Rsam Platform

Integration with SAML-based SSO

Version: 9.2 | December 2018

Contents

About this Guide

This guide provides information on integrating a SAML-based (Security Assertion Markup Language) SSO (Single Sign On) application with Rsam. The document is intended for the users responsible for configuring the SSO application in an Rsam customer environment.

Intended Audience

This document is intended to be used only by On-Premise Rsam customers. For customers accessing the Rsam cloud instance, SSO is already configured on the Rsam cloud and is maintained by the *Rsam Technical Support* team.

Overview

All Rsam users need to enter a valid combination of username and password to log in to Rsam. This manual authentication process can be eliminated if customers have SSO implemented in their environment. SSO may be implemented to log in to different software applications used in a customer environment. Rsam has the capability to integrate with SSO tools to make the login process seamless for users.

Note: Rsam recommends using *Shibboleth Service Provider (SP)* for the SSO integration. This document explains the steps to integrate Shibboleth SP with Rsam to enable SSO. *Rsam Customer Support* can provide guidance on configurations to enable SSO when Shibboleth SP is being used. Rsam will be unable to help with any other SP tools.

Definitions

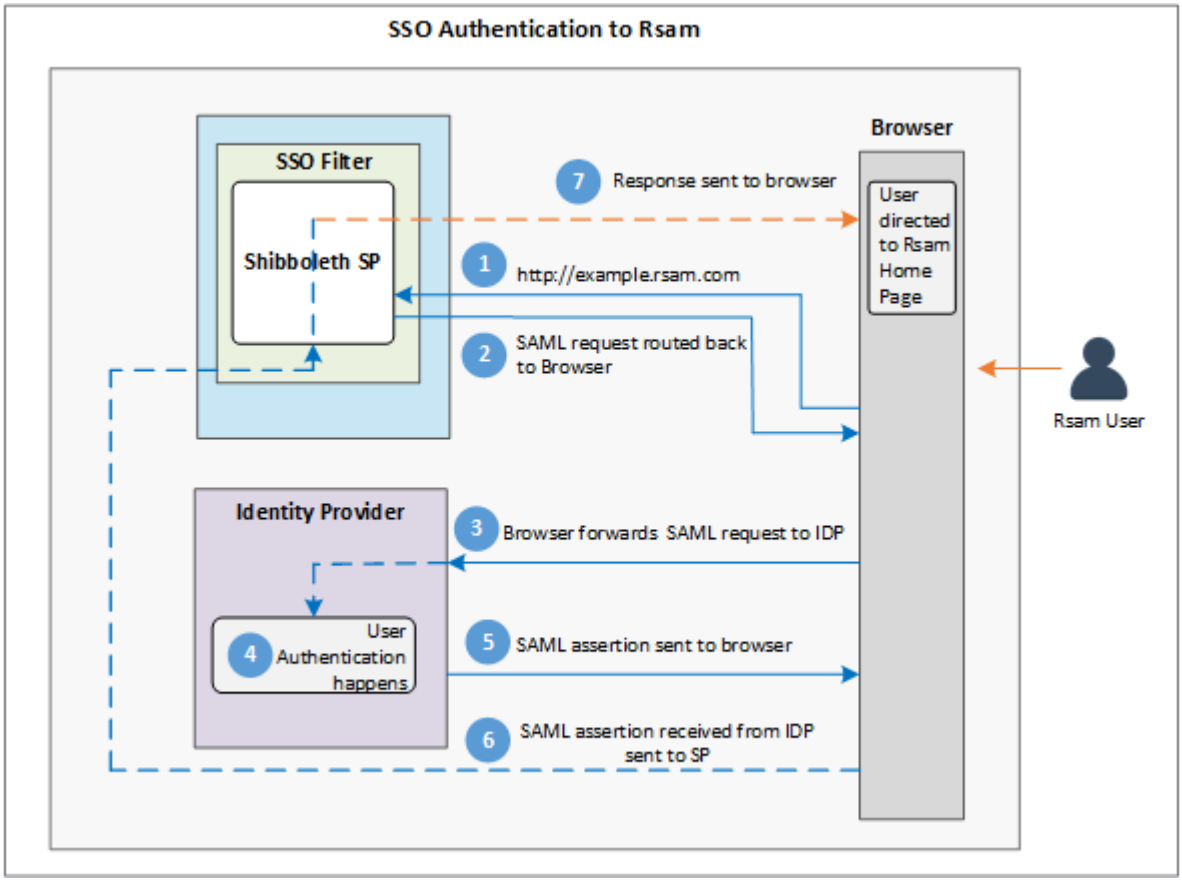
The following are the definitions of the commonly used terms in the document:

- **SSO -** Single Sign On (SSO) is a mechanism that allows users already authenticated to one application (such as a corporate domain) to automatically be authenticated to a set of other applications, such as Rsam. In Rsam, SSO is commonly used to allow Administrators and end-users already authenticated to the customer's corporate directory to access Rsam without having to re-authenticate.
- **SAML -** Security Assertion Markup Language (SAML) is a standard for exchanging authentication and authorization information between systems. The information is usually exchanged between an Identity Provider and a Service Provider. It is an open standard that allows security credentials to be shared across multiple applications by allowing one application to perform certain security functions on behalf of other applications, primarily authentication.
- **IDP -** Identity Provider (IDP) is system entity that authenticates users by means of security tokens. It issues authentication assertions in conjunction with an SSO profile of the SAML.
- **SP -** Service Provider (SP) is a system entity that receives and accepts authentication assertions in conjunction with an SSO profile of the SAML.

How SAML SSO Works with Rsam

SAML is a standard protocol for SSO using secure tokens. Implementation of SAML eliminates the use of passwords and instead uses digital signatures or cryptography to pass a secure sign-in token. On implementing SAML-based SSO in an organization, users need not manually authenticate to integrated applications, instead the SSO mechanism in place logs them into the applications automatically, when being accessed.

The following image represents the flow of operations in an SSO environment when user tries to access Rsam.



1. A user already logged into an application in the SSO environment, provides the URL to access Rsam UI. This request is passed to the Shibboleth SP. The request contains the credentials of the user from the SSO environment.
2. Shibboleth SP sends the SAML request back to the browser.
3. Browser routes the SAML request to the IDP as an authentication request.
4. IDP validates the request and gathers the required attribute values.
5. IDP sends the validation back to browser.
6. Browser routes the validation to Shibboleth SP.
7. Shibboleth SP passes the request to the Web Service to build the response.
8. Browser displays the Rsam home page to the user.

Note: The preceding flow assumes that the user session in the SSO environment is active and all SSO configuration and attribute values are correct.

Shibboleth SP Installation

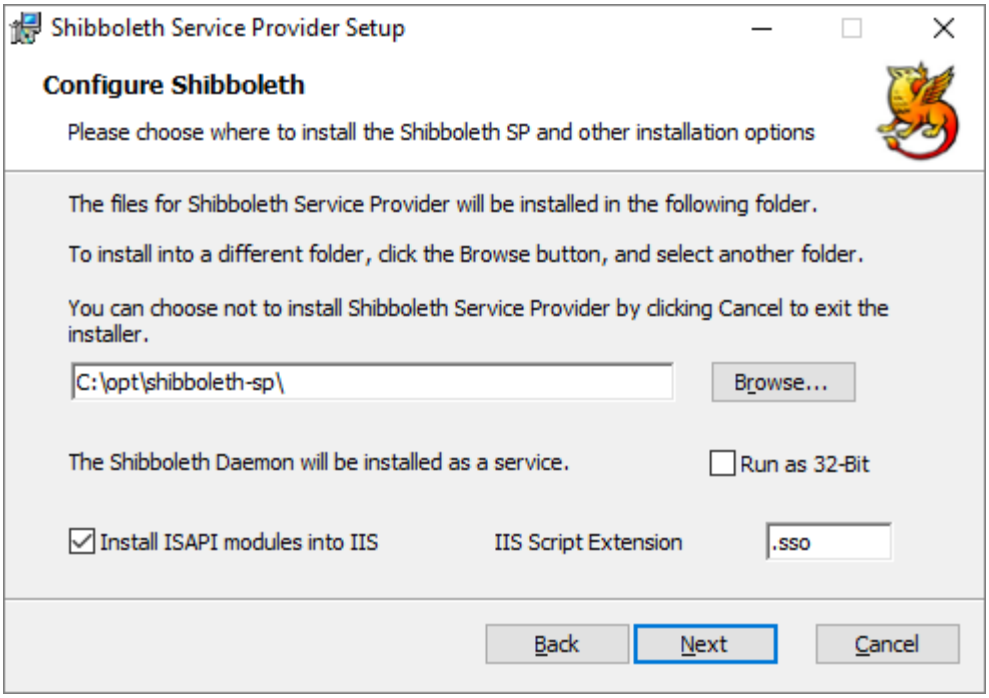
Shibboleth SP must be installed on a Windows Server. Refer the *Shibboleth documentation* for system requirements.

This chapter explains the steps to install Shibboleth SP and verify the installation for SAML SSO integration with Rsam.

Installing Shibboleth SP

To install Shibboleth SP, perform the following steps:

1. Download Shibboleth SP 2.6.1.4 from *https://shibboleth.net/downloads/service-provider/2.6.1/win64/*
2. Log in as a user with Administrator privileges and run the installer on the server.
3. In the installer, perform the following:
    a. Provide the path where Shibboleth must be installed.
    b. Select the **Install ISAPI modules into IIS** check box.
    c. Provide the value *.sso* in the **IIS Script Extension** field.

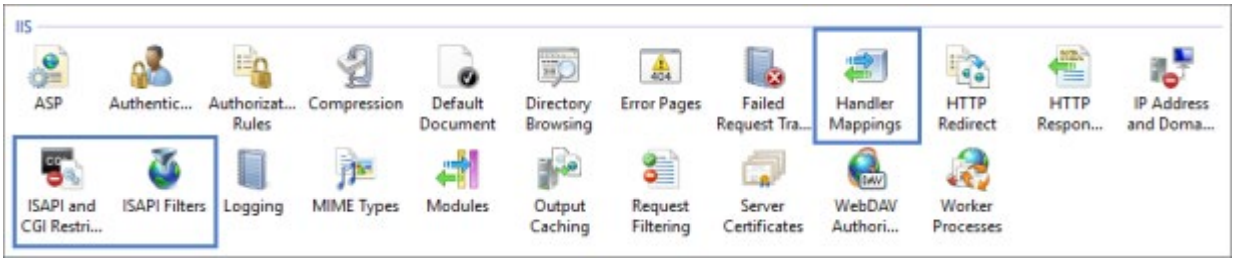


    d. Click **Next** and then **Install** to begin the installation.
    e. Click **Finish** when the installation completes.
4. When the installation is completed, the installer prompts you to reboot the system to apply the settings to IIS. Click **Yes** to reboot the system.

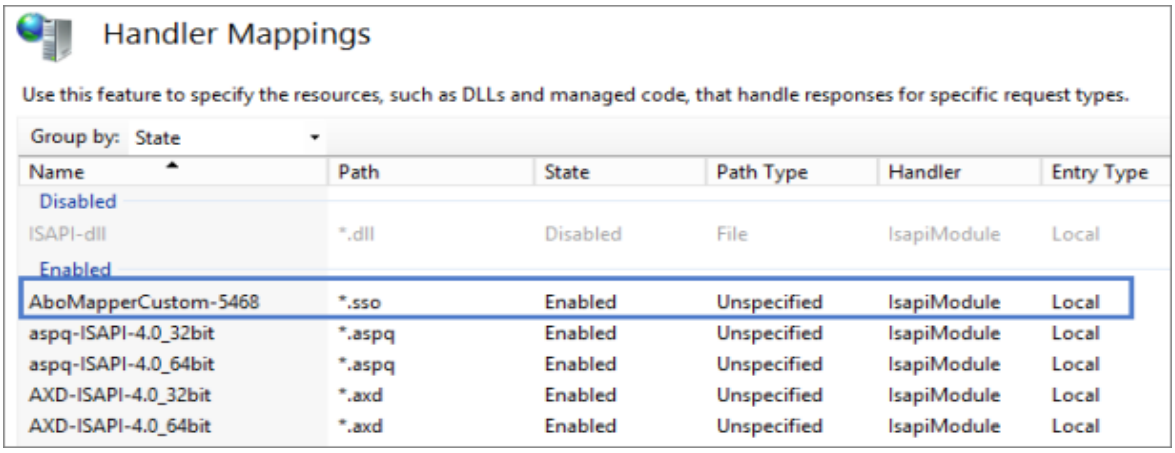
Verifying the Installation

To verify the installation, perform the following:

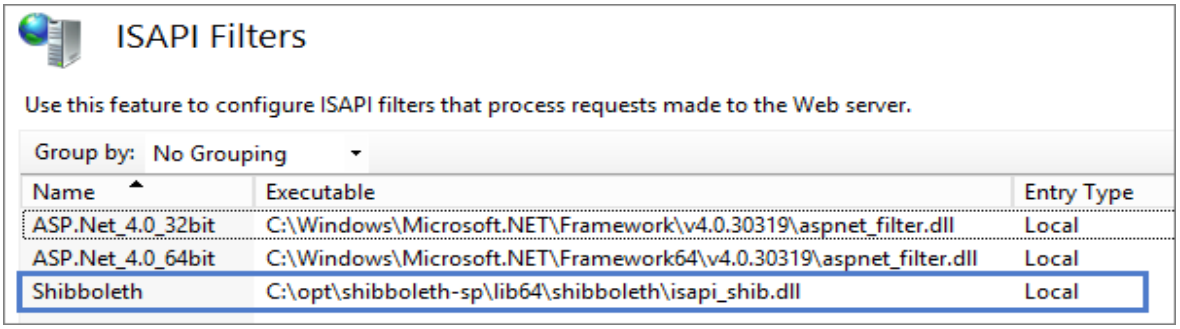
1. Log in to the system where Shibboleth SP was installed.
2. Open IIS Manager.
3. In the IIS section, verify the success of the Shibboleth installation in the **Handler Mappings**, **ISAPI Filters**, and **ISAPI and CGI Restrictions** sections.



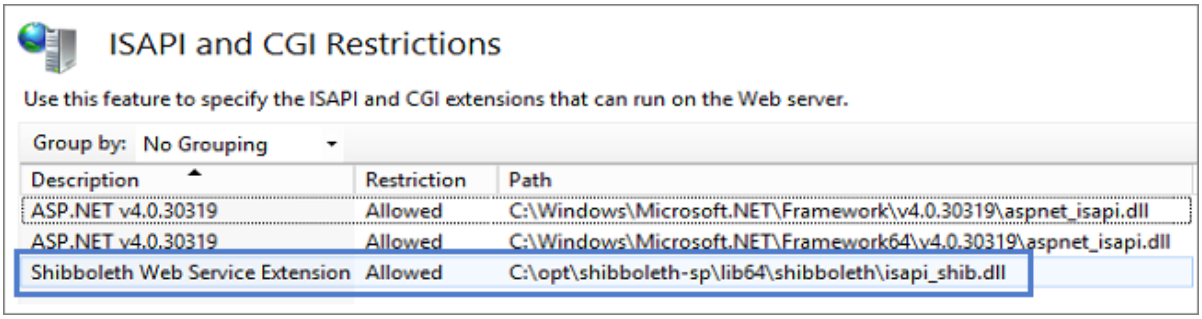
a. In the **Handler Mappings** pane, verify that an entry exists with **Path** value as ***.sso**.



b. In the **ISAPI Filters** pane, verify that there is an entry for **Shibboleth**.



c. In the **ISAPI and CGI Restrictions** pane, verify that there is an entry for **Shibboleth**.



Troubleshooting the Installation

If any of the preceding entries are missing in the IIS Server, perform the following steps:

1. On the IIS Server, open the *command prompt* as an **Administrator**.
2. Run the following commands:

   Note: The *.dll* paths in the commands may need to be updated to match the installation path in the customer environment.

   cd C:|Windows|System32|inetsrv

   appcmd set config /section:isapiFilters /+[name='shibboleth',path='C:|opt|shibboleth-sp|lib64|shibboleth|isapi_shib.dll',enabled='true']

   appcmd set config /section:handlers /+[name='Shibboleth',path='.sso',verb='*',scriptProcessor='C:|opt|shibboleth-sp|lib64|shibboleth|isapi_shib.dll',modules='IsapiModule']*

   appcmd set config /section:isapiCgiRestriction /+[path='C:|opt|shibbolethsp|lib64|shibboleth|isapi_shib.dll',description='Shibboleth',allowed='True']

   iisreset

   The preceding commands create the required Shibboleth IIS components and the last command restarts IIS.

Note: It is recommended to perform the troubleshooting steps after business hours. The last command restarts IIS and users might be impacted if you restart it during business hours.

Shibboleth SP Configuration

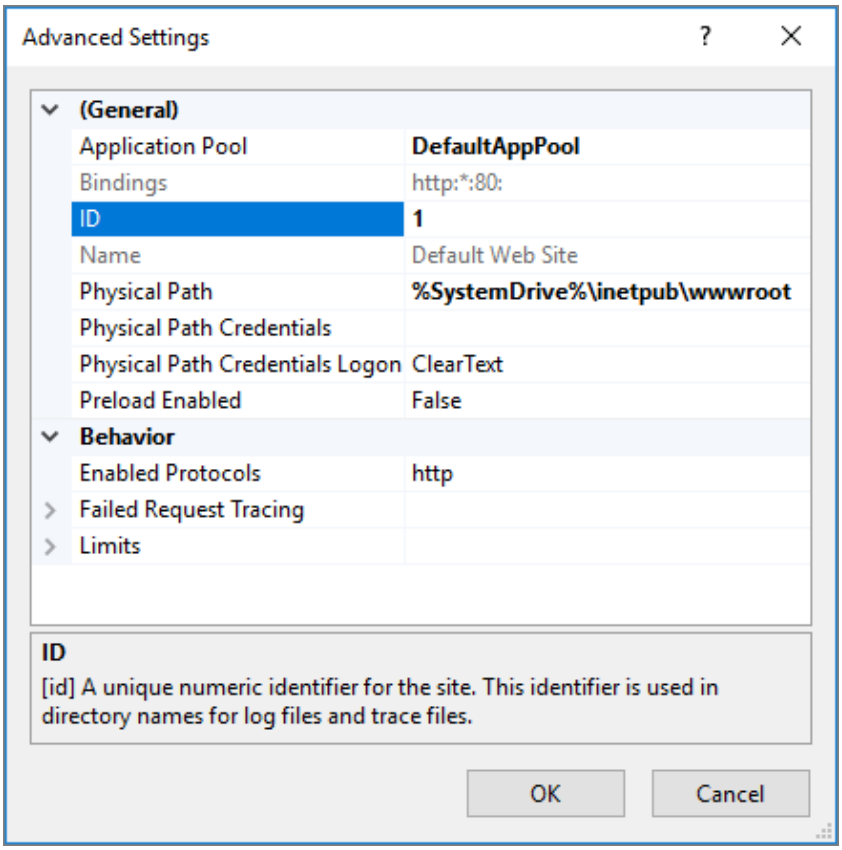
This section explains the following:

Checking Site Details

Shibboleth SP must be configured to enable SAML SSO integration with Rsam. To configure Shibboleth SP to work with Rsam, perform the following steps:

1. Open **IIS Manager** and navigate to the *Rsam site* in the **Connections** pane.
2. Right-click the site and select **Manage website > Advanced Settings**.

   The **Advanced Settings** pop-up appears.



3. Note the site **ID**. It will be used in the configuration steps explained later in this tutorial.

Backing Up Files

In the next sections, you will be making configuration changes to the following files and it is recommended to take a backup before making any update:

- shibboleth2.xml
- attribute-policy.xml
- attribute-map.xml

Note: The files are located in the **\etc\shibboleth** folder of the *Shibboleth installation directory*.

Configuring SP Metadata

The *shibboleth2.xml* file contains details of the sites, hosts, and metadata provider. To update the file, perform the following steps:

1. Navigate to ***<Shibboleth installation directory>\etc\shibboleth***.
2. Open the file **shibboleth2.xml** in a Text Editor of your choice.
3. Locate the appropriate **site node (htttp or https)** and update the values of **Site id** to match the values obtained from IIS Manager.

   Set the value for **name** to the DNS of the Rsam instance.

   HTTPS Node:

   Site id="42" name="example.rsam.com " scheme="https" port="443"/>

   HTTP Node:

   <Site id="1" name="example.rsam.com"/>

   Comment out any site nodes you are not using with ***<!-- -->***.
4. Locate the default **Host node** and replace it with the following example provided.

   Update the values of **Host name** and **applicationId** with the DNS of the Rsam instance.

   <Host name="example.rsam.com" applicationId="example.rsam.com" entityID="">

   <Path name="default.aspx" authType="shibboleth" requireSession="true">

   <Query name="SSO" regex="^0" authType="shibboleth"requireSession="false" />

   </Path>

   </Host>

   Note: The **entityID** value is the entityID from the IDP metadata. If the IDP metadata is not available at this stage of configuration, you may leave it blank.
5. Locate the file-based **MetadataProvider node** and uncomment it. Then update the value of **file** with the path to the Shibboleth metadata file. Specify the name you would provide the IDP file when you receive it from the IDP team.

   <MetadataProvider type="XML" file="C:|opt|shibbolethsp|metadata|ADFS1_IDP.xml"/>
6. Locate the example **ApplicationOverride node** and uncomment it. Then update the values as follows:

- Set the value of **ApplicationOverride id** to the DNS of the Rsam instance.
- Set the value of **entityID** to URL for the Rsam instance and append **/shibboleth** to it.

This sets the entityID that will be included when generating the SP metadata.

<ApplicationOverride id="example.rsam.com"
entityID="https://example.rsam.com/shibboleth"/>

7. Save and close the file.

Configuring Attribute Mapping

The attribute mapping configuration must be updated in the *attribute-map.xml* file. To update the file, perform the following steps:

1. Navigate to ***<Shibboleth installation directory>\etc\shibboleth***.
2. Open the file **attribute-map.xml** in a Text Editor of your choice.
3. Add the required attribute nodes to the file before the **</Attributes>** tag at the end of the file.

   The following are the mandatory attributes:

   - **Attribute names:** Can only contain alphabetic characters (A-Z, a-z).
   - **Unique ID:** Value must be the user ID of the account in Rsam.
   - **Full name:** Value must be in *givenName surname* format (example - John Smith).
   - **Email address:** Value must be the email address assigned to the user account.

   The following attributes are *optional*:

   - **Group name:** A multi-value list of groups used for group synching feature through SSO. The group list received in this attribute will replace the authenticating user's group membership in Rsam. Enabling group syncing can have unintended effects on permissions if group names do not match and therefore should be carefully planned before implementation.
   - **Distinguished Name (DN):** Value must be the user's DN attribute from the source directory. This is used only when combining an LDAP connection with SAML-based SSO.

   An example of unspecified nameFormat attribute nodes is as follows:

   <Attribute name="dn" id="dn"/>
   <Attribute name="uniqueid" id="uniqueid"/>
   <Attribute name="emailaddress" id="emailaddress"/>
   <Attribute name="fullname" id="fullname"/>
   <Attribute name="groupname" id="groupname"/>

An example of basic nameFormat attribute nodes is as follows:

```
<Attribute name="dn" nameFormat="urn:oasis:names:tc:SAML:2.0:attrnameformat:basic"
id="dn"/>
<Attribute name="uniqueid" nameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic" id="uniqueid"/>
<Attribute name="emailaddress" nameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic" id="emailaddress"/>
<Attribute name="fullname" nameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic" id="fullname"/>
<Attribute name="groupname" nameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic" id="groupname"/>
```

4. Save and close the file.

Configuring Attribute Policy

To configure an attribute policy, perform the following steps:

1. Navigate to ***<Shibboleth installation directory>\etc\shibboleth***.
2. Open the file **attribute-policy.xml** in a Text Editor of your choice.
3. Add the required attribute rule nodes as shown in the following example. The **attributeID** values must match the ***attribute name/id*** values used in the attribute map.

   An example attribute policy is as follows:

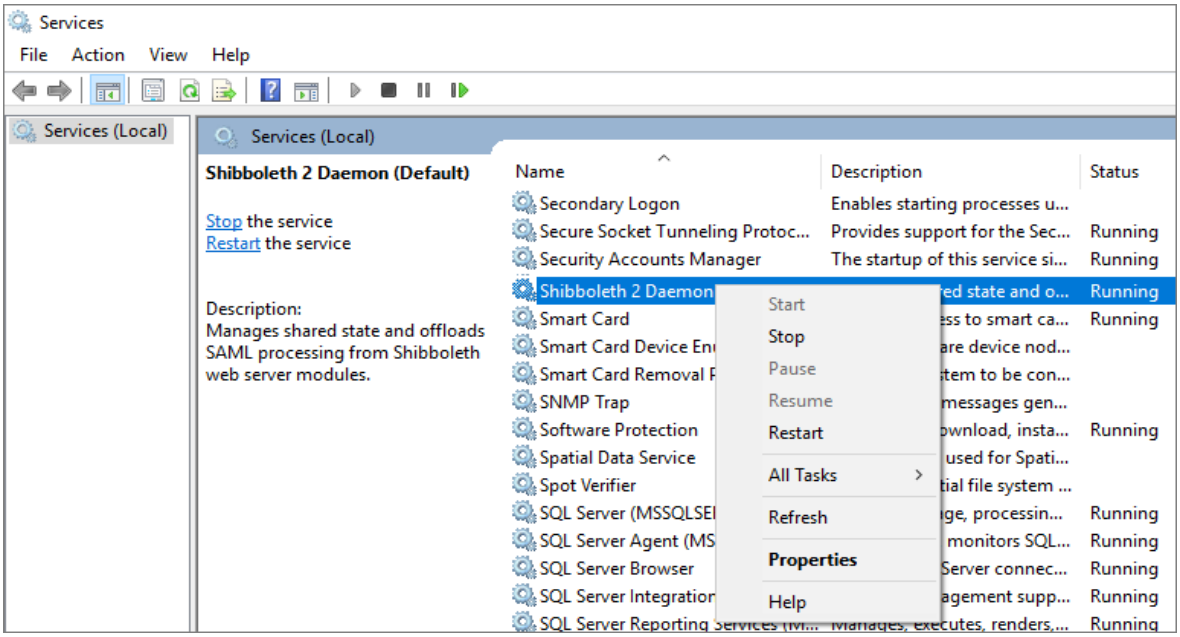
```
<afp:AttributeRule attributeID="dn">
<afp:PermitValueRule xsi:type="ANY"/>
</afp:AttributeRule>
<afp:AttributeRule attributeID="uniqueid">
<afp:PermitValueRule xsi:type="ANY"/>
</afp:AttributeRule>
<afp:AttributeRule attributeID="fullname">
<afp:PermitValueRule xsi:type="ANY"/>
</afp:AttributeRule>
<afp:AttributeRule attributeID="emailaddress">
<afp:PermitValueRule xsi:type="ANY"/>
</afp:AttributeRule>
<afp:AttributeRule attributeID="groupname">
<afp:PermitValueRule xsi:type="ANY"/>
</afp:AttributeRule>
```

4. Save and close the file.

Generating SP Metadata

The Shibboleth SP metadata must be generated and provided to the IDP team to make the necessary configurations to allow SSO. To generate the Shibboleth SP metadata, perform the following steps:

1. Ensure that changes made to the SP configuration files are saved.
2. Restart the Shibboleth SP service:
   a. Open the **Services** manager and locate the **Shibboleth 2 Daemon** service.
   b. Right-click the service and select **Restart**.



3. Open a browser and insert the URL ***https://<example.rsam.com>/Shibboleth.sso/Metadata***. Replace *example.rsam.com* with the Rsam instance URL.

   The Shibboleth Metadata file gets downloaded on your system to your **Downloads** folder.

   The name of the downloaded file will be **metadata** and will have XML content.

4. Rename the file to your choice and provide the ***.xml*** extension. For example, *rsam_metadata.xml*.

5. Open the file and verify if the URLs are correct.

   The following image shows an example Shibboleth metadata file with URLs.

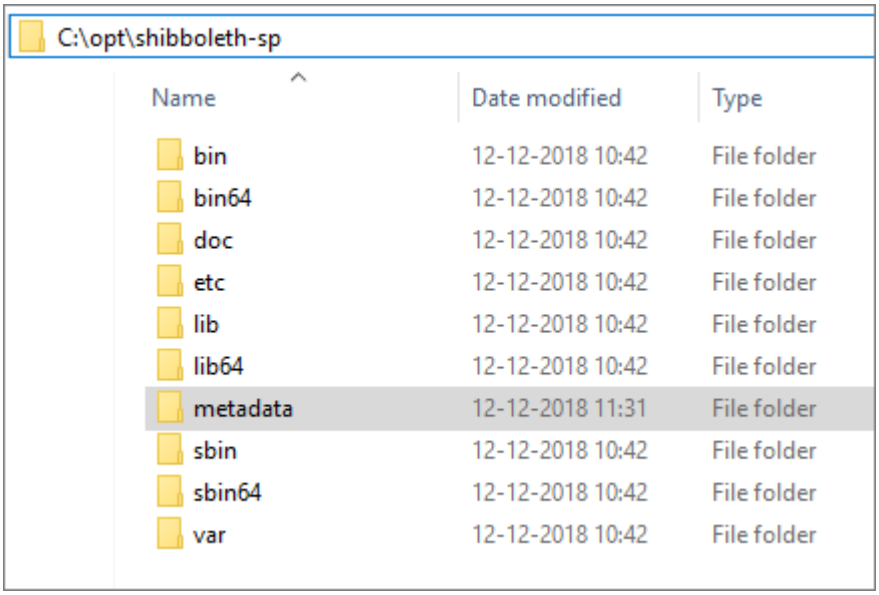
6. After verification, send the file to the IDP team.

Configuring SP Using IDP Metadata

When the Shibboleth SP metadata file is passed to the IDP team, the IDP team must input the received metadata into the IDP configuration and generate an IDP Metadata file. The IDP metadata file must contain the valid URLs to be used for redirecting the users and also certificates, if being used.

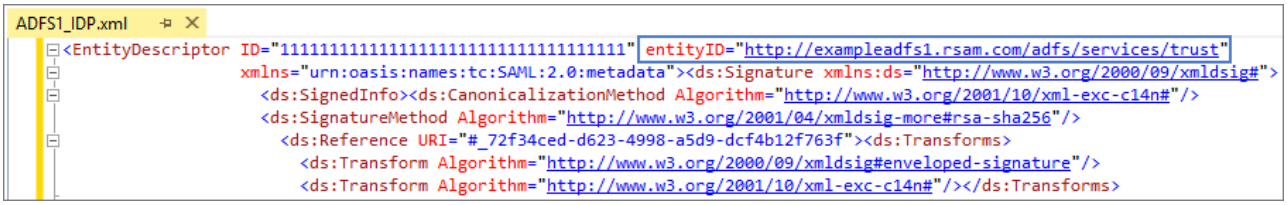
The IDP metadata received is used to configure the Shibboleth SP files. To configure the Shibboleth SP files, using the IDP metadata, perform the following steps:

1. Navigate to the *<Shibboleth installation directory>* and create a **metadata** folder.



2. Paste the IDP metadata file into the folder.

3. Open the IDP metadata file and note the value for **entityID**.



4. Navigate back to the installation directory and go to **\etc\shibboleth**.
5. Open the **shibboleth2.xml** file in a Text Editor of your choice.
6. Locate the **Host node** and provide the **entityID** value received from the IDP metadata file.

   <Host name="example.rsam.com" applicationId="example.rsam.com" entityID="http://exampleadfs1.rsam.com/adfs/services/trust">

   <Path name="default.aspx" authType="shibboleth" requireSession="true">

   <Query name="SSO" regex="^0" authType="shibboleth"requireSession="false" />

   </Path>

   </Host>

7. Save and close the file.
8. Restart the *Shibboleth SP* service.

Rsam Configuration

To enable SSO in Rsam, perform the following steps:

1. Log in to Rsam as an *Administrator*.
2. Navigate to **Manage** > **Administration** > **Options** > **Rsam Options**.
3. In the **Option Categories** drop down, select **Single Sign On options**. The **Single Sign On** options appear.
4. In the **SSO - Enable Single Sign On** drop down field, select the required SSO method. The values are as follows:
    - **Windows Authentication** - Users are authenticated to a central Active Directory.
    - **Other SSO** - For LDAP-based SSO solutions.
    - **Other SSO (Non-LDAP)** - For SSO solutions that do not have LDAP directories.
    - **Other SSO GUID based** - For SSO solutions that pass a GUID into the system.
5. Select the **Enable LDAP based authentication** check box to enable user authentication through user directories.

    For more information about the *Rsam Options*, refer the *Rsam Online Administrator Help*.

Logging in to Rsam

After configuring SSO, when users access an Rsam instance, they are automatically logged in using the credentials provided in the directory. Users do not need to provide manual authentication to use Rsam.

Troubleshooting

The following table lists the most common problems encountered when using SAML-based SSO for authenticating logins to Rsam and the steps to resolve or proceed further.

The log files are located at *<Shibboleth installation directory>/var/log/shibboleth*.

Problem	Probable Cause(s)	Workaround
Login fails and user is shown the *Rsam Sign-In* page	• Passed credentials do not match any users in Rsam • Unique ID is missing	Check the *transaction.log*. This log file tracks details of who is accessing the application and all sessions as they are created / deleted, and the attribute query operations that succeed or fail. You can check to confirm if the proper attribute values are being passed and make required updates in the directory or Rsam.
	Attributes names do not match the attribute map	Check the *shibd.log*. This is the main log file and tracks all details of the software. When attributes names do not match, they are skipped and logged in the *shibd.log*. You can check the log to verify the skipped attributes and correct it in the map.
	Options to enable SSO are not set in Rsam Options	Go to Rsam and configure the SSO settings. For more information, see Configuring Rsam Options.
User receives an error screen with IDP details	IDP metadata is not configured correctly	For more information, see Mapping IDP Metadata.
	Certificate mismatch	Occurs only if certificates are being used. Check with IDP Team to validate the certificates.