HP Select Federation

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

Software Version: 7.00

SPML Connector Guide

Document Release Date: August 2007
Software Release Date: September 2007

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

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 Waveset Technologies, Inc. (www.waveset.com).
- 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 manual'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://ovweb.external.hp.com/lpe/doc_serv/

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 online support 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 and HP Passport, go to:

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

Contents

1 Introduction

The Select Federation SPML Connector enables new federated users arriving at a Select Federation Service Provider (SF-SP) site to be provisioned to the local provisioning system. When a new user arrives at an SF-SP site for the first time, the user is directed to the Identity Provider (IDP) site to be authenticated.

If the provisioning of the user fails during the SPML call to the provisioning system (the system is down, user name is already in use, and so on), the provisioning of that user fails and an error message is displayed to the user. See Chapter 4, Error Messages for the types of error messages and their descriptions.

This chapter provides an overview of using the SPML connector in the following topics:

- Prerequisites
- Use Case

Prerequisites

This document assumes you have knowledge of the following:

- HP Select Federation (installation, configuration, concepts and so on)
- Provisioning systems, including HP Select Identity, on which the SPML connector was tested (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)

Use Case

Following is an example of how to use the SPML connector to provision a user to the Select Identity provisioning system.

The SPML Connector should NOT be used when using a ONE-TIME pseudonym. This is because the IDP site assigns a different pseudonym as the user ID whenever the same user logs on to the IDP site. This behavior causes too many obsolete IDs in the provisioning system.

Required Setup

Select Identity and the Select Federation IDP must be set up as follows:

- A Select Identity admin has created the required SPML attributes for Services, Service Roles, and Context in Select Identity.

- These SPML attributes are manually mapped to the Select Federation profile attributes in the `<SFInstallDir>/conf/tfsconfig.properties` file.
- The Select Identity admin (if needed) has defined the different Services, Service Roles and Context for each of the IDPs in the Select Identity system based on the `context` attribute configured in Select Identity.
- The Select Federation IDP is set up for this SP partner so that at least the required SPML profile attributes are sent by the IDP to the SP.

Use Case Flow

Following is the use case flow of provisioning a user to the Select Identity provisioning system:

1. When a new user arrives at the SP the user is auto-assigned a local user ID by Select Federation.
2. Select Federation sends the desired SPML message to Select Identity to provision the user.
3. The connector provides an option for a URL “hook” to a customizable page that is displayed to the user once a response is obtained from Select Identity.

2 Deploying the SPML Connector

This chapter includes the following topics:

- System requirements
- Deploying the SPML connector
- Rolling back the SPML connector to Select Federation 6.6.2
- SPML logging

System Requirements

The following software must be installed and configured:

- Select Federation 7.00 — already installed. See the *HP Select Federation Installation Guide* for installation instructions.
- Provisioning system — The SPML connector has been tested on HP Select Identity 4.01, 4.10 and 4.11.

Deploying the SPML Connector

When Select Federation is installed, the following SPML connector files are automatically deployed to the `<SF_INSTALL_DIR>\connectors\SPML\` directory:

- `spml-connector.jar`
- `activation.jar`
- `openspml.jar`
- `soap.jar`
- `mail.jar`
- `\docs\spml.pdf`

You need to complete the deployment of the SPML `JAR` files. The deployment process is dependent upon the particular application server you wish to use, as described in the following sections:

- Deploying the SPML Connector JAR Files for the Built-in Application Server in Standalone Mode
- Deploying the SPML Connector JAR Files for the Built-in Application Server as a Windows Service
- Deploying the SPML Connector JAR Files for the WebSphere Application Server 6.0.2

- Deploying the SPML Connector JAR Files for the WebLogic Application Server 8.1
- Deploying the SPML Connector JAR Files for the WebLogic Application Server 9.1

Deploying the SPML Connector JAR Files for the Built-in Application Server in Standalone Mode

Perform the following steps to deploy the JAR files for the built-in application server (Tomcat 5.5.23) in standalone mode:

1. Stop the built-in server.
2. Add the following line to the `<SF_INSTALL_DIR>\conf\tfsconfig.properties` file:

   ```
   spmlConnector.jar=<path_to>\spml-connector.jar
   ```

   This step assumes that the `tfsconfig.properties` file includes the following line for the SPML connector:

   ```
   spEventPlugin=spmlConnector
   ```

3. Add the following entries in the `Catalina.bat` file (Windows) or the `Catalina.sh` file (UNIX) in the `<SF_INSTALL_DIR>\bin\ directory`.

   Windows:

   ```
   set SPML_JARS=<SF-INSTALL-DIR>\connectors\SPML\activation.jar;
   <SF-INSTALL-DIR>\connectors\SPML\soap.jar;
   <SF-INSTALL-DIR>\connectors\SPML\mail.jar;
   <SF-INSTALL-DIR>\connectors\SPML\openspml.jar
   ```

   UNIX:

   ```
   SPML_JARS=:<SF-INSTALL-DIR>/connectors/SPML/activation.jar:
   <SF-INSTALL-DIR>/connectors/SPML/soap.jar:
   <SF-INSTALL-DIR>/connectors/SPML/mail.jar:
   <SF-INSTALL-DIR>/connectors/SPML/openspml.jar
   ```

4. Update the CLASSPATH variable with `SPML_JARS` as follows:

   Windows:

   ```
   set
   CLASSPATH=%CLASSPATH%:%CATALINA_HOME%\bin\bootstrap.jar;%$CATALINA_HOME%\
   bin\commons-logging-api.jar;%$CATALINA_HOME%\common\lib\tools.jar;%SPML_J
   ARS%
   ```

   UNIX:

   ```
   CLASSPATH="$CLASSPATH":"$CATALINA_HOME"/bin/
   bootstrap.jar:"$CATALINA_HOME"/bin/
   commons-logging-api.jar:"$CATALINA_HOME"/common/lib/tools.jar:$SPML_JARS
   ```

5. Restart the application server.

Deploying the SPML Connector JAR Files for the Built-in Application Server as a Windows Service

Perform the following steps to deploy the JAR files for the built-in application server as a Windows service:

1. Add the following line to the `<SF_INSTALL_DIR>\conf\tfsconfig.properties` file:

   ```
   spmlConnector.jar=<path_to>\spml-connector.jar
   ```

   This step assumes that the `tfsconfig.properties` file includes the following line for the SPML connector:

   ```
   spEventPlugin=spmlConnector
   ```

2. Add the following entries to the CLASSPATH parameter in `HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun 2.0\SelectFederation\Parameters\Java`:

   ```
   <SF_INSTALL_DIR>\connectors\SPML/activation.jar:
   <SF_INSTALL_DIR>\connectors\SPML\soap.jar:
   <SF_INSTALL_DIR>\connectors\SPML\mail.jar:
   <SF_INSTALL_DIR>\connectors\SPML\openspml.jarS
   ```

3. Restart the service.

Deploying the SPML Connector JAR Files for the WebSphere Application Server 6.0.2

Perform the following steps to deploy the JAR files for the WebSphere application server:

1. Add the following line to the `<SF_INSTALL_DIR>\conf\tfsconfig.properties` file:

   ```
   spmlConnector.jar=<path_to>\spml-connector.jar
   ```

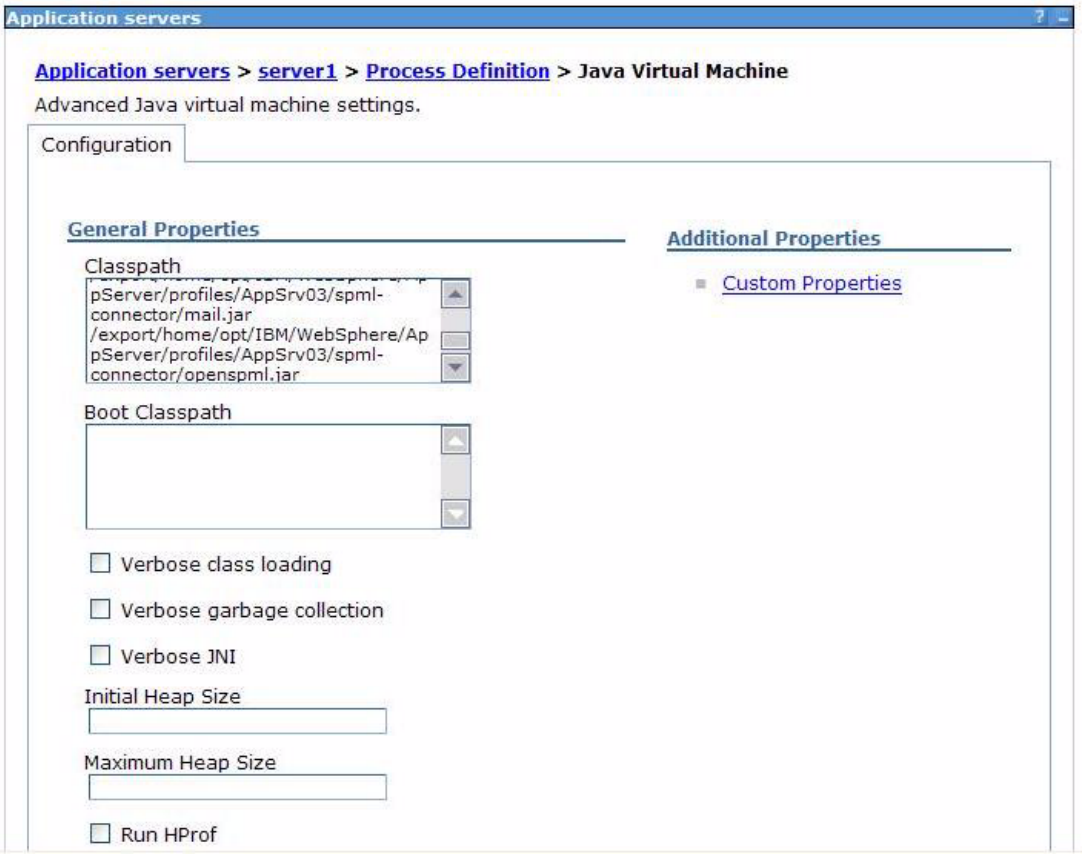
   This step assumes that the `tfsconfig.properties` file includes the following line for the SPML connector:

   ```
   spEventPlugin=spmlConnector
   ```

2. On the WebSphere Administration console, add the following JAR files located in the `<SF_INSTALL_DIR>\connectors\SPML\` directory to the General Properties Classpath:

   - `spml-connector.jar`
   - `activation.jar`
   - `openspml.jar`
   - `soap.jar`
   - `mail.jar`

Following is an example of the Classpath in the WebSphere console:



3 Restart the WebSphere server.

Deploying the SPML Connector JAR Files for the WebLogic Application Server 8.1

Perform the following steps to deploy the JAR files for the WebLogic 8.1 application server:

1 Add the following line to the `<SF_INSTALL_DIR>\conf\tfsconfig.properties` file:

```
spmlConnector.jar=<path_to>\spml-connector.jar
```

This step assumes that the `tfsconfig.properties` file includes the following line for the SPML connector:

```
spEventPlugin=spmlConnector
```

2 Open one of the following files to edit based on your operating system, where `$DOMAIN_HOME` represents the path to the Select Federation domain of WebLogic:

- On Windows: `$DOMAIN_HOME\startWebLogic.cmd`
- On UNIX: `$DOMAIN_HOME/startWebLogic.sh`

3 Define the `SPML_JARS` variable **before** you define the Classpath variable as follows:

- In the Windows `$DOMAIN_HOME\startWebLogic.cmd` file, enter:

```
@REM set spml jars
```

```
set SPML_JARS =%DOMAIN_HOME%\connectors\SPML\activation.jar;
%DOMAIN_HOME%\connectors\SPML\soap.jar;
%DOMAIN_HOME%\connectors\SPML\mail.jar;
%DOMAIN_HOME%\connectors\SPML\openspml.jar
```

- In the UNIX `$DOMAIN_HOME/startWebLogic.sh` file, enter:

```
# set spml jars
SPML_JARS =$DOMAIN_HOME/connectors/SPML/activation.jar:
$DOMAIN_HOME/connectors/SPML/soap.jar:
$DOMAIN_HOME/connectors/SPML/mail.jar:
$DOMAIN_HOME/connectors/SPML/openspml.jar
```

4. Add the `SPML_JARS` path name to the Classpath variable.
5. Restart the WebLogic server.

Deploying the SPML Connector JAR Files for the WebLogic Application Server 9.1

Perform the following steps to deploy the JAR files for the WebLogic 9.1 application server:

1. Add the following line to the `<SF_INSTALL_DIR>\conf\tfsconfig.properties` file:

   ```
   spmlConnector.jar=<path_to>\spml-connector.jar
   ```

   This step assumes that the `tfsconfig.properties` file includes the following line for the SPML connector:

   ```
   spEventPlugin=spmlConnector
   ```

2. Open one of the following files to edit based on your operating system, where `$DOMAIN_HOME` represents the path to the Select Federation domain of WebLogic:
   - On Windows: `$DOMAIN_HOME\bin\startWebLogic.cmd`
   - On UNIX: `$DOMAIN_HOME/bin/startWebLogic.sh`
3. Define the `SPML_JARS` variable **before** you define the Classpath variable as follows:
   - In the Windows `$DOMAIN_HOME\bin\startWebLogic.cmd` file, enter:

     ```
     @REM set spml jars
     set SPML_JARS =%DOMAIN_HOME%\connectors\SPML\activation.jar;
     %DOMAIN_HOME%\connectors\SPML\soap.jar;
     %DOMAIN_HOME%\connectors\SPML\mail.jar;
     %DOMAIN_HOME%\connectors\SPML\openspml.jar
     ```

   - In the UNIX `$DOMAIN_HOME/bin/startWebLogic.sh` file, enter:

     ```
     # set spml jars
     SPML_JARS =$DOMAIN_HOME/connectors/SPML/activation.jar:
     $DOMAIN_HOME/connectors/SPML/soap.jar:
     $DOMAIN_HOME/connectors/SPML/mail.jar:
     $DOMAIN_HOME/connectors/SPML/openspml.jar
     ```

4. Add the `SPML_JARS` path name to the Classpath variable.
5. Restart the WebLogic server.

Rolling Back the SPML Connector From the Select Federation Installation

You can roll back the SPML connector from the Select Federation installation. To do this, simply remove or comment out all the SPML-specific parameters from the `tfsconfig.properties` file.

SPML Connector Logging

SPML connector errors are logged in the Select Federation `log4j.properties` file in the `<SF_INSTALL_DIR>\properties` directory. You need to configure logging and set the logging level to DEBUG to provide detailed logging messages. For more information, see "Logging for WebLogic and WebSphere" in the *HP Select Federation Installation Guide*.

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 Configuring the SPML Connector

Be sure all the required software is installed and configured. See System Requirements on page 9 for details.

Configure the SPML connector by completing the following tasks:

- Task 1: Configure the Provisioning system.
- Task 2: Set up the Select Federation IDP site.
- Task 3: Configure the SPML connector.
- Task 4: Set up the user attribute-to-SPML Attribute mapping.

Task 1: Configure the Provisioning system.

Configure your provisioning system to create a provisioning service. See the provisioning system's documentation for details.

If you are using Select Identity on which the SPML connector was tested, see the Select Identity online help and web services guide for information required to create a Select Identity service.

Task 2: Set up the Select Federation IDP site.

You need to set up the Select Federation IDP site for the SP Partner so that the required SPML attributes are sent by the IDP to the SP site. You do this by specifying the profile attributes on the Application Attribute Policy page in the Select Federation Administration console for the IDP site.

Following are brief instructions for specifying the profile attributes. For complete instructions, see the *HP Select Federation Configuration and Administration Guide*.

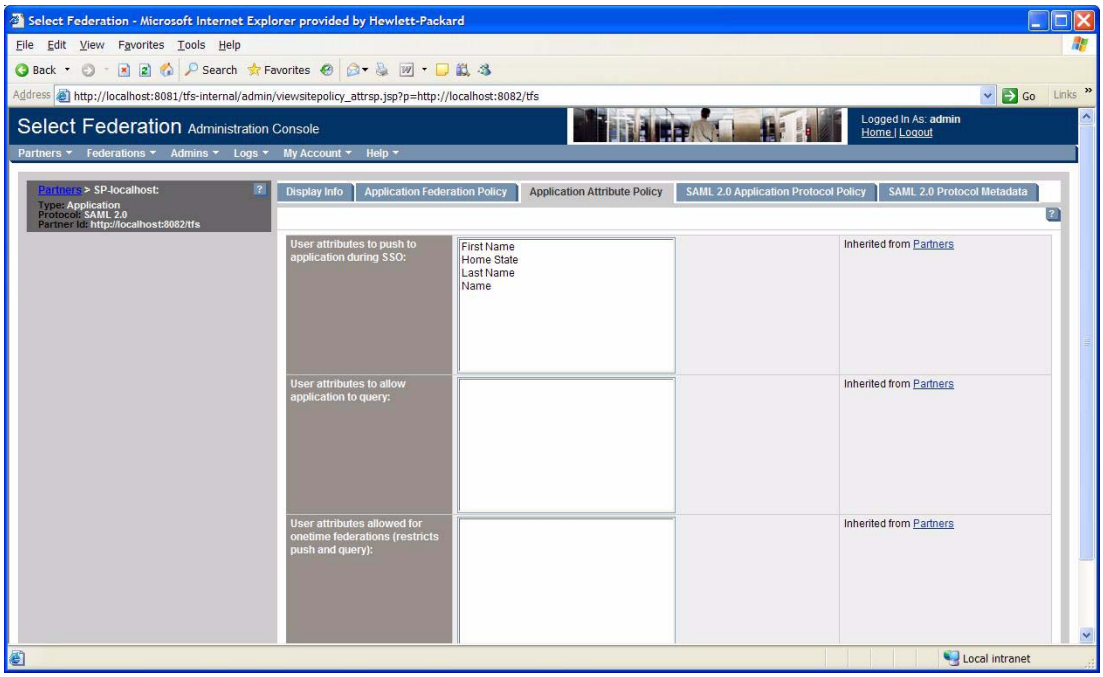
Perform the following steps to specify the profile attributes on the Application Attribute Policy page:

1. Select the **Partners** → **Manage Partners** menu options or click the **Manage Partners** link on the Welcome page.

   The Partners page opens
2. Click on the **Name** of the site that you want to edit.
3. Click on the Application Attribute Policy tab.

   The Application Attribute Policy page opens.
4. Click the **edit** button.

The Application Attribute Policy page opens to a page similar to the following figure with attribute choices in the right panel.



5 Select the profile attributes in the right panel that the IDP needs to send to the SP and click the left double arrows to add the attributes to the left panel.

The Name attribute must be selected since it must be mapped to the SPML userid attribute in the `tfsconfig.properties` file.

6 Click **Save** when you are finished.

Task 3: Configure the SPML connector.

Configure the SPML connector for the Select Federation SP site by adding and configuring SPML parameters in the `<SF_INSTALL_DIR>\conf\tfsconfig.properties` file.

Perform the following steps to configure the SPML connector:

1 Add the SPML connector as an SP EventPlugin.

For example, you can enter `spmlConnector` (the name of the connector) as follows:

`spEventPlugin=spmlConnector`

2 Add and configure the following required and optional parameters for the SPML connector.

> You must prefix the parameters with the name given to the connector in the 'spEventPlugin parameter. For example, in the example in step 1, the prefix would be `spmlConnector.<param-name>=value`.

Parameter Name	Required	Description	Value/Example
`class`	Yes	Connector class that will be invoked for provisioning.	`com.hp.selectfederation.spml.SPMLConnector`
`spmlUrl`	Yes	URL where the provisioning system has the SPML web service deployed.	Typically the URL is at **http(s)://<hostname>:<port>/lmz/webservice/**
`spmlAttrs`	Yes	Space separated list of SPML attributes defined for the provisioning service that the connector will use for provisioning.	See Task 4 for a detailed example.
`spmlUserUrn`	Yes	URN used for the user ID operational attribute.	`urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName`
`spmlPassUrn`	Yes	URN used for the password operational attribute.	`urn:trulogica:concero:2.0#password`
`servicesUrn`	Yes	URN used for the services operational attribute.	`urn:trulogica:concero:2.0#serviceName`
`spmlUser`	Yes	User ID that will be presented as part of the authentication to the provisioning system by the connector. This is an SPML operational attribute.	user ID
`spmlPass`	Yes	Password that will be presented as part of the authentication to the provisioning system by the connector. This is an SPML operational attribute.	password

Parameter Name	Required	Description	Value/Example
services	Yes	Provisioning service or services that the SPML request will be routed to. Multiple services are specified as a space separated list. This is an SPML operational attribute.	provisioning service

pendingUrl	No	URL to the jsp page that provides a customized message to the user. If this parameter is set up, then the jsp page that the URL points to must be constructed and deployed by the Select Federation SP administrator.	The jsp page must have the following snippets of code in the order shown:
			1) Get the return URL from the request.
			`<%//get the return url String rurl = request.getParameter ("RURL");%>`
			2) Set the return URL as a link embedded in the page. In the following example the user will click the link to go to the desired destination page.
			`Please click <ahref=" <%=rurl%>">here</a> to continue.`

<userAttr>.spmlAttr	Yes	There will be many of these mappings that associate the specified values defined in the userAttrs list to each of the values in the spmlAttrs.	See Task 4 for a detailed example.

Task 4: Set up the user attribute-to-SPML Attribute mapping.

The name profile attribute must be mapped to the SPML userid attribute.

The following example shows how to map the Select Identity user attributes to the SPML userid attribute. In this example, the SPML userid attribute is represented as UserName.

Select Identity user attribute mapping example:

Assume spmlAttrs is defined as follows.

```
spmlConnector.spmlAttrs= FirstName LastName UserName Email
```

The tfsconfig.properties file includes a list of profile attributes that are used by Select Federation as defined by the userAttrs parameter. Based on this example, the following profile attributes (Select Identity attributes in this case) may be added:

```
userAttrs=name name_title name_firstname name_lastname home_street
home_city home_state home_country home_postalCode personal_email
personal_phone work_street work_city work_state work_country
work_postalCode work_email work_phone
```

The `spmlAttr` attributes that are marked as required in the Select Identity console for the services specified in the `services` attribute must be mapped to a `userAttr`. The other `spmlAttr` may or may not be mapped to a `userAttr`. Do the mapping as follows:

```
spmlConnector.name_firstname.spmlAttr=FirstName
spmlConnector.name_lastname.spmlAttr=LastName
spmlConnector.name.spmlAttr=UserName
spmlConnector.work_state.spmlAttr=State
```

4 Error Messages

If the provisioning fails, the type of error message or messages that display to the user depends on how the `genericError` flag is set in the `<SF_INSTALL_DIR>\conf\tfsconfig.properties` file as follows:

- If the `genericError` flag is set to `true` (value=`1`), **and** you have not added any customized error messages through the `genericErrorMsg` attribute, the following default error message displays:

  `Response from provisioning system indicates a failure.`

- If the `genericError` flag is set to `false` (value=`0`), **and** you have not added any customized error messages through the `genericErrorMsg` attribute, the provisioning system sends the error message.

- If the `genericError` flag is set to `true` (value=`1`), **and** you created your own customized error messages through the `genericErrorMsg` attribute, then those messages display to the user.

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).

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.

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 bytecore 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.

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.

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 8.1 and 9.1.

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 login 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 login 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.

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 login URL and logout URL are unprotected URLs.

UPN

User Principal Name

UTC

See Universal Coordinated Time (UTC).

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).


invent


Java™
COMPATIBLE