFS to enable Single Sign-On (SSO), allowing users to authenticate once and access the application without additional logins.

- **Establish Secure Federation Trust Relationships**
  Create and maintain trust configurations between the ADFS server and the relying parties (applications), ensuring secure exchange of authentication tokens and claims.

- **Validate Authentication and Claim Rules**
  Implement and test claim rules to control user authorization and access, ensuring the correct identity attributes are passed securely to the test SSO application.

- **Monitor Federation Trust Health and Security**
  Continuously track and analyze federation trust relationships to detect anomalies such as expired certificates, unauthorized changes, or suspicious authentication failures, maintaining the integrity of the federation environment.

3. Methodology

This methodology outlines the step-by-step process followed to install and configure Active Directory Federation Services (ADFS) for a test Single Sign-On (SSO) application (Task 48), and to monitor the federation trust relationships for anomalies and security validation (Task 50). The approach is divided into two phases: the setup and configuration phase, followed by the monitoring and verification phase, ensuring a comprehensive deployment and ongoing trust health assessment.

3.1 Installation and Configuration of ADFS with Test SSO Application

The first phase focuses on setting up the ADFS infrastructure required for secure federated authentication. This involves installing the ADFS role, configuring DNS, establishing trust relationships, and validating the SSO process with a test application. Proper configuration in this phase is critical to enable seamless and secure user authentication across services.

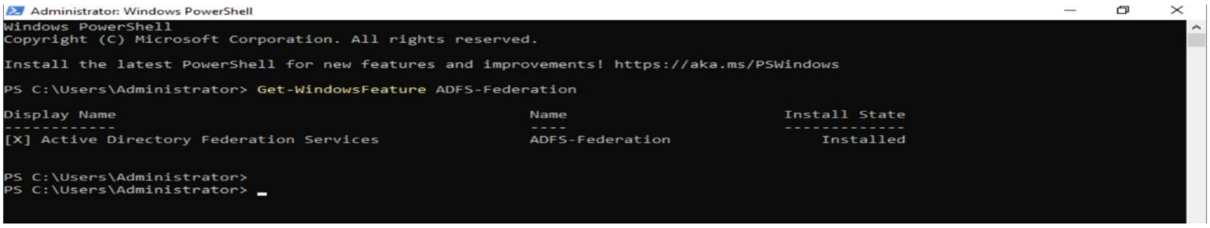
- **Install ADFS Role**

  Installing the ADFS role enables the server to function as a federation server, which handles claims-based authentication and enables SSO.

  Navigation:

  Open Server Manager > Manage > Add Roles and Features > Select Active Directory Federation Services under Server Roles > Complete the wizard and install.

  (Confirm the Installation.)



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> Get-WindowsFeature ADFS-Federation

Display Name                                            Name                       Install State
------------                                            ----                       -------------
[X] Active Directory Federation Services                 ADFS-Federation                Installed

PS C:\Users\Administrator>
PS C:\Users\Administrator> _
```

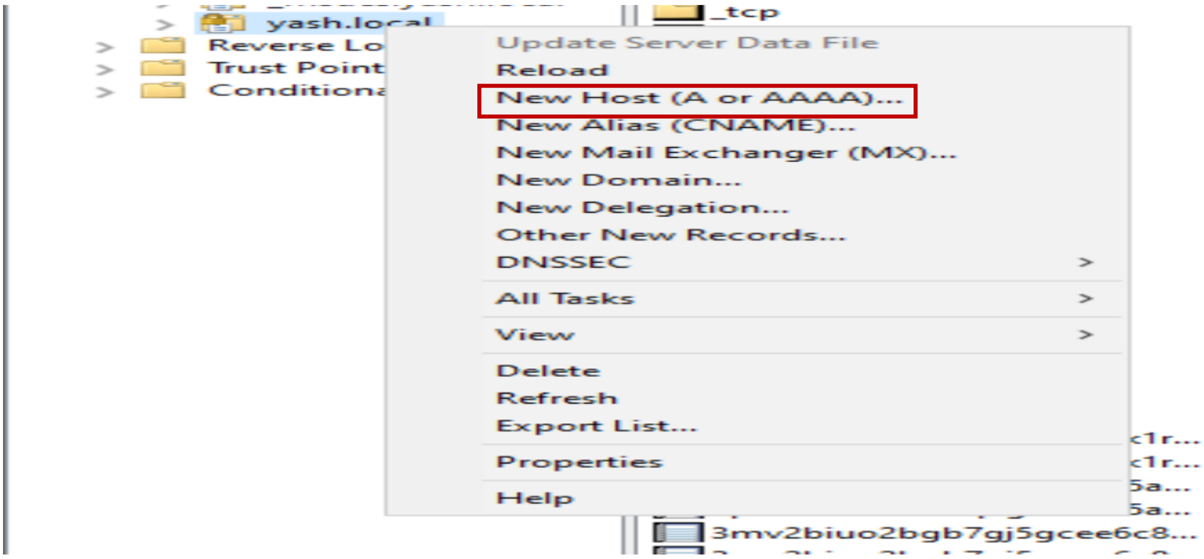
- **Configure DNS Resolution for ADFS Service**

  Proper DNS configuration allows clients and services to resolve the ADFS service URL correctly, which is essential for authentication requests to reach the federation server.

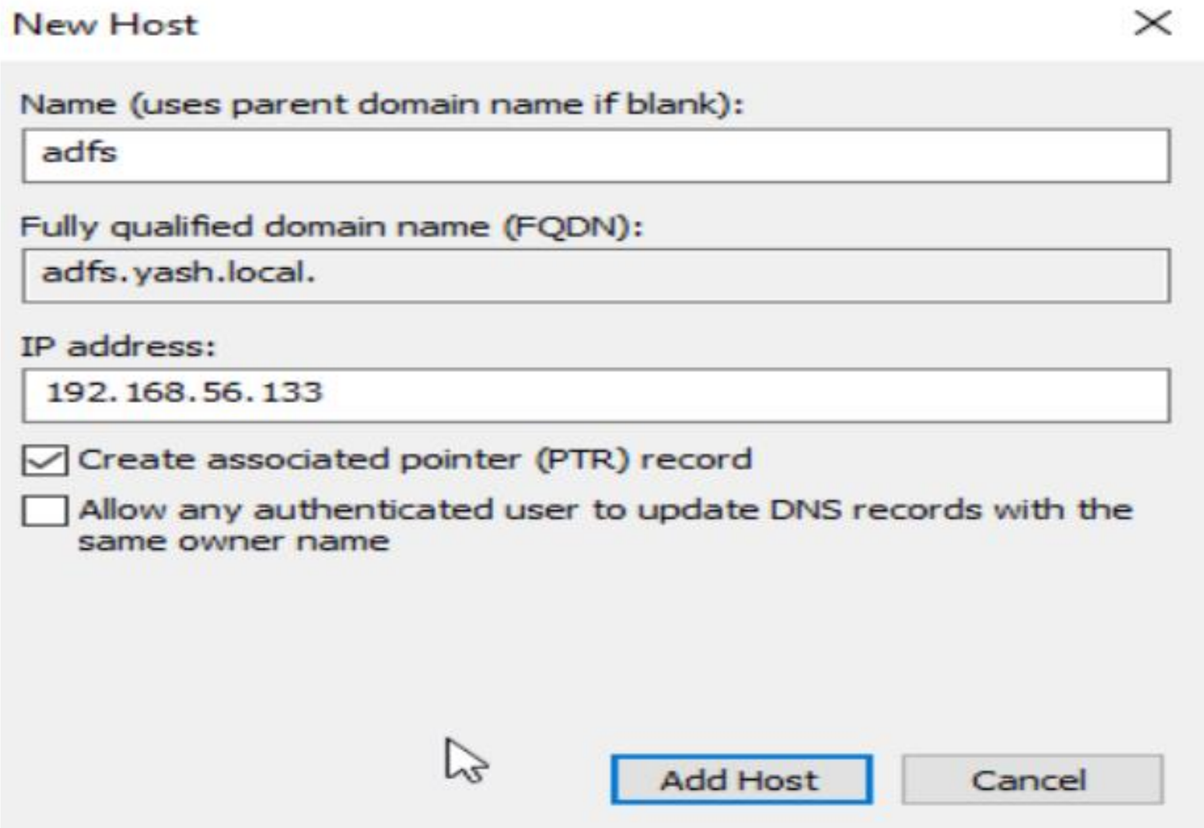
  Navigation:

  On the DNS server, open **DNS Manager** > Create a new **A (Host) record** for the ADFS service URL pointing to the ADFS server's IP address.

  (Creating a new host.)



(Configure DNS Resolution.)



Name (uses parent domain name if blank):
adfs

Fully qualified domain name (FQDN):
adfs.yash.local.

IP address:
192.168.56.133

☑ Create associated pointer (PTR) record

☐ Allow any authenticated user to update DNS records with the same owner name

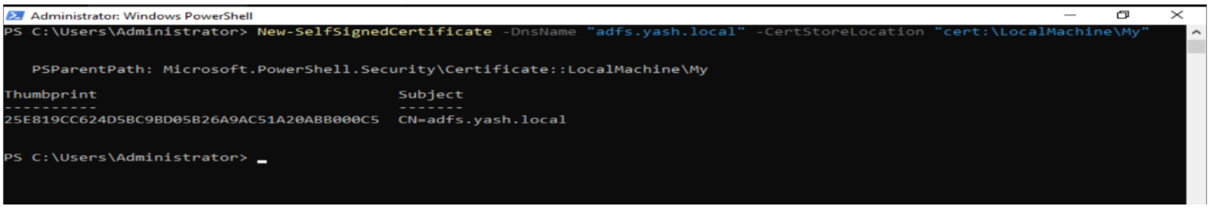
- **Configure ADFS Service**

  This sets up the federation service with the appropriate service name and certificates, establishing the foundation for secure federated authentication.

  Navigation:

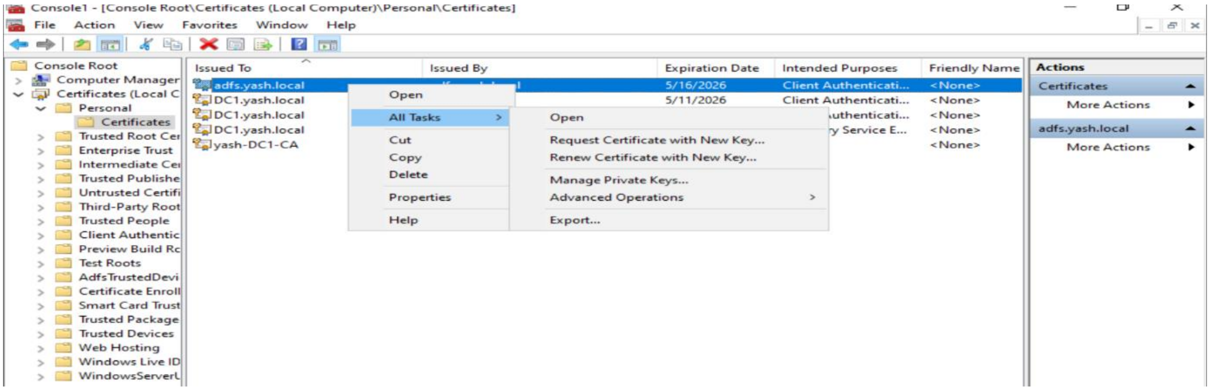
  Open the **AD FS Management Console** > Configure the federation service by specifying the federation service name and SSL certificate.

  (Genrate a SelfSignedCertificate.)



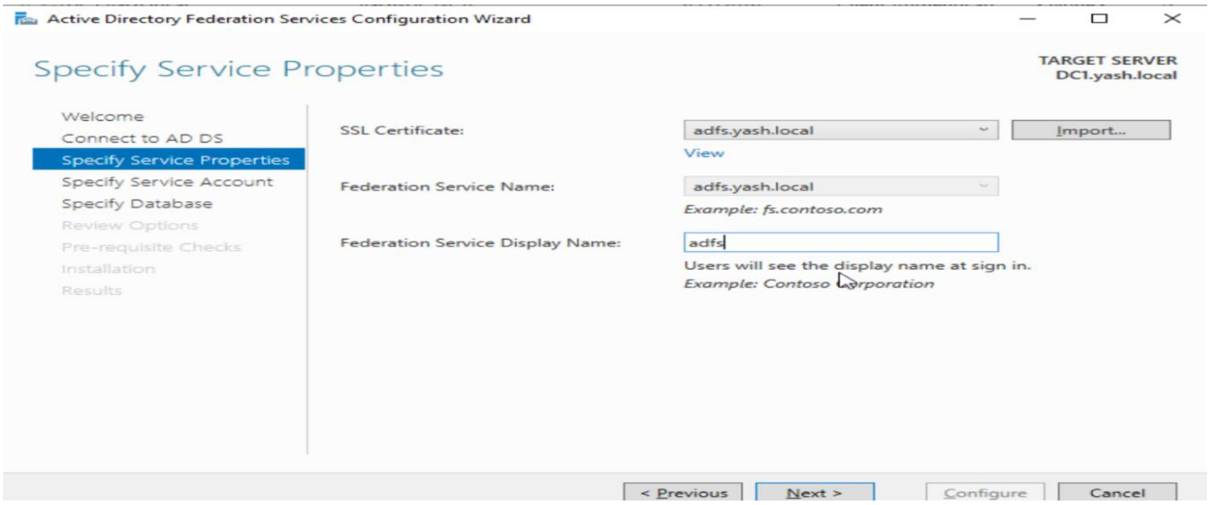
```
PS C:\Users\Administrator> New-SelfSignedCertificate -DnsName "adfs.yash.local" -CertStoreLocation "cert:\LocalMachine\My"


   PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint                                Subject
----------                                -------
25E819CC624D5BC9BD05B26A9AC51A20ABB000C5  CN=adfs.yash.local


PS C:\Users\Administrator> _
```

(Export the certificate later used in configuration.)



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
adfs.yash.local		5/16/2026	Client Authenticati...	<None>
DC1.yash.local		5/11/2026	Client Authenticati...	<None>
DC1.yash.local			uthenticati...	<None>
DC1.yash.local			y Service E...	<None>
yash-DC1-CA				<None>

(Import the certificate here.)



SSL Certificate: adfs.yash.local

Federation Service Name: adfs.yash.local

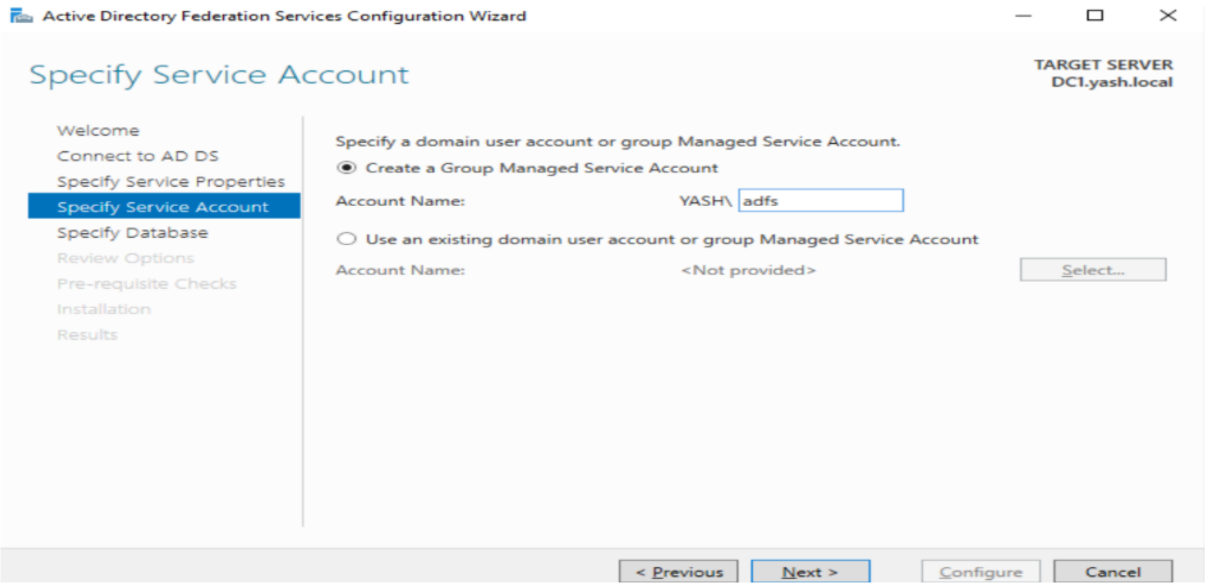
Example: fs.contoso.com

Federation Service Display Name: adfs

Users will see the display name at sign in.

Example: Contoso Corporation

(Service account created.)



Specify a domain user account or group Managed Service Account.

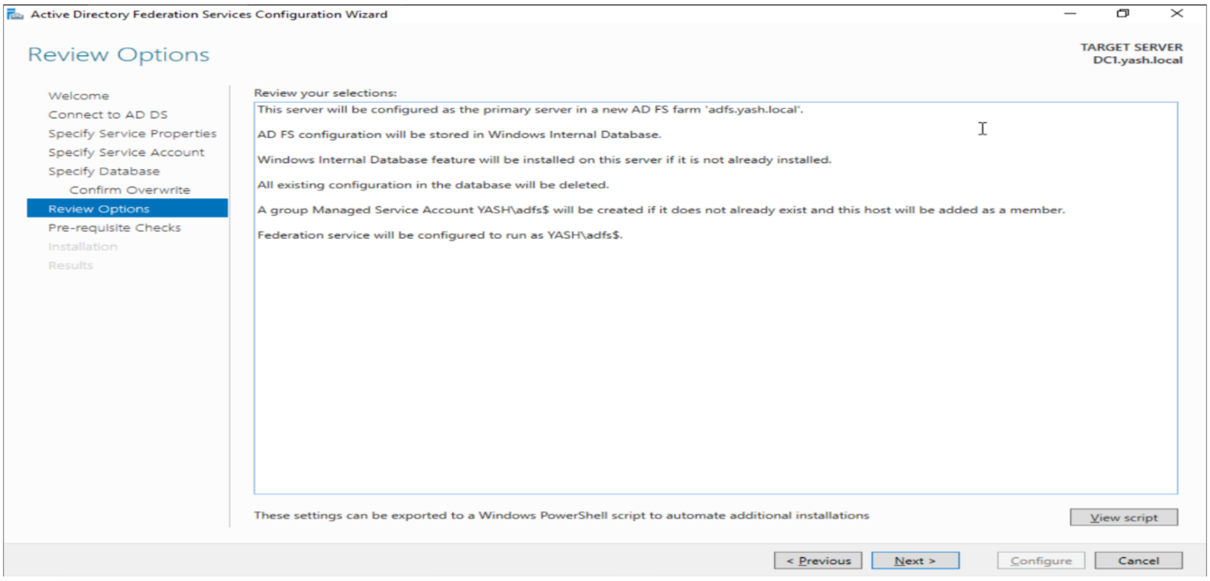
● Create a Group Managed Service Account

Account Name: YASH\ adfs

○ Use an existing domain user account or group Managed Service Account

Account Name: <Not provided>

(Review the options.)



Review your selections:

This server will be configured as the primary server in a new AD FS farm 'adfs.yash.local'.

AD FS configuration will be stored in Windows Internal Database.

Windows Internal Database feature will be installed on this server if it is not already installed.

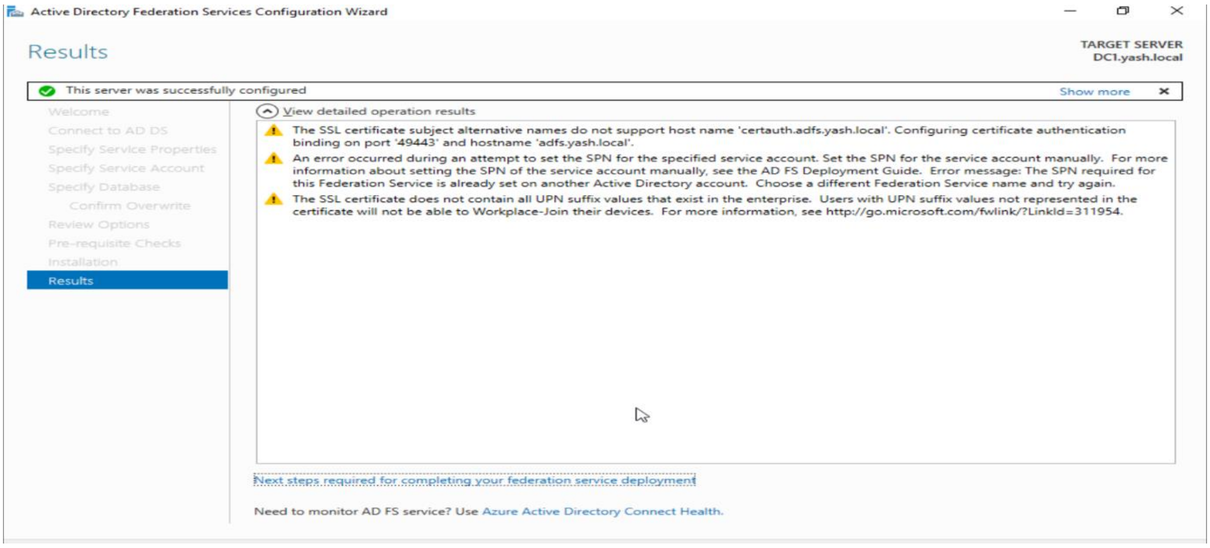
All existing configuration in the database will be deleted.

A group Managed Service Account YASH\adfs$ will be created if it does not already exist and this host will be added as a member.

Federation service will be configured to run as YASH\adfs$.

These settings can be exported to a Windows PowerShell script to automate additional installations

(Configuration Completed.)



This server was successfully configured

The SSL certificate subject alternative names do not support host name 'certauth.adfs.yash.local'. Configuring certificate authentication binding on port '49443' and hostname 'adfs.yash.local'.

An error occurred during an attempt to set the SPN for the specified service account. Set the SPN for the service account manually. For more information about setting the SPN of the service account manually, see the AD FS Deployment Guide. Error message: The SPN required for this Federation Service is already set on another Active Directory account. Choose a different Federation Service name and try again.

The SSL certificate does not contain all UPN suffix values that exist in the enterprise. Users with UPN suffix values not represented in the certificate will not be able to Workplace-Join their devices. For more information, see http://go.microsoft.com/fwlink/?LinkId=311954.

Next steps required for completing your federation service deployment

Need to monitor AD FS service? Use Azure Active Directory Connect Health.

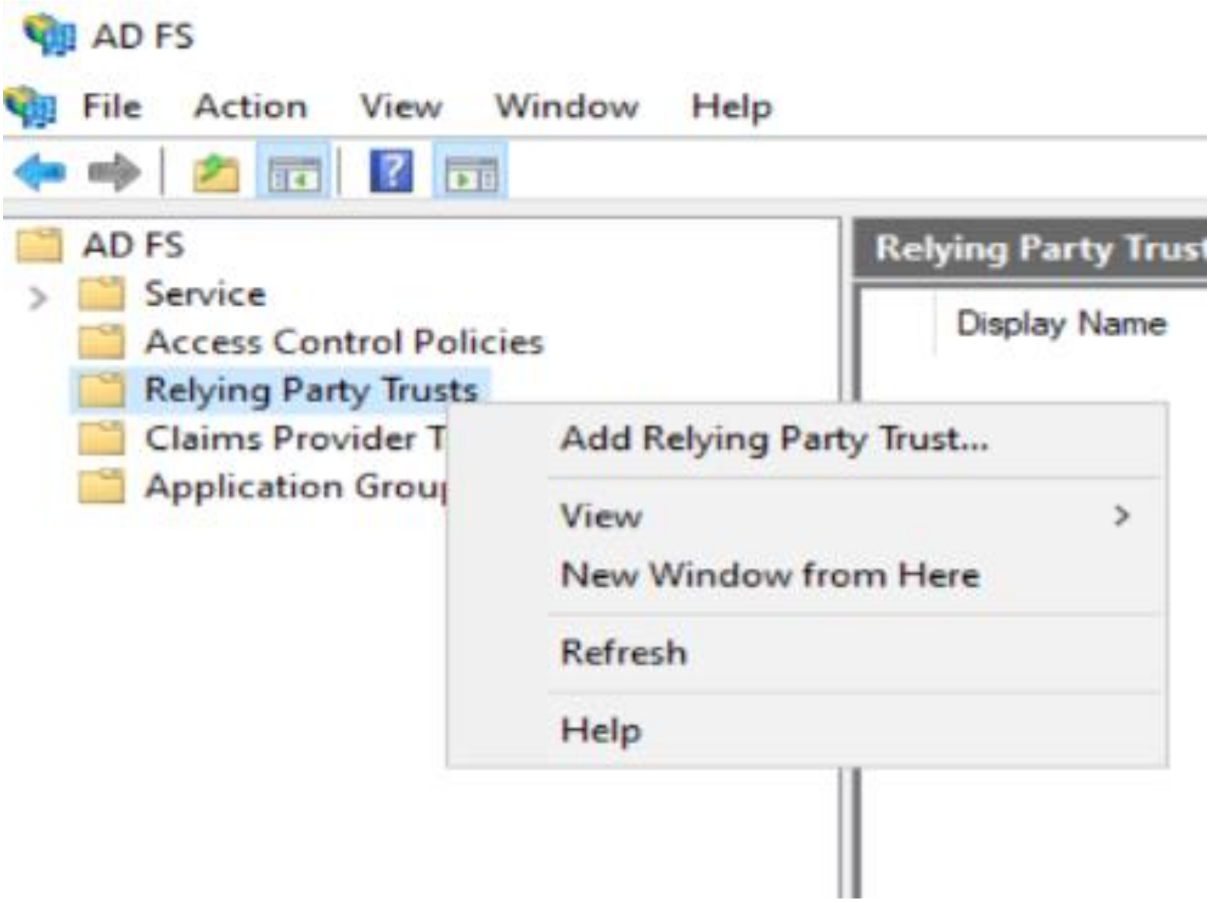
- **Add Relying Party Trust**

  This creates a trust relationship between ADFS and the test application, allowing ADFS to issue security tokens that the application will accept.

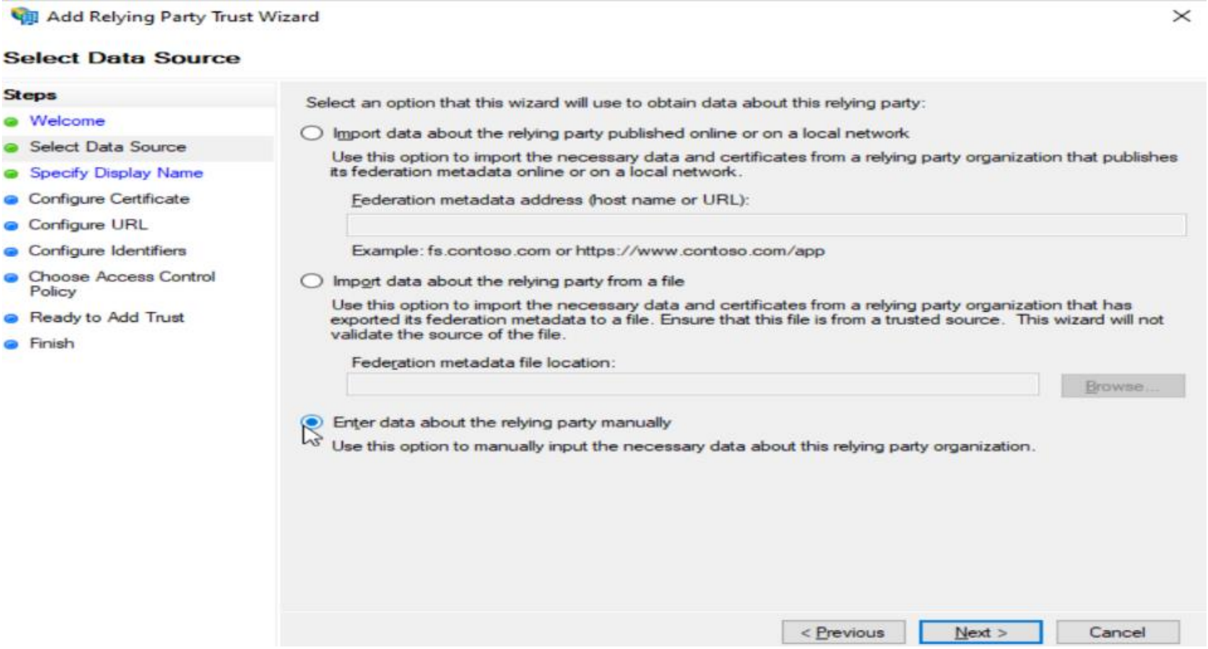
  Navigation:

  In AD FS Management, right-click Relying Party Trusts > Add Relying Party Trust > Follow the wizard to configure the test SSO application's details.

(Add a trusted relying party.)



(Selected the data source.)



Select Data Source

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

○ Import data about the relying party from a file

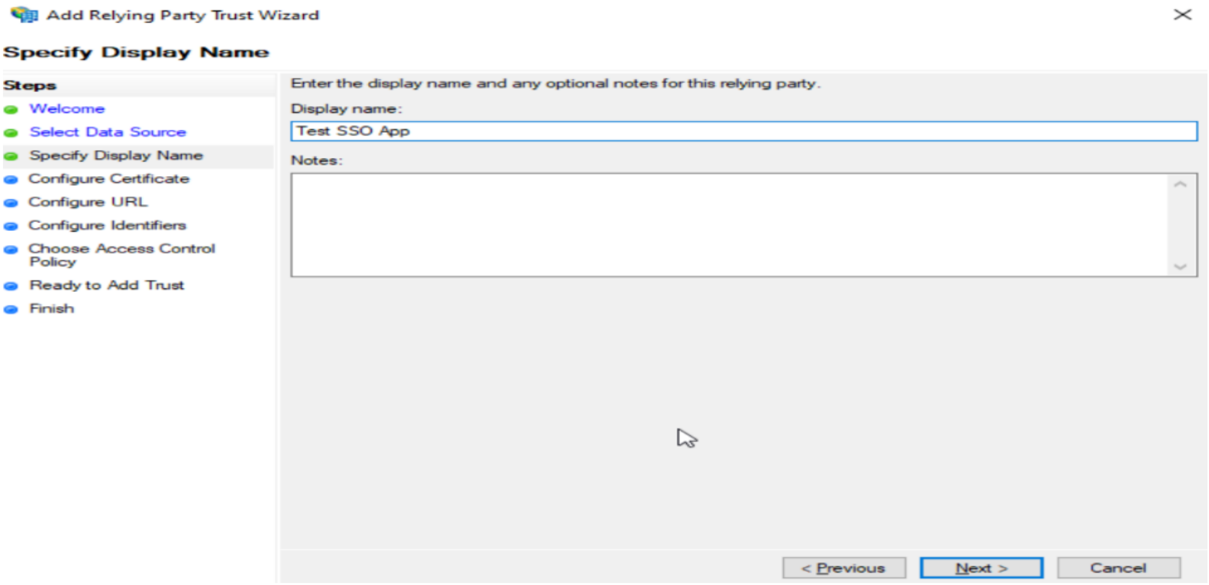
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

● Enter data about the relying party manually

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

(Named the Party)



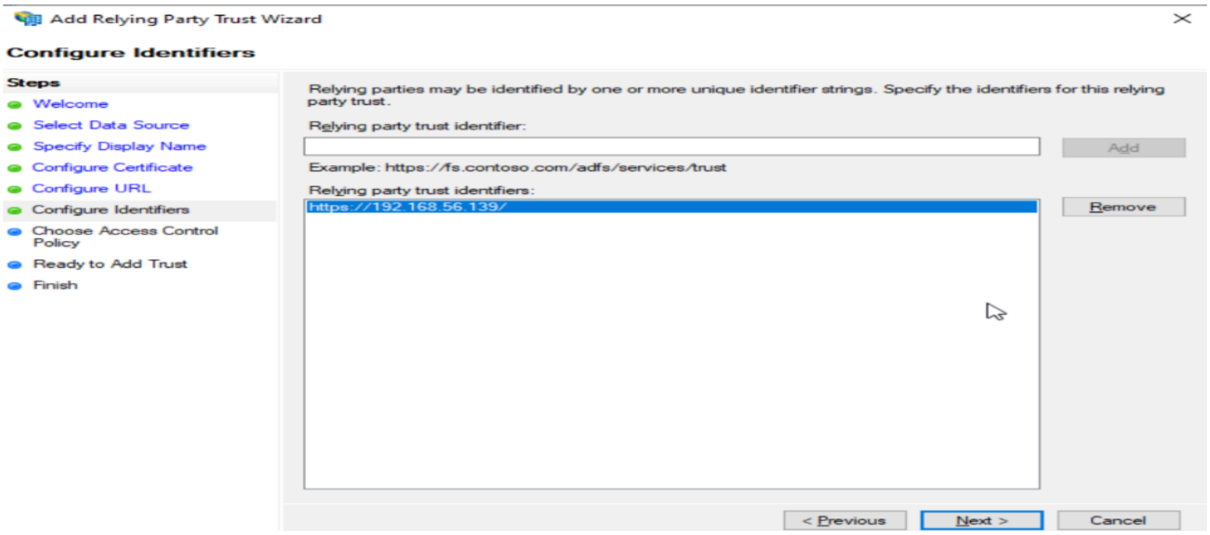
Enter the display name and any optional notes for this relying party.

Display name:

Test SSO App

Notes:

(Add identifier.)



Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

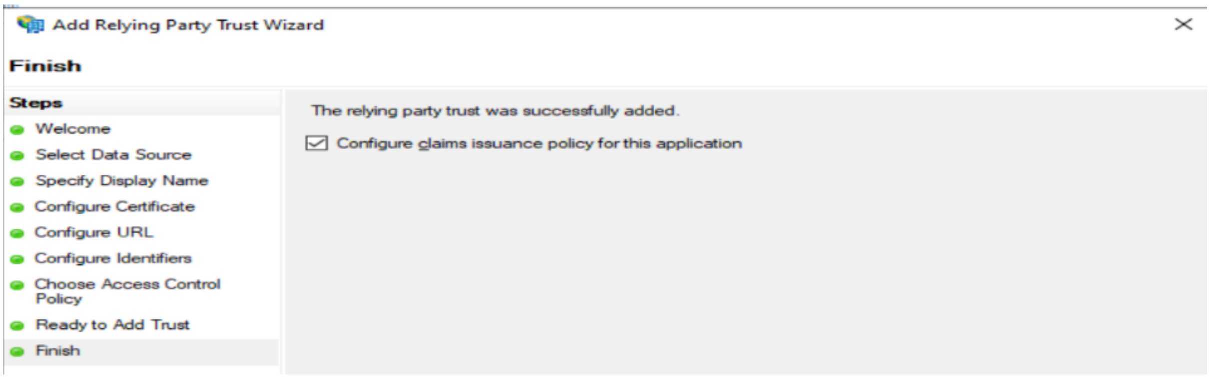
Relying party trust identifier:

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

Relying party trust identifiers:

https://192.168.56.139/

(Configuration completed)



The relying party trust was successfully added.

☑ Configure claims issuance policy for this application

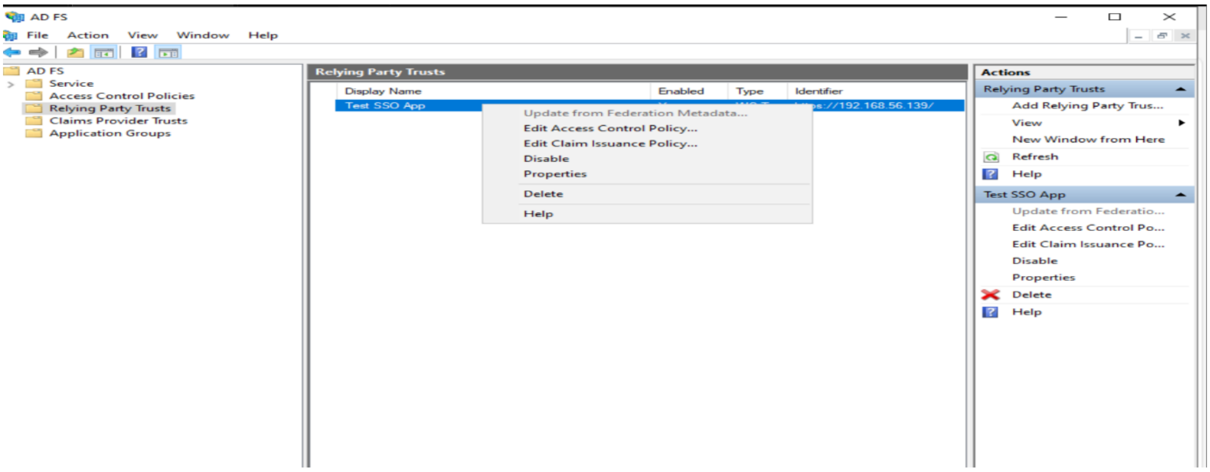
- **Configure Claim Issuance Policy**

  Claim rules define what identity information (claims) is sent to the application, controlling user access and permissions.

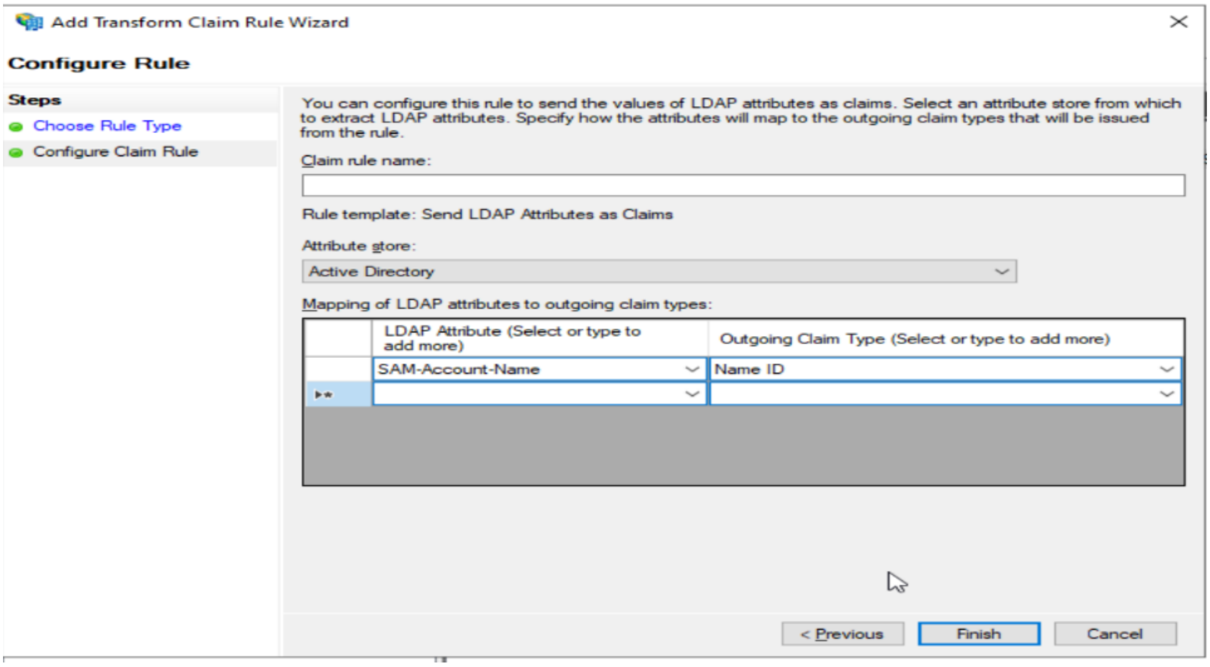
  Navigation:

  Within the newly added relying party trust, open Edit Claim Issuance Policy > Add claim rules that specify which user attributes are passed to the application.

  (Edited the claim issuance policy)



(Configured claim rule.)



Configure 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:

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

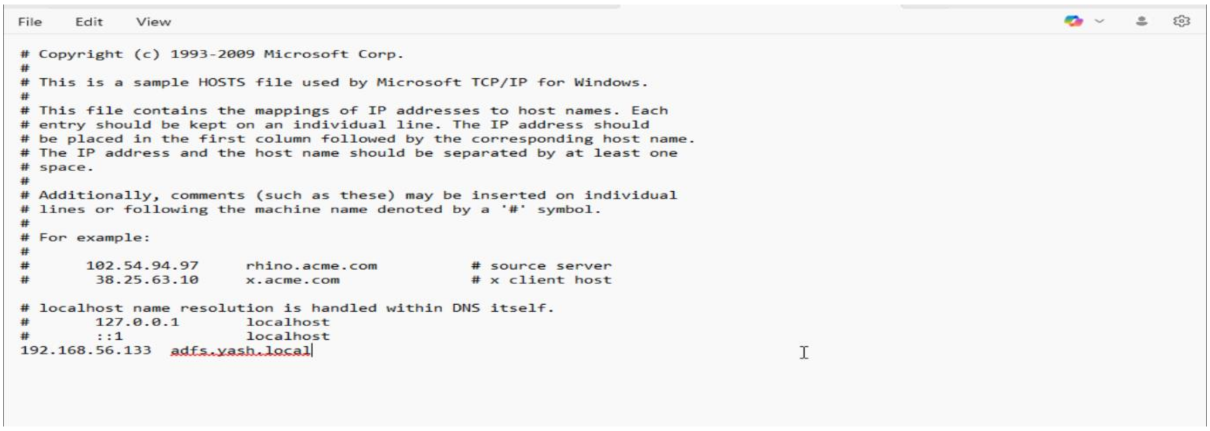
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	SAM-Account-Name	Name ID
▸*		

- **Modify Client Hosts File**

  This allows the client machine to resolve the ADFS service URL for testing, especially if DNS changes have not propagated or in isolated test environments.

  Navigation:

  On the client machine, open **Notepad** as Administrator > Edit the file at C:\Windows\System32\drivers\etc\hosts > Add an entry mapping adfs.task.local to the ADFS server's IP.



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
192.168.56.133  adfs.yash.local
```

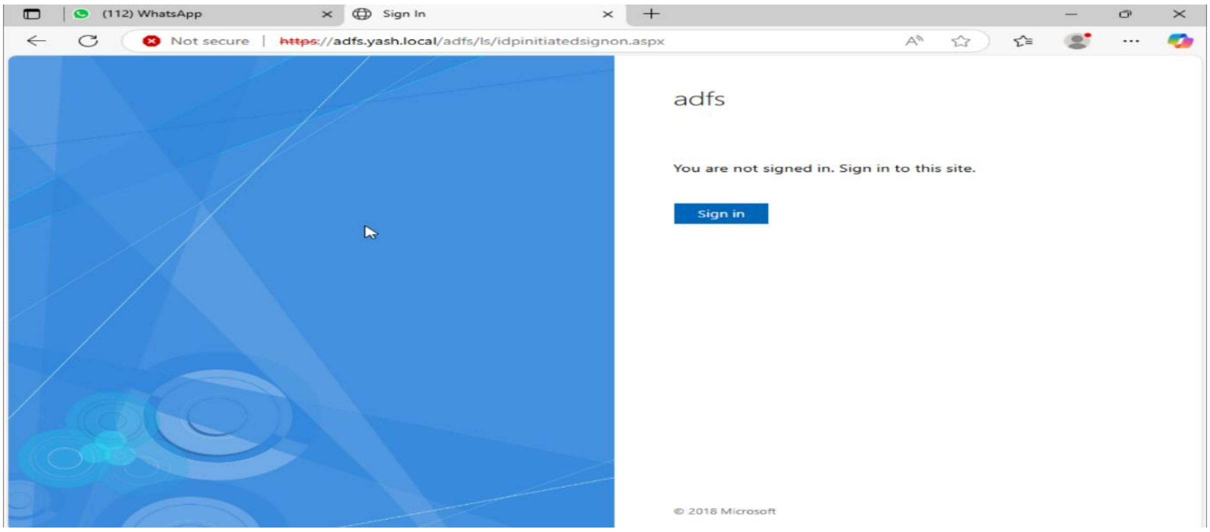
- **Verify SSO Login**

  Successful login confirms that the ADFS configuration and SSO integration are functioning correctly.

  Navigation:

  On the client, open a web browser and navigate to the test application's URL > Attempt to login using ADFS credentials.

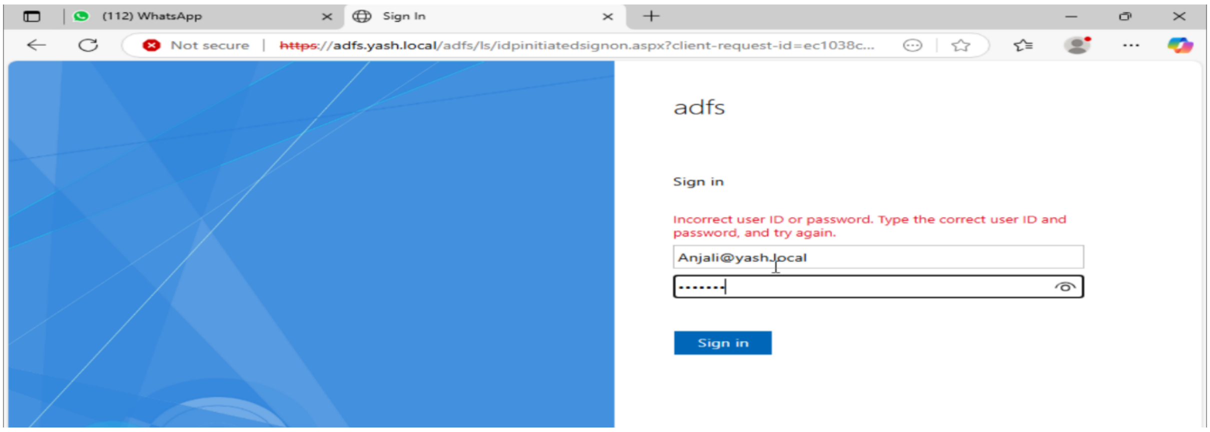
(Login page created successfully.)



adfs

You are not signed in. Sign in to this site.

(Tried login to test.)


(112) WhatsApp
Sign In
Not secure
https://adfs.yash.local/adfs/ls/idpinitiatedsignon.aspx?client-request-id=ec1038c...

adfs

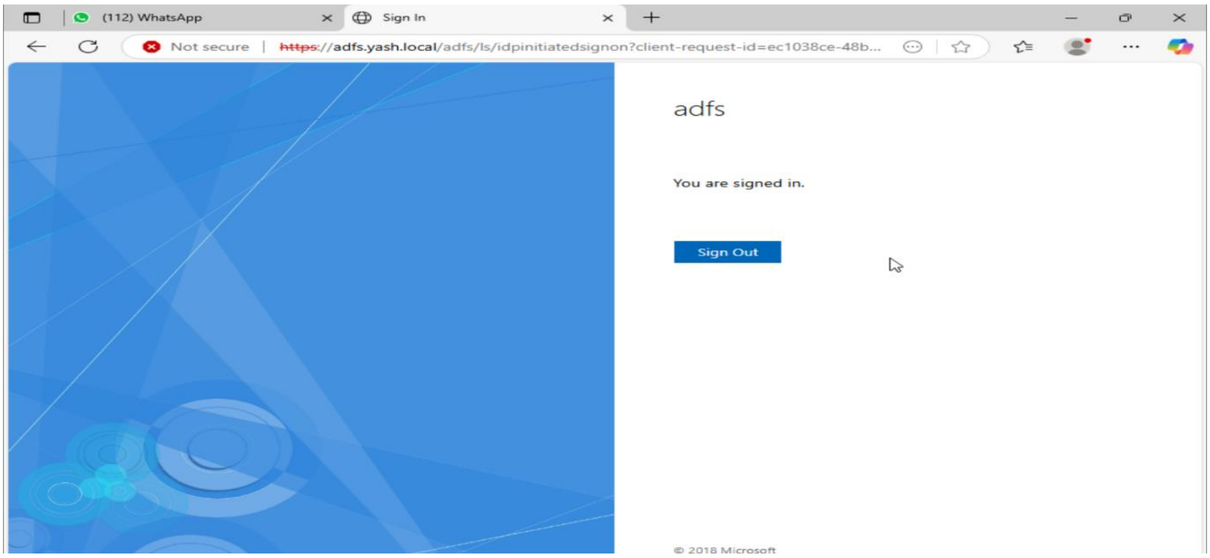
Sign in

Incorrect user ID or password. Type the correct user ID and password, and try again.

Anjali@yash.local

•••••••

(Login successful.)


(112) WhatsApp
Sign In
Not secure
https://adfs.yash.local/adfs/ls/idpinitiatedsignon?client-request-id=ec1038ce-48b...

adfs

You are signed in.

Sign Out
© 2018 Microsoft

3.2 Monitoring Federation Trust Relationships for Anomalies

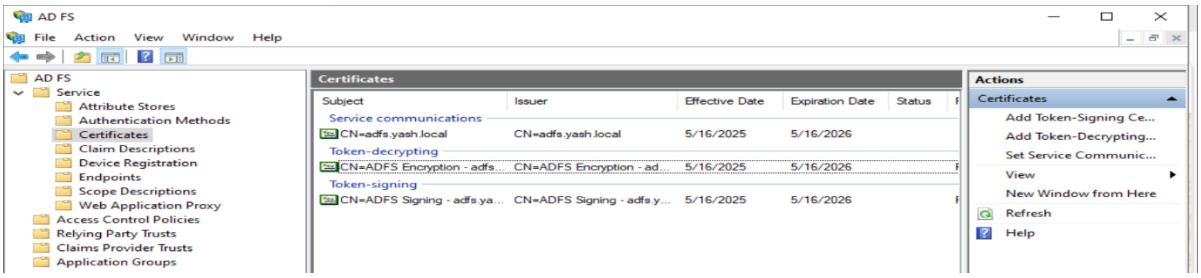
The second phase focuses on continuous monitoring and validation of the ADFS federation environment to detect anomalies or misconfigurations that could compromise security. This involves checking certificates, auditing trust relationships, and reviewing event logs to ensure the federation infrastructure remains secure and operational.

- **Verify Service Certificates**

  Certificates secure communication between clients, ADFS, and relying parties; expired or invalid certificates can cause authentication failures or security risks.

  Navigation:

  Open **AD FS Management** > **Service** > **Certificates** > Review the Signing, Encryption, and Service Communication certificates for validity and expiry dates.



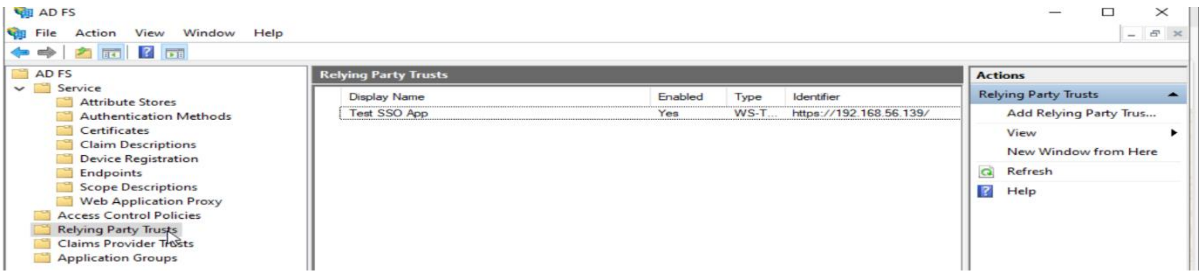
Subject	Issuer	Effective Date	Expiration Date	Status	F
Service communications					
CN=adfs.yash.local	CN=adfs.yash.local	5/16/2025	5/16/2026		
Token-decrypting					
CN=ADFS Encryption - adfs...	CN=ADFS Encryption - ad...	5/16/2025	5/16/2026		F
Token-signing					
CN=ADFS Signing - adfs.ya...	CN=ADFS Signing - adfs.y...	5/16/2025	5/16/2026		F

- **Audit Relying Party Trusts**

  Detecting unknown or misconfigured relying parties prevents unauthorized applications from gaining access via federation.

  Navigation:

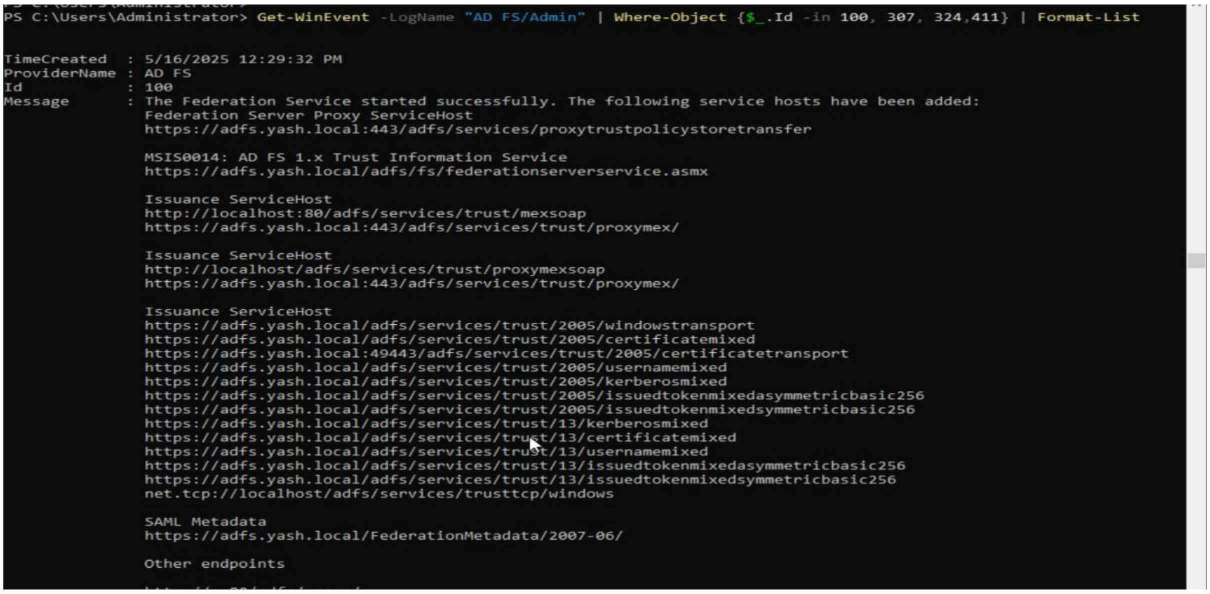
  In AD FS Management, under Relying Party Trusts, review the list of configured trusts to ensure all are recognized and correctly configured.



Display Name	Enabled	Type	Identifier
Test SSO App	Yes	WS-T...	https://192.168.56.139/

- **Query ADFS Admin Event Logs**

  Event logs provide detailed information about ADFS operations, errors, and warnings that help identify misconfigurations or security issues.



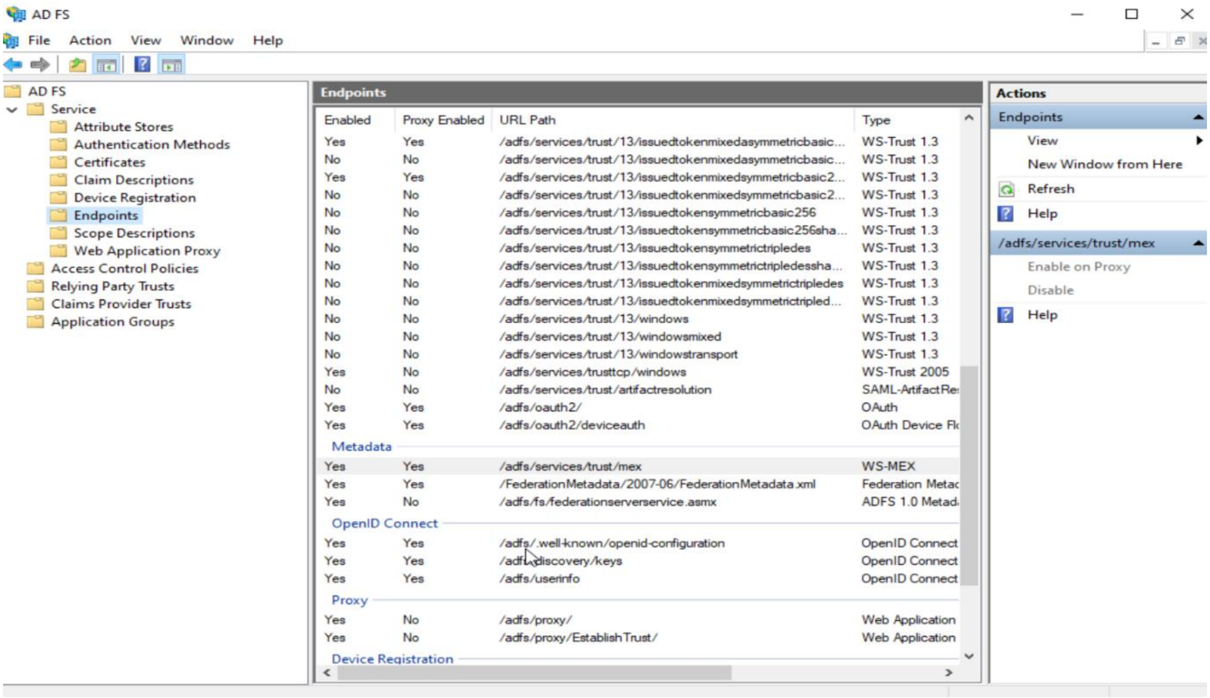
```
PS C:\Users\Administrator> Get-WinEvent -LogName "AD FS/Admin" | Where-Object {$_.Id -in 100, 307, 324,411} | Format-List

TimeCreated  : 5/16/2025 12:29:32 PM
ProviderName : AD FS
Id           : 100
Message      : The Federation Service started successfully. The following service hosts have been added:
               Federation Server Proxy ServiceHost
               https://adfs.yash.local:443/adfs/services/proxytrustpolicystoretransfer

               MSIS0014: AD FS 1.x Trust Information Service
               https://adfs.yash.local/adfs/fs/federationserverservice.asmx

               Issuance ServiceHost
               http://localhost:80/adfs/services/trust/mexsoap
               https://adfs.yash.local:443/adfs/services/trust/proxymex/

               Issuance ServiceHost
               http://localhost/adfs/services/trust/proxymexsoap
               https://adfs.yash.local:443/adfs/services/trust/proxymex/

               Issuance ServiceHost
               https://adfs.yash.local/adfs/services/trust/2005/windowstransport
               https://adfs.yash.local/adfs/services/trust/2005/certificatemixed
               https://adfs.yash.local:49443/adfs/services/trust/2005/certificatetransport
               https://adfs.yash.local/adfs/services/trust/2005/usernamemixed
               https://adfs.yash.local/adfs/services/trust/2005/kerberosmixed
               https://adfs.yash.local/adfs/services/trust/2005/issuedtokenmixedasymmetricbasic256
               https://adfs.yash.local/adfs/services/trust/2005/issuedtokenmixedsymmetricbasic256
               https://adfs.yash.local/adfs/services/trust/13/kerberosmixed
               https://adfs.yash.local/adfs/services/trust/13/certificatemixed
               https://adfs.yash.local/adfs/services/trust/13/usernamemixed
               https://adfs.yash.local/adfs/services/trust/13/issuedtokenmixedasymmetricbasic256
               https://adfs.yash.local/adfs/services/trust/13/issuedtokenmixedsymmetricbasic256
               net.tcp://localhost/adfs/services/trusttcp/windows

               SAML Metadata
               https://adfs.yash.local/FederationMetadata/2007-06/

               Other endpoints
```

- **Check Federation Service Endpoints and URLs**

  Ensures the federation endpoints clients interact with are valid and reachable, preventing disruptions in service.

  Navigation:

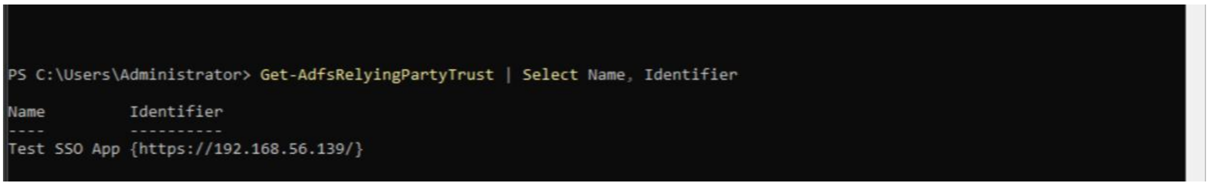
  Within **AD FS Management** > **Service** > **Endpoints** and check DNS entries on the DNS server to verify URLs like https://adfs.task.local/adfs/ls/ are correctly configured and accessible.



Endpoints

Enabled	Proxy Enabled	URL Path	Type
Yes	Yes	/adfs/services/trust/13/issuedtokenmixedasymmetricbasic...	WS-Trust 1.3
No	No	/adfs/services/trust/13/issuedtokenmixedasymmetricbasic...	WS-Trust 1.3
Yes	Yes	/adfs/services/trust/13/issuedtokenmixedsymmetricbasic2...	WS-Trust 1.3
No	No	/adfs/services/trust/13/issuedtokenmixedsymmetricbasic2...	WS-Trust 1.3
No	No	/adfs/services/trust/13/issuedtokensymmetricbasic256	WS-Trust 1.3
No	No	/adfs/services/trust/13/issuedtokensymmetricbasic256sha...	WS-Trust 1.3
No	No	/adfs/services/trust/13/issuedtokensymmetrictripledes	WS-Trust 1.3
No	No	/adfs/services/trust/13/issuedtokensymmetrictripledessha...	WS-Trust 1.3
No	No	/adfs/services/trust/13/issuedtokenmixedsymmetrictripledes	WS-Trust 1.3
No	No	/adfs/services/trust/13/issuedtokenmixedsymmetrictripled...	WS-Trust 1.3
No	No	/adfs/services/trust/13/windows	WS-Trust 1.3
No	No	/adfs/services/trust/13/windowsmixed	WS-Trust 1.3
No	No	/adfs/services/trust/13/windowstransport	WS-Trust 1.3
Yes	No	/adfs/services/trusttcp/windows	WS-Trust 2005
No	No	/adfs/services/trust/artifactresolution	SAML-ArtifactRe
Yes	Yes	/adfs/oauth2/	OAuth
Yes	Yes	/adfs/oauth2/deviceauth	OAuth Device Fl
Metadata			
Yes	Yes	/adfs/services/trust/mex	WS-MEX
Yes	Yes	/FederationMetadata/2007-06/FederationMetadata.xml	Federation Metac
Yes	No	/adfs/fs/federationserverservice.asmx	ADFS 1.0 Metad
OpenID Connect			
Yes	Yes	/adfs/.well-known/openid-configuration	OpenID Connect
Yes	Yes	/adfs/discovery/keys	OpenID Connect
Yes	Yes	/adfs/userinfo	OpenID Connect
Proxy			
Yes	No	/adfs/proxy/	Web Application
Yes	No	/adfs/proxy/EstablishTrust/	Web Application
Device Registration			

- **Inspect Relying Party Trusts via PowerShell**
  PowerShell queries provide a quick way to audit relying party trusts, confirming their status and configuration without manual inspection.



```
PS C:\Users\Administrator> Get-AdfsRelyingPartyTrust | Select Name, Identifier

Name         Identifier
----         ----------
Test SSO App {https://192.168.56.139/}
```

4. Results And Findings

This section presents the key observations and outcomes obtained from implementing the ADFS installation, test SSO configuration, and federation trust monitoring. It outlines both the functional results and security validation achieved throughout the process. Each finding confirms whether the objectives of seamless authentication and secure trust relationships were effectively met.

4.1 **Successful Federation Setup**

ADFS was successfully installed and configured with a valid SSL certificate, DNS entry, and federation service name. The setup proceeded without errors and the ADFS Management Console displayed all services as healthy.

4.2 **SSO Login Verification**

The test SSO application successfully redirected authentication requests to ADFS and allowed login with domain credentials, confirming correct trust and claim rule configuration.

4.3 **Certificate Integrity Validated**

All three certificates (service communication, signing, and encryption) were present and valid. No expired or missing certificates were detected during the review.

4.4 **Trust Relationships Consistent**

The configured relying party trust matched the intended test application setup. PowerShell and GUI outputs confirmed that only known applications were federated.

4.5 **Event Logs Showed No Critical Errors**

Event logs under "AD FS/Admin" revealed expected authentication and claim processing entries. No federation trust anomalies, certificate errors, or endpoint issues were observed.

5. Recommendations

Based on the configuration steps and analysis performed during the federation deployment and monitoring phases, this section provides actionable suggestions to further enhance security, stability, and scalability. These recommendations are derived from best practices and are aimed at maintaining a resilient and future-proof ADFS environment.

5.1 Regularly Audit Trust Relationships

Periodically review all relying party trusts to ensure no unauthorized or outdated entries are present, reducing the risk of federation abuse.

5.2 **Automate Certificate Monitoring**

Implement certificate monitoring tools or scheduled PowerShell scripts to detect expiring ADFS certificates early and renew them before causing service outages.

5.3 **Enable Advanced Logging**

Activate additional security logging (e.g., ADFS Auditing, Security Token Service logs) for improved visibility into authentication patterns and anomaly detection.

5.4 **Use Client DNS Policies in Production**

In production, replace manual hosts file entries with proper DNS zone delegation and resolution policies to ensure scalability and manageability.

5.5 **Test with Multiple Applications**

Expand testing to include more relying party applications (internal and external) to validate how ADFS handles different claim rules and SSO scenarios.

6. Conclusion

The successful implementation of Active Directory Federation Services (ADFS) and its integration with a test Single Sign-On (SSO) application marks a critical milestone in strengthening the identity and access management infrastructure. By configuring the ADFS role, establishing DNS resolution, and defining a secure relying party trust, federated authentication was enabled in a controlled and verifiable manner. The test application validated this configuration by seamlessly redirecting authentication requests to ADFS and allowing secure user access through claim-based authentication.

Furthermore, the federation trust monitoring phase provided assurance that the deployment remained secure and well-governed. All service certificates were verified as valid, relying party trusts were consistent with the intended configuration, and federation logs confirmed that service endpoints were functioning without anomalies. These checks are crucial in preventing unauthorized federation relationships, misconfigurations, and token-related attacks.