

HP Select Federation

For the Windows® operating system

Software Version: 7.00

Quick Start 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

© Copyright 2002-2007 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 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	7
	About This Guide	7
	Prerequisites	7
	Software Requirements	7
	Hardware Recommended Specifications	7
	Using this Guide	8
2	Installing the Select Federation IDP Instance	9
	Before You Begin	9
	Procedure	10
3	Installing the Select Federation SP Instance	15
	Before You Begin	15
	Procedure	16
4	Exchanging Metadata	21
	Introduction	21
	Downloading the SP's Metadata into the IDP Site	22
	Downloading the IDP's Metadata into the SDP Site	24
5	Using the Demonstration Program	27
	Introduction	27
	SP-Initiated Federation	28
	How an SP-Initiated Federation Works	28
	Procedure	29
	IDP-Initiated Federation	31
	How an IDP-Initiated Federation Works	31
	Procedure	32
	SP-Initiated Single Logout	34
	How an SP-Initiated Single Logout Works	34
	Procedure	35
	IDP-Initiated Single Logout	36
	How an IDP-Initiated Single Logout Works	36
	Procedure	37
	Glossary	39

1 Introduction

About This Guide

Quick start guide is intended for a quick, easy-to-use demonstration of Select Federation for customers and field personnel. This is not intended to be an introductory guide that explains what federation is or what Select Federation is. It is assumed that you are familiar with federation from a business and high-level technology point of view, is familiar with the terminology used and has read introductory material about Select Federation. This document does not replace the *HP Select Federation Installation Guide* and *HP Select Federation Configuration and Administration Guide*. If you have questions regarding the why's, how's, or would like to learn about the many advanced configuration options of Select Federation please refer to the *HP Select Federation Configuration and Administration Guide* included with the software.

When you deploy Select Federation in your site, you must set the site role. In this guide you will install one Select Federation instance as an Authority Site (IDP) on one machine and a second Select Federation instance as an Application Site (SP) on another machine. 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.

Prerequisites

Software Requirements

You must have the following software:

- Windows 2003
- Select Federation 7.0
- LDAP Directory accessible

Hardware Recommended Specifications

Following are the recommended hardware specifications:

- Intel Pentium PCs Processor Speed: 1 GHz
- Memory: 1 GB RAM or higher
- Disk Space: 2 GB disk space

Using this Guide

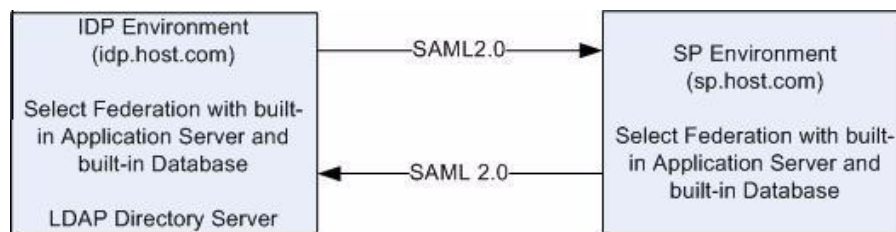
This guide walks you through the following procedures:



This guide assumes you are installing the IDP and SP instances on separate machines.

- [Installing the Select Federation IDP Instance](#) — shows how to install Select Federation as an Authority Site (IDP) on Windows 2003 using the Built-in Application Server and database.
- [Installing the Select Federation SP Instance](#) — shows how to install Select Federation as an Application Site (SP) on Windows 2003 using the Built-in Application Server and database.
- [Exchanging Metadata](#) — shows how to use Select Federation to exchange partner information using the SAML 2.0 protocol.
- [Using the Demonstration Program](#) — shows how to use the `sf-demo` Demo Application that is shipped with Select Federation. The Demo Application demonstrates federated Single Sign-On and other Select Federation capabilities.

Your environment for the purposes of this guide is shown in the following diagram:



2 Installing the Select Federation IDP Instance

This chapter provides instructions for installing the Select Federation IDP instance on the default Built-in Application Server using the Select Federation Derby Built-in database.



Be sure you install the IDP instance on a different machine than the SP instance.

Before You Begin

Gather the following information:

- Company Name
- Host Name where Select Federation will be run
- Port Number to use for the built-in application server
- LDAP Directory hostname
- LDAP Directory Port
- LDAP Directory Base DN
- LDAP Directory User ID attribute name
- Keystore password


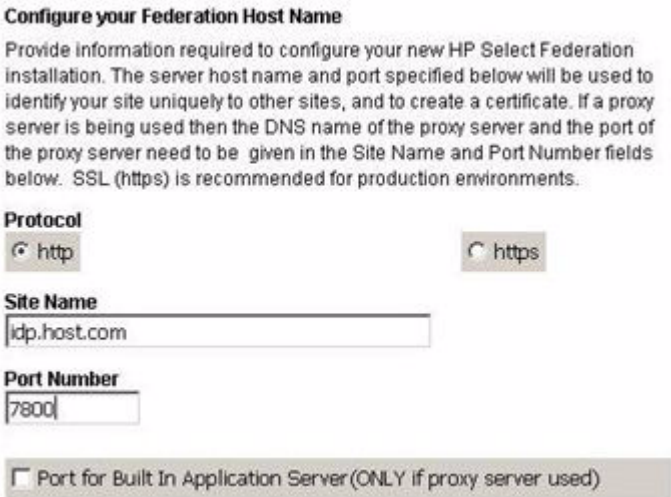


Notes on this data:

- **Company Name:** This is used to generate certificates and signing keys for Select Federation. This name must be an ASCII text string without special characters.
- **Keystore Password:** This will create and open the keyfile that stores the signing key. The password must be at least 6 characters long.

Procedure

Perform the following steps to install the Select Federation IDP instance.

Step	Action	✓
1	Start the installation by running the Select Federation install executable, <code>install.exe</code> , located on the CD.	
2	Read and select I accept the terms of the license agreement. → Next	
3	Enter a company name. → Next  This is used to generate certificates and signing keys for Select Federation. This name must be an ASCII text string without special characters.	
4	Choose Application Server as Built-in Application Server. → Next	
5	Select the Protocol. Enter the fully qualified Site Name. Enter the Port Number on which you want to run the server. Leave Port for built-in Application Server(ONLY if proxy server used) unchecked. → Next 	
6	Enter the keystore password twice. → Next	

Step	Action	✓
7	Enter or browse to the path where you will install Select Federation. → Next Where Would You Like to Install? <input type="text" value="C:\Program Files\HP>Select Federation"/> <input type="button" value="Restore Default Folder"/> <input type="button" value="Choose..."/>	
8	Select Derby (Built-in) database. → Next <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> Select the database you would like to use (no additional configuration is required if you use the HP Select Federation built-in database). </div> <input checked="" type="radio"/> Derby (Built-in) <input type="radio"/> Oracle <input type="radio"/> MS SQL	
9	Select IDP only as the site role for this instance of Select Federation. → Next <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> Choose a role for your site. Choosing a particular role will install features specific to that role, excluding the ones that are not required. </div> <input type="radio"/> SP only (all IDP functionality will be disabled) <input checked="" type="radio"/> IDP only (all SP functionality will be disabled) <input type="radio"/> Both IDP and SP <input type="radio"/> Federation Router <input type="radio"/> Federation Router and Local IDP	

Step	Action	✓
10	<p>Do not integrate Select Federation with Select Access. Leave Deploy HP Select Federation integrated with HP Select Access unchecked. → Next</p> <div data-bbox="483 422 1313 642" style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>Please select the check box if you want to deploy HP Select Federation and integrate it with an existing installation of HP Select Access.</p> </div> <p><input type="checkbox"/> Deploy HP Select Federation integrated with HP Select Access</p>	
11	<p>Select LDAPV3 as your Profile Service. → Next</p> <div data-bbox="483 835 1313 1056" style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>If you plan to have a profile server or attribute authority at your site, please specify the source of the profile information below. Note that the choices below are for the source of the profile information; whether the service is a SAML attribute authority or a Liberty Profile service is determined by the protocol used by the querying SP and by the namespace mapping of the profile parameters used in the query.</p> </div> <p><input type="radio"/> Active Directory</p> <p><input checked="" type="radio"/> LDAPv3</p> <p><input type="radio"/> I will not be configuring a profile service at this time</p>	

Step	Action	✓
12	<p>Configure your LDAP directory. → Next</p> <p>Configure LDAP Directory Enter the name or IP of the LDAP Directory Server, the administrative username and password, and if required, the Base DN (fixed component of the DN which is used to query the directory). If the Base DN input box is disabled, it means the base DN is not required at this time.</p> <p>Host <input type="text" value="ds.host.com"/></p> <p>Port <input type="text" value="400"/></p> <p>Login Name <input type="text" value="cn=Directory Manager"/></p> <p>Password <input type="password" value="*****"/></p> <p>Base DN <input type="text" value="dc=company,dc=com"/></p> <p><input type="checkbox"/> Connect to the directory server using SSL</p>	
13	<p>Enter the attribute name that maps to the user id in your Directory configuration.</p> <p>Check Enable sub tree search for directory. → Next</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>Additional Directory Configuration: Optionally configure some additional directory server parameters here. The first parameter is the name of attribute that contains the userid. This is prefixed to the userid and then concatenated to the base DN to form the full DN of the user object to be created. The checkbox can be selected to enable sub-tree searching for your directory.</p> </div> <p>The name of the attribute that would contain the user id <input type="text" value="uid"/></p> <p><input checked="" type="checkbox"/> Enable sub tree search for directory</p>	

Step	Action	✓
14	<p>Do not integrate with Select Audit. Leave Integrate HP Select Audit unchecked. → Next</p> <p>Integrate with HP Select Audit (optional) If you have HP Select Audit installed and would like to integrate it with HP Select Federation, specify the Select Audit Connector port number below (the value shown is the default). Otherwise, proceed to the next step in the installation.</p> <p><input type="checkbox"/> Integrate HP Select Audit</p> <p>Connector Port 9979</p>	
15	Verify that the installation information is correct. → Install	
16	<p>Select Done.</p> <p>A pop-up window opens asking if the browser needs to be launched. Select Yes.</p> <p>The Installer launches a Browser window to your site and closes. The Select Federation IDP instance has been installed.</p>	

3 Installing the Select Federation SP Instance

This chapter provides instructions for installing the Select Federation SP instance on the default Built-in Application Server using the Select Federation Derby Built-in database.



Be sure you install the SP instance on a different machine than the IDP instance.

Before You Begin

Gather the following information:

- Company Name
- Host Name where Select Federation will be run
- Port Number to use for the built-in application server
- Keystore password




Notes on this data:

- **Company Name:** This is used to generate certificates and signing keys for Select Federation. This name must be an ASCII text string without special characters.
- **Keystore Password:** This will create and open the keyfile that stores the signing key. The password must be at least 6 characters long.

Procedure

Perform the following steps to install the Select Federation SP instance.

Step	Action	✓
1	Start the installation by running the Select Federation install executable, <code>install.exe</code> , located on the CD.	
2	Read and select I accept the terms of the license agreement. → Next	
3	Enter a company name. → Next  This is used to generate certificates and signing keys for Select Federation. This name must be an ASCII text string without special characters.	
4	Choose Application Server as Built-in Application Server. → Next	

Step	Action	✓
5	<p>Select the Protocol.</p> <p>Enter the fully qualified Site Name.</p> <p>Enter the Port Number on which you want to run the server.</p> <p>Leave Port for built-in Application Server(ONLY if proxy server used) unchecked. → Next</p> <p>Configure your Federation Host Name</p> <p>Provide information required to configure your new HP Select Federation installation. The server host name and port specified below will be used to identify your site uniquely to other sites, and to create a certificate. If a proxy server is being used then the DNS name of the proxy server and the port of the proxy server need to be given in the Site Name and Port Number fields below. SSL (https) is recommended for production environments.</p> <p>Protocol</p> <p><input checked="" type="radio"/> http <input type="radio"/> https</p> <p>Site Name</p> <p><input type="text" value="sp.host.com"/></p> <p>Port Number</p> <p><input type="text" value="7801"/></p> <p><input type="checkbox"/> Port for Built In Application Server(ONLY if proxy server used)</p>	
6	Enter the keystore password twice. → Next	
7	<p>Enter or browse to the path where you will install Select Federation. → Next</p> <p>Where Would You Like to Install?</p> <p><input type="text" value="C:\Program Files\HP>Select Federation"/></p> <p><input type="button" value="Restore Default Folder"/> <input <="" p="" type="button" value="Choose..."/> </p>	

Step	Action	✓
8	<p>Select Derby (Built-in) database. → Next</p> <div data-bbox="488 331 1318 558" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Select the database you would like to use (no additional configuration is required if you use the HP Select Federation built-in database).</p> </div> <p> <input checked="" type="radio"/> Derby (Built-in) <input type="radio"/> Oracle <input type="radio"/> MS SQL </p>	
9	<p>Select SP only as the site role for this instance of Select Federation. → Next</p> <div data-bbox="488 869 1318 1096" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Choose a role for your site. Choosing a particular role will install features specific to that role, excluding the ones that are not required.</p> </div> <p> <input checked="" type="radio"/> SP only (all IDP functionality will be disabled) <input type="radio"/> IDP only (all SP functionality will be disabled) <input type="radio"/> Both IDP and SP <input type="radio"/> Federation Router <input type="radio"/> Federation Router and Local IDP </p>	
10	<p>Do not integrate Select Federation with Select Access. Leave Deploy HP Select Federation integrated with HP Select Access unchecked. → Next</p> <div data-bbox="488 1535 1318 1761" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Please select the check box if you want to deploy HP Select Federation and integrate it with an existing installation of HP Select Access.</p> </div> <p> <input type="checkbox"/> Deploy HP Select Federation integrated with HP Select Access </p>	

Step	Action	✓
11	<p>Do not integrate with Select Audit. Leave Integrate HP Select Audit unchecked. → Next</p> <p>Integrate with HP Select Audit (optional) If you have HP Select Audit installed and would like to integrate it with HP Select Federation, specify the Select Audit Connector port number below (the value shown is the default). Otherwise, proceed to the next step in the installation.</p> <p><input type="checkbox"/> Integrate HP Select Audit</p> <p>Connector Port 9979</p>	
12	Verify that the installation information is correct. → Install	
13	<p>Select Done.</p> <p>A pop-up window opens asking if the browser needs to be launched. Select Yes.</p> <p>The Installer launches a Browser window to your site and closes. The Select Federation SP instance has been installed.</p>	

4 Exchanging Metadata

Introduction

Metadata in a federation is a description of the Trusted Partner site with which you want to federate. Metadata is an online exact description of a site in a federation. The metadata 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 Select Federation, site configuration is done using the Administration Console. The Administration Console enables an administrator to publish the site's metadata as well as import other sites' metadata. To add Trusted Partner sites to your federation, both you and your Trusted Partner need to upload each other's metadata. Metadata exchange is mutual, so you need to ensure that the other site has added your metadata to its federation.

There are two ways to get data from your Partners:

- If the Partner's metadata file is available, download it from a well-known URL or obtain the metadata securely from the administrator of the Partner. See “Adding a Partner for which Metadata is Available” in the *HP Select Federation Configuration and Administration Guide*.
- If a metadata file or download is NOT available, see “Adding a Partner for Which Metadata is Not Available” in the *HP Select Federation Configuration and Administration Guide*.

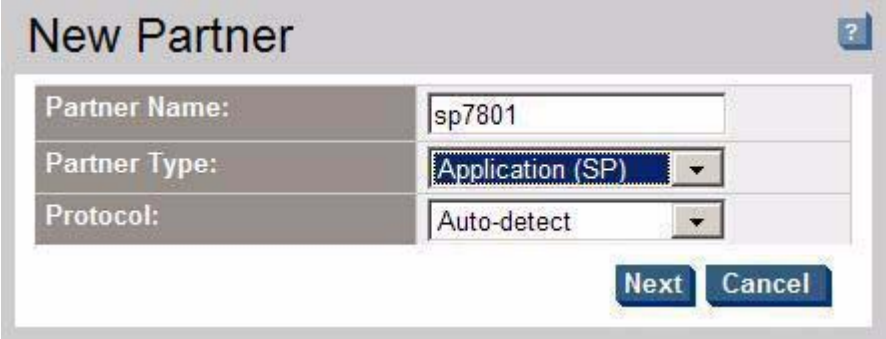
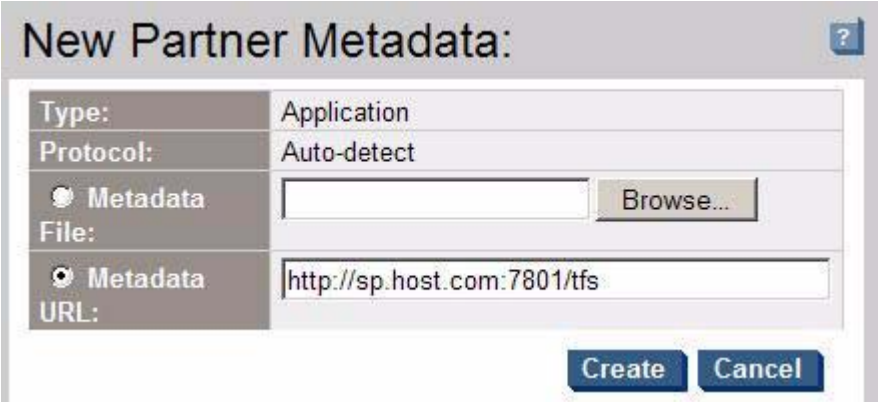
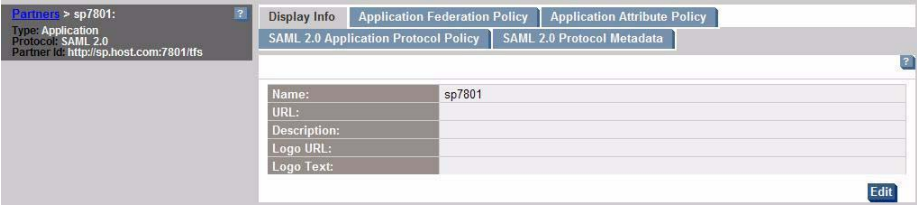
The following sections describe how to download the metadata from a URL:

- [Downloading the SP's Metadata into the IDP Site](#)
- [Downloading the IDP's Metadata into the SDP Site](#)

Downloading the SP's Metadata into the IDP Site

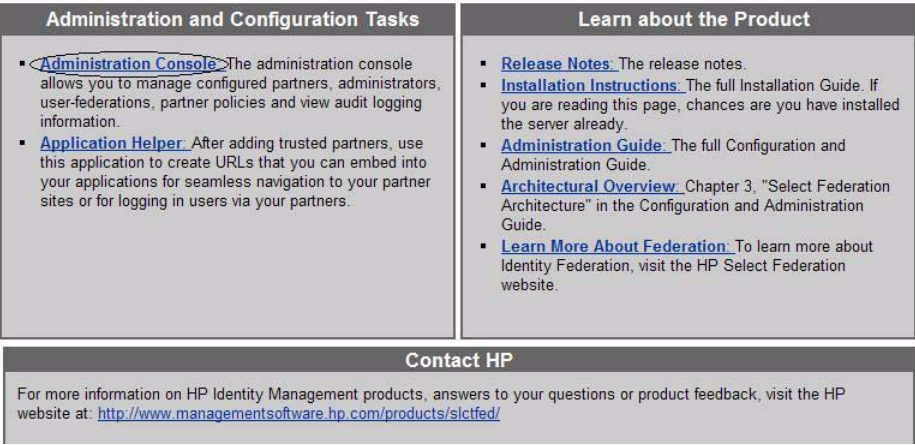
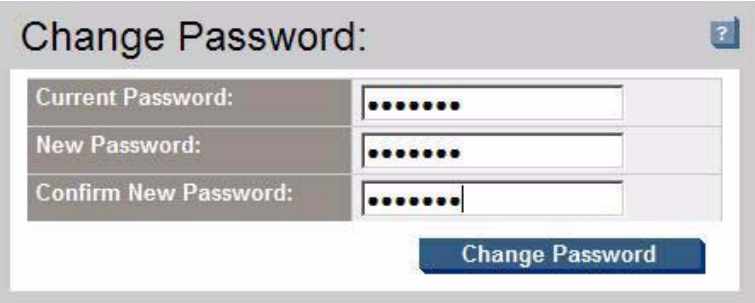
Perform the following steps to download the SP's metadata into the IDP site.

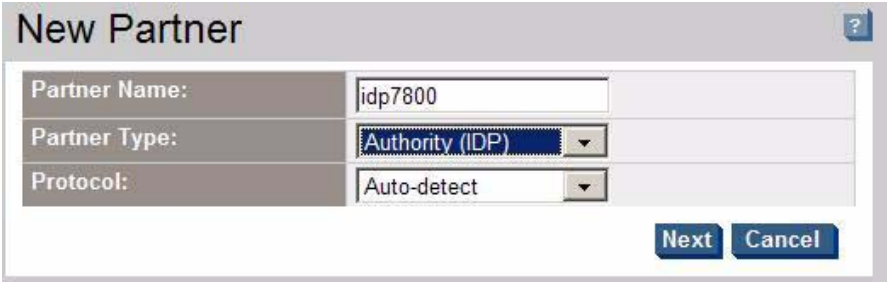
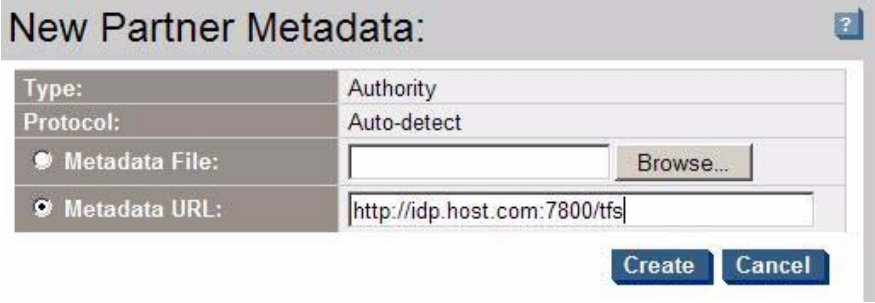
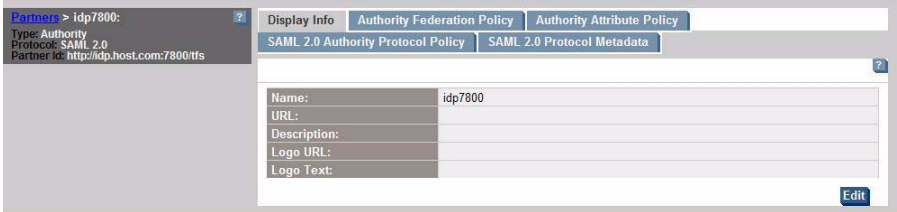
Step	Action	✓						
1	<p>Open the Select Federation Administration Console startup page at http://<base-url>/tfs-internal.</p> <p>Replace <base-url> with your <code>hostname:port</code>.</p> <p>Click on Administration Console to open the Administration Console login page.</p> <div data-bbox="462 672 1372 1113" style="border: 1px solid gray; padding: 5px;"> <table border="0" style="width: 100%;"> <tr> <td style="width: 50%; vertical-align: top;"> <p>Administration and Configuration Tasks</p> <ul style="list-style-type: none"> ▪ Administration Console The administration console allows you to manage configured partners, administrators, user-federations, partner policies and view audit logging information. ▪ Application Helper After adding trusted partners, use this application to create URLs that you can embed into your applications for seamless navigation to your partner sites or for logging in users via your partners. </td> <td style="width: 50%; vertical-align: top;"> <p>Learn about the Product</p> <ul style="list-style-type: none"> ▪ Release Notes The release notes. ▪ Installation Instructions The full Installation Guide. If you are reading this page, chances are you have installed the server already. ▪ Administration Guide The full Configuration and Administration Guide. ▪ Architectural Overview Chapter 3, "Select Federation Architecture" in the Configuration and Administration Guide. ▪ Learn More About Federation To learn more about Identity Federation, visit the HP Select Federation website. </td> </tr> <tr> <td colspan="2" style="text-align: center; background-color: #f0f0f0;"> <p>Contact HP</p> <p>For more information on HP Identity Management products, answers to your questions or product feedback, visit the HP website at: http://www.managementsoftware.hp.com/products/slctfed/</p> </td> </tr> </table> </div>	<p>Administration and Configuration Tasks</p> <ul style="list-style-type: none"> ▪ Administration Console The administration console allows you to manage configured partners, administrators, user-federations, partner policies and view audit logging information. ▪ Application Helper After adding trusted partners, use this application to create URLs that you can embed into your applications for seamless navigation to your partner sites or for logging in users via your partners. 	<p>Learn about the Product</p> <ul style="list-style-type: none"> ▪ Release Notes The release notes. ▪ Installation Instructions The full Installation Guide. If you are reading this page, chances are you have installed the server already. ▪ Administration Guide The full Configuration and Administration Guide. ▪ Architectural Overview Chapter 3, "Select Federation Architecture" in the Configuration and Administration Guide. ▪ Learn More About Federation To learn more about Identity Federation, visit the HP Select Federation website. 	<p>Contact HP</p> <p>For more information on HP Identity Management products, answers to your questions or product feedback, visit the HP website at: http://www.managementsoftware.hp.com/products/slctfed/</p>				
<p>Administration and Configuration Tasks</p> <ul style="list-style-type: none"> ▪ Administration Console The administration console allows you to manage configured partners, administrators, user-federations, partner policies and view audit logging information. ▪ Application Helper After adding trusted partners, use this application to create URLs that you can embed into your applications for seamless navigation to your partner sites or for logging in users via your partners. 	<p>Learn about the Product</p> <ul style="list-style-type: none"> ▪ Release Notes The release notes. ▪ Installation Instructions The full Installation Guide. If you are reading this page, chances are you have installed the server already. ▪ Administration Guide The full Configuration and Administration Guide. ▪ Architectural Overview Chapter 3, "Select Federation Architecture" in the Configuration and Administration Guide. ▪ Learn More About Federation To learn more about Identity Federation, visit the HP Select Federation website. 							
<p>Contact HP</p> <p>For more information on HP Identity Management products, answers to your questions or product feedback, visit the HP website at: http://www.managementsoftware.hp.com/products/slctfed/</p>								
2	<p>Change the default system password .</p> <p>The default Admin account is <code>admin</code> and the default password is <code>tgadmin</code>.</p> <div data-bbox="479 1260 1226 1564" style="border: 1px solid gray; padding: 10px; background-color: #f0f0f0;"> <p>Change Password: ?</p> <table border="0" style="width: 100%;"> <tr> <td style="width: 40%;">Current Password:</td> <td><input type="password" value="....."/></td> </tr> <tr> <td>New Password:</td> <td><input type="password" value="....."/></td> </tr> <tr> <td>Confirm New Password:</td> <td><input type="password" value="....."/></td> </tr> </table> <p style="text-align: center;">Change Password</p> </div>	Current Password:	<input type="password" value="....."/>	New Password:	<input type="password" value="....."/>	Confirm New Password:	<input type="password" value="....."/>	
Current Password:	<input type="password" value="....."/>							
New Password:	<input type="password" value="....."/>							
Confirm New Password:	<input type="password" value="....."/>							
3	<p>Select Partners → Manage Partners.</p> <p>The Partners page opens.</p>							
4	<p>Click the New Partner button.</p> <p>The New Partner page opens.</p>							

Step	Action	✓
5	Enter the Partner Name , Partner Type and Protocol on the New Partner page. → Next 	
6	Click Metadata URL and enter the metadata URL → Create 	
7	The SP Partner information has been registered at the IDP Site. 	

Downloading the IDP's Metadata into the SDP Site

Perform the following steps to download the IDP's metadata into the SP site.

Step	Action	✓
1	<p>Open the Select Federation Administration Console startup page at <a href="http://<base-url>/tfs-internal">http://<base-url>/tfs-internal.</p> <p>Click on Administration Console to open the Administration Console login page.</p> 	
2	<p>Change the default system password.</p> <p>The default Admin account is admin and the default password is tgadmin.</p> 	
3	<p>Select Partners → Manage Partners.</p> <p>The Partners page opens.</p>	
4	<p>Click the New Partner button.</p> <p>The New Partner page opens.</p>	

Step	Action	✓
5	Enter the Partner Name , Partner Type and Protocol on the New Partner page. → Next 	
6	Click Metadata URL and enter the metadata URL → Create 	
7	The IDP Partner information has been registered at the SP Site. 	

5 Using the Demonstration Program

Introduction

Demo Application is a J2EE application that demonstrates federated single sign-on and other capabilities provided by Select Federation. The Demo Application is bundled with Select Federation. The Demonstration program can also serve as sample code, which you can use to enable your own applications.

You can navigate to the Demonstration program using the following address at the top-level URL: **<base-url>/sf-demo**

The Demo application consists of two parts:

- Identity Provider Demo
- Service Provider Demo

The out-of-box demo application focuses on two concepts:

- **Identity Federation:** The act of linking a user's account at an IDP to the user's account at an SP. An opaque identifier (called federated id) generated by IDP for that particular user and that particular SP. IDP and SP map federated id to local ids.
- **Federation Termination:** Also known as Single Logout (SLO) is the act of de-linking the accounts, users terminated in the home domain lose access to all the common applications.

This chapter provides the following Demo use cases:

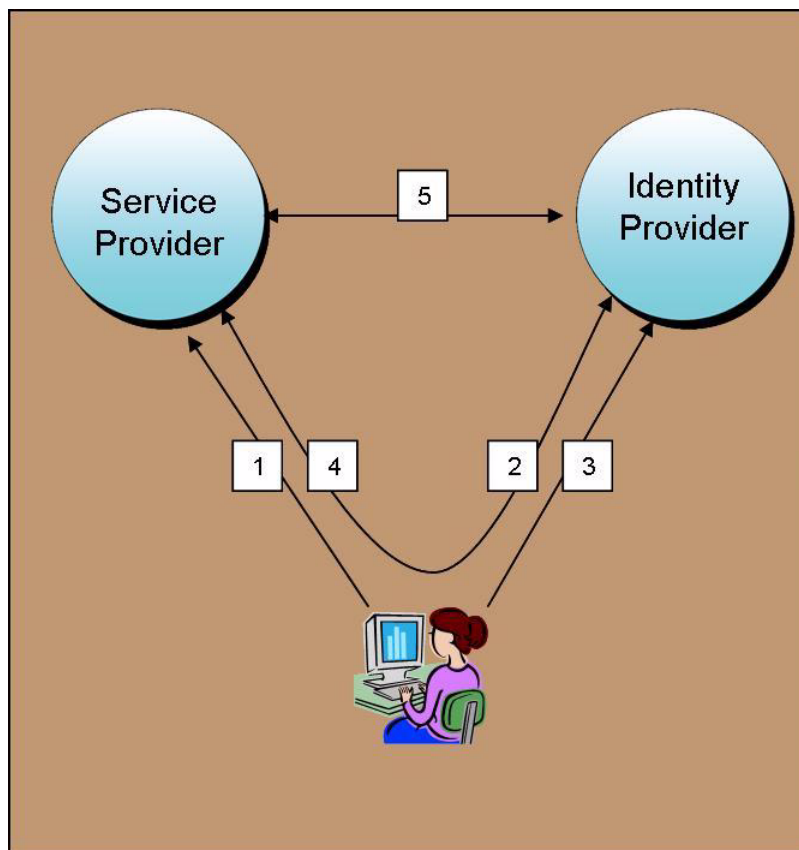
- SP initiated federation
- IDP initiated federation
- SP initiated single log-out
- IDP initiated single log-out

The Demo application pages are color coded. All SP functionality is shown with orange colored headers and all IDP functionality with green colored headers. Functionality that is shared by both IDP and SP is in neutral colors. Demo application uses pseudonyms as the name federation policy. For details on Name Federation Policy, see the *HP Select Federation Configuration and Administration Guide*.

SP-Initiated Federation

How an SP-Initiated Federation Works

Figure 1 SP-Initiated Federation Flow with an SP-Initiated SSO

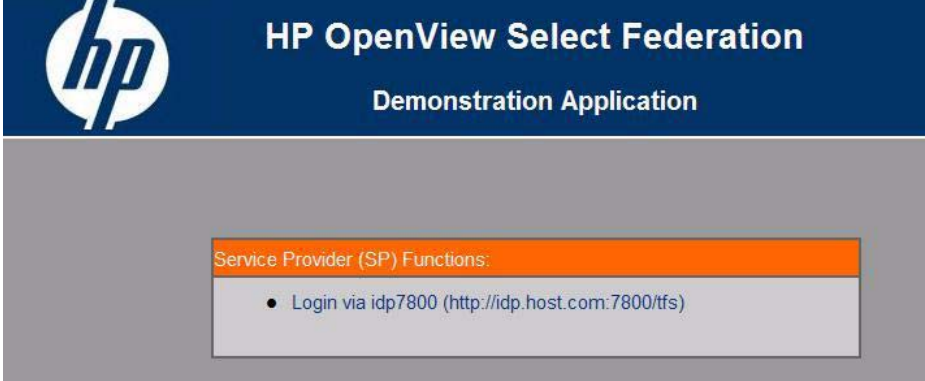



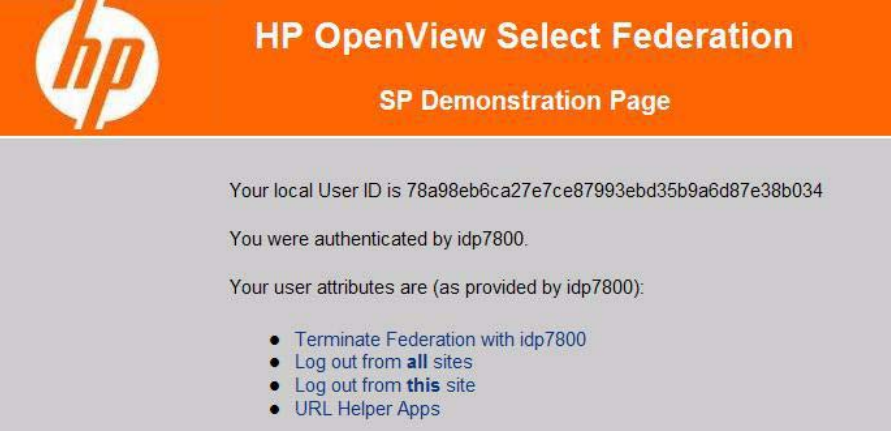
Following is a step-by-step explanation of this diagram:

- 1 User attempts to access SP SF-Demo application and is prompted to federate.
- 2 User selects the IDP from the list of IDPs and user is redirected to IDP.
- 3 User logs in at IDP.
- 4 IDP generates federated ID and redirects user back to SP.
- 5 SP picks up federated ID from artifact at IDP using a back-channel.
- 6 User accesses service at SP as federated user.

Procedure

Perform the following steps to create an SP-initiated federation.

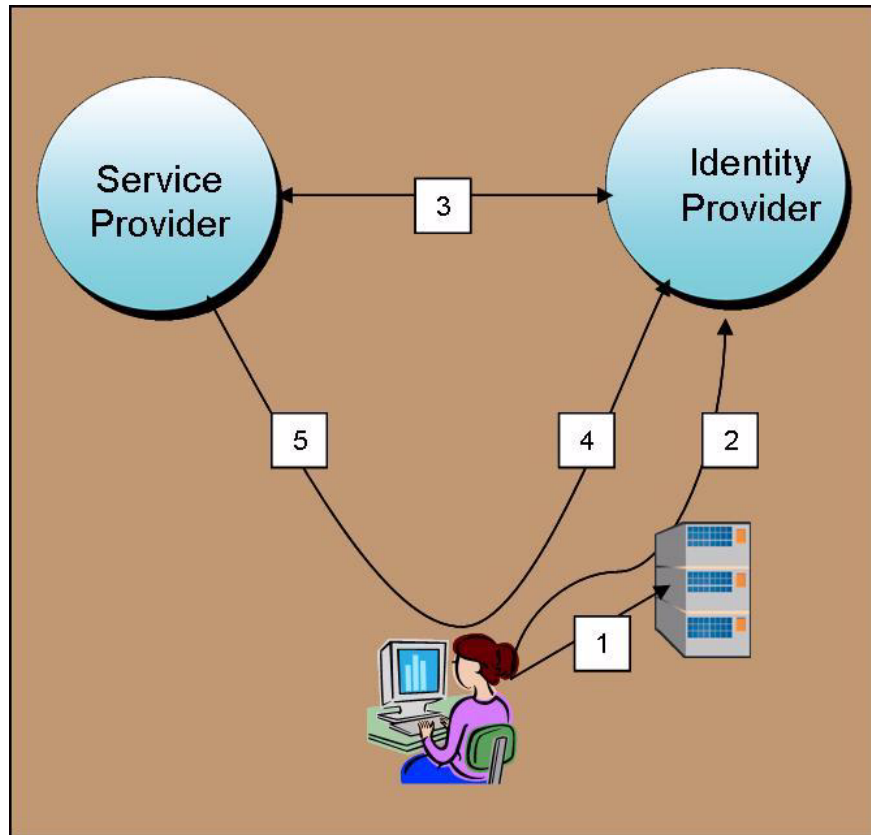
Step	Action	✓
1	<p>In a Browser window, access the sf-demo application. For example: http://sp.host.com:7801/sf-demo.</p> 	
2	Click on login via idp .	

Step	Action	✓
3	<p>You are redirected to an IDP for authentication.</p> 	
4	<p>Enter your credentials (Account and Password) and click Login.</p> <p>The credentials are validated against the LDAP directory you configured for the IDP.</p>	
5	<p>The SP Demo page opens. This page provides links for you to Terminate federation, logout from all sites (single logout) or logout from the SP site only.</p> <p>The SP Initiated federation is complete.</p> 	

IDP-Initiated Federation

How an IDP-Initiated Federation Works

Figure 2 IDP-Initiated Federation Flow.

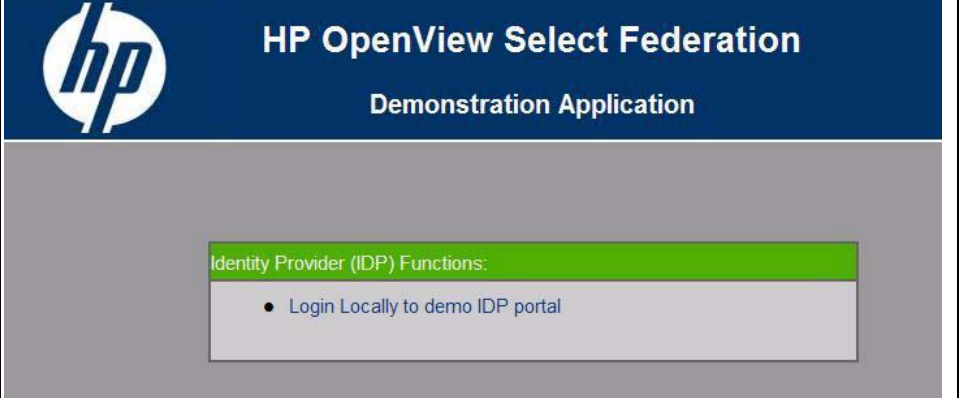
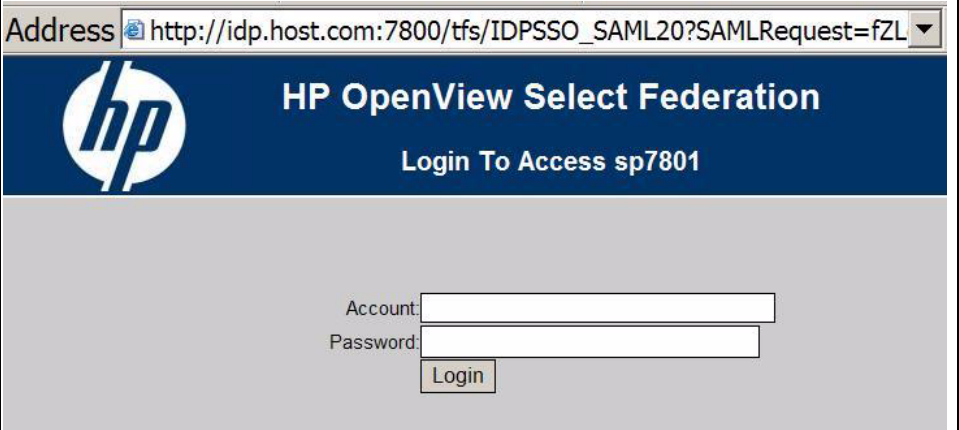


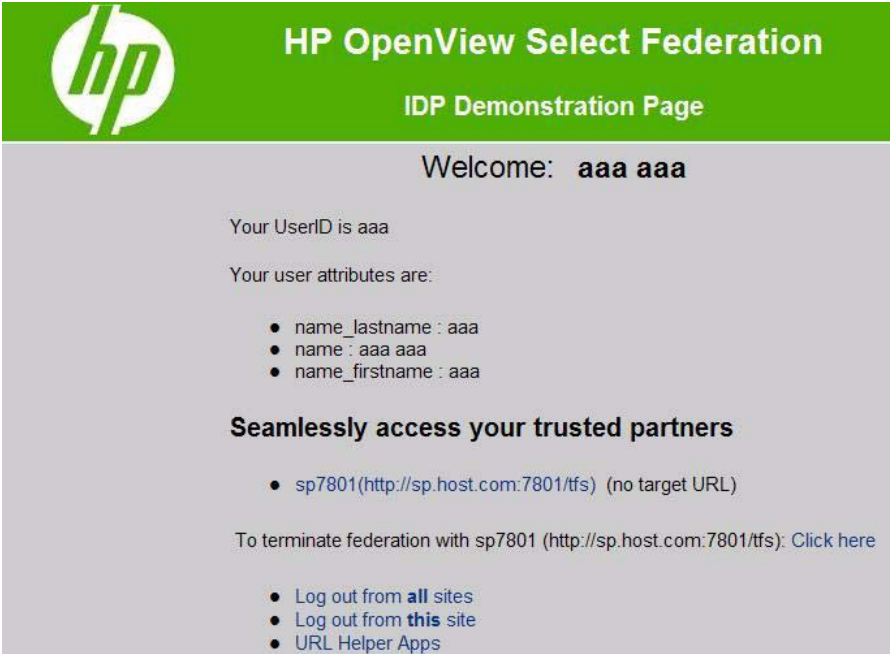

Following is a step-by-step explanation of what is happening in an IDP-Initiated SSO:

- 1 User logs in locally at an IDP site.
- 2 User selects a “federated” link to access the federated SP site and is sent to the IDP first
- 3 IDP verifies the user authentication and authenticates to the SP to obtain token for user.
- 4 IDP generates federated ID and redirects user to SP.
 - Signed assertions
 - Artifact reference
- 5 User accesses service at SP as federated user.

Procedure

Perform the following steps to create an IDP-initiated federation.

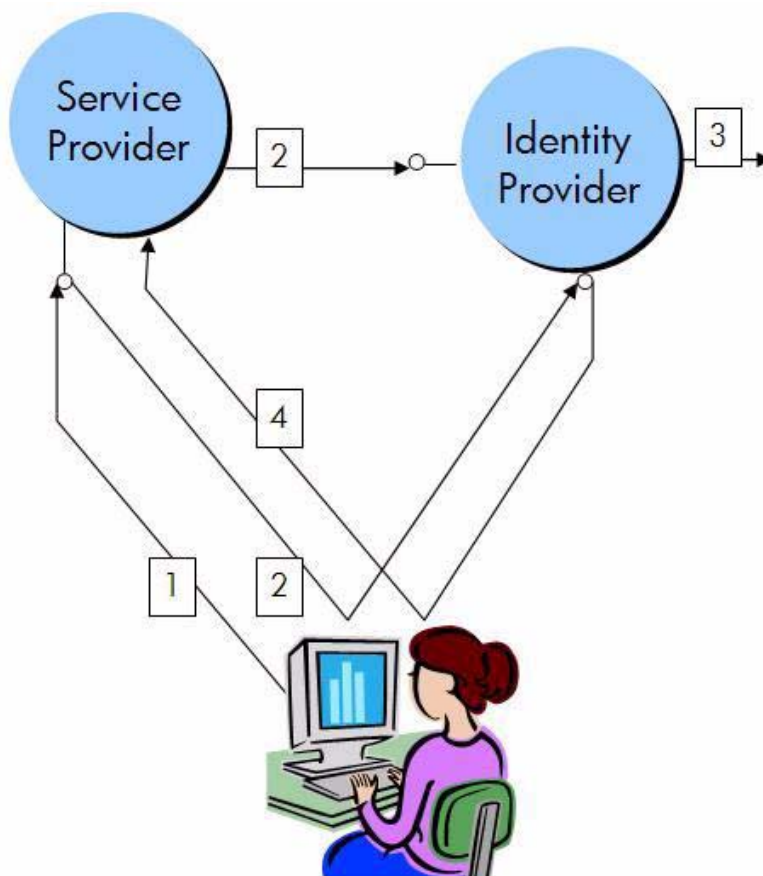
Step	Action	✓
1	<p>In a Browser window, access the sf-demo application. For example: http://idp.host.com:7800/sf-demo.</p> 	
2	Click on Login Locally to demo IDP portal.	
3	<p>A login page opens.</p> 	

Step	Action	✓
4	<p>Enter your credentials (Account and Password) and click Login.</p> <p>The credentials are validated against the LDAP directory you configured for the IDP.</p>	
5	<p>The IDP Demo page opens. This page provides links for you to access your Trusted Partners, logout from all sites (Single Logout) or log out from the IDP site.</p> 	
6	<p>Click on your Trusted Partner link to access your SP Demo page.</p> <p>The IDP-initiated federation is complete</p> 	

SP-Initiated Single Logout

How an SP-Initiated Single Logout Works

Figure 3 SP-Initiated Single Logout Flow.


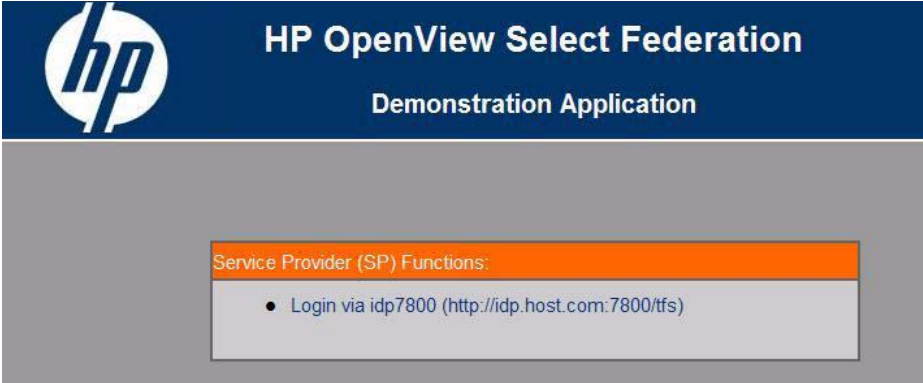


Following is a step-by-step explanation of this diagram:

- 1 User requests global logout at SP
- 2 Using redirect, SP initiates the single logout at the IDP. (SP can initiate a logout using various mechanism, please check the configuration guide for the different options)
- 3 IDP initiates single logout at other SPs (either using GET, redirects or using the SOAP service)
- 4 IDP redirects user back to Single Logout Return URL at originating SP.

Procedure

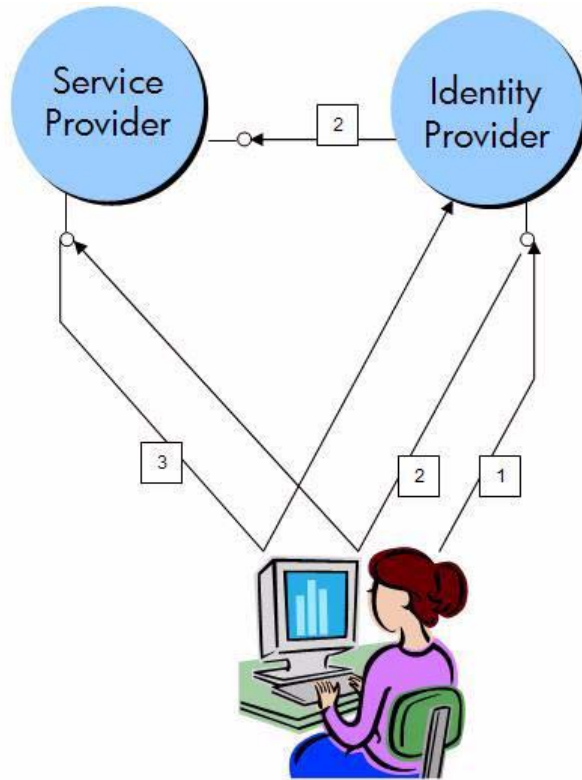
Perform the following steps to create an SP-initiated Single Logout:

Step	Action	✓
1	<p>Click on Log out from all sites, on your SP application.</p>  <p>The screenshot shows the HP OpenView Select Federation SP Demonstration Page. It features the HP logo on the left and the title 'HP OpenView Select Federation' and 'SP Demonstration Page' on the right. Below the title, it displays the local User ID: 78a98eb6ca27e7ce87993ebd35b9a6d87e38b034. It states 'You were authenticated by idp7800.' and 'Your user attributes are (as provided by idp7800):'. A list of actions is provided: Terminate Federation with idp7800, Log out from all sites, Log out from this site, and URL Helper Apps.</p>	
2	<p>The Demo start page opens when Single Logout is performed.</p>  <p>The screenshot shows the HP OpenView Select Federation Demonstration Application. It features the HP logo on the left and the title 'HP OpenView Select Federation' and 'Demonstration Application' on the right. Below the title, there is a section titled 'Service Provider (SP) Functions:' with a list of functions: Login via idp7800 (http://idp.host.com:7800/tfs).</p>	

IDP-Initiated Single Logout

How an IDP-Initiated Single Logout Works

Figure 4 IDP-Initiated Single Logout Flow.


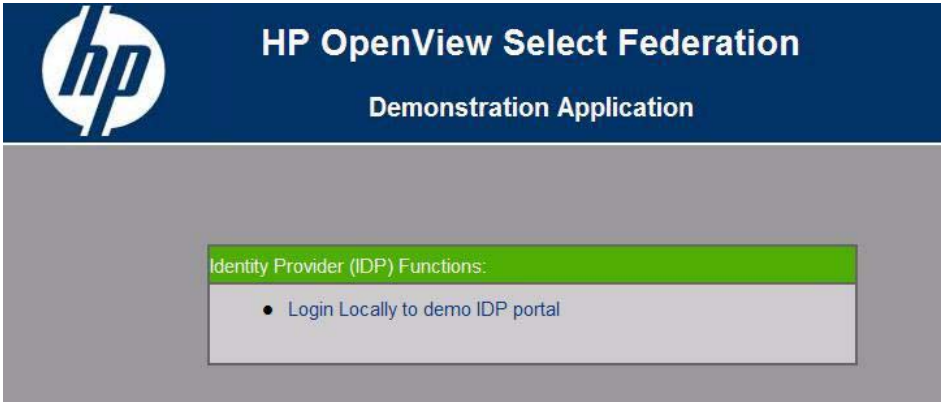


Following is a step-by-step explanation of this diagram:

- 1 User requests global logout at the IDP Site.
- 2 For each SP that the user is logged onto, the IDP initiates a redirect based logout.
- 3 If using a redirect based logout, the SP logs out the user and redirects the user back to the Single Logout Return URL at the IDP.

Procedure

Perform the following steps to create an IDP-initiated Single Logout:

Step	Action	✓
1	<p>Click on Log out from all sites, on your IDP application.</p> 	
2	<p>The Demo start page opens when Single Logout is performed.</p> 	

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 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.

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 \(WSP\)](#).

