IBM® InfoSphere Information Server

IBM InfoSphere Information Server Single Sign-On (SSO) by using SAML 2.0 and Microsoft Active Directory Federation Services (AD FS)

Installation and Configuration Guide

Table of Contents

About this publication

IBM InfoSphere Information Server Version 11.5 implements solutions for federated single sign-on for its web applications. This guide describes how to install and configure IBM InfoSphere Information Server with SAML 2.0 and Microsoft Active Directory Federation Services (AD FS).

Intended audience

The target audience for this book includes network security architects, system administrators, network administrators, and system integrators. Readers of this book should have working knowledge of networking security issues, encryption technology, keys, and certificates. Readers should also be familiar with the implementation of authentication and authorization policies in a distributed environment. This includes experience with deploying applications into an IBM® WebSphere® Application Server environment.

Publications and Prerequisites

Refer to the instructions for accessing publications online. To use the information in this book effectively, you should have some knowledge about related software products, which you can obtain from the following sources:

- **InfoSphere Information Server version 11.5:** http://www.ibm.com/support/knowledgecenter/SSZJPZ_11.5.0/com.ibm.swg.im.iis.productization.iisinfsv.home.doc/topics/kc_homepage_IS.html
- **Prerequisites for installing AD FS (on Windows 2012 R2):** https://technet.microsoft.com/library/bf7f9cf4-6170-40e8-83dd-e636cb4f9ecb
- **To enable your system to use the SAML web single sign-on (SSO) feature:** http://www.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/twbs_enablesamlsso.html

Additional documentation can be found in the Useful Links section in this document.

Chapter 1: Planning the installation

In order to enable single sign on functionality to the web applications of IBM InfoSphere Information Server you will need to install and configure:

- Microsoft Active Directory Federation Services (AD FS)
- Configuration of the SAML TAI, in the **WAS ND** version 8.5.5.8 or higher installation of IBM InfoSphere Information Server.
  Note that **WebSphere Liberty (LWAS)** is not supported and cannot be used for this configuration.
- Establishing the Trust Relationships between AD FS and WebSphere
- Install IBM InfoSphere Information Server version 11.5.0.1 or higher. Other patches may be required. Check Chapter 4: InfoSphere Information Server Configuration - Requirements for details
- LDAP Configuration

The components can all be installed on one computer or can be installed across multiple computers. Installations on one computer are common for prototype or test environments. Installations across multiple computers are common in production environments.

Chapter 2: Microsoft AD FS

Planning the installation

Microsoft Active Directory Federation Services (AD FS) is available 'out of the box' on Windows Server 2012. Only step required is the addition of a new server role for AD FS and its configuration.
AD FS uses Active Directory as the source of its user information. Therefore, it is highly recommended that any new AD FS setups are created in their own Active Directory domain. This gives you full control over users, groups, and other Active Directory fields.

This document uses domain name `ISF_DEV / isf_dev.com` in the installation examples that follow. Administrator user accounts have been added to such domain.

Installation

Details of the installation can be found in the formal documentation from Microsoft about the installation and configuration of Active Directory Federation Services (AD FS). For example, follow directions on "How to deploy AD FS in Windows Server 2012 R2" from the Microsoft link https://technet.microsoft.com/en-us/library/dn303423. The AD FS Technical reference is also found at https://technet.microsoft.com/en-us/library/dn303410.

Below are general installation steps to follow, however, reference the formal Microsoft AD FS documentation for details and updates:

1. Log in to the Microsoft Windows AD FS Server machine as user with Domain Admin privileges
2. Add AD FS Server Role via the Windows Server Manager console. This starts the installation of the AD FS software.
3. After the installation, a message indicates that "Additional steps are required to configure Active Directory Federation Services on this machine". Follow the link to "Configure the federation service on this server".
4. The link launches the Active Directory Federation Services Configuration Wizard, with the following message:

   ```
   Before you begin configuration, you must have the following:
   - An Active Directory domain administrator account.
   - A publicly trusted certificate for SSL server authentication
   ```

5. The Prerequisites for installing AD FS (on Windows 2012 R2) are found at the Microsoft link https://technet.microsoft.com/library/bf7f9cf4-6170-40e8-83dd-e636cb4f9ecb where you find details on the certificate:

a. SSL Server Authentication Certificate: This certificate must be trusted publicly (chained to a public root certification authority) or explicitly trusted by all computers that require access to the federation service.
b. You must have both the certificate and its private key available. For example, if you have the certificate and its private key in a .pfx file, you can import the file directly into the Active Directory Federation Services Configuration Wizard.
c. The Subject name or subject alternative name of this SSL certificate must contain the exact name of your federation service such as `fs.isf_dev.com` or a matching wildcard expression such as `*.isf_dev.com`
d. If you plan to use DRS for Active Directory Workplace Join, the subject name or subject alternative name must contain the value `enterpriseregistration` followed by the UPN suffix of your organization. For example, `enterpriseregistration.corp.isf_dev.com`.
e. If your organization uses multiple UPN suffixes, the SSL certificate must contain a subject alternative name entry for each suffix.

At the end, the Review Options show as follows:

```
This server will be configured as the primary server in a new AD FS farm
'fs.isf_dev.com'.
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.
Federation service will be configured to run as ISF_DEV\ADFS.
```

Complete the Pre-Requisite Checks. At the end the 'Configure' Results should show: “This server was successfully configured”.

Chapter 3: WAS SAML TAI

Overview of installation and configuration

IBM WebSphere Application Server — and stack products running on top of a WebSphere Application Server platform — has had a customizable authentication framework since V5.1 based on the **Trust Association Interceptor (TAI)** interface. There are multiple product implementations of this interface. In 2012, the WebSphere Application Server full profile edition shipped a new **Security Assertion Markup Language (SAML)** TAI that is available on WebSphere Application Server from version 7.0 on.

The actors involved are:

- **Identity Provider (IdP)**
- **Service Provider (SP)** sometime known as the Relying Party, or RP.

The job of the IdP is to authenticate the end user (exactly how the IdP does this is immaterial), and to produce some assertions or claims about the user. These assertions are digitally signed by the IdP. The SAML specification defines the format of these assertions. The SP receives the assertions and, if the SP is satisfied that the assertions came from a trusted IdP, logs the user in based upon some parts of the assertion.

The WebSphere SAML TAI does not truly support a Service Provider (SP) initiated authentication path. For a SP initiated authentication, the SP generates a SAML Request which it sends to the SAML IdP. Essentially the user accesses the protected URI without an LTPA token, the SAML TAI intercepts, the TAI doesn't find a SAML token and the TAI error page is triggered. The SAML TAI configuration specifies the IdP login page in the TAI error page property (e.g. `sso_1.sp.login.error.page`). This URL is therefore invoked. The IdP URL points back to the SAML TAI via another URL specified as a RelayState parameter. And that RelayState parameter URL itself contains a RelayState parameter that points to the post authentication target URL.

The mentioned steps are depicted in Figure 1 below:

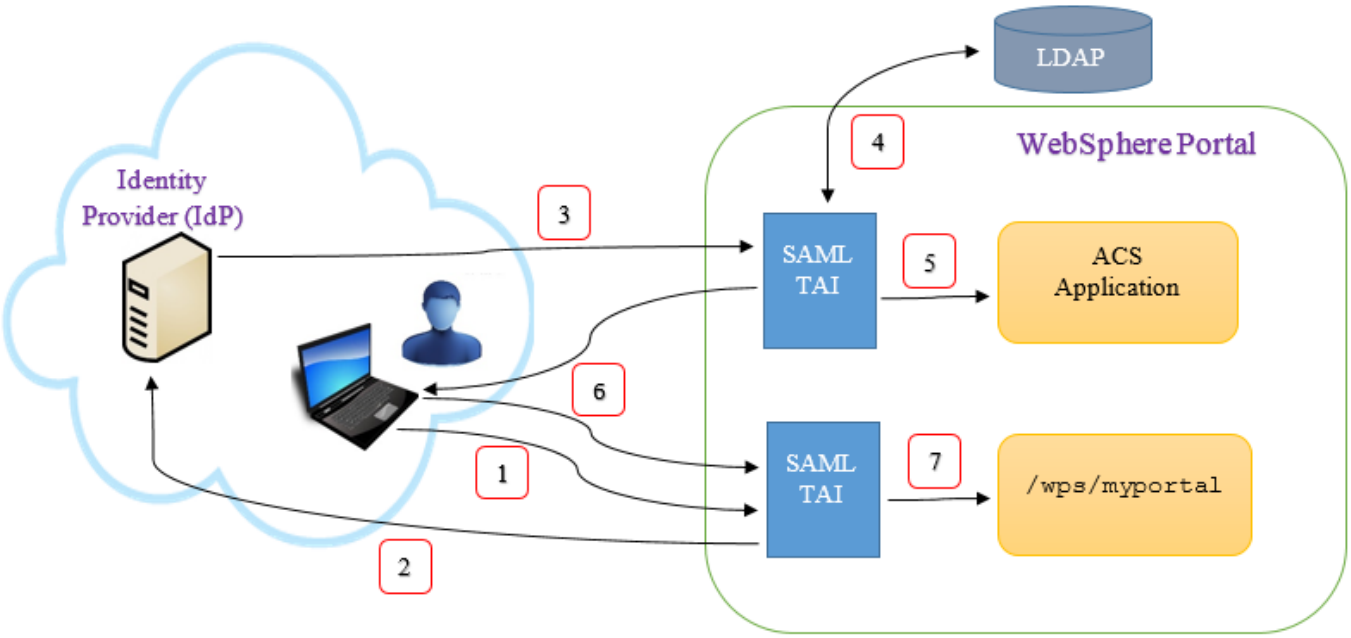


Figure 1.

1. The user starts the process by following a link to the application's URL at the SP. For example, this would be https://portal.uac.com/wps/myportal.
2. The SAML TAI is called twice. Because this URL is not the ACS, the TAI does not initially intercept the request. The Web Inbound configuration looks for a LtpaToken2 cookie. None is found. The SAML TAI is called a second time. Based on some data in the incoming request and the TAI configuration, the TAI returns an HTTP 302 redirects to the correct IdP. A cookie is set by the TAI. This is set to the value of the **original referrer URL**, which in this example is https://portal.uac.com/wps/myportal. As discussed above, the user authenticates to the IdP.
3. Based on configuration in the IdP and the original URL provided to the IdP, a SAML response is created and sent via an HTTP Post redirect to an Assertion Consumer Service (ACS) in the SP. This SAML response is signed by the IdP.
4. The SAML TAI consumes the SAML response and logs the user in. In this example, the user identity exists in the UAC LDAP. Know, however, that this is not a requirement for SAML Web SSO. A JAAS subject is created in memory, and various WebSphere Application Server security tokens are created, including an SSOToken, which is also known as the LtpaToken2. From this SSOToken, an LtpaToken2 cookie is created.
5. With the user logged in, the request is dispatched to the ACS. It is an application whose sole purpose is to redirect the user to the correct landing page after being logged in by the SAML TAI. The ACS has a Java™ EE security constraint defined, in order to cause the WebSphere Application Server container security and the SAML TAI to be called. An ACS application is shipped as part of the support for the SAML TAI.
6. The ACS redirects the user to the landing page for the application (possibly based upon something in request, or possibly based on configuration). In this example, this URL is: https://portal.uac.com/wps/myportal. This HTTP redirection includes the new LtpaToken2 cookie. The browser follows the redirection and resends the LtpaToken2.
7. The SAML TAI is called again, this time to check if there is a SAML response in the request. There is not, but there is a LtpaToken2 cookie, so the standard Web Inbound login configuration processing occurs.

Installation

Before you can use the SAML Web SSO feature, you must:

1. **Install the SAML Assertion Consumer Service (ACS) application on the IIS application server.** This server will be referenced by the URLs specified on the `sso_.sp.acsUrl` SAML TAI custom properties.
2. **Enable the SAML TAI**

For both steps, follow the instructions in the WebSphere Knowledge Center article on installing and enabling the WAS SAML TAI "Enabling your system to use the SAML web single sign-on (SSO) feature" here:
http://www.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/twbs_enablesamlsso.html

Make sure to have installed the SAML ACS Application (in step 1. above) before continuing.

To enable the SAML TAI (step 2.), you can use either the `wsadmin` command utility or the WAS administrative console. If enabling SAML TAI using the administrative console:

a. Log on to the WebSphere Application Server administrative console.
b. If your WAS ND environment is not clustered
   - Click **Security->Global security**.
   - Expand Web and SIP security and click **Trust association**.
c. If your WAS ND environment is clustered
   - Click **Security->Security domains -> IBM_Information_Server_sd.**
   - Click and expand **Trust association**. Select Customize for this domain

d. Select the **Enable trust association** check box and click **Interceptors**.
e. Click New and enter `com.ibm.ws.security.web.saml.ACSTrustAssociationInterceptor` in the Interceptor class name field.
f. Do not remove the existing interceptor `com.ibm.iis.isf.j2ee.impl.was.security.WASTrustAssociationInterceptor2`. This interceptor is created by the IS installation and is used by the system for trusted session management.
g. Under Custom properties of the new interceptor, provide the following custom property information:

NAME	VALUE
sso_1.sp.acsUrl	https://**<ACS-SERVER:port>**/samlsps/ibm/iis/launchpad/secure
sso_1.sp.idMap	localRealmThenAssertion
sso_1.idp_1.EntityID	http://**<IdPDomain>**/adfs/services/trust
sso_1.sp.useRelayStateForTarget	true
sso_1.sp.login.error.page	https://**<IdPDomain>**/adfs/ls/idpinitiatedsignon.aspx?RelayState=RPID%3Dhttps%253A%252F%252F**<ACS-SERVER>**%253A**<PORT>**%252Fsamlsps%252Fibm%252Fiis%252Flaunchpad%252Fsecure%26RelayState%3Dhttps%253A%252F%252F**<ACS-SERVER>**%253A**<PORT>**%252Fibm%252Fiis%252Flaunchpad%252Fsecure
sso_1.sp.filter	request-url^=/ibm/iis/launchpad/secure

Some fields in the example above contain the <ACS-SERVER> and <PORT> placeholder. Modify the server name and port with the ones from your IIS installation, that is, the host name of the system where WebSphere Application Server with IIS is installed and the Web server SSL port number (WC_defaulthost_secure).

The value of field `sso_1.sp.acsUrl` has format *https://<hostname>:<sslport>/samlsps/<any URI pattern string>*. If you need to have multiple, similar entry points for your SAML workflows, you can specify a wildcard value instead of a specific URI pattern string. Specifying a wildcard eliminates the need to separately configure each of the similar entry points.
If needed, include a wildcard as part of the value of the `sso_1.sp.acsUrl` property, for example:
https://<server>/<context_root>/ep1/path1/p*
https://<server>/<context_root>/ep1/path1/*
https://<server>/<context_root>/ep1/*

The `sso_1.sp.login.error.page` field specifies the RelayStates that must be URL-encoded to prevent them from being mangled. To create the value for this field, you can use the following Microsoft page that contains a form based RelayState generator for AD FS:
http://social.technet.microsoft.com/wiki/contents/articles/13172.ad-fs-2-0-relaystate-generator.aspx
Use this RelayState generator page to create the string value used in the `sso_1.sp.login.error.page` property.

The RelayState specified in the above example configures the IIS Secure Launchpad as the landing URL where a user is automatically forwarded after a successful login from AD FS. To modify the landing page, follow the instructions in the next chapter Changing the landing URL page after a successful AD FS login.

An example of the WAS configuration of the new Interceptor is shown in Figure 2.

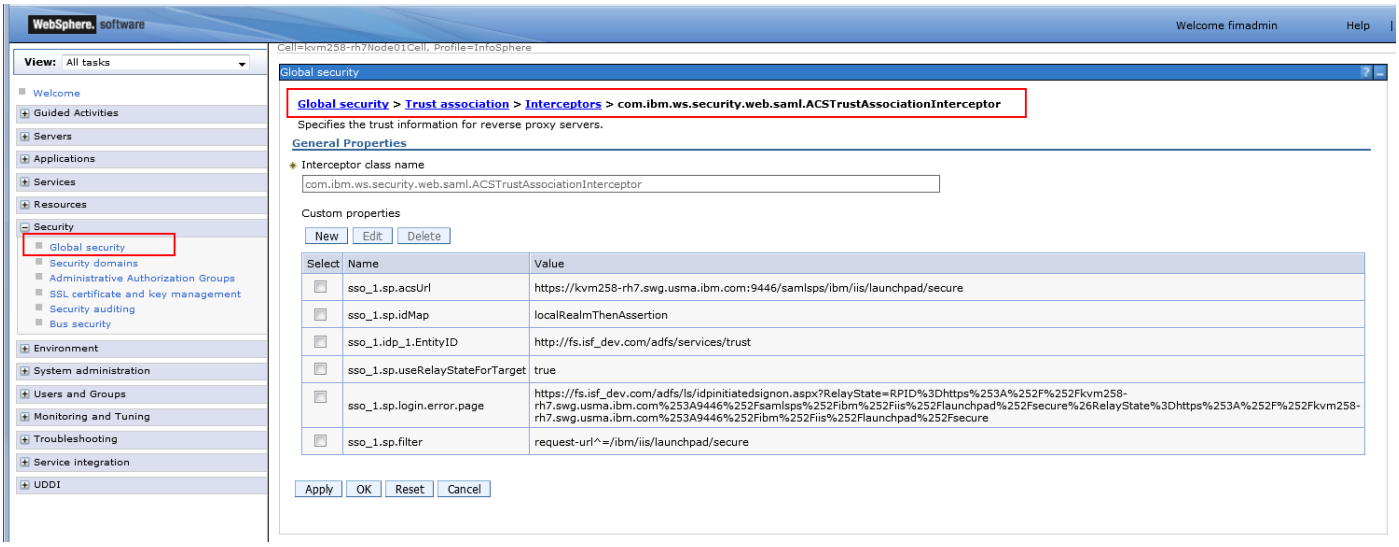


Figure 2.

Changing the landing URL page after a successful AD FS login

The default configuration described in this document uses the IIS Secure Launchpad application as the target location after a successful login to AD AF. To change the landing URL where users are forwarded after a successful AD FS login, follow these instructions. This example uses the IIS Information Governance Catalog (IGC) application as the new landing page.

1. Modify the SAML TAI property `sso_1.sp.login.error.page`:
   Use the AD FS relay state generation page from Microsoft to generate the URL encoded string. It should contain
   - RelayState= Target App: fully qualified URL of the IGC application (instead of the Secure Launchpad), like for example:

     https://**<IdPDomain>**/adfs/ls/idpinitiatedsignon.aspx?RelayState=RPID%3Dhttps%253A%252F%252F**<ACS-SERVER>**%253A**<PORT>**%252Fsamlsps%252Fibm%252Fiis%252Flaunchpad%252Fsecure%26RelayState%3Dhttps%253A%252F%252F**<ACS-SERVER>**%253A**<PORT>**%252Fibm%252Fiis%252Figc

2. Disable the cookie `'WasSamlSpReqURL'` containing the Secure Launchpad URL. By default, WAS and SAML provide this cookie in the request to the IdP, which forces AD FS to always redirect to the original requester (i.e. the Secure Launchpad), regardless how the `RelayState` has been configured. To remove the cookie `WasSamlSpReqURL`, create the following property in the SAML TAI configuration:
   `sso_1.sp.preserveRequestState` and set it `false`.

   The following example highlights the modified SAML TAI properties:

NAME	VALUE
sso_1.sp.acsUrl	https://**<ACS-SERVER:port>**/samlsps/ibm/iis/launchpad/secure
sso_1.sp.idMap	localRealmThenAssertion
sso_1.idp_1.EntityID	http://<IdPDomain>/adfs/services/trust
sso_1.sp.useRelayStateForTarget	true
sso_1.sp.login.error.page	https://**<IdPDomain>/**adfs/ls/idpinitiatedsignon.aspx?RelayState=RPID%3Dhttps%253A%252F%252F**<ACS-SERVER:port>**%253A9446%252Fsamlsps%252Fibm%252Fiis%252Flaunchpad%252Fsecure%26RelayState%3Dhttps%253A%252F%252F**<ACS-SERVER>**%253A**<PORT>**%252Fibm%252Fiis%252Figc
sso_1.sp.filter	request-url^=/ibm/iis/launchpad/secure
sso_1.sp.preserveRequestState	false

3. By default, the IIS ISF framework checks for cross-site request forgery attacks and will deny the forwarding to a URL other than the Secure Launchpad. ISF provides an IIS repository flag where you specify the list of allowed *Referer domain names* that will be ignored by the check for cross-site forgery attack.

From the `<IIS_HOME>\ASBServer\bin` folder run the command:

```
./iisAdmin.sh -set -key com.ibm.iis.isf.security.AllowedRefererDomainNames
              -value "<domain of the ADFS server>"
```

for example:

```
./iisAdmin.sh -set -key com.ibm.iis.isf.security.AllowedRefererDomainNames
              -value "IdPDomain.com"
```

This AD FS domain is specified in the SAML TAI property `sso_1.sp.login.error.page (<IdPDomain>)`. Specify only the root domain of AD FS. Do not use additional subdomains, as it will not be recognized by the cross-site request forgery attack test. For example, use "isf_dev.com" and not "fs.isf_dev.com".

Should you receive an error in your WAS log indicating a "`Possible Cross-Site Request Forgery Attack`", this domain is found in the HTTP Referer Header, in the WAS error. For example, if the WAS error you are getting is:

```
https://kvmrh7.ibm.com:9446/ibm/iis/igc HTTP Referer Header:
https://fs.isf_dev.com/adfs/ls/idpinitiatedsignon.aspx?....
Possible Cross-Site Request Forgery Attack.
```

set the Registry key `com.ibm.iis.isf.security.AllowedRefererDomainNames` to `"isf_dev.com"`.

4. Make sure you leave the IIS registry keys as described in the InfoSphere Information Server Configuration chapter in this document:

```
./iisAdmin.sh -display -key com.ibm.iis.isf.security.SAML*
com.ibm.iis.isf.security.SAMLSecureURL=/ibm/iis/launchpad/secure
com.ibm.iis.isf.security.SAML=true
```

5. Restart WAS.

Establishing a Trust Relationship between AD FS and WebSphere

Overview

The AD FS server and WebSphere need to be configured to trust each other. Complete the following steps:

- Add the WebSphere SAML TAI to AD FS as a Service Provider (SP).
- Add the AD FS server to WebSphere as a trusted Identity Provider (IdP)

Add the WebSphere SAML TAI to AD FS as a Service Provider (SP)

As a first step, export the SAML TAI Service Provider metadata from WebSphere. Follow directions in article "Exporting SAML web service provider metadata using the wsadmin command-line utility" at http://www.ibm.com/support/knowledgecenter/en/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/twbs_exportsamlspmetadata.html?cp=SSAW57_8.5.5 to export the metadata from WebSphere.

An example of the procedure on a Linux machine follows:

```
# cd /opt/IBM/WebSphere/AppServer/profiles/InfoSphere/bin
# ./wsadmin.sh -lang jython
Realm/Cell Name: <default>
Username: wimadmin
Password:

WASX7209I: Connected to process "server1" on node ipsvm00182Node01 using SOAP connector;
The type of process is: UnManagedProcess
WASX7031I: For help, enter: "print Help.help()" wsadmin>AdminTask.exportSAMLSpMetadata('-
spMetadataFileName /tmp/spdata.xml -ssoId 1')
'true'
wsadmin>quit

# ls -l /tmp/spdata.xml
-rw-r--r-- 1 root root 700 May  9 21:15 /tmp/spdata.xml
```

The example above yields file `/tmp/spdata.xml` with the SAML TAI's SP information. Now you need to add the service provider partner to the identity provider AD FS.

Using the data file from the previous example, follow these steps:

- Copy `/tmp/spdata.xml` from the Linux WebSphere server to the Windows AD FS server (for example to `C:\tmp\spdata.xml`).
- On the AD FS machine, start the AD FS Manager Console.
- In the ADFS Manager: `Actions > Add Relying Party Trust... > Start`
- Import data about the relying party from a file `> Federation metadata file location = C:\tmp\spdata.xml`
- Next
- `Display name = WAS SAML ACS, profile = saml`
- Next
- Do not select Multi-factor Auth
- Next
- Permit all users
- Next
- Next

- Leave the checkbox for open the Edit Claims Rules dialog
- Close

Now you need to configure the AD FS Claim Rules.

Configure AD FS Claim Rules

The claim rule definitions determine what is returned in the SAML Response to WebSphere.
In the Claim Rule dialog, choose the following settings:

- claim rule: "Send LDAP Attributes as Claims"
- claim Name (provide a descriptive name): LDAP NameID mapping
- Attribute Store: Active Directory
- LDAP Attribute: SAM-Account-Name
- Outgoing claim type: Name ID

The above configuration makes sure the userid short name is returned in the NameID field of the SAML Response. The LDAP filter in WebSphere needs also to be configured to use the userid short name so that the SAML TAI userid mapping is able to find a match.

Adding AD FS to WebSphere as an Identity Provider (IdP)

To add the AD FS server as a trusted Identity Provider (IdP) follow directions in article "Configuring single sign-on (SSO) partners" here
http://www.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/twbs_configuresamlssopartners.html

An example of the procedure follows:

1. **Add an identity provider to the WebSphere Application Server SAML service provider for single sign-on:**
   To use the WebSphere Application Server SAML service provider for single sign-on with an identity provider, you need to add the identity provider as a partner. Three equivalent procedures are described in the article. In the example we have selected
   "Import the SAML token signer certificate using the administrative console"

   A. To export the token signer certificate from AD FS, follow this example:
      - In the AD FS Management console: Go to Service > Certificates, select the Token-signing certificate > click View Certificate in the Actions pane.
        The standard Windows certificate viewing window pops up.
      - Click the Details tab
      - Click 'Copy to file...'. The Certificate Export Wizard is shown.
      - Select Next
      - Select 'Base-64 encoded X.509 (.CER)'
      - Select Next
      - Provide file name: `C:\tmp\ADFS_Token-signing_Cert.CER`
      - Select Next
      - Select Finish

   B. To import the token signer certificate from AD FS onto WebSphere
      - Copy the exported file `ADFS_Token-signing_Cert.CER` to the WebSphere machine.
      - Log on to the WebSphere Application Server administrative console.

- Click `Security > SSL certificate and key management > Key stores and certificates > NodeDefaultTrustStore > Signer certificates`.
  Use **CellDefaultTrustStore** instead of **NodeDefaultTrustStore** for a deployment manager.
- Click Add.
- Provide the certificate information by using the exported .CER file
- Click Apply.

2. **Add IdP realms to the list of inbound trusted realms**:
   For each Identity provider that is used with your WebSphere Application Server service provider, you must grant inbound trust to all the realms that are used by the identity provider.
   You can grant inbound trust to the identity providers using either the administrative console or the `wsadmin` command utility.

   To add inbound trust using the administrative console:
   - Click Global security
   - Under user account repository, click Configure.
   - Click Trusted authentication realms - inbound.
   - Click Add External Realm.
   - Provide the external realm name.
   - Click OK and Save changes to the master configuration.

   As an example, add the following to the inbound trusted realms:

```
External realm name  = https://fs.isf_dev.com/adfs/ls/
                     = http://fs.isf_dev.com/adfs/services/trust
```

Chapter 4: InfoSphere Information Server Configuration

Requirements

IBM InfoSphere Information Server Version 11.5.0.1 or higher implements solutions for federated single sign-on for its web applications. However, you will also need to:

- Upgrade WebSphere ND to version 8.5.5.8 or higher. Note that currently WebSphere Liberty does not support a SAML configuration and therefore cannot be used for this purpose.

- If using IIS version 11.5.0.1 GA, installation of the following patches is required:
  - ISF Patch JR57496
  - If you are using the Information Governance Catalog (IGC), installation of Governance Rollup 7 Patch or higher is also required.

- If using IIS version 11.5.0.2 GA, or higher, no additional patches or fixes are necessary.

Configuration

There are two InfoSphere Information Server repository key-value pairs that are used to enable and activate the SAML configuration and provide the proper redirection to the configured IdP provider login page:

- `com.ibm.iis.isf.security.SAML`
- `com.ibm.iis.isf.security.SAMLSecureURL`

Setting `com.ibm.iis.isf.security.SAML` to 'true' will enable the SAML forwarding behavior. This basically allows the redirection of the un-authorized user to the configured SAML IdP login page.

The `com.ibm.iis.isf.security.SAMLSecureURL` is the URI where an un-authenticated user is redirected when trying to access a protected IIS application. Set this value to the IIS secure Launchpad URI ("`/ibm/iis/launchpad/secure`"). The URI contains the short address of the web application, and cannot contain server or port information.

To list the existing IIS Repository settings, use:

```
cd /opt/IBM/InformationServer/ASBServer/bin
./iisAdmin.sh -display -key com.ibm.iis.isf.security.SAML*
```

To turn on SAML principal forwarding use:

```
./iisAdmin.sh -set –key com.ibm.iis.isf.security.SAML -value true
```

To change the URI for redirection when accessing a protected IIS application:

```
./iisAdmin.sh -set -key com.ibm.iis.isf.security.SAMLSecureURL –value
"/ibm/iis/launchpad/secure"
```

To unset the URL and the SAML forwarding (e.g. turn off forwarding):

```
./iisAdmin.sh -unset -key com.ibm.iis.isf.security.SAMLSecureURL
./iisAdmin.sh -unset -key com.ibm.iis.isf.security.SAML
```

You will need to restart WAS for any of the above changes to take effect.

Chapter 5: LDAP Configuration

Overview of installation and configuration

You need to configure the LDAP access to Active Directory underlying the SAML IdP, either as a Federated Repository or Stand-alone LDAP Repository. Note that the SAML Assertion only provides identity information that InfoSphere Information Server can use for authentication. It does not provide other information needed for authorization, such as group memberships. So, even though the SAML Assertion can be configured to provide additional user info, the WAS SAML TAI cannot process such additional information at this time.

The SAML TAI provides a mapping between the authenticated user id and the LDAP user id (when the TAI idMap parm is set, e.g. `sso_1.sp.idMap = localRealmThenAssertion`). When this mapping takes place InfoSphere Information Server can obtain user authentication data via the SAML assertion, then obtain the needed and additional user information via LDAP.

Chapter 6: Additional WebSphere configuration changes

Configuration changes

One additional WebSphere configuration change is required:

In the WebSphere Console:
`Servers > Server Types > WebSphere Application Servers > server1 > Server Infrastructure > Java and Process Management > Process Definition > Additional Properties > Java Virtual Machine`

add the additional Generic JVM argument:
`-Dcom.ibm.ws.security.web.saml.decodeURL=false`

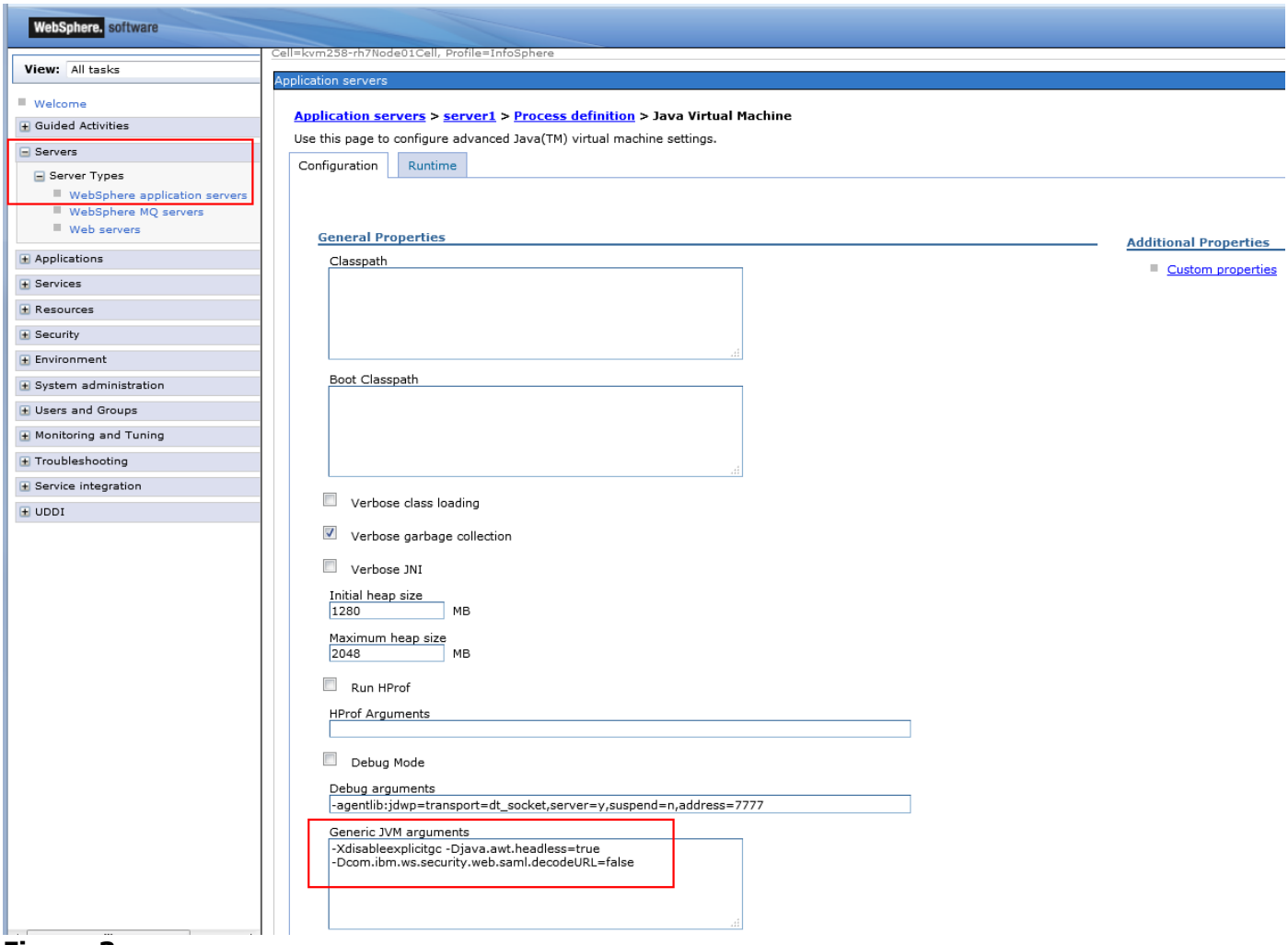


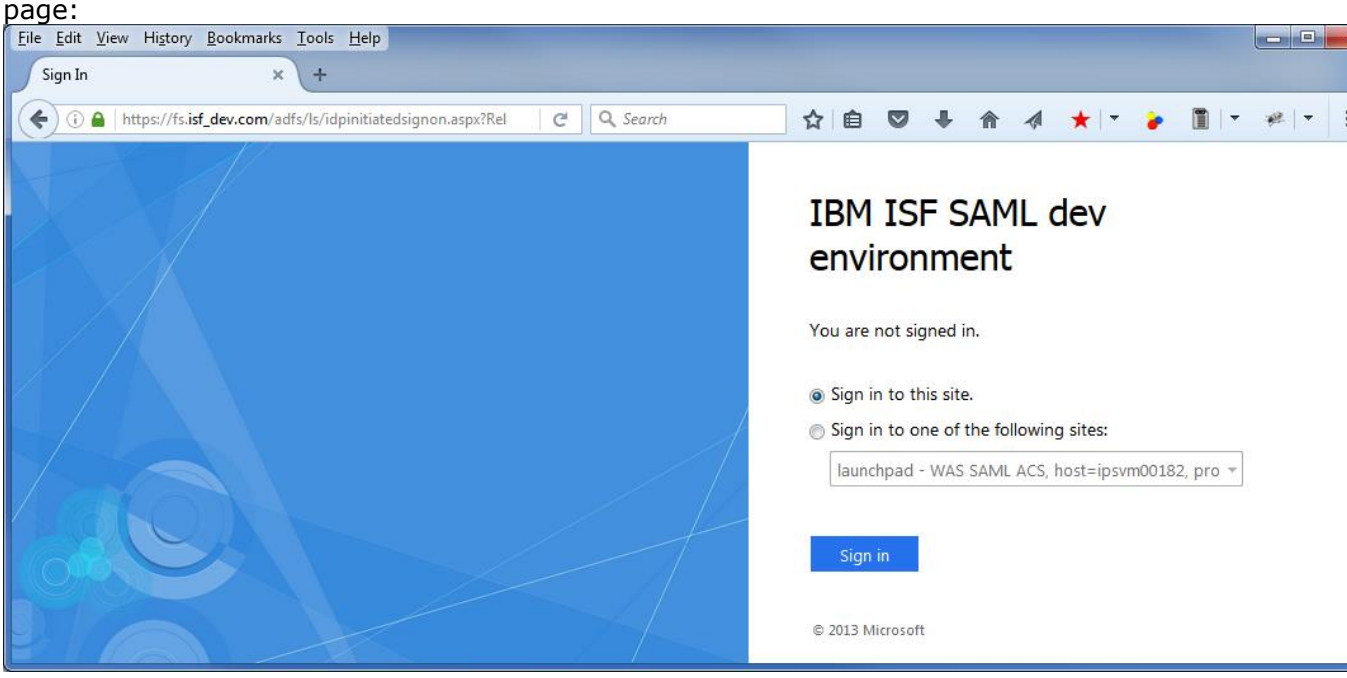
Figure 3.

Chapter 7: User scenarios and standard behavior

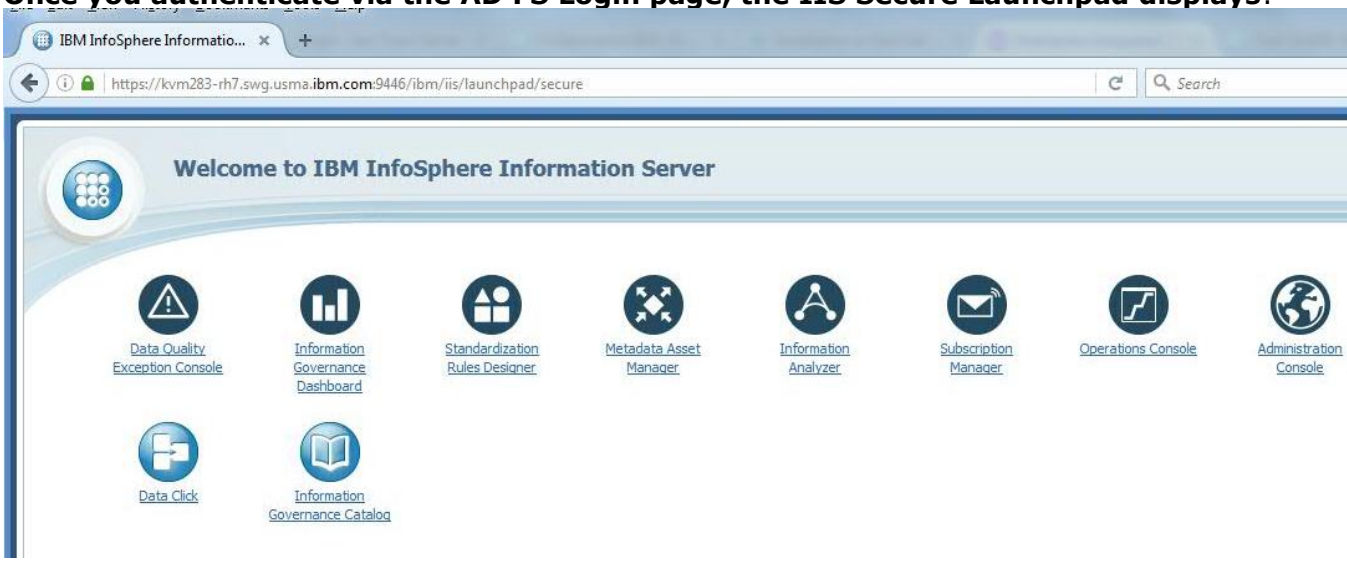
Once the system is completely configured and running, we expect the following scenarios and operations behavior:

Single Sign-On:

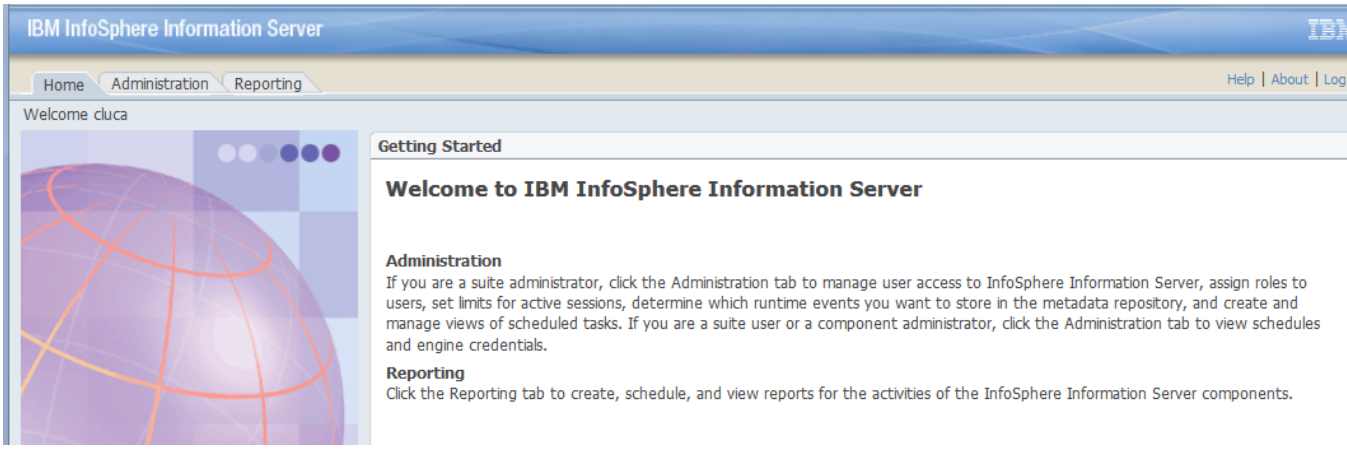
1. **Accessing the IIS Secure Launchpad:**
   Access the IIS Secure Launchpad via: https://<IISServer>:<port>/ibm/iis/launchpad/secure
   If not already authenticated via the configured IdP, user is redirected to the AD FS IdP Login page:



2. **Once you authenticate via the AD FS Login page, the IIS Secure Launchpad displays**:

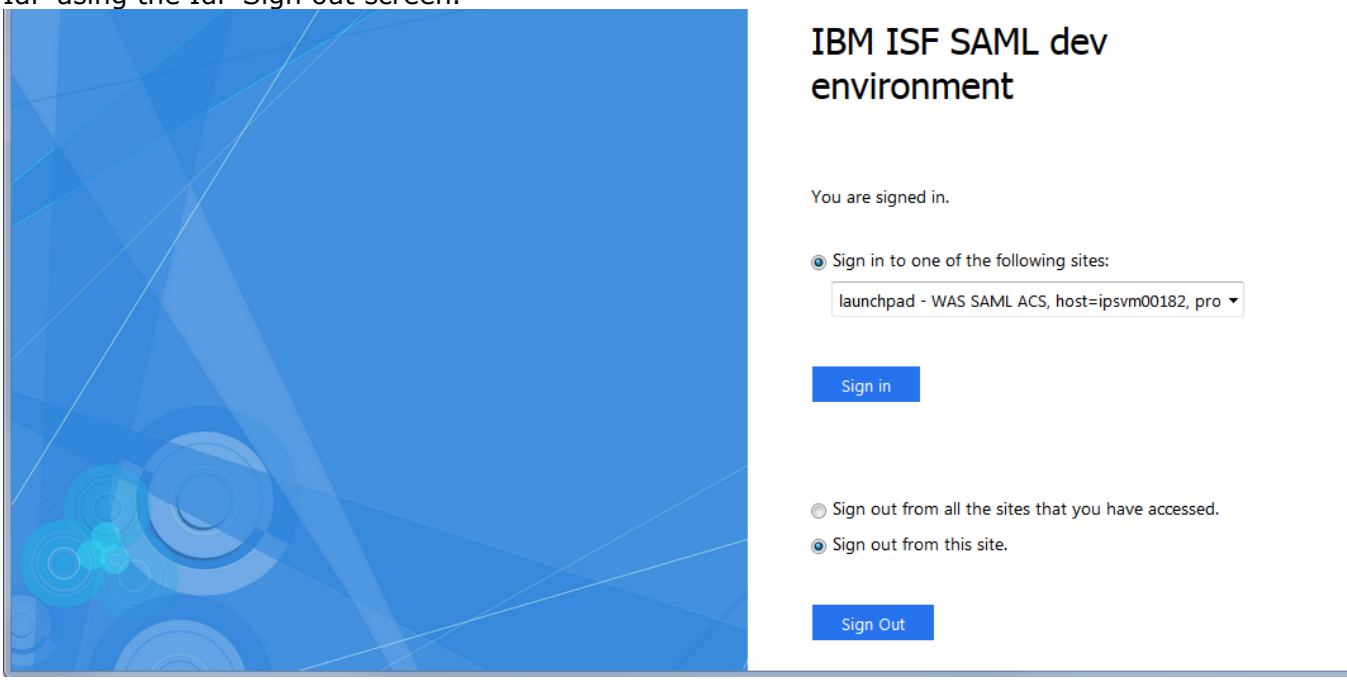


3. **Once authenticated, invoke any of the IIS web applications** without a request for further authentication.



Single Log Out (SLO):

1. Once the user has logged out from one of the IIS web applications, the active WAS LTPA token is invalidated and user is therefore logged out from all of the active IIS web applications running within instances of the same web browser type (Internet Explorer, FireFox, etc).
2. Once logged out, the user is redirected to the SAML IdP login to renew the authentication.
3. Once a WAS LTPA token or the SAML token expires (via time-out), it cannot be used for any further interaction by any of the IIS web applications. The token expiration essentially acts as a logout for each of the active web applications. User is redirected to the IdP login page when this scenario occurs.
4. If you want to logout of the IIS application in order to switch user ID, log out of the SAML IdP using the IdP Sign out screen.



Chapter 8: Troubleshooting notes and issues

Unsupported Functions

IIS and the SAML configuration do not support the following functions and tasks:

- IIS trusted and system user authentication.
- IIS thick clients, like the IIS Windows Console
- IIS command line clients
- ISD Web Services, as deployed by the IIS ISD Console.

Information Server 11.7.x web applications not supporting SAML SSO

In InfoSphere Information Server version 11.7.x, the following web applications do not recognize and adhere to the SAML 2.0 SSO login protocol. An explicit login to these applications is necessary even after an SSO login:

- Information Governance Catalog New
- Governance Monitor (New)
- Enterprise Search (New)

Known issues

Due to the different nature of the IIS applications, you may encounter the following behavior in particular situations:

- The IIS application Standardization Rules Designer (SRD), after a logout, does not return to the main SAML IdP login screen to renew the authentication, but shows its proprietary SRD login screen instead. However, the Single Log Out feature still functions correctly, as it invalidates the active WAS LTPA token.

  Solution: After a logout from the SRD application, when the SRD proprietary login screen shows, do not login onto the SRD application directly, but manually redirect your browser to the IIS Secure Launchpad via https://<IISServer>:<port>/ibm/iis/launchpad/secure or to your SAML IdP login screen to properly login with SSO via SAML.

- Within one instance of a browser, if you have multiple browser tabs open running different IIS applications, a logout from one application in one browser tab may not be immediately reflected in the applications running on other background tabs. Applications in these background tabs may show an error and may fail to automatically redirect you to the SAML IdP login screen.

  Solution: Refresh the browser window (F5 key) of these secondary tabs to redirect you to the SAML login screen.

- The WAS LTPA token or the SAML token may expire and a time-out will occur after the configured amount of time. This event produces the same behavior as a logout event, where the expired LTPA token is not valid any longer. When this happens, some IIS applications may report an error to the user. A similar error may occur when you have multiple browser tabs open with IIS applications running in them.

  Solution: This behavior is expected, especially in the browser background tabs. Refresh the browser window (F5 key) of these secondary tabs to redirect you to the SAML login screen.

Troubleshooting notes

There following notes will help you avoid usual pitfalls and describe expected behavior when working with a SAML installation:

1. If you **set or reset the two InfoSphere Information Server repository key-value pairs**
   `com.ibm.iis.isf.security.SAML`
   `com.ibm.iis.isf.security.SAMLSecureURL`
   you need to restart WAS in order for the change in the repository keys to be acknowledged.

2. **Installing and Configuring the WebSphere SAML TAI** - Deploying the application using the ' installSamlACS.py' script
   You may find issues deploying the SAML TAI application, as in the following example:

```
cd C:\IBM\WebSphere\AppServer\profiles\saml\bin
C:\IBM\WebSphere\AppServer\profiles\saml\bin>wsadmin -f installSamlACS.py install
ipsvm00529Node02 server1

 WASX7209I: Connected to process "server1" on node ipsvm00529Node02 using SOAP
connector;  The type of process is: UnManagedProcess
 WASX7303I: The following options are passed to the scripting environment and are
available as arguments that are stored in the argv variable: "[install,
ipsvm00529Node02, server1]"
 WASX7011E: Cannot find file "installSamlACS.py"
```

   However, "installSamlACS.py" is in `C:\IBM\WebSphere\AppServer\bin`, not the profile bin. So, you need to run the command from the `AppServer\bin` dir:

```
cd C:\IBM\WebSphere\AppServer\bin
C:\IBM\WebSphere\AppServer\bin>wsadmin -f installSamlACS.py install ipsvm00529Node02
server1

WASX7209I: Connected to process "server1" on node ipsvm00529Node02 using SOAP
connector;  The type of process is: UnManagedProcess
WASX7303I: The following options are passed to the scripting environment and are
available as arguments that are stored in the argv variable: "[install,
ipsvm00529Node02, server1]"
Installing Saml ACS service...
Deploying WebSphereSamlSP.ear
ADMA0073W: Custom permissions are found in the [("java.security.AllPermission" "<all
permissions>" "<all actions>")] policy file. Custom permissions can compromise the
integrity of Java 2 Security.
    WASX7327I: Contents of was.policy file:
           grant codeBase "file:${application}" {
           permission java.security.AllPermission;
          };
ADMA5016I: Installation of WebSphereSamlSP started.
ADMA5058I: Application and module versions are validated with versions of deployment
targets.
ADMA5005I: The application WebSphereSamlSP is configured in the WebSphere
Application Server repository.
ADMA5005I: The application WebSphereSamlSP is configured in the WebSphere
Application Server repository.
ADMA5081I: The bootstrap address for client module is configured in the WebSphere
Application Server repository.
ADMA5053I: The library references for the installed optional package are created.
ADMA5005I: The application WebSphereSamlSP is configured in the WebSphere
Application Server repository.
ADMA5001I: The application binaries are saved in
```

```
C:\IBM\WebSphere\AppServer\profiles\saml\wstemp\Script15430e2fa33\workspace\cells\ip
svm00529Node02Cell\applications\WebSphereSamlSP.ear\WebSphereSamlSP.ear
ADMA5005I: The application WebSphereSamlSP is configured in the WebSphere
Application Server repository.
SECJ0400I: Successfully updated the application WebSphereSamlSP with the
appContextIDForSecurity information.
ADMA5005I: The application WebSphereSamlSP is configured in the WebSphere
Application Server repository.
ADMA5005I: The application WebSphereSamlSP is configured in the WebSphere
Application Server repository.
ADMA5113I: Activation plan created successfully.
ADMA5011I: The cleanup of the temp directory for application WebSphereSamlSP is
complete.
ADMA5013I: Application WebSphereSamlSP installed successfully.
```

3. **Exporting the SAML TAI Service Provider metadata from a Windows WebSphere**
When exporting the SAML TAI SP information from a Windows WebSphere system, you may run in some syntax issues:

```
cd C:\IBM\WebSphere\AppServer\profiles\saml\bin
C:\IBM\WebSphere\AppServer\profiles\saml\bin>wsadmin -lang jython

WASX7209I: Connected to process "server1" on node ipsvm00529Node02 using SOAP
connector;  The type of process is: UnManagedProcess
WASX7031I: For help, enter: "print Help.help()"
wsadmin>AdminTask.exportSAMLSpMetadata('-spMetadataFileName c:\tmp\spdata.xml -ssoId
1')
WASX7015E: Exception running command: "AdminTask.exportSAMLSpMetadata('-
spMetadataFileName c:\tmp\spdata.xml -ssoId 1')"; exception information:
com.ibm.websphere.management.cmdframework.CommandException: Unable to write c:
mp\spdata.xml
```

The Windows wsadmin command still needs the Unix style path information:

```
wsadmin>AdminTask.exportSAMLSpMetadata('-spMetadataFileName /tmp/spdata.xml -ssoId
1')
'true'
wsadmin>quit
C:\IBM\WebSphere\AppServer\profiles\saml\bin>dir C:\tmp\spdata.xml
 Volume in drive C has no label.
 Volume Serial Number is 5ED6-13CF
 Directory of C:\tmp
     04/19/2016  08:21 PM               694 spdata.xml
                    1 File(s)            694 bytes
                    0 Dir(s)  134,752,227,328 bytes free
```

4. **NameID missing from SAML Assertions**
After completing the steps to enable the SAML TAI, adding the WebSphere server to AD FS as a SAML Service Provider (SP, or a Relying Party Trust), and adding AD FS to WebSphere as a trusted IdP, and restarting WebSphere, you may encounter the following error:

In the web browser:
```
Error 403: AuthenticationFailed
```

And in the WAS SystemOut.log:

```
[] 00000089 WebAuthentica E   SECJ0126E: Trust Association failed during validation.
The exception is com.ibm.websphere.security.WebTrustAssociationFailedException:
key:null
```

```
At
com.ibm.ws.security.web.saml.ACSTrustAssociationInterceptor.createTAIErrorResult(ACS
TrustAssociationInterceptor.java:678)
       at
com.ibm.ws.security.web.saml.ACSTrustAssociationInterceptor.invokeTAIbeforeSSO(ACSTr
ustAssociationInterceptor.java:555)
       at
com.ibm.ws.security.web.saml.ACSTrustAssociationInterceptor.negotiateValidateandEsta
blishTrust(ACSTrustAssociationInterceptor.java:335)
       at
com.ibm.ws.security.web.TAIWrapper.negotiateAndValidateEstablishedTrust(TAIWrapper.j
ava:101)
       at
com.ibm.ws.security.web.WebAuthenticator.handleTrustAssociation(WebAuthenticator.jav
a:421)
…
com.ibm.ws.security.web.saml.ACSTrustAssociationInterceptor.createTAIErrorResult(ACS
TrustAssociationInterceptor.java:669)
       ... 31 more
```

Make sure that the setup is correct and that the user credentials are valid.

To get more descriptive logs, you can increase the trace level for WebSphere to the following:

```
*=info:com.ibm.iis.xmeta.*=warning:com.ibm.xmeta.*=warning:com.ibm.ws.security.web.*
=all:com.ibm.ws.webcontainer.*=all:com.ibm.wsspi.webcontainer.*=all:HTTPChannel=all:
GenericBNF=all:com.ibm.ws.jsp=all:com.ibm.ws.session.*=all:com.ibm.websphere.wim.*=a
ll:com.ibm.ws.wim.*=all:com.ibm.wsspi.wim.*=all:com.ibm.iis.isf.j2ee.*=all:com.ascen
tial.acs.security.*=all:com.ibm.iis.isf.security.*=all:com.ibm.websphere.wssecurity.
*=all:com.ibm.ws.wssecurity.*=all:com.ibm.ws.wssecurity.platform.audit.*=off
```

The above will produce a verbose (maybe an overachieving) trace log. But it adds the following message to the trace log:

```
[] 00000089 ACSTrustAssoc 3   SAMLResponse could not be verified.key:null
```

NOTE: The above message indicates you may be still using WAS ND version 8.5.5.7 or earlier version. You will need to upgrade WAS ND to version 8.5.5.8 or later.

After installing the required WAS ND 8.5.5 FP8, after attempting to login via AD FS, the error will show as:

```
CWSML7010E: The [NameID] sub-element of the [Subject] element in the SAML assertion
element is missing or empty.
```

The NameID is missing from the SAML response. The WAS SAML TAI expects the NameID field to identify the user being authenticated.

When setting up the SAML-Account-Name, in the claim rule on the AD FS side you need:

```
Claim rule template: Send LDAP Attributes as Claims
Attribute Store: Active Directory
Mapping of LDAP attributes to outgoing claim types:
LDAP Attribute: SAM-Account-Name → Outgoing Claim Type: NameID
```

So, The LDAP SAM-Account-Name is mapped to the NameID in the outgoing claims.

5. **Incorrect WebSphere Trusted Realm setup**
   After correctly configuring the missing NameID in the SAML response, you may still encounter the following error in the WebSphere SystemOut.log file:

   ```
   [] 0000008f WebAuthentica E   SECJ0126E: Trust Association failed during validation.
   The exception is com.ibm.websphere.security.WebTrustAssociationFailedException:
   com.ibm.wsspi.wssecurity.core.SoapSecurityException: CWWSS8036E: A SAML assertion
   with ID [_d1f9be20-eb88-4e6c-b1fb-bdea8ed6fea1] has already been received and
   processed.
   ```

   This may indicate an incorrect trusted realm. The realm is by default mapped to the <Issuer> field in the SAML Response, as for example:
   "<Issuer>http://fs.isf_dev.com/adfs/services/trust</Issuer>"

   So add 'http://fs.isf_dev.com/adfs/services/trust' to the trusted realms, i.e.:
   Security > Global security > Under user account repository, click Configure > Click Trusted authentication realms - inbound > External Realm
   and add: http://fs.isf_dev.com/adfs/services/trust

   Also add the URL in the sso_1.idp_1.SingleSignOnUrl, i.e. https://fs.isf_dev.com/adfs/ls/ to trusted Inbound realms:
   Security > Global security > Under user account repository, click Configure > Click Trusted authentication realms - inbound > External Realm
   add: https://fs.isf_dev.com/adfs/ls/

   The above may produce in the trace log:

   ```
   [] 00000085 WSCredentialT W   SECJ5008W: The realm specified in
   com.ibm.wsspi.security. cred.realm (http://fs.isf_dev.com/adfs/services/trust) does
   not match the current realm (IPSVM00529). This could cause problems when trying to
   make a downstream request.
   ```

   Then also use
   Security > Global security > RMI/IIOP security > CSIv2 outbound communications > Trusted authentication realms - outbound > Add External Realm
   and add
   http://fs.isf_dev.com/adfs/services/trust

   At which point the WAS configuration should be complete in accepting the IDs asserted by AD FS.

6. **Information Server commands, operations, and web applications not working after configuration of SAML and SSO**
   If you are using IS 11.5.0.1 with the ISF 11.5 RUP4 patch installed, after configuration of SAML and SSO, some operations and functions may not work, as for example:
   - Invocation of the ASBAgent (node agent) NodeAgents.sh/bat reports error and agent is not listening to configured port.
   - Invocation of Information Server web applications, even after a validated Identity Provider login, redirects the user to the Identity Provider login screen, if the user does not have DataStage/QualityStage User and DataClick Author/User roles.

   Solution: Install ISF Patch JR57496, as recommended in the Requirements paragraph in this document.

7. **Information Server web applications are not working with SSO when using IS 11.5.0.1 with Patch JR57496, or when using IIS 11.5.0.2**
   You may encounter issues with the web applications behavior in SSO mode, if you have IIS 11.5.0.1 and Patch JR57496, or IIS 11.5.0.2. For example:
   - IA and DataClick icons are not displayed in the secure launchpad screen
   - You are unable to launch any web clients from the secure launchpad, if the user has only Suite User and IGC User roles.
   - After successful login to the IdP, attempt to launch any web application redirects the browser to the IdP login page.

   Solution: Verify the existing IIS Repository settings, using:

```
cd /opt/IBM/InformationServer/ASBServer/bin
./iisAdmin.sh -display -key com.ibm.iis.isf.security.SAML*
```

   Make sure you have both registry keys defined:
   `com.ibm.iis.isf.security.SAML` has value `true`
   `com.ibm.iis.isf.security.SAMLSecureURL` has a value, like `"/ibm/iis/launchpad/secure"`

   To turn on SAML principal forwarding use:

```
./iisAdmin.sh -set –key com.ibm.iis.isf.security.SAML -value true
```

   To change the default URI for redirecting an un-authenticated user:

```
./iisAdmin.sh -set -key com.ibm.iis.isf.security.SAMLSecureURL –value
"/ibm/iis/launchpad/secure"
```

   Note that the URL specified for `com.ibm.iis.isf.security.SAMLSecureURL` can only contain the URL short address of the web application, without server or port specified, as for example in `"/ibm/iis/launchpad/secure"`.
   You will need to restart WAS for any of the above changes to take effect.

Useful links

The following documents and links can provide additional information and explanations on SAML, AD FS, and WebSphere Application Server with a SAML environment:

SAML

- Video presentation on SAML and SPNEGO concepts: "BP104 -- Simplifying The S's: Single Sign-On, SPNEGO and SAML -- Gabriella Davis, The Turtle Partnership -- Chris Miller, Connectria" - http://w3.tap.ibm.com/medialibrary/media_view?id=243931

AD FS

- "Active Directory Federation Services (Overview, Example code)" - https://msdn.microsoft.com/en-us/library/bb897402.aspx
- "Simplify Single Sign-on Using ADFS" - https://technet.microsoft.com/en-us/magazine/2006.07.simplify.aspx
- "A Developer's Introduction To Active Directory Federation Services" - http://blogs-sso-ashutoshmisra.blogspot.com/2014/06/a-developers-introduction-to-active.html
- "ADFS Deep-Dive: Comparing WS-Fed, SAML, and Oauth" - https://blogs.technet.microsoft.com/askpfeplat/2014/11/02/adfs-deep-dive-comparing-ws-fed-saml-and-oauth/
- "AD FS 2.0 Cmdlets in Windows PowerShell" - https://technet.microsoft.com/en-us/library/ee892329.aspx

WebSphere application Server

- A good overview of WebSphere authentication: "IBM WebSphere Developer Technical Journal: Advanced authentication in WebSphere Application Server" - http://www.ibm.com/developerworks/websphere/techjournal/0508_benantar/0508_benantar.html
- "Understanding the WebSphere Application Server SAML Trust Association Interceptor" - http://www.ibm.com/developerworks/websphere/techjournal/1307_lansche/1307_lansche.html
- "Identity federation using SAML and WebSphere software" - http://www.ibm.com/developerworks/library/ws-SAMLWAS/
- This WAS Portal example is not completely applicable to WebSphere Application Server, but contains some useful insights: "Step by step guide to implement SAML 2.0 for Portal 8.5" - https://developer.ibm.com/digexp/docs/docs/customization-administration/step-step-guide-implement-saml-2-0-portal-8-5/
- This WAS Portal example is not fully applicable to IIS, but still interesting. "Front Side SAML SSO with Microsoft product (ADFS -> WAS SAML TAI)" - https://www.ibm.com/developerworks/community/blogs/8f2bc166-3bdc-4a9d-bad4-3620dbb3e46c/entry/Front_Side_SAML_SSO_with_microsoft_product_ADFS_WAS_SAML_TAI?lang=en
- Knowledge Center doc on the SAML TAI properties. "SAML web single sign-on (SSO) trust association interceptor (TAI) custom properties" - http://www.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/rwbs_samltaiproperties.html

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.