HP OpenView Select Federation

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

Software Version: 6.5

Architecture Guide

Legal Notices

Warranty

Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices

Trademark Notices

- Trustgenix, IdentityBridge, and Trustgenix Federation Server are U.S. trademarks of Trustgenix, Inc.

- BEA and WebLogic are registered trademarks of BEA Systems, Inc.

- IBM, Tivoli, WebSphere are trademarks of International Business Machines in the United States, other countries or both.

- Linux is a U.S. registered trademark of Linus Torvalds.

- Microsoft®, Windows®, and Windows NT® 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.

- Sun, Sun Microsystems, Solaris, and Java™ are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

- All other trademarks, trade names, service marks, and logos referenced herein belong to their respective companies/owners.

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, visit the following URL:

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 OpenView support web site at:

http://www.hp.com/managementsoftware/support

This Web site provides contact information and details about the products, services, and support that HP OpenView offers.

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valuable support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit enhancement requests online
- Download software patches
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter 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://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

http://www.managementsoftware.hp.com/passport-registration.html

Contents

1 Introducing the Select Federation Architecture Guide

Introduction

This *HP OpenView Select Federation Architecture Guide* gives an overview of the basic architecture that underly Select Federation and describes the features that allow you to create a federation with your Trusted Partners.

Audience

This guide is intended for:

- Persons or teams responsible for installing and configuring Select Federation with existing network technologies
- Persons or teams responsible for the ongoing administration of Select Federation

Prerequisites

This guide assumes a working knowledge of:

- Identity Management
- Federated Identity
- HP OpenView Select Access

Chapters Summary

The table that follows provides an overview of this guide's contents.

Table 1   Contents Summary

Chapter	Description
Chapter 1, Introducing the Select Federation Architecture Guide	This chapter provides a brief description of this Architecture Guide. It is geared to provide users with a quick overview of the information contained herein.
Chapter 2, What Does Select Federation Do?	This chapter gives a brief overview of identity federation and briefly describes Select Federation's key features.

Chapter	Description
Chapter 3, How is Select Federation Architected?	This chapter describes how Select Federation works with Select Access and provides an overview on the architecture and components of Select Federation.
Chapter 4, **Error! Reference source not found.**	This chapter describes Select Federation's features in detail.

2　What Does Select Federation Do?

This chapter gives you a brief overview on identity federation and an overview of HP OpenView Select Federation's capabilities. A detailed description of Select Federation's features can be found in Chapter 4, **Error! Reference source not found.**.

What is Identity Federation?

Federated Identity or Identity Federation is a new approach to solving the single sign-on problem through a secure exchange of identity information among cooperating organizations, whether within an company or between companies using open standards. Select Federation helps companies that use Select Access to achieve cross-domain single sign-on quickly and easily.

Federation solves the pain points left unaddressed by or created by conventional identity management by giving companies a secure open standards methodology to exchange user data across independent identity domains within their intranet and across the extranet.

Users typically have an account that they use regularly, such as their corporate account and independent accounts at one or more web sites that they use less frequently. Once the accounts are federated, users can access all the federated web sites through their most frequently used account without having to remember multiple passwords and signing in each time they need to access the less used web sites.

What are the Select Federation's Key Features?

Select Federation is a J2EE-based server that can run on top of many J2EE servlet engines (such as BEA WebLogic, IBM WebSphere, and Apache Tomcat). It has the following features:

- **Comprehensive federation features** including:
  — **Single Sign-On**: Provides seamless navigation to common applications
  — **Provisioning**: Provides instant activation of users at common applications
  — **Coarse-Grained Privilege Management**: With this feature, you can set the LDAP directory to control which end-users have access to which common applications
  — **Termination**: Also known as single logout, with this feature users terminated in home domain lose access to all the common applications
- **Multi-protocol support**. As detailed in the next section "Which Open Federation Standards Does Select Federation Support?," Select Federation supports all of the popular federation protocols, including Liberty Alliance ID-FF 1.1, Liberty Alliance ID-FF 1.2, Liberty Alliance ID-WSF, SAML 1.0, and SAML1.1.
- **Easy integration with LDAP directories:** Select Federation readily integrates with an LDAP directory for obtaining user-profile and authentication information. Using an LDAP directory is simply a matter of configuration, no code required. Select Federation connects to the LDAP directory through the HP Select Access Adapter. The Select Access Adaptor is a component of Select Federation that connects Select Federation with the Select Access Policy and your LDAP repository (see Figure 1 to see how the Select Access

Adaptor connects Select Federation with Select Access. Chapter 3 has more details on the Select Access Adaptor.).

- **Scalability and reliability:** Designed to be deployed on multiple servers, Select Federation can scale to handle large transaction loads.

A more detailed explanation on Select Federation's features can be found in Chapter 4, **Error! Reference source not found.**.

Which Open Federation Standards Does Select Federation Support?

Select Federation is one of the most comprehensive federation protocol solutions. It supports multiple federated identity protocol standards which provides flexibility when connecting with multiple Trusted Partners with multiple federated identity protocol. Select Federation simultaneously supports different Trusted Partners in a federation that may be communicating using multiple federation protocols.

Select Federation supports all existing Liberty Alliance and Security Assertion Markup Language (SAML) protocols, including the following popular federation protocols:

- Liberty Identity Federation Framework (ID-FF) 1.1
- Liberty Identity Federation Framework (ID-FF) 1.2
- Liberty Identity-based Web Services Framework (ID-WSF) 1.0
- SAML 1.0 and SAML 1.1

Liberty Identity Federation Framework (ID-FF) 1.1

The first version of the Liberty Identity Federation Framework (ID-FF 1.1) provides basic single sign-on capabilities. Select Federation is a Liberty ID-FF 1.1 certified interoperable product, and hence has support for all features of Liberty ID-FF 1.1 specified by the interoperability specification, available at:

        http://www.projectliberty.org/specs/liberty-idff-1.1-scr-v1.0.pdf

Liberty Identity Federation Framework (ID-FF) 1.2

The second version of the Liberty Identity Federation Framework (ID-FF 1.2), coupled with the Liberty Identity-based Web Services Framework (ID-WSF), extends the standards into identity-based web-services capabilities. Select Federation supports all capabilities of Liberty ID-FF 1.2 that are included in Liberty ID-FF 1.1. Select Federation also supports all of the new features, including the new meta-data format, publishing meta-data at URLs, etc.

Liberty Identity-based Web Services Framework (ID-WSF) 1.0

ID-WSF 1.0 provides the standards for discovering and invoking identity based web services. Identity Service Interface Specifications is a set of standard service interfaces specified to provide commonly required services. In the Liberty specifications, this is limited to a "personal profile" service and "employee profile" service. Select Federation provides a Liberty ID-WSF 1.0 compatible Discovery Service and a configurable number of Data Services Template (DST)-based services such as the Personal Profile service (ID-PP) and the

Employee Profile service (ID-EP). In the ID-WSF security mechanisms, Select Federation supports the null, clientTLS and X509 security mechanisms.

SAML 1.0 and SAML 1.1

The SAML specification is an XML framework for exchanging authentication and authorization information. Select Federation provides comprehensive support for both the SAML 1.0 and SAML 1.1 standards, including the ability to create and consume signed SAML authentication and attribute assertions. Select Federation provides a SAML Authentication Authority and an Attribute Authority.

What Deployment Modes are Available?

When you deploy Select Federation at your site, you will have to set your site to be an "authority site," an "application site," or both an authority and application site. Typically, you and your Trusted Partner agree in advance how the federation will be set up. One site will host the application, while the other provides the authentication so that the end-users can to seamlessly access the application.

Authority Site

An authority site [also called a SAML Producer or Identity Provider (IDP) Site] 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.

Application Site

An application site [also called a SAML Consumer or Service Provider (SP) Site] 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. In the extranet example, the site hosting the extranet is the application site.

Both Authority Site and Application Site

Using the Liberty ID-FF 1.2 protocol, a single Select Federation instance can handle both the application site and authority site roles. For example, you may host an extranet for your partners' employees to access, in which case you are the application site. However, your partners may also host applications that require your employees to authenticate at your site.

3   How is Select Federation Architected?

Select Federation was architected to support all the federation protocols, with scaleability and reliability in mind. Select Federation is a complete, easy-to-install federation solution that integrates seamlessly with your existing Select Access deployment.

How Does Select Federation Work with Select Access?

Select Federation is designed to complement an enterprise's existing Select Access deployment, adding the specialized function of federated identity management. Select Federation in effect extends the identity management capabilities of Select Access to disjoint domains which may or may not be in your organization. Select Federation's deployment model is described by the following "concept diagram," as shown in Figure 1.

Figure 1   Select Federation concept diagram
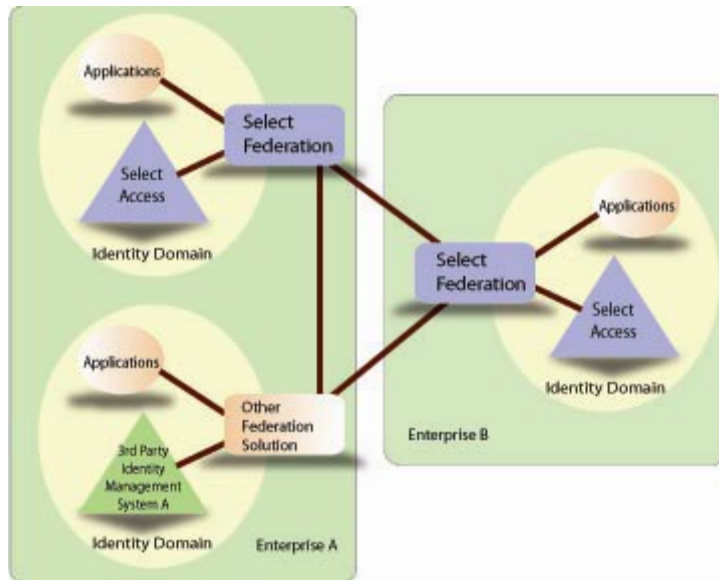
Select Federation delivers the federation capabilities that allow you to connect to all your Trusted Partners regardless of which federation protocol and federation solution the partners selected. As shown in Figure 1, Select Federation is connected to Select Access and the associated applications that your end-users need to access. Thus, with one instance of Select Federation, your Select Access users are able to connect to with all your trusted partners' applications without the user needing to login separately each time.

What are the Components of Select Federation's Architecture?

Select Federation depends upon Select Access for authentication. Figure 2 gives you an overview of Select Federation's architecture and details how its components integrate with

Select Access via the Select Access Policy. The Select Access Policy is created using Select Access Policy Builder. For more information on creating the Select Access Policy, see the Chapter 3 of the *Select Federation Configuration and Administration Guide.*

Select Federation is comprised of these key components which are detailed in this chapter:

- Protocol Responders
- Unified Federation Management Core
- Select Access Adapter
- Administration Console
- Key Store
- Privacy Manager

Select Federation also connects to third party software (an open source federation repository is bundled with Select Federation) for these components:

- Federation Repository
- LDAP Repository

Figure 2   Select Federation architecture and how it integrates with Select Access
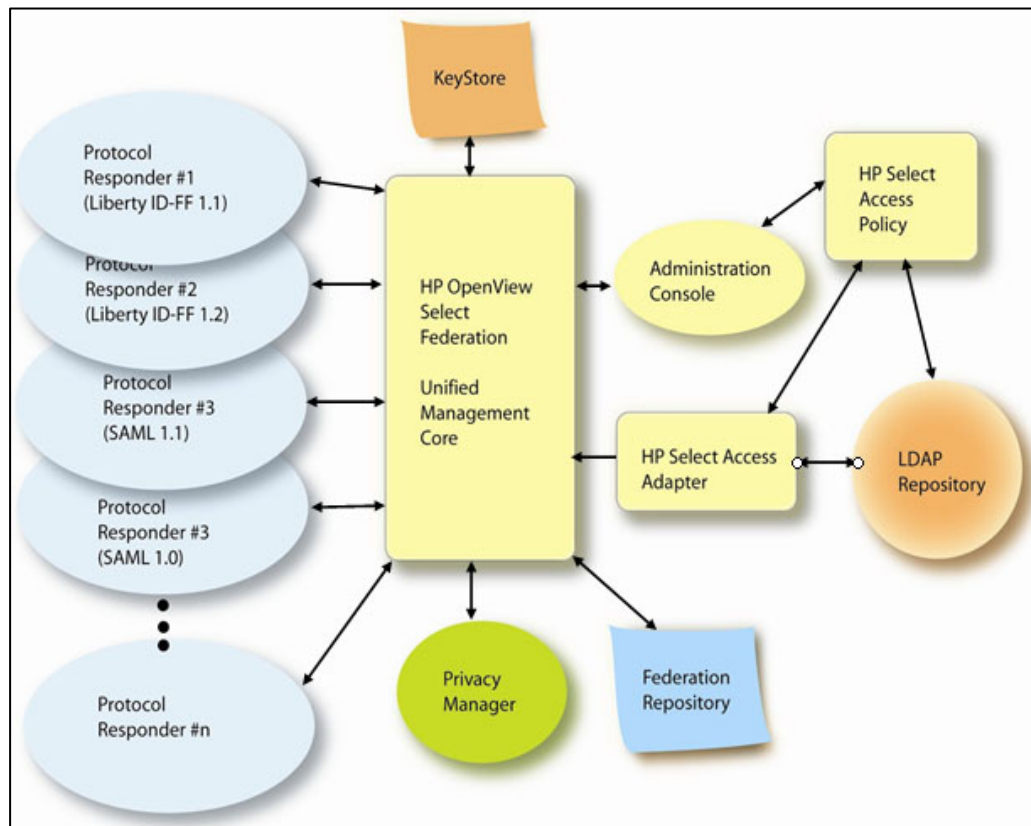
Protocol Responders

Protocol responders are J2EE servlets that receive messages either on the front-channel (from a user-agent such as a browser) or on the back-channel (e.g. a SOAP message from another Select Federation server). The front-channel and back-channel servlets are packaged in separate "web-archives" or WARs so that they may be deployed on different servers or ports with independent firewall configurations. These protocol responders represent:

- **Front-channel URLs:** Examples of front-channel URLs include the SAML Single Sign-On Service URL or the Liberty Assertion Consumer Service URL. These URLs are available and are advertised in the meta-data.

- **Back-channel Web-Services:** Examples of back-channel Web-services include the Liberty Profile Service or the SAML Attribute Authority Service. These URLs may be advertised through the meta-data (as in the case of the Liberty 1.1 SOAP service), or through the Liberty Discovery Service which is also a part of the protocol responders.

Unified Federation Management Core

The Select Federation Unified Federation Management Core provides the basic infrastructure for Select Federation to work. It manages the user-federation-session information, federation mappings of user identities, circle-of-trust information of your Trusted Partner sites, and audit events. It uses the federation repository to store all this information.

Federation Repository

The federation repository is a relational database used by the Unified Federation Management Core to manage all internal data required for federation. Select Federation supports Oracle 9i and Apache Derby database servers. Apache Derby is bundled with Select Federation so there is no need to install it separately.

Select Access Adapter

The Select Access Adapter is a component of Select Federation that connects Select Federation with Select Access and an LDAP v3 compatible directory to provide integrated federated user authentication and user profile information. The Select Access Adapter obtains information about the location of the LDAP directory using a configuration file that is generated in the installation process. This configuration file can be manually edited for subsequent changes. The LDAP directory is referenced for profile attributes of the user as well as verifying membership for privileged access to external applications.

Administration Console

Select Federation provides a Administration Console that allows the root administrator to add and configure additional delegated administrators to Select Federation, and to monitor the activities of these delegated administrators and the enable end users. The administration console is a web front-end that connects into the Select Access Policy. It allows the administrator to monitor existing federations with Trusted Partners including capabilities such as defining trusted sites, manually deleting user federations, and viewing audit log.

Key Store

The key store is a Java Cryptography Architecture-compliant key store that can be realized in software or hardware. Select Federation requires the key store to be co-resident with it on the same application server.

Privacy Manager

The Select Federation Privacy Manager is a unique component that empowers end users to control the exchange of their personal attributes and their preferences about exchanging such information between trusted sites. The Privacy Manager is only provided with Select Federation Premium Edition. It enables end users to consent the personal information that may be exchanged between federated sites. This exchange of personal information typically occurs as a part of a Liberty Profile Service query or a SAML Attribute query.

Additional Utilities that Aid in Application Integration and Testing

Select Federation provides two additional utilities for easing application integration and testing. They are the Application Helper and Demo Application.

Application Helper

The Application Helper is designed to enable web site administrators to obtain URLs that enable seamless navigation between federated sites or that enable an administrator to request federated login from a select Identity Provider or Authority Site. The Application Helper can be found on the Select Federation Welcome Page, as shown in Figure 3.

Figure 3   Select Federation Application Helper is on the Welcome page
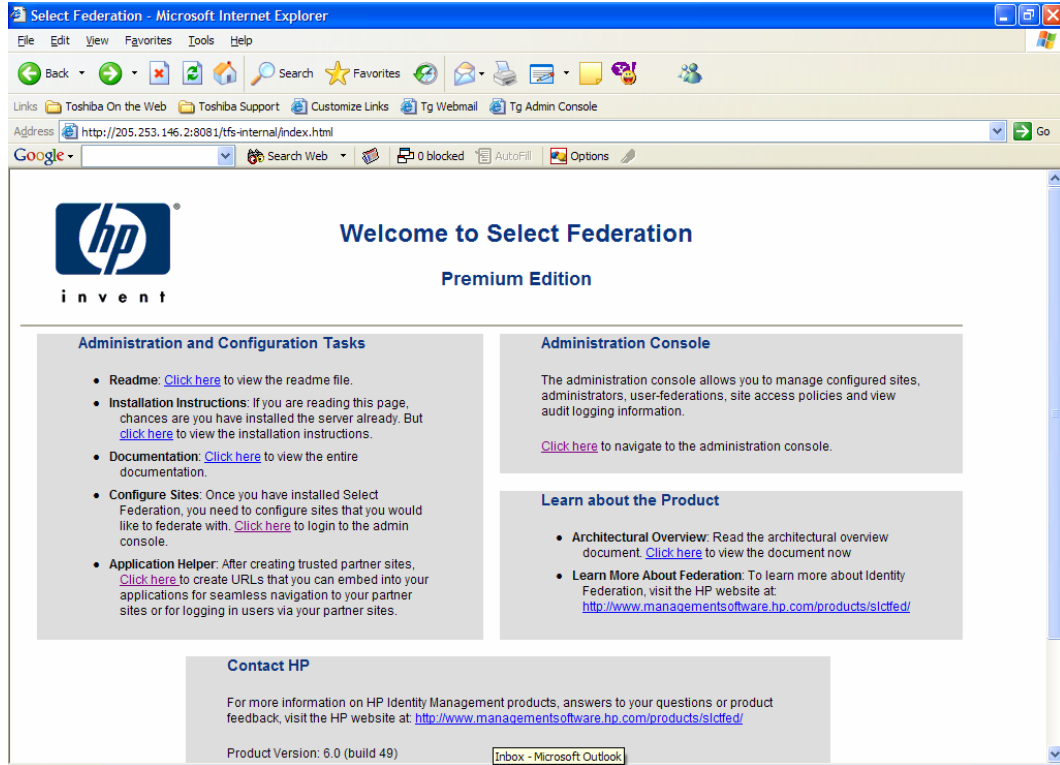
Demo Application

The Demo Application is a regular J2EE application that uses the Select Access Servlet Enforcer. It demonstrates that normal Select Access applications can benefit from the seamless federated single sign-on and other capabilities provided by Select Federation. The Demo Application is bundled with Select Federation and can be found at /sf-demo.

4 What are Select Federation's Key Capabilities?

This chapter is intended to give you a detailed description of how the Select Federation features work in a federation. For instructions on how to install and configure Select Federation, see the HTML instructions on the CD and the *Select Federation Configuration and Administration Guide.*

How Does Select Federation's Features Work?

In a typical federation environment, multiple sites are seamlessly connected. It is important that sites share their on-line descriptions or *meta-data* with each other. This ensures that a site knows where to send messages to another site in its federation, or a site knows that a message that it has received is guaranteed to be from a site that it trusts and has not been tampered with.

Meta-data

Meta-data in a federation is a description of the Trusted Partner site with which you want to federate. It is an online exact description of a site in a federation. Meta-data describes the various URLs at which different site services (such as single sign-on and 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.

In the SAML 1.0, SAML 1.1, and Liberty ID-FF 1.1 protocols, the meta-data specifications are either informal specifications or just a convention in the community about how to define the meta-data. Under the Liberty ID-FF 1.2 federation protocol, the meta-data specification is formalized, and meta-data using this protocol is conforming and has been certified under interoperability testing.

In Select Federation, site configuration is done using the administration console. The administration console enables an administrator to publish the site's meta-data as well as import other sites' meta-data. Select Federation simplified the process of obtaining your meta-data for all the popular federation protocols. With one click, you can download your site information into any of the needed federation protocol formats. Alternatively, if your partner prefers the information in text format, all information is readily available on the web page so that you can cut and paste the text.

User Provisioning / Activation

Select Federation supports user-provisioning or "activation" across identity domains. The first time a new user accesses the Application Site, the user attributes that are needed by the Application Site are requested from the Authority Site in order to automatically active this new user account. This is how user provisioning works, assuming both the Authority and Application Sites use Select Federation:

1 A new user logs in to his local "employee portal" or other internal application that enables him to access a federated partner site for the first time.

2 Select Access at the user's home site uses the local Identity Management System or LDAP repository to authenticate the user.

3 When the user clicks the external link, he is redirected to the local instance of Select Federation. This generates a SAML or Liberty assertion for the user with a new "federated-identifier" – an opaque large number that represents the user at the partner site. The Select Federation at the local site then redirects the user to the Select Federation at the external Application Site and transmits the assertion message.

4 The Select Federation at the partner site receives the assertion message and obtains the "federated identifier" from the assertion message. If Select Federation does not recognize the federated identifier, it knows that the user is coming to the site for the first time and thus requires provisioning or activation.

5 Select Federation then triggers the request for the activation profile from the user's home Select Federation.

6 The home Select Federation queries the LDAP repository for the user's profile information.

7 The home Select Federation provides the required profile attributes to the requesting Select Federation (after verifying that the site policy allows such disclosure).

8 The Select Federation at the partner site then populates a new entry with all the profile attributes in the partner's LDAP repository that is known to the Select Access installation there. It automatically assigns a local user ID for this new user.

Single Sign-On

Similar to the provisioning and activation feature, single sign-on works as follows:

1 The user clicks a link at an Application Site or an Authority Site and is redirected to the Select Federation instance at the Authority site. Such links can be generated using the Application Helper as described in Chapter 3 under Application Helper.

2 In order to authenticate the user, Select Federation redirects the user to the Select Access Adapter. The Select Access Adapter provides the authenticated user information to Select Federation and redirects the user back to Select Federation.

3 Select Federation then generates a SAML or Liberty assertion for the user and redirects the user to the destination Application Site.

4 The Select Federation at the Application Site receives and verifies the assertion. It then identifies the local user.

5 Using the Select Access Adapter, the Select Federation at the Application Site sets a temporary cookie in the browser. The cookie allows the user to seamlessly navigate to any site protected by that Application Site's Select Access instance.

6   The Select Federation at the Application Site then redirects the user to the final destination URL to which he initially intended to go.

Single Logout or Termination

The user may click a "global logout" or "single logout" button at an application t to indicate that he wishes to logout from all active sites. Select Federation provides a "single logout URL" to which the application can redirect the user in order to do a global logout.

Select Federation redirects the user to his Authority Site with a signed logout request. The Select Federation at the Authority Site keeps track of all the sites at which the user is logged in and sends signed messages to all such Application Sites, thus enabling a global Logout.

Name Federation Policy

Select Federation allows users to connect to Trusted Partner web sites in three ways: using the user's local name which has identifiable user information, using a unique identifier that does not reveal the users' identities to outside sites or totally anonymity. This feature is called the Name Federation Policy. Regardless of which federation protocol is being used between two sites, the authority site can determine a name-federation policy. This policy can be one of three values:

- **Local names:** The local user IDs at the authority site are revealed unmodified to the partner site. This is typically useful when two internal sites are using Select Federation to enable single sign-on between them.

- **Pseudonyms:** These are also identifiers or tokens that are generated to keep the user's local identity unknown to the Service Provider. Select Federation automatically generates an opaque large random number mapping for a local user ID. Note that this pseudonym is unique to each partner site that the user is federated with. Thus, unlike the One Time Pseudonym, each time the user goes to the Trusted Partner site, the same identifier is presented. The Service Provider or Application site will know that this user's activity at its site. This is an useful name ID policy in a typical business-to-business (B2B) scenario.

- **One-time pseudonyms:** These are anonymous identifiers or tokens (also an opaque large random number) that is generated each time the user accesses a Trusted site. Every time the same user visits the same partner site, Select Federation will generate a new pseudonym for the user. This provides complete anonymity for the user at the partner site and is useful in business-to-consumer (B2C) scenarios.

Attribute Exchange

Select Federation provides extensive support for exchanging personal information (user attributes) between Trusted Partner sites. Applications typically need attributes about the authenticated users. In a federated system, the most recent values for these user attributes are at the original source of the authentication, i.e. the Identity Provider or SAML Producer.

The administrator at the authority site can choose to allow, on a per partner site basis, certain attributes to be pushed along with an authentication assertion (SAML or Liberty) and certain attributes to be queried by a particular partner site. Attributes are configured in the Select Federation properties file and are fetched on every user authentication. Select Federation can further be configured to "push" attributes on every outbound user authentication when working as a SAML producer or IDP, further saving the overhead in fetching attributes about the user. Please refer to the *Select Federation Configuration and Administration Guide* for information on how to configure attribute exchange.

Privacy Manager

The Privacy Manager is available only with the Select Federation Premium Edition. It is the only component of Select Federation that is end-user visible. Therefore, it also has extensive customization abilities. The Privacy Manager resides at the relative URL: /pm within the Select Federation deployment.

The Privacy Manager consists of two parts:

1   The Preference Setting service (`privacy`).

2   The Interaction / Consent service (`irs`).

The Preference Setting service is available only in HTML and is used like a regular application by the user to set his privacy preferences before any information about that user has been exchanged.

The Interaction / Consent service is available in HTML and WML and is invoked when the user has set a preference that he should be asked before information about him is disclosed to a partner site and the transaction that the user is undergoing results in the need for such disclosure.

When using the SAML protocols (1.1 or 1.0), the Interaction / Consent screen is invoked only on attributes that are "pushed" with the authentication assertion. Since the SAML 1.1 or 1.0 protocols do not specify a mechanism to handle interactions during attribute queries, such queries fail if the user sets the preferences that he needs to consent such information.

When using the Liberty protocols (1.1 or 1.2 and ID-WSF), the Interaction / Consent screen may be invoked either during an attribute "push" within the Liberty Authentication Response message or during a Liberty Profile Service query.

The Interaction / Consent service displays the details of the information that is about to be provided to the partner site.

Artifact Pickup Security Mechanisms

Select Federation provides extensive support for various security mechanisms between Trusted Partner sites for picking up SAML artifacts. The mechanisms supported by Select Federation are:

*   **Signature:** The site requesting an artifact should digitally sign the request.

*   **SSL/TLS Client Authentication:** The site requesting the artifact is required to provide a digital certificate to successfully complete an SSL or TLS client Authentication handshake before the artifact may be disclosed.

*   **HTTP Basic Authentication:** The site requesting the artifact needs to authenticate with a user name and password. This option is provided mainly to support federation products that do not support the other two security mechanisms.

Select Federation Deployment Considerations

Select Federation may be deployed three different ways, depending on your existing architecture and the level of redundancy you need.

*   Three-tier deployment

*   Multi-server deployment

- Redundancy

Three-tier deployment

In a three-tier architecture, Select Federation should be deployed in the middle-tier and the federation repository will be a part of the data tier. The Select Federation protocol responders are accessed by external resources such as users' browsers or Select Federation or other identity federation deployments at partner sites. Thus, you should deploy J2EE connectors from your web server to the application server(s) that host Select Federation.

Multi-server deployment

In the simplest case, Select Federation and all its components can co-reside with an application or other infrastructure on a single J2EE App Server. However, Select Federation is flexible enough that its various components can be deployed on multiple servers.

For example, the front-channel protocol responders can be on one application server, the back-channel protocol responders can be on another application server, the Administration Console can be on a third application server and the Java API can be on yet another one.

This flexibility allows you to deploy on redundant servers as well as allows you to configure firewall rules separately. The federation repository is shared by all these components, so it should be accessible from all Select Federation components.

Redundancy

Designed for reliability, Select Federation components can be deployed on redundant servers sharing the same federation repository. In such a configuration, if one of the server goes down, the other server can continue servicing transactions, including ones that were being processed by the server that went down.