

# HP Select Federation

For the Windows® and Linux operating systems

Software Version: 7.01

---

## Quick Start Guide

Document Release Date: March 2008  
Software Release Date: March 2008



## Legal Notices

### Warranty

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

The information contained herein is subject to change without notice.

### Restricted Rights Legend

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

### Copyright Notices

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

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

- Apache Derby, Apache Xalan Library, Apache Xerces Library, and Apache XML Dsig Library.
- Software developed by the Waveset Technologies, Inc. ([www.waveset.com](http://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://h20230.www2.hp.com/selfsolve/manuals>**

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

The following table indicates changes made to this document since the last released edition.

### Changes to this Document

Chapter	Changes
All chapters	Added the Red Hat Linux operating system-specific information where applicable.
Documentation Updates	Updated the documentation URL.
Support	Updated this section's information and URLs.
Chapter 2, Installing the Select Federation IDP Instance	<ul style="list-style-type: none"><li>• Changed the installation to an HTTPS installation.</li><li>• In step 1, changed the Windows executable from <code>install.exe</code> to <code>installSF.exe</code>.</li></ul>
Chapter 3, Installing the Select Federation SP Instance	<ul style="list-style-type: none"><li>• Changed the installation to an HTTPS installation.</li><li>• In step 1, changed the Windows executable from <code>install.exe</code> to <code>installSF.exe</code>.</li></ul>
Chapter 4, Exchanging Metadata	<ul style="list-style-type: none"><li>• Added server certificate transfer sections:<ul style="list-style-type: none"><li>— <a href="#">Adding the SP Site's Server Certificate to the IDP's Trust Store</a> on page 24.</li><li>— <a href="#">Adding the IDP Site's Server Certificate to the SP's Trust Store</a> on page 29.</li></ul></li><li>• Changed the section heading "Downloading the IDP's Metadata into the SDP Site" to <a href="#">Downloading the IDP's Metadata into the SP Site</a> on page 34.</li></ul>
Chapter 5, Using the Demonstration Application	<ul style="list-style-type: none"><li>• Updated the explanation of Figure 1 in <a href="#">How an SP-Initiated Federation Works</a> on page 38.</li><li>• Updated the screen shots in each section to reflect the HTTPS installation.</li></ul>

## Support

You can visit the HP Software Support web site at:

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

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

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

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

To find more information about access levels, go to:

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

For more information about HP Passport, go to:

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

# Contents

<b>1</b>	<b>Introduction</b> .....	7
	About This Guide .....	7
	Prerequisites .....	7
	Software Requirements .....	7
	Hardware Recommended Specifications .....	7
	Using this Guide .....	8
<b>2</b>	<b>Installing the Select Federation IDP Instance</b> .....	9
	Before You Begin .....	9
	Procedure .....	10
<b>3</b>	<b>Installing the Select Federation SP Instance</b> .....	17
	Before You Begin .....	17
	Procedure .....	18
<b>4</b>	<b>Exchanging Metadata</b> .....	23
	Introduction .....	23
	Adding the SP Site's Server Certificate to the IDP's Trust Store .....	24
	Adding the IDP Site's Server Certificate to the SP's Trust Store .....	29
	Downloading the SP's Metadata into the IDP Site .....	32
	Downloading the IDP's Metadata into the SP Site .....	34
<b>5</b>	<b>Using the Demonstration Application</b> .....	37
	Introduction .....	37
	SP-Initiated Federation .....	38
	How an SP-Initiated Federation Works .....	38
	Procedure .....	39
	IDP-Initiated Federation .....	41
	How an IDP-Initiated Federation Works .....	41
	Procedure .....	42
	SP-Initiated Single Logout .....	44
	How an SP-Initiated Single Logout Works .....	44
	Procedure .....	45
	IDP-Initiated Single Logout .....	46
	How an IDP-Initiated Single Logout Works .....	46
	Procedure .....	47
	<b>Glossary</b> .....	49
	<b>Index</b> .....	59



# 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 or Red Hat Linux AS, version 3.0 Update 5 and 4.0
- Select Federation 7.00
- 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

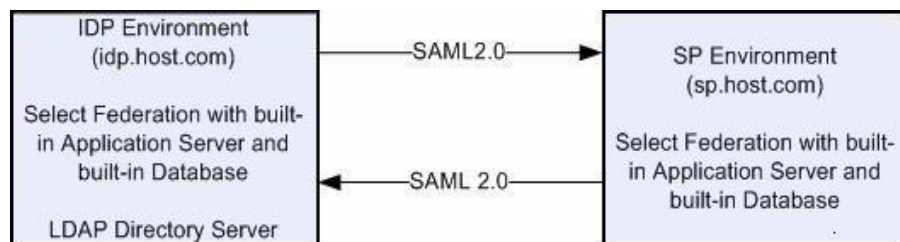
This guide walks you through the following procedures:



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 and Red Hat Linux AS, version 3.0 Update 5 and 4.0 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 and Red Hat Linux AS, version 3.0 Update 5 and 4.0 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 Application](#) — 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:


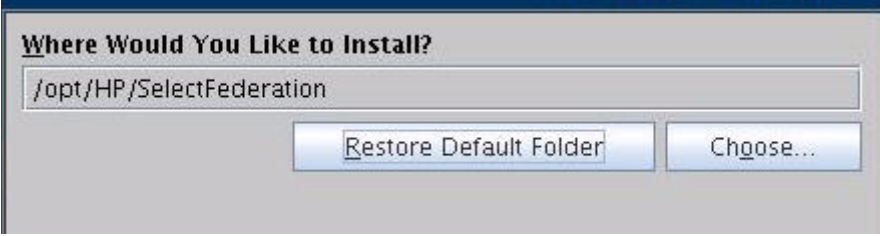
- **Company Name:** This is used to generate certificates and signing keys for Select Federation. This name must be an ASCII text string without special characters.
- **Keystore Password:** This creates and opens the key file that stores the signing key. The password must be at least 6 characters long.

## Procedure

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

<b>Step</b>	<b>Action</b>	✓
<b>1</b>	Start the installation by running the Select Federation install executable located on the CD: <ul style="list-style-type: none"><li>• For Windows: <code>installSF.exe</code></li><li>• For Linux: <code>installSF.bin</code></li></ul>	
<b>2</b>	Read and select <b>I accept the terms of the license agreement.</b> → <b>Next</b>	
<b>3</b>	Enter a company name. → <b>Next</b>   This is used to generate certificates and signing keys for Select Federation. This name must be an ASCII text string without special characters.	
<b>4</b>	Choose <b>Application Server as Built-in Application Server.</b> → <b>Next</b>	

Step	Action	✓
5	<p>Configure your federation host name:</p> <ul style="list-style-type: none"> <li>a Select the <b>Protocol</b>.</li> <li>b Enter the fully qualified <b>Site Name</b>.</li> <li>c Enter the <b>Port Number</b> on which you want to run the server.</li> <li>d Leave <b>Port for built-in Application Server(ONLY if proxy server used)</b> unchecked.</li> <li>e Click <b>Next</b>.</li> </ul> <div data-bbox="477 621 1276 1285" style="border: 1px solid gray; padding: 10px; background-color: #f0f0f0;"> <p><b>Configure your Federation Host Name</b></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 using Websphere or Weblogic enter the port number used by the profile(websphere) or domain(weblogic) on which Select Federation will be deployed. 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><b>Protocol</b></p> <p><input type="radio"/> http <input checked="" type="radio"/> https</p> <p><b>Site Name</b></p> <p>idp.host.com</p> <p><b>Port Number</b></p> <p>7800</p> <p><input type="checkbox"/> Port for Built In Application Server(ONLY if proxy server used)</p> </div>	
6	Enter the keystore password twice. → <b>Next</b>	

Step	Action	✓
7	<p>Enter or browse to the path where you will install Select Federation. → <b>Next</b></p> <p>Windows example:</p>  <p>Linux example:</p> 	
8	<p>Select <b>Derby (Built-in)</b> database. → <b>Next</b></p> <div data-bbox="492 1010 1321 1234" style="border: 1px solid gray; 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>	

Step	Action	✓
9	<p>Select <b>IDP only</b> as the site role for this instance of Select Federation. → <b>Next</b></p> <div data-bbox="488 331 1318 554" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <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 type="radio"/> SP only (all IDP functionality will be disabled)  <input checked="" type="radio"/> <b>IDP only (all SP functionality will be disabled)</b>  <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 <b>Deploy HP Select Federation integrated with HP Select Access</b> unchecked.  → <b>Next</b></p> <div data-bbox="483 1018 1313 1241" style="border: 1px solid black; 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 <b>LDAPV3</b> as your Profile Service. → <b>Next</b></p> <div data-bbox="488 1434 1318 1656" style="border: 1px solid black; 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  <input checked="" type="radio"/> <b>LDAPV3</b>  <input type="radio"/> I will not be configuring a profile service at this time </p>	

Step	Action	✓
12	<p>Configure your LDAP directory. → <b>Next</b></p> <p><b>Configure LDAP Directory</b>  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><b>Host</b>  <input type="text" value="ds.host.com"/></p> <p><b>Port</b>  <input type="text" value="400"/></p> <p><b>Login Name</b>  <input type="text" value="cn=Directory Manager"/></p> <p><b>Password</b>  <input type="password" value="*****"/></p> <p><b>Base DN</b>  <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 <b>Enable sub tree search for directory</b>. → <b>Next</b></p> <div data-bbox="483 1312 1317 1539" style="border: 1px solid gray; padding: 5px;"> <p><b>Additional Directory Configuration:</b>  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"/> <b>Enable sub tree search for directory</b></p>	

<b>Step</b>	<b>Action</b>	✓
<b>14</b>	<p>Do not integrate with Select Audit.            Leave <b>Integrate HP Select Audit</b> unchecked. → <b>Next</b></p> <p><b>Integrate with HP Select Audit (optional)</b>            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><b>Connector Port</b>            9979</p>	
<b>15</b>	Verify that the installation information is correct. → <b>Install</b>	
<b>16</b>	<p>Select <b>Done</b>.</p> <p>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.

<b>Step</b>	<b>Action</b>	✓
1	Start the installation by running the Select Federation install executable located on the CD: <ul style="list-style-type: none"><li>• For Windows: <code>installSF.exe</code></li><li>• For Linux: <code>installSF.bin</code></li></ul>	
2	Read and select <b>I accept the terms of the license agreement.</b> → <b>Next</b>	
3	Enter a company name. → <b>Next</b>   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 <b>Application Server as Built-in Application Server.</b> → <b>Next</b>	

Step	Action	✓
5	<p>Configure your federation host name:</p> <ul style="list-style-type: none"> <li>a Select the <b>Protocol</b>.</li> <li>b Enter the fully qualified <b>Site Name</b>.</li> <li>c Enter the <b>Port Number</b> on which you want to run the server.</li> <li>d Leave <b>Port for built-in Application Server(ONLY if proxy server used)</b> unchecked.</li> <li>e Click <b>Next</b>.</li> </ul> <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p><b>Configure your Federation Host Name</b></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 using Websphere or Weblogic enter the port number used by the profile(websphere) or domain(weblogic) on which Select Federation will be deployed. 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><b>Protocol</b></p> <p><input type="radio"/> http <span style="margin-left: 200px;"><input checked="" type="radio"/> https</span></p> <p><b>Site Name</b></p> <p><input type="text" value="sp.host.com"/></p> <p><b>Port Number</b></p> <p><input type="text" value="7801"/></p> <p><input type="checkbox"/> <b>Port for Built In Application Server(ONLY if proxy server used)</b></p> </div>	
6	Enter the keystore password twice. → <b>Next</b>	

Step	Action	✓
7	<p>Enter or browse to the path where you will install Select Federation. → <b>Next</b></p> <p>Windows example:</p> <div data-bbox="483 380 1317 520"> <p><b>Where Would You Like to Install?</b></p> <p>C:\Program Files\HP&gt;Select Federation</p> <p>Restore Default Folder Choose...</p> </div> <p>Linux example:</p> <div data-bbox="480 632 1352 865"> <p><b>Where Would You Like to Install?</b></p> <p>/opt/HP/SelectFederation</p> <p>Restore Default Folder Choose...</p> </div>	
8	<p>Select <b>Derby (Built-in)</b> database. → <b>Next</b></p> <div data-bbox="492 1020 1320 1243"> <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>	

<b>Step</b>	<b>Action</b>	✓
<b>9</b>	<p>Select <b>SP only</b> as the site role for this instance of Select Federation. → <b>Next</b></p> <div data-bbox="485 338 1313 562" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <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> <ul style="list-style-type: none"> <li><input checked="" type="radio"/> SP only (all IDP functionality will be disabled)</li> <li><input type="radio"/> IDP only (all SP functionality will be disabled)</li> <li><input type="radio"/> Both IDP and SP</li> <li><input type="radio"/> Federation Router</li> <li><input type="radio"/> Federation Router and Local IDP</li> </ul>	
<b>10</b>	<p>Do not integrate Select Federation with Select Access.</p> <p>Leave <b>Deploy HP Select Federation integrated with HP Select Access</b> unchecked. → <b>Next</b></p> <div data-bbox="485 999 1313 1224" style="border: 1px solid black; 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>	

<b>Step</b>	<b>Action</b>	✓
<b>11</b>	<p>Do not integrate with Select Audit.  Leave <b>Integrate HP Select Audit</b> unchecked. → <b>Next</b></p> <p><b>Integrate with HP Select Audit (optional)</b>  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><b>Connector Port</b>  9979</p>	
<b>12</b>	Verify that the installation information is correct. → <b>Install</b>	
<b>13</b>	<p>Select <b>Done</b>.</p> <p>The Select Federation SP instance has been installed.</p>	

# 4 Exchanging Metadata

## Introduction

Metadata in a federation is an online exact description of the Trusted Partner site with which you want to federate. 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 get 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*.

In this chapter, you will download each Partner's metadata from a URL. But, before you exchange metadata, you need to add each Partner's server certificate to the Trusted Partner's trust store. To do this, you will use the Certificate Management Tool (CMT) that is bundled with Select Federation.

The following sections describe the process of exchanging metadata from a URL:

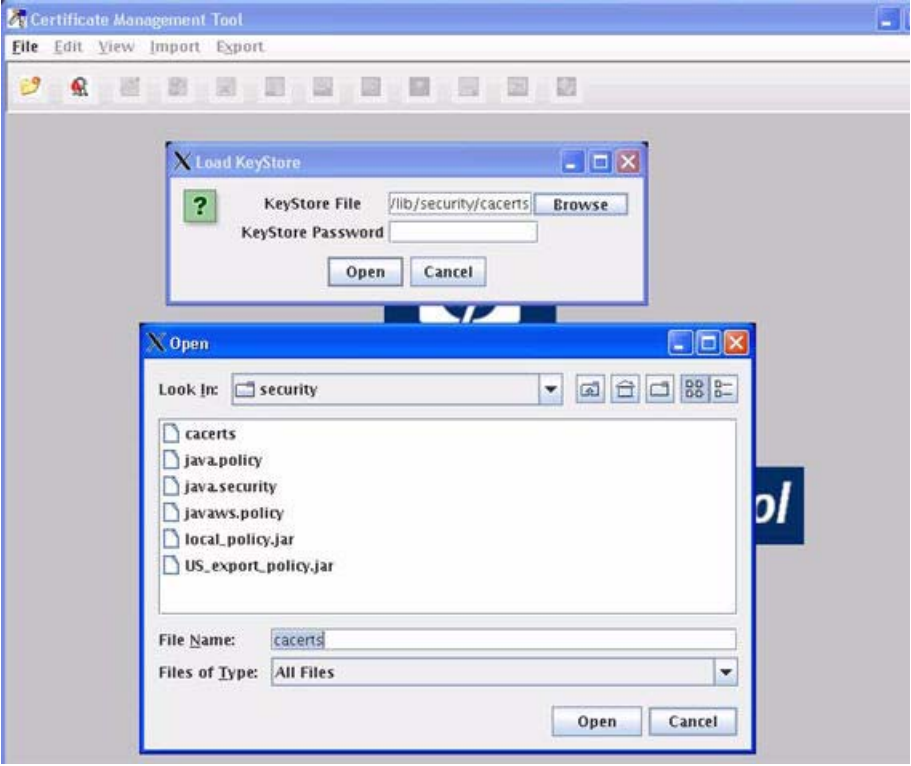
- [Adding the SP Site's Server Certificate to the IDP's Trust Store](#)
- [Adding the IDP Site's Server Certificate to the SP's Trust Store](#)
- [Downloading the SP's Metadata into the IDP Site](#)
- [Downloading the IDP's Metadata into the SP Site](#)

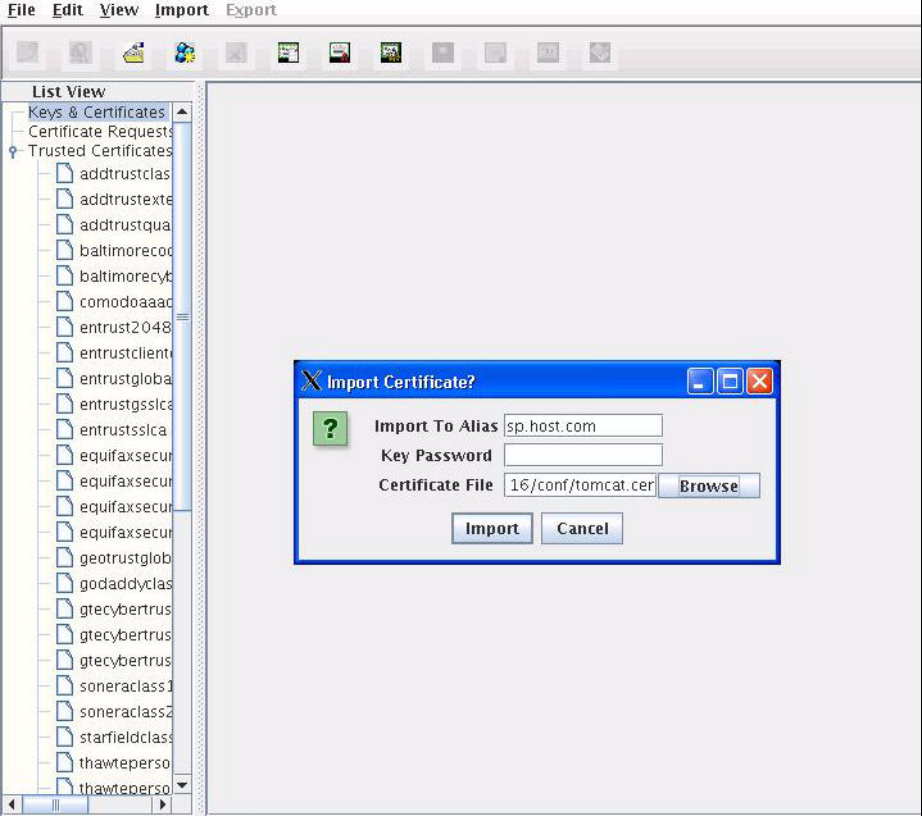
## Adding the SP Site's Server Certificate to the IDP's Trust Store

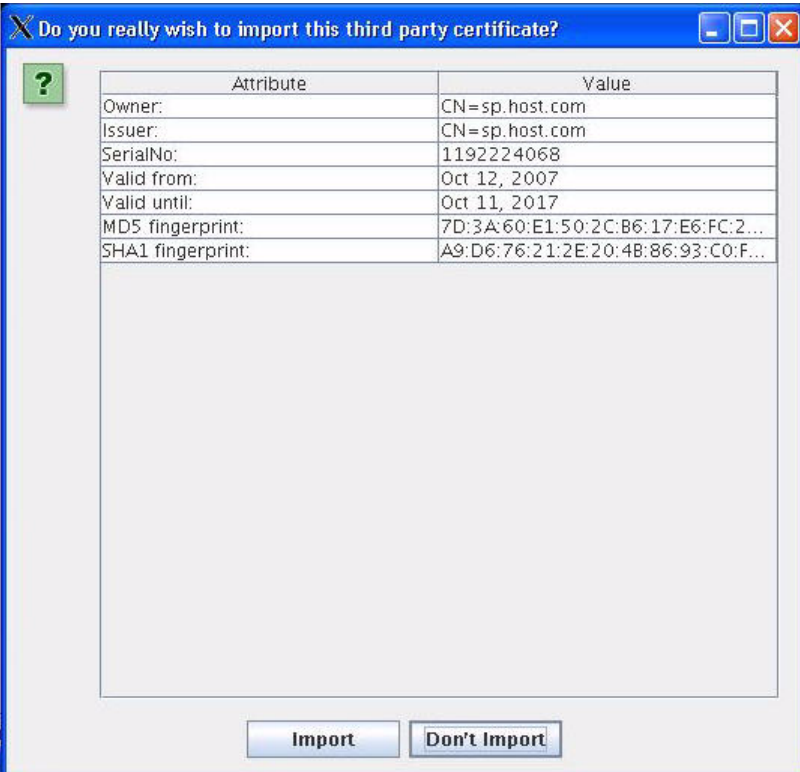
Perform the following steps to add the SP site's server certificate to the IDP's trust store.

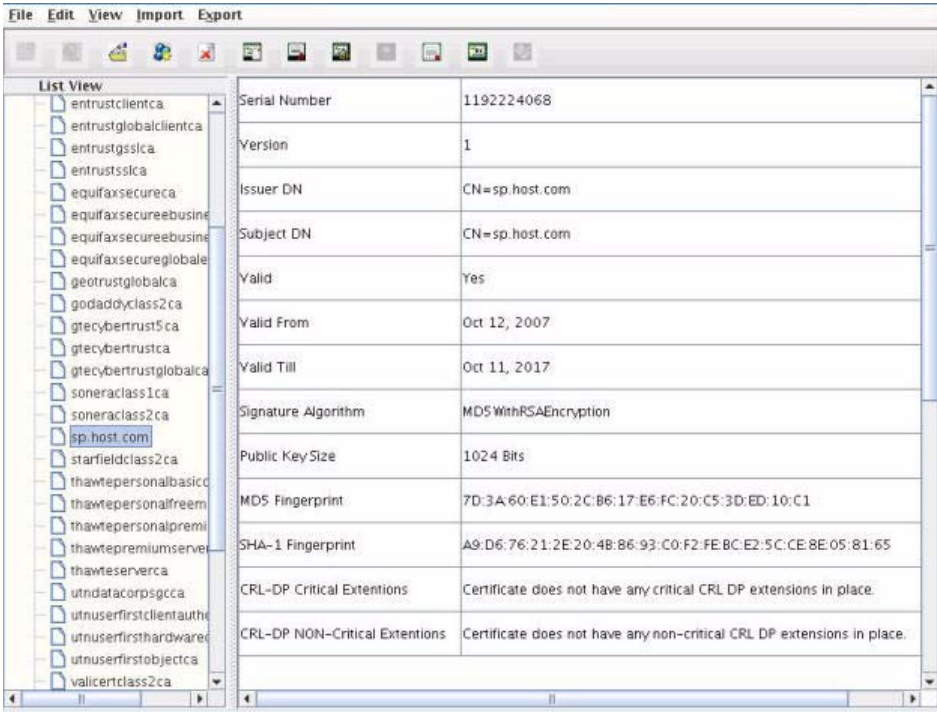
<b>Step</b>	<b>Action</b>	✓
<b>1</b>	<p>Transfer the SP site's server certificate to the machine hosting your IDP.</p> <ul style="list-style-type: none"><li>a Go to the <code>\$SF_HOME/conf</code> directory. This is where the Built-in application server's SSL certificate (<code>tomcat.cer</code>) file is located.</li><li>b Copy the <code>tomcat.cer</code> file to the machine that hosts your IDP using a secure file transfer mechanism.</li></ul>	
<b>2</b>	<p>Launch the Certificate Management Tool on the IDP machine as follows:</p> <ul style="list-style-type: none"><li>• For Windows: <pre>cd &lt;IDP_Install_Dir&gt;\tools\cmt cmt.bat</pre></li><li>• For Linux: <pre>cd &lt;IDP_Install_Dir&gt;/tools/cmt ./cmt.sh</pre></li></ul> <p>The Certificate Management Tool graphical interface opens.</p>	



Step	Action	✓
<p><b>3</b></p>	<p>Select <b>File</b> → <b>Open Keystore</b>.</p> <p>The Open Keystore page opens.</p> 	
<p><b>4</b></p>	<p>Browse to the <code>jre/lib/security</code> directory and do the following:</p> <ul style="list-style-type: none"> <li>a Open the keystore named <b>cacerts</b>.</li> <li>b Enter the password <b>changeit</b>.</li> <li>c Click <b>Open</b>.</li> </ul> <p>This is the trust store of your IDP installation.</p>	

Step	Action	✓
5	<p>Select the <b>Import</b> menu and browse to find the SP server SSL certificate that you copied to the IDP machine.</p>  <p>The screenshot shows the Java KeyStore application window. The 'List View' on the left shows a tree structure under 'Trusted Certificates'. The main area displays a dialog box titled 'Import Certificate?'. The dialog contains the following fields and buttons:</p> <ul style="list-style-type: none"> <li><b>Import To Alias:</b> sp.host.com</li> <li><b>Key Password:</b> (empty field)</li> <li><b>Certificate File:</b> 16/conf/tomcat.cer</li> <li><b>Buttons:</b> Import, Cancel, and a 'Browse' button next to the Certificate File field.</li> </ul> <p>Below the dialog, a status message reads: 'KeyStore Was Opened Successfully.'</p>	
6	Leave the key password field blank.	

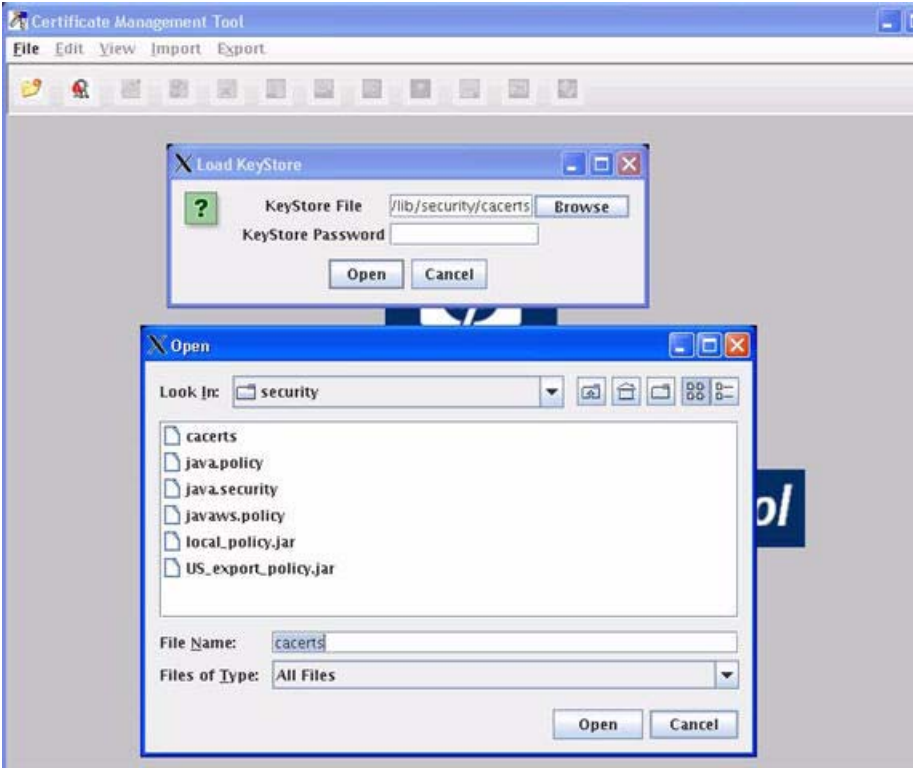
Step	Action	✓																
7	<p>Click <b>Import</b> to confirm importing the SSL certificate</p>  <p>The screenshot shows a dialog box with the following table:</p> <table border="1" data-bbox="576 388 1250 577"> <thead> <tr> <th>Attribute</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Owner:</td> <td>CN=sp.host.com</td> </tr> <tr> <td>Issuer:</td> <td>CN=sp.host.com</td> </tr> <tr> <td>SerialNo:</td> <td>1192224068</td> </tr> <tr> <td>Valid from:</td> <td>Oct 12, 2007</td> </tr> <tr> <td>Valid until:</td> <td>Oct 11, 2017</td> </tr> <tr> <td>MD5 fingerprint:</td> <td>7D:3A:60:E1:50:2C:B6:17:E6:FC:2...</td> </tr> <tr> <td>SHA1 fingerprint:</td> <td>A9:D6:76:21:2E:20:4B:86:93:C0:F...</td> </tr> </tbody> </table> <p>At the bottom of the dialog are two buttons: <b>Import</b> and <b>Don't Import</b>.</p>	Attribute	Value	Owner:	CN=sp.host.com	Issuer:	CN=sp.host.com	SerialNo:	1192224068	Valid from:	Oct 12, 2007	Valid until:	Oct 11, 2017	MD5 fingerprint:	7D:3A:60:E1:50:2C:B6:17:E6:FC:2...	SHA1 fingerprint:	A9:D6:76:21:2E:20:4B:86:93:C0:F...	
Attribute	Value																	
Owner:	CN=sp.host.com																	
Issuer:	CN=sp.host.com																	
SerialNo:	1192224068																	
Valid from:	Oct 12, 2007																	
Valid until:	Oct 11, 2017																	
MD5 fingerprint:	7D:3A:60:E1:50:2C:B6:17:E6:FC:2...																	
SHA1 fingerprint:	A9:D6:76:21:2E:20:4B:86:93:C0:F...																	


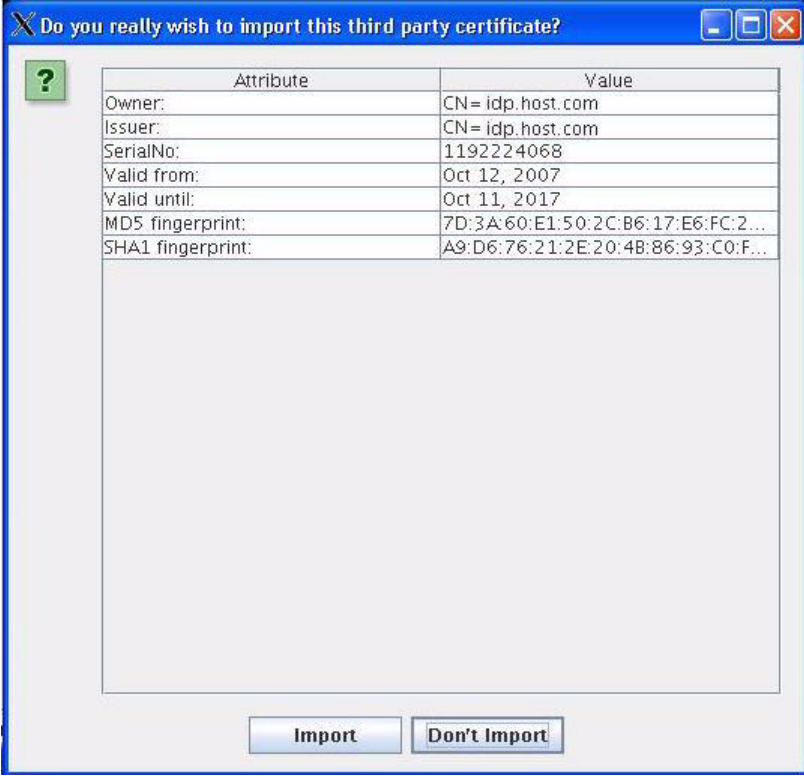
Step	Action	✓
	<p>The IDP trust store displays the SP imported certificate.</p> 	
8	Select <b>File</b> → <b>Save Keystore</b> , then select <b>Close Keystore</b> .	

## Adding the IDP Site's Server Certificate to the SP's Trust Store

Perform the following steps to add the IDP site's server certificate to the SP's trust store.

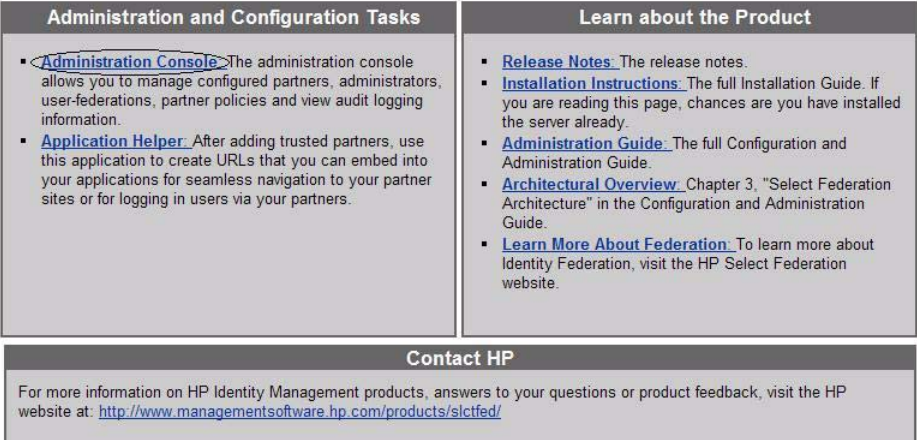
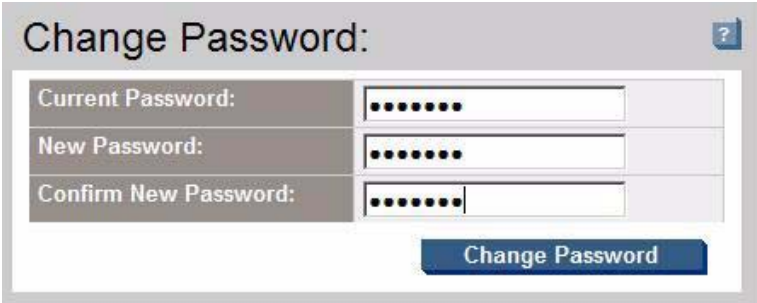
<b>Step</b>	<b>Action</b>
<b>1</b>	Transfer the IDP site's server certificate to the machine hosting your SP. <ul style="list-style-type: none"><li data-bbox="500 499 1406 562">a Go to the <code>\$\$SF_HOME/conf</code> directory to access the Built-in application server's SSL certificate (<code>tomcat.cer</code>) file.</li><li data-bbox="500 579 1390 642">b Copy the <code>tomcat.cer</code> file to the machine that hosts your SP using a secure file transfer mechanism.</li></ul>
<b>2</b>	Launch the Certificate Management Tool on the SP machine as follows: <ul style="list-style-type: none"><li data-bbox="456 751 927 877">• For Windows: <pre>cd &lt;SP_Install_Dir&gt;\tools\cmt cmt.bat</pre></li><li data-bbox="456 898 927 1024">• For Linux: <pre>cd &lt;SP_Install_Dir&gt;/tools/cmt ./cmt.sh</pre></li></ul> The Certificate Management Tool graphical interface opens.

Step	Action
<p>3</p>	<p>Select <b>File</b> → <b>Open Keystore</b>. The Open Keystore page opens.</p> 
<p>4</p>	<p>Browse to the <code>jre/lib/security</code> directory and do the following:</p> <ul style="list-style-type: none"> <li>a Open the keystore named <b>cacerts</b>.</li> <li>b Enter the password <b>changeit</b>.</li> <li>c Click <b>Open</b>.</li> </ul> <p>This is the trust store of your SP installation.</p>

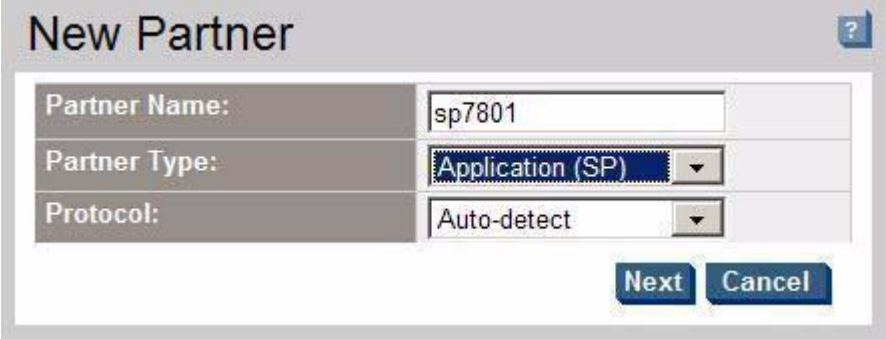
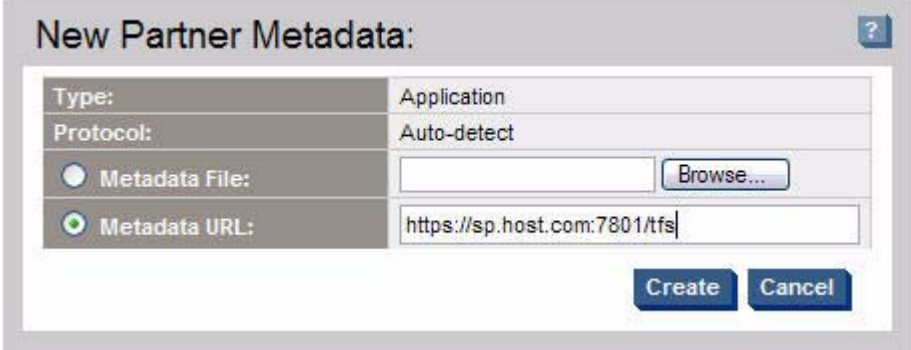
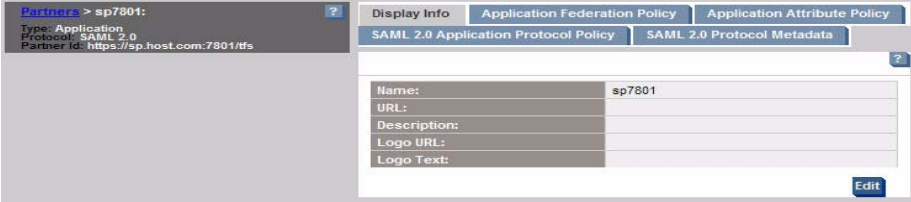
Step	Action
5	<p>Select the <b>Import</b> menu and browse to find the IDP server SSL certificate that you copied to the SP machine.</p> 
6	<p>Leave the key password field blank.</p>
7	<p>Click <b>Import</b> to confirm importing the SSL certificate</p>  <p>The SP trust store displays the IDP imported certificate.</p>
8	<p>Select <b>File</b> → <b>Save Keystore</b>, then select <b>Close Keystore</b>.</p>

# Downloading the SP's Metadata into the IDP Site

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


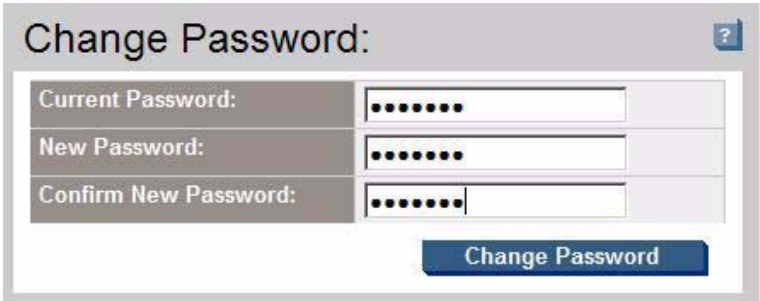
Step	Action	✓
1	<p>Open the Select Federation Administration Console startup page at <b>https://&lt;base-url&gt;/tfs-internal</b>.</p> <p>Replace <b>&lt;base-url&gt;</b> with your <code>hostname:port</code>.</p> <p>Click on <b>Administration Console</b> to open the Administration Console login page.</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> 	
3	<p>Select <b>Partners</b> → <b>Manage Partners</b>.</p> <p>The Partners page opens.</p>	
4	<p>Click the <b>New Partner</b> button.</p> <p>The New Partner page opens.</p>	


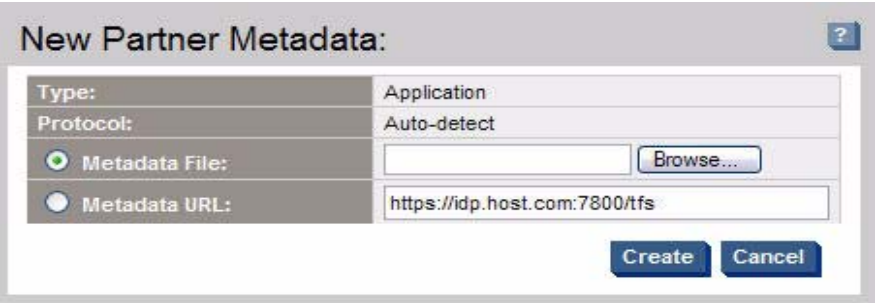
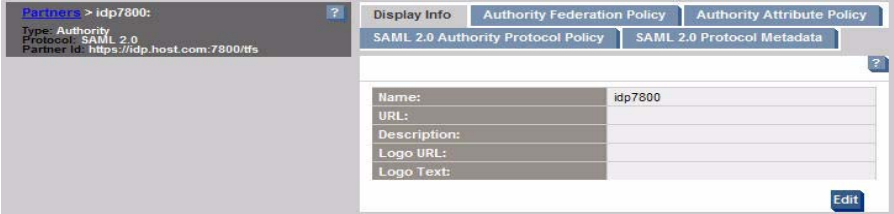


Step	Action	✓
5	Enter the <b>Partner Name</b> , <b>Partner Type</b> and <b>Protocol</b> on the New Partner page. → Next  	
6	Click <b>Metadata URL</b> and enter the metadata URL → Create  	
7	The SP Partner information has been registered at the IDP Site.  	

# Downloading the IDP's Metadata into the SP 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 <b>https://&lt;base-url&gt;/tfs-internal</b>.</p> <p>Click on <b>Administration Console</b> 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 <b>Partners</b> → <b>Manage Partners</b>.</p> <p>The Partners page opens.</p>	
4	<p>Click the <b>New Partner</b> button.</p> <p>The New Partner page opens.</p>	

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



# 5 Using the Demonstration Application

## Introduction

Demonstration application is a J2EE application that demonstrates federated Single Sign-On and other capabilities provided by Select Federation. The Demonstration application is bundled with Select Federation. The Demonstration application can also serve as sample code, which you can use to enable your own applications.

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

The Demonstration application consists of two parts:

- Identity Provider (IDP) Demo
- Service Provider (SP) Demo

The Select Federation Demonstration 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 Demonstration application use cases:

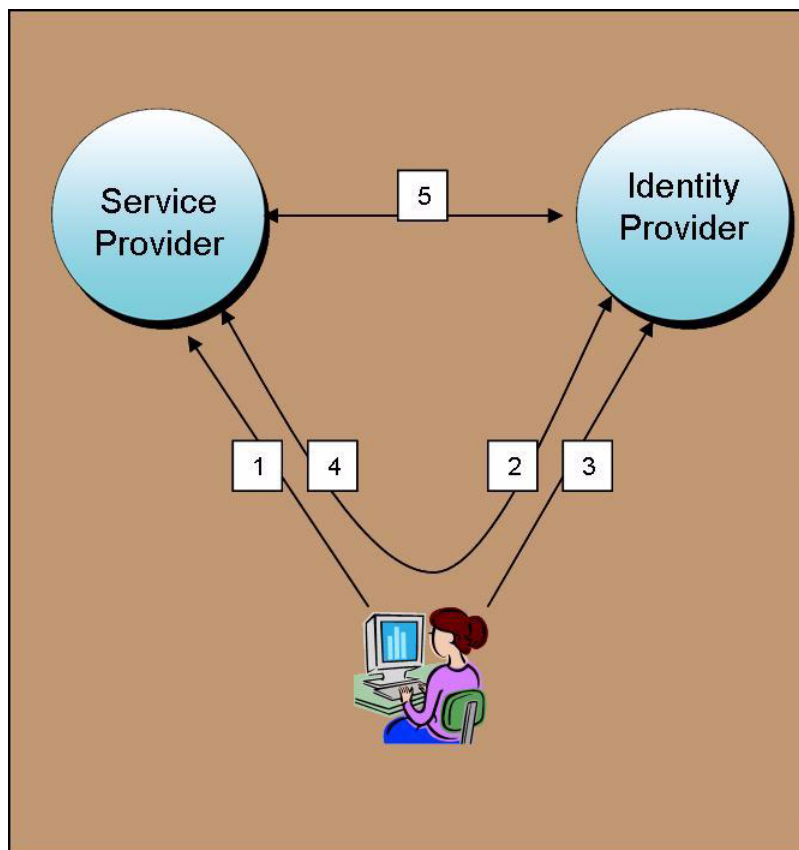
- [SP-Initiated Federation](#)
- [IDP-Initiated Federation](#)
- [SP-Initiated Single Logout](#)
- [IDP-Initiated Single Logout](#)

The Demonstration 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. The Demonstration application uses pseudonyms as the name federation policy. For details on the 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 the SP Demonstration application and is prompted to federate.
- 2 User selects the IDP from the list of IDPs and the user is redirected to the IDP.
- 3 User logs on at the IDP.
- 4 IDP generates a federated ID and redirects the user back to the SP.
- 5 SP picks up the federated ID from the artifact at the IDP using a back-channel and accesses the service at the SP as a 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: <a href="https://sp.host.com:7801/sf-demo">https://sp.host.com:7801/sf-demo</a>.</p> 	
2	Click on <b>login via idp</b> .	

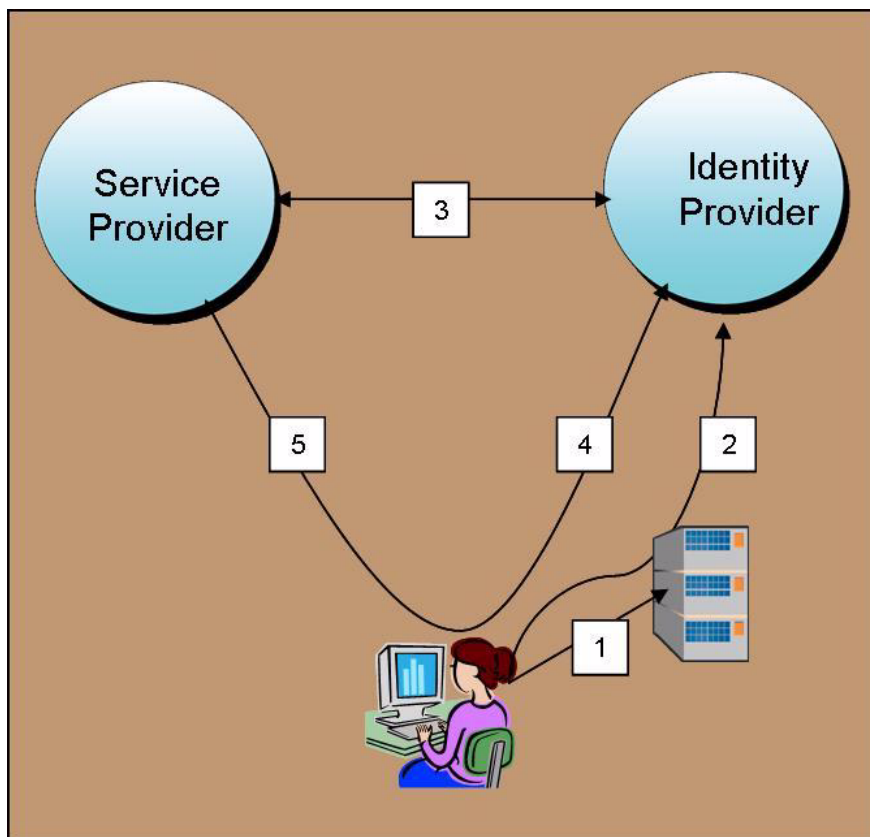
Step	Action	✓
3	<p>You are redirected to an IDP for authentication.</p> 	
4	<p>Enter your credentials (Account and Password) and click Login.</p> <p>The credentials are validated against the LDAP directory you configured for the IDP.</p>	
5	<p>The SP Demonstration Page opens. This page provides links 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.**

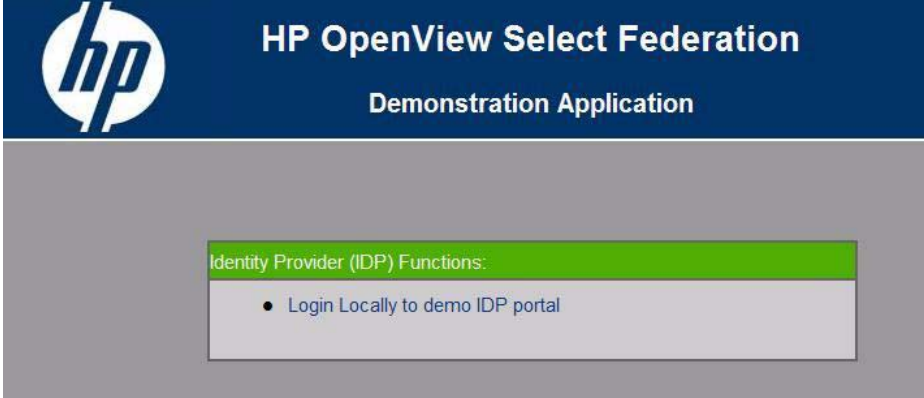



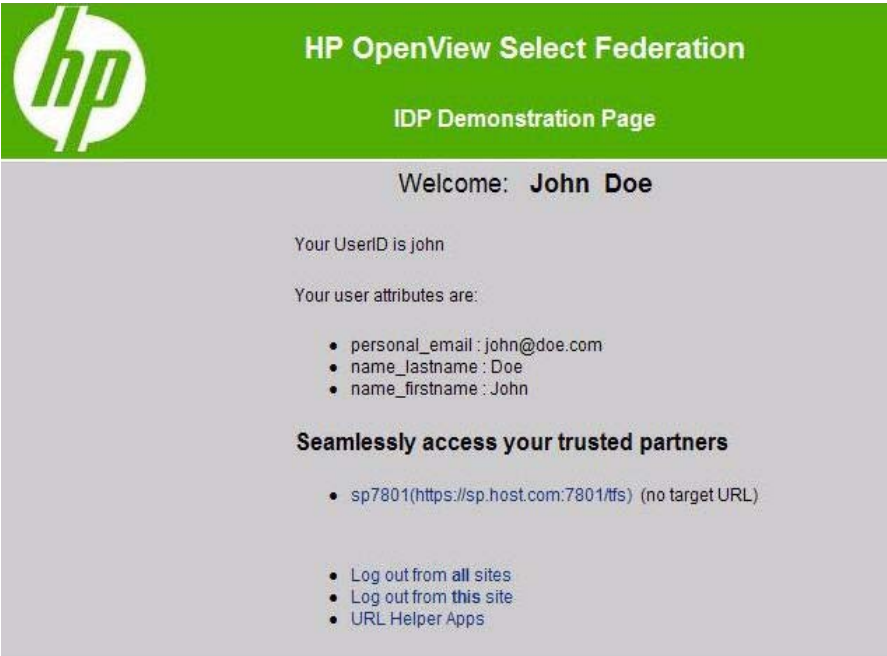

Following is a step-by-step explanation of what is happening in an IDP-Initiated SSO:

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

## Procedure

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

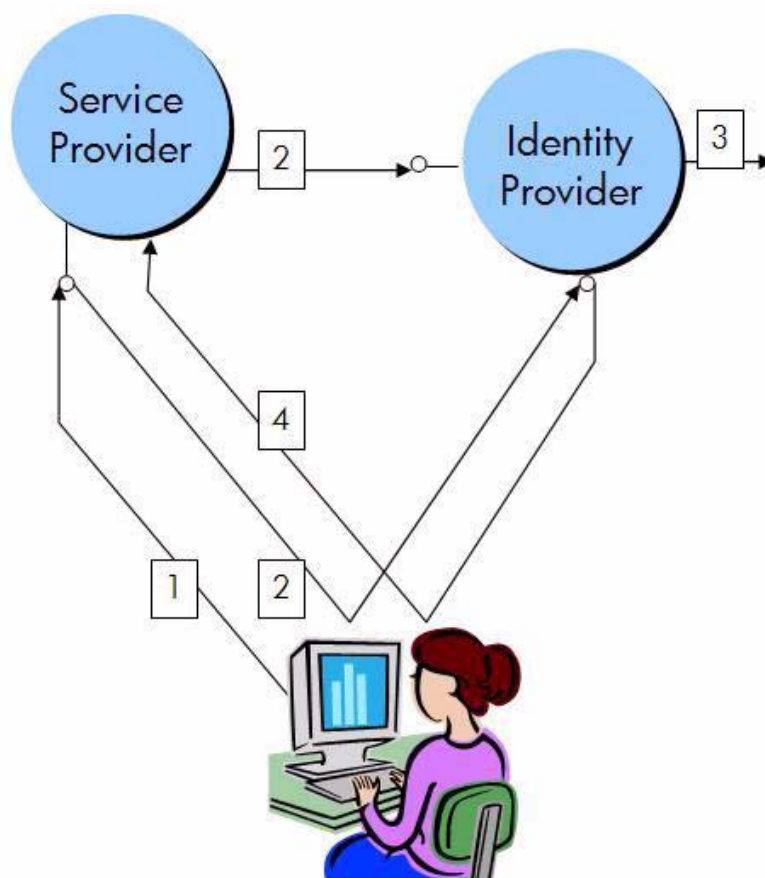
Step	Action	✓
1	<p>In a Browser window, access the sf-demo application. For example: <b>https://idp.host.com:7800/sf-demo.</b></p> 	
2	Click on <b>Login Locally to demo IDP portal.</b>	
3	<p>A login page opens.</p> 	

Step	Action	✓
4	<p>Enter your credentials (Account and Password) and click <b>Login</b>.</p> <p>The credentials are validated against the LDAP directory you configured for the IDP.</p>	
5	<p>The IDP Demonstration 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 Demonstration 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 the SP site.
- 2 Using redirect, the SP initiates the Single Logout at the IDP. (The SP can initiate a logout using various mechanisms. See the *HP Select Federation Configuration and Administration 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 the user back to the Single Logout Return URL at the originating SP.

## Procedure

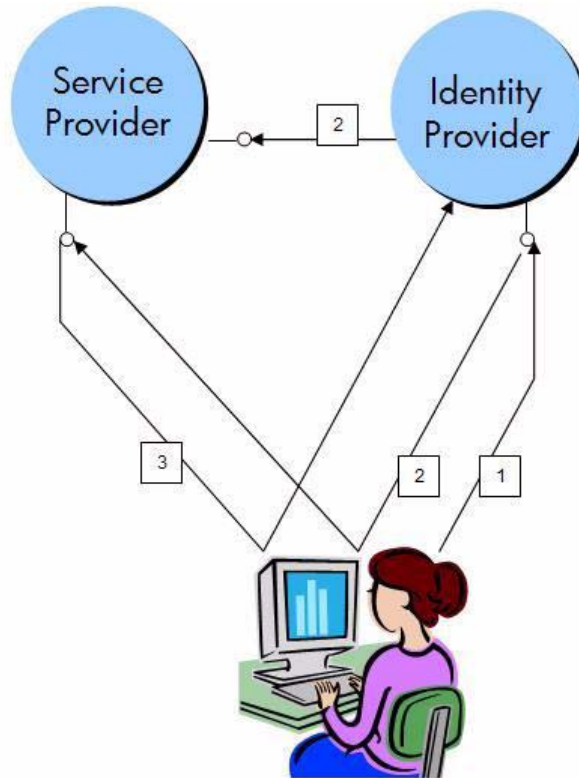
Perform the following steps to create an SP-initiated Single Logout:

Step	Action	✓
1	<p>Click on <b>Log out from all sites</b>, on your SP application.</p>  <p>Your local User ID is 78a98eb6ca27e7ce87993ebd35b9a6d87e38b034</p> <p>You were authenticated by idp7800.</p> <p>Your user attributes are (as provided by idp7800):</p> <ul style="list-style-type: none"><li>• Terminate Federation with idp7800</li><li>• Log out from <b>all</b> sites</li><li>• Log out from <b>this</b> site</li><li>• URL Helper Apps</li></ul>	
2	<p>The Demonstration Application start page opens when Single Logout is performed.</p>  <p>Service Provider (SP) Functions:</p> <ul style="list-style-type: none"><li>• Login via idp7800 (<a href="https://idp.host.com:7800/tfs">https://idp.host.com:7800/tfs</a>)</li></ul>	

# IDP-Initiated Single Logout

## How an IDP-Initiated Single Logout Works

**Figure 4 IDP-Initiated Single Logout Flow.**


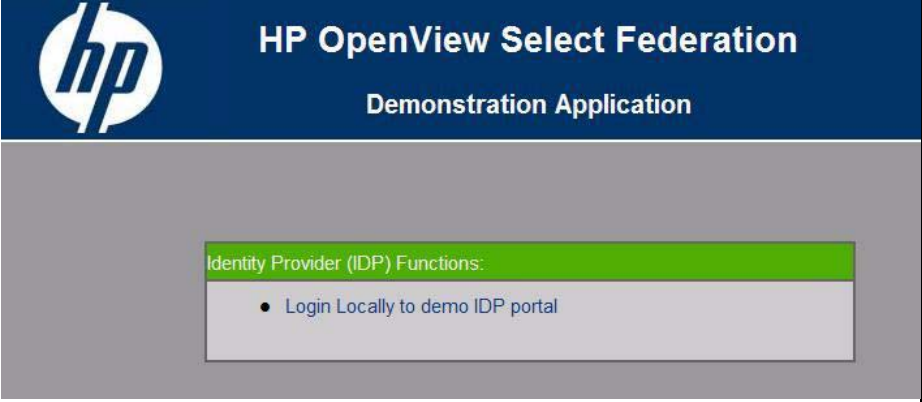


Following is a step-by-step explanation of this diagram:

- 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 <b>Log out from all sites</b>, on your IDP application.</p> 	
2	<p>The Demonstration Application 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 \(IDP-FSS\)](#).

**ADAM**

Active Directory Application Mode

**ADFS**

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

**Administrator**

An identity with full permission to manage Select Federation.

**API**

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

**Application Helper**

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

**Application Program Interface (API)**

An interface that enables programmatic access to an application.

## **Application Site Role**

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

## **Artifact Binding**

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

## **ASP**

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

## **Attribute**

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

## **Authentication**

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

## **Authority Site Role**

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

## **Authorization**

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

## **Bindings**

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

## **CA**

Certificate Authority

## **CardSpace**

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

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

### **Certificate Revocation Checking**

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

### **Context**

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

### **CSR**

Certificate Service Request

### **Delegated Administrator**

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

### **Domain-Local Users**

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

### **DS**

Discover Service

### **DST**

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

### **Edge Router**

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

### **Event**

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

### **Event Plugin Chain**

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

## **Federation**

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

## **Federation Router**

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

## **Filter-Support**

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

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

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

## **FSS**

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

## **GMT**

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

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

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

## **Group**

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

## **Identity Mapping**

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

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

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

**Identity Provider (IDP)**

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

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

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

**IDP**

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

**IDP-FSS**

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

**ID-WSF**

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

**IE**

Internet Explorer

**IIS**

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

**Impersonation Token**

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

**Inbound Windows Integration (IWI)**

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

**Integrated Windows Authentication (IWA)**

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

**Internet Information Server (IIS)**

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

**IWA**

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

**IWI**

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

**JAVA**

Object-oriented programming language.

**JVM**

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

**Keystore**

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

**LDAP**

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

**LECP**

Liberty Enabled Client/Proxy Service.

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

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

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

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

**Lightweight Directory Access Protocol (LDAP)**

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

**LUAD-WSC**

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

**Metadata**

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

**Microsoft Management Console (MMC)**

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

**MIME**

Multipurpose Internet Mail Extension

**MMC**

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

**NTLM (NT LAN Manager)**

Default network authentication protocol for Windows NT 4.0.

**OCSP**

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

**Online Certificate Status Protocol (OCSP)**

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

**Partner**

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

**Passive URLs**

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

**PDC**

Primary Domain Controller

**Plugin**

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

**POST Binding**

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

**Presence Service**

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

**Privacy Manager**

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

## **Protected URLs**

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

## **Protocol**

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

## **Root Administrator**

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

## **SAML**

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

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

A handshake protocol, which supports server and client authentication.

## **Service Provider (SP)**

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

## **Single Logout (SLO)**

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

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

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

## **Site Role**

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

## **SLO**

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



**SOAP**

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

**SP**

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

**SSC**

Self Signed Certificate

**SSL**

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

**SSO**

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

**TLS**

Transport Layer Security

**Universal Coordinated Time (UTC)**

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

**Unprotected URLs**

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

**UPN**

User Principal Name

**UTC**

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

**WAP**

Wireless Application Protocol

**Web Service Consumer (WSC)**

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

**Web Service Provider (WSP)**

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

**WSC**

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

**WSP**

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

# Index

## A

- about this guide, 7
- Administration console, used to exchange metadata, 23

## D

- Demonstration application
  - IDP and SP, 37
  - IDP-initiated federation use case, 41
  - overview, 37
  - sf-demo, 37
  - SP-initiated federation use case, 38
  - SP-initiated Single Logout use case, 44, 46

## H

- hardware recommended specifications, 7

## I

- IDP-initiated federation use case
  - how it works, 41
  - procedure, 42
- IDP-initiated Single Logout use case
  - how it works, 46
  - procedure, 47
- IDP instance
  - adding the IDP's server certificate to the SP's trust store, 29
  - before you begin installing, 9
  - downloading the IDP's metadata to the SP's site, 34
  - procedure, 10
- installing
  - before you begin for the IDP, 9
  - before you begin for the SP, 17
  - procedure for the IDP instance, 10
  - procedure for the SP, 18

## M

- metadata
  - adding the IDP's server certificate to the SP's trust store, 29
  - adding the SP's server certificate to the IDP's trust store, 24
  - download from a well-known URL, 23
  - downloading the IDP's metadata to the SP's site, 34
  - downloading the SP's metadata to the IDP's site, 32
  - exchange using the Administration console, 23
  - get securely from the Partner, 23
  - overview, 23

## O

- overview
  - Demonstration application, 37
  - metadata, 23
  - of this guide, 7

## P

- passive URLs, 55
- prerequisites, 7
  - hardware recommended specifications, 7
  - software requirements, 7
- procedures
  - adding the IDP's server certificate to the SP's trust store, 29
  - adding the SP's server certificate to the IDP's trust store, 24
  - downloading the IDP's metadata to the SP's site, 34
  - downloading the SP's metadata to the IDP's site, 32
  - for this guide, 8
  - IDP-initiated federation use case, 42
  - IDP-initiated Single Logout use case, 47
  - installing the IDP instance, 10
  - installing the SP instance, 18
  - SP-initiated federation use case, 39
  - SP-initiated Single Logout use case, 45

## R

### requirements

- hardware recommended specifications, 7
- software, 7

## S

### sf-demo, Demonstration application, 37

### Single Logout

- how an IDP-initiated Single Logout works, 46
- how an SP-initiated Single Logout works, 44

### software requirements, 7

### SP-initiated federation use case

- how it works, 38
- procedure, 39

### SP-initiated Single Logout use case

- how it works, 44
- procedure, 45

### SP instance

- adding the SP's server certificate to the IDP's trust store, 24
- before you begin installing, 17
- downloading the SP's metadata to the IDP's site, 32
- procedure, 18

## T

### trust store

- adding the IDP's certificate to the SP, 29
- adding the SP's certificate to the IDP, 24

## U

### URL classes

- passive, 55

### use cases

- IDP-initiated federation, 41
- IDP-initiated Single Logout, 46
- SP-initiated federation, 38
- SP-initiated Single Logout, 44

