HP OpenView Select Federation

For the HP-UX, Linux, Solaris and Windows® Operating Systems

Software Version: 6.60

Installation Guide

Document Release Date: November 2006
Software Release Date: November 2006

hp invent

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 2002-2006 Hewlett-Packard Development Company, L.P.

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

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

Trademark Notices

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

Documentation Updates

This 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 OpenView Support web site at:

www.hp.com/managementsoftware/support

HP OpenView 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, go to:

www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

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

Contents

1 Introduction

This *HP OpenView Select Federation Installation Guide* describes how to install Select Federation.

This chapter provides a brief overview of the capabilities of HP OpenView Select Federation. The installation and operating instructions are given in their respective chapters, which also provide detailed descriptions of Select Federation's various functions.

Prerequisites

This guide assumes a general knowledge about installation and configuration of web servers, databases, and so on for the target operating environment.

This guide also assumes a working knowledge of:

- Identity Management
- Federated Identity

What does Select Federation Do?

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

Users typically have a web account that they use regularly such as their corporate account. They also have many independent accounts at one or more web sites that they use less frequently. Once these accounts are federated, users can access all the federated web sites through their most frequently used account without having to log in each time.

Built on the latest federated identity standards, Select Federation does not require any radical changes to the existing technology infrastructure. It provides a de-centralized approach to cross-domain single sign-on, provisioning and privilege management across identity domains.

If required, Select Federation can be used standalone or together with HP OpenView Select Access. With Select Access, Select Federation adds standards-based cross-domain single sign on capabilities to Select Access, the HP OpenView product for centralized access management.

Setting Your Site Role When Deploying Select Federation

A federation is established between Trusted Partners. Before you deploy Select Federation, you and your Trusted Partner need to agree in advance how the federation is to be set up. That is, each site must have a **site role**, which determines whether a site hosts the application (Application site role) or provides authentication (Authority site role) so that the end users can seamlessly access the application. A single installation can act in both roles at various times, towards various partners and/or for different users. However it is not very common for a single installation to play both an Application and an Authority role.

The following sections describe each type of site role.

Authority Site

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

Application Site

An Application site (also called a SAML Consumer or Service Provider (SP) Site) is a Trusted Partner site that participates in a federation to provide a service or application to common users and relies on an authority site to provide authoritative user authentication and other information. In the extranet example, the site hosting the extranet is the application site.

Both Authority Site and Application Site

A single Select Federation instance can handle both the Application site and Authority site roles. For example, you may host an extranet for your partners' employees to access, in which case you are the Application site. However, your partners may also host applications that require your employees to authenticate at your site, in which case you are the Authority site.

Before Installation

- Create the databases and directories you will be using. Then, collect information about these databases and directories, including server addresses, database accounts, and so on. Any of these settings can also be changed after the installation.

- Determine if your installation is going to be an Authority only site (only asserting local users' identities to partners) or Application only site (only allowing federated users to login to your web sites) or both.

- You can find Select Federation documentation in the `docs/` folder. The documents are in Adobe Acrobat PDF and/or HTML formats.

- Check the `docs/relnotes.pdf` on the installation CD for any late minute additions or possible manual errata.

- If you are installing Select Federation 6.60 on a computer that already has 6.5, skip to Chapter 7, Upgrading From Select Federation Version 6.5 for the upgrade instructions.

Installation Checklist

The installation of Select Federation includes the following steps:

1 **Make sure that your systems match or exceed the systems requirements.** The full list of systems requirements can be found in Chapter 2, System Requirements.

2 **Install Select Federation.** Start the installation by running the Select Federation install executable located on the CD and follow the on-screen instructions. See the instructions in Installation Procedure on page 21.

3 **If using Select Access, Integrate Select Access with Select Federation.** Configure policies in the Select Access Policy Builder for proper operation of Select Federation. See instructions in Integrating Select Access with Select Federation on page 63.

4 **Add Groups and Partners.** The first step in creating an operational federation is to set up your Groups and Partners. See the instructions in the "Managing Partners" chapter in the *HP OpenView Select Federation Configuration and Administration Guide*.

5 **Configure Groups and Partners.**

6 **Enable Applications using the Application Helper.** Select Federation has a special Application Helper that enables you to create URLs for embedding in your application. See the instructions in "Using the Application Helper" in the *HP OpenView Select Federation Configuration and Administration Guide*.

⚠ Due to how the Windows operating system works, if you are uninstalling, installing, upgrading or configuring Select Federation components on a Windows host computer, be sure that you do not have the Services window or any other Control Panel application open. An open Control Panel application triggers conflicts that causes the installer to behave abnormally.

▶ **I**f you decide to use HP OpenView Select Audit for logging after installing Select Federation, you need to change the system configuration. See the instructions in Integrating Select Audit with Select Federation Manually on page 68

2 System Requirements

Select Federation is designed to work with a number of hardware and operating systems configurations. The flexibility inherent in Select Federation extends to the third-party applications that it supports, namely the application servers, database servers, and LDAP servers.

Hardware Systems Requirements

Select Federation is qualified to run on any of the hardware shown in Table 1:

Table 1   Hardware upon which Select Federation runs

Hardware	Minimum Specifications
Intel Pentium PCs	Processor Speed: 1 GHz Main Memory: 1 GB Free Disk Space: 2 GB
HP-UX PA-RISC based servers	Processor Speed: 500 MHz Main Memory: 1 GB Free Disk Space: 2 GB
HP-UX Itanium based servers	Processor Speed: 1 GHz Main Memory: 1 GB Free Disk Space: 2 GB
Sun SPARC based servers	Processor Speed: 450 MHz Main Memory: 1 GB Free Disk Space: 2 GB

Operating System Requirements

Select Federation is qualified to run on any of the operating systems shown in the following table (where applicable):

Table 2   Supported Operating Systems

Operating System
HP-UX 11.23 (Itanium) and PA-RISC
Red Hat Linux AS, version 3.0 Update 5 and 4.0
Microsoft Windows 2003 Server and Window 2003 Server R2
Sun Solaris 9, Sun Solaris 10

> Select Federation is a 32-bit program. Even if the operating system is a 64-bit operating system, Select Federation runs in the 32-bit compatibility mode.

Java Software Requirements

Select Federation is qualified to run on any of the Java Development Kits (JDKs) shown in Table 3:

Table 3   Supported Java Development Kits

Java Development Kits
JDK 1.4.2_08
JDK 1.5.0

Supported Third-Party Servers

Select Federation is designed for flexibility and runs a number of application servers, database servers, and LDAP servers.

Application Servers

Select Federation is qualified to run on any of the Application Servers shown in Table 4.

Table 4   Supported Applications Servers

Server
BEA WebLogic 8.1 SP5 (for SA-integrated mode and standalone mode) BEA WebLogic 9.1 (for standalone mode only)
IBM WebSphere 6.0.2
Built-in application server (included with Select Federation based on Jakarta Tomcat 5.5)

The built-in application server can be run without having an external application server such as WebLogic or WebSphere.

➤ For WebSphere 6.0.2, Fix Pack 15 is required for the client-authentication and CRL checking features.

Database Servers

Select Federation is qualified to run on any of the database software shown in Table 5.

Table 5   Supported Database Servers

Database
Oracle 10g
Oracle 9i
Microsoft SQL Server 2000
Built-in (Apache Derby 10.0)

Select Federation also includes a built-in database that is based on Apache Derby. It can be run without having an external database such as Oracle or Microsoft SQL Server.

The above products require a particular database instance to be able to create tables in. In the installation process, the tables are provided a unique table prefix, so that they do not collide with other tables that may exist..

➤ If you are using non-ASCII characters with your Select Federation Oracle database, you need to configure it to store these characters correctly. By default, the Oracle wizard sets the default character set based on the language of the host computer's operating system.

If you need to use another character set other than this default, set a new UTF-8 character set when you are creating your database. For details, see Language Support on page 1-6 of the *Oracle10g Globalization Support Guide*.

LDAP Servers

Select Federation is qualified to run on any of the LDAP Servers shown in Table 6.

Table 6   Supported Directory Servers

LDAP Servers
Microsoft Active Directory for Windows 2003 and Windows 2003 Server R2
Sun Java System Directory Server 5.1
NDS eDirectory 8.7.3
Critical Path Directory 4.2
Oracle Internet Directory 9.2
CA eTrust 8
Red Hat Directory Server

Select Federation supports the above directory servers as an external user repository for either user-authentication or attribute retrieval or both. A subset of these directory servers shown in the following table are supported by Select Federation 6.60 as a federation repository as well.

Table 7   Supported Subset of the Directory Servers

LDAP Servers
Microsoft Active Directory for Windows 2003 Server and Windows 2003 Server R2
Sun Java System Directory Server 5.1

Supported Third-Party Filters

Select Federation supports the following filters, which are listed with the web servers and platforms on which they are supported:

Table 8   Supported Filters

Filters	Web Server	Platform
Apache	Apache 1.x and 2.x	• Windows 2003 Server and Windows Server R2 • Red Hat Linux AS, version 3.0 Update 5 and 4.0
IIS	Internet Server Application Programming Interface (ISAPI)	• Windows 2003 Server and Windows Server R2
Java Access	• WebSphere 6.0.2 • WebLogic 8.1 and 9.1 • Apache Tomcat 5.5	• Windows 2003 Server and Windows Server R2 • HP-UX 11.23 Itanium and PA-RISC • Red Hat Linux AS, version 3.0 Update 5 and 4.0 • Sun Solaris 9 and 10

HP OpenView Suite of Identity Management Products

Select Federation 6.60 can be integrated with other components of the HP OpenView suite of identity management products.. The following table lists the HP OpenView components.

Table 9   HP OpenView Components that can be Integrated with Select Federation Components

HP OpenView Select Access 6.1 SP3
HP OpenView Select Access 6.2
HP OpenView Select Audit 1.0
HP OpenView Self-Healing Services 1.4

System Time Synchronization

All the machines involved in an installation must have synchronized system time, which is required by the federation protocols. This includes the machines used for databases, LDAP directories, and so on. If the machine system times are not synchronized, it can result in audit log event timestamps not matching with the protocol messages.

It is strongly recommended that you run all systems in the GMT (Greenwich Meridian Time) time zone, especially for installations that operate across time zones. Also, the database software must be in the same time zone as the machine on which it is running and therefore, in the same time zone as the Select Federation machine.

Select Federation does all of its computations in GMT. Therefore, its basic operation is not affected by the change in the daylight savings time scheme.

3 Installing Select Federation

Installation Overview

From an installation perspective, HP OpenView Select Federation is a Java Servlet-based web application that needs to be deployed on an appropriate web application server such as the built-in application server, BEA WebLogic or IBM WebSphere. For proper operation, Select Federation needs to read and write various kinds of information to persistent data storage. Much of the installation process and most of the configuration is about identification of the various data stores. In the most simple case, all data is stored into the built-in database, but many installations will require integration with existing databases or other databases and directories. The following gives some background in order to better understand the questions asked during installation.

Select Federation manages federation data and to this end needs a data store. There are three kinds of federation data:

- **Federation session data.** This is information about end users being authenticated, assertions that have been issued or received, and so on. Federation session data is not to be confused with browser session data. Federation session data is typically longer lived and stored by Select Federation. Browser session data is maintained by the web application server (which may use a database for this purpose). Federation session data requires a relational database.

- **User federations.** These are the persistent links between accounts for users at different partners. It is possible to store user federations in a relational database or in a LDAP directory.

- **Partner data.** This is information about your trusted partners, including friendly name, various policies to apply, and so on. Partner data can be stored in a relational database or in a LDAP directory.

A Select Federation installation that will act as an Authority (Identity Provider, IDP) should be typically integrated with a (pre-existing) user directory. This directory can be used to authenticate end users and to provide profile attributes of end users. HP OpenView Select Federation supports both relational databases as well as LDAP directories for this purpose. Moreover, Select Federation offers a plug-in interface that allows developers to write modules that hook up to other directories (see the *HP OpenView Select Federation Web Application Developer's Guide,* which is provided on the Select Federation CD).

Likewise, a Select Federation installation that will act as an Application (Service Provider, SP)), and is protected by Select Access, needs to populate the LDAP directory that is used by Select Access.

Select Federation also maintains audit logs. These audit logs can be written to a relational database, to an Select Audit connector or both. Select Federation supports the use of end user privacy policies. These are normally stored in a relational database, but can be stored in a LDAP directory too.

Many of the federation protocols require signed messages and encrypted traffic, and Select Federation needs keys and certificates. Keys and certificates are kept in Java compliant *keystores*. The installer can generate a keystore populated with self-signed certificates that are usually fine, but in some cases company policy requires the use of existing or other certificates.

In summary, Select Federation always requires a relational database, and can use an LDAP directory for some of its data. Many Select Federation installations need to be connected to existing LDAP directories and relational database systems.

➤ Before beginning the actual installation of Select Federation, collect information about the databases and directories to be used, including server addresses, database accounts, and so on. Any of these settings can also be changed after the installation. See Before Installation on page 10 for more information.

See Chapter 2, System Requirements for a detailed list of supported application servers, databases and directories.

Installation Settings for International Character Support

Setting Unicode Escaped Character Representations in the tfsconfig.properties File

Select Federation uses the `tfsconfig.properties` system configuration file in the `conf/` subdirectory, which is a Java properties file. If the `tfsconfig.properties` parameter values contain characters that are not supported in the `ISO-8859-1` encoding option, they must be entered in their Unicode Escaped representation.

For example the following entry that includes unsupported characters:

```
hpsf.ldapUserBaseDN=cn=検索オプション,OU=sf,OU=ov,OU=hp,DC=domain,DC=com
```

must be entered in the `tfsconfig.properties` file as follows:

```
hpsf.ldapUserBaseDN=cn=\u691c\u7d22\u30aa\u30d7\u30b7\u30e7\u30f3,OU=sf,O
U=ov,OU=hp,DC=domain,DC=com
```

Optionally you can use tools such as native2ascii (available in the Sun JDK) to convert a file with native-encoded characters (characters which are non-Latin 1 and non-Unicode) to one with Unicode-encoded characters.

Setting JVM Character Encoding Options

If you want your installation to support international characters, set the `-Dfile.encoding=UTF-8` option for your application server. If you are using WebSphere or WebLogic as your application server for Select Federation, follow the steps in the following sections to set the JVM options. This option is already set in the built-in application server for Select Federation.

Setting Character Encoding for WebSphere

Perform the following steps to set the `-Dfile.encoding=UTF-8` option for WebSphere:

1 Start the WebSphere Administrative Console.

2 Click **Servers**.

3 Click **Application Servers**.

4 Click your server.

5 Click the **Configuration** tab.

6 Expand the **Java and Process Management** link.

7 Click **Process Definition**.

8 Click **Java Virtual Machine**.

9 Scroll to the Generic JVM Arguments text box and add **`-Dfile.encoding=UTF-8`**.

10 Click **Apply**.

11 Click **Save link to the master configuration** at the top.

12 Restart the WebSphere application server.

Setting Character Encoding for WebLogic

Perform the following steps to set the `-Dfile.encoding=UTF-8` option for WebLogic:

1 **Edit** `<BEA DOMAIN HOME DIRECTORY>/bin/setDomainEnv.sh`.

2 In the `JAVA_PROPERTIES` variable, add **-Dfile.encoding=UTF-8**.

For example, the `JAVA_PROPERTIES` variable after it has been modified is as follows:

```
JAVA_PROPERTIES="-Dplatform.home=${WL_HOME} -Dwls.home=${WLS_HOME}
-Dwli.home=${WLI_HOME} -Dfile.encoding=UTF-8"
```

3. Save the file.

4. Restart the WebLogic application server.

Installation Procedure

➤ If you are installing Select Federation 6.60 on a computer that already has 6.5, skip to Chapter 7, Upgrading From Select Federation Version 6.5 for the upgrade instructions.

The following instructions and screen captures are given for a Microsoft Windows installation. Installation on other supported operating systems is the same for all practical purposes. The differences are primarily with respect to the filenames and default paths.

To install HP OpenView Select Federation using the automated installer, perform the following steps:

⚠ Due to how the Windows OS works, if you are uninstalling, installing, upgrading or configuring Select Federation components on a Windows host computer, ensure that you do not have the Services window or any other Control Panel application open. An open Control Panel application triggers conflicts that causes the installer to behave abnormally.

1 **Start Installation.**

Start the installation by running the Select Federation install executable located on the CD.

2   **License agreement**.

Read the license agreement and accept or reject it by clicking the appropriate radio button. You must accept the license agreement in order to continue the installation procedure. Click **Next** to continue.

3   **Enter company name**.

Enter the company name that you wish to use in generating certificates and signing keys for Select Federation. Click **Next** to continue.

> The Company Name must always be an ASCII text string without special characters

.
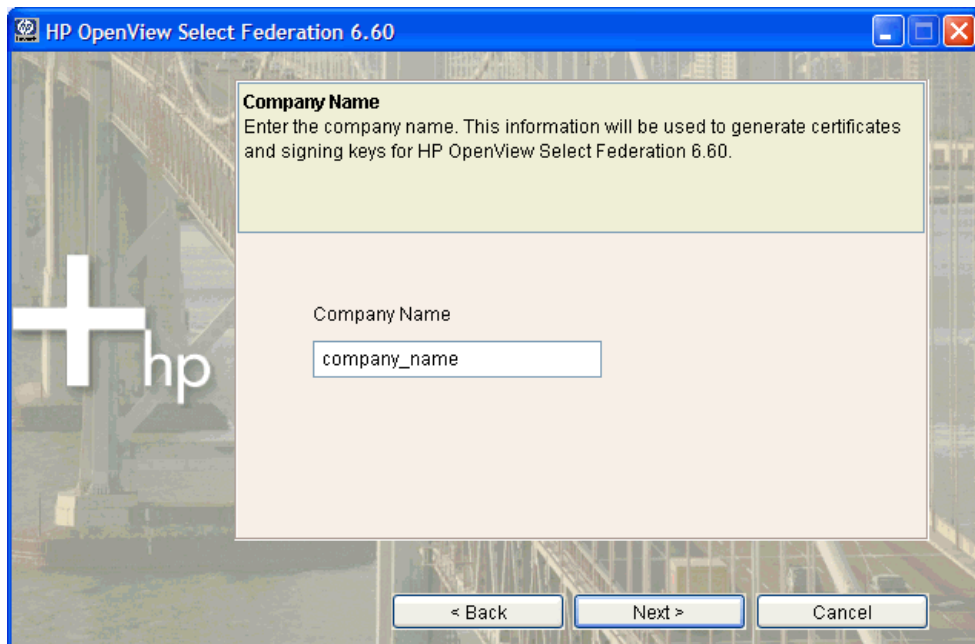
4   **Choose the application server**.

Choose the application server that you would like to use with Select Federation by using the radio buttons and drop-down menu. Select Federation has a built-in application server, which you can use if you do not have a supported application server of your own. If you use the built-in application server, the Installer will complete all the necessary steps for you. If you decide to use an existing application server, some steps will have to be performed to complete the installation. These are described in detail in the next step. Click **Next** to continue.
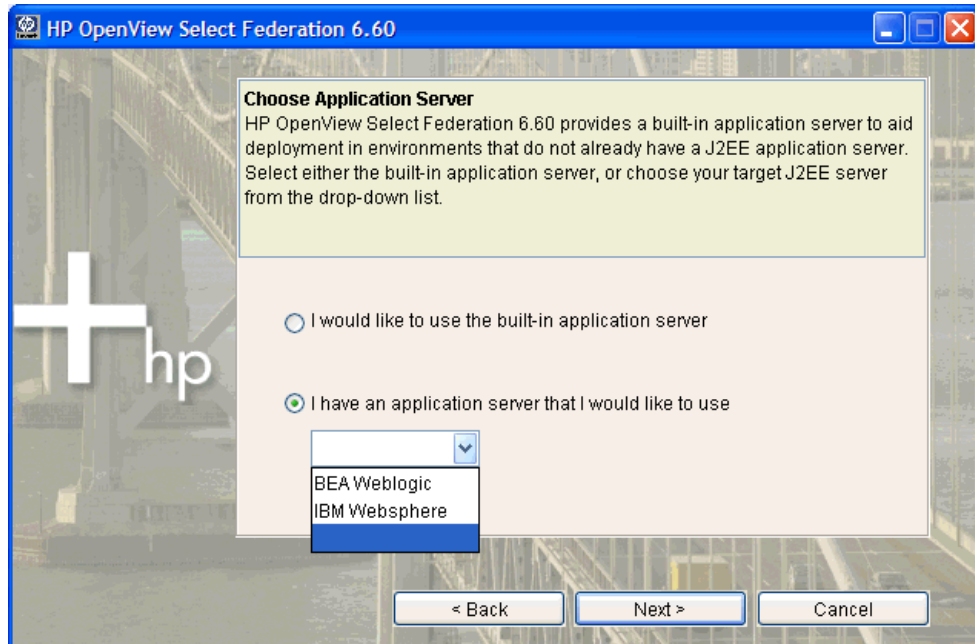
5 **Configure the application server**.

This step describes how to configure the application server you chose: built-in or existing application server.

a **Configure the built-in application server.**

Select Federation uses this information to make itself available over the Internet and also for the generating configuration files and keystore. If you plan to make the application server the front-end for Select Federation (this is, not using a web server), then do the following:

— Choose **I will not be using a proxy server** from the drop-down list.
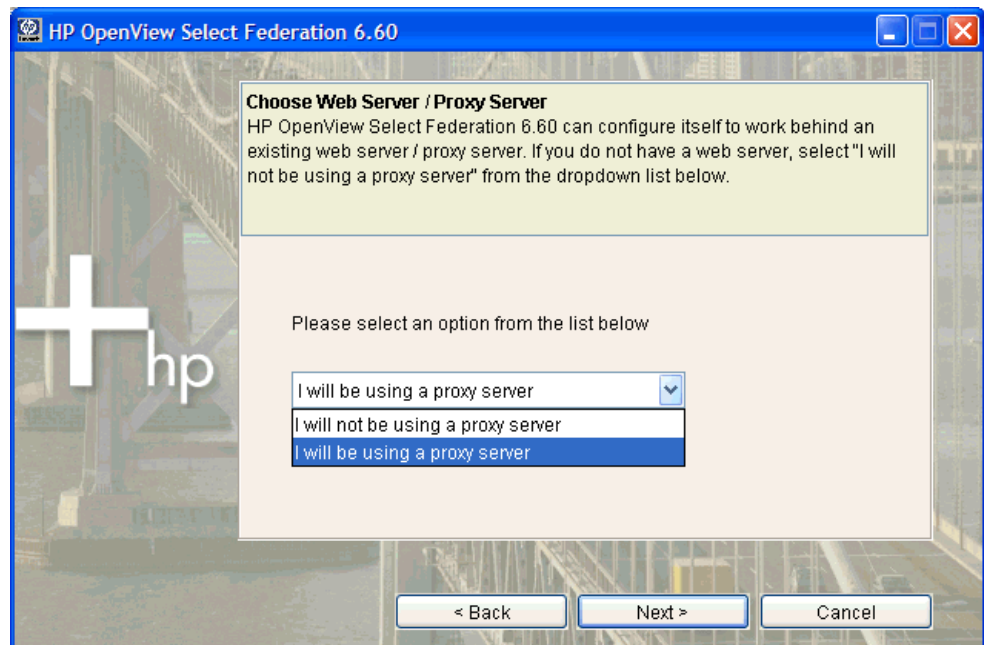

— Click **Next** to continue.

— You are prompted for the following additional information:

Protocol — Choose HTTP
Site name — Enter a name for the local host that will be a part of the URL

➤ On Windows, you must add the site name to the host file in
`C:\windows\system32\drivers\etc\`.

Port — The back-end server can be configured to run on any port you choose as long as there is no conflict with other ports. The default port is 8080. If you want to change the port, click **I use a non-standard port** and enter the port number.
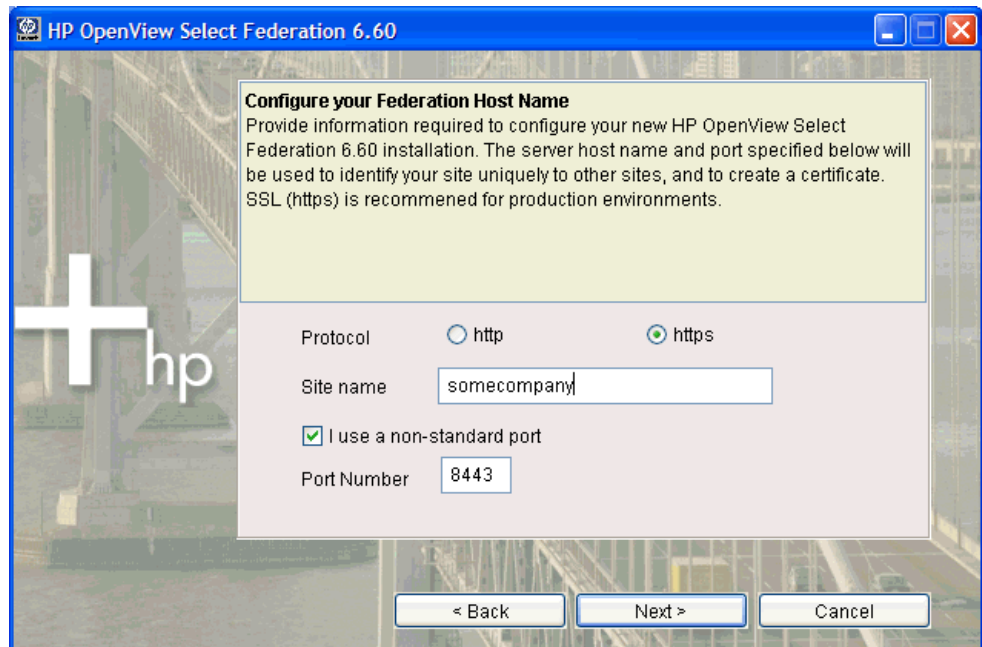
b **Configure the existing application server**.

The server host name and port specified are used to identify your site uniquely to other sites, and to create a signing certificate. SSL (https) is recommended for **production** environments. Click **Next** to continue.

6 **Select the destination directory.**

Use the **Browse** button to define the installation destination directory or enter the path information on the indicated space. The screen that you see will vary depending on which server you chose.

- If you chose to use the built-in application server, the specified path is the home (base) of the application server. Following is an example of a path for the built-in application:
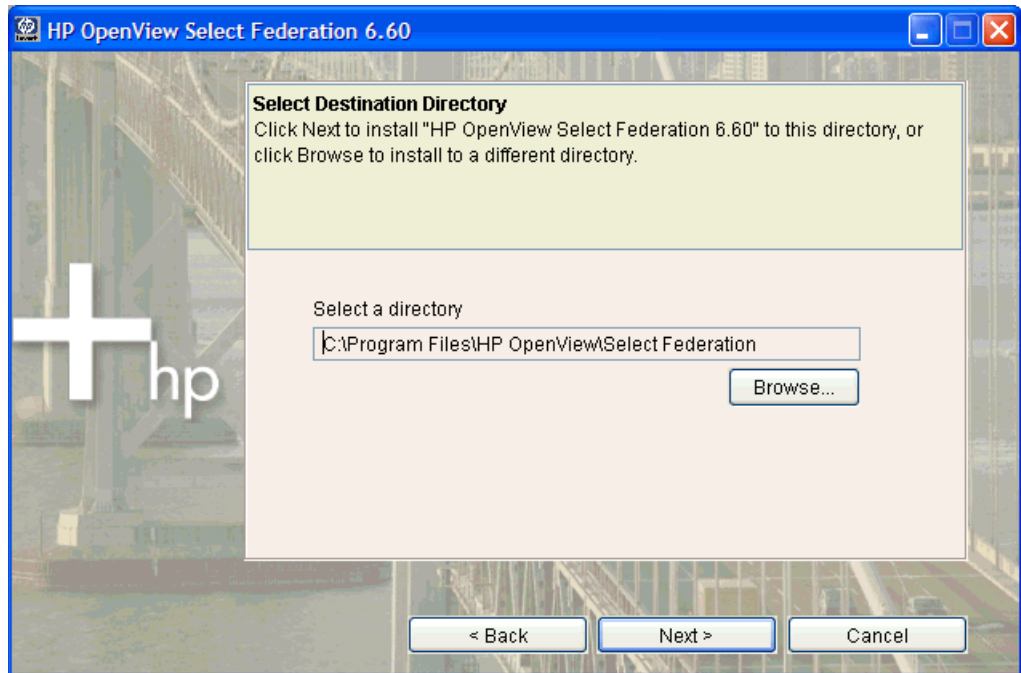
- If you chose an existing WebLogic or WebSphere server in your environment, specify the base directory (home) of the particular application server instance. Note that the base of the server could be different from the top-level home directory of the server.

For example, in the case of the BEA WebLogic application server, there is a notion of a "domain". A domain is the basic administration unit for WebLogic server instances. Therefore, if you created a domain called `sf66` in your Windows system, the installation directory that you specify should look something like the following:

`C:\BEA\user_projects\domains\sf66`

See the documentation of the application server you are using for additional help.

Click **Next** to continue..

➤ If you have previously installed Select Federation, make sure that the directory being specified in this step (the Destination Directory) does not contain configuration files from a previous installation of Select Federation. This may cause the installation to not function. These configuration files are normally removed by the Uninstaller, but if you have not used the uninstaller or if the uninstaller did not complete successfully, you need to verify this manually. See Chapter 7, Upgrading From Select Federation Version 6.5 for upgrading information.

Following is an example of the destination directory screen for the WebLogic server:
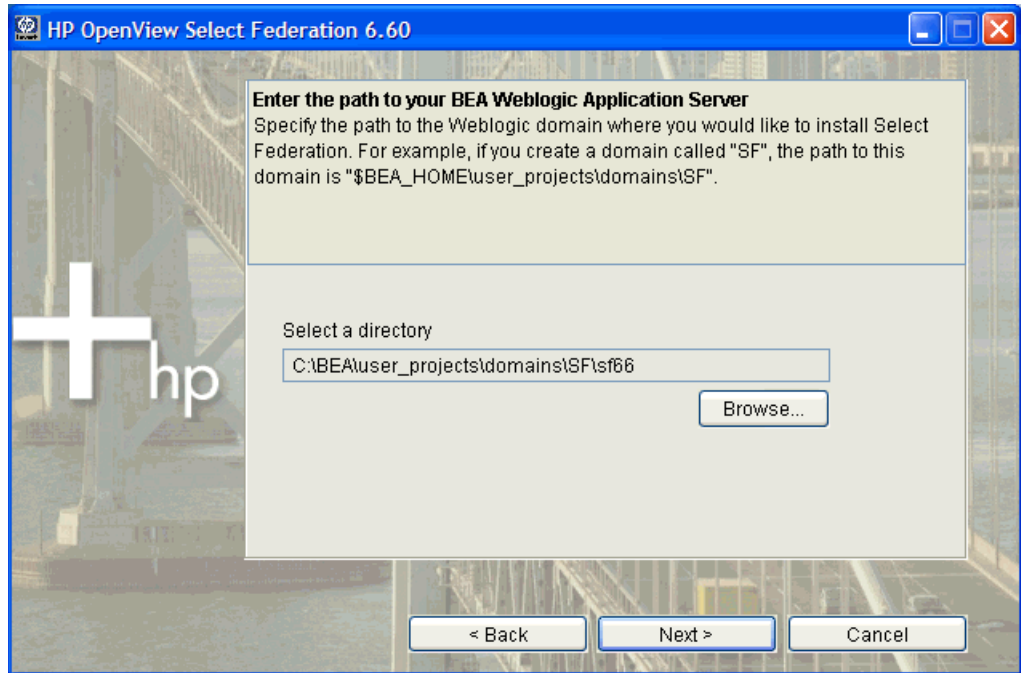
7   **Configure the Select Federation Keystore**.

Enter the Keystore password twice to create and open the keyfile that stores the signing key. The password must be at least 6 characters long. Click **Next** to continue.
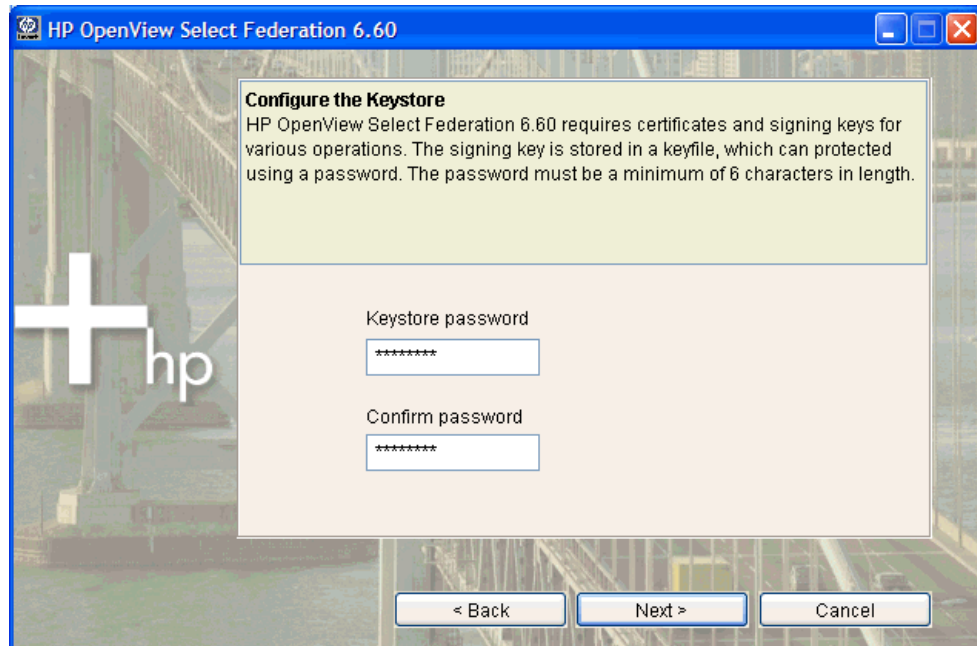
8   **Select a database**.

Choose the database you would like to use.
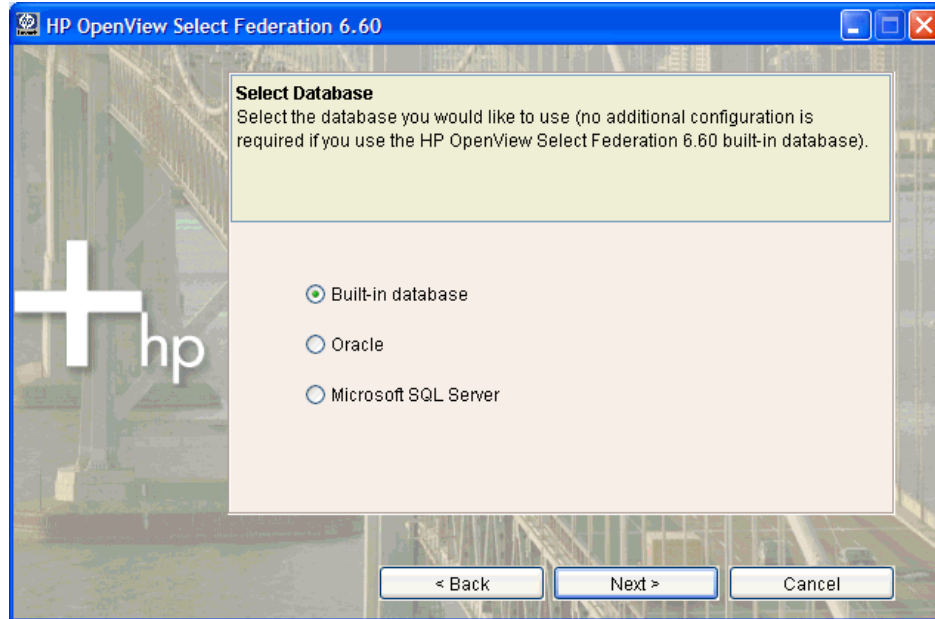
- If you choose the Select Federation built-in database, no further database configuration is necessary. Click **Next** and the Choose Mode of Deployment screen opens. Go to step 9 on page 28.

- If you choose one of the other databases, when you click **Next,** you are directed to the following two screens to configure the database.
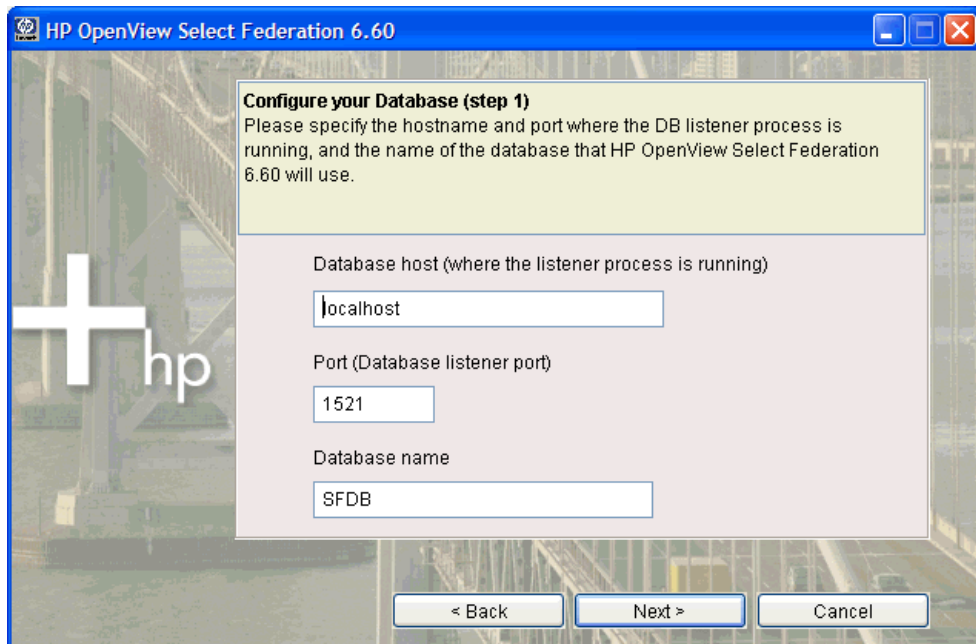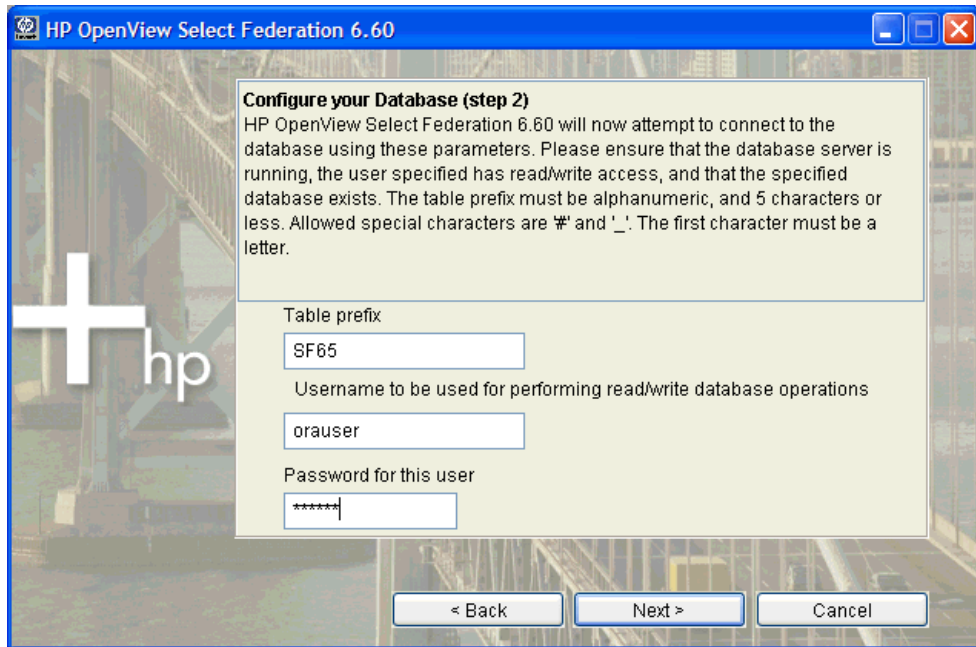
After you enter the database details, the Installer establishes a connection to the **database** with the supplied parameters. In case of any problems with connecting to the database, the Installer reports the error with supporting details of the exception. You need to take the appropriate corrective action in such an event. Click **Next** to continue.

9 **Choose a mode of deployment**.

Using the radio buttons, choose to deploy Select Federation in standalone mode or integrated with HP OpenView Select Access. Click **Next** to continue.
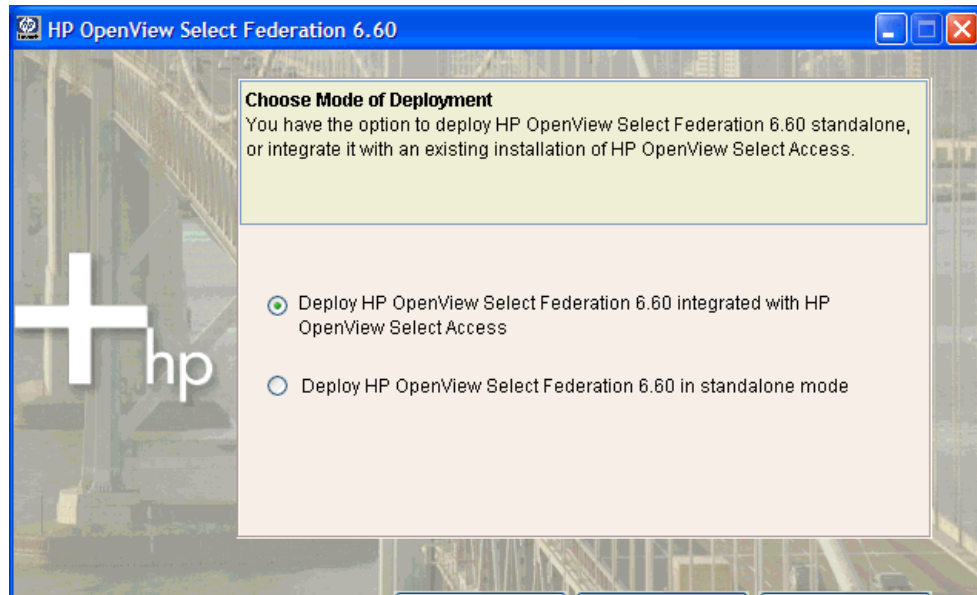
10 **(Optional) Integrate with HP OpenView Select Audit**.

Select **Integrate with HP OpenView Select Audit** and specify the Select Audit **Connector port**.
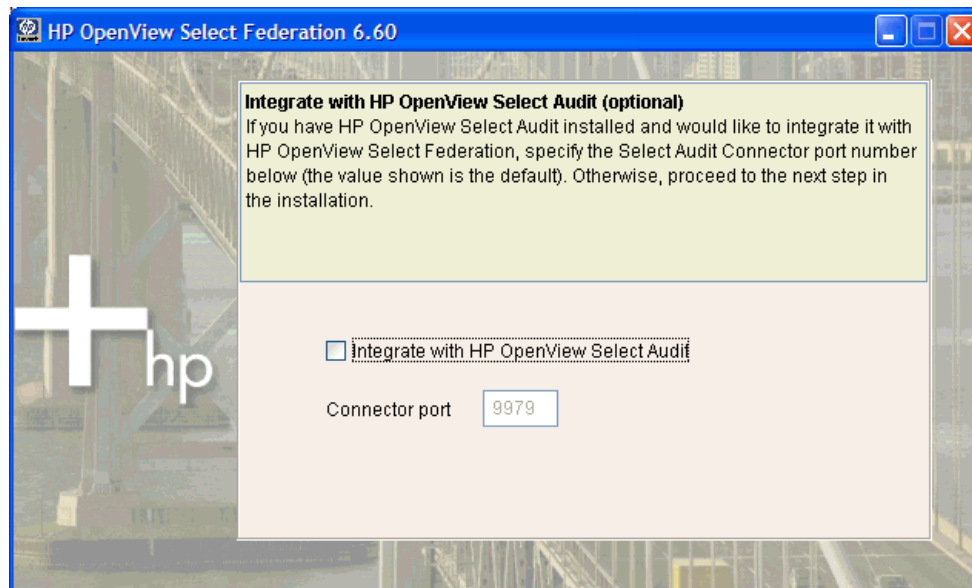
11 **Choose a site role**.

Choose your site role from either IDP and SP (both Identity Provider and Service Provider), IDP only or SP only configurations. Choosing a particular role enables functionality specific to that role. See Setting Your Site Role When Deploying Select Federation on page 10 for a description of site roles.

Click **Next** to continue.
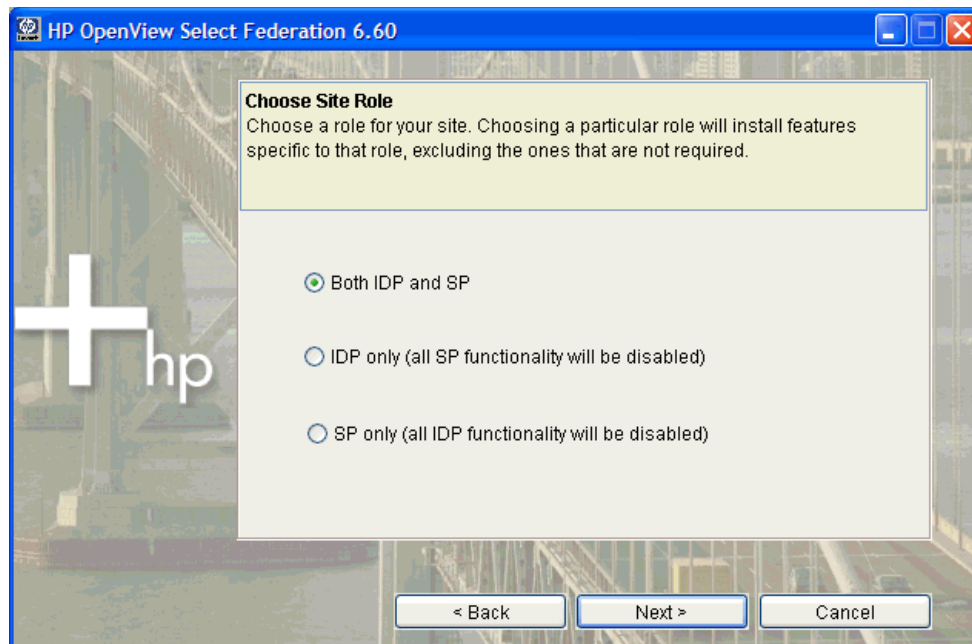
12 **Configure the profile service**.

Choose the profile service that you wish to configure. You are asked to choose the source of the profile information. This is the directory server that will be integrated with Select Federation and serve as the source for the user attribute information. Click **Next** to continue.
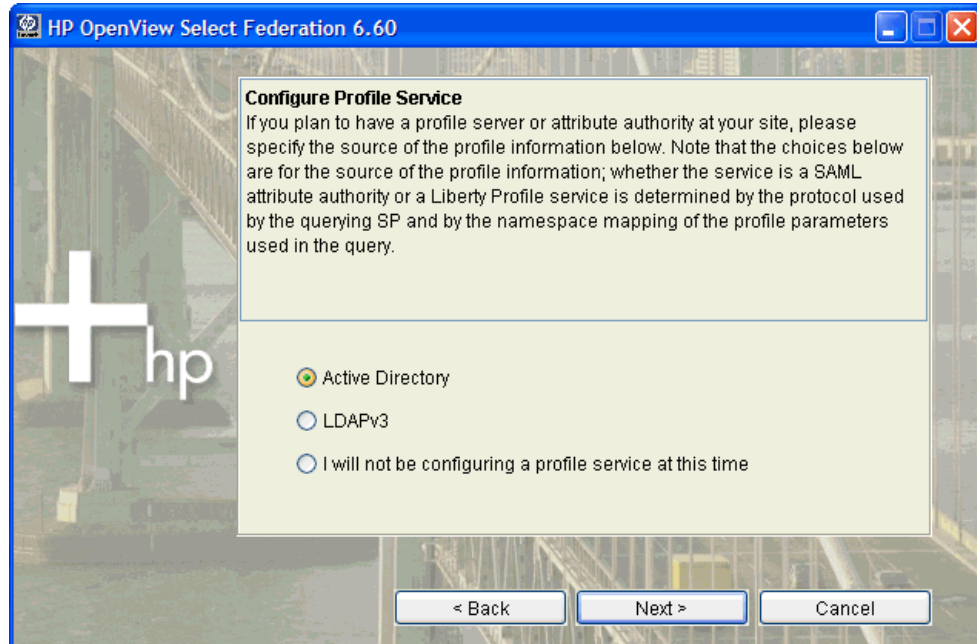
If you want to integrate Select Federation with your existing authentication environment (either off-the-shelf products or other implementations), there are other ways of integrating Select Federation that are not supported by the Installer. If you want to use this advanced integration with your environment, select the **I will not be configuring a profile service at this time** option.

When you choose the option **I will not be configuring a profile service at this time**, Select Federation uses a simple flat file to retrieve user attributes and authenticate users as follows:

- In Select Access integrated mode, Select Federation refers to this file to retrieve attributes only.

- In standalone-mode, Select Federation used this file for user authentication, retrieving attributes as well as verifying group membership.

This flat-file based configuration is not suited for real-world deployment, but acts as a stand-in until you plug in your own advanced implementation.

To enable these features and functions, you can use the Select Federation APIs. The Select Federation SDK includes sample code that can be used to integrate Select Federation with your existing environment. In addition, a directory plugin that can interface with the JDBC databases is documented in the "DirPlugin_JDBC: The JDBC Directory Plugin" section in the "Configuring Attributes" chapter of the *HP OpenView Configuration and Administration Guide*. You may use any of these options or develop your own plugin implementations or API-based implementations to achieve this.

13 **Configure the directory server**.

Depending on your choice, provide the following configuration details about either your ADS installation or any other LDAPv3 server such as SunOne. Then, click **Next** to continue.

- **PDC Name or IP** — Enter the Primary Domain Controller (PDC) or IP name.

- **Port** — Enter the port number.

- **Login name** — Enter the login name specified by the type of directory:

  — For LDAPv3 directory servers, enter the full DN suffix. For example:

    `cn=administrator,cn=users,dc=hp,dc=net`

  — For Active Directory, enter the user principal name of the administrative user. For example:

    `admin@domain.com`

- **Password** — Enter the login password.

- **Base DN** — The Base DN has a different meaning depending on whether you are integrating with Select Access.

  — For a standalone deployment (it is not integrated with Select Access), the Base DN is the location that the Identity Provider uses to look up and authenticate users.

  — For a deployment that is integrated with Select Access, the Base DN represents the location where new (incoming) users will be created at the Service Provider.

  ▶ If you are configuring Select Federation to use Active Directory, you will not be prompted for a base DN.

- **Connect to the directory server using SSL** — Select this checkbox if you would like Select Federation to use SSL to communicate with the directory server. This would require SSL to be previously set up on the directory server. See the next step for more information.
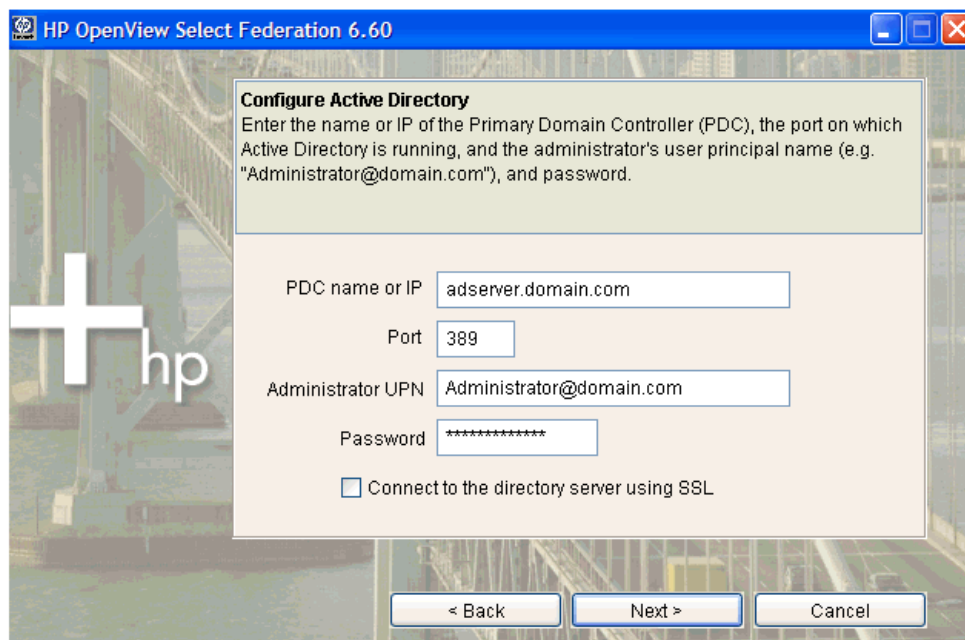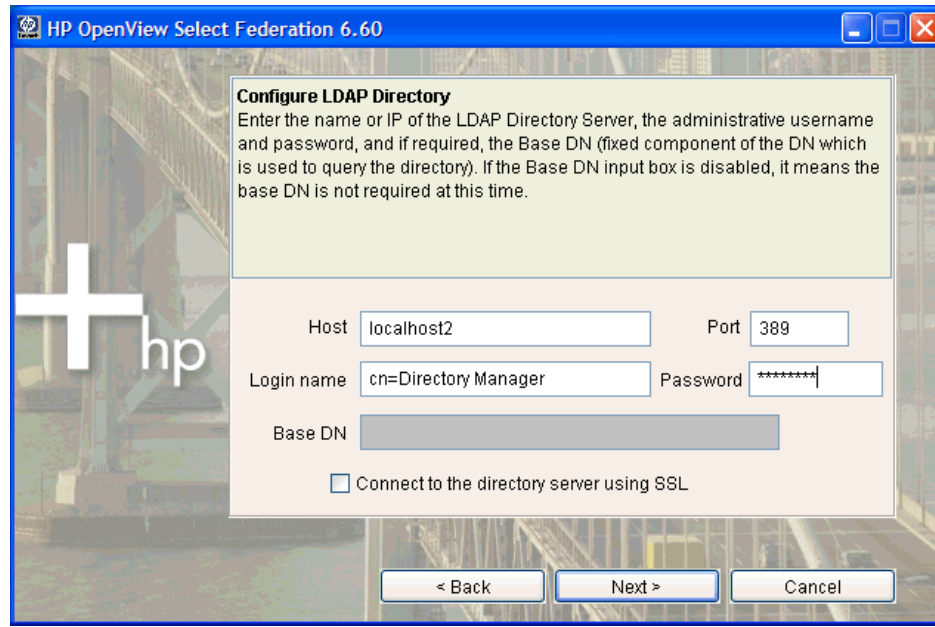
For the Active Directory or LDAPv3 configuration, the screens that follow depend on the provider type and deployment chosen.

a **Configuring the directory server with IDP and SP deploying with Select Access**

— Configure the Profile Service screen (choose Active Directory or LDAPv3 in step 12 Configure the profile service), followed by:

— Configure the Directory screen for the IDP with all the required parameters. You do not need the Base DN information for the IDP in this case.

— SP LDAP Base DN. Note that there is no prompt for other connection parameters, since that information is available from the previous IDP dialog.

► Make sure the Base DN you specify has the ability to create "Organizational Unit" or OU entries under it. For example, locations created in Active Directory through Select Access would not be able to accommodate OUs under them.
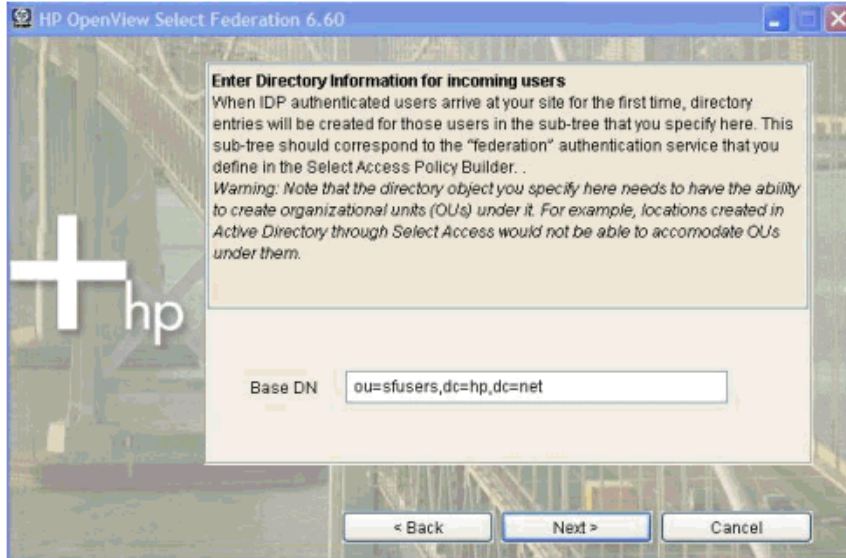
b **Configuring the directory server with IDP and SP deploying without Select Access**

— Configure the Profile Service screen (choose Active Directory or LDAPv3 in step 12 Configure the profile service), followed by:

— Configure the Directory server screen for the IDP.
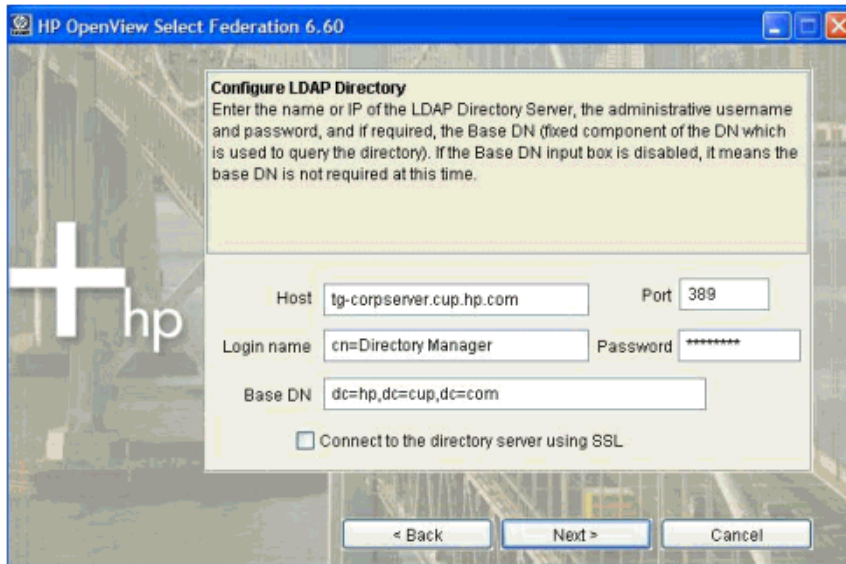
c **Configuring the directory server with IDP only deploying with Select Access**

— Configure the Profile Service screen (choose Active Directory/LDAPv3 in step 12 Configure the profile service), followed by:

— Configure the Directory server screen for the IDP. The Base DN information for the IDP is not needed.

d **Configuring the directory server with IDP only deploying without Select Access**

— Configure the Profile Service screen (choose Active Directory/LDAPv3 in step 12 Configure the profile service), followed by:

— Configure the Directory server screen for the IDP.

e **Configuring the directory server with SP deploying with Select Access**

— Configure the Profile Service screen (choose Active Directory/LDAPv3 in step 12 Configure the profile service), followed by:

— LDAP connection information screen for the SP, which is used for incoming IDP authenticated users.

➤ Make sure that the Base DN you specify has the ability to create "Organizational Unit" or OU entries under it. For example, locations created in Active Directory through Select Access would not be able to accommodate OUs under them.
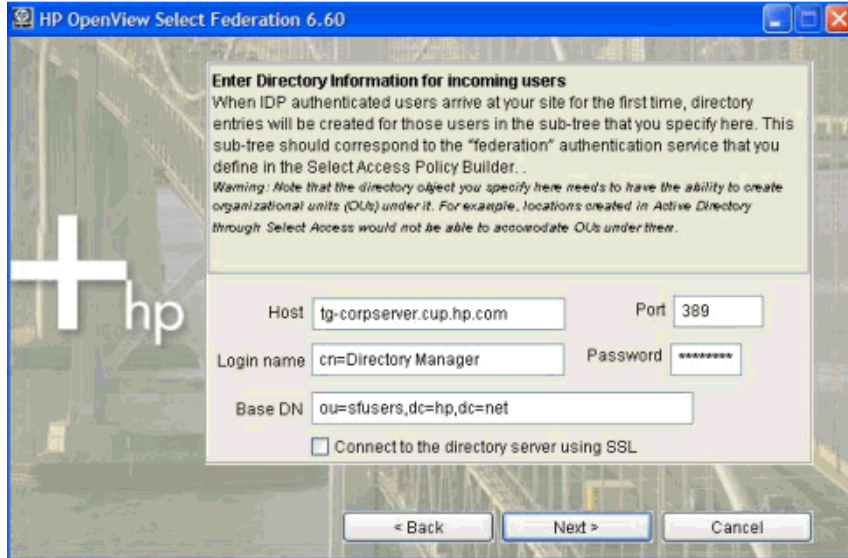
f **Configure the directory server with SP only deploying without Select Access**

No LDAP or Active Directory configuration is required.

14 **(Optional) Configure additional directory server parameters.**

This screen opens only if you chose LDAPv3 as the Directory server.

- If required, you can change the name of the attribute that contains the user id from `cn` to something like `uid`.

- Select the **Enable sub-tree search for Directory** checkbox to enable a sub-tree search in your directory. Click **Next** to continue.
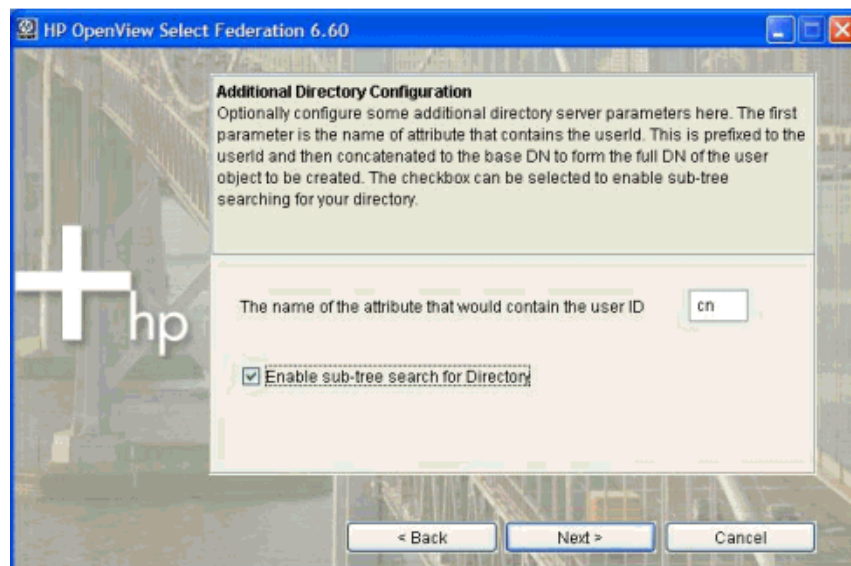
15 **Install Select Federation**.

Verify that the installation information is correct and click **Install**. Installation progress is shown in a progress bar as percentage completed.

16 **View the summary information**.

Verify that the installation has been successful by reading the summary information. Click **Finish**. The Installer launches a browser window to your site and closes.

Finishing Installation

After you install Select Federation, you need to deploy it on the application server you chose during the installation process, as described in the following sections.

▶ If you need more advanced configuration changes, such as for attributes, privacy management, and so on, you can further configure Select Federation by editing the `tfsconfig.properties` file. See the "Customizing Select Federation" chapter in the *HP OpenView Select Federation Configuration and Administration Guide* for details.

Deploying on an Existing Application Server

If you chose to deploy Select Federation on an existing application server, there are a few simple steps required to complete the installation process.

Perform the following steps and links to complete the installation process:

1 Deploy Select Federation on an existing server:

   — See Deploying Select Federation on the BEA WebLogic Server on page 43, or

   — See Logging for WebLogic and WebSphere on page 50.

2 Verify that Select Federation is installed successfully by navigating to the Select Federation Administration Console.

Deploying on the Select Federation Built-In Application Server

If you chose to deploy Select Federation on the built-in application server, you must start and stop the built-in application server from the installation directory. Otherwise, the server may not start or stop correctly.

▶ Choosing the Built-In Application Server option during installation installs Select Federation as a service that automatically starts/stops during system startup and shutdown.

On Windows servers, the Select Federation service is registered as "HP OpenView Select Federation." On Linux, Solaris and HP-UX, `init` scripts containing start/stop commands are installed, which are invoked at different run levels.

Starting and Stopping the Built-In Application Server on Linux, Solaris or HP-UX

To start the built-in application server on Linux, Solaris or HP-UX, enter the following commands:

    cd $SF_HOME/

    ./bin/startup.sh

To stop the server on Linux, Solaris or HP-UX, enter the following commands:

    cd $SF_HOME/

```
./bin/shutdown.sh
```

Starting and Stopping the Built-In Application Server on Windows

To start the built-in application server on Windows, enter the following commands:

```
cd $SF_HOME/

./bin/startup.bat
```

To stop the server on Windows, enter the following commands:

```
cd $SF_HOME/

./bin/shutdown.bat
```

Uninstallation

If for some reason you need to uninstall Select Federation, you can use the uninstaller located in `sf_uninst/uninstaller` in the directory where you installed Select Federation. Follow the on-screen instructions and select the features that you want to uninstall. See Figure 1.

The following figures show Windows uninstallation screens. Uninstallation on other supported operating systems is the same except for a pop-up dialog asking you to stop the server before uninstallation.

➤ Make sure that you stop the Select Federation server before starting the Uninstall wizard. If your Select Federation instance is running on the built-in application server, follow the instructions in Deploying on the Select Federation Built-In Application Server on page 36. Otherwise, see the specific application server's administration guide for instructions on stopping the server.

Figure 1   Uninstallation Welcome Page
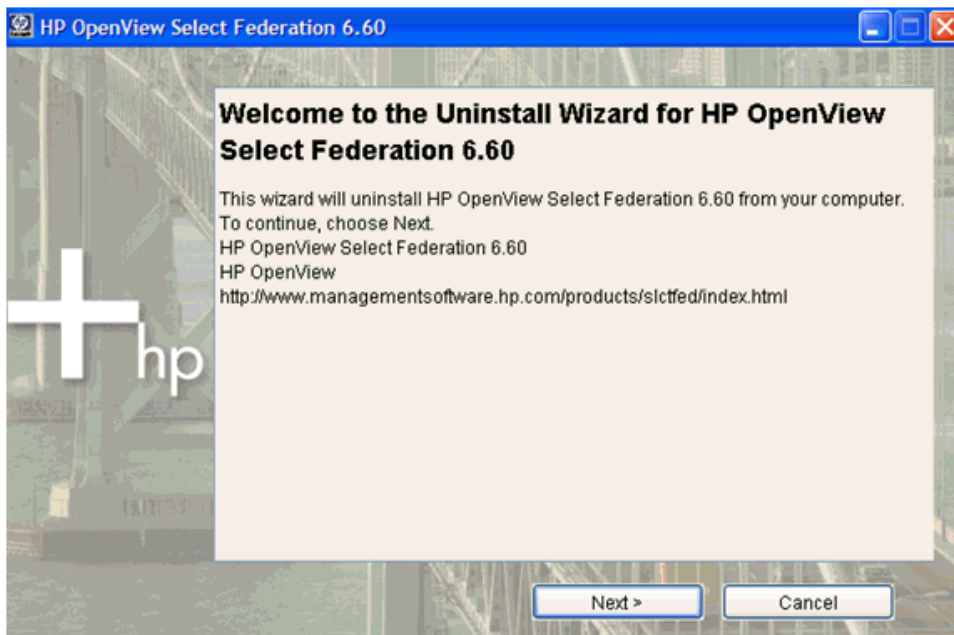
Figure 2   Uninstallation Summary Page
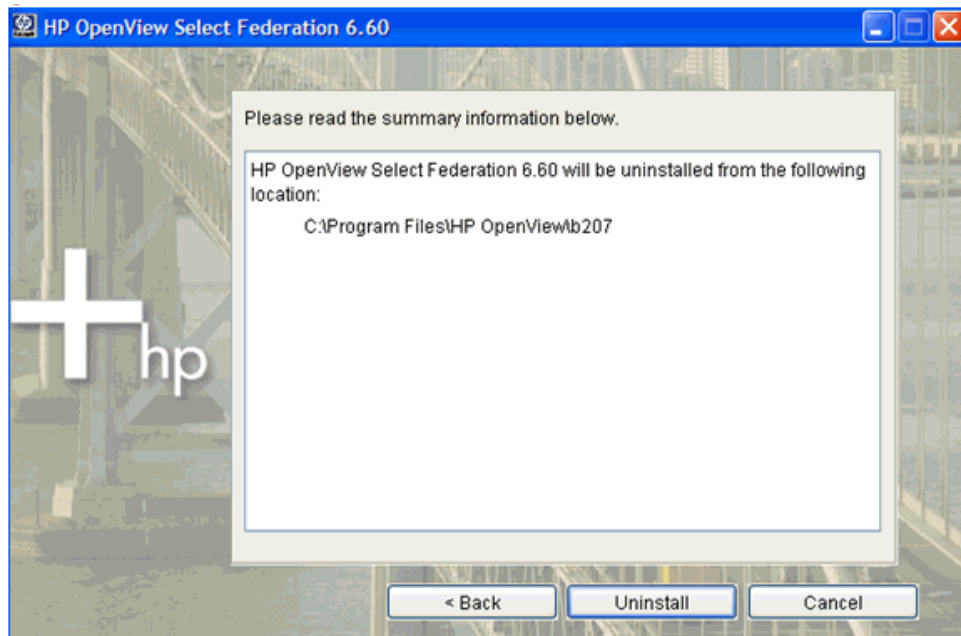
If you installed Select Federation with either Oracle or MSSQL as the database, a dialog will open asking you if you would like to delete the tables being used by this instance. If you have a clustered environment with multiple Select Federation instances, it is possible that some other instance might be using these tables. Be sure the tables are not being used before deleting the tables.

4 Select Federation Deployment Considerations

Deployment Methods

Select Federation may be deployed in three different ways, depending on your existing architecture and the level of redundancy you need. (See Chapter 5, Deploying the Installed Select Federation on an Existing Application Server for more information.)

- Three-tier deployment
- Multi-server deployment
- Redundancy

Three-tier deployment

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

Multi-server deployment

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

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

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

Redundancy

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

Considerations for a Production Deployment

Further Select Federation configuration and maintenance is mainly performed by editing the `tfsconfig.properties` system configuration file.

Whereas the install process sets up a fully functional system, a large-scale production environment can greatly benefit from some further configuration. Some hints and tips have been collected below.

➤ It is recommended that you deploy `tfs-internal` on a separate server for security reasons. This way, no one can get to Select Federation from the internet.

End User Considerations

During evaluation, it is typical for technical personnel to interact with the system, whereas in a production deployment, most end users will have little or no knowledge about federation. Hence it will important to ensure that the end user experience meets expectations. It is worth to consider the following:

- **Branding end user pages** through the presentation service stylesheets (see "Branding the End User Pages" in the *HP OpenView Select Federation Configuration and Administration Guide*)

- The **errorDetails** configuration entry

- The **look and feel** of the login page

Performance and Reliability Considerations

System performance is greatly dependent on the overall deployment architecture. In general, Select Federation is a set of web applications, so considerations for the performance of web applications do apply. Some examples include:

- **Use of data sources can greatly enhance performance.** Data source setup is dependent on the application server in use. If data sources are used, the system configuration entry for `jdbcDataSource` should be set accordingly. Note that this entry could appear in all configuration files.

- **Clustering provides scalability and reliability.** Note that the various web application deployment descriptors in the `tfs.ear` file refer to the `conf/tfsconfig.properties` file. Therefore, each node in the cluster needs its own copy of the configuration directory. Alternatively, a shared file system can be used. In that case the `tfs.ear` file needs to be unpacked and each of the `.war` files in it need to be unpacked. In the unpacked web applications the `WEB-INF/web.xml` files need to be edited in such a way that the `<env-entry>` element points to the correct location of the system configuration file. Note that whereas such use of a shared file system may be convenient from a configuration maintenance point of view, it is less advantageous from a reliability point of view. The shared directory becomes a single point of failure.

- Provide the Base DN for the IDP where your users will be authenticated (only if Select Federation is configured to use Active Directory). If you configured Select Federation to use an Active Directory Server, the default behavior is to perform a search using the rootDSE of your directory server (the root of your AD forest) as the base DN. If your Active Directory forest is fairly large, this might lead to high latencies during user

authentication and attribute query operations. Therefore, it is recommended that you set the exact base DN and the value of the RDN attribute that should be used for authenticating users as shown in the example below:

```
ldapUserBaseDN=OU=sf,OU=ov,OU=hp,DC=domain,DC=com
```

```
ldapUserAttr=cn
```

Security

Security is an important aspect of a production deployment. Select Federation has a good level of security in a standard deployment, but again it is advisable to consider at least the following aspects:

- HPSF needs to access various databases and other components that most probably should reside in an protected intranet. A good solution is to have a web proxy.

- The `tfs-internal` web application should be accessible only to administrators. It is advisable to deploy this web application on a separate application server that is not reachable from the Internet. Also, if Select Access is used for authentication, the Select Access policies should be set up in such a way that only authorized administrators have access.

- File permissions on Select Federation configuration files such as the `tfsconfig.properties` file, should be set up so that they are readable only by the Select Federation server and administrators.

- Passwords stored in the configuration files can be masked by running a utility called `ConfigPasswordMask.bat` on Windows and `ConfigPasswordMask.sh` on UNIX. This utility is located in `<SF_Install_Dir>/tools/config`.

  You can use this utility to mask passwords for the following fields in the `tfsconfig.properties` file:

  - `ldapPassword`
  - `jdbcPassword`
  - `keystorePassword`
  - `keyPassword`
  - `encKeystorePassword`
  - `encKeyPassword`
  - `pkixCertValidation.caKeystorePassword`

  Usage for this utility is:

```
ConfigPasswordMask.bat passwordToBeMasked.
```

  This returns the masked password which can then be replaced in the `tfsconfig.properties` file.

  For example, if `keystorePassword=changeit` is in the `tfsconfig.properties` file, administrators can run the `ConfigPasswordMask.bat/sh` and mask the password to prevent obvious disclosure of the `keystorePassword`. The value returned by this utility should be replaced by the administrator in the `tfsconfig.preperties` file. The keystorePassword parameter would appear as follows in `tfsconfig.properties`:

```
keystorePassword= {Mask}OTI7ND0/My4=
```

  Example of usage on Windows:

```
C:\test-area\idp\inst7500\tools\config>ConfigPasswordMask.bat
Usage: ConfigPasswordMask password

C:\test-area\idp\inst7500\tools\config>ConfigPasswordMask.bat changeit
{Mask}OTI7ND0/My4=
```

Example usage on UNIX:

```
/cygdrive/c/test-area/idp/inst7500/tools/config
$ ./ConfigPasswordMask.sh
Usage: ConfigPasswordMask password

/cygdrive/c/test-area/idp/inst7500/tools/config
$ ./ConfigPasswordMask.sh changeit
{Mask}OTI7ND0/My4=
```

5 Deploying the Installed Select Federation on an Existing Application Server

▶ Select Federation must be installed to deploy it on an application server. If you have not installed Select Federation, follow the instructions in Chapter 3, Installing Select Federation.

The Select Federation Installer can install a built-in application server during the installation procedure. However, if you want to use an existing application server instead, you need to follow these basic steps to deploy the server:

1 Refer to the configuration file from the WAR files.

2 Deploy the configured EAR.

3 Run the EAR.

For production environments, it is recommended that you use JDBC Data Sources to improve performance with Select Federation. Using data sources also reduces the number of times a database connection is opened and closed. The JDBC Data Sources need to be turned on explicitly by going through certain configuration steps. See Configuring JDBC Data Sources on page 52 for configuration instructions for each application server.

The deployment process is dependent upon the particular application server you wish to use. Deployment for BEA Weblogic and IBM WebSphere application servers is explained in more detail in the following sections:

- Deploying Select Federation on the BEA WebLogic Server
- Deploying Select Federation on the IBM WebSphere 6.0.2 Server
- Testing the Deployment
- Configuring JDBC Data Sources

Deploying Select Federation on the BEA WebLogic Server

Complete the following tasks to deploy Select Federation on the BEA WebLogic Server Versions 8.1 and 9.1. Tasks 1 through 5 are common for both 8.1 and 9.1:

- Task 1: Verify configuration
- Task 2: Use the recommended JDK
- Task 3: Configure the JDBC DataSource for WebLogic
- Task 4: (Windows only) Modify the server class path
- Task 5: Enable logging for WebLogic
- Task 6: For WebLogic 8.1, deploy the configured EAR
- Task 7: For WebLogic 9.1, deploy the configured EAR

Task 1:   Verify configuration

After the Installer has successfully installed Select Federation, verify that the `conf` directory exists in the WebLogic domain that was specified as the destination directory during installation.

Task 2:   Use the recommended JDK

BEA WebLogic comes bundled with two JDKs:

*   JRockit JDK

*   Sun JDK.

It is recommended that you use the Sun JDK for the server domain where Select Federation is installed.

Task 3:   Configure the JDBC DataSource for WebLogic

The JDBC DataSource used by Select federation needs to be set up on the WebLogic domain where Select Federation is to be deployed.

*   If you are deploying Select Federation on WebLogic 8.1, see Configure Data Sources in BEA WebLogic 8.1 on page 53 for configuration instructions.

*   If you are deploying Select Federation on WebLogic 9.1, see Configure Data Sources in BEA WebLogic 9.1 on page 55 for configuration instructions.

*   Be sure to follow the instructions in Configure Select Federation to Use the Configured Data Source in the Application Server on page 60.

Task 4:   (Windows only) Modify the server class path

This step is required only if you have deployed Select Federation on Windows, and integrated with Select Access. If you have a standalone Select Federation deployment, or if you deployed it on any of the other supported operating systems, go to the next task.

The Select Federation package is a J2EE "Enterprise Archive" or EAR located at `$SF_HOME/sf_ear/tfs.ear` in the distribution.

To modify the server class path, perform the following steps:

1   Unpack the `EAR`:

   a   Create a new directory (`<staging-directory>` directory in the example below) in a working area.

   b   Unpack the `EAR` in the `<staging-directory>` directory using the following commands:

```
% mkdir <staging-directory>

% cd <staging-directory>

% jar xf $SF_HOME/sf_ear/tfs.ear
```

The `<staging-directory>` then contains a number of files, some with the extension `.jar`, others with the extension `.war` and a `META-INF` directory.

2   Open the `startWebLogic.cmd` server startup script to edit the server class path.

The startup script is located in `$DOMAIN_HOME` for WebLogic 8.1 or `$DOMAIN_HOME/bin` for WebLogic 9.1. This is the path to the WebLogic domain where Select Federation is installed.

3   Add the following `JAR` files in the `<staging-directory>` to the BEA WebLogic class path:

- `bcprov-jdk14.jar`

- `castor-0.9.3.19-xml.jar`

- `EnforcerAPI.jar`

- `jakarta-oro-2_0.jar`

- `jdom.jar`

- `ldapjdk.jar`

- `msgsresources.jar`

- `protomatter.jar`

- `servletenforcer.jar`

- `shared.jar`

- `xml.jar`

- `xmlsec.jar`

- `selectauditclient.jar`

- `commons-pool-1.2.jar`

- `commons-logging.jar`

- `log4j-1.2.5.jar`

- `xalan.jar`

- `xerceslmpl.jar`

- `xml-apis.jar`

- `xmlParserAPIs.jar`

Following are examples of appending the above jar files to the class path. The `<staging-directory>` is the location of the jar files.

> The existing default class path entries may be different based on WebLogic versions, fix packs and any other configuration changes.

Default classpath:

```
set
CLASSPATH=%WEBLOGIC_CLASSPATH%;%POINTBASE_CLASSPATH%;%JAVA_HOME%\jre\lib\
rt.jar:%WL_HOME%\server\lib\webservices.jar;%CLASSPATH%
```

Updated classpath:

```
set
CLASSPATH=%WEBLOGIC_CLASSPATH%;%POINTBASE_CLASSPATH%;%JAVA_HOME%\jre\lib\
rt.jar:%WL_HOME%\server\lib\webservices.jar;<staging-directory>\bcprov-jd
k14.jar;<staging-directory>\castor-0.9.3.19-xml.jar;<staging-directory>\E
nforcerAPI.jar;<staging-directory>\jakarta-oro-2_0.jar;<staging-directory
>\jdom.jar;<staging-directory>\dapjdk.jar;<staging-directory>\msgsresourc
es.jar;<staging-directory>\protomatter.jar;<staging-directory>\servletenf
orcer.jar;<staging-directory>\shared.jar;<staging-directory>\xml.jar;<sta
ging-directory>\xmlsec.jar;<staging-directory>\selectauditclient.jar;<sta
ging-directory>\commons-pool-1.2.jar;%CLASSPATH%
```

4   If your WebLogic server is running, you need to stop and restart the WebLogic server.

stopWebLogic.cmd

startWebLogic.cmd

Task 5:   Enable logging for WebLogic

Select Federation uses the log4j.properties file in the $SF_HOME\properties directory to log errors to the console. See Logging for WebLogic and WebSphere on page 50 for more information about the log4j.properties file.

You need to enable the log4j.properties file and set the logging level to DEBUG to provide detailed logging messages.

To enable logging and set the DEBUG logging level, perform the following steps:

1   Be sure you have the commons-logging.jar file in a *<staging-directory>* directory you create.

If you do not have the commons-logging.jar file, follow the instructions in step 1 in Task 4 on page 44 to unpack the $SF_HOME/sf_ear/tfs.ear and copy the commons-logging.jar file to the *<staging-directory>*.

2   Open the server startup script (startWebLogic.cmd for Windows and startWebLogic.sh for UNIX) to edit the server class path.

The startup script is located in $DOMAIN_HOME for WebLogic 8.1 or $DOMAIN_HOME/bin for WebLogic 9.1. This is the path to the WebLogic domain where Select Federation is installed.

- For WebLogic 8.1, the startup script path is as follows:

    Windows: $DOMAIN_HOME\startWebLogic.cmd

    UNIX: $DOMAIN_HOME/startWebLogic.sh

- For WebLogic 9.1, the startup script path is as follows:

    Windows: $DOMAIN_HOME\bin\startWebLogic.cmd

    UNIX: $DOMAIN_HOME/bin/startWebLogic.sh

3   Add the $SF_HOME\properties directory that contains the log4j.properties file to the server class path as follows:

c   Define the SF_HOME and SF_JARS variables for Windows or UNIX:

— For Windows:

    set SF_HOME=*<Destination_directory_chosen_during_installation>*

    set SF_JARS=*<path to the staging directory created above>*

— For UNIX:

    SF_HOME=*<Destination_directory_chosen_during_installation>*

    SF_JARS=*<path to the staging directory created above>*

d   Add the following to the CLASSPATH variable:

— For Windows:

    %SF_HOME%\properties;%SF_JARS%\commons-logging.jar;*<optionally_all_ other_jars>*

— For UNIX:

```
${SF_HOME}/properties:${SF_JARS}/commons-logging.jar:
<optionally_all_other_jars>
```

4 Change the logging level in the `log4j.properties` file from INFO to DEBUG:

```
log4j.rootLogger=DEBUG, A1
```

Task 6:   For WebLogic 8.1, deploy the configured EAR

1 Open a browser window and start the BEA WebLogic Console for the domain on which Select Federation is to be deployed.

   In a single server configuration, the console is typically at the URL path `/console` in the server.

2 In the left pane, select the **Applications** container. Then click **Configure a New Application** in the right pane.

3 In the next screen (**Load Application or Components to Configure**), follow the two steps given on the **Locate Application or Component to Configure** page as follows:

   a Upload the `$SF_HOME/sf_ear/tfs.ear`.

   b Select the `tfs.ear` in the list seen at the bottom of the screen.

4 In the next screen (**Configure Application or Component**), select the WebLogic server instance on which you wish to deploy Select Federation and then click **Configure and Deploy**.

   In the next screen, you will see Select Federation being deployed and eventually see the status of the **Activate application tfs on <server>** as **Completed**.

▶ If anything goes wrong in running Select Federation, you can check the `log4j.properties` file for DEBUG messages, which you set in Task 5 on page 46.

Task 7:   For WebLogic 9.1, deploy the configured EAR

1 Add the `xalan.jar` and `xercesImpl.jar` files that are in the `$DOMAIN_HOME/ redist` directory to the `<SELECTED_BEA_JDK>/jre/lib/endorsed` directory.

   If the `endorsed` directory does not exist, create it.

2 Start the WebLogic Administration server for the Select Federation profile.

3 *For Unix installations only*: If Select Federation is installed as a user other than root, then write permission should be granted to create the following directory:

   /var/opt/hpsupport

4 Click on the **Lock and Edit** button in the top-left navigation section of the console.

5 Click on **Deployments** in the left pane on the Console.

6 Click on the **Install** button on the main pane of the screen.

7 Navigate to the `sf-ear` folder created by the Select Federation installation in the weblogic domain.

8 Select `tfs.ear` and click the **Next** button.

9 Make sure that the **Install this deployment as an Application** button is selected and click **Next** to continue.

10 Make sure the following values are selected on this page and click **Next** to continue:

    Name: **tfs**

Security: **DDOnly**

Source Accessibility: Use the default defined by the deployment descriptors.

Location: **<location of sf_ear>\tfs.ear**

11 Select the following option:

Additional Configuration: No, I will review the configuration later.

12 Click the **Finish** button to complete the deployment.

13 Click on the **Activate Changes** button that appears on the upper-left corner of the screen.

14 Select the check box beside **tfs** on the Deployments screen.

The State column shows tfs as **Prepared**.

15 Click on the **Start** button and select **Service all requests**.

16 On the confirmation page click **Yes**.

The State column now shows tfs as **Active**. The application is now available for use.

▶ If anything goes wrong in running Select Federation, you can check the `log4j.properties` file for DEBUG messages, which you set in Task 5 on page 46.

Deploying Select Federation on the IBM WebSphere 6.0.2 Server

Deploy Select Federation on WebSphere 6.0.2 by completing the following tasks:

• Task 1: Verify configuration

• Task 2: Configure the JDBC DataSource for WebSphere

• Task 3: Deploy the configured EAR on IBM WebSphere

• Task 4: Configure logging

Task 1: Verify configuration

After the Installer has successfully installed Select Federation, verify that the `conf` directory exists in the WebSphere server profile that was specified as the destination directory during installation.

Task 2: Configure the JDBC DataSource for WebSphere

The JDBC DataSource used by Select federation needs to be set up on the WebSphere profile where Select Federation is to be deployed.

• If you are deploying Select Federation on WebSphere 6.0.x, see Configure Data Sources in IBM WebSphere 6.0.2 on page 57 for configuration instructions.

• Be sure to follow the instructions in Configure Select Federation to Use the Configured Data Source in the Application Server on page 60.

Task 3: Deploy the configured EAR on IBM WebSphere

Perform the following steps to deploy the configured EAR on WebSphere:

1 Start the IBM WebSphere server that has the administration console.

2	Point your browser to the administration console. You can do this by clicking the **Administration Console** option in the **First Steps** program or by typing in the URL (typically in the /ibm/console of the administration port of the application server).

3	In the left pane, expand the **Applications** container. Then click **Install New Application** in the left-pane.

4	In the right pane, locate the Select Federation EAR (at $SF_HOME/sf_ear/tfs.ear), click **Next**.

5	In the next 4 screens (shown as steps 1 through 4 in the right pane), click **Next** on all screens and then click **Finish** in the end.

6	Click **Save to Master Configuration** in the resulting screen, and click **Save** again in the next screen.

7	Click **Enterprise Applications** in the left-pane.

	The new **Select Federation** appears in the list in the right pane.

8	Check the box next to the line corresponding to Select Federation and click **Start**.

	When the server starts, a green arrow appears in the right pane. Select Federation will be running.

Task 4:	Configure logging

Select Federation uses the log4.properties file in the $SF_HOME\properties directory for diagnostic logging. These messages can be seen in the server console, which is written to the log file, <profile>\logs\server1\SystemOut.txt. Any changes to the log4.properties file is reflected in the <profile>\logs\server1\SystemOut.txt file.

You need to configure logging and set the logging level to DEBUG to provide detailed logging messages. See Logging for WebLogic and WebSphere on page 50 for more information.

To configure logging and set the DEBUG logging level, perform the following steps:

1	Log in to the WebSphere Administrative console of the Select Federation profile.

2	Select **Servers → application servers** on the left navigation bar.

3	Click on **server1** on the main panel.

4	Click on **Process Definition** under Java and Process Management.

5	Click on **Java Virtual Machine**.

6	Add the path up to the properties folder where the log4j.properties file is located in the Classpath text box.

	For example: /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/properties

7	Stop and restart the WebSphere server.

	•	For Windows:

		stopWebSphere.cmd

		startWebSphere.cmd

	•	For UNIX:

		./stopWebSphere.sh

		./startWebSphere.sh

8	Change the logging level in the log4j.properties file from INFO to DEBUG:

	log4j.rootLogger=DEBUG, A1

Logging for WebLogic and WebSphere

Select Federation provides a logging file for WebLogic and WebSphere called `log4j.properties` in the `$SF_HOME\properties` directory. This file defines how Select Federation logs messages and exceptions when deployed on WebLogic or WebSphere. You can specify the level of logging output for all messages. You can set the logging levels from FATAL (smallest amount of log information) to DEBUG (greatest amount of log information). The default is INFO.

The main logging levels are defined as follows (listed in order of decreasing amount of information that is sent to the logs):

- DEBUG — Specifies logging of detailed informational messages that are helpful for debugging an application.

- INFO — Specifies logging of general information about the progress of the application without much detail.

- WARN - Specifies logging of potentially harmful situations.

- ERROR - Specifies logging of error events that might still allow the application to continue running.

- FATAL - Specifies logging of severe error events that may abort the application.

Following are the contents of the `log4j.properties` file:

```
# Set root logger level to INFO and its only appender to A1.
log4j.rootLogger=INFO, A1

# Suppress output from xml-security library
log4j.logger.org.apache.xml.security=FATAL
log4j.logger.org.apache=FATAL

# A1 is set to be a ConsoleAppender.
log4j.appender.A1=org.apache.log4j.ConsoleAppender

# A1 uses PatternLayout.
log4j.appender.A1.layout=org.apache.log4j.PatternLayout
log4j.appender.A1.layout.ConversionPattern=[%d{ISO8601}|%t|%p] %c %x -
%m%n
```

To see the logging errors, you need to enable the `log4j.properties` file. For instructions, see Task 5 in Deploying Select Federation on the BEA WebLogic Server on page 43 or Task 4 in Deploying Select Federation on the IBM WebSphere 6.0.2 Server on page 48.

Testing the Deployment

You are now ready to test if Select Federation has been deployed. Navigate to the Select Federation Administration Console home page. If you have deployed Select Federation Admin WAR to the URL path `/tfs-internal` on your server `sf.mycompany.com`, then the home page for Select Federation is `https://sf.mycompany.com/tfs-internal`.

When you enter the URL, the Select Federation Administration Console startup page opens with links to the documentation and various resources. It also includes a link to the Administration Console, as shown in the following figure.

Figure 3   Select Federation Startup Page
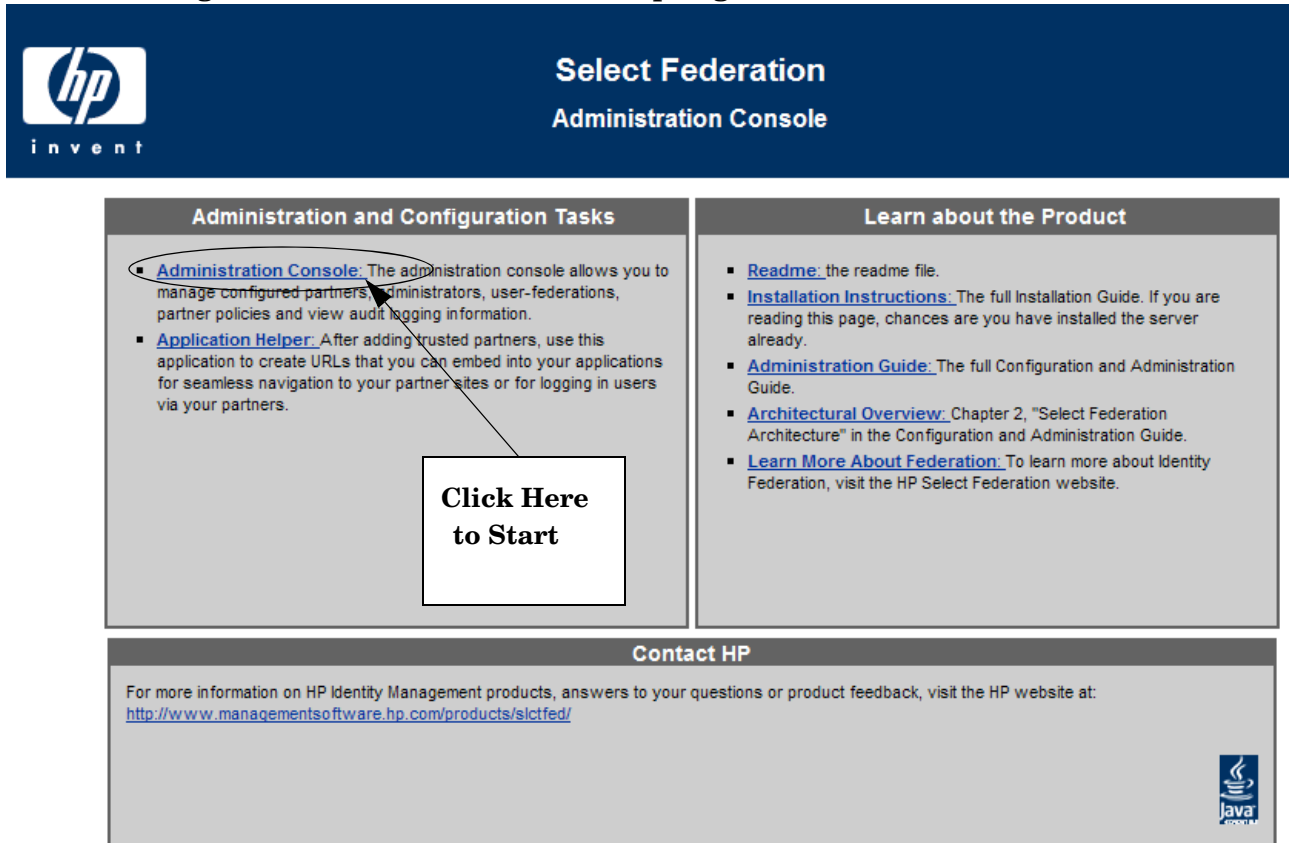
Click on **Administration Console** to open the Administration Console login page.

Figure 4   Select Federation Administration Console Login Page
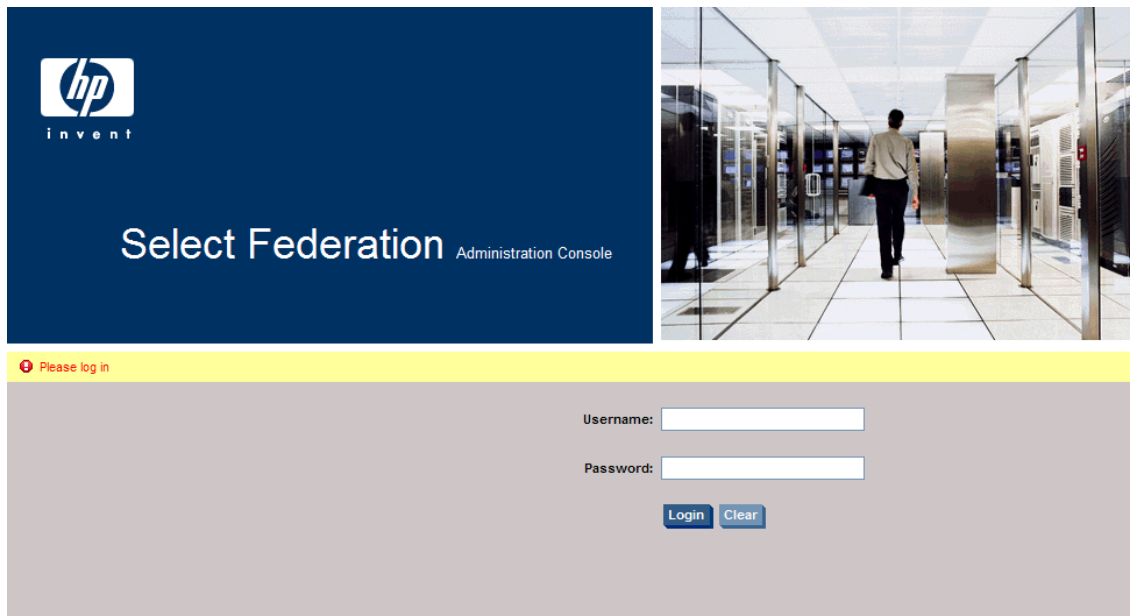
If Select Federation is running in Standalone mode (Select Federation is not integrated with Select Access), the default Admin account is "admin" and the default password is "tgadmin".

Change the default password immediately after installing Select Federation.

➤ If Select Federation is running in Select Access-Integrated mode to protect the Select Federation installation, then Select Access prompts for credentials, and the Select Federation login page is not shown.

Configuring JDBC Data Sources

Overview

JDBC Data Sources allow an Application Server to have better control of connections to databases, and allow for advanced features such as connection pooling and distributed transactions. Select Federation can directly use the JDBC drivers or use JDBC data sources. When using the built-in application server, data sources are enabled by default, but when using one of the other supported application servers, data sources need to be turned on explicitly by going through certain configuration steps.

Advantages of Using Data Sources

Connection pooling offered by data sources can improve Select Federation performance and is recommended for production environments. Using data sources also reduces the number of times a database connection is opened and closed, further adding to the efficiency achieved.

Configuring Data Sources

Configuring JDBC data sources involves setting up the data source in the application server's configuration and then configuring Select Federation to use the data source configured in the application server. If you are using the built-in application server in Select Federation, data sources are automatically enabled and used with the database you specify during installation. However, if you are using another application server, you need to first configure that application server to have a data source that Select Federation can use.

Follow the instructions in the following sections to configure your application server to use JDBC Data Sources:

- Verify the JDBC Drivers in the Application Server Class Path
- Configure Data Sources in BEA WebLogic 8.1
- Configure Data Sources in BEA WebLogic 9.1
- Configure Data Sources in IBM WebSphere 6.0.2
- Configure Select Federation to Use the Configured Data Source in the Application Server

Verify the JDBC Drivers in the Application Server Class Path

When you set up your application server for Select Federation, you would have included the JDBC driver for the database you are using in the application server's class path. You do not need to do anything further to use data sources.

Configure Data Sources in BEA WebLogic 8.1

The way that you configure data sources in WebLogic 8.1 depends on the database you are using. Follow the instructions in the following sections based on your database:

- Setting Up the Built-in Derby Database for WebLogic 8.1
- Configuring Data Sources in BEA WebLogic 8.1 for All Databases

Setting Up the Built-in Derby Database for WebLogic 8.1

For the Derby database, you must complete the following steps BEFORE you set up the data source on the Administrative console.

Perform the following steps on the WebLogic Administrative console to set up the built-in Derby database:

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

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

2   Define the `DERBY_HOME` variable **before** you define the class path variable as follows:

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

```
@REM set derby home path
set DERBY_HOME=%DOMAIN_HOME%\database\drivers\derby.jar
```

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

```
# set derby home path
DERBY_HOME=$DOMAIN_HOME/database/drivers/derby.jar
```

3   Add the `derby.jar` path name to the `CLASSPATH` variable in the appropriate file:

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

4   Restart the WebLogic server.

- For Windows:

   stopWebLogic.cmd

   startWebLogic.cmd

- For UNIX:

   ./stopWWebLogic.sh

   ./startWebLogic.sh

Configuring Data Sources in BEA WebLogic 8.1 for All Databases

Perform the following steps on the WebLogic Administrative console to configure data sources for the database you are using:

1   Start the administrative console of the WebLogic domain for Select Federation.

2   Use the left Navigation menu to Navigate to **Services** → **JDBC** → **Connection Pools**.

3   Click on the **Configure a new JDBC Connection Pool** link and add the properties based on the database you are using.

The values depend upon the database you are using.

The database-specific values are:

- Built-in Database / Derby

  Database Type: CloudScape

  Database Driver: Other

- Oracle 10g

  Database Type: Oracle

  Database Driver: Oracle Driver(Thin) Versions 9.0.1,9.0.2,10

- Microsoft SQL Server 2000

  Database Type: MS SQL Server

  Database Driver: BEA's MS SQL Server Driver(Type 4) Versions 7.0, 2000

4 Click **Continue** and add the properties on the next screen based on the database you are using.

The database-specific values are:

- Built-in Database / Derby

  Name: SF JDBC Connection Pool

  Driver Class Name: org.apache.derby.jdbc.EmbeddedDriver

  URL: jdbc:derby:<*database_name*>

  > <*database_name*> is the full path name to the Select Federation database (SFDB). For example: /opt/bea/user_projects/domains/mydomain/database/ SFDB.

  Database UserName: <database username>

  Password: <database password>

  Confirm Password: <database password>

- Oracle 10g

  Name: SF JDBC Connection Pool

  Database Name: <database name>

  Host Name: <database server name>

  Port: <database port number>

  Database UserName: <database username>

  Password: <database password>

  Confirm Password: <database password>

- Microsoft SQL Server 2000

  Name: SF JDBC Connection Pool

  Database Name: <database name>

  Host Name: <db server name>

  Port: <db port number>

  Database UserName: <db username>

Password: `<db password>`

Confirm Password: `<db password>`

5 Click **Continue** and click on **Create and Deploy.**

6 Navigate to **Services** → **JDBC** → **DataSources** using the left Navigation menu.

7 Click on the **Configure a new JDBC Datasource** link and enter the following properties:

```
Name: SF DataSource

JNDI Name: jdbc/SFDataSource
```

8 For **Pool Name**, select **JDBC Connection Pool** from the drop-down list that was created in the above step. Leave the default values for the other fields and click **Continue**.

9 Select your server instance and click on the **Create** button.

Configure Data Sources in BEA WebLogic 9.1

The way that you configure data sources in WebLogic 9.1 depends on the database you are using. Follow the instructions in the following sections based on your database:

• Setting Up the Built-In Derby Database for WebLogic 9.1

• Configuring Data Sources in BEA WebLogic 9.1 for All Databases

Setting Up the Built-In Derby Database for WebLogic 9.1

For the Derby database, you must complete the following steps BEFORE you set up the data source on the Administrative console.

Perform the following steps on the WebLogic Administrative console to set up the built-in Derby database:

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

• On Windows: `$DOMAIN_HOME\bin\startWebLogic.cmd`

• On UNIX: `$DOMAIN_HOME/bin/startWebLogic.sh`

2 Define the `DERBY_HOME` variable **before** you define the class path variable as follows:

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

```
@REM set derby home path
set DERBY_HOME=%DOMAIN_HOME%\database\drivers\derby.jar
```

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

```
# set derby home path
DERBY_HOME=$DOMAIN_HOME/database/drivers/derby.jar
```

3 Add the `derby.jar` path name to the `CLASSPATH` variable in the appropriate file:

• On Windows: `$DOMAIN_HOME\bin\startWebLogic.cmd`

• On UNIX: `$DOMAIN_HOME/bin/startWebLogic.sh`

4 Restart the WebLogic server.

Perform the following steps on the WebLogic Administrative console to configure data sources for the database you are using:

1 Start the administrative console of the WebLogic domain for Select Federation.

2 Click on the **Lock and Edit** button in the top-left navigation section of the console.

3 Use the left Navigation menu to navigate to **Services** → **JDBC** → **DataSources**.

4 Click on **New** and add the properties based on the database you are using.

   The values depend upon the database you are using.

   The database-specific values are:

   • Built-in Database / Derby

      Name: `SF Derby JDBC Data Source`

      JNDI Name: `jdbc/SFDataSource`

      Database Type: `CloudScape`

      Database Driver: `Other`

   • Oracle 10g

      Name: `SF Oracle JDBC Data Source`

      JNDI Name: `jdbc/SFDataSource`

      Database Type: `Oracle`

      Database Driver: `Oracle Driver(Thin) Versions 9.0.1,9.0.2,10`

   • Microsoft SQL Server 2000

      Name: `SF MSSQL JDBC Data Source`

      JNDI Name: `jdbc/SFDataSource`

      Database Type: `MS SQL Server`

      Database Driver: `BEA's MS SQL Server Driver(Type 4) Versions 7.0, 2000`

5 Click **Next** and keep the default values.

6 Click **Next** and add the properties on the next screen based on the database you are using.

   The database-specific values are:

   • Built-in Database / Derby

      Database Name: `<db_name>` (for example, `SFDB`)

      Host Name: `<db_server_name>` (for example, `localhost`)

      Port: `<port_where_database_is_running>`
      (For embedded Derby this port is the same port where the Select Federation profile WebLogic server is running.)

      Database User Name: `<user_name>` (leave this blank)

      Password: `<password>` (leave this blank)

      Confirm Password: `<password>`

   • Oracle 10g

      Database Name: `<db_name>`

Host Name: ***<db_server_name>***

Port: ***<port_where_database_is_running>***

Database User Name: ***<user_name>***

Password:**<password>**

Confirm Password: **<password>**

- Microsoft SQL Server 2000

    Database Name: ***<db_name>***

    Host Name: ***<db_server_name>***

    Port: ***<port_where_database_is_running>***

    Database User Name: ***<user_name>***

    Password:**<password>**

    Confirm Password: **<password>**

7   Click **Next**.

8   If you are configuring for the built-in Derby database, a screen opens in which you need to add Derby properties. For all other databases, go to the next step.

    Add the following properties for the Built-in Derby database:

    Driver Class Name: **org.apache.derby.jdbc.EmbeddedDriver**

    URL: **jdbc:derby:<db>** For example:
    c:\bea91\user_projects\domains\SF_Derby\database\SFDB

    Leave the default values for the rest of the fields.

9   Make sure you select the server where the Select Federation application is being deployed and click **Finish**.

10 Click on **Activate Changes**.

Configure Data Sources in IBM WebSphere 6.0.2

Instructions for configuring data sources for IBM WebSphere 6.0.2 are specific to the database you are using. Follow the instructions for your database below.

Built-in Derby Database

1   Start the Administrative Console for WebSphere.

2   Navigate to **Resources** → **JDBC providers** in the left Navigation menu.

3   Select the **Server** radio button and the application server where Select Federation is to be installed. Click the **Apply** button.

4   Click **New** and set the following values on the General Properties screen. Click **Next**.

    Database type: **Derby**

    Provider type: **Derby JDBC Provider**

    Implementation: **Connection Pool data source**

5   Select/Add the following properties on the **JDBC Provider** screen and click **Apply**:

    Name: **SF Derby JDBC Provider**

Desc: `Derby embedded non-XA JDBC Provider (default value)`

Path: `${WAS_INSTALL_ROOT}/derby/lib/derby.jar (default value)`

Implementation class name:
`org.apache.derby.jdbc.EmbeddedConnectionPoolDataSource (default value)`

6   Click on **Data Sources** in the **Additional Properties** section on the right-side of the screen.

7   Click **NEW** on the Data Sources screen and enter the following values:

Name: `Derby DataSource for SF`

JNDI Name: `jdbc/SFDataSource`

8   Uncheck the checkbox **Use this Data Source in container managed persistence (CMP)**.

9   Select **Select a data store helper class,** then select **Derby Data Store Helper.**

10   Enter the following for the Database Name:

Database Name: `<directory path>/SFDB (example /export/home/was6/ profiles/AppSrv01/database/SFDB)`

11   Click **Apply**.

12   Click the **Save** link in the messages box at the top of the page.

13   Click the **Save** button on the next screen to save the configuration information.

Oracle 10g Database

Setting up data sources in IBM WebSphere requires the following steps. Some of these are specific to the database you are using, as described below.

1   Start the administrative console for WAS.

2   Navigate to **Environment** → **WebSphere Variables** in the left navigation menu to define a WAS environment variable required for the data source configuration.

3   Select the **Server** radio button and the application server where Select Federation is to be installed. Click the **Apply** button.

4   Enter the following values on the screen and click the **Save** button.

Name: `ORACLE_JDBC_DRIVER_PATH`

value: `${WAS_INSTALL_ROOT}/lib`

Description: `Oracle driver path`

5   Navigate to **Security** → **Global Security** in the left navigation menu.

6   Expand **JAAS configuration** on the right-hand side menu and click on the **J2EE Connector Architecture (J2C) authentication data entries** link.

7   Click on **New** and add the following properties.:

Alias: `Oracle SF DataSource`

User ID: `<Oracle username>`

Password: `<Oracle Password>`

Description: `Oracle SF alias`

8   Navigate to **Resources** → **JDBC providers** in the left Navigation menu.

9   Select the **Server** radio button and the application server where Select Federation is to be installed. Click the **Apply** button.

10   Click **NEW** and set the following values on the General Properties screen:

```
database type: Oracle

provider type: Oracle JDBC Provider

Implementation: Connection Pool data source
```

Click **Next**.

11   Select/Add the following properties on the JDBC Provider screen and click the **Apply** button:

Name: `Oracle JDBC Provider`

Desc: `Oracle JDBC Driver`

Path: `<keep the default value>`

Implementation class name: `<keep the default value>`

12   Click on **Data Sources** in the **Additional Properties** section on the right-side of the screen.

13   Click **NEW** on the Data Sources screen and enter the following values:

Name: `Oracle JDBC Driver DataSource`

JNDI Name: `jdbc/SFDataSource`

Keep the default value for the checkbox **Use this Data Source in container managed persistence (CMP)**

14   Select the radio button **Data store helper classes provided by WebSphere Application Server**.

15   Select **Oracle 10g Datastore Helper** and click the **Apply** button.

16   Select **<node>/Oracle SF DataSource** in the **Component Managed Authentication Alias** drop down list.

17   Enter the database URL in the following format in the URL field:

`jdbc:oracle:thin:@<server>:<port number>:<SID>`

18   Click the **Save** link in the messages box at the top of the page.

19   Click the **Save** button on the next screen to save the configuration information.

Microsoft SQL Server 2000 Database

1   Start the administrative console for WAS.

2   Navigate to **Security → Global Security** using the left Navigation menu.

3   Expand **JAAS configuration** on the right-hand side menu and click on the **J2EE Connector Architecture (J2C) authentication data entries** link.

4   Click on **New** and add the following properties.

Alias: `MS SQL SF DataSource`

User ID: `<MS SQL username>`

Password: `<MS SQL password>`

Description: `MS SQL SF alias`

5   Navigate to **Resources → JDBC providers** in the left Navigation menu.

6   Select the **Server** radio button and the application server where Select Federation is to be installed. Click the **Apply** button.

7   Click **New** and set the following values on the **General Properties** screen, then click **Next**.

> **database type**: `Sql Server`
>
> **provider type**: `WebSphere embedded ConnectJDBC Driver for MS SQL server`
>
> **Implementation**: `Connection Pool data source`

8   Select/Add the following properties on the **JDBC Provider** screen and click the **Apply** button:

> **Name**: `MS SQL JDBC Provider`
>
> **Desc**: `MS SQL JDBC Driver`
>
> **Path**: `<keep the default value>`
>
> **Implementation class name**: `<keep the default value>`

9   Click on **Data Sources** in the **Additional Properties** section on the right-side of the screen.

10   Click **NEW** on the Data Sources screen and enter the following values:

> **Name**: `MS SQL JDBC Driver DataSource`
>
> **JNDI Name**: `jdbc/SFDataSource`

11   Keep the default value for the check box **Use this Data Source in container managed persistence (CMP)**.

12   Select **Data store helper classes provided by WebSphere Application Server**.

13   Select **WebSphere branded Connect JDBC data store Helper** and click **Apply**.

14   Select **<node>/MS SQL SF DataSource** in the **Component Managed Authentication Alias** drop-down list and enter the following values:

> **Database name**: `<name of your database> (by default SFDB)`
>
> **Server name**: `<database server name>`
>
> **Port number**: `<database listener port number> (by default 1433)`

15   Click **Save** in the messages box at the top of the page.

16   Click **Save** on the next screen to save the configuration information.

Configure Select Federation to Use the Configured Data Source in the Application Server

Once you have configured the data source in the application server, you need to modify all the Select Federation configuration files to refer to the data source that you just configured. Following are the configuration files, which are located in `<SF_Install_Directory>\conf\`:

```
tfsconfig.properties
idpapiconfig.properties
spapiconfig.properties.
```

For WebSphere and WebLogic, add the following line in the three configuration files:

> **`jdbcDataSource=jdbc/SFDataSource`**

For the built-in application server, add the following line in the three configuration files:

> **`jdbcDataSource=java:comp/env/jdbc/SFDataSource`**

In all three configuration files, comment out the lines starting with:

- `jdbcDriver`
- `jdbcAddr`
- `jdbcUser`
- `jdbcPassword`

Be sure that the `jdbcProvider` property in the configuration files has the correct entries when using the Oracle database as follows:

- For WebSphere 6.0.x, the entry should be:

  `jdbcProvider=com.trustgenix.tfs.JDBCProvider_Oracle_WebsphereDS`

- For the built-in application server, the entry should be:

  `jdbcProvider=com.trustgenix.tfs.JDBCProvider_Oracle_TomcatDS`

6 Integrating HP OpenView Products with Select Federation

This chapter describes integrating the following HP OpenView products with Select Federation:

- Integrating Select Access with Select Federation
- Integrating Select Audit with Select Federation Manually

Integrating Select Access with Select Federation

Select Federation can be deployed standalone, where Select Access is not needed for authentication purposes. However, you may use Select Access by following the instructions below.

It is important to configure and set appropriate protection for the Select Federation resources in the Select Access Policy Builder. Integrating Select Access with Select Federation primarily centers around five Select Access configuration tasks:

- **Configuring the Enforcer**: Since Select Federation uses the generic enforcer, it needs to be configured. The default name of the enforcer configuration file used by Select Federation is `enforcer_servlet.xml`. Refer to the chapter titled "Configuring the Enforcer Plugins" in the *HP OpenView Select Access Installation Guide* for instructions on configuring a Generic Enforcer.

▶ While configuring the generic enforcer, only specify the name of the directory where you want the enforcer configuration file to be stored. This is typically the `bin` directory under the Select Access installation directory.

▶ You must restart the application to initialize the Enforcer.

- **Federated authentication:** To enable users of your Trusted Partners' sites to seamlessly login to your site, you need to create a special Authentication Server based on a type that is built into Select Access. This Authentication Server Type is called "Trusted Server".

- **Logout rule:** To enable users to perform global logouts in a federated environment, a special logout rule needs to be created in Select Access.

- **Register SF resources**: Once you have created the authentication server and the logout rule, you can apply them to certain resources within Select Federation to enable operational integration between the two products and to protect the Select Federation administration console.

- **Access policies:** Select Federation assets need to be protected with the appropriate combination of access policies that authorize identity entitlements accordingly.
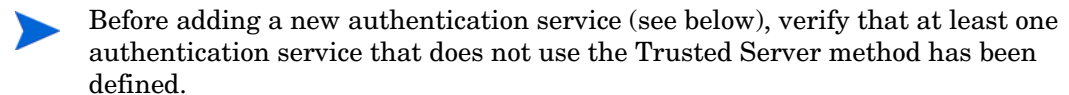
The following section documents how to configure this authentication service. If you already have configured a Trusted Server authentication service, no additional integration steps are required.

Configuring the Federation Authentication Server

To configure the federation authentication server, perform the following steps:

1 Start the Select Access Policy Builder.

2 Click **Tools → Authentication Servers**.

   The Authentication Services dialog appears.

   > Before adding a new authentication service (see below), verify that at least one authentication service that does not use the Trusted Server method has been defined.

3 Click **Add**.

   The Authentication Servers dialog appears.

4 Click **Trusted Server** and name the server "`federation`".

5 Click **OK**.

   The New Integrated Windows Service/Trusted Server Authentication Server dialog appears.

6 Click **Browse** and select the location in the directory where the federated users will be created.

7 Click **OK** on the dialogs to return to the Policy Builder.

Creating a Logout Rule

To create a logout rule, perform the following steps:

1 Start the Select Access Policy Builder

2 Click **Tools → Rule Builder**.

   The Rule Builder window appears.

3 Click **File → New Rule**.

4 Choose the **Policy** and enter a name for this rule, for example, "Logout".

5 Click the **Logout** terminal point icon and drag it below the starting node of the rule.

6 Save the rule.

Adding Select Federation Resources to the Policy Matrix

To add Select Federation Resources to the policy matrix, perform the following steps:

1 Create a new service on the Resources Tree in the Select Access Policy Builder.

2 Name the service appropriately for your deployment, such as. "Select Federation."

This service will host the application server upon which Select Federation has been deployed.

➤ For details on how to create a new service, see the "Building Your Identities and Resources Tree" chapter of the *HP OpenView Select Access Policy Builder User's Guide*.

3 Create Select Federation resources in Select Access by importing the resource list provided for this purpose.

The resource list is automatically saved to /conf/sf_URLs.txt.

The sf-URLs.txt file allows you to quickly import the Select Federation resources in the **Policy Builder**, and thereby avoid having to add these resources manually.

➤ For details on how to create a new resource, see Chapter 4 of the *HP OpenView Select Access Policy Builder User's Guide*.

When you are finished you will have created entries that look like the following figure.
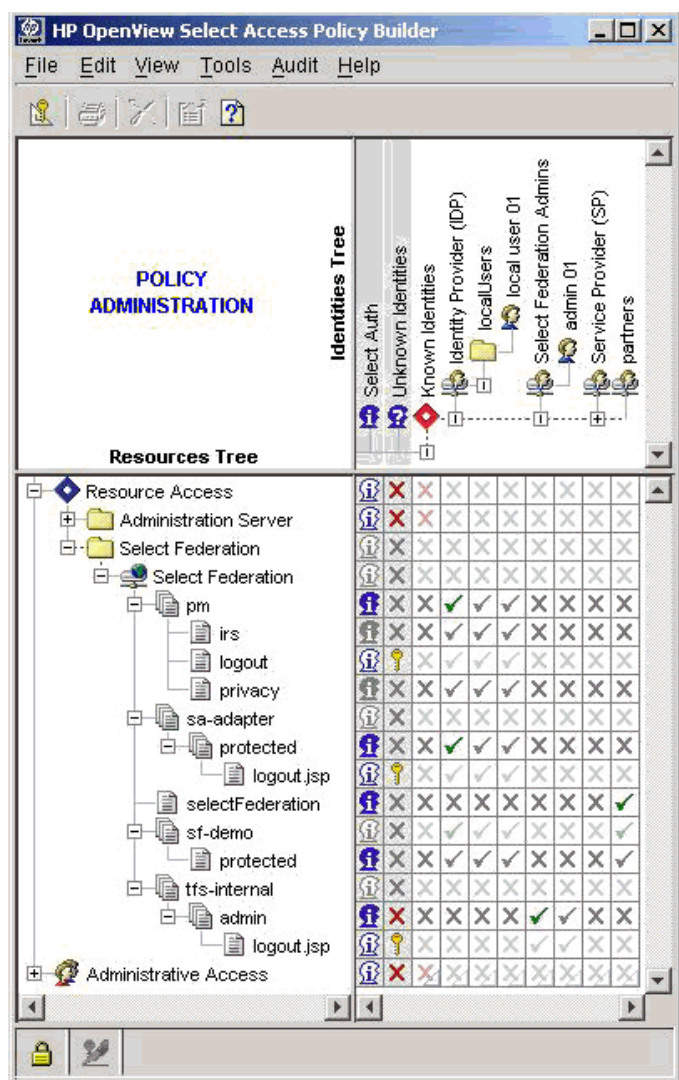
Authorizing Entitlements with Access Policies

Configure each resource as follows:

pm

1   Right-click the cell where the **Select Auth** column and the newly-created `pm` resource intersect.

2   From the popup menu click, **Enable Select Auth**. The **Select Auth Properties** dialog appears.

3   Click **Add** to configure the authentication service that will be needed to authenticate identities that request access to this resource. HP recommends that you only use both the **password** and **federation** authentication servers in this instance.

4   Right-click the cells where your federation-capable users and the newly-created `pm` resource intersect. In this example, you are enabling users in the IDP folder.

5   From the popup menu, click **Allow Access**.

6   Right-click the column where federation capable users and `irs` resource intersect and select **Allow Access**.

7   Right-click the column where federation capable users and `privacy` resource intersect and select **Allow Access**.

8   For the resource `logout`, **Disable Select Auth**

9   Right-click the cell where the **Unknown Identities** column and the newly-created `logout` resource intersect.

10 From the popup menu click, **Conditional Access**. The **Conditional Rule Selection** dialog appears.

11 Click the **Logout** rule you created earlier in this integration process.

sa-adapter

1   Right-click the cell where the Select Auth column and the newly-created `protected` resource under `sa-adapter` intersect.

2   From the popup menu click, **Enable Select Auth**. The **Select Auth Properties** dialog appears.

3   In the **Select Auth Properties** dialog, click **Add** to configure the authentication servers that will be needed to authenticate identities that request access to this resource. HP recommends that you use the following servers:

   • The **federation** authentication server you created. This allows Select Access's Policy Validator to create the cookie required to allow identities to access this resource.

   • At least one more authentication server, such as password, certificate, SecurID, Radius. This is to enable local login for outbound users.

4   Right-click the cells where your federation-capable users and the newly-created `protected` resource under `sa-adapter` intersect. In this example, you are enabling users in the IDP folder.

5   From the popup menu, click **Allow Access**.

6   Right-click the cell where the Select Auth column and the newly-created `logout.jsp` resource under `sa-adapter/protected` intersect.

7   From the popup menu click, **Disable Select Auth**.

8   Right-click the cell where the **Unknown Identities** column and the newly-created `logout.jsp` resource intersect.

9   From the popup menu click, **Conditional Access**. The **Conditional Rule Selection** dialog appears.

10   Click the **Logout** rule you created earlier in this integration process.

selectFederation

1   Right-click the cell where the **Select Auth** column and the newly-created `selectFederation` resource intersect.

2   From the popup menu click, **Enable Select Auth**. The **Select Auth Properties** dialog appears.

3   In the **Select Auth Properties** dialog, click **Add** to configure the authentication server that will be needed to authenticate identities that request access to this resource.

> ➤ HP recommends that you only use the federation authentication server created earlier in this instance.

4   Right-click the cells where your visiting users and the newly-created `selectFederation` resource intersect. In this example, accounts for visiting users authenticated by other authorities are created in the folder "partners".

5   From the popup menu, click **Allow Access**.

sf-demo

1   Right-click the cell where the **Select Auth** column and the newly-created `sf-demo/protected` resource intersect.

2   From the popup menu click, **Enable Select Auth**. The **Select Auth Properties** dialog appears.

3   Click **Add** to configure the authentication service that will be needed to authenticate identities that request access to this resource.

> ➤ HP recommends that you only use both the **password** and **federation** authentication servers in this instance.

4   Right-click the cells where your federation-capable users and the newly-created `sf-demo` resource intersect. In this example, you are enabling users in the IDP folder.

5   From the popup menu, click **Allow Access**.

6   Right-click the cells where your visiting users and the `sf-demo` resource intersect. In this example, accounts for visiting users authenticated by other authorities are created in the folder "partners".

7   From the popup menu, click **Allow Access**.

tfs-internal

1   Right-click the cell where the **Select Auth** column and the newly-created admin resource under `tfs-internal` intersect.

2   From the popup menu click, **Enable Select Auth**. The **Select Auth Properties** dialog appears.

3   Click **Add** to configure the authentication service that will be used to authenticate **Select Federation** administrators. (You could use password, certificate, SecurID, Radius, and so on.)

4   Right-click the cell where the **Known Users** column and the newly-created admin resource under `tfs-internal` intersect.

5   From the popup menu, click **Deny Access**.

6   Right-click all cells for users who are administrators and the newly-created admin resource intersect.

7   From the popup menu, click **Allow Access**. This restricts access to those identities that require administrative access to Select Federation.

> ▶ Alternatively, you can create a group for all identities with Select Federation administration entitlements. That way you only need to assign one cell an allow policy. For details on how to create groups, see Chapter 4 of the *HP OpenView Select Access Policy Builder User's Guide*.

8   Right-click the cell where the **Select Auth** column and the newly-created `logout.jsp` resource under `tfs-internal/admin` intersect.

9   From the popup menu click, **Disable Select Auth**. Right-click the cell where the **Unknown Users** column and the newly-created `logout.jsp` resource under `tfs-internal/admin` intersect.

10 From the popup menu click, **Conditional Access**. The **Conditional Rule Selection** dialog appears.

11 Click the **Logout** rule you created earlier in this integration process.

Integrating Select Audit with Select Federation Manually

This section explains how to integrate HP OpenView Select Audit with Select Federation manually. Follow the instructions in this section only if you did not choose to integrate with Select Audit during the installation process (see step 10 in Installation Procedure on page 21). If you chose to integrate with Select Audit during installation, then Select Audit has been configured and you can skip this section.

When integrated with Select Audit, Select Federation sends operational and administrative log events to Select Audit. These log events do not include the diagnostic log entries that are added to the web application server's log files.

To enable Select Audit integration, modify the `tfsconfig.properties` file as follows:

• To write system audit logs to Select Audit, uncomment the following line and make sure that the `conf` directory has a file "`selectaudit.properties`" with correct settings for the port and so on. (For more information, see the *HP OpenView Select Audit Installation Guide*):

    auditDataProvider=com.trustgenix.hpsf.selectaudit.AuditDataProvider_Selec
    tAudit

• Uncommenting the following line ensures concurrent logging to the default AuditDataProvider:

    AuditDataProvider_SelectAudit.auditToHPSF=1

• Set the following configuration parameters in the `tfsconfig.properties` file to enable audit logging:

```
# Other Audit Configuration parameters
#AuditDataProvider_SelectAudit.clientId=$providerid
#AuditDataProvider_SelectAudit.host=localhost
#AuditDataProvider_SelectAudit.port=9979
```

In the above description the `providerid` should be the provider ID of the installed Select Federation software.

7 Upgrading From Select Federation Version 6.5

This chapter describes how to upgrade from Select Federation Version 6.5 to Version 6.60 in the following topics:

- Upgrade Procedure
- Finishing the Upgrade Process

▶ If you are upgrading from a version that is older than 6.5, contact HP Support. See Support on page 4 for contact information.

Upgrade Procedure

When you upgrade, you begin with some pre-install steps that need to be performed depending on the application server that Select Federation 6.5 was deployed on. The installation process is similar to starting a new product installation, as described in Installation Procedure on page 21. After the install wizard finishes, complete the upgrade process by performing some application server specific tasks.

▶ Be sure to back up your Select Federation 6.5 files before you upgrade.

Preparing to Upgrade

BEA WebLogic

1   Stop and uninstall the Select Federation server by doing the following:

   a   Navigate to the BEA WebLogic Console for the domain on which Select Federation is deployed.

   b   Login to the console.

   c   In the Navigation frame, click **Deployments** → **Applications**.

   d   Click the particular EAR entry corresponding to Select Federation; the EAR will typically be called tfs.ear.

   e   Select the **Deploy** tab. You will see a list of modules for this application in a table. Click **Stop Application**.

   f   In the table of modules, check that all modules states change to "Inactive" in the Module Status column and "Success" in the Status of Last Action column.

   g   Click **Applications** again; in the table that appears, click the Delete icon in adjacent to the Select Federation EAR entry.

2   Shutdown the server instance:

    a   In the Navigation frame, click Servers.

    b   Click on the Select Federation server instance.

    c   Now select the Start/Stop tab, and click on "Graceful shutdown of this server…"

IBM WebSphere

Stop the server instance that Select Federation is running on by doing the following:

1   Navigate to the IBM WebSphere Console for the domain on which Select Federation is deployed.

2   Login to the console.

3   In the Navigation frame, click Enterprise applications.

4   Check the Select Federation server box and click Stop.

Built-In Application Server

On Windows, the Select Federation service is stopped automatically by the upgrade installer. If the Built-In Application Server is running either on Linux, HP-UX or Solaris, the server will have to be stopped manually using the following commands:

```
cd $SF_HOME/
./bin/shutdown.sh
```

➤ You must run the shutdown and startup commands from the Select Federation installation directory. Otherwise, the server may not start/stop correctly.

Running the Upgrade Wizard

To run the Upgrade Wizard, perform the following steps:

1   Start the installation by running the Select Federation install executable located on the CD.

A Welcome message page opens, followed by an Upgrade notification dialog.

2   Click **Next** to continue.

The software license agreement page open.

3   Accept the License agreement.

Read the license agreement and accept or reject it by clicking the appropriate radio
button. You must accept the license agreement to continue the installation procedure.

4   Click **Next** to continue.

5   The 6.60 installer will now prompt you to enter the location where Select Federation 6.5
was installed. This location will vary depending on the application server that Select
Federation was deployed on.
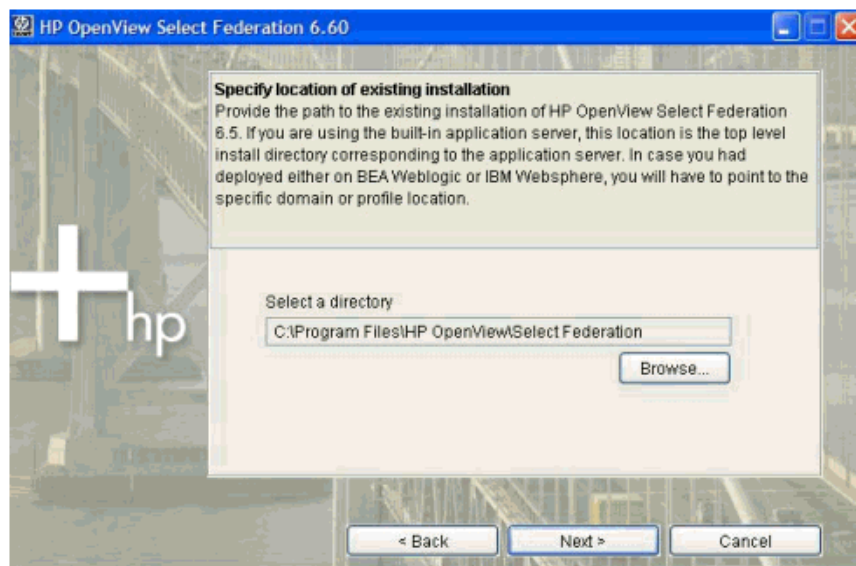
6   Click **Next** to continue.

After you specify the path, the installer performs a check on the application server type. If the specified location is incorrect, you are prompted to change the path. Once the application server is verified, you are shown an upgrade prompt as shown in the following figure.
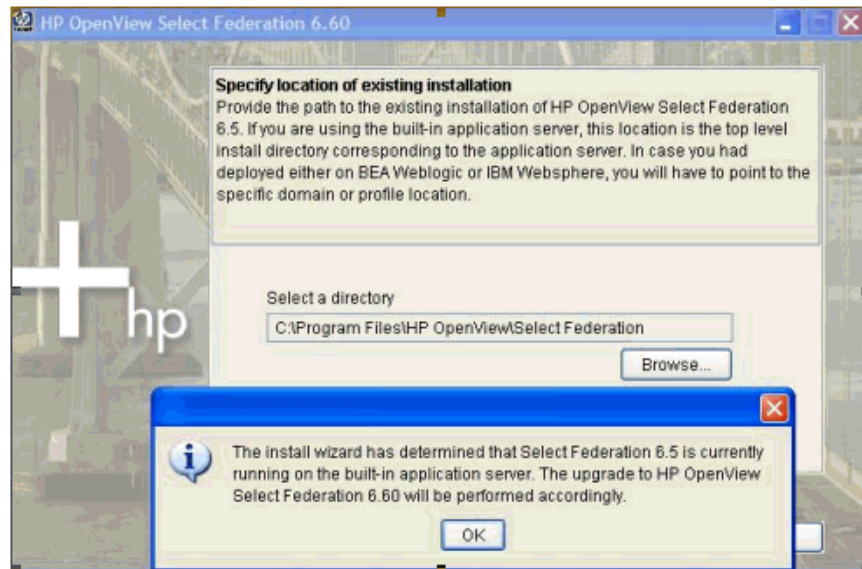
7   Click **OK** to continue.

A summary dialog opens.
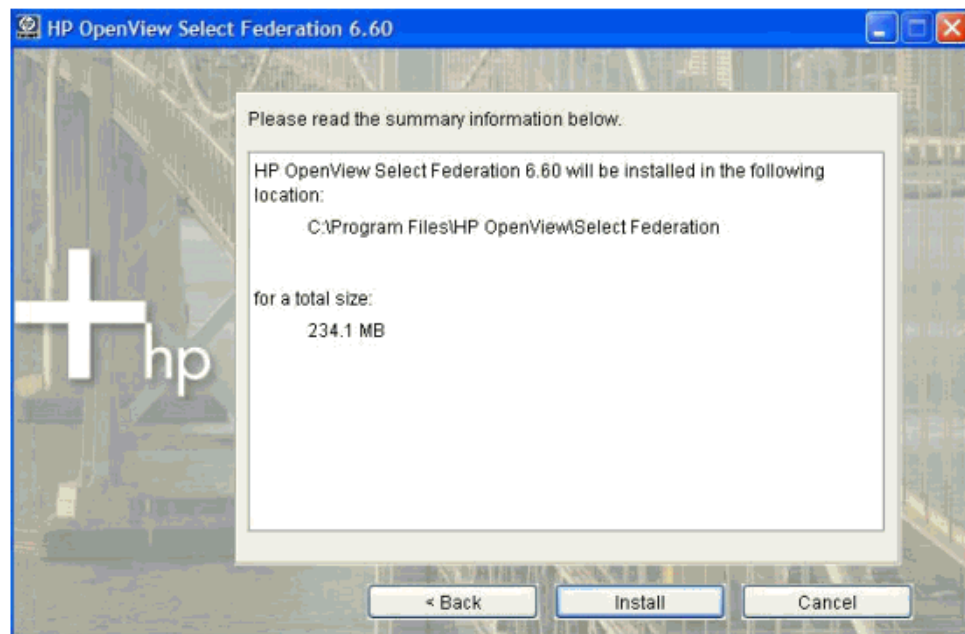
8   Click **Install** to start the upgrade.

A final summary page opens.
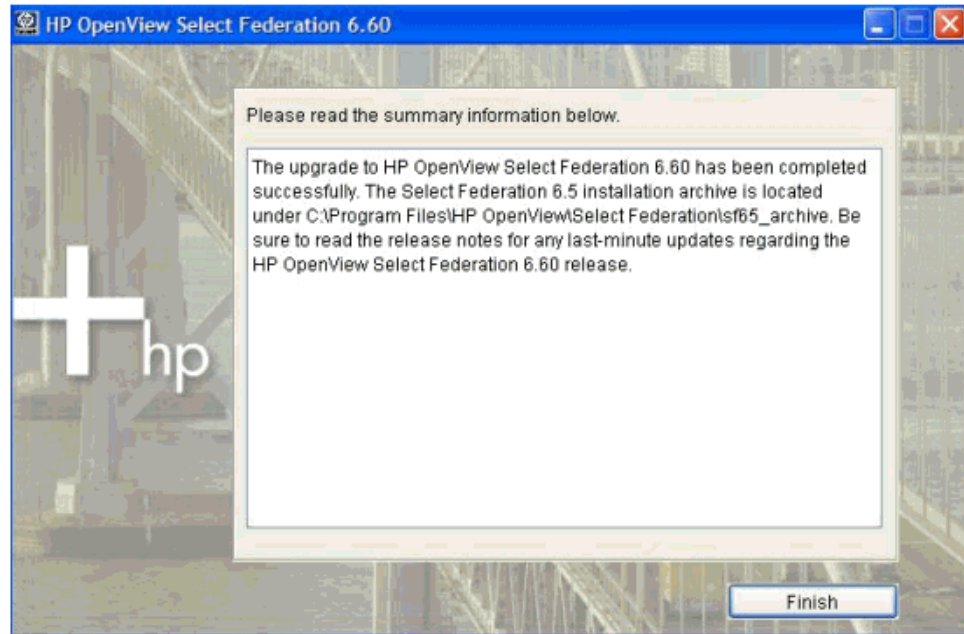
9   Click **Finish** to complete the upgrade installation and exit the Upgrade Wizard.

Finishing the Upgrade Process

Depending on the application server that Select Federation is running on, there are a few steps required to complete the upgrade process.

BEA WebLogic

Install the new Select Federation 6.60 EAR by doing the following:

1   In the Navigation frame, click **Deployments** --> **Applications**.

2   Click on **Deploy a new Application**.

3   Browse to the `sf_ear` subdirectory of the installation.

    The install wizard copied the Select Federation 6.60 EAR at this location.

4   Click on **upload**.

5   Once uploaded, select the tfs.ear file in the list of modules. Give an appropriate name for this application.

6   In the Configure Application or Component screen, select the WebLogic Server instance on which you wish to deploy the new EAR, then click Configure and Deploy.

7   Status messages appear indicating the progress of your new deployment. Eventually, the status of the application should read Completed.

IBM WebSphere

1   Stop and uninstall the Select Federation server by doing the following:

a   Navigate to the IBM WebSphere Console for the domain on which Select Federation is deployed.

b   Login to the console.

c   In the Navigation frame, click Enterprise applications. Check the Select Federation server box and click Stop.

d   Click Uninstall. WebSphere will begin uninstalling Select Federation.

e   Once you see a message such as `Select Federation was uninstalled successfully`, click **Save to Master Configuration** in the resulting screen.

f   Click **Save** in the next screen.

2   Install the new Select Federation 6.60 EAR by doing the following:

a   In the same IBM WebSphere Console Navigation frame, click Install New Application.

b   Browse to the sf_ear sub-directory of the profile that is being used for Select Federation.

c   Accept all IBM WebSphere defaults on all subsequent panes by clicking **Next**.

d   Click **Finish** to begin the installation.

e   Upon completion, click **Save to Master Configuration** in the resulting screen.

f   Click **Save** in the next screen.

3   Restart your updated Select Federation server by doing the following:

a   In the same IBM WebSphere Console Navigation frame, click Enterprise Applications.

b   Check the Select Federation server box and click Start. If the update was successful, you will see a green arrow in the right pane.

Built-In Application Server

If Select Federation is running on the Built-in Application Server on Windows, you do not need to do anything more. The windows service corresponding to Select Federation is automatically started after finishing the upgrade install wizard.

If, however, the Built-in Application Server is running on Linux, HP-UX or Solaris, you will have to manually start the Select Federation server.

To restart the server enter the following commands:

```
cd $SF_HOME/
./bin/startup.sh
```

Verifying the Upgrade

Verify your updated deployment by doing the following:

1   Navigate to the Select Federation Administration Console home page.

2   Login to the console.

3   Verify that you see Select Federation 6.60 at the bottom of this page. You will also notice that the administration console has a new look and feel.

Additional Information on the Upgrade

The installer performs the following steps during the upgrade:

1 Archives the existing contents into a directory called sf65_archive. This directory is located one level above the Select Federation installation directory.

2 Updates the product documentation, EAR file, stylesheets

3 Several new tools are installed under a sub-directory called tools. More information regarding these tools can be found in the Configuration guide.

Rolling Back the Upgrade

This section provides instructions on how to roll back your upgrade to Select Federation 6.5. During the upgrade to Select Federation 6.60, the installer archives your 6.5 installation in a directory called `sf65_archive` one level above the installation directory.

Built-in Application Server

Complete the following tasks to roll back Select Federation on the built-in application server:

Task 1: Stop the server

On Windows, stop the built-in server by performing the following steps:

1 Go to the service panel.

2 Stop the service called **HP OpenView Select Federation**.

On Linux, HP-UX or Solaris, stop the built-in server manually using the following commands:

```
cd $SF_HOME/
./bin/shutdown.sh
```

▶ You must run the shutdown and startup commands from the Select Federation installation directory. Otherwise, the server may not start/stop correctly.

Task 2: Remove the Select Federation Service

On Windows, remove the Select Federation service by performing the following steps:

1 Open a command prompt shell and go to the Select Federation install directory.

2 Remove the Select Federation windows service as shown in the example below:

```
cd C:\Program Files\HP OpenView\Select Federation
bin\service.bat remove SelectFederation
The service 'SelectFederation' has been removed…
```

On HPUX, Linux, or Solaris, remove the Select Federation auto-start services by performing the following steps:

1 Open a shell and go to the Select Federation install directory.

2 Remove the services as shown in the example below:

```
./bin/remove-sfservice.sh
```

Task 3: Restore Select Federation 6.5 contents from the archive

1   Delete all the Select Federation 6.60 contents under the install directory.

2   Go up one directory above the install location.

    You will see a directory called `sf65_archive`.

3   Copy the contents of the `sf65_archive` directory and place them in your install directory.

Task 4: (Windows only) Install the Select Federation 6.5 service

1   Open a command prompt shell and go to the Select Federation install directory.

2   Install the Select Federation 6.5 windows service as shown in the example below:

```
C:\Program Files\HP OpenView\Select Federation>bin\service.bat install

Installing the service 'SelectFederation' ...

Using CATALINA_HOME:    C:\PROGRA~1\HPOPEN~1\SELECT~1

Using JAVA_HOME:        C:\PROGRA~1\HPOPEN~1\SELECT~1\_jvm

Using JVM:
C:\PROGRA~1\HPOPEN~1\SELECT~1\_jvm\bin\client\jvm.dll

The service 'SelectFederation' has been installed.
```

Task 5: Start the built-in server

On Windows, start the built-in server by performing the following steps:

1   Go to the service panel.

2   Start the service called **HP OpenView Select Federation 6.5 Enterprise/Premium edition**.

On Linux, HP-UX or Solaris, start the built-in server manually using the following commands:

```
cd $SF_HOME/

./bin/startup.sh
```

▶ You must run the shutdown and startup commands from the Select Federation installation directory. Otherwise, the server may not start/stop correctly.

Task 6: Verify the roll back to Select Federation 6.5

1   Navigate to the Select Federation Administration Console home page.

2   Log in to the console.

    You should see the 6.5 landing page.

BEA WebLogic

Complete the following tasks to roll back Select Federation on the BEA WebLogic application server:

Task 1: Uninstall Select Federation 6.60

1 Stop and uninstall the Select Federation 6.60 server by doing the following:

   a Navigate to the BEA WebLogic Console for the domain on which Select Federation is deployed.

   b Login to the console.

   c In the Navigation frame, click **Deployments** → **Applications**.

   d Click the particular EAR entry corresponding to Select Federation; the EAR will typically be called tfs.ear.

   e Select the **Deploy** tab. You will see a list of modules for this application in a table. Click **Stop Application**.

   f In the table of modules, check that all modules states change to "Inactive" in the Module Status column and "Success" in the Status of Last Action column.

   g Click **Applications** again; in the table that appears, click the Delete icon in adjacent to the Select Federation EAR entry.

2 Shutdown the server instance:

   a In the Navigation frame, click Servers.

   b Click on the Select Federation server instance.

   c Now select the Start/Stop tab, and click on "Graceful shutdown of this server…"

Task 2: Restore Select Federation 6.5 contents from the archive

1 Delete all the Select Federation 6.60 contents under the install directory.

2 Go up one directory above the install location.

   You will see a directory called sf65_archive.

3 Copy the contents of the sf65_archive directory and place them in your install directory.

Task 3: Install the Select Federation 6.5 EAR

1 In the Navigation frame, click **Deployments** --> **Applications**.

2 Click on **Deploy a new Application**.

3 Browse to the sf_ear subdirectory of the installation.

   You will find the Select Federation 6.5 EAR at this location.

4 Click on **upload**.

5 Once uploaded, select the tfs.ear file in the list of modules. Give an appropriate name for this application.

6 In the Configure Application or Component screen, select the WebLogic Server instance on which you wish to deploy the new EAR, then click Configure and Deploy.

7   Status messages appear indicating the progress of your new deployment. Eventually, the
    status of the application should read Completed.

1   Navigate to the Select Federation Administration Console home page.

2   Log in to the console.

    You should see the 6.5 (build 127) landing page.

IBM WebSphere

Complete the following tasks to roll back Select Federation on the IBM WebSphere
application server:

1   Navigate to the IBM WebSphere Console for the domain on which Select Federation is
    deployed.

2   Log in to the console.

3   Click **Enterprise applications** in the Navigation frame. Check the **Select Federation server**
    box and click **Stop**.

4   Click **Uninstall**.

    WebSphere begins uninstalling Select Federation 6.60.

5   Once you see a message such as `Select Federation was uninstalled successfully`,
    click **Save to Master Configuration** in the resulting screen.

6   Click **Save** in the next screen.

1   Delete all the Select Federation 6.60 contents under the install directory.

2   Go up one directory above the install location.

    You will see a directory called `sf65_archive`.

3   Copy the contents of the `sf65_archive` directory and place them in your install
    directory.

1   In the IBM WebSphere Console Navigation frame, click Install New Application.

2   Browse to the `sf_ear` subdirectory of the profile that is being used for Select Federation.

3   Accept all IBM WebSphere defaults on all subsequent panes by clicking **Next**.

4   Click **Finish** to begin the installation.

5   Upon completion, click **Save to Master Configuration** in the resulting screen.

6   Click **Save** in the next screen.

7   Restart your updated Select Federation server by doing the following:

    a   Click **Enterprise Applications** in the same IBM WebSphere Console Navigation frame.

    b   Check the **Select Federation** server box and click **Start**.

If the update was successful, you will see a green arrow in the right pane.

1   Navigate to the Select Federation Administration Console home page.

2   Log in to the console.

You should see the 6.5 landing page.

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.

ADFS (WS-Federation 1.0)

Active Directory Federation Services (ADFS) is a feature of Microsoft Windows 2003 Server R2. ADFS allows a federation with Active Directory-based users, by using the WS-Federation 1.0 protocol.

Administrator

An identity with full permission to manage Select Federation.

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 Site Role

An application site (also called a SAML Consumer or 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.

ASP

Microsoft Active Server Pages log users in by invoking the IDP-FSS over a secure channel.

Attribute

One or more characteristics that are part of an identity profile. Attributes are name/value pairs with a type that is assigned a 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 a SAML Producer or 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. Authentication is a prerequisite for authorization. See Access Control and Authentication.

CA

Certificate Authority

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).

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.

ID-WSF

Liberty Identity Web Services Framework security mechanism.

IDP

An Identity Provider or IDP is an 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.

IDP-FSS

IDP filter-support service, which is 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.

IIS

The Internet Information Server (IIS) is the web server that is bundled with Windows 2003 Server.

Integrated Windows Authentication (IWA)

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.

Keystore

A keystore is 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 (Lightweight Directory Access Protocol)

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.

LECP

Liberty Enabled Client/Proxy Service.

MMC

Microsoft Management Console, used to set up server authentication and to import the `pkcs`/ `pfx` format file into your local store on the IIS machine.

NTLM

NT LAN Manager [web definition: is a challenge/response form of authentication that was the default network authentication protocol in Windows NT 4.0.]

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).

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.

Presence Service

A service that informs the WSC if a user is online, available, and so on.

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. See Delegated Administrator.

SOAP

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

SP

A Service Provider (SP) is an application that allows authenticated access based on an authentication performed by an IDP using a federated identity protocol such as Liberty or SAML.

SSL

Secure Sockets Layer handshake protocol, which supports server and client authentication.

SSO

Single Sign-On session/authentication process that permits a user to enter one set of credentials (name and password) to access multiple applications. A Web SSO is a specialized SSO system for web applications.

SAML

Security Assertion Markup Language protocol.

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.

WSC

A Web Service Consumer (WSC) is 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.

WSP

A Web Service Provider (WSP) is a web service application that services requests it receives based on XML and typically SOAP-based communication.

Index