

# HP Select Federation

for the HP-UX, Linux, Solaris and Windows® operating systems

Software Version: 7.01

---

## Sun Java System Access Manager Connector Guide

Document Release Date: March 2008

Software Release Date: March 2008



## Legal Notices

### Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

### Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

### Copyright Notices

© Copyright 2002-2008 Hewlett-Packard Development Company, L.P.

HP Select Federation includes software developed by third parties. The software in Select Federation includes:

- Apache Derby, Apache Xalan Library, Apache Xerces Library, and Apache XML Dsig Library.
- Software developed by the University Corporation for Advanced Internet Development <<http://www.ucaid.edu>>Internet2 Project.

### Trademark Notices

- Java™ and all Java based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.
- Microsoft®, Windows®, and Windows XP® are U.S. registered trademarks of Microsoft Corporation.
- Oracle® is a registered trademark of Oracle Corporation. Various product and service names referenced herein may be trademarks of Oracle Corporation.
- UNIX® is a registered trademark of The OpenGroup.

## Documentation Updates

This guide's title page contains the following identifying information:

- Software Version number, which indicates the software version.
- Document release date, which changes each time the document is updated.
- Software release date, which indicates the release date of this version of the software.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

**<http://h20230.www2.hp.com/selfsolve/manuals>**

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

## Support

You can visit the HP Software Support web site at:

**<http://www.hp.com/go/hpsoftwaresupport>**

HP Software Support Online provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

**[http://h20230.www2.hp.com/new\\_access\\_levels.jsp](http://h20230.www2.hp.com/new_access_levels.jsp)**

For more information about HP Passport, go to:

**<http://h20229.www2.hp.com/passport-registration.html>**

# Contents

<b>1</b>	<b>Introduction</b> .....	7
	Select Federation Sun Access Manager Connector Components .....	7
	Prerequisites .....	8
	Using the Select Federation Sun Access Manager Connector .....	8
	Using Sun Access Manager with SP and IDP Integration .....	8
	Using Sun Access Manager with the Select Federation Administration Console and Privacy Manager	10
<b>2</b>	<b>Deploying the Select Federation Sun Access Manager Connector</b> .....	13
	System Requirements .....	13
	Software Requirements .....	13
	Platform Requirements .....	13
	Deploying the Select Federation Sun Access Manager Connector .....	13
	Rolling Back the Select Federation Sun Access Manager Connector .....	15
	Rolling Back the Select Federation Sun Access Manager Connector From the IDP Integration ....	15
	Rolling Back the Select Federation Sun Access Manager Connector From the SP Integration ....	15
	Select Federation Sun Access Manager Connector Logging .....	16
<b>3</b>	<b>Integrating the Select Federation Sun Access Manager Connector with an IDP Site</b> .....	17
	Requirements .....	17
	Integration Mechanisms for an SF-IDP .....	17
	Using a Login URL .....	18
	Using the Select Federation Agent .....	18
	Configuring Sun Access Manager for the IDP Integration .....	19
	Step 1: Prepare the Environment for Federated Applications .....	19
	Step 2: Configure Sun Access Manager .....	21
	Step 3: Configure the SF-IDP for the Sun Access Manager Integration .....	25
	Step 4: Configure Profile Attributes for Federated Users .....	29
	Step 5: (Optionally) Test the Sun Access Manager Connector Integration with the Demonstration	
	Application .....	30
<b>4</b>	<b>Integrating the Select Federation Sun Access Manager Connector with an SP Site</b> .....	31
	Requirements .....	31
	Integration Mechanisms for an SF-SP .....	31
	Using a Login URL .....	32
	Using the Select Federation Agent .....	32
	Configuring Sun Access Manager for the SP Integration .....	33
	Step 1: Determine a User Activation Scheme .....	33
	Configuring Select Federation .....	33
	Using the Activate URL Plugin for the User Activation Scheme .....	34

Step 2: (Optionally) Set User Profile Attributes as a Cookie .....	34
Step 3: Configure Sun Access Manager .....	35
Step 4: Configure the SF-SP for the Sun Access Manager Integration .....	43
Step 5: (Optionally) Test the Sun Access Manager Connector Integration with the Demonstration Application .....	47
<b>5 Error Messages</b> .....	<b>49</b>
Error Message Terminology .....	49
Error Messages and Descriptions .....	49
SAMAmPlugin Error Messages .....	50
SAMAAuthnPlugin Error Messages .....	50
SAMEventPlugin Error Messages .....	51
SAMUtil Error Messages .....	52
<b>A Troubleshooting</b> .....	<b>55</b>
<b>Glossary</b> .....	<b>57</b>
<b>Index</b> .....	<b>67</b>

# 1 Introduction

This guide describes how to deploy, integrate and configure the Sun Java System Access Manager (Sun Access Manager) connector. The Select Federation Sun Java System Access Manager connector integrates with Select Federation IDP and SP sites, and the Administration console and Privacy Manager.

Following are example use-cases where you would use the Sun Access Manager connector

- An enterprise that manages its users and applications through Sun Access Manager needs to enable its users to seamlessly access any federated applications offered by its enterprise partners. An IDP-only mode installation of Select Federation (SF-IDP) can be integrated with Sun Access Manager through the Sun Access Manager connector to accomplish this goal.
- An enterprise that manages its users and applications through Sun Access Manager needs to enable federated users to access its domain-local applications. An SP-only mode installation of Select Federation (SF-SP) can be integrated with Sun Access Manager through the Sun Access Manager connector to accomplish this goal.
- An enterprise that manages its users and applications through Sun Access Manager, needs to enable the following:
  - Sun Access Manager users to seamlessly access any federated applications offered by its enterprise partners
  - Federated users to access its domain-local applications. An SP and IDP mode installation of Select Federation (SF-SP&IDP) can be integrated with Sun Access Manager through the Sun Access Manager connector to accomplish this goal.

This chapter describes the Sun Access Manager connector integration with Select Federation in the following topics:

- [Select Federation Sun Access Manager Connector Components](#)
- [Prerequisites](#)
- [Using the Select Federation Sun Access Manager Connector](#)

## Select Federation Sun Access Manager Connector Components

The Select Federation Sun Access Manager connector consists of the following components:

- IDP side component, which includes the Sun Access Manager-protected Select Federation Administration console, Privacy Manager and Demonstration application (`sf-demo`).
- SP side component, which includes the Sun Access Manager-protected Select Federation Administration console, Privacy Manager and Demonstration application (`sf-demo`).

The Select Federation Sun Access Manager connector provides the ability to integrate Select Federation SP and IDP sites with Sun Access Manager 7.1.



Select Federation can only be integrated with one access management system at a time.

## Prerequisites

This document assumes you have knowledge of the following:

- HP Select Federation (installation, configuration, concepts and so on)
- Sun Access Manager 7.1 (installation, configuration, concepts and so on)
- Web application servers: Select Federation's built-in server (Tomcat 5.5.23), WebLogic 8.1 and 9.1, and WebSphere 6.0.2 (installation, configuration, concepts, and so on)



The Select Federation Sun Access Manager 7.1 connector is not supported on WebLogic 9.2.

## Using the Select Federation Sun Access Manager Connector

Many organizations may already have third-party Access Management systems deployed such as Sun Access Manager. These organizations may also assume the role of an identity provider (IDP) or service provider (SP). Select Federation integrates with Sun Access Manager out-of-the-box.

You can choose to integrate Sun Access Manager with Select Federation both as an IDP and as an SP. When you integrate Sun Access Manager with an SP or IDP, the Select Federation Administration console and Privacy Manager are protected by Sun Access Manager.

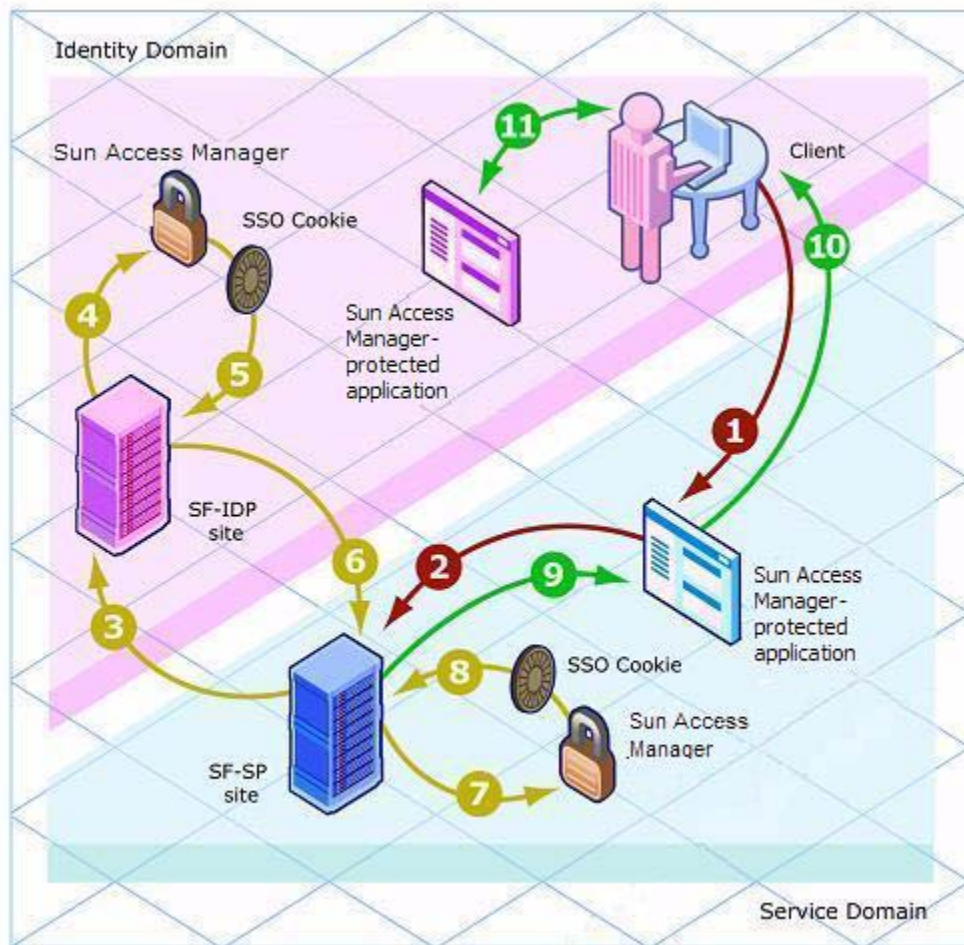
### Using Sun Access Manager with SP and IDP Integration

The advantage of integrating Sun Access Manager with a Select Federation SP and/or IDP site is that once a user is authorized to access a Sun Access Manager-protected application in the Service Domain and/or Identity Domain, the user is no longer challenged for credentials and the user has full access each time.

[Figure 1](#) illustrates the process of authorizing a user to access a Sun Access Manager-protected application both in the Service and Identity Domains.



**Figure 1 Authorization Flow to Access a Sun Access Manager-Protected Application**



Following is a step-by-step explanation of this diagram:

- 1 An unauthenticated user begins at a client, such as a browser, and tries to access a Sun Access Manager-protected application in the Service Domain that is integrated with Sun Access Manager.
- 2 The application redirects the user to the SF-SP site.
- 3 The SF-SP site redirects the user to the SF-IDP site, which is integrated with Sun Access Manager for authentication.
- 4 During the authentication process, the SF-IDP site presents the user with a login page, collects the credentials and calls to Sun Access Manager to generate a Sun Access Manager SSO Cookie.
- 5 Sun Access Manager replies with a Sun Access Manager SSO cookie for the Identity domain.
- 6 The SF-IDP returns the user to the SF-SP site after processing the request, generates an assertion and a Sun Access Manager SSO Cookie.
- 7 The SF-SP site calls out to Sun Access Manager to generate a Sun Access Manager SSO Cookie for the user using the assertion.

- 8 Sun Access Manager returns the Sun Access Manager SSO Cookie for the Service Domain.

The user is now authenticated.

- 9 The SF-SP site returns control to the application in the Service Domain.

- 10 The application is then presented to the client for the user to access.

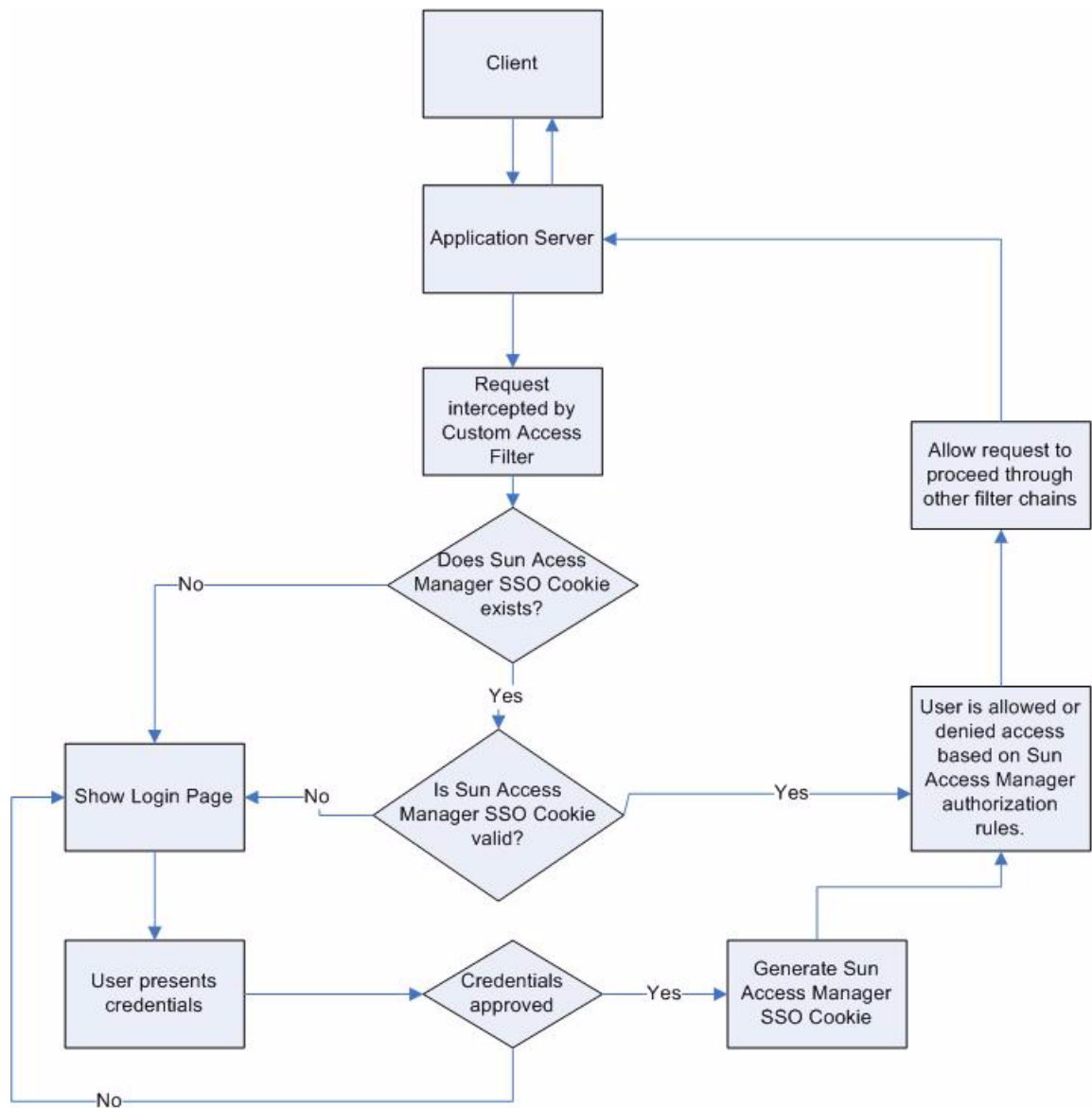
Since the Sun Access Manager SSO cookie has been generated for both the Service Domain and Identity Domain, the user is not challenged for credentials again. The user now has access to any application protected by Sun Access Manager within both Domains.

- 11 The user is able to access the application in the Identity Domain without being challenged.

## Using Sun Access Manager with the Select Federation Administration Console and Privacy Manager

The Select Federation Administration console and Privacy Manager are protected with Sun Access Manager using an access filter. [Figure 2](#) illustrates a user request flow to a Sun Access Manager-protected Administration console..

**Figure 2 Flow Diagram of the Administration Console Protected by Sun Access Manager**



Following is a step-by-step explanation of this diagram:

- 1 The user tries to access the Select Federation Administration console on an Application server, from a client such as a browser.
- 2 The Select Federation Access Filter intercepts the request and checks if a valid Sun Access Manager SSO Cookie exists.
- 3 If a valid Sun Access Manager SSO Cookie exists, the Access Filter either allows or denies access to the Administration console and Privacy Manager interfaces.

The decision to allow or deny access is based on the authorization policies configured in Sun Access Manager and if the request is allowed. Processing continues to other filters in the chain.

- 4 If no Sun Access Manager SSO Cookie exists or the cookie is not valid, the user is presented with a login page.

- 5 Once the user presents the credentials, the credentials are validated.
- 6 If the credentials are valid, the Sun Access Manager SSO Cookie is generated, and step 3 is performed.
- 7 If the credentials are invalid, the user is taken to step 4.

## 2 Deploying the Select Federation Sun Access Manager Connector

This chapter includes the following topics:

- System Requirements
- Deploying the Select Federation Sun Access Manager Connector
- Rolling Back the Select Federation Sun Access Manager Connector
- Select Federation Sun Access Manager Connector Logging

### System Requirements

#### Software Requirements

The following software must be installed and configured:

- Select Federation 7.00 plus 7.01 Patch — see the *HP Select Federation Installation Guide* for installation instructions
- Sun Java System Access Manager 7.1 — See the Sun Access Manager 7.1 documentation for installation instructions.



If you want your installation to support international characters, be sure you have properly set up the following to support these characters:

- Platforms on which Select Federation and Sun Access Manger are installed
- Databases and/or LDAP directories used by Select Federation and Sun Access Manager

#### Platform Requirements

The Select Federation Sun Access Manager Connector can work on any Select Federation platform that is compatible with the Sun Access Manager 7.1.



The Select Federation Sun Access Manager 7.1 connector is not supported on WebLogic 9.2.

## Deploying the Select Federation Sun Access Manager Connector

This section provides the basic steps for deploying the Select Federation Sun Access Manager connector on any application server on which Select Federation and Sun Access Manager are installed. For detailed instructions on application server-specific tasks, see the application server's documentation.

After the Select Federation patch has been applied, and Sun Access Manager has been installed, perform the following steps to deploy the Select Federation Sun Access Manager connector files:

- 1 On the machine or machines where Select Federation is installed, create a new directory under `$SF_HOME` called `sam_jars`.
- 2 Copy the following files from your Sun Access Manager installation (which may be on a different machine) to `$SF_HOME/sam_jars`:
  - `am_services.jar`
  - `amclientsdk.jar`
- 3 Copy the following files from the `$SF_PATCH/connectors/SAM/` directory to the `$SF_HOME/connectors/SAM/` directory:
  - `SAMConnector.jar`
  - `docs/SAM.pdf`
- 4 Modify `CLASSPATH` on your Select Federation instance so that it includes all the `jar` files that exist in the `$SF_HOME/sam_jars/` directory.

For example:

```
set CLASSPATH=<path_to_SF_HOME>/sam_jars/am_services.jar;  
<path_to_SF_HOME>/sam_jars/amclientsdk.jar;%CLASSPATH%
```

For exact instructions on how to modify the `CLASSPATH` for the application server on which Select Federation is installed, see the application server documentation.

- 5 Restart your application server.

All the variables should be set so that they are visible to the application server on which Select Federation is running. You may check the application server's logs to make sure that all the variables and their values have been picked-up by the application server.

- 6 Integrate the Select Federation Sun Access Manager connector with one of the following site roles:
  - Before you begin, make a backup copy of the `$SF_Home/conf/tfsconfig.properties` file. You can use this backup copy to roll back the Sun Access Manager connector integration. See [Rolling Back the Select Federation Sun Access Manager Connector](#) on page 15 for details.
  - Identity Provider (IDP) site — see [Chapter 3, Integrating the Select Federation Sun Access Manager Connector with an IDP Site](#) for complete integration and configuration instructions.
  - Service Provider (SP) site — see [Chapter 4, Integrating the Select Federation Sun Access Manager Connector with an SP Site](#) for complete integration and configuration instructions. Integrating Sun Access Manager with an SP site is the same as integrating Sun Access Manager with an SP+IDP site.
  - When you start up Select Federation, be sure that your Sun Access Manager instance is running so that the Sun Access Manager connector can be initialized properly.

# Rolling Back the Select Federation Sun Access Manager Connector

You can roll back the Select Federation Sun Access Manager connector integration from the Select Federation installation. To do this, copy your backed up version of the `$$SF_Home/conf/tfsconfig.properties` file over the existing `tfsconfig.properties` file.

If you did not back up the Select Federation installation `tfsconfig.properties` file, then follow the steps in the following sections.

## Rolling Back the Select Federation Sun Access Manager Connector From the IDP Integration

Perform the following steps to roll back the Select Federation Sun Access Manager connector from the IDP integration:

- 1 Comment out the following lines in the `tfsconfig.properties` file:

```
idpAuthnPlugin=myAuthPlugin
myAuthPlugin.class=com.hp.selectfederation.sam.SAMAuthnPlugin
myAuthPlugin.jar=<SF_INSTALL_DIR>/connectors/SAM/SAMConnector.jar
amPlugin=myAdminPlugin
myAdminPlugin.jar=<SF_INSTALL_DIR>/connectors/SAM/SAMConnector.jar
myAdminPlugin.class=com.hp.selectfederation.sam.SAMAmPlugin
```

- 2 Uncomment or add the following line where `<user-base-dn>` is your User repository Base DN and `user-id-attr` is your User ID attribute name:

```
idpAuthnPlugin=com.trustgenix.tfsIDP.util.IDPAuthnPlugin_Dir
ldapUserBaseDN=<user-base-dn>
ldapUserAttr=<user-id-attr>
```

- 3 Comment out or remove any of the parameters from the table in [Step 3: Configure the SF-IDP for the Sun Access Manager Integration](#) on page 25 that were added for the Sun Access Manager integration.

## Rolling Back the Select Federation Sun Access Manager Connector From the SP Integration

Perform the following steps to roll back the Select Federation Sun Access Manager connector from the SP integration:

- 1 Comment out the following lines in the `tfsconfig.properties` file:

```
spEventPlugin=myEventPlugin
myEventPlugin.class=com.hp.selectfederation.sam.SAMEventPlugin
myEventPlugin.jar=<SF_INSTALL_DIR>/connectors/SAM/SAMConnector.jar
amPlugin=myAdminPlugin
myAdminPlugin.jar=<SF_INSTALL_DIR>/connectors/SAM/SAMConnector.jar
myAdminPlugin.class=com.hp.selectfederation.sam.SAMAmPlugin
```

- 2 Comment out or remove any of the parameters from the table in [Step 3: Configure Sun Access Manager](#) on page 35 that were added for the Sun Access Manager integration.

## Select Federation Sun Access Manager Connector Logging

The Select Federation Sun Access Manager connector errors are logged based on settings in the Select Federation `log4j.properties` file in the `$SF_HOME/properties` directory. Use the Select Federation log file to view logged messages. The location of the log file depends on the application server on which you have Select Federation installed.

For WebLogic and WebSphere, you need to enable logging, if you have not done so already. Logging is already enabled for the built-in server.

- For instructions on enabling logging for WebLogic, see “Deploying Select Federation on the BEA WebLogic Server” in the *HP Select Federation Installation Guide*.
- For instructions on enabling logging for WebSphere, see “Deploying Select Federation on the IBM WebSphere 6.0.2 Server” in the *HP Select Federation Installation Guide*.



# 3 Integrating the Select Federation Sun Access Manager Connector with an IDP Site

This chapter provides instructions for integrating and configuring the Select Federation Sun Access Manager connector with an IDP-only mode installation of Select Federation (SF-IDP). The instructions assume knowledge of Sun Access Manager terminology and configuration setup. For more details on how to configure the authentication scheme or configure resources to be protected, see the Sun Access Manager documentation.

It is important to configure and set appropriate protection for the Select Federation resources in Sun Access Manager.

## Requirements

The following requirements must be met before integrating the Sun Access Manager connector with an SF-IDP:

- HP Select Federation 7.00 + Patch 7.01 is installed
- Sun Access Manager 7.1 is installed
- Sun Access Manager connector is deployed

## Integration Mechanisms for an SF-IDP

Integrating the Select Federation Sun Access Manager connector with an IDP site requires that you configure Sun Access Manager and Select Federation. When you integrate the Select Federation Sun Access Manager connector with an IDP site, the Select Federation Administration console, Privacy Manager and Demonstration application (`sf-demo`) are also integrated with Sun Access Manager.

There are two integration mechanisms possible for the IDP site:

- Login URL — Use the Login URL, which can be used to point to a resource protected by any Sun Access Manager Agent, which allows that agent to perform the authentication. This gives you the flexibility to use any authentication scheme offered by the Sun Access Manager Agent. See [Using a Login URL](#) on page 18 for details.
- Select Federation Agent — Use the Select Federation Agent when password validation is enough for authenticating users. The Sun Access Manager client SDK is used to perform authentication and authorization. See [Using the Select Federation Agent](#) on page 18 for more information.

## Using a Login URL

When you use the Login URL mechanism, the Sun Access Manager IDP connector redirects the login request to the resource to which the Login URL is pointing. This resource is protected by the Sun Access Manager Agents that perform the authentication and authorization. The resource then redirects the request to the original resource that the user was trying to access. At this point, when the Sun Access Manager IDP connector receives the request, it has a valid Sun Access Manager SSO cookie. The connector validates the cookie. If the cookie is valid, the user is then shown the page that the user was trying to access.

You can use the `com.ipplanet.am.authurl` login parameter in the `$SF_HOME/conf/tfsconfig.properties` file to set the Login URL to be used for authentication. The value for this parameter is a resource that exists on the Web Server or Application Server. This resource must be protected by Sun Access Manager agents. Based on the deployment requirements, Sun Access Manager administrators can do the following:

- Configure the authentication mechanism for this resource.
- Give access permission to this resource based on the users who are allowed to federate.

For more details on how to configure resources to be protected by Sun Access Manager agents, see the Sun Access Manager documentation.

The resource being protected by Sun Access Manager Agents must be able to do the following:

- Read the value of a parameter named "E" and if the value is set to 1 then inform the user that an error has occurred.
- Read the value of a parameter named "RURL" and redirect the user to the parameter.

For example, a `sample-login.asp` protected by Sun Access Manager Agents can be as simple as the following code:

```
<%
Dim returnURL, error
returnURL = Request("RURL")
error = Request("E")

If (error = "1") Then
    Response.Write "ERROR: Check Select Federation logs."
    Response.End
End If

If (returnURL = "") Then
    Response.Write "ERROR: No RURL found."
Else
    Response.Status="302"
    Response.AddHeader "Location", returnURL End If %>
```

## Using the Select Federation Agent

When you use the Select Federation Agent, the authentication mechanism is limited to password validation. This mechanism uses the Sun Access Manager Client SDK for authentication.

# Configuring Sun Access Manager for the IDP Integration

Complete the following main steps to integrate the Sun Access Manager connector with an SF-IDP (see each step for instructions):

- [Step 1: Prepare the Environment for Federated Applications](#)

For ease of integration into your existing environment, Select Federation provides a special Application Helper component. You can use the Application Helper to generate the URLs for federated applications and then place them at meaningful locations such as Enterprise Portals for users to access.

If you do not have your existing environment set up for a federation yet, you can set up a dummy environment as described in Step 5: (Optionally) Test the Sun Access Manager Integration with the Demonstration Application on page 37, and then complete the following steps.

- [Step 2: Configure Sun Access Manager](#)

This step integrates the SF-IDP with Sun Access Manager for authentication. It also authenticates users to access any Select Federation applications (such as the Administration console and Privacy Manager). You need to set policies for these applications to configure users who are authorized to access them.

- [Step 3: Configure the SF-IDP for the Sun Access Manager Integration](#)

This step enables the Sun Access Manager connector with the SF-IDP.

- [Step 4: Configure Profile Attributes for Federated Users](#)

SF-IDP installations provide user attributes contained in a data source to application partners. You need to configure Select Federation to use your data source to populate user attributes for outgoing federated users.

- [Step 5: \(Optionally\) Test the Sun Access Manager Connector Integration with the Demonstration Application](#)

You can use the Select Federation Demonstration application to test your integration.

## Step 1: Prepare the Environment for Federated Applications

The Application Helper is a unique feature of Select Federation that simplifies the way in which you initiate federation actions such as federated login and global logout. Using the Application Helper, you enter a “target URL” that you would like your users to go to after a federated login. The Application Helper will return a transformed URL that you can paste into your portal for your users to click on. When the users click on this transformed URL, they will arrive seamlessly at the target URL using their Sun Access Manager credentials.

To use the Application Helper to generate URLs to federated applications, perform the following steps:

- 1 Navigate to the Select Federation Administration console landing page.

The landing page is usually deployed at:

```
http://<base-url>/tfs-internal
```

or

```
https://<base-url>/tfs-internal
```

<base-url> is the root of the application server on which you have deployed Select Federation. Replace <base-url> with your hostname:port.

The landing page opens as shown in the following figure:

The screenshot shows the 'Select Federation Administration Console' landing page. It features a dark blue header with the title. Below the header, there are two main columns: 'Administration and Configuration Tasks' and 'Learn about the Product'. The 'Administration and Configuration Tasks' column contains two bullet points: 'Administration Console' and 'Application Helper'. The 'Learn about the Product' column contains four bullet points: 'Release Notes', 'Installation Instructions', 'Administration Guide', and 'Architectural Overview'. At the bottom, there is a 'Contact HP' section with a link to the HP website and a Java logo.

- 2 Click the **Application Helper** link.

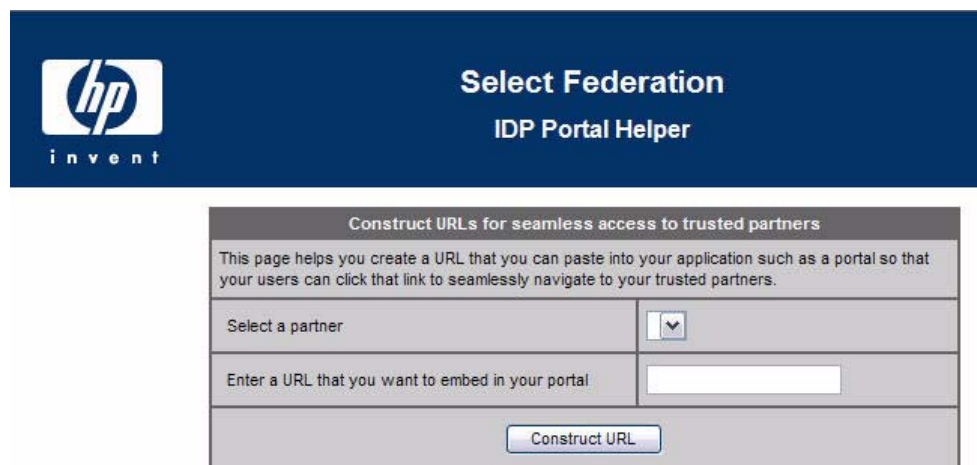
The Federation Application Helper page opens:

The screenshot shows the 'Select Federation Federation Application Helper' page. It features a dark blue header with the HP logo and the title. Below the header, there is a table with two rows. The first row describes the URL for Authority Sites, SAML Producers, or Liberty Identity Providers, linking to 'idphelper.jsp'. The second row describes the URL for Application Sites, SAML Consumers, or Liberty Service Providers, linking to 'sphelper.jsp'.

The pages below help you create URLs that you can embed into your applications	
If your site is an Authority Site, SAML Producer or Liberty Identity Provider, you can obtain the appropriate URLs by visiting this page:	<a href="#">idphelper.jsp</a>
If your site is an Application Site, SAML Consumer or Liberty Service Provider, you can obtain the appropriate URLs by visiting this page:	<a href="#">sphelper.jsp</a>

- 3 Select **idphelper.jsp**.

The IDP Portal Helper page opens.



- 4 Select a partner in the list and enter the target URL that you want your users to go to after a federated logon.

➤ If the partners list is empty, you need to first exchange metadata with your trusted partners and add your partners through the Select Federation Administration console. Then the partners list on this page will be populated with the partners you added.

Following is an example of a partner and URL:

**Partner:** HealthCare

**URL:** <https://www.healthcare.com/myBenefitsApp>

- 5 Click **Construct URL**.

A transformed URL is returned that you can paste into your portal for your users to click on. By clicking this URL, a user can arrive seamlessly at the target URL by using their domain-local credentials.

## Step 2: Configure Sun Access Manager

You need to configure Sun Access Manager to perform authentication for the SF-IDP integration, using either of the following integration mechanisms:

- **Login URL:** If you choose this integration mechanism, you can configure your resource to be protected by any authentication scheme. Make sure that you set the same value for `cookieDomain` for the Sun Access Manager Agent and in the `$SF_HOME/conf/tfsconfig.properties` file. This is so that both the Sun Access Manager Agent and Select Federation can read the cookies.
- **Select Federation Agent:** If you choose this integration mechanism, only password authentication is supported.

For more details on using Sun Access Manager, see the Sun Access Manager documentation. It is assumed that you have the Sun Access Manager installed and running. It is also assumed that you are familiar with Sun Access Manager configuration,

Complete the following basic tasks to configure Sun Access Manager for the IDP side integration. These tasks are the same for both Login URL and Select Federation Agent integration mechanisms. You need to perform the configuration in your Sun Access Manager install.

- Task 1: Create and configure Policies.
- Task 2: Create a Rule for the Select Federation Privacy Manager.
- Task 3: Create a Rule for the Select Federation Administration console.
- Task 4: Create a Rule for the Select Federation IDPAuthnPlugin.
- Task 5: Create a Rule for the HP AM Integrator.
- Task 6: Create a Rule for the Demonstration application, SF-Demo.
- Task 7: Configure Subjects for the policy.

**Task 1:** Create and configure Policies.

- 1 Open the Sun Java System Access Manager console.
- 2 Select **Access Control** → **Realm**.
- 3 Select the default **Realm**.
- 4 Click on **Policies**.

The New Policy page opens.

VERSION User: amAdmin Server: pukiIDC LOG OUT HELP  
Sun Java™ System Access Manager  
Access Control > Realm - selected > New Policy  
New Policy OK Cancel  
General Subjects Response Providers  
Rules Conditions \* Indicates required field  
General  
\* Name: SF Policy  
Description: Policy used for HP Select Federation integration  
Active:  Yes  
Back to top

- 5 Fill in the necessary information, including the following required information, then click **OK**:
  - **Name:** Enter the new policy name, such as **SF Policy**.
  - **Description:** Describe the policy.

The Policy page opens.

**Task 2:** Create a Rule for the Select Federation Privacy Manager.

- 1 Select the **Policy** that you just created (such as **SF Policy**).  
The Edit Policy page for this policy opens.
- 2 Click **New** under the **Rules** subsection.

The Step 1 of 2: Select Service Type for the Rule page opens.

VERSION | LOG OUT | HELP  
User: amAdmin Server: pulkitDC  
Sun Java™ System Access Manager  
Sun™ Microsystems, Inc.  
Access Control > Realm - selected > Policy - SF Policy > New Rule

**Step 1 of 2: Select Service Type for the Rule** [Back] [Next] [Cancel]

\* Service Type:  Discovery Service (with resource name)  
 Liberty Personal Profile Service (with resource name)  
 URL Policy Agent (with resource name)

\* Indicates required field

- 3 Select **URL Policy Agent** as the service type and click **Next**.

The Step 2 of 2: New Rule page opens.

Access Control > Realm - selected > Policy - SF Policy > New Rule

**Step 2 of 2: New Rule** [Back] [Finish] [Cancel]

\* Service Type: URL Policy Agent  
\* Name: Protect PM  
\* Resource Name: /\*/\*pm\*

Actions  
\* One or more actions are required.

Action	Value
<input checked="" type="checkbox"/> GET	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
<input checked="" type="checkbox"/> POST	<input checked="" type="radio"/> Allow <input type="radio"/> Deny

\* Indicates required field

- 4 Fill in the necessary information, including the following required information, then click **Finish**:

- **Name:** Enter **Protect PM**
- **Resource Name:** Enter **\*/pm\***
- Under **Actions:** Select **Get** and **Post**  
Be sure the **Value** for both is **Allow**.

The Edit Policy page opens.

**Task 3:** [Create a Rule for the Select Federation Administration console.](#)

- 1 Click **New** under the **Rules** subsection.

The Step 1 of 2: Select Service Type for the Rule page opens.

- 2 Select **URL Policy Agent** as the service type and click **Next**.

The Step 2 of 2: New Rule page opens.

- 3 Fill in the necessary information, including the following required information, then click **Finish**:

- **Name:** Enter **Protect Admin Console**
- **Resource Name:** Enter **\*/tfs-internal/admin/\***

- Under **Actions**: Select **Get** and **Post**  
Be sure the **Value** for both is **Allow**.  
The Edit Policy page opens.

**Task 4:** Create a Rule for the Select Federation IDPAuthnPlugin.

- 1 Click **New** under the **Rules** subsection.  
The Step 1 of 2: Select Service Type for the Rule page opens.
- 2 Select **URL Policy Agent** as the service type and click **Next**.  
The Step 2 of 2: New Rule page opens.
- 3 Fill in the necessary information, including the following required information, then click **Finish**:
  - **Name**: Enter **Protection rule for IDPAuthnPlugin**
  - **Resource Name**: Enter **\*/select-federation\***
  - Under **Actions**: Select **Get** and **Post**  
Be sure the **Value** for both is **Allow**.  
The Edit Policy page opens.

**Task 5:** Create a Rule for the HP AM Integrator.

- 1 Click **New** under the **Rules** subsection.  
The Step 1 of 2: Select Service Type for the Rule page opens.
- 2 Select **URL Policy Agent** as the service type and click **Next**.  
The Step 2 of 2: New Rule page opens.
- 3 Fill in the necessary information, including the following required information, then click **Finish**:
  - **Name**: Enter **Protection rule for HP AM Integrator**
  - **Resource Name**: Enter **\*/hpamintegrator/protected/\***
  - Under **Actions**: Select **Get** and **Post**  
Be sure the **Value** for both is **Allow**.  
The Edit Policy page opens.

**Task 6:** Create a Rule for the Demonstration application, SF-Demo.

- 1 Click **New** under the **Rules** subsection.  
The Step 1 of 2: Select Service Type for the Rule page opens.
- 2 Select **URL Policy Agent** as the service type and click **Next**.  
The Step 2 of 2: New Rule page opens.
- 3 Fill in the necessary information, including the following required information, then click **Finish**:
  - **Name**: Enter **Protection rule for SF-Demo**
  - **Resource Name**: Enter **\*/sf-demo/protected/\***
  - Under **Actions**: Select **Get** and **Post**



Be sure the **Value** for both is **Allow**.

The Edit Policy page opens.

- 4 Click **Save** to save your rule settings.

#### Task 7: Configure Subjects for the policy.

- 1 Click **New** under the **Subjects** subsection.

The Step 1 of 2: Select Subject Type opens.

- 2 Select **Access Manager Identity Subject** as the subject type and click **Next**.

The Step 2 of 2: New Subject - Access Manager Identity Subject page opens.

Access Control > Realm - selected > Policy - SF Policy > New Subject

Step 2 of 2: New Subject - Access Manager Identity Subject

Back Finish Cancel

\* Indicates required field

\* Name: Users for HP Select Federation integration

Exclusive:

Filter: -- Select Identity Type -- \* Search

Available: amAdmin, anonymous, foo bar, goo, john doe

Selected:

Add > Add All >> < Remove << Remove All

- 3 Fill in the necessary information, including the following required information, then click **Finish**:
  - **Name:** Enter **Users for HP Select Federation integration**
  - **Filter:** Click **Search** to display all available users in the **Available** list.
  - **Selected:** Add users you want to be authorized, from the **Available** list to the **Selected** list.

The Edit Policy page opens.

- 4 Click **Save** to save your settings.

### Step 3: Configure the SF-IDP for the Sun Access Manager Integration

Perform the following steps to configure the `$SF_HOME/conf/tfsconfig.properties` file for the Sun Access Manager integration with the IDP site:

- 1 Comment out the following line, if it is not already commented out:

```
idpAuthnPlugin=com.trustgenix.tfsIDP.util.IDPAuthnPlugin_Dir
```

- 2 Add the following required lines:

```
idpAuthnPlugin=myAuthPlugin
myAuthPlugin.class=com.hp.selectfederation.sam.SAMAuthnPlugin
myAuthPlugin.jar=$SF_HOME/connectors/sam/SAMConnector.jar
amPlugin=myAdminPlugin
myAdminPlugin.jar=$SF_HOME/connectors/sam/SAMConnector.jar
myAdminPlugin.class=com.hp.selectfederation.sam.SAMAmPlugin
```

- 3 Make the following substitution in these lines:

`$SF_HOME` = Your IDP Select Federation install directory.

For example: `c:/test-area/idp/inst7501`

- 4 Add and configure required and optional Sun Access Manager parameters that do not have default values in the `tfscnfig.properties` file. Or, the default values do not match your installation.

▶ If the Sun Access Manager server is SSL-enabled, then you must install the Sun Access Manager server's certificate in the Select Federation application server's trust store.

All parameters with default values are required. You only need to add them if you want to change the default value. Also, some parameters without default values are required.

The following table lists and describes the Sun Access Manager parameters for an IDP integration:

**Table 1 Select Federation Sun Access Manager Connector Parameters**

<b>Parameter Name</b>	<b>Parameter Value</b>	<b>Description</b>	<b>Example</b>	<b>Required/Optional (default value)</b>
<code>com.ipplanet.am.naming.url</code>	Naming URL for Sun Access Manager install	The value of this property represents the URL where the Client SDK would retrieve the URLs of Access Manager internal services. This is the URI for the Naming Service.	<code>http://sam.vm.net:9919/amserver/namingsevice</code>	Required (None)
<code>com.ipplanet.am.defaultOrg</code>	Value is set at Sun Access Manager installation for <code>defaultOrg</code> .	Specifies the top-level realm or organization in the Access Manager information tree. The value for this parameter is in the Sun Access Manager install <code>AMConfig.properties</code> file.	<code>dc=vm,dc=net</code>	Required (None)
<code>com.ipplanet.am.server.protocol</code>	Protocol	Server protocol to be used by Authentication Service. The value for this parameter is in the Sun Access Manager install <code>AMConfig.properties</code> file.	<code>http</code>	Required (http)

**Table 1 Select Federation Sun Access Manager Connector Parameters**

<b>Parameter Name</b>	<b>Parameter Value</b>	<b>Description</b>	<b>Example</b>	<b>Required/Optional (default value)</b>
com.iplanet.am.server.host	HostName	Server host to be used by the Authentication Service. The value for this parameter is in the Sun Access Manager install AMConfig.properties file.	myDC.vm.net	Required (None)
com.iplanet.am.server.port	Port Number	Server port to be used by the Authentication Service. The value for this parameter is in the Sun Access Manager install AMConfig.properties file.	9919	Required 80
com.iplanet.am.service.secret	Encryption Key	Contains the encrypted value of the password. The value for this parameter is in the Sun Access Manager install AMConfig.properties file.	AQIC2PJavDlo7/D+jyCpjE2qcmadltFqcqHw	Required (None)
com.iplanet.am.authurl	URL protected by a Sun Access Manager Agent	Value for this parameter is the URL protected by a Sun Access Manager Agent. This page must be able to redirect the user back to the originally requested URL. The originally requested URL is appended as a parameter called "RURL". This parameter must be set if you are using the Login URL integration mechanism.	http://idp.vm.net:82/test/samplelogin.jsp	Optional (None)
com.sun.identity.agents.notification.url	Notification URL	Defines the notification URL for a remote policy API.	http://myDC.vm.net:9919/amserver/notification/service	Required (None)

**Table 1 Select Federation Sun Access Manager Connector Parameters**

<b>Parameter Name</b>	<b>Parameter Value</b>	<b>Description</b>	<b>Example</b>	<b>Required/Optional (default value)</b>
<code>com.sun.identity.agents.polling.interval</code>	Integer value specifying number of minutes	Specifies the polling interval, which is the number of minutes after which an entry is dropped from the Client API's cache.	4	Optional (3)
<code>com.iplanet.cookieDomain</code>	Cookie Domain	Cookie Domain for Sun Access Manager SSO Cookie. When you use the LoginURL integration mechanism, make sure that the cookie domain configuration for the Sun Access Manager Agents allows cookies to be received by the Select Federation IDP.	<code>.vm.net</code>	Optional (None)
<code>authzResource</code>	Resource URL	Select Federation Agent URL used for IDP authentication.	<code>/select-federation</code>	Required (/select-federation)

**Table 1 Select Federation Sun Access Manager Connector Parameters**

Parameter Name	Parameter Value	Description	Example	Required/Optional (default value)
com.iplanet.am.cookie.name	Cookie Name	Cookie name used by the Authentication Service to set the valid session handler ID. The value of this cookie name is used to retrieve the valid session information. The value for this parameter is in the Sun Access Manager install AMConfig.properties file.	iPlanetDirectoryPro	Optional (iPlanetDirectoryPro)
com.sun.identity.agents.app.username	Admin user name	Specifies the user name to use with read access for the Sun Access Manager configuration.	amAdmin	Required (amAdmin)
com.iplanet.am.service.password	Admin password	Encrypted password for the Admin user (user name you use to log into the Sun Access Manager Admin console). To encrypt the password, use the ConfigPasswordMask.sh/bat utility tool shipped with Select Federation. For details on how to run this tool, see the “Security” section of the <i>HP Select Federation Installation Guide</i> .	{Mask}OTI7ND0/My4=	Required

## Step 4: Configure Profile Attributes for Federated Users

Configure the Select Federation Directory Plugin settings in the `tfconfig.properties` file to get user attribute information, as follows:

- 1 Set the `ldapURL`, `ldapPrincipal`, and `ldapPassword` properties to point to the User Directory Server that your Sun Access Manager install is configured against.

For example:

```
ldapURL=ldap://idp.company.net:400
ldapPrincipal=cn=Directory Manager
ldapPassword=password
```

- 2 Make sure you comment out the following:
  - `ldapUserBaseDN` and `ldapUserAttr`
  - Any older `dirplugin` parameter

## Step 5: (Optionally) Test the Sun Access Manager Connector Integration with the Demonstration Application

As a convenience, a Demonstration application is provided with Select Federation that you can use to test your integration. It is meant to emulate a portal page with a list of all the federated applications that are accessible to Sun Access Manager users. It is not meant for production use and should only be used for sanity-testing the connector integration.

The Demonstration application can be integrated with Sun Access Manager using either the Login URL or the Select Federation Agent integration mechanism. This depends on the configuration options that you have chosen for your integration.

To use the Demonstration application, complete the following tasks.

### Task 1: Set up an environment for the Demonstration application.

Following is a bare-minimum setup for the purposes of testing with the Demonstration application:

- 1 Set up different machines with different site roles:
  - One Select Federation install with the IDP role (which is integrated with Sun Access Manager): SF-IDP
  - One Select Federation install with the SP role: SF-SP.
- 2 Exchange metadata between the following sites: SF-IDP with SF-SP.

If you are not familiar with setting up site roles or exchanging metadata, see the *HP Select Federation Administration and Configuration Guide* for detailed instructions.

### Task 2: Run the Demonstration application.

To test the SF-IDP with the SF-SP, perform the following steps:

- 1 Navigate to the Demonstration application using the following URL:  
`http(s)://<sf-idp-url>:<port>/sf-demo`  
The Demonstration application landing page opens.
- 2 Select **Login locally to demo IDP application**.  
The Login authentication page opens. This page is integrated with Sun Access Manager.
- 3 Enter your Sun Access Manager credentials.  
The IDP Demonstration page opens.
- 4 Select an available link to the configured SF-SP.

## 4 Integrating the Select Federation Sun Access Manager Connector with an SP Site

This chapter provides instructions for integrating and configuring the Select Federation Sun Access Manager connector with an SP-only mode installation of Select Federation (SF-SP). The instructions assume knowledge of Sun Access Manager terminology and configuration setup. For more details on how to configure the authentication scheme or configure resources to be protected, see the Sun Access Manager documentation.



All information in this chapter also applies to an SP + IDP installation of Select Federation.

It is important to configure and set appropriate protection for the Select Federation resources in Sun Access Manager.

### Requirements

The following requirements must be met before integrating the Sun Access Manager connector with an SF-SP:

- HP Select Federation 7.00 + Patch 7.01 is installed
- Sun Access Manager 7.1 is installed
- Sun Access Manager connector is deployed

### Integration Mechanisms for an SF-SP

Integrating the Select Federation Sun Access Manager connector with a SP site requires that you configure Sun Access Manager and Select Federation. When you integrate the Select Federation Sun Access Manager connector with a SP site, the Select Federation Administration console, Privacy Manager and Demonstration application (sf-demo) are also integrated with Sun Access Manager.

There are two mechanisms to integrate the Administration console, Privacy Manager and demo application (sf-demo) for the SP site:

- Login URL — Use the Login URL, which can be used to point to a resource protected by any Sun Access Manager Agent, which allows that agent to perform the authentication. This gives you the flexibility to use any authentication scheme offered by the Sun Access Manager Agent. See [Using a Login URL](#) on page 32 for details.
- Select Federation Agent — Use the Select Federation Agent when password validation is enough for authenticating users. The Sun Access Manager client SDK is used to perform authentication and authorization. See [Using the Select Federation Agent](#) on page 32 for more information.

## Using a Login URL

When you use the Login URL mechanism, the Sun Access Manager IDP connector redirects the login request to the resource to which the Login URL is pointing. This resource is protected by the Sun Access Manager Agents that perform the authentication and authorization. The resource then redirects the request to the original resource that the user was trying to access. At this point, when the Sun Access Manager IDP connector receives the request, it has a valid Sun Access Manager SSO cookie. The connector validates the cookie. If the cookie is valid, the user is then shown the page that the user was trying to access.

You can use the `com.iplanet.am.authurl` login parameter in the `$$SF_HOME/conf/tfsconfig.properties` file to set the login URL to be used for authentication. The value for this parameter is a resource that exists on the Web Server or Application Server. This resource must be protected by Sun Access Manager agents. Based on the deployment requirements, Sun Access Manager administrators can do the following:

- Configure the authentication mechanism for this resource.
- Give access permission to this resource based on the users who are allowed to federate.

For more details on how to configure resources to be protected by Sun Access Manager agents, see the Sun Access Manager documentation.

The resource being protected by Sun Access Manager Agents must be able to do the following:

- Read the value of a parameter named "E" and if the value is set to 1 then inform the user that an error has occurred.
- Read the value of a parameter named "RURL" and redirect the user to the parameter.

For example, a `sample-login.asp` protected by Sun Access Manager Agents can be as simple as the following code:

```
<%
Dim returnUrl, error
returnUrl = Request("RURL")
error = Request("E")

If (error = "1") Then
    Response.Write "ERROR: Check Select Federation logs."
    Response.End
End If

If (returnUrl = "") Then
    Response.Write "ERROR: No RURL found."
Else
    Response.Status="302"
    Response.AddHeader "Location", returnUrl End If %>
```

## Using the Select Federation Agent

When you use the Select Federation Agent, the authentication mechanism is limited to password validation. This mechanism uses the Sun Access Manager Client SDK for authentication.



# Configuring Sun Access Manager for the SP Integration

Complete the following main steps to integrate the Sun Access Manager connector with an SF-SP (see each step for instructions):

- [Step 1: Determine a User Activation Scheme](#)  
Select the User Activation scheme and plug it into the SF-SP so that it runs before the Sun Access Manager connector runs.
- [Step 2: \(Optionally\) Set User Profile Attributes as a Cookie](#)  
Configure the incoming user profile information from an Authority (IDP) partner to be set as a profile cookie.
- [Step 3: Configure Sun Access Manager](#)  
This step integrates the SF-SP with Sun Access Manager. It also authenticates users to access any Select Federation applications (such as the Administration console, Privacy Manager and Demonstration application `sf-demo`). You need to set policies for these applications to configure users who are authorized to access them.
- [Step 4: Configure the SF-SP for the Sun Access Manager Integration](#)  
This step enables the Sun Access Manager connector with the SF-SP.
- [Step 5: \(Optionally\) Test the Sun Access Manager Connector Integration with the Demonstration Application](#)  
You can use the Select Federation Demonstration application to test your integration.

## Step 1: Determine a User Activation Scheme

On the SP side when a new user arrives, you need to configure an Activation Event Plugin to activate the new user. The Select Federation Sun Access Manager connector assumes that the user is activated and the `localUserId` of the user is set when the control reaches the Select Federation Sun Access Manager connector in the processing logic. Based on your mapping requirements, there are different ways to configure Select Federation to set up a unique identity mapping between incoming federated users and the users in your Sun Access Manager environment. See the “Event Plugins” chapter in the *HP Select Federation Configuration and Administration Guide* for more information.

## Configuring Select Federation

You need to configure Select Federation in your SP's `$SF_HOME\conf\tfsconfig.properties` file to set up a unique identity mapping between incoming federated users and the users in your Sun Access Manager environment.

To configure Select Federation, perform the following steps to edit the `tfsconfig.properties` file:

- 1 Make a backup copy of the `tfsconfig.properties` file before editing it.
- 2 Edit the `tfsconfig.properties` file according to the Activation Event Plugin for your deployment.

As an example, see the following section, [Using the Activate URL Plugin for the User Activation Scheme](#) on page 34, which demonstrates how to use one of the event plugins from the “Event Plugins” chapter in the *HP Select Federation Configuration and Administration Guide*.

- 3 Restart the application server.

## Using the Activate URL Plugin for the User Activation Scheme

These instructions are only for the Activate URL Event Plugin. You should replace this event plugin with one that meets your deployment requirements.

A demo activation page, `activate-demo.jsp`, has been bundled for testing purposes. This page exists in the Demonstration application (`sf-demo`), which is bundled with Select Federation. The demo activation page shows how an activation page fulfills its responsibilities by mapping the user's identity. Do not use `activate-demo.jsp` in your deployments. This is for demo purposes only. Replace the activation plugin with your deployment-specific activation plugin.

The following example configuration assumes that the User Activation Scheme is sufficient for your needs. In this case, the user is successfully mapped if an attribute from the incoming federated user's profile can be used to locate a unique user in the directory server. This configuration uses the Activate URL Event Plugin which is shipped with the product. For more details, see the “Event Plugins” chapter in the *HP Select Federation Configuration and Administration Guide*.

```
#####  
### SAMPLE CONFIGURATION  
#####  
##  
spEventPlugin=myActivatePlugin  
##  
myActivatePlugin.class=com.trustgenix.tfsSP.util.SPEventPlugin_ActivateURL  
SPEventPlugin_ActivateURL.spActivateURL=http://sp.vm.net:2001/sf-demo/  
activate-demo.jsp  
##  
  
#Dir plugin configuration below should point to the Directory Server that  
# your Sun Access Manager is configured against  
  
dirPlugin=com.trustgenix.tfsIDP.util.DirPlugin_LDAP  
ldapURL=<ldap|ldaps>://<sun-am-machine>:<sun-am-port>  
ldapPrincipal=cn=Directory Manager  
ldapPassword=password  
ldapUserBaseDN=dc=domain,dc=com  
ldapUserAttr=uid  
ldapSearchSubtree=1
```

## Step 2: (Optionally) Set User Profile Attributes as a Cookie

(On the SP side integration, any incoming user profile information for a federated user from an Authority (IDP) partner can be set as a profile cookie.

Perform the following steps to set the user profile attributes and to set `tfssessionld` as a cookie in the `$SF_HOME/conf/tfsconfig.properties` file:

- 1 Add the following lines:

Add the Profile Attribute Event Plugin to the SP Event Plugin chain:

```

spEventPlugin=<activation_event_plugin> profileCookieEP
profileCookieEP.class=
com.trustgenix.tfsSP.util.SPEventPlugin_ProfileCookie

```

- Optionally, add and configure the optional parameters in the following table that do not have default values.

For parameters with default values, you only need to add them if you want to change the default value.

Parameter Name	Description	Example	Required/ Optional (default value)
ProfileCookieEP.cookieDomain	Cookie Domain	Domain.com	Optional (None)
ProfileCookieEP.cookieName	Profile Cookie Name	HPSFProfileAttrCookie	Optional (HPSFProfileAttrCookie)
ProfileCookieEP.cookiePath	Profile Cookie Path	/	Optional (/)
ProfileCookieEP.tfsSessionIdStrName	Attribute Name within the Cookie which will contain the tfsSessionId.	hpSFSessionId	Optional (hpSFSessionId)
ProfileCookieEP.setUserInfoFromIDP	Determines if all information about the user from the IDP is to be set in the cookie. Value=1 sets all user information in the cookie.	1	Optional (0)

### Step 3: Configure Sun Access Manager

You need to configure Sun Access Manager to perform authentication for the SF-SP integration. You can integrate your Select Federation Administration console, Privacy Manager and Demonstration application (sf-demo) using either of the following integration mechanisms:

- Login URL:** If you choose this integration mechanism, you can configure your resource to be protected by any authentication scheme. Make sure that you set the same value for `cookieDomain` for the Sun Access Manager Agent and in the `$SF_HOME/conf/tfsconfig.properties` file. This is so that both the Sun Access Manager Agent and Select Federation can read the cookies.
- Select Federation Agent:** If you choose this integration mechanism, only password authentication is supported.

For more details on using Sun Access Manager, see the Sun Access Manager documentation. It is assumed that you have the Sun Access Manager installed and running. It is also assumed that you are familiar with Sun Access Manager configuration,

Complete the following basic tasks to configure Sun Access Manager for the SP side integration. These tasks are the same for both Login URL and Select Federation Agent integration mechanisms. You need to perform the configuration in your Sun Access Manager install.

- [Task 1: Deploy the Custom Authentication Module on Sun Access Manager](#)
- [Task 2: Configure the Custom Authentication Module on Sun Access Manager](#)
- [Task 3: Create and configure Policies.](#)
- [Task 4: Create a Rule for the Select Federation Privacy Manager.](#)
- [Task 5: Create a Rule for the Select Federation Administration console.](#)
- [Task 6: Create a Rule for the Select Federation AuthnPlugin.](#)
- [Task 7: Create a Rule for the HP AM Integrator.](#)
- [Task 8: Create a Rule for the Demonstration application, SF-Demo.](#)
- [Task 9: Configure Subjects for the policy.](#)

#### Task 1: [Deploy the Custom Authentication Module on Sun Access Manager](#)

Deploying the Custom Authentication module, requires that you copy files shown in the following steps from the Select Federation 7.01 Patch location (`$SF_PATCH`) to the specified locations. Following are sample locations for a Sun Access Manager install on a Windows platform. Notice that the `$WEB_SERVER_BASE` location is inside the Sun Access Manager install location (`$SAM_HOME`).

```
Sample $SAM_HOME=C:\Program Files\Sun\JavaES5\  
Sample $WEB_SERVER_BASE= C:\Program Files\Sun\JavaES5\WebServer7\  
Sample $HOST=enterprise.domain.com
```

Perform the following steps to deploy the Custom Authentication module:

- 1 Copy the `$SF_PATCH/connectors/sam/SFAMLoginModule.xml` file to the `$WEB_SERVER_BASE/https-$HOST/web-app/$HOST/amserver/config/auth/default/` directory.
- 2 Copy the `$SF_PATCH/connectors/sam/SFSAMAuthnModule.jar` file to the `$WEB_SERVER_BASE/https-$HOST/web-app/$HOST/amserver/WEB-INF/lib/` directory.
- 3 Update the `$WEB_SERVER_BASE/https-$HOST/config/server.xml` file by adding the location of the `SFSAMAuthnModule.jar` file to the `<server-class-path>` node.
- 4 Restart the Web Server.

#### Task 2: [Configure the Custom Authentication Module on Sun Access Manager](#)

For the Select Federation SP integration, a Custom Authentication module needs to be configured in the Sun Access Manager. The Select Federation Custom Authentication module must be active and only require a valid user id in the directory service. Once the user is found in the directory service, the login module creates a valid SSO token.

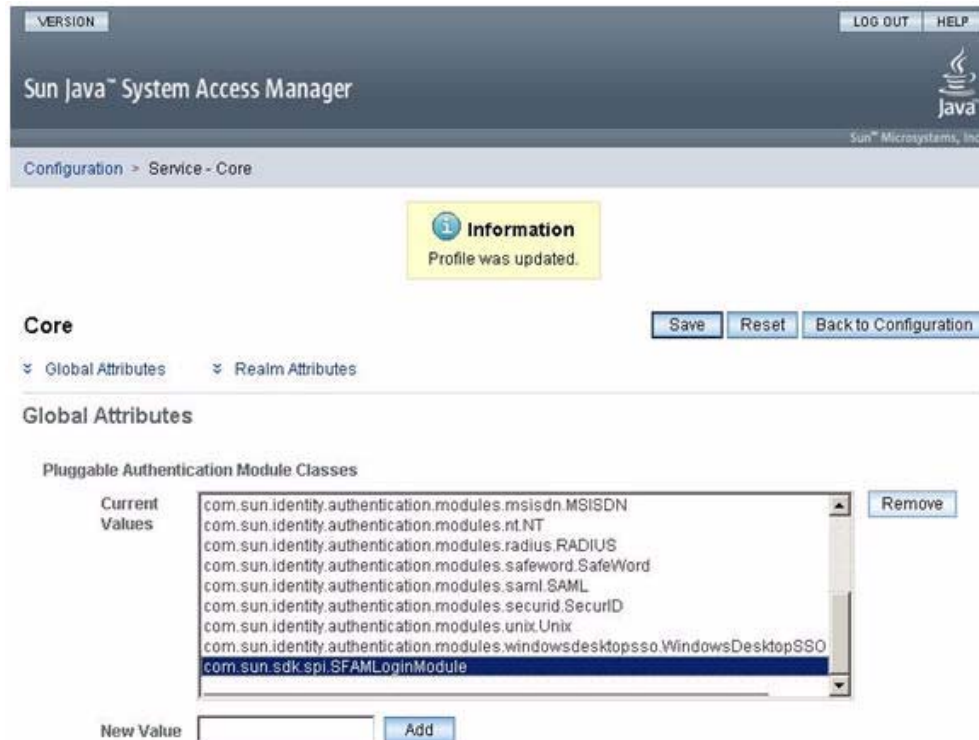
Perform the following steps to configure the Custom Authentication module:

- 1 Log on to the Access Manager Console as **amAdmin**, using the following URL:  
**`http(s)://host:port/amserver/UI/Login`**

- Click the **Configuration** tab.  
The Configuration page opens.



- Under the Authentication panel, click the **Core** service.  
The Core page opens.
- In the **New Value** field, enter **com.sun.sdk.spi.SFAMLoginModule** and click **Add**.  
The **com.sun.sdk.spi.SFAMLoginModule** value appears in the Current Values list.

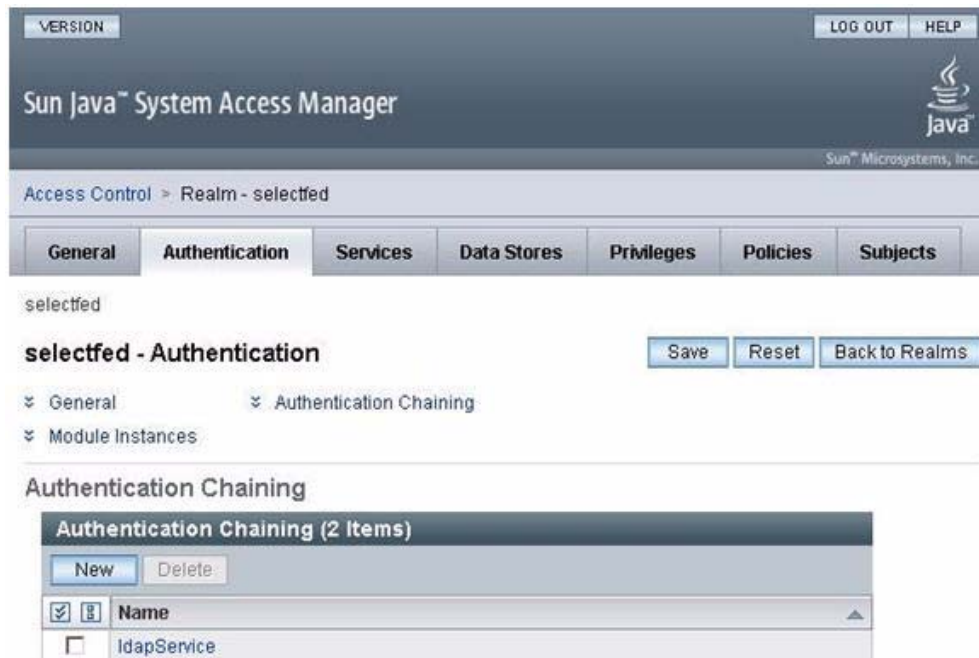


- Click **Save**.

- 6 Click the **Back to Configuration** button.
  - 7 Click the **Access Control** tab.
- The Access Control Realms page opens.



- 8 Select the **Realm** that will use the custom authentication module. For example, click on **selected**.
  - 9 Click the **Authentication** tab.
- The Authentication page opens.



- 10 Under the **Authentication Chaining** panel, click the **New** button.
  - 11 Enter a Core service name in the **Name** field and click **OK**.
- For example: **federationService**

The Properties page opens for the service name you specified.

VERSION LOG OUT HELP  
User: amAdmin Server: pulkitDC  
Sun Java™ System Access Manager  
Sun™ Microsystems, Inc.  
Access Control > Realm - selected > Authentication Chain - federationService

**Information**  
The authentication chain properties were updated.

**federationService - Properties** Save Reset Back to Authentication

(1 Items)

Add Remove Reorder

<input checked="" type="checkbox"/>	Instance	Criteria	Options
<input type="checkbox"/>	SFAMLoginModule	REQUIRED	

- 12 Click the **Add** button.
- 13 Select **SFAMLoginModule** from the **Instance** drop-downlist.
- 14 Select **REQUIRED** from the **Criteria** drop-down list.
- 15 Click **Save** then the **Back to Authentication** button.
- 16 Click **Save**.

The Authentication page opens with the new, configured Core service, **federationService**, added.

### Task 3: Create and configure Policies.

- 1 Open the Sun Java System Access Manager console.
- 2 Select **Access Control** → **Realm**.
- 3 Select the default **Realm**.
- 4 Click on **Policies**.

The New Policy page opens.

VERSION User: amAdmin Server: pulkitDC LOG OUT HELP

Sun Java™ System Access Manager

Access Control > Realm - selected > New Policy

**New Policy** OK Cancel

General Subjects Response Providers  
Rules Conditions

\* Indicates required field

**General**

\* Name: SF Policy

Description: Policy used for HP Select Federation integration

Active:  Yes

Back to top

- 5 Fill in the necessary information, including the following required information, then click **OK**:
  - **Name:** Enter the new policy name, such as **SF Policy**.
  - **Description:** Describe the policy.

The Policy page opens.

**Task 4: Create a Rule for the Select Federation Privacy Manager.**

- 1 Select the **Policy** that you just created (such as **SF Policy**).

The Edit Policy page for this policy opens.

- 2 Click **New** under the **Rules** subsection.

The Step 1 of 2: Select Service Type for the Rule page opens.

VERSION User: amAdmin Server: pulkitDC LOG OUT HELP

Sun Java™ System Access Manager

Access Control > Realm - selected > Policy - SF Policy > New Rule

**Step 1 of 2: Select Service Type for the Rule** Back Next Cancel

\* Indicates required field

\* Service Type:  Discovery Service (with resource name)  
 Liberty Personal Profile Service (with resource name)  
 URL Policy Agent (with resource name)

- 3 Select **URL Policy Agent** as the service type and click **Next**.



The Step 2 of 2: New Rule page opens.

Access Control > Realm - selected > Policy - SFPolicy > New Rule

**Step 2 of 2: New Rule** Back Finish Cancel

\* Indicates required field

\*Service Type: URL Policy Agent

\*Name: Protect PM

\*Resource Name: /\*pm\*

Actions

\* One or more actions are required.

Actions (2 Items)	
Action	Value
<input checked="" type="checkbox"/> GET	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
<input checked="" type="checkbox"/> POST	<input checked="" type="radio"/> Allow <input type="radio"/> Deny

4 Fill in the necessary information, including the following required information, then click **Finish**:

- **Name:** Enter **Protect PM**
- **Resource Name:** Enter **\*/pm\***
- Under **Actions:** Select **Get** and **Post**  
Be sure the **Value** for both is **Allow**.

The Edit Policy page opens.

**Task 5:** [Create a Rule for the Select Federation Administration console.](#)

1 Click **New** under the **Rules** subsection.

The Step 1 of 2: Select Service Type for the Rule page opens.

2 Select **URL Policy Agent** as the service type and click **Next**.

The Step 2 of 2: New Rule page opens.

3 Fill in the necessary information, including the following required information, then click **Finish**:

- **Name:** Enter **Protect Admin Console**
- **Resource Name:** Enter **\*/tfs-internal/admin/\***
- Under **Actions:** Select **Get** and **Post**  
Be sure the **Value** for both is **Allow**.

The Edit Policy page opens.

**Task 6:** [Create a Rule for the Select Federation AuthnPlugin.](#)

1 Click **New** under the **Rules** subsection.

The Step 1 of 2: Select Service Type for the Rule page opens.

2 Select **URL Policy Agent** as the service type and click **Next**.

The Step 2 of 2: New Rule page opens.

3 Fill in the necessary information, including the following required information, then click **Finish**:

- **Name:** Enter **Protection rule for AuthnPlugin**
- **Resource Name:** Enter **\*/select-federation\***
- Under **Actions:** Select **Get** and **Post**  
Be sure the **Value** for both is **Allow**.

The Edit Policy page opens.

**Task 7:** Create a Rule for the HP AM Integrator.

- 1 Click **New** under the **Rules** subsection.  
The Step 1 of 2: Select Service Type for the Rule page opens.
- 2 Select **URL Policy Agent** as the service type and click **Next**.  
The Step 2 of 2: New Rule page opens.
- 3 Fill in the necessary information, including the following required information, then click **Finish**:
  - **Name:** Enter **Protection rule for HP AM Integrator**
  - **Resource Name:** Enter **\*/hpamintegrator/protected/\***
  - Under **Actions:** Select **Get** and **Post**  
Be sure the **Value** for both is **Allow**.
 The Edit Policy page opens.

**Task 8:** Create a Rule for the Demonstration application, SF-Demo.

- 1 Click **New** under the **Rules** subsection.  
The Step 1 of 2: Select Service Type for the Rule page opens.
- 2 Select **URL Policy Agent** as the service type and click **Next**.  
The Step 2 of 2: New Rule page opens.
- 3 Fill in the necessary information, including the following required information, then click **Finish**:
  - **Name:** Enter **Protection rule for SF-Demo**
  - **Resource Name:** Enter **\*/sf-demo/protected/\***
  - Under **Actions:** Select **Get** and **Post**  
Be sure the **Value** for both is **Allow**.
 The Edit Policy page opens.
- 4 Click **Save** to save your rule settings.

**Task 9:** Configure Subjects for the policy.

- 1 Click **New** under the **Subjects** subsection.  
The Step 1 of 2: Select Subject Type opens.
- 2 Select **Access Manager Identity Subject** as the subject type and click **Next**.

The Step 2 of 2: New Subject - Access Manager Identity Subject page opens.

Access Control > Realm - selected > Policy - SF Policy > New Subject

Step 2 of 2: New Subject - Access Manager Identity Subject

Back Finish Cancel

\* Indicates required field

\* Name: Users for HP Select Federation integration

Exclusive:

Filter: -- Select Identity Type -- Search

Available:

- amAdmin
- anonymous
- foo bar
- geo
- john doe

Add >

Add All >>

< Remove

<< Remove All

Selected:

3 Fill in the necessary information, including the following required information, then click **Finish**:

- **Name:** Enter **Users for HP Select Federation integration**
- **Filter:** Click **Search** to display all available users in the **Available** list.
- **Selected:** Add users you want to be authorized, from the **Available** list to the **Selected** list.

The Edit Policy page opens.

4 Click **Save** to save your settings.

## Step 4: Configure the SF-SP for the Sun Access Manager Integration

Perform the following steps to configure the `$SF_HOME/conf/tfsconfig.properties` file for the Sun Access Manager integration with the SP site:

1 Comment out the following line, if it is not already commented out:

```
idpAuthnPlugin=com.trustgenix.tfsIDP.util.IDPAuthnPlugin_Dir
```

2 Add the following required lines:

```
idpAuthnPlugin=myAuthPlugin
myAuthPlugin.class=com.hp.selectfederation.sam.SAMAuthnPlugin
myAuthPlugin.jar=$SF_HOME/connectors/sam/SAMConnector.jar
amPlugin=myAdminPlugin
myAdminPlugin.jar=$SF_HOME/connectors/sam/SAMConnector.jar
myAdminPlugin.class=com.hp.selectfederation.sam.SAMAmPlugin

spEventPlugin=<myActivationPlugin> samEventPlugin
samEventPlugin.class=com.hp.selectfederation.sam.SAMEventPlugin
# Windows Flavored Platforms
samEventPlugin.jar=$SF_HOME\\connectors\\sam\\SAMConnector.jar
# UNIX Flavored Platforms
samEventPlugin.jar=$SF_HOME/connectors/sam/SAMConnector.jar
```

3 Make the following substitution in these lines:

```
$SF_HOME = Your SP Select Federation install directory.
```

For example:

```
c:/test-area/sp/inst7501
```

- 4 Add and configure required and optional Sun Access Manager parameters that do not have default values in the `tfscnfig.properties` file. Or the default values do not match your installation.

▶ If the Sun Access Manager server is SSL-enabled, then you must install the Sun Access Manager server's certificate in the Select Federation application server's trust store.

All parameters with default values are required. You only need to add them if you want to change the default value. Some parameters without default values are also required.

The following table lists and describes the Sun Access Manager parameters for an SP integration:

**Table 2 Select Federation Sun Access Manager Connector Parameters**

Parameter Name	Parameter Value	Description	Example	Required/Optional (default value)
<code>com.ipplanet.am.naming.url</code>	Naming URL for Sun Access Manager install	The value of this property represents the URL where the Client SDK would retrieve the URLs of Access Manager internal services. This is the URI for the Naming Service.	<code>http://sam.vm.net:9919/amserver/namingservice</code>	Required (None)
<code>com.ipplanet.am.defaultOrg</code>	Value is set at Sun Access Manager installation for <code>defaultOrg</code> .	Specifies the top-level realm or organization in the Access Manager information tree. The value for this parameter is in the Sun Access Manager install <code>AMConfig.properties</code> file.	<code>dc=vm,dc=net</code>	Required (None)
<code>com.ipplanet.am.server.protocol</code>	Protocol	Server protocol to be used by Authentication Service. The value for this parameter is in the Sun Access Manager install <code>AMConfig.properties</code> file.	<code>http</code>	Required (http)
<code>com.ipplanet.am.server.host</code>	HostName	Server host to be used by the Authentication Service. The value for this parameter is in the Sun Access Manager install <code>AMConfig.properties</code> file.	<code>myDC.vm.net</code>	Required (None)

**Table 2 Select Federation Sun Access Manager Connector Parameters**

<b>Parameter Name</b>	<b>Parameter Value</b>	<b>Description</b>	<b>Example</b>	<b>Required/Optional (default value)</b>
com.ipplanet.am.server.port	Port Number	Server port to be used by the Authentication Service. The value for this parameter is in the Sun Access Manager install AMConfig.properties file.	9919	Required 80
com.ipplanet.am.service.secret	Encryption Key	Contains the encrypted value of the password. The value for this parameter is in the Sun Access Manager install AMConfig.properties file.	AQIC2PJavDlo7/D+jyCpjE2qcmadltFqcqHw	Required (None)
com.ipplanet.am.authurl	URL protected by a Sun Access Manager Agent	Value for this parameter is the URL protected by a Sun Access Manager Agent. This page must be able to redirect the user back to the originally requested URL. The originally requested URL is appended as a parameter called "RURL". This parameter must be set if you are using the Login URL integration mechanism.	http://idp.vm.net:82/test/samplelogin.jsp	Optional (None)
com.sun.identity.agents.notification.url	Notification URL	Defines the notification URL for a remote policy API.	http://myDC.vm.net:9919/amserver/notification/service	Required (None)
com.sun.identity.agents.polling.interval	Integer value specifying number of minutes	Specifies the polling interval, which is the number of minutes after which an entry is dropped from the Client API's cache.	4	Optional (3)

**Table 2 Select Federation Sun Access Manager Connector Parameters**

<b>Parameter Name</b>	<b>Parameter Value</b>	<b>Description</b>	<b>Example</b>	<b>Required/Optional (default value)</b>
com.iplanet.cookieDomain	Cookie Domain	Cookie Domain for Sun Access Manager SSO Cookie. When you use the LoginURL integration mechanism, make sure that the cookie domain configuration for the Sun Access Manager Agents allows cookies to be received by the Select Federation IDP.	.vm.net	Optional (None)
authzResource	Resource URL	Select Federation Agent URL used for IDP authentication.	/select-federation	Required (/select-federation)
com.iplanet.am.cookie.name	Cookie Name	Cookie name used by the Authentication Service to set the valid session handler ID. The value of this cookie name is used to retrieve the valid session information. The value for this parameter is in the Sun Access Manager install AMConfig.properties file.	iPlanetDirectoryPro	Optional (iPlanetDirectoryPro)
com.sun.identity.agents.app.username	Admin user name	Specifies the user name to use with read access for the Sun Access Manager configuration.	amAdmin	Required (amAdmin)

**Table 2 Select Federation Sun Access Manager Connector Parameters**

Parameter Name	Parameter Value	Description	Example	Required/Optional (default value)
com.ipplanet.am.service.password	Admin password	Encrypted password for the Admin user (user name you use to log into the Sun Access Manager Admin console). To encrypt the password, use the ConfigPasswordMask.sh/bat utility tool shipped with Select Federation. For details on how to run this tool, see the “Security” section of the <i>HP Select Federation Installation Guide</i> .	{Mask}OTI7ND0/My4=	Required

## Step 5: (Optionally) Test the Sun Access Manager Connector Integration with the Demonstration Application

As a convenience, a Demonstration application is provided with Select Federation that you can use to test your integration. It is meant to emulate a portal page with a list of all the federated applications that are accessible to Sun Access Manager users. It is not meant for production use and should only be used for sanity-testing the connector integration.

The Demonstration application can be integrated with Sun Access Manager using either the Login URL or the Select Federation Agent integration mechanism. This depends on the configuration options that you have chosen for your integration.

To use the Demonstration application, complete the following tasks.

### Task 1: Set up an environment for the Demonstration application.

Following is a bare-minimum setup for the purposes of testing with the Demonstration application:

- 1 Set up different machines with different site roles:
  - One Select Federation install with the SP role (which is integrated with Sun Access Manager): SF-SP
  - One Select Federation install with the SP role: SF-IDP.

- 2 Exchange metadata between the following sites: SF-IDP with SF-SP.

If you are not familiar with setting up site roles or exchanging metadata, see the *HP Select Federation Administration and Configuration Guide* for detailed instructions.

#### Task 2: Run the Demonstration Application

To test the SF-IDP with the SF-SP, perform the following steps:

- 1 Navigate to the Demonstration application using the following URL:

```
http(s)://<sf-idp-url>:<port>/sf-demo
```

The Demonstration application landing page opens.

- 2 Select **Login locally to IDP demo application**.

The Login authentication page opens.

- 3 Enter a user name and password that can be validated against the directory server that was configured during the installation process.

The IDP Demonstration page opens.

- 4 Select an available link to the configured SF-SP which is integrated with Sun Access Manager.



# 5 Error Messages

This chapter lists error messages that are reported by the Select Federation Sun Access Manager connector. The exact wording may change.

## Error Message Terminology

The following terminology is used in the Sun Access Manager error messages:

- `SAMAmPlugin` – Module used for Select Federation Administration console and Privacy Manager integration.
- `SAMAuthnPlugin` – Module used for IDP side integration of Select Federation with Sun Access Manager.
- `SAMEventPlugin` – Module used for SP side integration of Select Federation with Sun Access Manager.
- `SAMUtil` – Utility Module used for Sun Access Manager integration.
- `XXXException` – Exception message from Exception class.
- `XXX` – Represents parameter substitutions.

## Error Messages and Descriptions

The Sun Access Manager connector reports error messages for the following plugin modules and utility:

- [SAMAmPlugin Error Messages](#)
- [SAMAuthnPlugin Error Messages](#)
- [SAMEventPlugin Error Messages](#)
- [SAMUtil Error Messages](#)

## SAMAmPlugin Error Messages

The following table lists the SAMAmPlugin error messages and explanations:

**Table 3 SAMAmPlugin Error Messages**

<b>Error Message</b>	<b>Explanation</b>
Unable to create SAMUtil class	Error occurred when creating Utility class samUtil.
Unable to instantiate SPAPI. Please check your configuration file	Unable to instantiate SPAPI. Check your <code>tfsconfig.properties</code> file to make sure your configuration parameters are specified correctly.
An error occurred in isAuthorized: XXXException	Details of exception are included in the XXXException message.
Error cleaning SAM session :: XXXException	Error when deleting SAM session during logout. Details included in the XXXException message.

## SAMAuthnPlugin Error Messages

The following table lists the SAMAuthnPlugin error messages and explanations:

**Table 4 SAMAuthnPlugin Error Messages**

<b>Error Message</b>	<b>Explanation</b>
Unable to create SAMUtil class	Error occurred when creating Utility class samUtil.
Invalid Login URL format.Please check <code>com.iplanet.am.authurl</code> configuration property.	Invalid value specified in the <code>com.iplanet.am.authurl</code> configuration property. Check the property value in the <code>tfsconfig.properties</code> file.
User: XXX is not authorized to access the resource: XXX". Please check your SAM Configuration...	Authorization access is incorrectly specified in your <code>authzResourc</code> resource parameter. Check the value for this parameter in the <code>tfsconfig.properties</code> file. Then make sure that you have authorization permissions set on this resource value.
Error loading <code>com.iplanet.am.authurl: XXXException</code>	Details of exception are included in the XXXException message.
Error cleaning SAM session: XXXException	Error when deleting SAM session during logout. Details included in the XXXException message.

<b>Error Message</b>	<b>Explanation</b>
An error occurred in authenticateUser: XXXException	Details of exception are included in the XXXException message.
Cannot URL-encode with UTF-8. XXXException	URL encoding failed. Details included in the XXXException message.
Error redirecting to login url: XXXException	Error redirecting to the Login URL. Details included in the XXXException message.

## SAMEventPlugin Error Messages

The following table lists the SAMEventPlugin error messages and explanations:

**Table 5 SAMEventPlugin Error Messages**

<b>Error Message</b>	<b>Explanation</b>
Unable to create SAMUtil class	Error occurred when creating Utility class samUtil.
Exception occurred in Event Plugin constructor : XXXException	Details of exception are included in the XXXException message.
User not activated. Please configure an activation event plugin :	User is not activated. The user is expected to be activated before control reaches this plugin. Check your activation plugin configuration.
Error cleaning SAM session: XXXException	Error when deleting a Sun Access Manager session during logout. Details included in the XXXException message.
Error when creating SAM session: XXXException	Error creating a Sun Access Manager session. Details of exception are included in the XXXException message.

## SAMUtil Error Messages

The following table lists the SAMUtil error messages and explanations:

**Table 6 SAMUtil Error Messages**

<b>Error Message</b>	<b>Explanation</b>
Required Param missing : com.iplanet.am.service.secret	Required parameter is missing: com.iplanet.am.service.secret. Check your configuration in the tfsconfig.properties file.
Required Param missing : com.iplanet.am.server.host	Required parameter is missing: com.iplanet.am.server.host. Check your configuration in the tfsconfig.properties file.
Required Param missing : com.iplanet.am.naming.url	Required parameter is missing: com.iplanet.am.naming.url. Check your configuration in the tfsconfig.properties file.
Required Param missing : com.iplanet.am.defaultOrg	Required parameter is missing: com.iplanet.am.defaultOrg. Check your configuration in the tfsconfig.properties file.
Required Param missing : com.sun.identity.agents.notification. url	Required parameter is missing: com.sun.identity.agents.notification. url. Check your configuration in the tfsconfig.properties file.
Failed to initialize Sun Access Manager Client SDK. Please check your configuration parameters	Failed to initialize the Sun Access Manager Client SDK. Check your configuration parameters in the tfsconfig.properties file.
Exception occurred in loginUser : XXXException	Details of exception are included in the XXXException message.
Sun Access Manager token is not valid	Invalid Access Manager token.
SSO exception has occurred : XXXException	Details of exception are included in the XXXException message.
Login exception has occurred : XXXException	Details of exception are included in the XXXException message.
An exception has occurred : XXXException	Details of exception are included in the XXXException message.
Unsupported call back exception : XXXException	Unsupported call back. Details of exception are included in the XXXException message.
Unsupported operation exception has occurred : XXXException	Unsupported operation exception. Details of exception are included in the XXXException message.

<b>Error Message</b>	<b>Explanation</b>
A Policy exception has occurred : XXXException	Details of exception are included in the XXXException message.
Exception occurred when getting user attributes: XXXException	Details of exception are included in the XXXException message.
AuthLogin exception : XXXException	Login Exception. Details of exception are included in the XXXException message.



# A Troubleshooting

Use the Select Federation log file to view logged messages. The location of the log file depends on the application server on which you have Select Federation installed.

There could be some exceptions caused due to incorrect syntax or configuration. Following are some common problems:

## Error

```
com/iplanet/sso/SSOException
```

## Problem

Your application server CLASSPATH does not contain the Sun Access Manager jar files needed for the integration.

## Solution

Make sure the Sun Access Manager `am_services.jar` and `amclientsdk.jar` files are set in your CLASSPATH and restart the Select Federation server. For details on how to set the CLASSPATH for your application server, see your application server documentation.

## Error

```
java.util.MissingResourceException: Can't find bundle for base name  
amAuthContext, locale en_US
```

## Problem

Your application server CLASSPATH does not contain the Sun Access Manager jar files needed for the integration.

## Solution

Make sure the Sun Access Manager `am_services.jar` and `amclientsdk.jar` files are set in your CLASSPATH and restart the Select Federation server. For details on how to set the CLASSPATH for your application server, see your application server documentation.

## Error

```
com.hp.selectfederation.sam.SAMUtil - In getSessionToken  
com.sun.identity.authentication.spi.AuthLoginException(1):null  
  
com.iplanet.services.comm.client.SendRequestException(2):Connection refused:  
connect  
  
com.iplanet.services.comm.client.SendRequestException: Connection refused:  
connect
```

### Problem

Your Sun Access Manager server is down.

### Solution

Start your Sun Access Manager server and then restart the Select Federation server.

### Error

```
com.hp.selectfederation.sam.SAMUtil - In getSessionTokencom.sun.identity.  
authentication.spi.AuthLoginException: Failed to create new Authentication  
Context: Naming Service is not available.
```

### Problem

Your Sun Access Manager server may be down.

### Solution

Start your Sun Access Manager server and then restart the Select Federation server.



---

# Glossary

**Access Control**

The authorization policies and conditions that regulate identity access to resources with a goal towards preventing unauthorized use or use in an unauthorized manner.

**Access Management**

The process of authentication and authorization.

**Activation**

Process of setting up mapping from a federated name identifier to a local user ID.

**Active Directory Federation Services (ADFS) (WS-Federation 1.0)**

A feature of Microsoft Windows 2003 Server R2, which allows a federation with Active Directory-based users, by using the WS-Federation 1.0 protocol.

**Active Server Pages (ASP)**

Microsoft pages, which log users in by invoking the IDP-FSS over a secure channel. See also [Identity Provider Filter-Support Service \(IDP-FSS\)](#).

**ADAM**

Active Directory Application Mode

**ADFS**

See [Active Directory Federation Services \(ADFS\) \(WS-Federation 1.0\)](#).

**Administrator**

An identity with full permission to manage Select Federation.

**API**

See [Application Program Interface \(API\)](#).

**Application Helper**

Select Federation component that helps you configure URLs in your application for seamless navigation to the Service Provider (SAML Consumer) sites or for authentication through the Identity Provider (SAML Producer) sites.

**Application Program Interface (API)**

An interface that enables programmatic access to an application.

## **Application Site Role**

An Application Site (also called a Service Provider (SP) Site), which is a Trusted Partner site that participates in a federation to provide a service or application to common users and relies on an authority site to provide authoritative user authentication and other information. For example, in a federation of an extranet with partners' corporate portals, the site hosting the extranet is the Application Site.

## **Artifact Binding**

Specifies that the browser should be redirected from the Authority Site (IDP) to the Application Site (SP) using a random string known as the "artifact" and that string should then be used by the SP over a SOAP call to retrieve the actual protocol message.

## **ASP**

See [Active Server Pages \(ASP\)](#).

## **Attribute**

One or more characteristics that are part of an identity profile. For each identity, an attribute has a corresponding value. For example, an attribute called "Department" may be assigned the values of, "IT", "Sales", or "Support". These attributes are interpreted and assigned appropriately to profiles in different applications (LDAP-compliant directories, databases, SAPs, and so on) based on the mapping rules defined for that application.

## **Authentication**

The act of verifying the credentials of an identity and matching them with an identity profile. The evaluation of credentials ensures that the identity is truly who or what they claim to be.

## **Authority Site Role**

An Authority Site (also called an Identity Provider (IDP) Site), which is a Trusted Partner site that participates in a federation to authenticate users and provide other authoritative user information to other sites. For example, in a federation of an extranet with partners' corporate portals, the portals act as the Authority Site.

## **Authorization**

The process of defining and enforcing the entitlements of an identity. Checking whether the entitlements of an authenticated principal permit the principal to perform the requested operation. Authentication is a prerequisite for authorization. See [Access Control](#) and [Authentication](#).

## **Bindings**

Possible ways in which messages can be conveyed in the context of a browser-based user transaction between an Authority Site (IDP) and an Application Site (SP).

## **CA**

Certificate Authority

## **CardSpace**

An active client software protocol that manages the release of identity information to Service Providers (SP). Identity information is organized into "cards" on the end user's computer. Each computer contains a set of "claims" or identity attributes, such as name or email

address. Each time the user is required to authenticate to an SP, the user selects one of these cards, which determines the set of claims that will be sent.

### **Certificate Revocation Checking**

Verifies the validity of certificates against a certification authority's published list of revoked certificates. Select Federation provides a simple means of enabling certificate revocation checking via Certificate Revocation Lists or CRLs.

### **Context**

A Select Identity concept that defines a logical grouping of users that can access a Service.

### **CSR**

Certificate Service Request

### **Delegated Administrator**

An identity that has been added by the root administrator. The delegated administrator can perform all functions that the root administrator performs except admin-related functions such as add and remove admins and change admin passwords. When Select Federation is running in Standalone mode, the delegated administrator also cannot view the Admin Audit log. But when Select Federation is integrated with Select Access, then the delegated administrator can view the Admin Audit log. See [Root Administrator](#).

### **Domain-Local Users**

Set of users who are limited to the domain controlled by an access management system (such as Select Access, SiteMinder, COREid, or Sun Access Manager).

### **DS**

Discover Service

### **DST**

(Data Services Template) DST-based services such as the Personal Profile service (ID-PP) and the Employee Profile service (ID-EP).

### **Edge Router**

A Federation Router that is located at the edge of an enterprise where employees of that enterprise use applications offered by partners of the enterprise. Those applications request authentication of users (employees) of the Federation Router, and the Federation Router “routes” that authentication request to the appropriate departmental authority. See [Federation Router](#).

### **Event**

Federation activity such as **Logged In**, **Received Logout Request**, **Logged Out**, and so on. Select Federation logs server events (operational activities of enabled users) and administrator events (all the federated identity activities of each administrator).

### **Event Plugin Chain**

A set of plugins that are called in order whenever an event occurs. A chain may contain one or more Event Plugins. See [Event](#).

## **Federation**

The combination of business and technology practices to enable identities to span systems, networks and domains in a secure and trustworthy fashion. This is analogous to how passports are used to assert our identity as we travel between countries.

## **Federation Router**

A Select Federation installation that simplifies trust relationships between Authority Sites (IDPs) and Application Sites (SPs). The Federation Router acts as an intermediary for multiple organizational entities.

## **Filter-Support**

A dedicated Java web application, which integrates Select Federation with the filters provided for the corresponding web servers: IIS, Apache 2.0 and Java Servlet Containers. Filter-Support also integrates Select Federation with web servers that cannot access the Select Federation databases, which are normally kept behind a firewall.

## **Filter-Support Service (FSS)**

A servlet component that exposes Select Federation functionality to non-java applications, which can make web requests through xml messages. FSS exposes two main pieces of functionality: a) allowing trusted programs to inject a Windows-authenticated `user-id` into an IDP session, and b) allowing trusted programs to query for user attributes.

## **FSS**

See [Filter-Support Service \(FSS\)](#).

## **GMT**

See [Greenwich Mean Time \(GMT\)](#).

## **Greenwich Mean Time (GMT)**

Standard time used throughout the world based on the mean solar time of the meridian of Greenwich. See [Universal Coordinated Time \(UTC\)](#).

## **Group**

For Select Federation, a Group shares a common set of policies. All groups and partners within that Group inherit those policies. An administrator may override the Group setting for a particular partner within that Group.

## **Identity Mapping**

The process of determining a local user ID against which to map an incoming federated name identifier. Two common techniques for identity mapping are either generating a random local user ID based on the federated name identifier or using any attributes available to determine a local user ID.

## **Identity Provider Filter-Support Service (IDP-FSS)**

A servlet component of the Integrated Windows Authentication (IWA). The IDP-FSS enables a trusted program to add a Windows-authenticated user ID into an IDP session.

**Identity Provider (IDP)**

An Authority organization or web site that asserts the identity of users to the Service Providers or SPs in a federated network. The assertion of the user identity is done using standard protocols such as SAML and Liberty.

**Identity Web Services Framework (ID-WSF)**

Liberty Identity Web Services Framework security mechanism, which is a federated web service protocol. ID-WSF is used to build federated (identity-based) web services.

**IDP**

See [Identity Provider \(IDP\)](#).

**IDP-FSS**

See [Identity Provider Filter-Support Service \(IDP-FSS\)](#).

**ID-WSF**

See [Identity Web Services Framework \(ID-WSF\)](#).

**IE**

Internet Explorer

**IIS**

See [Internet Information Server \(IIS\)](#).

**Impersonation Token**

Any token that allows actions to be carried out on the user's behalf. For example, in Windows, tokens issued through Kerberos are often used for impersonating users. Various technologies running on Windows have APIs defined that take an impersonation token and apply them to threads and/or processes that can then leverage them for whatever actions they need to perform on behalf of the users.

**Inbound Windows Integration (IWI)**

Inbound-integration that seamlessly integrates federated users at a Select Federation Application (SP) site to applications hosted on the Windows environment.

**Integrated Windows Authentication (IWA)**

Outbound integration that allows Select Federation to leverage a user's Windows logon credentials to seamlessly authenticate the user and transfer the user to a Trusted Federation Partner site.

**Internet Information Server (IIS)**

The web server that is bundled with the Windows 2003 Server.

**IWA**

See [Integrated Windows Authentication \(IWA\)](#).

**IWI**

See [Inbound Windows Integration \(IWI\)](#).

**JAVA**

Object-oriented programming language.

**JVM**

Java Virtual Machine. A platform independent execution environment that converts Java bytecode into machine language then executes it.

**Keystore**

A database of keys. The private keys are associated with a certificate chain, which authenticates the corresponding public key. The keystore also contains certificates from trusted entities. By generating the keystore, you add another layer of security to the data that is exchanged in the Select Federation system.

**LDAP**

See [Lightweight Directory Access Protocol \(LDAP\)](#).

**LECP**

Liberty Enabled Client/Proxy Service.

**Liberty Identity-based Web Services Framework (ID-WSF)**

A protocol that provides standards for discovering and invoking identity-based web services.

**Liberty Identity Federation Framework (ID-FF)**

An open standard federation standard protocol that provides basic single sign-on capabilities.

**Lightweight Directory Access Protocol (LDAP)**

A set of open protocols for accessing information directories. LDAP can make the physical network topology and protocols transparent so that a network identity can access any resource without knowing where or how it is physically connected.

**LUAD-WSC**

Liberty-enabled User-Agent or Device that acts as a [WSC](#).

**Metadata**

Online exact description of a Trusted Partner site in a federation. The metadata describes the various URLs at which its site services (such as Single Sign-On, Single Logout) are available. It also describes the public key certificates so that sites receiving messages from these Trusted Partner sites can confirm that the messages are signed correctly and have not been tampered with. See [Single Sign-On \(SSO\)](#) and [Single Logout \(SLO\)](#).

**Microsoft Management Console (MMC)**

MMC is used to set up server authentication and to import the pkcs / pfx format file into your local store on the IIS machine.

**MIME**

Multipurpose Internet Mail Extension

**MMC**

See [Microsoft Management Console \(MMC\)](#).

**NTLM (NT LAN Manager)**

Default network authentication protocol for Windows NT 4.0.

**OCSP**

See [Online Certificate Status Protocol \(OCSP\)](#).

**Online Certificate Status Protocol (OCSP)**

OCSP support exists in JDK 1.5. OCSP support is available for the Built-in application server (Tomcat 5.5.23) and WebLogic 9.1 and 9.2.

**Partner**

For Select Federation, the main entity in a federation trust relationship. A partner is described in terms of its protocol metadata, various descriptive attributes, and policy information. Select Federation allows partners to be grouped together in “Groups.”

**Passive URLs**

Passive URLs are for resources where users’ personalized content is not critical for the application. Users are allowed to access these URLs even though they cannot be authenticated without being prompted. However, if the user is already logged in at the IDP, has a federation session with Select Federation, or can be authenticated without being prompted, the user’s identity and attribute information is presented in the federation session to the application.

**PDC**

Primary Domain Controller

**Plugin**

Compiled code that can interact with the core product to provide additional functionality, without replacing parts of the core product. In the context of Select Federation, the “compiled code” can be thought of as Java compiled code that is packaged in JARs and the “core product” can be thought of as any Select Federation install.

**POST Binding**

Specifies that the protocol message is to be delivered to an SP from an IDP through an auto-posted HTML form.

**Presence Service**

A service that informs the WSC if a user is online, available, and so on. See [Web Service Consumer \(WSC\)](#).

**Privacy Manager**

End-user visible component of Select Federation. Its visibility allows extensive customizing.

## **Protected URLs**

Protected URLs require users to be authenticated to allow access to these URLs. If a user is not authenticated, the filter redirects the user to Select Federation for authentication. The Select Federation installation may authenticate the user locally or initiate federated logon at another Authority (IDP).

## **Protocol**

A set of rules that controls or enables communication between two endpoints. In the context of Select Federation, an endpoint is software that is capable of using any one of the many protocols that Select Federation supports.

## **Root Administrator**

The “super user” administrator who has complete entitlement to all functionality in the Select Federation Administration Console. The root administrator’s logon is always **admin**. Only the root administrator can add and remove delegated administrators and change administrators’ passwords.

## **SAML**

Security Assertion Markup Language open standard federation protocol. Identity federation standard that was created by the OASIS Security Services Technical Committee (SSTC).

## **Secure Sockets Layer (SSL)**

A handshake protocol, which supports server and client authentication.

## **Service Provider (SP)**

An application that allows authenticated access based on an authentication performed by an IDP using a federated identity protocol such as Liberty or SAML.

## **Single Logout (SLO)**

Permits a user to do a global log out from all active sites.

## **Single Sign-On (SSO)**

Session/authentication process that permits a user to enter one set of credentials (such as name/password, secureId, fingerprint, and so on) to access multiple applications. A Web SSO is a specialized SSO system for web applications.

## **Site Role**

Type of web site in a federation. Typically, you and your Trusted Partner agree in advance on how to set up the federation. Generally, one site hosts the application, while the other provides the authentication for end users to seamlessly access the application. When you deploy Select Federation in your site, you must set the site role as one of the following: (1) an Authority Site, (2) an Application Site, (3) both an Authority and Application Site, or (4) a Federation Router. See also [Service Provider \(SP\)](#), [Identity Provider \(IDP\)](#), and [Federation Router](#).

## **SLO**

See [Single Logout \(SLO\)](#).



**SOAP**

Simple Object Access Protocol is a fundamental web services standard for XML-based communication between web service providers and consumers.

**SP**

See [Service Provider \(SP\)](#).

**SSC**

Self Signed Certificate

**SSL**

See [Secure Sockets Layer \(SSL\)](#).

**SSO**

See [Single Sign-On \(SSO\)](#).

**TLS**

Transport Layer Security

**Universal Coordinated Time (UTC)**

Standard time used throughout the world based on the mean solar time of the meridian of Greenwich. Formerly known as Greenwich Mean Time (GMT).

**Unprotected URLs**

Unprotected URLs allow users access to these URLs without being authenticated. Typically, special URLs such as the logon URL and logout URL are unprotected URLs.

**UPN**

User Principal Name

**UTC**

See [Universal Coordinated Time \(UTC\)](#).

**WAP**

Wireless Application Protocol

**Web Service Consumer (WSC)**

An application that uses web services. It may not be a web service in itself, but uses XML and typically SOAP-based communication with a web service to perform some of its functions.

**Web Service Provider (WSP)**

A web service application that services requests it receives based on XML and typically SOAP-based communication.

**WSC**

See [Web Service Consumer \(WSC\)](#).

**WSP**

See [Web Service Provider \(WSP\)](#).

# Index

## Symbols

"E" IDP parameter, 18

"E" SP parameter, 32

"RURL" IDP parameter, 18

"RURL" SP parameter, 32

## A

access filter, 10

activate-demo.jsp, demo activation page, 34

Administration console

    creating a rule for an IDP integration, 23

    creating a rule for an SP integration, 41

    Sun Access Manager-protected user request flow diagram, 10

    using with Sun Access Manager, 10

Application Helper

    using for IDP federated applications, 19

attributes

    configuring federated user profile, 29

authentication

    configuring Sun Access Manager for an SF-IDP, 21

    configuring Sun Access Manager for an SF-SP, 35

AuthnPlugin

    creating a rule for an SF-SP, 41

authorization flow

    diagram, 9

    explanation, 9

authzResource parameter, 46

## C

com.iplanet.am.authn1 parameter

    for IDP integration, 18

    for SP integration, 32

com.iplanet.am.authn1 parameter, 45

com.iplanet.am.cookie.name parameter, 46

com.iplanet.am.defaultOrg parameter, 44

com.iplanet.am.naming.url parameter, 44

com.iplanet.am.server.host parameter, 44

com.iplanet.am.server.port parameter, 45

com.iplanet.am.server.protocol parameter

    Sun Access Manager for an SP integration, 44

com.iplanet.am.service.password parameter, 47

com.iplanet.am.service.secret parameter

    Sun Access Manager for an SP integration, 45

com.iplanet.cookieDomain parameter, 46

com.sun.identity.agents.app.username parameter, 46

com.sun.identity.agents.notification.url parameter, 45

com.sun.identity.agents.polling.interval parameter, 45

components

    IDP, 7

    SP, 7

configuring

    custom Authentication module for an SP integration, 36

    Select Federation for an SF-SP, 33

    SF-IDP for Sun Access Manager integration, 25

    SF-SP for the Sun Access Manager integration, 43

    Sun Access Manager for IDP integration, 19

    Sun Access Manager for SP integration, 33

    tfsconfig.properties file or Sun Access Manager integration with SF-IDP, 25

- configuring Sun Access Manager
  - basic tasks for an IDP integration, 22
  - basic tasks for an SP integration, 36
  - configuring for authentication for an IDP integration, 21
  - configuring for authentication for an SP integration, 35
  - configuring profile attributes, 29
  - configuring subjects for the policy for an SF-IDP integration, 25
  - configuring subjects for the policy for an SF-SP integration, 42
  - configuring the custom authentication module, 36
  - configuring the SF-IDP, 25
  - creating and configuring policies for an SF-IDP, 22
  - creating and configuring policies for an SF-SP, 39
  - creating an SF-IDP HP AM integrator rule, 24
  - creating an SF-IDP SF-Demo rule, 24
  - creating an SF-SP HP AM integrator rule, 42
  - creating an SF-SP SF-Demo rule, 42
  - creating a Privacy Manager rule for an SF-IDP, 22
  - creating a Privacy Manager rule for an SF-SP, 40
  - creating a rule for an SF-IDP Administration console, 23
  - creating a rule for an SF-IDP IDPAuthnPlugin, 24
  - creating a rule for an SF-SP Administration console, 41
  - creating a rule for an SF-SP AuthnPlugin, 41
  - deploying the custom authentication module, 36
  - Login URL for IDP integration, 21
  - Login URL for SP integration, 35
  - main steps for an SF-IDP, 19
  - main steps for an SF-SP, 33
  - parameters for an IDP integration, 26
  - Select Federation agent for an SF-IDP, 21
  - Select Federation agent for an SF-SP, 35
  - user activation scheme for an SF-SP, 33
  - using Application Helper for an SF-IDP, 19
- custom Authentication module
  - configuring for an SP integration, 36
  - deploying for an SP integration, 36

## D

- Demonstration application
  - running to test the SF-IDP with SF-SP, 30, 48
  - see SF-Demo for creating rules, 24
  - setting up an environment for testing an SF-IDP integration, 30
  - setting up an environment for testing an SF-SP integration, 47
  - testing the Sun Access Manager connector integration with an SF-IDP overview, 30
  - testing the Sun Access Manager connector integration with an SF-SP overview, 47
- deploying
  - custom Authentication module for an SP integration, 36
  - Sun Access Manager connector, 13

## E

- error messages
  - SAMAMPlugin, 50
  - SAMAAuthnPlugin, 50
  - SAMEventPlugin, 51
  - SAMUtil, 52
  - terminology, 49

## H

- HP AM integrator
  - creating a rule to configure Sun Access Manager for an SF-IDP, 24
  - creating a rule to configure Sun Access Manager for an SF-SP, 42

## I

- identity mapping
  - setting up in the SP's tfsconfig.properties file, 33
- IDPAuthnPlugin
  - creating a rule for an SF-IDP, 24
- IDP integration
  - configuring Sun Access Manager, 19, 22
  - configuring Sun Access Manager for authentication, 21
  - example using with Sun Access Manager, 8
  - integration mechanisms, 17
  - Login URL integration mechanism, 17
  - preparing the environment, 19
  - rolling back Sun Access Manager from, 15
  - Select Federation Agent integration mechanism, 17
  - Sun Access Manager parameters, 26
  - testing with the Demonstration application, 30
  - using a Login URL overview, 18
  - using the Select Federation agent overview, 18

## L

logging, 16

Login URL

- com.iplanet.am.authurl IDP login parameter, 18
- com.iplanet.am.authurl SP login parameter, 32
- configuring Sun Access Manager for an SF-IDP, 21
- configuring Sun Access Manager for an SF-SP integration, 35
- IDP integration mechanism, 17
- overview for an IDP integration, 18
- overview for an SP integration, 32
- SP integration mechanism, 31

## P

parameters

- "E" for IDP integration, 18
- "E" for SP integration, 32
- "RURL" for IDP integration, 18
- "RURL" for SP integration, 32
- com.iplanet.am.authurl IDP login, 18
- com.iplanet.am.authurl SP login, 32
- com.iplanet.am.authurl, 45
- com.iplanet.am.cookie.name, 46
- com.iplanet.am.defaultOrg, 44
- com.iplanet.am.naming.url, 44
- com.iplanet.am.server.host, 44
- com.iplanet.am.server.port, 45
- com.iplanet.am.server.protocol, 44
- com.iplanet.am.service.password, 47
- com.iplanet.am.service.secret, 45
- com.sun.identity.agents.app.username, 46
- com.sun.identity.agents.notification.url, 45
- com.sun.identity.agents.polling.interval, 45
- com.sun.identity.agents.polling.interval parameter, 46
- for an IDP integration, same as SP integration parameters, 26
- ProfileCookieEP.cookieDomain, 35
- ProfileCookieEP.cookiePath, 35
- ProfileCookieEP.setUserInfoFromIDP, 35
- ProfileCookieEP.tfsSessionIdStrName, 35
- Sun Access Manager, 44
- Sun Access Manager for an IDP integration, 26
- Sun Access Manager with SP integration, 35

passive URLs, 63

platform requirements, 13

policies

- configuring subjects for an SF-IDP integration, 25
- configuring subjects for an SF-SP integration, 42
- creating and configuring to configure Sun Access Manager for an SF-IDP, 22
- creating and configuring to configure Sun Access Manager for an SF-SP, 39

prerequisites, 8

Privacy Manager

- creating a rule to configure Sun Access Manager for an SF-IDP, 22
- creating a rule to configure Sun Access Manager for an SF-SP, 40
- using with Sun Access Manager, 10

ProfileCookieEP.cookieDomain parameter, for SP integration, 35

ProfileCookieEP.cookieName parameter, for an SP integration, 35

ProfileCookieEP.cookiePath parameter, for SP integration, 35

ProfileCookieEP.setUserInfoFromIDP parameter, for SP integration, 35

ProfileCookieEP.tfsSessionIdStrName parameter, for SP integration, 35

## R

requirements

- SP integration, 31

rolling back

- from an IDP integration, 15
- from an SP integration, 15

rules

- creating for Administration console for an SF-IDP, 23
- creating for Administration console for an SF-SP integration, 41
- creating for an SF-IDP IDPAuthnPlugin, 24
- creating for an SF-SP AuthnPlugin, 41
- creating for the Privacy Manager for an SF-IDP integration, 22
- creating for the Privacy Manager for an SF-SP integration, 40
- creating for the SF-IDP HP AM integrator, 24
- creating for the SF-IDP SF-Demo, 24
- creating for the SF-SP HP AM integrator, 42
- creating for the SF-SP SF-Demo, 42

## S

SAMAMPlugin error messages, 50

SAMAuthnPlugin error messages, 50

- SAMEventPlugin error messages, 51
  - SAMUtil error messages, 52
  - Select Federation Agent
    - IDP integration mechanism, 17
    - SP integration mechanism, 31
  - Select Federation agent
    - configuring Sun Access Manager for an SF-IDP, 21
    - configuring Sun Access Manager for an SF-SP, 35
    - overview for an IDP integration, 18
    - overview for an SP integration, 32
  - SF-Demo
    - creating a rule to configure Sun Access Manager for an SF-IDP, 24
    - creating a rule to configure Sun Access Manager for an SF-SP, 42
  - software requirements, 13
  - SP integration
    - com.iplanet.am.server.protocol Sun Access Manager parameter, 44
    - com.iplanet.am.service.secret Sun Access Manager parameter, 45
    - configuring a custom Authentication module, 36
    - configuring for the Sun Access Manager integration, 43
    - configuring Sun Access Manager, 33, 36
    - configuring Sun Access Manager for authentication, 35
    - deploying a custom Authentication module, 36
    - determining a user activation scheme, 33
    - example using with Sun Access Manager, 8
    - integration mechanisms, 31
    - Login URL integration mechanism, 31
    - ProfileCookieEP.cookieDomain parameter, 35
    - ProfileCookieEP.cookiePath parameter, 35
    - ProfileCookieEP.setUserInfoFromIDP, 35
    - ProfileCookieEP.tfsSessionIdStrName parameter, 35
    - requirements, 31
    - rolling back Sun Access Manager from, 15
    - Select Federation Agent integration mechanism, 31
    - setting up identity mapping in the tfsconfig.properties file, 33
    - setting user profile attributes, 34
    - Sun Access Manager parameters, 35, 44
    - testing with the Demonstration application, 47
    - using a Login URL overview, 32
    - using the Activate URL plugin, 34
    - using the Select Federation agent overview, 32
  - Sun Access Manager components, 7
  - Sun Access Manger-protected Administration
    - console
      - user request step-by-step explanation, 11
  - system requirements
    - platform, 13
    - software, 13
- ## T
- testing
    - Sun Access Manager connector with an SF-IDP integration, 30
    - Sun Access Manager connector with an SF-SP integration, 47
  - tfsconfig.properties file
    - configuring for Sun Access Manager integration with SF-IDP, 25
    - configuring profile attributes for an SF-IDP integration, 29
    - configuring the SF-SP for the Sun Access Manager integration, 43
    - modify to roll back Sun Access Manager from the IDP integration, 15
    - modify to roll back Sun Access Manager from the SP integration, 15
    - setting the user profile attributes for an SP integration, 34
    - setting up identity mapping for an SP integration, 33
  - troubleshooting, 55
- ## U
- URL classes
    - passive, 63
  - user activation scheme
    - configuring Select Federation for an SF-SP, 33
    - determining for an SP integration, 33
    - using the Activate URL plugin for an SP integration, 34
  - using Sun Access Manager
    - with Administration console, 10
    - with Privacy Manager, 10
    - with SP and IDP, 8

