SAML Single Sign-On Configuration for OAS on Windows

Agenda:

Configure SAML SSO to OAS without editing the OAS Binaries like *.ear files and their web.xml and weblogic.xml as we are not supposed to edit the ear files in OAS.

Purpose and Approach:

The approach described in this paper is different from the approach taken in the Oracle Business Intelligence (OBIEE) product.

The approach for OAS is based on deploying an Apache HTTP Server ("httpd") with the mod_shib_24 shibboleth service provider module (for SAML) in front of OAS.

This HTTP server will perform the SAML based SSO authentication and pass the user ID of the successfully authenticated user to OAS.

OAS will use a WebLogic Identity Asserter to receive the user ID and assert the user just like a regular OAM based SSO configuration.

Consequently, the solution is a regular OAM based i.e. HTTP Header based Single Sign-On (SSO) solution as far as OAS is aware meaning that all functionality that is certified for regular SSO also works with this approach.

The Apache HTTP Server with the required Shibboleth SP (SAML SP) are installed on Windows Server on which OAS is running or can be on a different Windows Server.

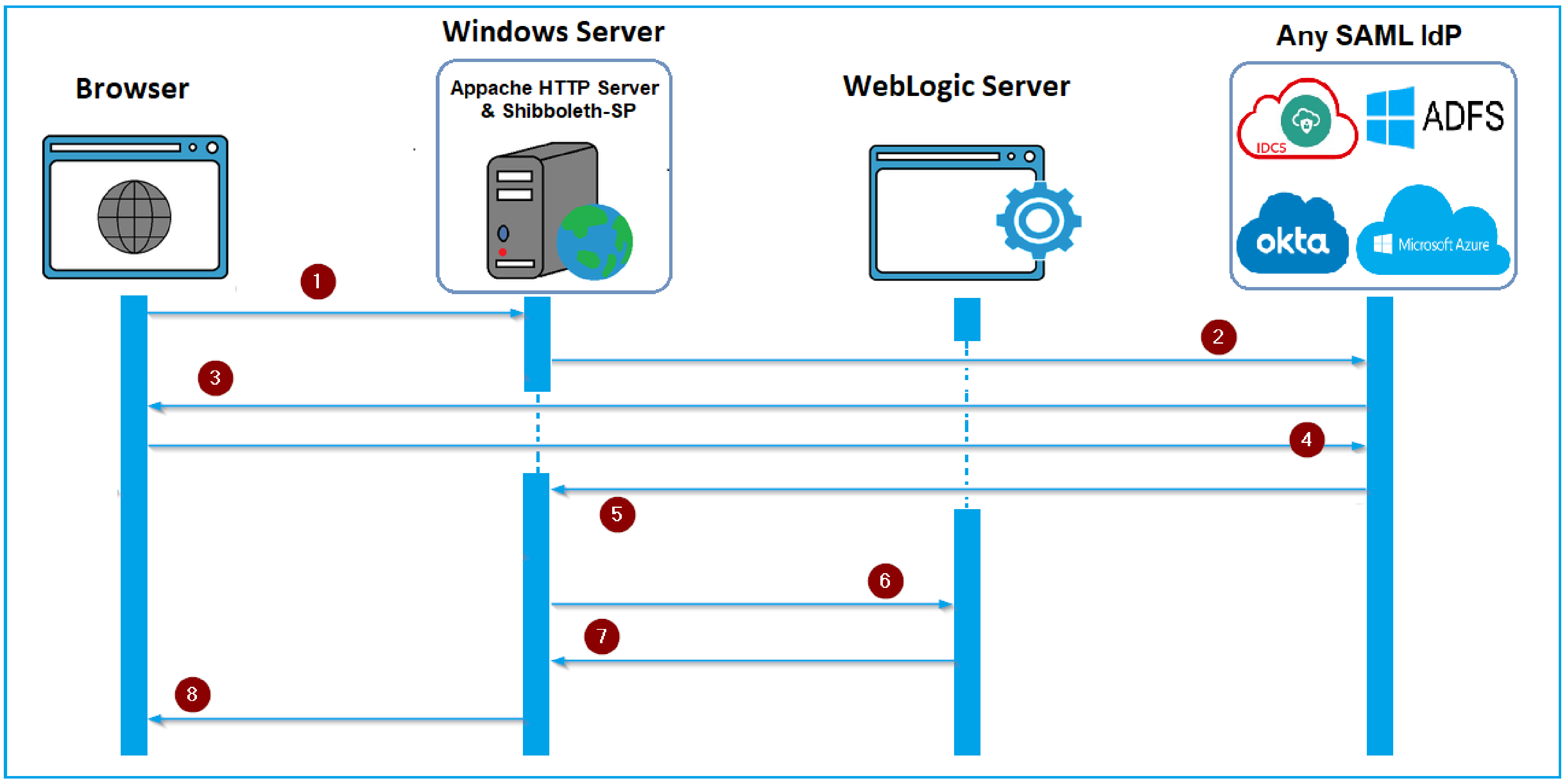
Apache HTTP Server and Shibboleth-SP configuration batch script will be run to configure the SSO.

Scope

This document is aimed at Oracle Analytics professionals familiar with SAML SSO Authentication flow using a WebLogic Identity Asserter.

About SAML Authentication Flow

This sequence diagram shows the authentication flow during SAML SSO, and all the communication that happens between the Browser, Windows Server where Apache and Shibboleth-SP are running, SAML Identity Provider and the Oracle WebLogic Server in which Oracle Analytics Server is deployed.



NOTE: This sequence diagram doesn't cover the detailed communication between the browser, Windows Server (SAML SP), OAS Server and Any SAML 2.0 compatible Identity Provider.

1. The user accesses the Oracle Analytics Server URL through Apache HTTP Server in the browser (`/dv` or `/analytics`).
2. The web server in the Windows Server with the shibboleth service provider redirects the user to the SAML Identity Provider for Authentication.
3. The SAML IdP will display the SSO Login Page in the Browser or use the Authentication Method setup at SAML IdP.
4. The user submits the login credentials to the SAML IdP.
5. Upon Successful Authentication at the SAML IdP, IdP send the authenticated user in a SAMLResponse to the Shibboleth-SP in the Windows Server.
6. The web server, using the Shibboleth-SP sends the userID in a HTTP Header such as `OAM_REMOTE_USER` to the Oracle WebLogic Server where OAS is running.
7. The Oracle WebLogic Server extracts the userID from the HTTP Header using Oracle Access Manager Identity Asserter (`OAMIdentityAsserter`). If the user exists, Oracle Analytics Server grants the application roles to the user and allows access to the requested resource (`/dv or /analytics`) through the web server.
8. The web server serves the requested resource to the user in the Browser.

Prerequisites for SAML SSO Configuration

1. Oracle Analytics Server is up and running.
2. Configure External LDAP or Active Directory with OAS as user Store to maintain the same user base between OAS and SSO Providers.
3. Oracle WebLogic Server in which Oracle Analytics Server is deployed, must be configured with an identity asserter, such as Oracle Access Manager Identity Asserter (OAMIdentityAsserter).
4. WebLogic Plugin should be enabled for the OAS Weblogic domain, bi_server (n) and bi_cluster.
5. The Apache HTTP server acts as a web server for Oracle Analytics Server. The Apache HTTP server can reside on a separate host server or on the same host server as Oracle Analytics Server.
6. Apache server should be running in SSL.
7. Decide on the DNS Name you may be using for Apache Server and get the SSL Server Certificate supporting the DNS name.
8. Also get the CA Intermediate and CA Root certificates that signed the Apache Server Certificate.
9. Get the SAML Identity Provider's Metadata xml File.
10. Some SAML IdP's require SAML Service Provider's metadata prior to config the SSO application in IDP.
    In such case you can share the Below Information with your SAML IDP and ask them to create a Relaying Party Trust (ADFS) or Application (other SAML IDP's) and get the SAML IDP Metadata XML File.
    ----
    entityID = https://oas.example.com/analytics/shibboleth
    SingleLogoutService = https://oas.example.com/Shibboleth.sso/SLO/POST
    AssertionConsumerService = https://oas.example.com/Shibboleth.sso/SAML2/POST
    Signing or Encryption Certificates are the same that we generated for Apache HTTP Server/LB

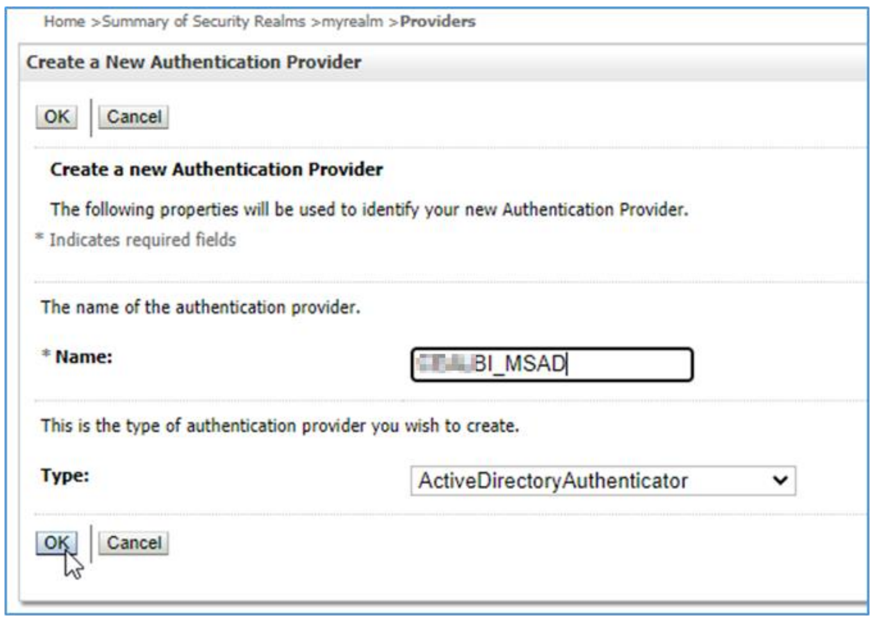
    NOTE: oas.example.com is a e.g Apache or Load Balancer Hostname change it accordingly.

In WebLogic Admin Console:

Configure External LDAP:

For SAML SSO, Configure any OAS Supported LDAP Server and use the same user attribute that the IDP will send in the SAMLResponse.

Set the Control Flag of External LDAP and Default Authenticator to SUFFICIENT


Home >Summary of Security Realms >myrealm >Providers

Create a New Authentication Provider

Create a new Authentication Provider

The following properties will be used to identify your new Authentication Provider.

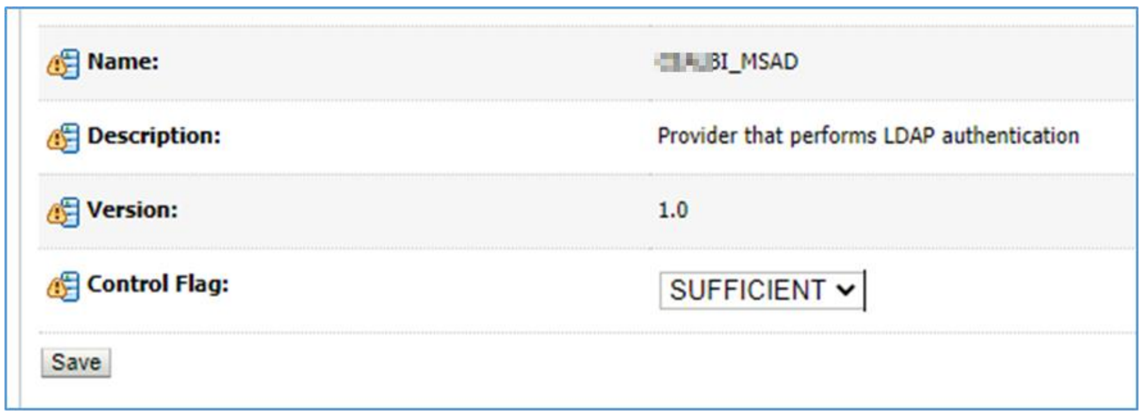
* Indicates required fields

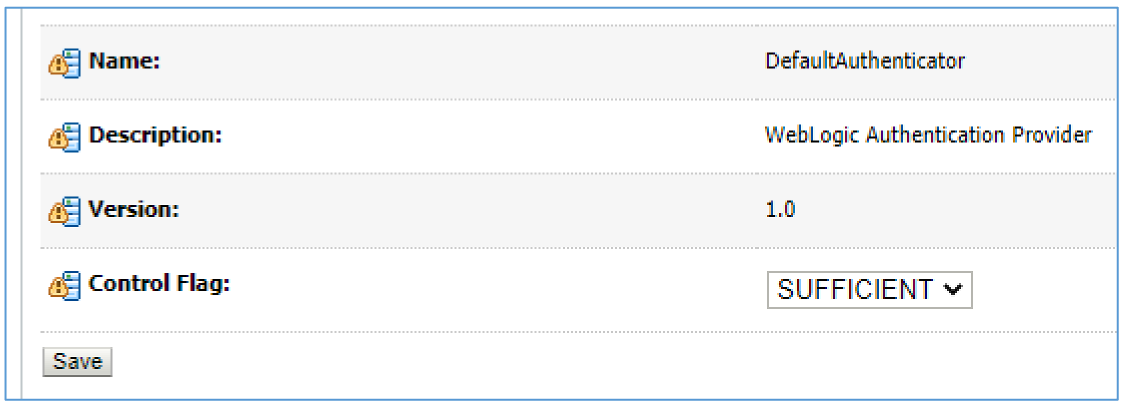
The name of the authentication provider.

* Name: [redacted]BI_MSAD

This is the type of authentication provider you wish to create.

Type: ActiveDirectoryAuthenticator


Name:	[redacted]BI_MSAD
Description:	Provider that performs LDAP authentication
Version:	1.0
Control Flag:	SUFFICIENT

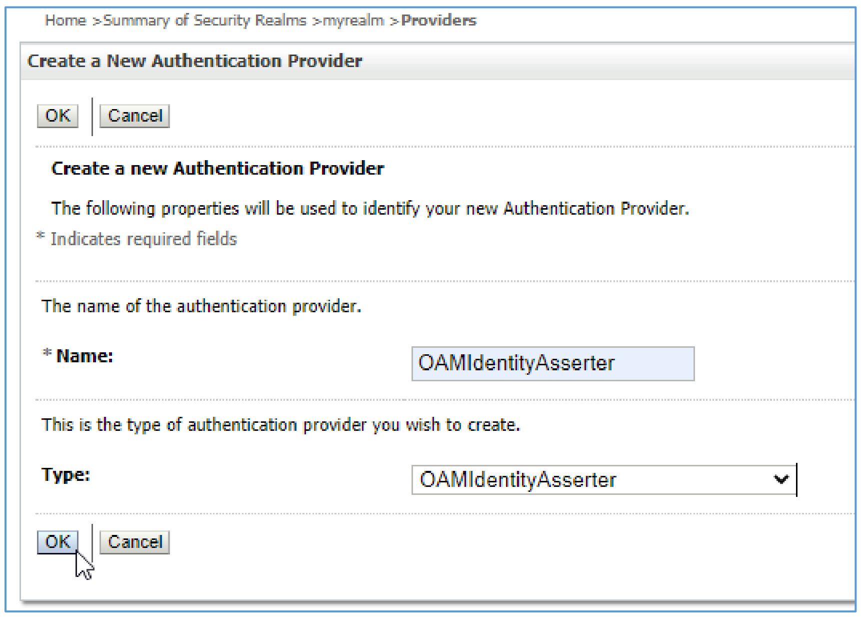

Name:	DefaultAuthenticator
Description:	WebLogic Authentication Provider
Version:	1.0
Control Flag:	SUFFICIENT

Configure OAMIdentityAsserter:

Add OAM Identity Asserter in WebLogic admin console and set it with OAM_REMOTE_USER header.

Set the Control Flag of OAMIdentityAsserter to REQUIRED

Reorder the Providers and make OAMIdentityAsserter to be the first in the list.


Home >Summary of Security Realms >myrealm >Providers

Create a New Authentication Provider

Create a new Authentication Provider

The following properties will be used to identify your new Authentication Provider.

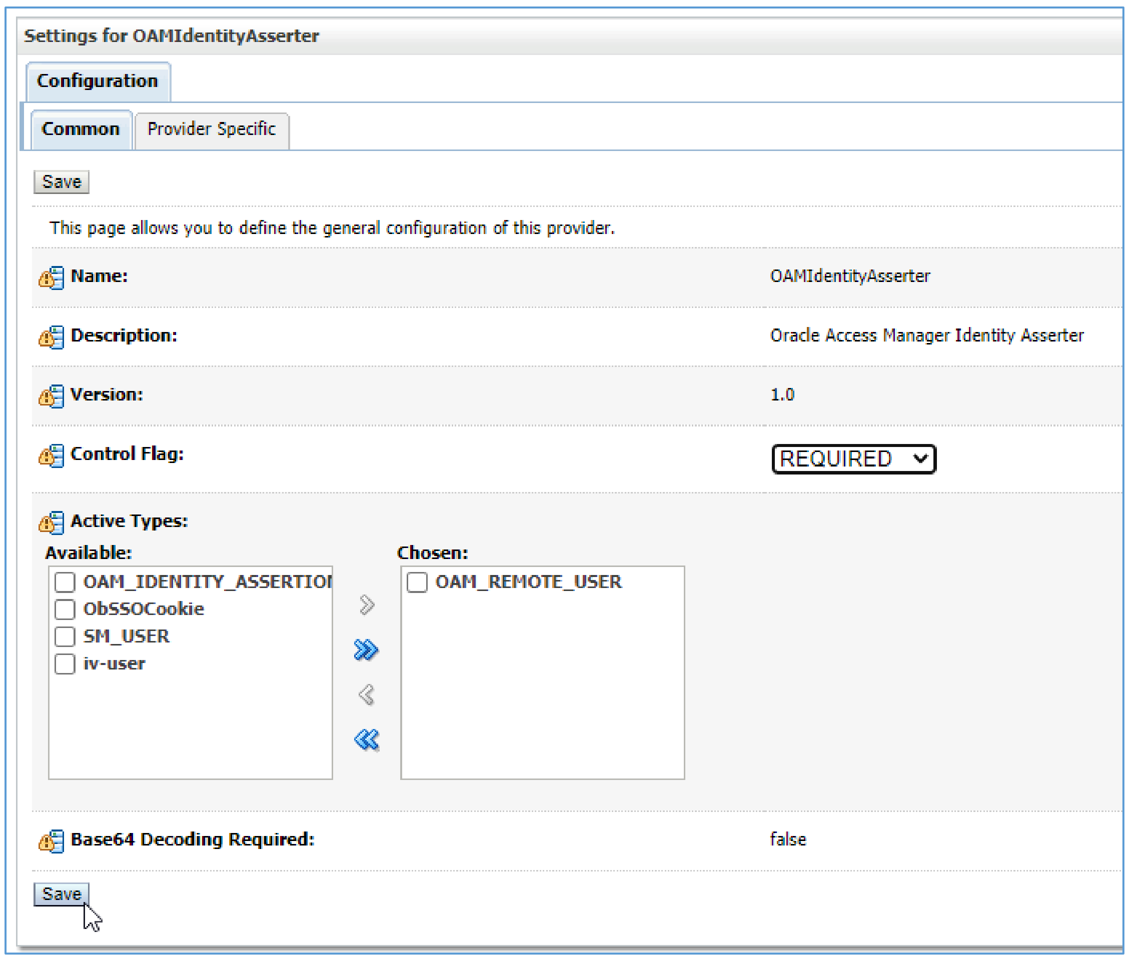
* Indicates required fields

The name of the authentication provider.

* Name: OAMIdentityAsserter

This is the type of authentication provider you wish to create.

Type: OAMIdentityAsserter



Settings for OAMIdentityAsserter

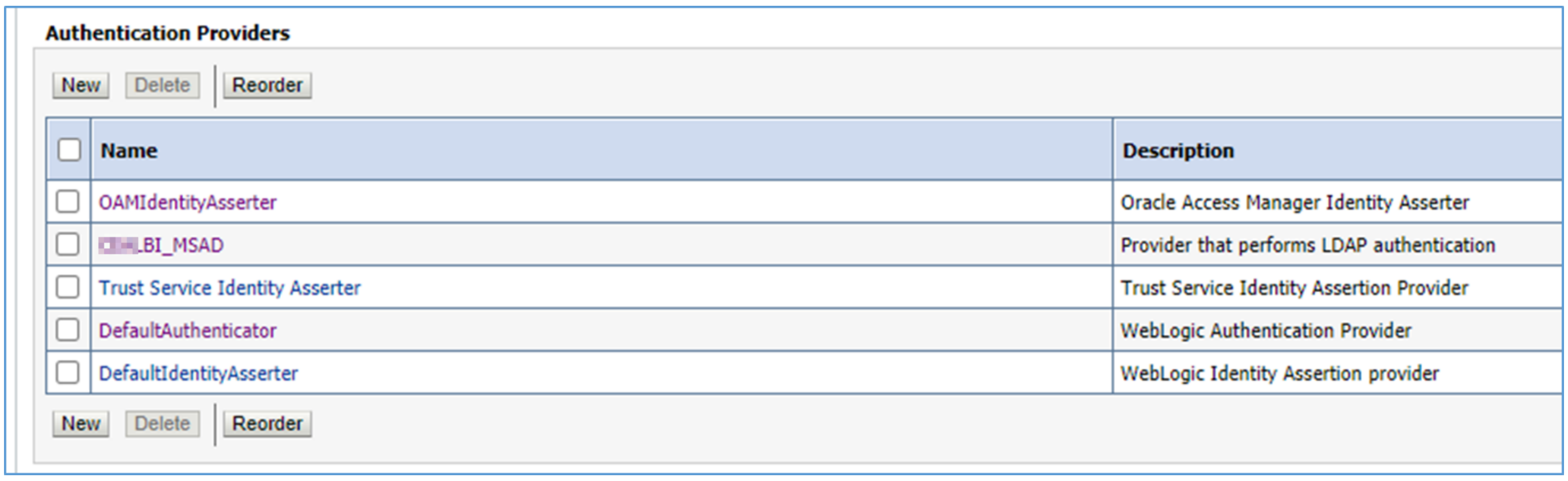
This page allows you to define the general configuration of this provider.

Name:	OAMIdentityAsserter
Description:	Oracle Access Manager Identity Asserter
Version:	1.0
Control Flag:	REQUIRED

Active Types:

Available:	Chosen:
□ OAM_IDENTITY_ASSERTIOI	□ OAM_REMOTE_USER
□ ObSSOCookie	
□ SM_USER	
□ iv-user	

Base64 Decoding Required: false



Authentication Providers

□	Name	Description
□	OAMIdentityAsserter	Oracle Access Manager Identity Asserter
□	[redacted]LBI_MSAD	Provider that performs LDAP authentication
□	Trust Service Identity Asserter	Trust Service Identity Assertion Provider
□	DefaultAuthenticator	WebLogic Authentication Provider
□	DefaultIdentityAsserter	WebLogic Identity Assertion provider

Enable WebLogic Plugin:

For DV we need to enable WebLogic Plugin in WebLogic admin console

Login to WebLogic admin console:

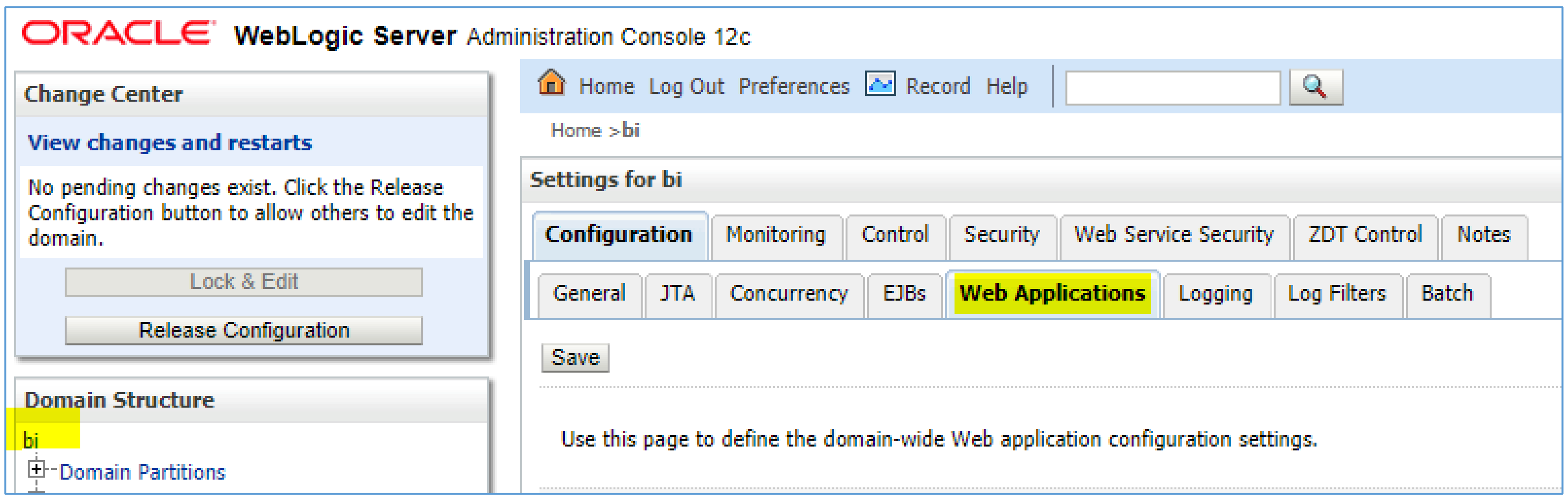
1. Navigate to the top of the Domain tree and select "bi" -> Web Applications -> Check the "Enable WebLogic Plugin" checkbox.

2. Navigate to Environment -> Servers -> bi_server1 -> Expand Advanced -> expand the dropdown of the "Enable WebLogic Plugin" and select "Yes".

3. Repeat the above step for all the available bi_serverN

4. Navigate to Environment -> Cluster -> bi_cluster -> Expand Advanced -> expand the dropdown of the "Enable WebLogic Plugin" and select "Yes".

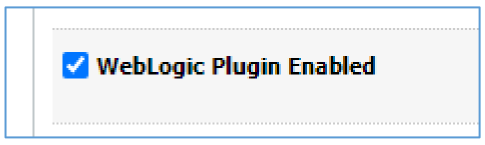
NOTE: This required for DV to work when the Managed WebLogic Server is under a Load balancer or Web Server.



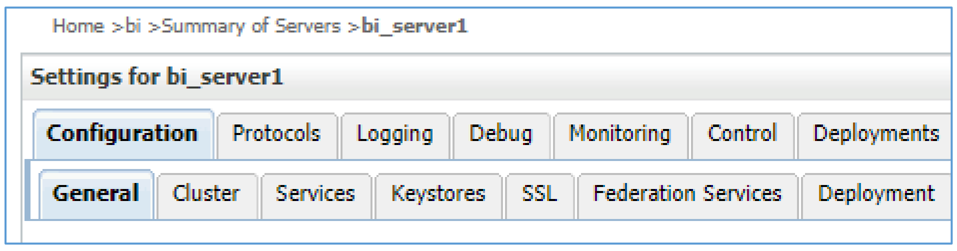
Settings for bi

No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

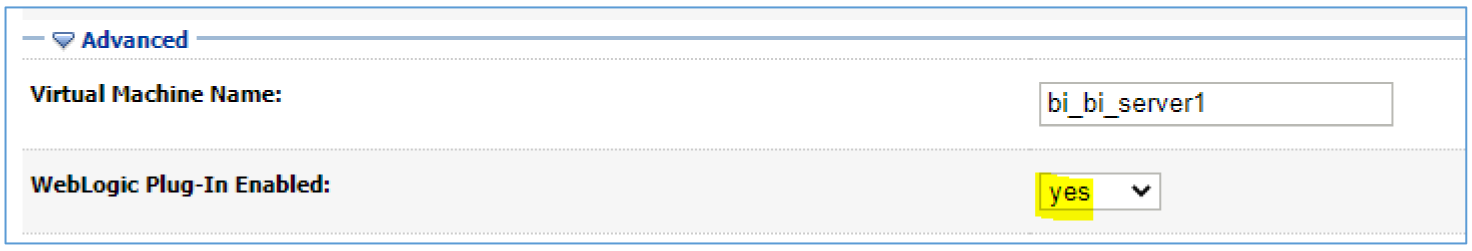
Use this page to define the domain-wide Web application configuration settings.



☑ WebLogic Plugin Enabled

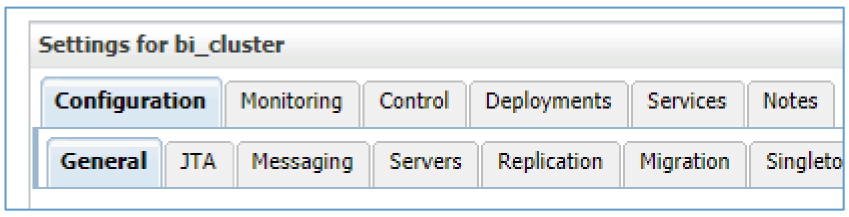


Settings for bi_server1

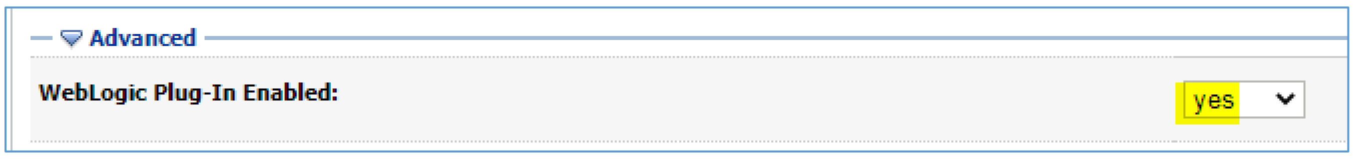


Virtual Machine Name: bi_bi_server1

WebLogic Plug-In Enabled: yes



Settings for bi_cluster



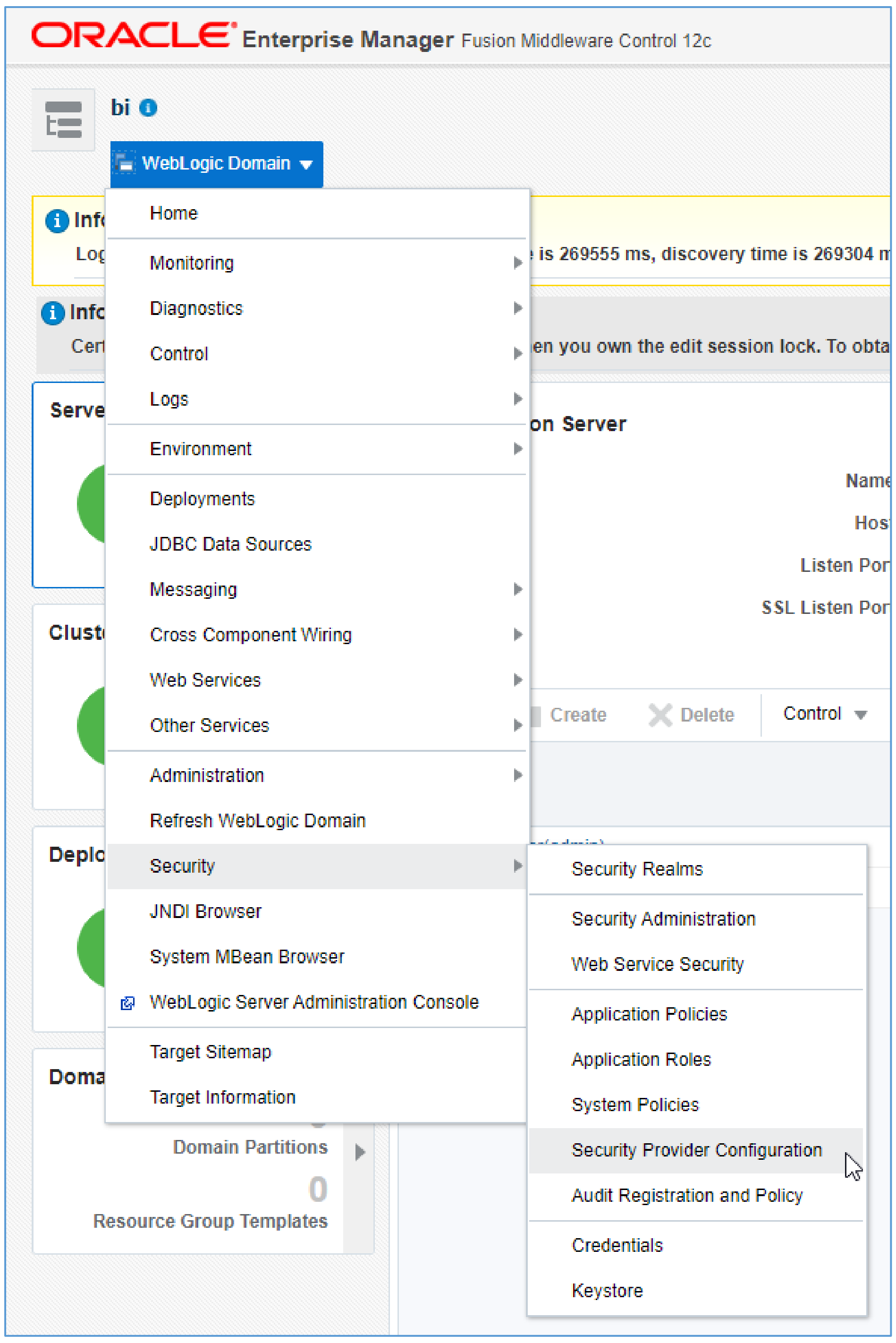
WebLogic Plug-In Enabled: yes

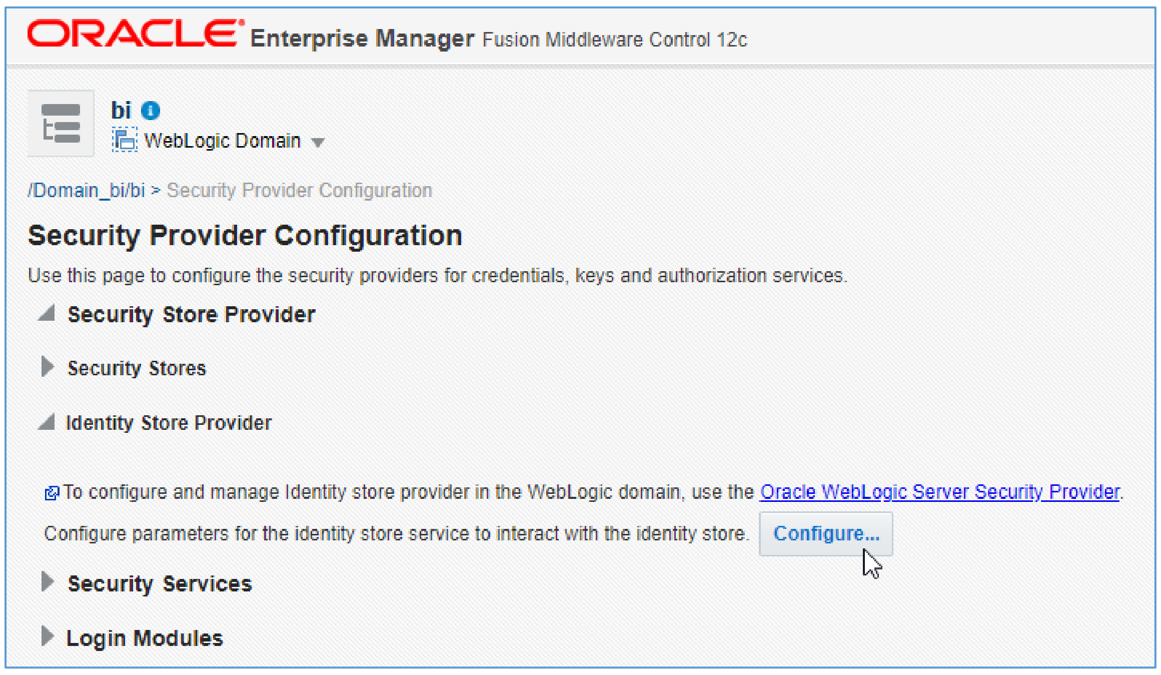
In WebLogic FMW EM:

Set **Virtualize=true** and **OPTIMIZE_SEARCH=true** parameters in EM when using External LDAP

For **SAML SSO**, set the SSO Logoff URL to **/logout.html**

Restart all OAS Services




ORACLE Enterprise Manager Fusion Middleware Control 12c
bi
WebLogic Domain
/Domain_bi/bi > Security Provider Configuration

Security Provider Configuration

Use this page to configure the security providers for credentials, keys and authorization services.

Security Store Provider

Security Stores

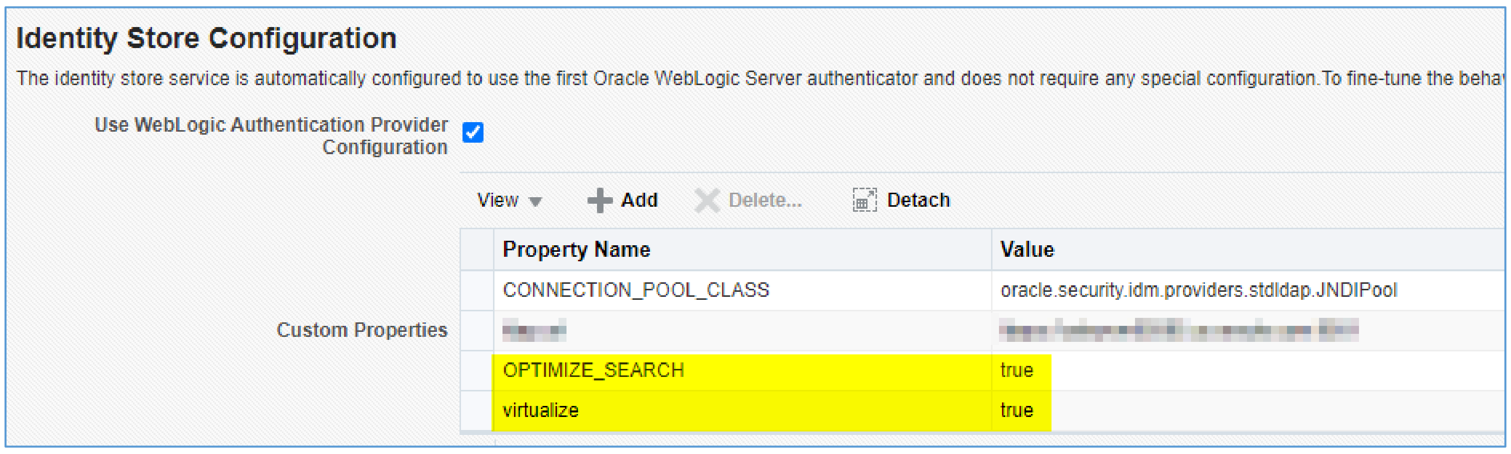
Identity Store Provider

To configure and manage Identity store provider in the WebLogic domain, use the Oracle WebLogic Server Security Provider.

Configure parameters for the identity store service to interact with the identity store. Configure...

Security Services

Login Modules



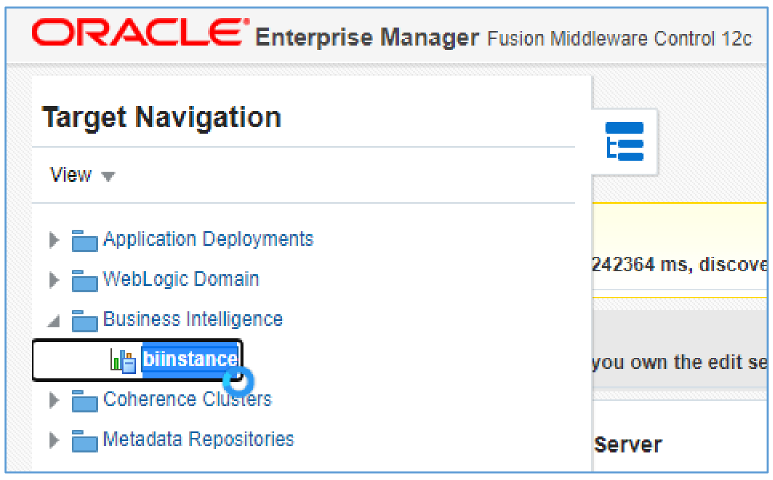
Identity Store Configuration

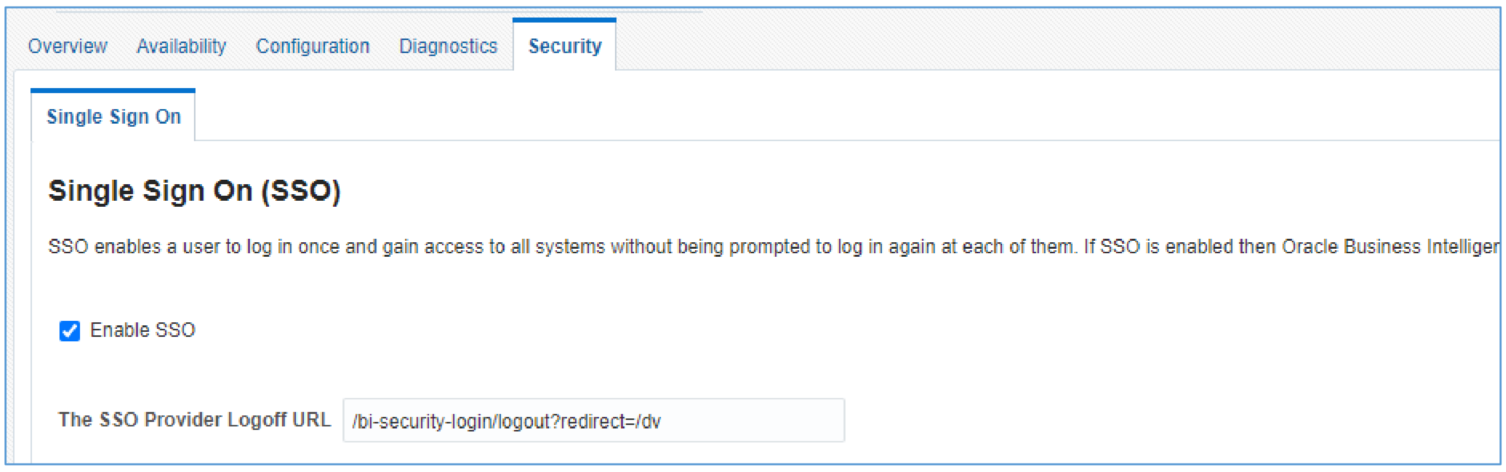
The identity store service is automatically configured to use the first Oracle WebLogic Server authenticator and does not require any special configuration.To fine-tune the beha

Use WebLogic Authentication Provider Configuration ☑

Custom Properties

Property Name	Value
CONNECTION_POOL_CLASS	oracle.security.idm.providers.stdldap.JNDIPool
[redacted]	[redacted]
OPTIMIZE_SEARCH	true
virtualize	true





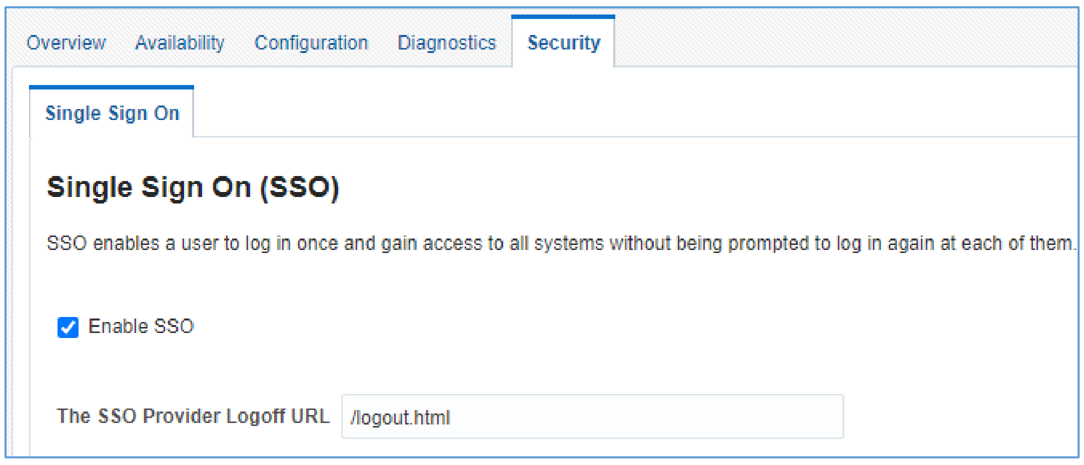
Single Sign On (SSO)

SSO enables a user to log in once and gain access to all systems without being prompted to log in again at each of them. If SSO is enabled then Oracle Business Intelliger

☑ Enable SSO

The SSO Provider Logoff URL /bi-security-login/logout?redirect=/dv

Lock&Edit, Change to /logout.html and Click on "Apply". Then "Activate Changes"



Single Sign On (SSO)

SSO enables a user to log in once and gain access to all systems without being prompted to log in again at each of them.

☑ Enable SSO

The SSO Provider Logoff URL /logout.html

Generate the SSL Certificates for the Apache HTTP Server

Decide on the DNS Name that Apache HTTP Server will be using and generate SSL certificate.

NOTE: If Load Balancer is the Front end, can use Load Balancer SSL Certificates as well.

Get the SSL Certificate signed by your Internal CA or Public CA as per your Organization requirements.

We need below Base-64 encoded X.509 certificate files:

1. Apache HTTP Server Certificate
2. Private Key for the Apache HTTP Server Certificate
3. Get the CA Chain Certificate by flowing below steps.
   Create the CA chain certificate by taking the CA Intermediate Certificate content into a notepad and append it with the content of the CA Root Certificate.
   e.g.
   -----BEGIN CERTIFICATE------
   Gdjsgdx-Intermediate-sa7s90809
   -----END CERTIFICATE------
   -----BEGIN CERTIFICATE------
   Ddjsgdxguiy-Root-8089d890808
   -----END CERTIFICATE------

openssl commands to generate a certificate:

Generating new server key

```
> openssl genrsa -aes256 -passout pass:Oracle123 -out server1.key 2048
```

Removing the PassPhrase from server1.key

```
> openssl rsa -passin pass:Oracle123 -in server1.key -out server.key
```

Generating server certificate sign request i.e server.csr

```
> openssl req -subj "/C=US/ST=California/L=RedwoodShores/O=Oracle Corporation/OU=Oracle Analytics Server/CN=oas.example.com" -out server.csr -key server.key -new -sha256
```

Get the CSR signed by your Internal or Public CA, we will get CA signed server.crt

Get the CA Intermediate and CA Root Certificates

For internal testing we can sign the CSR with the Private Key and generating a self-signed certificate

```
> openssl x509 -req -days 365 -sha256 -in server.csr -signkey server.key -out server.crt
```

Here we used Internal CA to sign the certificate.

Copy the SSL Certificates to conf folder

server.crt

server.key

server-ca.crt (CAIntermediate cert content appended with CARoot cert content)

If oas.example.com.p12 file is delivered by your IT team

Extract the Certificate from a pfx/p12 file

```
openssl pkcs12 -in oas.example.com.p12 -clcerts -nokeys -nodes -out server.crt
```

(Enter Password when prompted)

Extract the Private Key from a pfx/p12 file

```
openssl pkcs12 -in oas.example.com.p12 -nocerts -out server_encrypted.key
```

(Enter Password when prompted)

Remove the Passpharse for the Private Key

```
openssl rsa -in server_encrypted.key -out server.key
```

Get the CA Intermediate and CA Root Certificated from your IT Team.

Create the CA chain certificate by taking the CA Intermediate Certificate content into a notepad and append it with the content of the CA Root Certificate.

There are two ways to config SAML SSO for OAS on Windows

Method 1:

Create the OASSO docker image following the steps in the Support Doc ID 2761678.1

Run the OASSO Docker image on Windows using Docker Desktop (Which is now a licensed product)

https://docs.docker.com/desktop/

https://www.docker.com/pricing

Method 2:

Install and Configure required software manually without a docker container.

Here we are covering Method 2, Install and Configure required software manually without docker container.

Install Apache 2.4 Version on Windows Server

Download Apache for Windows:

https://httpd.apache.org/docs/current/platform/windows.html#down

https://www.apachelounge.com/download/

https://www.apachelounge.com/download/VS16/binaries/httpd-2.4.51-win64-VS16.zip

Extract the Zip file and place the folder where you want to run from. e.g D:\

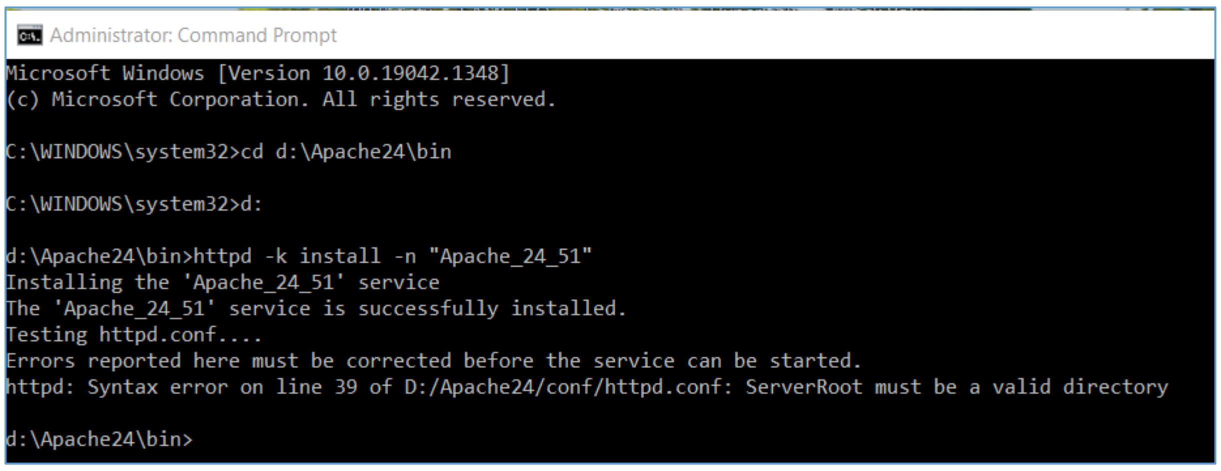
D:\Apache24

Install and Run Apache as a Service:

Open Command Prompt as Administrator

cd D:\Apache24\bin

httpd.exe -k install -n “Apache_24_51”



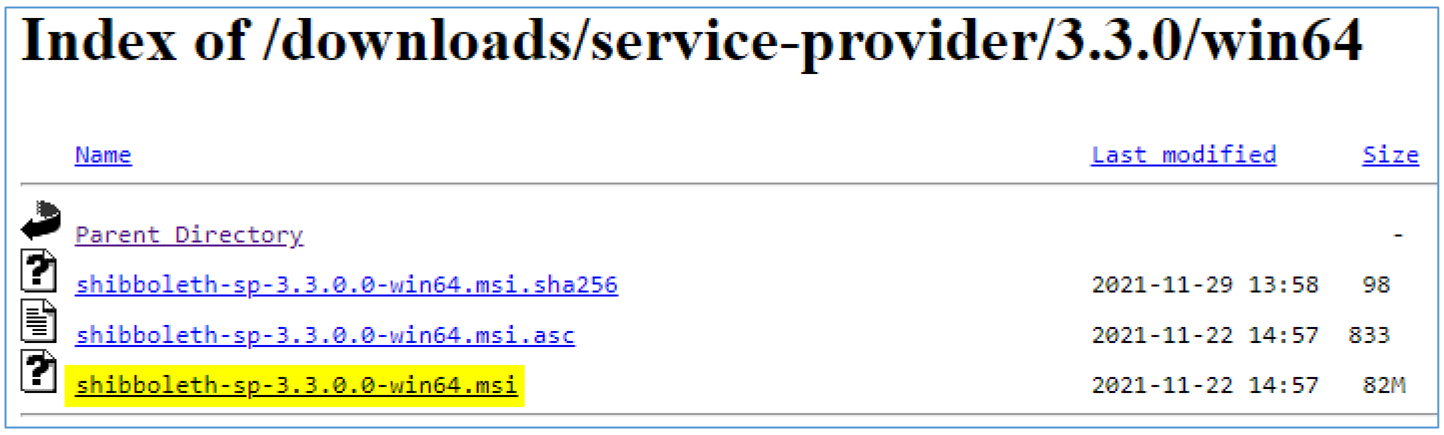
```
Microsoft Windows [Version 10.0.19042.1348]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd d:\Apache24\bin

C:\WINDOWS\system32>d:

d:\Apache24\bin>httpd -k install -n "Apache_24_51"
Installing the 'Apache_24_51' service
The 'Apache_24_51' service is successfully installed.
Testing httpd.conf....
Errors reported here must be corrected before the service can be started.
httpd: Syntax error on line 39 of D:/Apache24/conf/httpd.conf: ServerRoot must be a valid directory

d:\Apache24\bin>
```

Later we can correct the syntax errors

Install Shibboleth Service Provider for Windows

Download Shibboleth SP 3:

https://shibboleth.net/downloads/service-provider/3.3.0/win64/



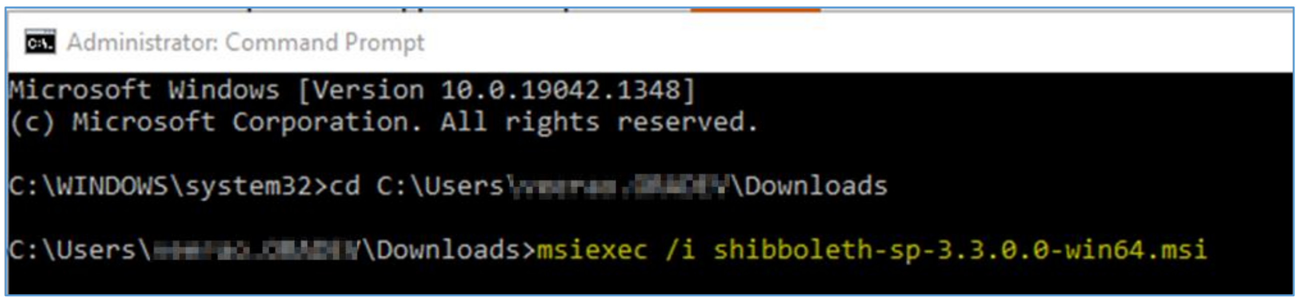
Index of /downloads/service-provider/3.3.0/win64

Name	Last modified	Size
Parent Directory		-
shibboleth-sp-3.3.0.0-win64.msi.sha256	2021-11-29 13:58	98
shibboleth-sp-3.3.0.0-win64.msi.asc	2021-11-22 14:57	833
shibboleth-sp-3.3.0.0-win64.msi	2021-11-22 14:57	82M

https://shibboleth.net/downloads/service-provider/3.3.0/win64/shibboleth-sp-3.3.0.0-win64.msi

Installation of Shibboleth SP 3:

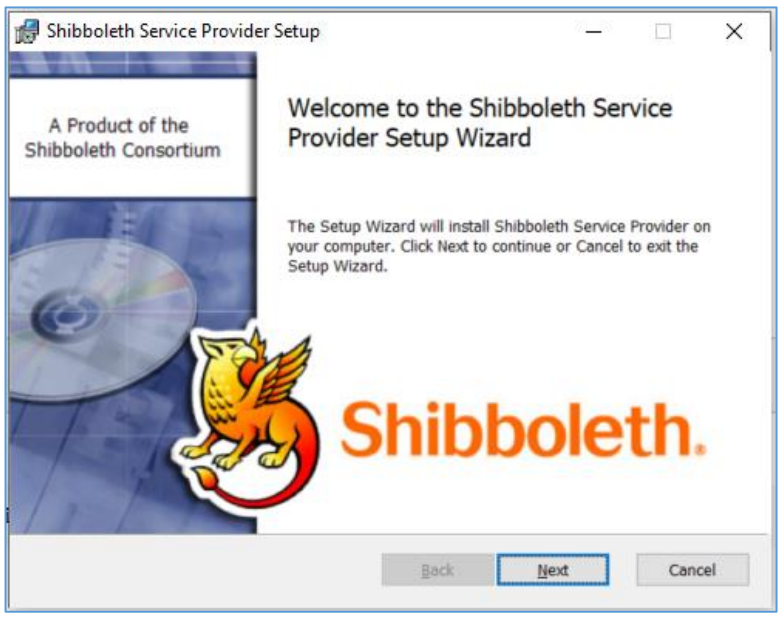
https://shibboleth.atlassian.net/wiki/spaces/SP3/pages/2065335545/Install+on+Windows



Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.19042.1348]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Users\[redacted]\Downloads

C:\Users\[redacted]\Downloads>msiexec /i shibboleth-sp-3.3.0.0-win64.msi
```

Open Command Prompt as Administrator

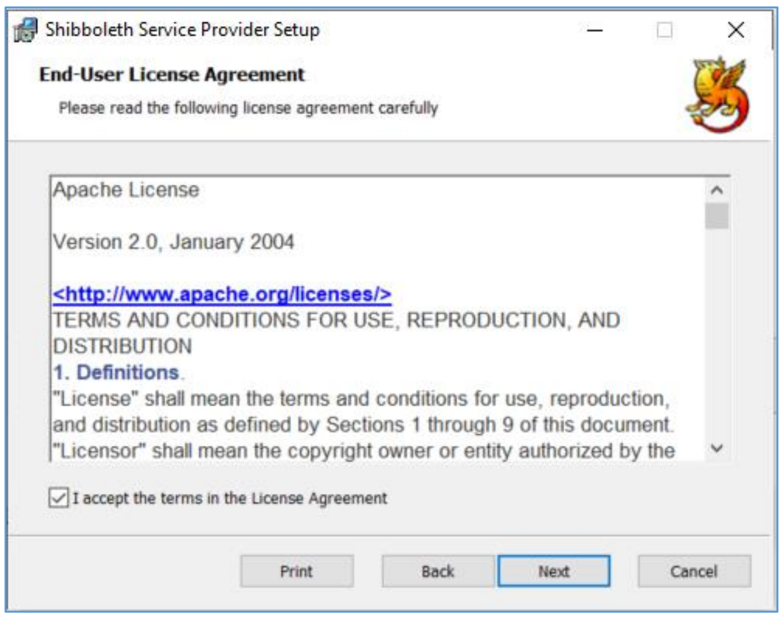


Shibboleth Service Provider Setup

A Product of the Shibboleth Consortium

Welcome to the Shibboleth Service Provider Setup Wizard

The Setup Wizard will install Shibboleth Service Provider on your computer. Click Next to continue or Cancel to exit the Setup Wizard.



Shibboleth Service Provider Setup

End-User License Agreement

Please read the following license agreement carefully

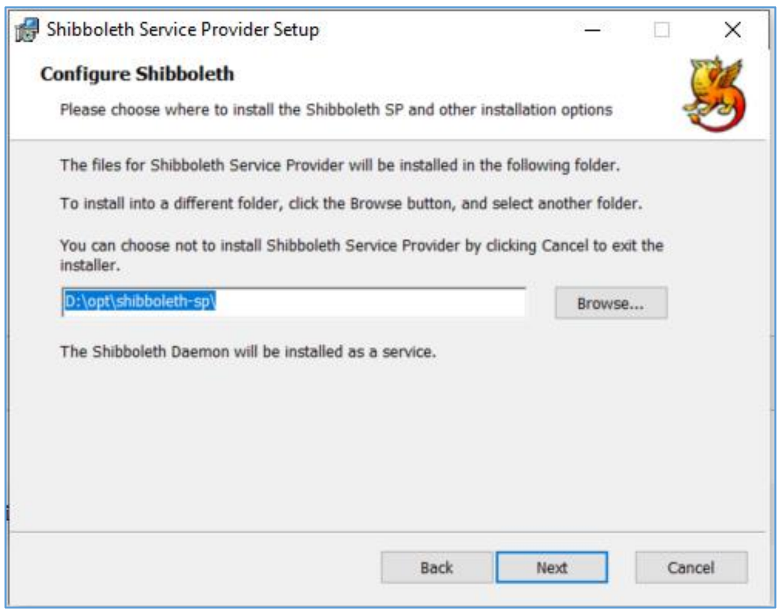
Apache License

Version 2.0, January 2004

<http://www.apache.org/licenses/>
TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION
1. Definitions.
"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.
"Licensor" shall mean the copyright owner or entity authorized by the

☑ I accept the terms in the License Agreement

Here we are installing the SW to D:\



Shibboleth Service Provider Setup

Configure Shibboleth

Please choose where to install the Shibboleth SP and other installation options

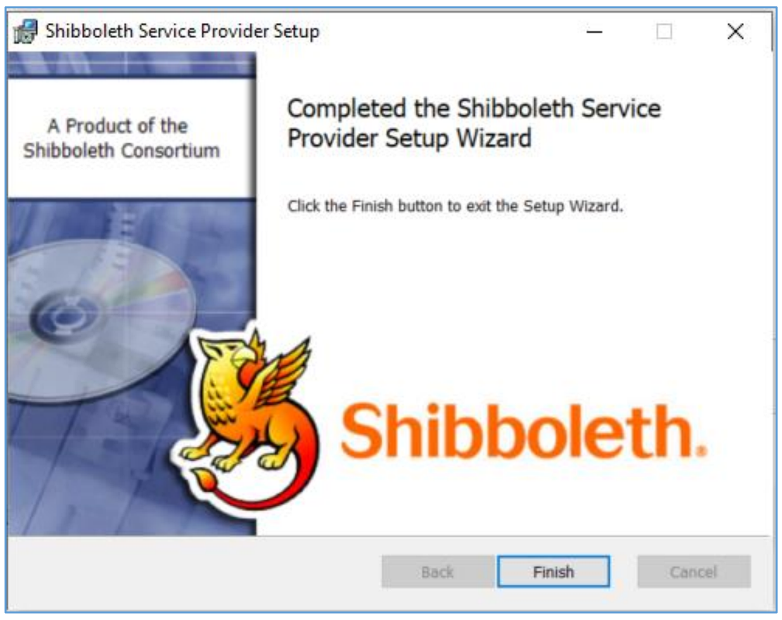
The files for Shibboleth Service Provider will be installed in the following folder.

To install into a different folder, click the Browse button, and select another folder.

You can choose not to install Shibboleth Service Provider by clicking Cancel to exit the installer.

D:\opt\shibboleth-sp\

The Shibboleth Daemon will be installed as a service.



Shibboleth Service Provider Setup

A Product of the Shibboleth Consortium

Completed the Shibboleth Service Provider Setup Wizard

Click the Finish button to exit the Setup Wizard.

D:\opt\shibboleth-sp is the **Install** folder.

D:\opt\shibboleth-sp\etc\shibboleth is the **config** folder.

Download and Extract the scripts and necessary files from Oracle provided Zip File

OAS_WIN_SAML.zip

Unzip the downloaded OAS_WIN_SAML.zip file to e.g D:\

cd D:\OAS_WIN_SAML

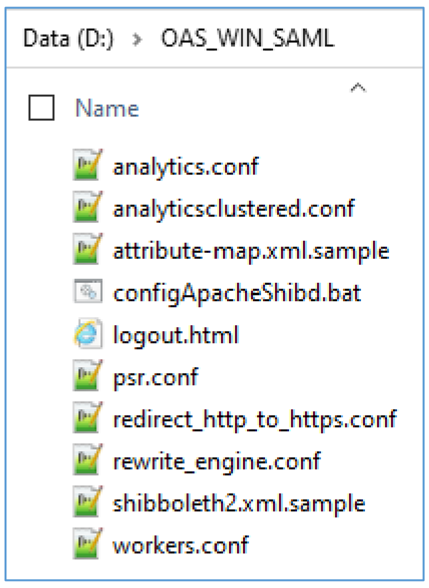
Copy the Apache HTTP Server's or Load Balancer's SSL Certificates to e.g. D:\OAS_WIN_SAML folder

Also copy the SAML IDP Metadata xml file to e.g. D:\OAS_WIN_SAML folder

NOTE: If these certs and IDP Metadata xml files are not copied to the script folder, the config script will exist and runs only if these files exist.

NOTE: If your SSL Certificate is Self-Signed, we don't have CA Chain Cert and we don't need to copy that file.

Folder should have all required Files

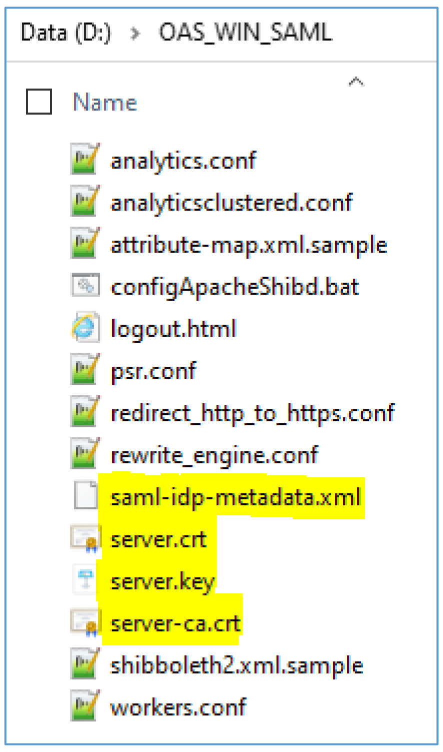


Data (D:) › OAS_WIN_SAML

□ Name

analytics.conf
analyticsclustered.conf
attribute-map.xml.sample
configApacheShibd.bat
logout.html
psr.conf
redirect_http_to_https.conf
rewrite_engine.conf
shibboleth2.xml.sample
workers.conf

After copying SSL Certificates and SAML IDP Metadata.xml files

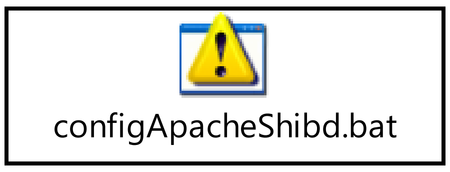


Data (D:) › OAS_WIN_SAML

□ Name

analytics.conf
analyticsclustered.conf
attribute-map.xml.sample
configApacheShibd.bat
logout.html
psr.conf
redirect_http_to_https.conf
rewrite_engine.conf
saml-idp-metadata.xml
server.crt
server.key
server-ca.crt
shibboleth2.xml.sample
workers.conf

Configure SSO using config script (configApacheShibd.bat)



configApacheShibd.bat

D:\OAS_WIN_SAML\configApacheShibd.bat

This script needs Input value while running the script.

e.g Running the script from D:\OAS_WIN_SAML

....

Apache HTTP Server Configuration

....

Enter Apache HTTP Server Install Path e.g C:\Apache24 : D:\Apache24

Enter Apache HTTP Server or Load Balancer Hostname whichever will be the Front End URL DNS Name

Enter Apache HTTP Server or Load Balancer Hostname : oas.example.com

NOTE: Apache/LB SSL Certs and Private Key along with CA Intermediate and CA Root Certificates as Chain cert (i.e. server.crt, server.key, server-ca.crt) should be copied to Location where configApacheShibd.bat file runs

Checking if the Apache or Load Balancer SSL Certificates are copied to D:\OAS_WIN_SAML or not

If SSL Certificates does not exist program will exit

Re-run after copying the SSL Certificates to D:\OAS_WIN_SAML

OAS WebLogic Managed Server Hostname : oas.subnet1234.vcn1234.oraclevcn.com

OAS WebLogic Managed Server Port Number : 9502

Is the OAS WebLogic Managed Server running is SSL (yes/no) : no

....

Shibboleth SP Configuration

....

Enter Shibboleth SP Install Path e.g C:\opt\shibboleth-sp : D:\opt\shibboleth-sp

Signing Enabled for SAML Assertions (yes/no) :no

Encryption Enabled for SAML Assertions (yes/no) :no

Enter SAML Identity Provider's EntityID :http://adfs-server.com/adfs/services/trust

Enter E-Mail ID of the Support Contact :ssoadmin@company.com

NOTE: SAML IDP Metadata XML file should be copied to the Location where configApacheShibd.bat file runs with a name as saml-idp-metadata.xml

Checking if the SAML IDP Metadata XML file named (saml-idp-metadata.xml) is copied to D:\OAS_WIN_SAML or not

If saml-idp-metadata.xml does not exist program will exit

Re-run after copying the saml-idp-metadata.xml to D:\OAS_WIN_SAML

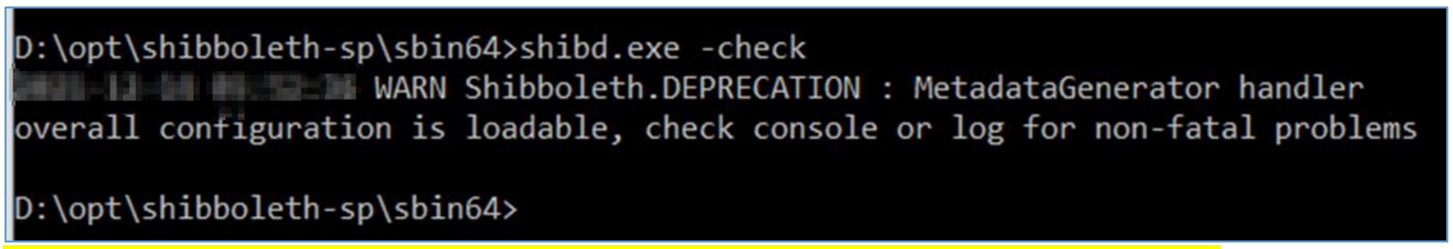
Enter any of these NameID Formats unspecified or emailAddress or persistent

Enter the NameID Attribute from any of these unspecified or emailAddress or persistent : unspecified

After gathering the required Inputs, the script continues to complete the configuration

Test the shibboleth configuration

D:\opt\shibboleth-sp\sbin64\shibd.exe -check



```
D:\opt\shibboleth-sp\sbin64>shibd.exe -check
[redacted] WARN Shibboleth.DEPRECATION : MetadataGenerator handler
overall configuration is loadable, check console or log for non-fatal problems

D:\opt\shibboleth-sp\sbin64>
```

overall configuration is loadable, check console or log for non-fatal problems

Start or Restart Apache and Shibboleth Services

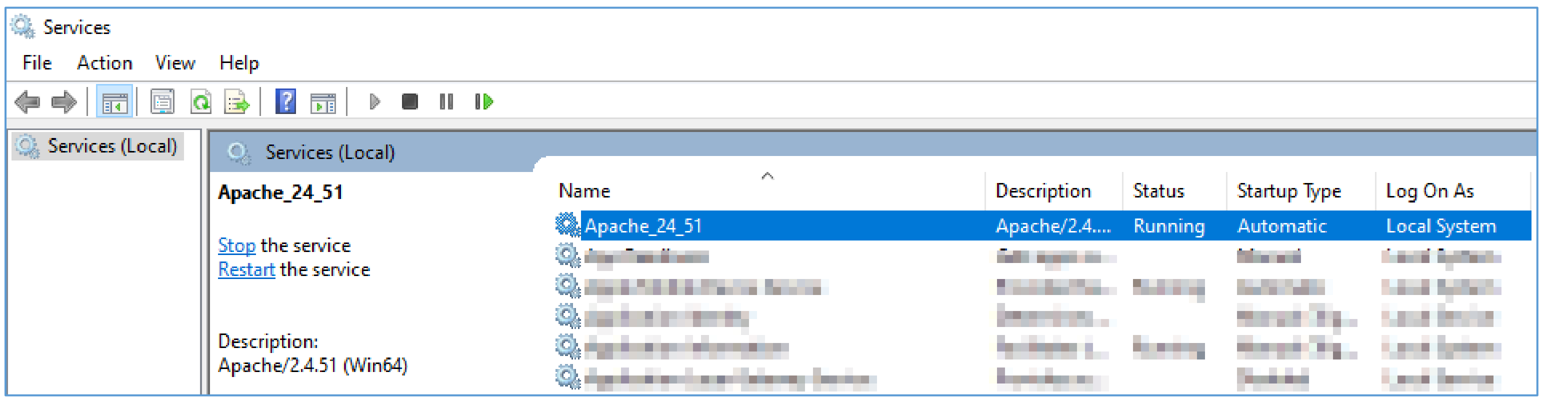
Apache HTTP Server:

D:\Apache24\bin\httpd -k stop -n “Apache_24_51”

D:\Apache24\bin\httpd -k start -n “Apache_24_51”

D:\Apache24\bin\httpd -k restart -n “Apache_24_51”

Or through Services



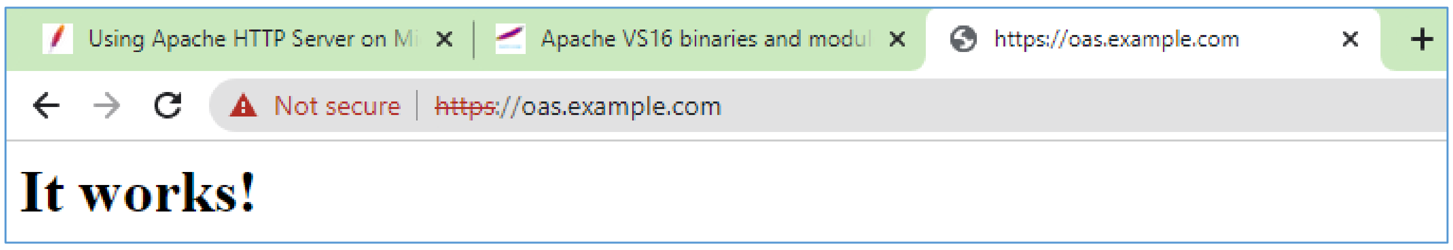
Apache_24_51

Stop the service
Restart the service

Description:
Apache/2.4.51 (Win64)

Name	Description	Status	Startup Type	Log On As
Apache_24_51	Apache/2.4....	Running	Automatic	Local System
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Test Apache:



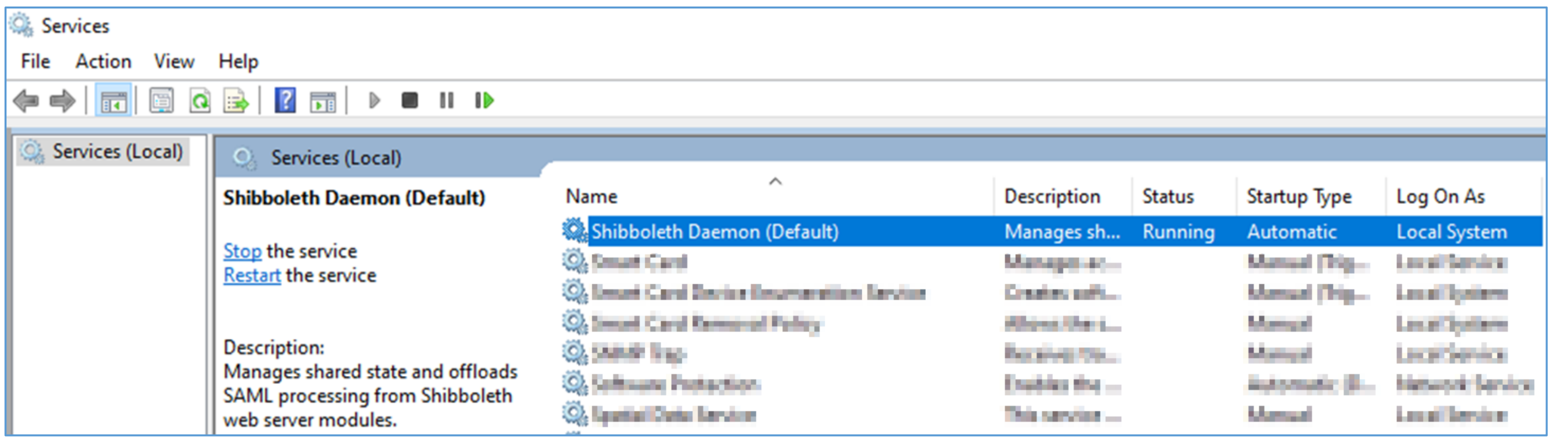
Using Apache HTTP Server on Mi
Apache VS16 binaries and modul
https://oas.example.com
Not secure
~~https~~://oas.example.com

It works!

Shibboleth SP:

Command Line: c:\> sc start shibd_default

Or through services



Shibboleth Daemon (Default)

Stop the service
Restart the service

Description:
Manages shared state and offloads SAML processing from Shibboleth web server modules.

Name	Description	Status	Startup Type	Log On As
Shibboleth Daemon (Default)	Manages sh...	Running	Automatic	Local System
[redacted]	[redacted]		[redacted]	[redacted]
[redacted]	[redacted]		[redacted]	[redacted]
[redacted]	[redacted]		[redacted]	[redacted]
[redacted]	[redacted]		[redacted]	[redacted]
[redacted]	[redacted]		[redacted]	[redacted]
[redacted]	[redacted]		[redacted]	[redacted]

Test the OAS SAML SP Metadata URL

https://oas.example.com/Shibboleth.sso/Metadata

oas_metadata.xml

SAML SP Metadata sample

****

```
<!--
This is example metadata only. Do *NOT* supply it as is without review,
and do *NOT* provide it in real time to your partners.
-->
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ID="_23ccbcbf9d46af1e15d583a65cd91d72bde57e54"
entityID="https://oas.example.com/analytics/shibboleth">

 <md:Extensions xmlns:alg="urn:oasis:names:tc:SAML:metadata:algsupport">
  <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"/>
  <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha384"/>
  <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
  <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha224"/>
  <alg:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <alg:SigningMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512"/>
  <alg:SigningMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384"/>
  <alg:SigningMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256"/>
  <alg:SigningMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha224"/>
  <alg:SigningMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha512"/>
  <alg:SigningMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha384"/>
  <alg:SigningMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
  <alg:SigningMethod Algorithm="http://www.w3.org/2009/xmldsig11#dsa-sha256"/>
  <alg:SigningMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha1"/>
  <alg:SigningMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
  <alg:SigningMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
 </md:Extensions>

 <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <md:Extensions>
   <init:RequestInitiator xmlns:init="urn:oasis:names:tc:SAML:profiles:SSO:request-init" Binding="urn:oasis:names:tc:SAML:profiles:SSO:request-init"
Location="https://oas.example.com/Shibboleth.sso/Login"/>
  </md:Extensions>
  <md:KeyDescriptor use="signing">
   <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:KeyName>oas.example.com</ds:KeyName>
```

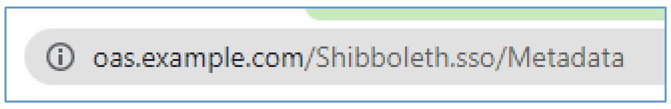
```
      <ds:X509Data>
        <ds:X509SubjectName>emailAddress=ssoadmin@company.com,CN=oas.example.com,OU=CEAL Team,O=Oracle Corporation,L=Redwood Shores,ST=California,C=US</ds:X509SubjectName>
        <ds:X509Certificate>MIIFGjCCBAKgAwIBAgIBdDANBgkqhkiG9w0BAQsFADCBwDELMAkGA1UEBhMCVVMx
EzARBgNVBAgTCkNhbGlmb3JuaWExFDASBgNVBAcTC1NhbnRhIENsYXJhMRswGQYD
AxMeT3JhY2xlIEJpIENlYWwgSW50ZXJtZWRpYXRlIENBMS8wLQYJKoZIhvcNAQkB
FiB2ZWVyYS5yYWdoYXZlbmRyYS5yYW9Ab3JhY2xlLmNvbTAeFw0yMTEyMTMyMTM4
...
...
Xwg85zLCtDyWHBauwwIDAQABo4IBJDCCASAwCQYDVR0TBAIwADAdBgNVHQ4EFgQU
cmF0aW9uMQ8wDQYDVQQLEwZCSUNFQUwxLTArBgNVBAMTJE9yYWNsZSBCaSBDZWFs
xqo1wBmQBc1ak20Nh5cI5Qa0Z+3Wuux2H7KsEcLWkgc/DcCpZi+ZFCsblztXdE8e
wJYK6+GB1ouKjbeTkWA=
</ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </md:KeyDescriptor>
  <md:KeyDescriptor use="encryption">
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:KeyName>oas.example.com</ds:KeyName>
      <ds:X509Data>
        <ds:X509SubjectName>emailAddress=ssoadmin@company.com,CN=oas.example.com,OU=CEAL Team,O=Oracle Corporation,L=Redwood Shores,ST=California,C=US</ds:X509SubjectName>
        <ds:X509Certificate>MIIFGjCCBAKgAwIBAgIBdDANBgkqhkiG9w0BAQsFADCBwDELMAkGA1UEBhMCVVMx
EzARBgNVBAgTCkNhbGlmb3JuaWExFDASBgNVBAcTC1NhbnRhIENsYXJhMRswGQYD
VQQKExJPcmFjbGUgQ29ycG9yYXRpb24xDzANBgNVBAsTBkJJQ0VBTDEnMCUGA1UE
...
...
ER1Yn3l2PNuhgcykgckwgcYxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9y
bmlhMRQwEgYDVQQHEwtTYW50YSBDbGFyYTEbMBkGA1UEChMST3JhY2xlIENvcnBv
wJYK6+GB1ouKjbeTkWA=
</ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
    <md:EncryptionMethod Algorithm="http://www.w3.org/2009/xmlenc11#aes128-gcm"/>
    <md:EncryptionMethod Algorithm="http://www.w3.org/2009/xmlenc11#aes192-gcm"/>
    <md:EncryptionMethod Algorithm="http://www.w3.org/2009/xmlenc11#aes256-gcm"/>
    <md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
    <md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes192-cbc"/>
    <md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
    <md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
    <md:EncryptionMethod Algorithm="http://www.w3.org/2009/xmlenc11#rsa-oaep"/>
    <md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>
  </md:KeyDescriptor>
  <md:ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://oas.example.com/Shibboleth.sso/Artifact/SOAP" index="1"/>
  <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://oas.example.com/Shibboleth.sso/SLO/SOAP"/>
  <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://oas.example.com/Shibboleth.sso/SLO/Redirect"/>
  <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://oas.example.com/Shibboleth.sso/SLO/POST"/>
  <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="https://oas.example.com/Shibboleth.sso/SLO/Artifact"/>
  <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://oas.example.com/Shibboleth.sso/SAML2/POST" index="1"/>
```

```
   <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign"
Location="https://oas.example.com/Shibboleth.sso/SAML2/POST-SimpleSign" index="2"/>

   <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
Location="https://oas.example.com/Shibboleth.sso/SAML2/Artifact" index="3"/>

   <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:PAOS" Location="https://oas.example.com/Shibboleth.sso/SAML2/ECP"
index="4"/>

  </md:SPSSODescriptor>


</md:EntityDescriptor>
```

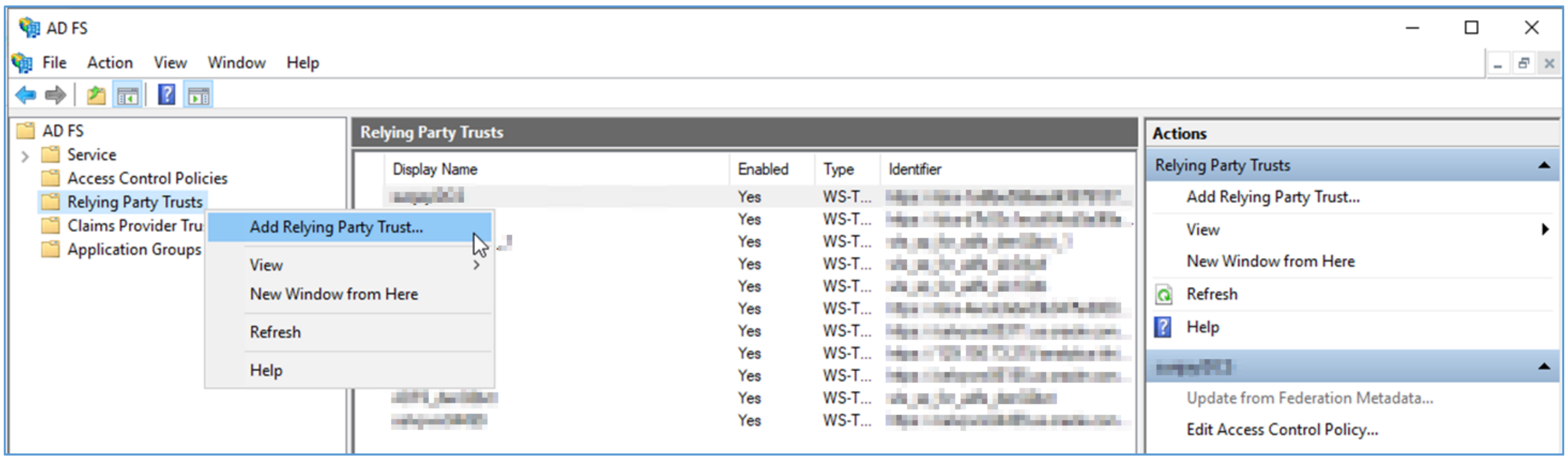
****

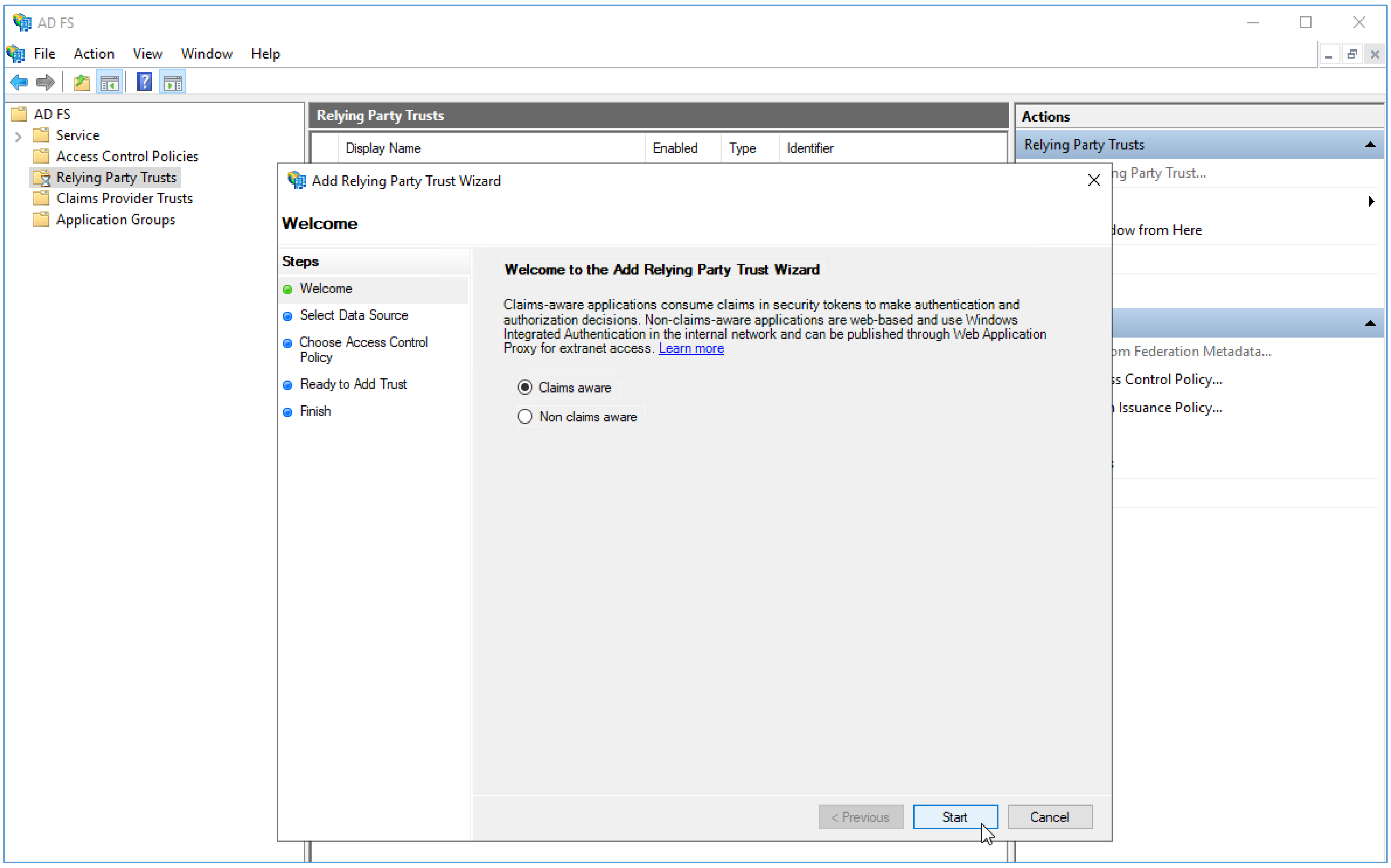
NOTE: We can delete the green Highlighted comments and share this file with SAML IDP Administrator.

Sample Configuration steps at ADFS Server:



oas.example.com/Shibboleth.sso/Metadata



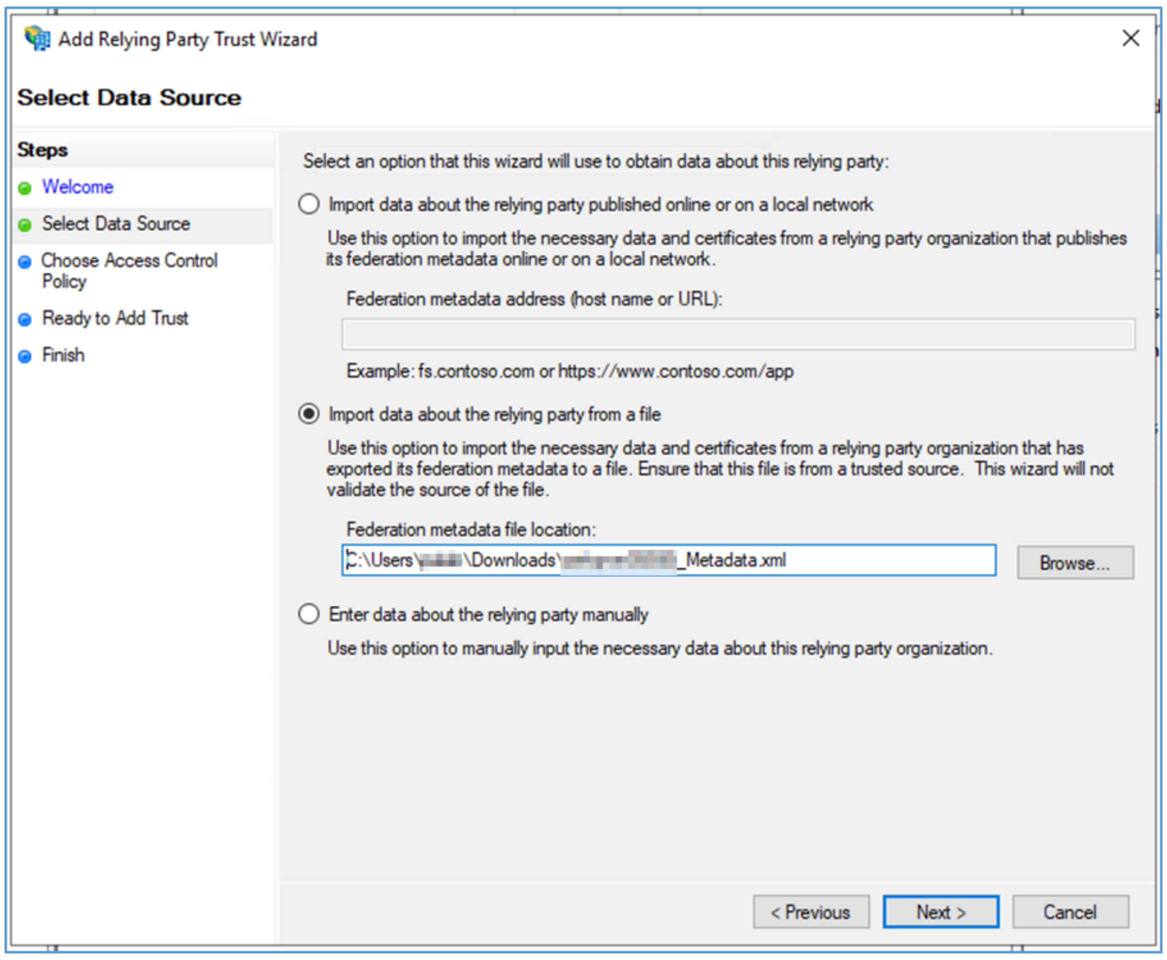


Welcome to the Add Relying Party Trust Wizard

Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. Learn more

● Claims aware

○ Non claims aware



Add Relying Party Trust Wizard

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

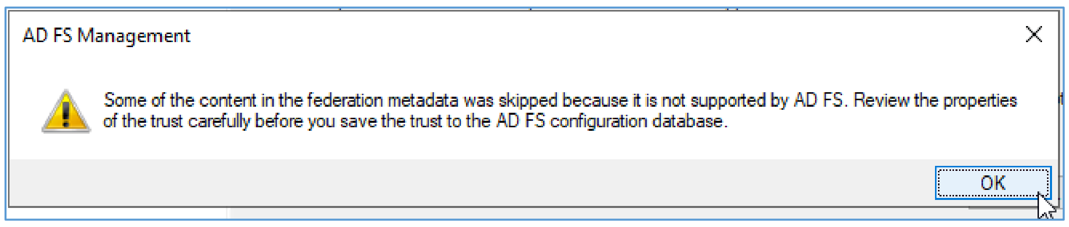
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

C:\Users\[redacted]\Downloads\[redacted]_Metadata.xml

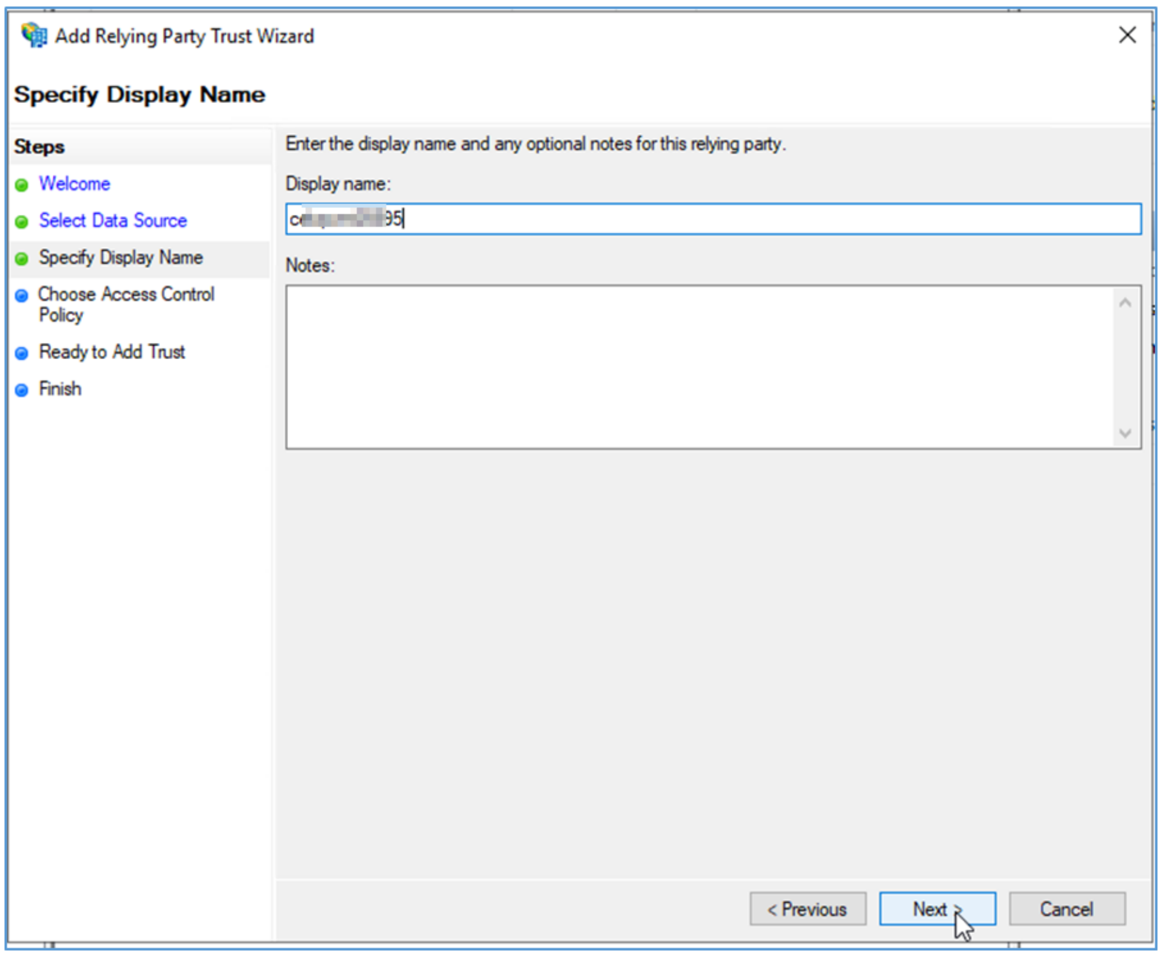
○ Enter data about the relying party manually

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



AD FS Management

Some of the content in the federation metadata was skipped because it is not supported by AD FS. Review the properties of the trust carefully before you save the trust to the AD FS configuration database.



Add Relying Party Trust Wizard

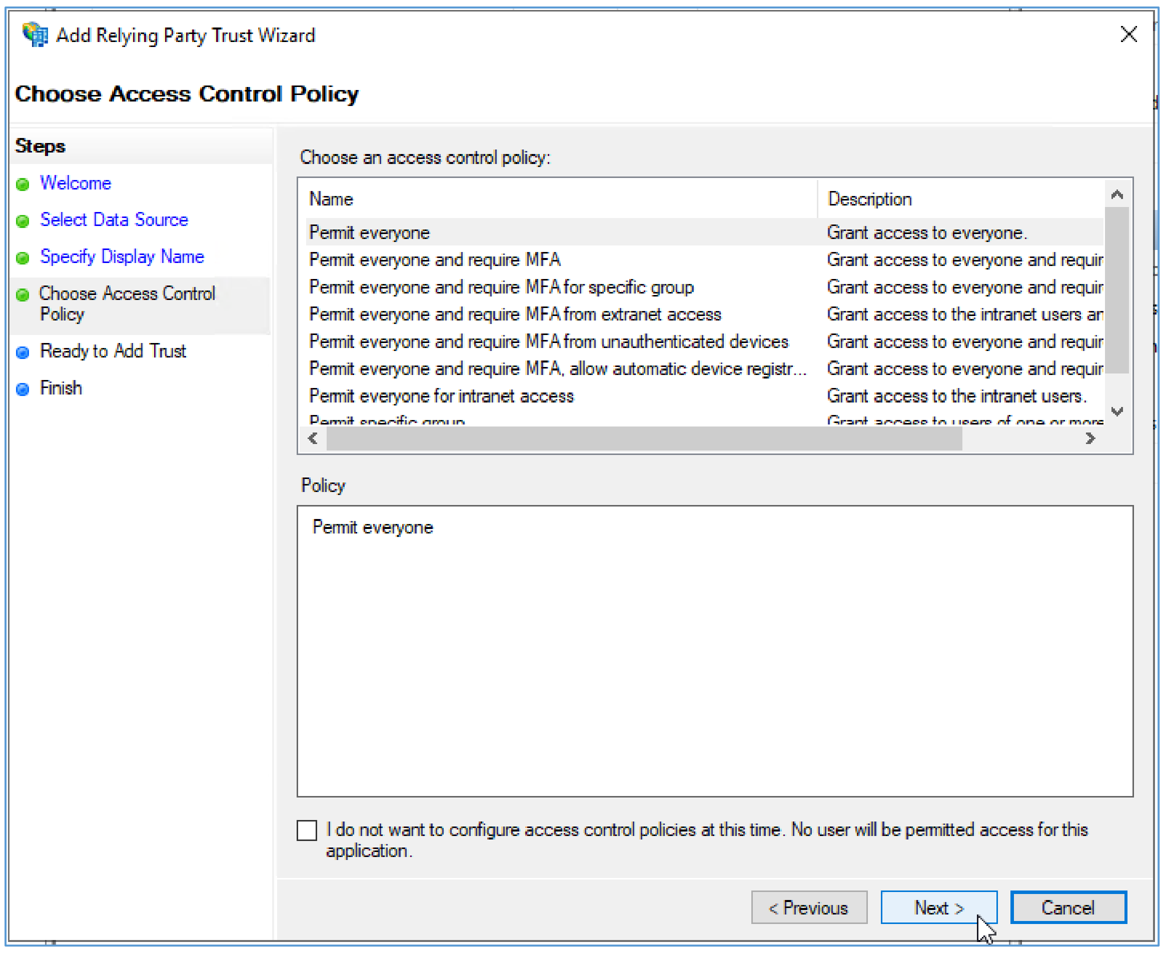
Specify Display Name

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

Display name:

ce[redacted]95

Notes:



Add Relying Party Trust Wizard

Choose Access Control Policy

Steps
- Welcome
- Select Data Source
- Specify Display Name
- Choose Access Control Policy
- Ready to Add Trust
- Finish

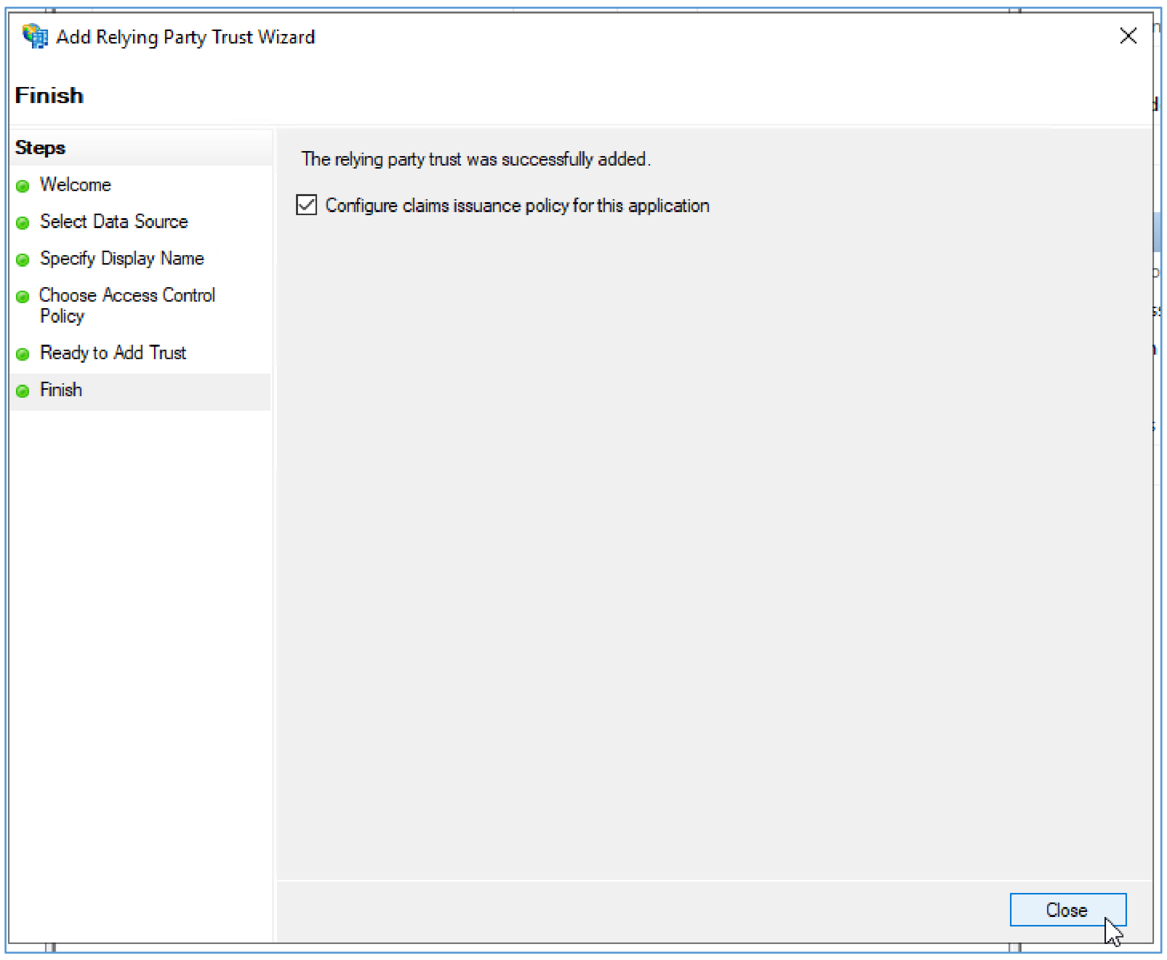
Choose an access control policy:

Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and requir
Permit everyone and require MFA for specific group	Grant access to everyone and requir
Permit everyone and require MFA from extranet access	Grant access to the intranet users ar
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and requir
Permit everyone and require MFA, allow automatic device registr...	Grant access to everyone and requir
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more

Policy

Permit everyone

□ I do not want to configure access control policies at this time. No user will be permitted access for this application.



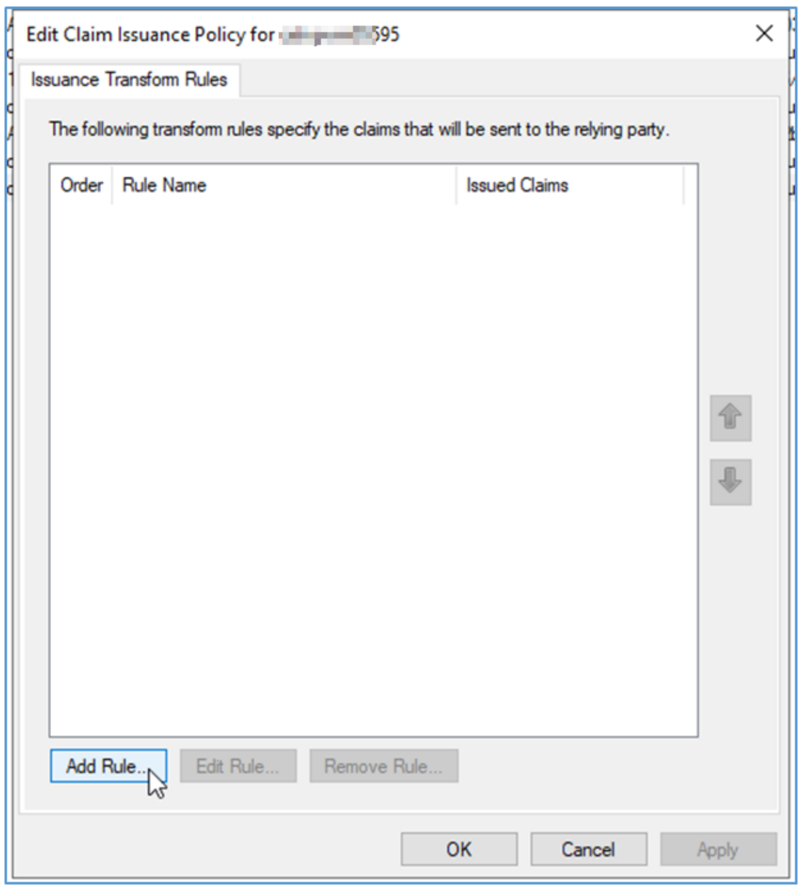
Add Relying Party Trust Wizard

Finish

Steps
- Welcome
- Select Data Source
- Specify Display Name
- Choose Access Control Policy
- Ready to Add Trust
- Finish

The relying party trust was successfully added.

☑ Configure claims issuance policy for this application

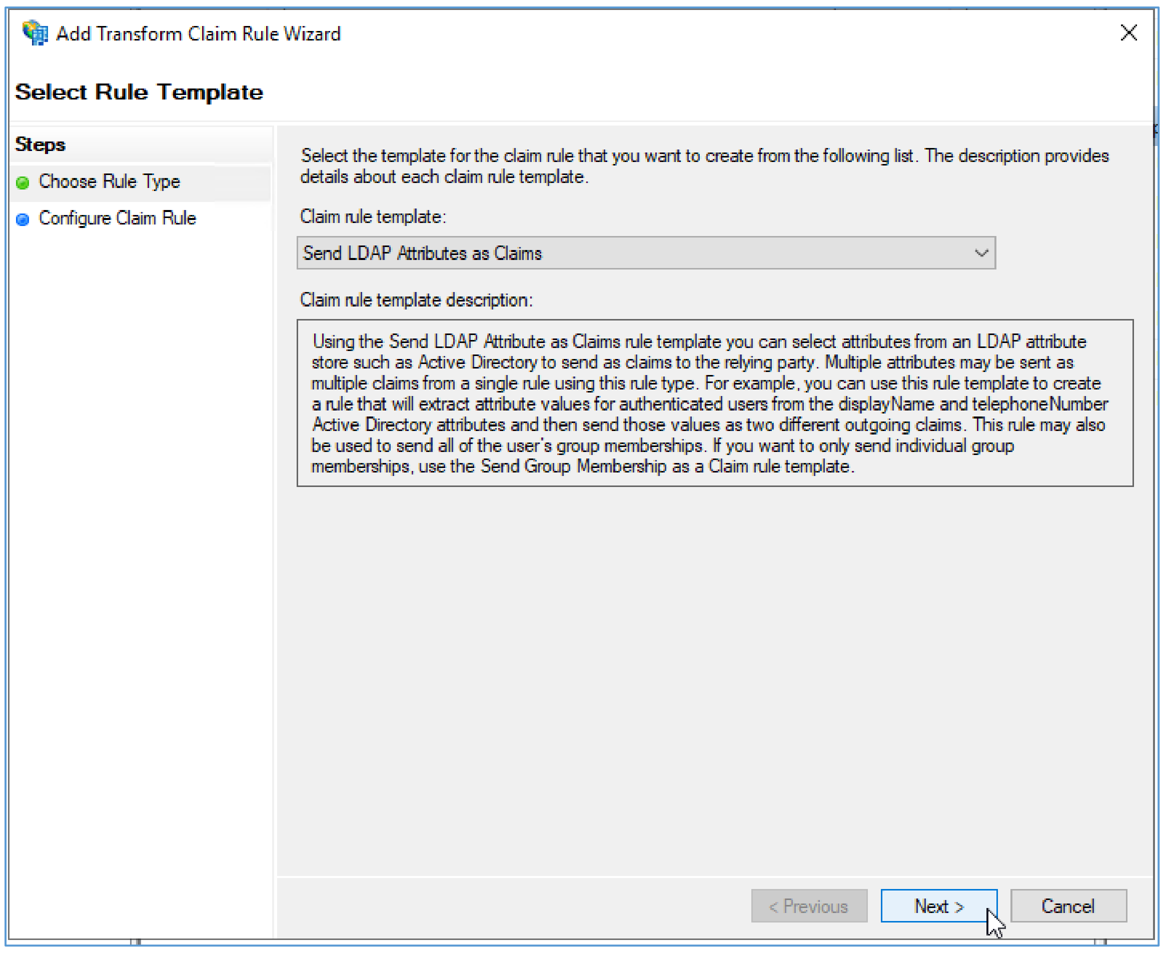


Edit Claim Issuance Policy for [redacted]595

Issuance Transform Rules

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

Order	Rule Name	Issued Claims



Add Transform Claim Rule Wizard

Select Rule Template

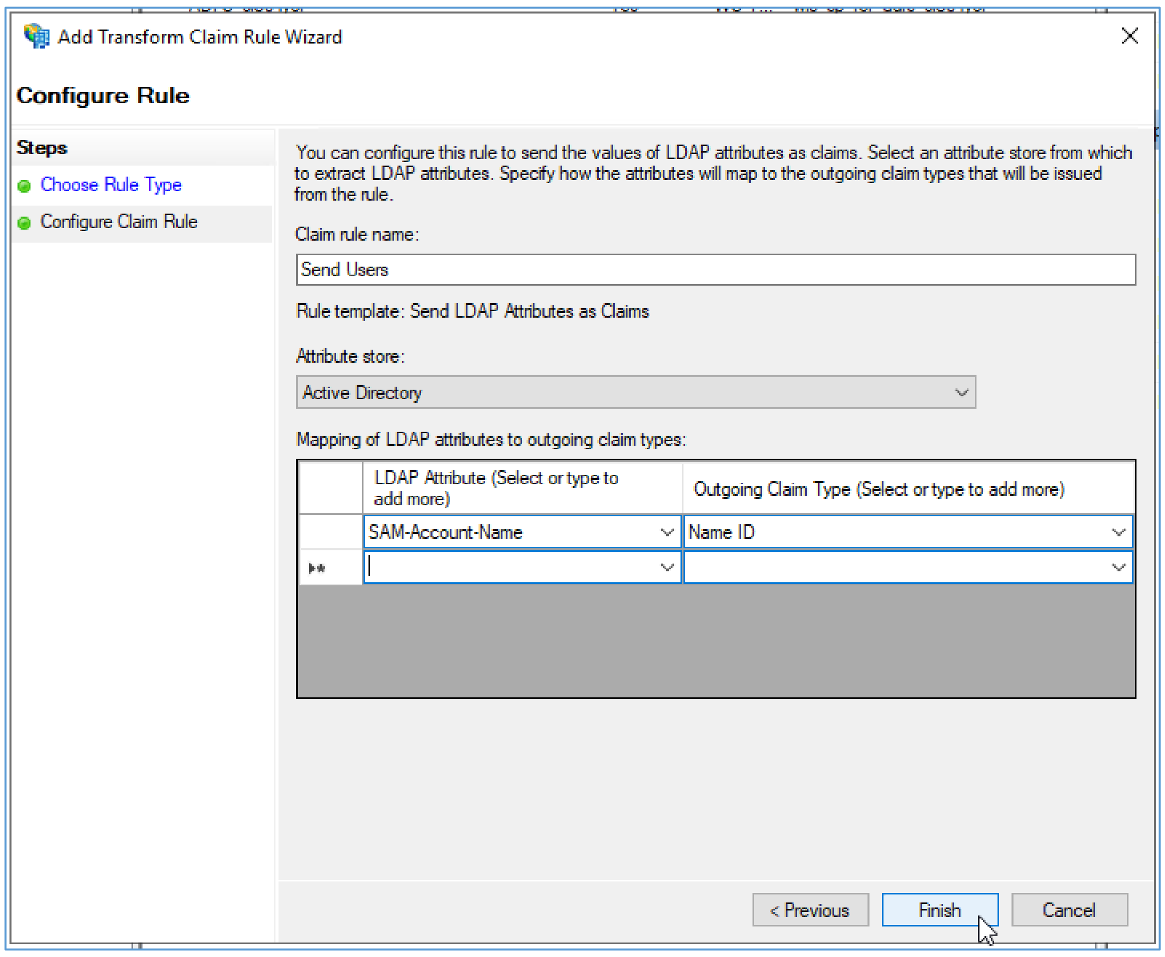
Steps
- Choose Rule Type
- Configure Claim Rule

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.



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.

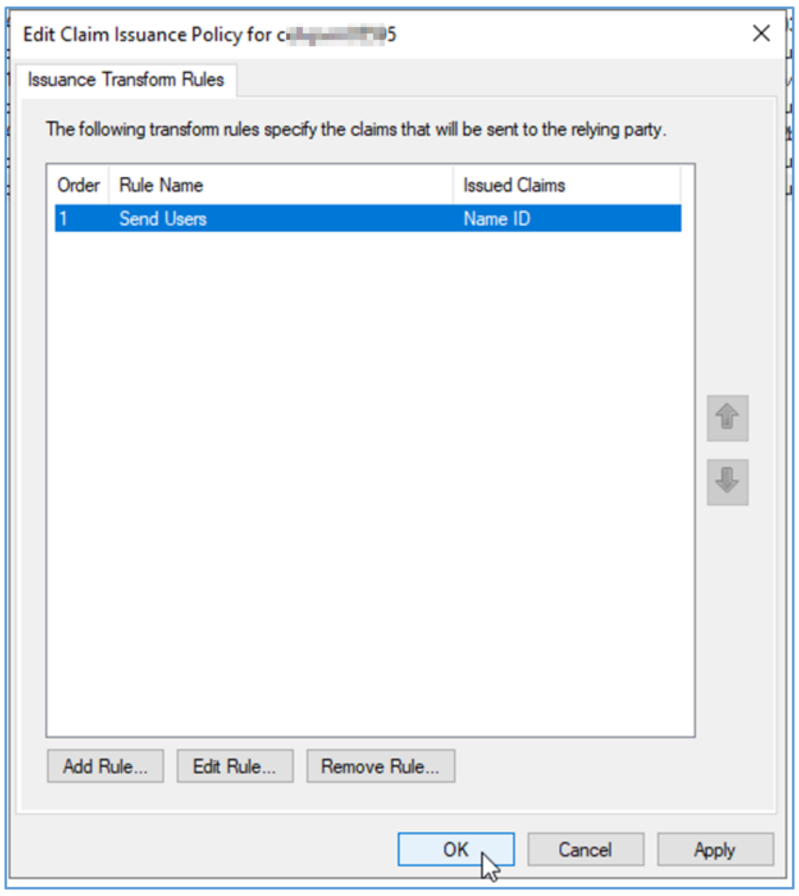
Claim rule name: Send Users

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
▸*		

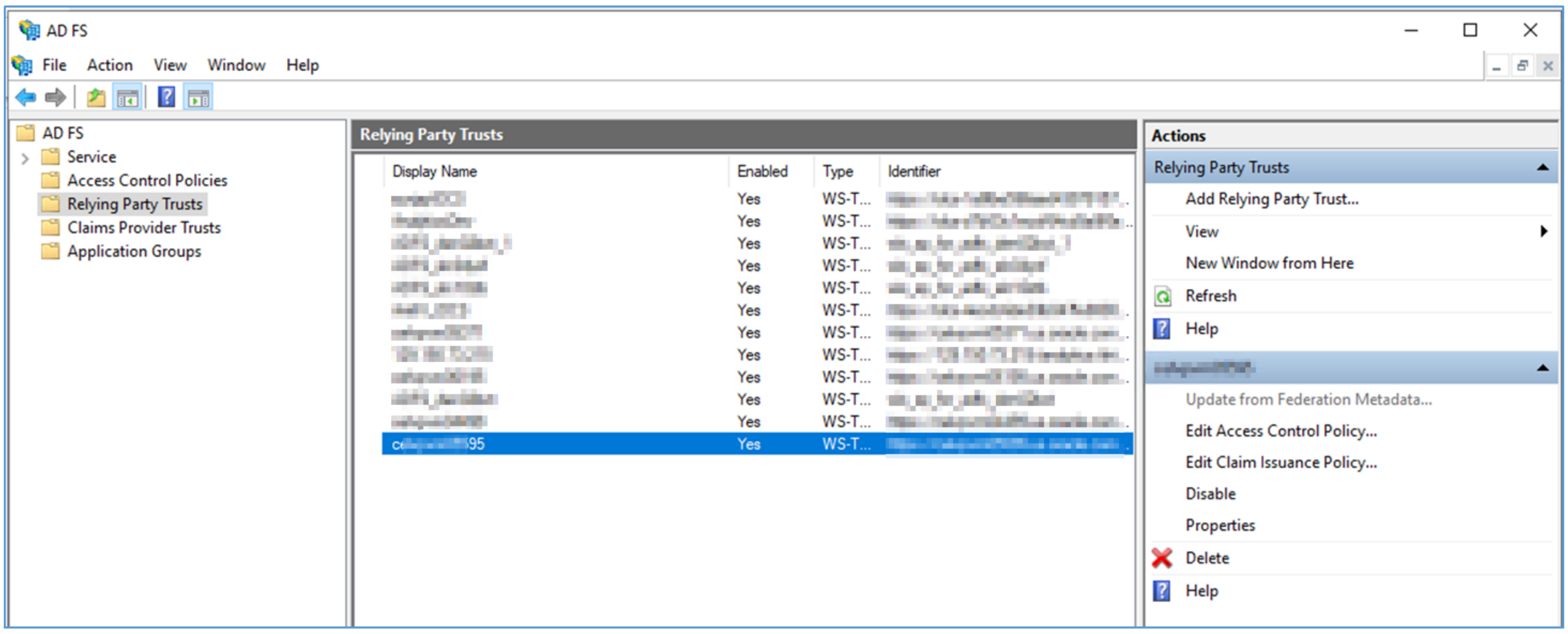


Edit Claim Issuance Policy for c[redacted]5

Issuance Transform Rules

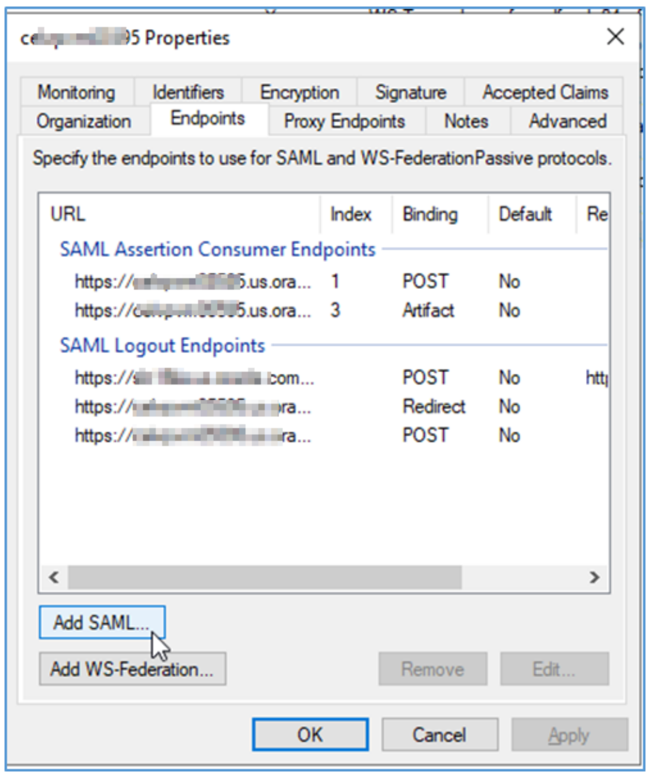
The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Send Users	Name ID



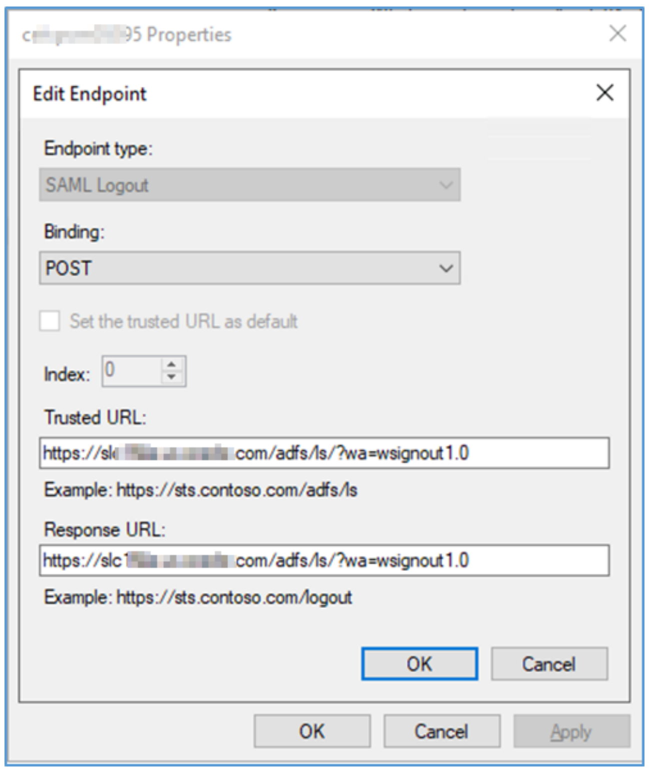
Display Name	Enabled	Type	Identifier
[redacted]	Yes	WS-T...	[redacted]
[redacted]	Yes	WS-T...	[redacted]
[redacted]	Yes	WS-T...	[redacted]
[redacted]	Yes	WS-T...	[redacted]
[redacted]	Yes	WS-T...	[redacted]
[redacted]	Yes	WS-T...	[redacted]
[redacted]	Yes	WS-T...	[redacted]
[redacted]	Yes	WS-T...	[redacted]
[redacted]	Yes	WS-T...	[redacted]
[redacted]	Yes	WS-T...	[redacted]
[redacted]	Yes	WS-T...	[redacted]
ce[redacted]95	Yes	WS-T...	[redacted]

Edit and add the SAML Logout End point for the relying party.



Specify the endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	Binding	Default	Re
SAML Assertion Consumer Endpoints				
https://[redacted]5.us.ora...	1	POST	No	
https://[redacted]5.us.ora...	3	Artifact	No	
SAML Logout Endpoints				
https://[redacted].com...		POST	No	htt
https://[redacted]ra...		Redirect	No	
https://[redacted]ra...		POST	No	



Endpoint type: SAML Logout

Binding: POST

□ Set the trusted URL as default

Index: 0

Trusted URL: https://sl[redacted].com/adfs/ls/?wa=wsignout1.0

Example: https://sts.contoso.com/adfs/ls

Response URL: https://slc[redacted].com/adfs/ls/?wa=wsignout1.0

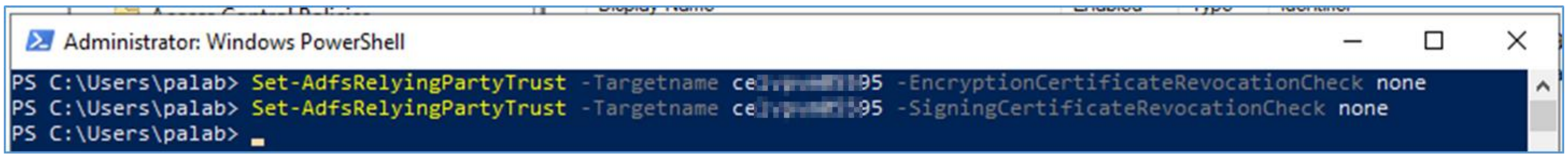
Example: https://sts.contoso.com/logout

https://adfs-server.oracle.com/adfs/ls/?wa=wsignout1.0

We need to disable the RevocationCheck for the certificates in ADFS

Set-AdfsRelyingPartyTrust -Targetname cexxxxxxxxx95 -EncryptionCertificateRevocationCheck none

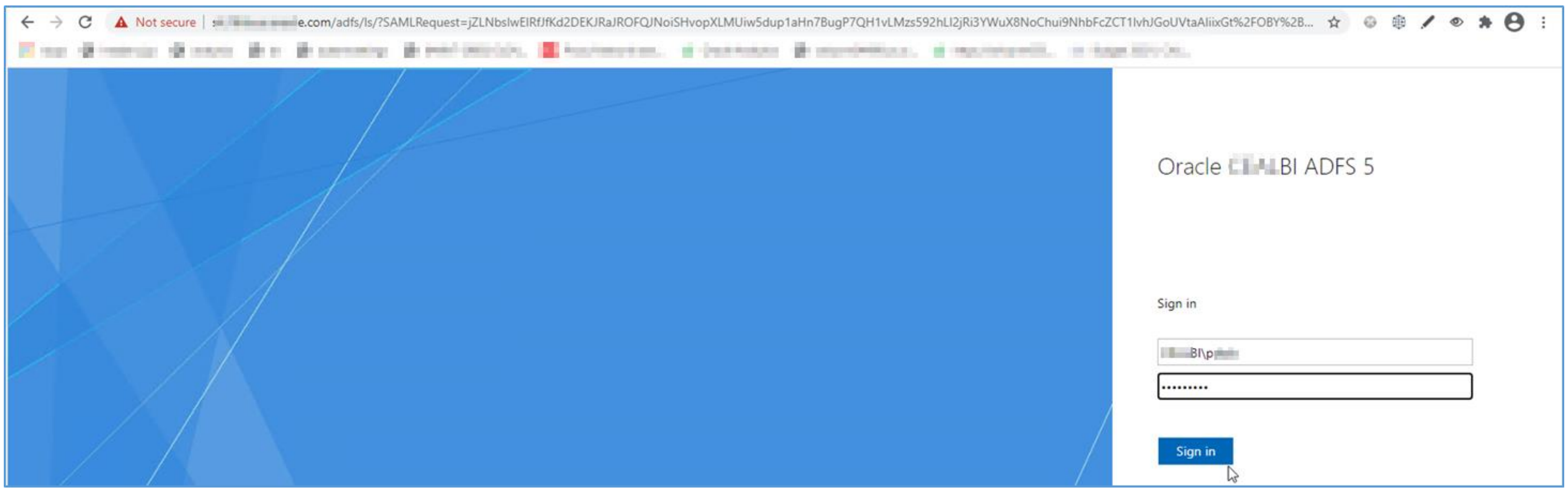
Set-AdfsRelyingPartyTrust -Targetname cexxxxxxxxx95 -SigningCertificateRevocationCheck none



```
PS C:\Users\palab> Set-AdfsRelyingPartyTrust -Targetname ce[redacted]95 -EncryptionCertificateRevocationCheck none
PS C:\Users\palab> Set-AdfsRelyingPartyTrust -Targetname ce[redacted]95 -SigningCertificateRevocationCheck none
PS C:\Users\palab> _
```

Test SAML SSO

https://oas.example.com/analytics



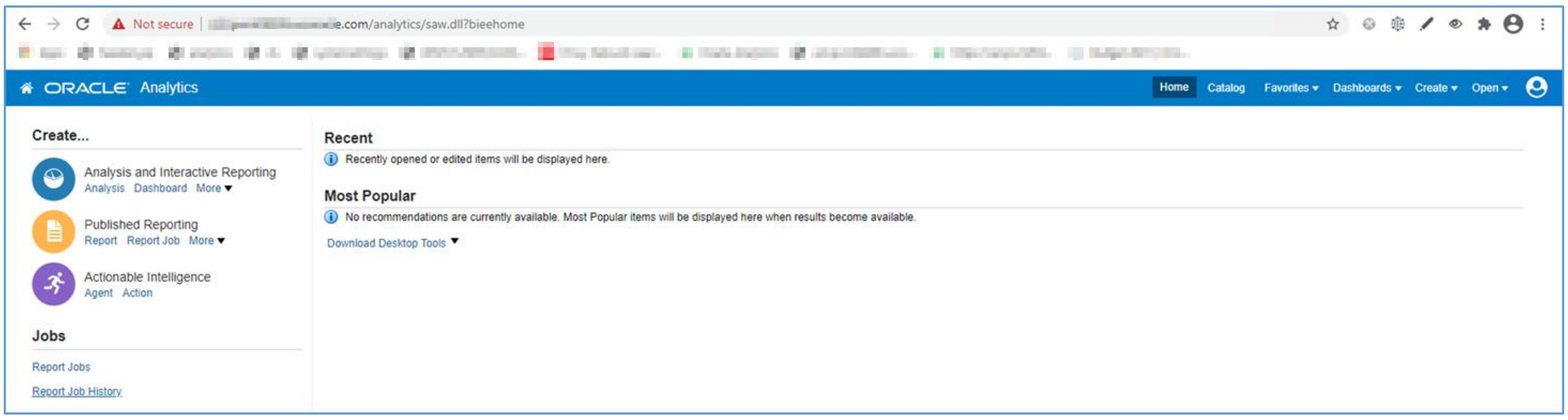
Not secure | [redacted]e.com/adfs/ls/?SAMLRequest=jZLNbslwEIRfJfKd2DEKJRaJROFQJNoiSHvopXLMUiw5dup1aHn7BugP7QH1vLMzs592hLI2jRi3YWuX8NoChui9NhbFcZCT1lvhJGoUVtaAliixGt%2FOBY%2B...

Oracle [redacted] BI ADFS 5

Sign in

[redacted]BI\p[redacted]

••••••••••

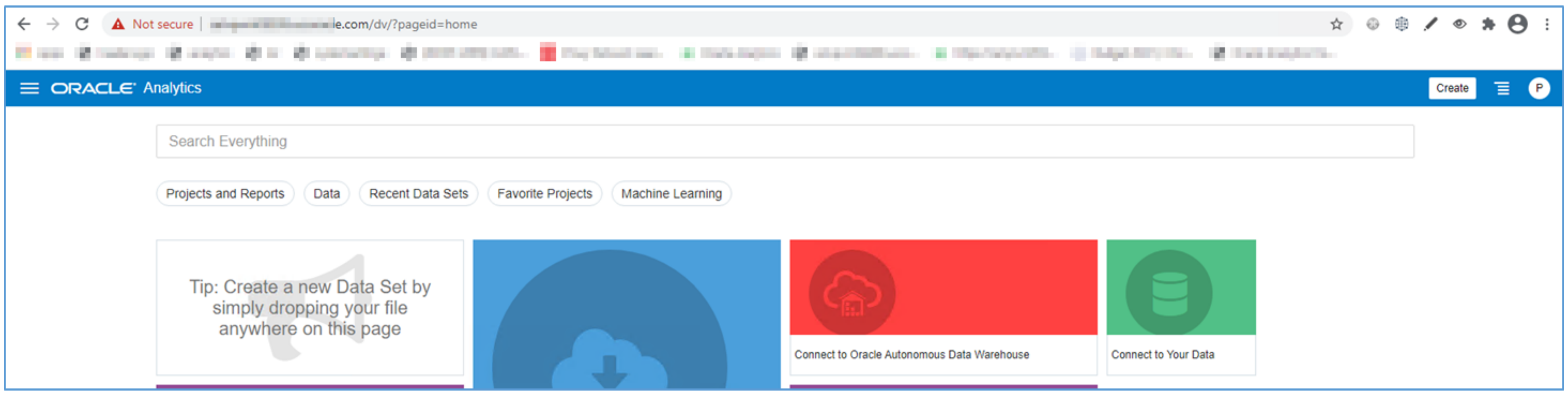


Not secure | [redacted]e.com/analytics/saw.dll?bieehome

Recently opened or edited items will be displayed here.

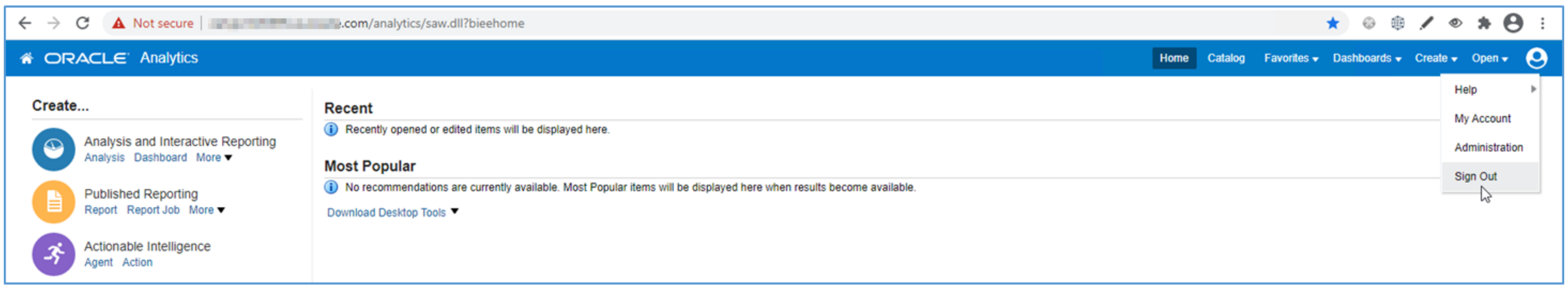
No recommendations are currently available. Most Popular items will be displayed here when results become available.

https://oas.example.com/dv



Not secure | [redacted]e.com/dv/?pageid=home

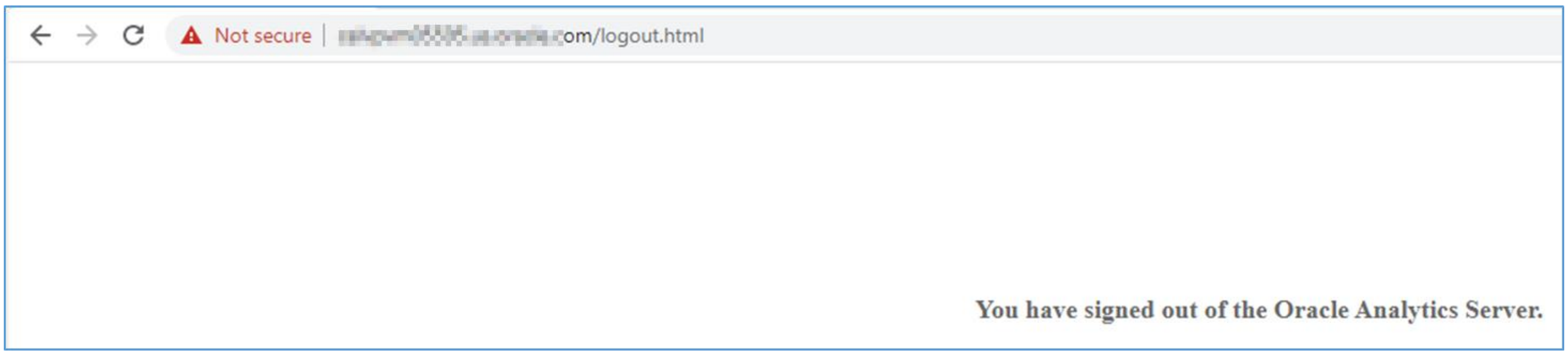
Tip: Create a new Data Set by simply dropping your file anywhere on this page



Not secure | [redacted].com/analytics/saw.dll?bieehome

Recently opened or edited items will be displayed here.

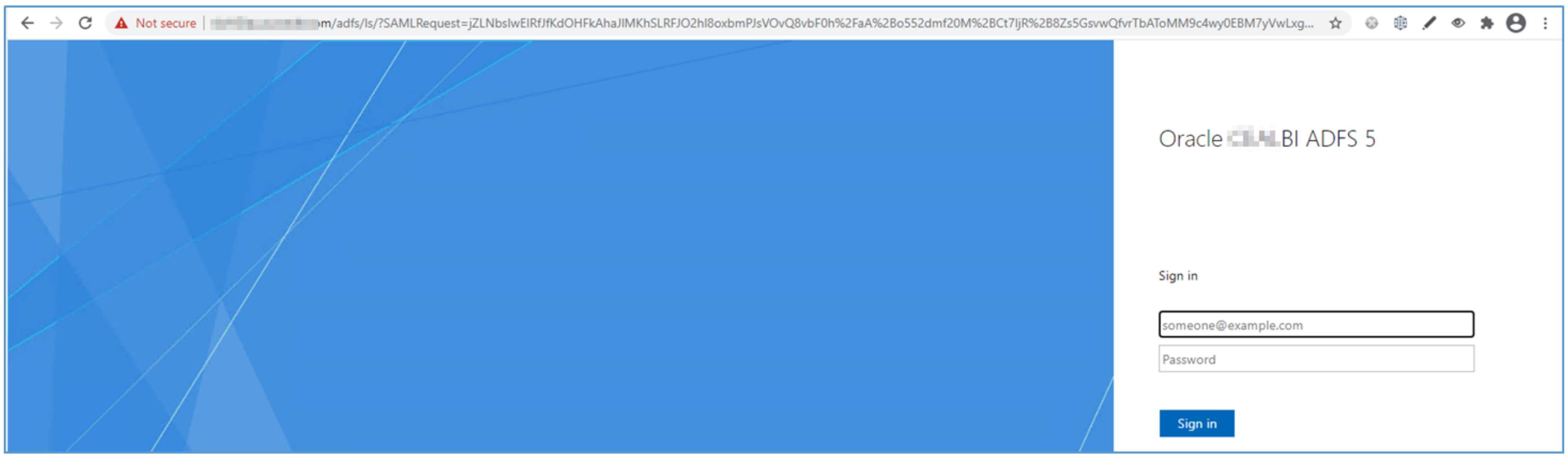
No recommendations are currently available. Most Popular items will be displayed here when results become available.



Not secure | [redacted]com/logout.html

You have signed out of the Oracle Analytics Server.

Again in the same browser/tab access analytics URL



Not secure | [redacted]m/adfs/ls/?SAMLRequest=jZLNbslwEIRfJfKdOHFkAhaJIMKhSLRFJO2hl8oxbmPJsVOvQ8vbF0h%2FaA%2Bo552dmf20M%2BCt7IjR%2B8Zs5GsvwQfvrTbAToMM9c4wy0EBM7yVwLxg...

Oracle [redacted] BI ADFS 5

Sign in

someone@example.com

Password

Sign in

It goes to ADFS Login page.

Configuring WebLogic to prevent direct access to BI

Follow the WebLogic documentation to configure a Connection Filter so that only the Apache HTTP Server is protected by the SAML SP module and machines running BI components are allowed to access the WebLogic server:

Instructions on configuring the default connection filter are contained in the section entitled “Using Connection Filters” in the WebLogic documentation at:

Using Network Connection Filters
Instructions on writing an appropriate filter rule are contained in the section entitled “Guidelines for Writing Connection Filter Rules” in WebLogic documentation at:

Guidelines for Writing Connection Filter Rules
Your filter rule should look like this:

[Apache http server IP Address] * [WebLogic Admin Server Port] allow
[Apache http IP Address] * [WebLogic Managed Server Port] allow

[BI component server IP Address] * [WebLogic Admin Server Port] allow

[Another BI component server IP Address (if it exists)] * [WebLogic Managed Server Port] allow

0.0.0.0/0 * * deny

Test that you can access the WebLogic Administration Console and Analytics URLs via the web server, but not directly from any other machine.

Protecting direct HTTP access to OBIPS

Follow the guidance in the 'Managing Security for Oracle Analytics Server' documentation guide,

SSO Implementation Considerations

For convenience, an extract from the OAS document is shown below.

When implementing an SSO solution with Oracle Analytics Server you should consider the following:

When accepting trusted information from the HTTP server or servlet container, you must secure the machines that communicate directly with Presentation Services. In the instanceconfig.xml file, specify the list of HTTP Server or servlet container IP addresses in the Listener\Firewall node. The Firewall node must include the IP addresses of all Oracle BI Scheduler instances, Oracle Presentation Services instances, and Oracle Analytics Server JavaHost instances.

If any of these components are co-located with Oracle BI Presentation Services, you must add the 127.0.0.1 address in Firewall node. Setting the list of HTTP Server or servlet container IP addresses does not control end-user browser IP addresses. When using mutually-authenticated SSL, you must specify the Distinguished Names (DNs) of all trusted hosts in the Listener\TrustedPeers node.

For example:

```
<Listener port="XXXX" ssl="false">
<Firewall>
<Allow address="127.0.0.1"/>
<Allow address="XXX.XXX.X.XXX"/>
<Allow address="XXX.XXX.X.XXY"/>
</Firewall>
</Listener>
```

Uninstalling Configuration

It's a manual task as of now

For Apache HTTP Server

cd D:\Apache24

copy the **conf** folder from Apache Installer zip file and replace it under D:\Apache24

delete D:\Apache24\htdocs\logout.html

For Shibboleth

cd D:\opt\shibboleth-sp\etc\shibboleth

copy **shibboleth2.xml.original** shibboleth2.xml

copy **attribute-map.xml.original** attribute-map.xml

Re-Configure

Run D:\OAS_WIN_SAML\configApacheShibd.bat to re-configure

High Availability of OAS Nodes

NOTE: Current Apache and Shibboleth Configuration is by default for OAS Single Node SSO setup.

If we need High Availability perform below steps

Edit D:\Apache24\conf\httpd.conf

goto end of the file

```
***************************************************************************************************************

# If the OAS env is a Single node env uncomment below line to load analytics.conf

Include conf/analytics.conf                                   Comment this line

# If the OAS env is a multi node clustered env

# Comment above analytics.conf and Uncomment below analyticsclustered.conf and workers.conf

#Include conf/analyticsclustered.conf                         Uncomment this line

#Include conf/workers.conf                                    Uncomment this line

***************************************************************************************************************
```

Edit D:\Apache24\conf\workers.conf

```
*******************************************************************************************************************

ProxyPreserveHost On

<Proxy "balancer://workers">

   BalancerMember "http://<oas-server1.com>:9502"   Edit the values accordingly to the env

   BalancerMember "http://<oas-server2.com>:9502"   Also add more BalancerMembers based on no of OAS Servers

   ProxySet lbmethod=bytraffic

</Proxy>

*******************************************************************************************************************
```

High Availability of SSO Installation/Setup

Considering you need High Availability of SSO setup

We need to Install and configure Apache HTTP Server and Shibboleth-SP Software ad Configure on two or more Windows machines.

While Configuring:

Use same Apache HTTP Server or Load Balancer Hostname

Use same Load Balancer SSL Certificates

On first SSO Windows Server, In the analytics.conf use OAS Node1 Hostname

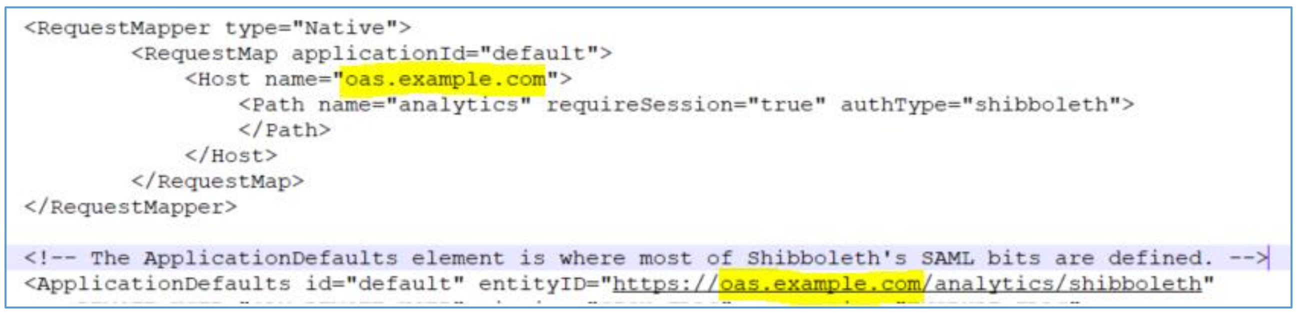
On second SSO Windows Server, In the analytics.conf use OAS Node2 Hostname

Continue for how many OAS server exist in the env.

On each SSO Node go to D:\opt\shibboleth-sp\etc\shibboleth\shibboleth2.xml

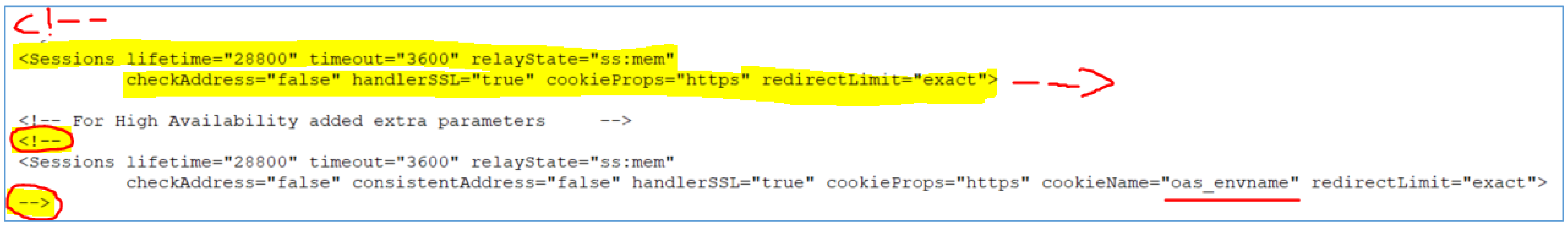
Enter same Hostname i.e of Load Balancer Hostname in all SSO Nodes.

Also maintain the same SAML SP EntityID in all SSO Nodes.



```
<RequestMapper type="Native">
        <RequestMap applicationId="default">
            <Host name="oas.example.com">
                <Path name="analytics" requireSession="true" authType="shibboleth">
                </Path>
            </Host>
        </RequestMap>
</RequestMapper>

<!-- The ApplicationDefaults element is where most of Shibboleth's SAML bits are defined. -->
<ApplicationDefaults id="default" entityID="https://oas.example.com/analytics/shibboleth"
```

Edit Sessions section:



```
<!--
<Sessions lifetime="28800" timeout="3600" relayState="ss:mem"
          checkAddress="false" handlerSSL="true" cookieProps="https" redirectLimit="exact"> -->

<!-- For High Availability added extra parameters     -->
<!--
<Sessions lifetime="28800" timeout="3600" relayState="ss:mem"
          checkAddress="false" consistentAddress="false" handlerSSL="true" cookieProps="https" cookieName="oas_envname" redirectLimit="exact">
-->
```

Add Comment to existing sessions section

Remove comments to the High availability Sessions section

Also set a proper unique cookieName like OASDEV, OASPROD, etc.