HP OpenView Select Federation

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

Software Version: 6.5

Configuration and Administration Guide

HP Select Federation 6.5 Enterprise Media: T3983BA

HP Select Federation 6.5 Premium Media: T3984BA

February 2006

Legal Notices

Warranty

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

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

Restricted Rights Legend

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

Hewlett-Packard Company
United States of America

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

Copyright Notices

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

- Software developed by Trustgenix, Inc. Copyright © Trustgenix, Inc. 2002-2005. All rights reserved.
- 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

- Trustgenix, IdentityBridge, and Trustgenix Federation Server are U.S. trademarks of Hewlett Packard Development Company, L.P.
- BEA and WebLogic are registered trademarks of BEA Systems, Inc.
- IBM, Tivoli, WebSphere are trademarks of International Business Machines in the United States, other countries or both.
- Linux is a U.S. registered trademark of Linus Torvalds.
- Microsoft®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.
- Oracle is a registered trademark of Oracle Corporation. Various product and service names referenced herein may be trademarks of Oracle Corporation.
- Sun, Sun Microsystems, Solaris, and Java™ are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.
- All other trademarks, trade names, service marks, and logos referenced herein belong to their respective companies/owners.

Documentation Updates

This manual's title page contains the following identifying information:

- Software Version number, which indicates the software version
- Document release date, which changes each time the document is updated
- Software release date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition, visit the following URL:

http://ovweb.external.hp.com/lpe/doc_serv/

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

Support

You can visit the HP OpenView support web site at:

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

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

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

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

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

To find more information about access levels, go to:

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

To register for an HP Passport ID, go to:

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

Contents

1 Introducing the HP OpenView Select Federation Configuration and Administration Guide

Introduction

This *HP OpenView Select Federation Configuration and Administration Guide* describes how to configure Select Federation, and how to perform basic administration tasks on Select Federation, once it has been installed.

Audience

This guide is intended for:

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

Prerequisites

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

This guide also assumes a working knowledge of:

- Identity Management
- Federated Identity

Chapters Summary

Table 1 provides an overview of this guide's contents.

Table 1 Contents Summary

Chapter	Description
Chapter 1, *Introducing the HP OpenView Select Federation Configuration and Administration Guide*	This chapter provides a brief description of this Configuration and Administration Guide. It is geared to provide users with a quick overview of the information contained herein.

Chapter	Description
Chapter 2, *Getting Started*	This chapter gives a brief overview of HP OpenView Select Federation.
Chapter 3, *Installation*	This chapter describes how to install and deploy HP OpenView Select Federation. This chapter includes directions on how to integrate Select Federation with HP OpenView Select Access.
Chapter 4, *Navigating the HP OpenView Select Federation Administration Console*	This chapter provides an overview of the Select Federation Administration Console.
Chapter 5, *Setting Up Partnerships*	This chapter provides detailed instructions on how to setup partnerships for secure data exchange. It covers the concept of metadata in federations, and how to create your partnerships.
Chapter 6, *Adding Partners to Your Installation*	This chapter provides details on how to add and remove partners and groups of partners to your installation.
Chapter 7, *Editing Partner Settings*	This chapter provides details on how to edit your partners and partner groups.
Chapter 8, *Enabling Applications*	This chapter gives a short description on how to enable applications to work with Select Federation using the Application Helper.
Chapter 9, *Regular Administration Tasks*	This chapter provides guidance on regular post-deployment, maintenance and tasks for administrators.
Chapter 10, *Configuring Attributes*	This chapter gives instruction on how to configure Select Federation attributes.
Chapter 11, *Configuring Privacy Manager*	Select Federation allows the end users to control the transmission of their personal attributes to application partners. This chapter provides an overview of the Select Federation Privacy Manager and explains how to configure the Privacy Manager.
Chapter 12, *Authentication Contexts*	This chapter describes how to configure authentication contexts in HP OpenView Select Federation.
Chapter 13, *Configuring Liberty Introduction Service*	This chapter explains how the IDP introduction problem is solved using the Liberty Introduction Service. HP OpenView Select Federation can be configured to use this service.
Chapter 14, *Certificate Management*	This chapter provides information on the setup of certificates used to authenticate the installation and its partners.
Chapter 15, *Localizing and Customizing HP OpenView Select Federation*	This chapter explains how the end user UI can be localized.
Chapter 16, *Troubleshooting*	This chapter lists common problems with Select Federation and their solutions.

Chapter	Description
Appendix A, *Configuration Parameters*	This appendix has the configuration parameters that can be manually typed into the `tfsconfig.properties` file in order to customize your installation.
Appendix B, *Running Apache Derby as a Network Service*	This appendix describes the steps for running Apache Derby as a network service, rather than using it in embedded mode.

2 Getting Started

This chapter gives you a brief overview on HP OpenView Select Federation's capabilities. The installation and operating instructions are given in their respective chapters, which also give detailed explanations of Select Federation's various functions.

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, HP OpenView 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, HP OpenView 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.

Before Installation

- HP OpenView Select Federation documentation can be found 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.

Installation Checklist

The installation of HP OpenView Select Federation has 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 *Systems 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*.

3 **If using HP OpenView Select Access, Integrate Select Access with Select Federation.** Configure policies in the Select Access Policy Builder for proper operation of Select Federation.

4 **Change the system configuration to use HP OpenView Select Audit for logging.** See the instructions in *Integrating HP OpenView Select Audit with HP OpenView Select Federation.*

5 **Further Configuration of Select Federation.** If you need more advanced configuration changes, such as for attributes, privacy management, etc., you can further configure Select Federation by editing the `tfsconfig.properties` file. See the instructions in *Further Configuration*.

6 **Add Groups and Partners.** The first step in creating an operational federation is setting up your Groups and Partners. See the instructions in *Setting Up Partnerships* and *Adding Partners to Your Installation*.

7 **Configure Groups and Partners.**

8 **Enable Applications using the Application Helper.** HP OpenView 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*.

⚠ 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.

3 Installation

Installation Overview

From an installation perspective, HP OpenView Select Federation is itself 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, etc. 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.
- **Partner data.** This is information about your trusted partners, including friendly name, various policies to apply, etc.

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 *HP OpenView Select Federation Programmers Guide* which is provided on the Select Federation SDK CD).

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

HP OpenView Select Federation also maintains audit logs. These audit logs can be written to a relational database, to a HP OpenView Select Audit connector or both. HP OpenView Select Federation Premium Edition 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 commencing with the actual installation of Select Federation, collect information about the databases and directories to be used, including server addresses, database accounts, etc. Any of these settings can also be changed after the installation.

See *Systems Requirements* for a detailed list of supported application servers, databases and directories.

Systems Requirements

HP OpenView 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

HP OpenView 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 Specs
Intel Pentium III / AMD Athlon based IBM compatible PCs	Processor Speed: 800 MHz Main Memory: 512 MB Free Disk Space: 1 GB
HP PA-RISC based servers	Processor Speed: 500 MHz Main Memory: 512 MB Free Disk Space: 1 GB
Sun SPARC based servers	Processor Speed: 450 MHz Main Memory: 512 MB Free Disk Space: 1GB

Operating System Requirements

HP OpenView Select Federation is qualified to run on any of the operating systems shown in Table 2 (where applicable):

Table 2 Operating Systems upon which Select Federation runs

Operating System
HP-UX 11.23
Red Hat Linux AS, version 3.0 or 4.0
Windows 2000 or Windows 2003
Sun Solaris 9, Sun Solaris 10

Please note that Select Federation is a 32-bit program and where the operating system is a 64 bit operating system, it runs in the 32-bit compatibility mode.

Java Software Requirements

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

Table 3 Java Development Kits upon which Select Federation runs

Java Development Kits
JDK 1.4.2
JDK 1.5.0

Supported Third-Party Servers

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

Application Servers

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

Table 4 Applications Servers upon which Select Federation runs

Server
BEA WebLogic 8.1 SP5
IBM WebSphere 6.0.2
built-in application server

Database Servers

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

Table 5 Database Servers upon which Select Federation runs

Database
Oracle 10g
Oracle 9i
built-in database
Microsoft SQL Server 2000

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

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

Table 6 Applications Servers upon which Select Federation Runs

LDAP Server
Microsoft Active Directory for Windows 2000 with SP4 and for Windows 2003
Microsoft ADAM 1.0 (for Windows 2003)
OpenLDAP 2.2.23
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

HP OpenView

HP OpenView Select Federation 6.5 can be integrated with other components of the HP OpenView suite of identity management products.

Table 7 OpenView suite components which Select Federation can be integrated with

Components
HP OpenView Select Access 6.1 SP3
HP OpenView Select Access 6.5
HP OpenView Select Audit

System Time Synchronization

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

Installation Procedure

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

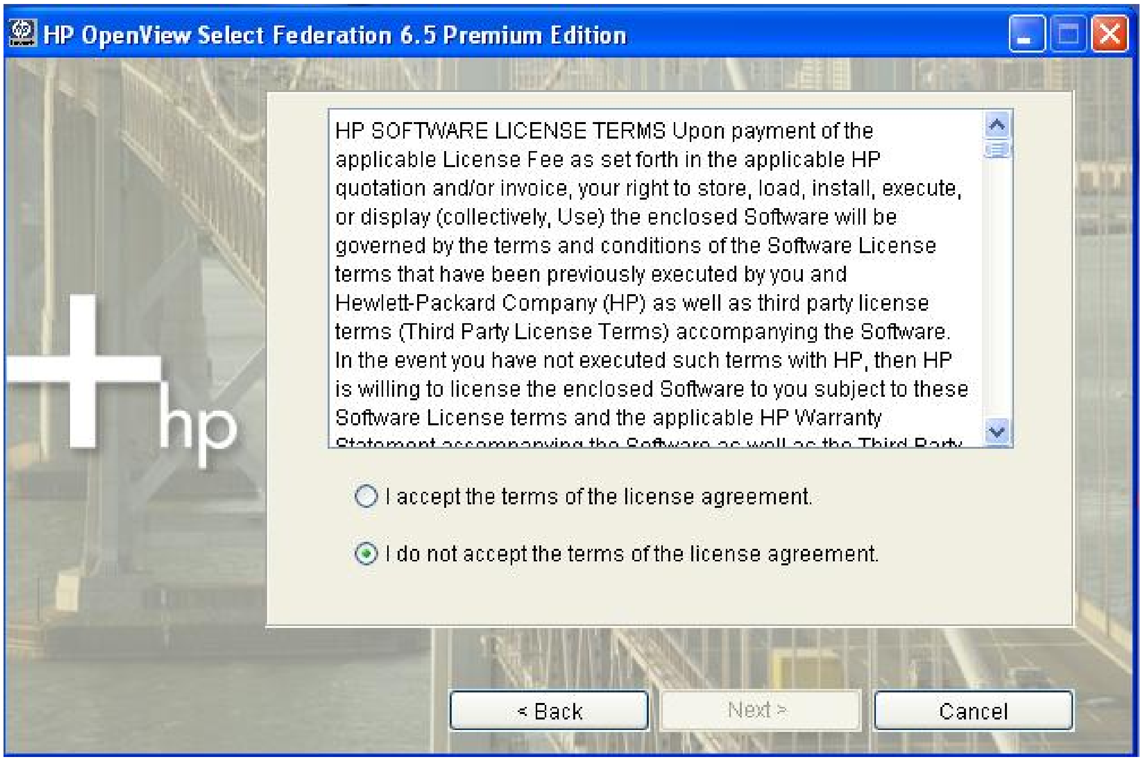
Install HP OpenView Select Federation using the automated installer by following these steps:

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 HP OpenView Select Federation install executable located on the CD.

2 **License agreement**. Read the license agreement and accept or reject it by using the radio buttons (see Figure 1). You must accept the license agreement in order to continue the installation procedure. Click **Next** to continue.

Figure 1 License agreement



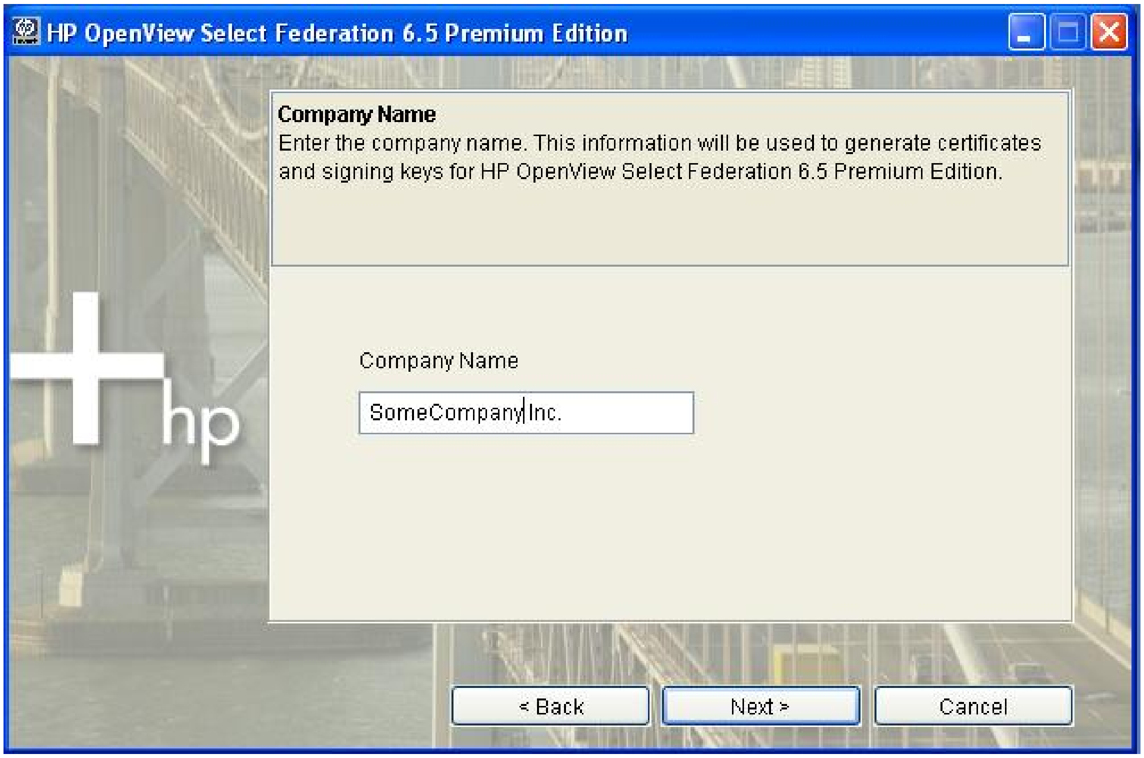
HP SOFTWARE LICENSE TERMS Upon payment of the applicable License Fee as set forth in the applicable HP quotation and/or invoice, your right to store, load, install, execute, or display (collectively, Use) the enclosed Software will be governed by the terms and conditions of the Software License terms that have been previously executed by you and Hewlett-Packard Company (HP) as well as third party license terms (Third Party License Terms) accompanying the Software. In the event you have not executed such terms with HP, then HP is willing to license the enclosed Software to you subject to these Software License terms and the applicable HP Warranty Statement accompanying the Software as well as the Third Party

○ I accept the terms of the license agreement.

● I do not accept the terms of the license agreement.

3 **Enter company name.** Enter the company name that you wish to use in generating certificates and signing keys for Select Federation. See Figure 2. Click **Next** to continue.

Figure 2 Enter company name



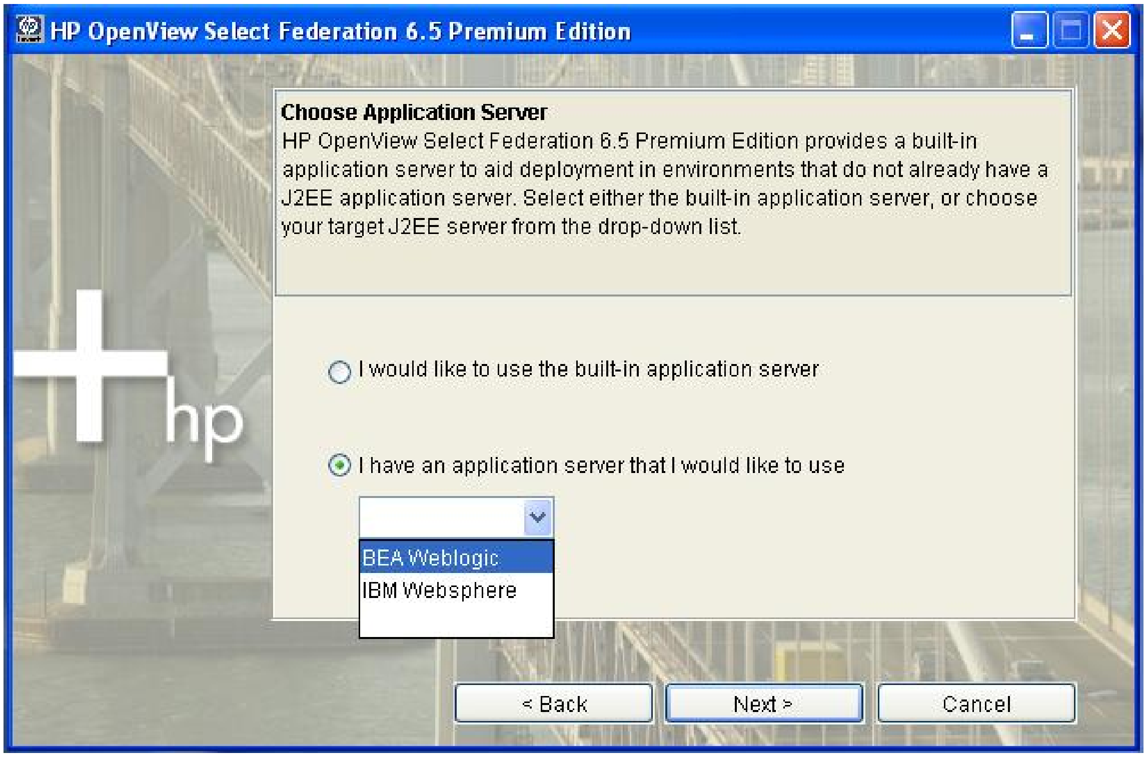
Company Name
Enter the company name. This information will be used to generate certificates and signing keys for HP OpenView Select Federation 6.5 Premium Edition.

Company Name: SomeCompany Inc.

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

4 **Choose 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 section. See Figure 3. Click **Next** to continue.

Figure 3 Choose application server



Choose Application Server

HP OpenView Select Federation 6.5 Premium Edition provides a built-in application server to aid deployment in environments that do not already have a J2EE application server. Select either the built-in application server, or choose your target J2EE server from the drop-down list.

○ I would like to use the built-in application server

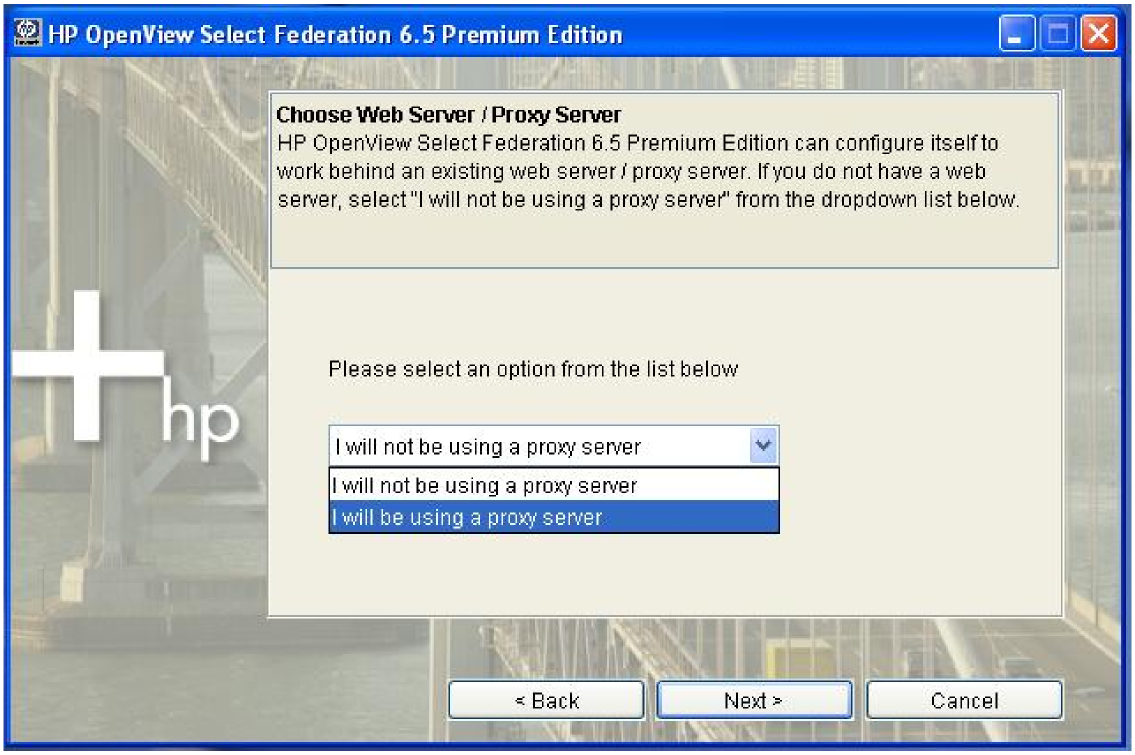
● I have an application server that I would like to use

The following three screens show the configuration required if you choose the bundled application server.

5 **Configure Application server.**

a **Bundled 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 (i.e. not using a web server), then choose **I will be using a proxy server** from the drop-down list. You will be prompted for additional information like site name, port number and protocol of your application server. The back-end server can be configured to run on any port of the user's choice as long as there is no conflict with other ports. The default port is 8080. See Figure 4, Figure 5 and Figure 6. Click **Next** to continue.

Figure 4 Choose web server / proxy server



HP OpenView Select Federation 6.5 Premium Edition

Choose Web Server / Proxy Server

HP OpenView Select Federation 6.5 Premium Edition can configure itself to work behind an existing web server / proxy server. If you do not have a web server, select "I will not be using a proxy server" from the dropdown list below.

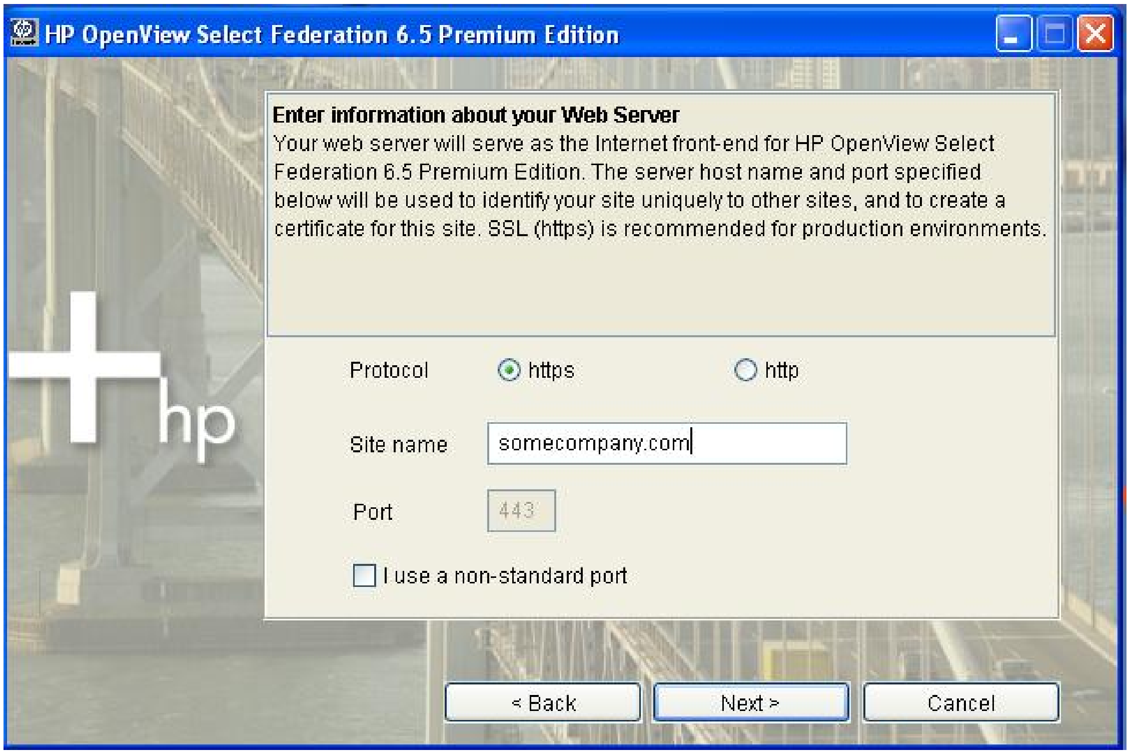
Please select an option from the list below

I will not be using a proxy server

I will not be using a proxy server

I will be using a proxy server

Figure 5 Enter information about your web server



HP OpenView Select Federation 6.5 Premium Edition

Enter information about your Web Server

Your web server will serve as the Internet front-end for HP OpenView Select Federation 6.5 Premium Edition. The server host name and port specified below will be used to identify your site uniquely to other sites, and to create a certificate for this site. SSL (https) is recommended for production environments.

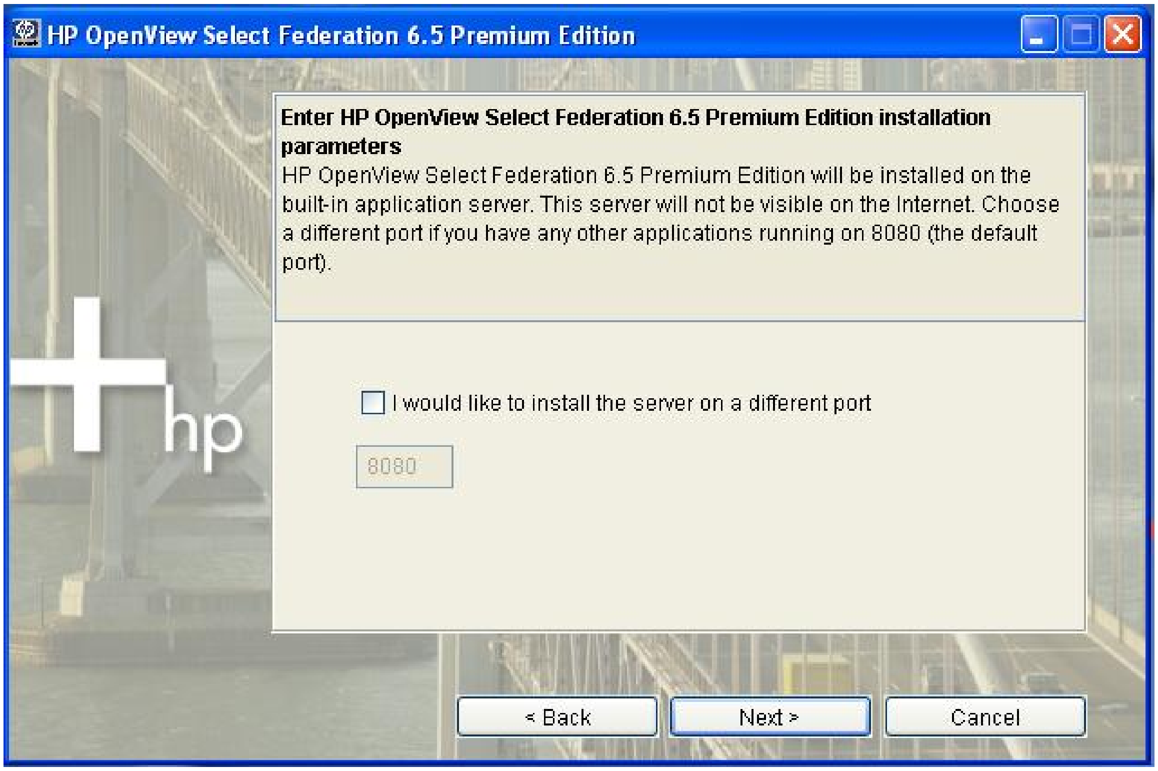
Protocol ● https ○ http

Site name somecompany.com

Port 443

□ I use a non-standard port

Figure 6 Enter HP OpenView Select Federation 6.5 Premium Edition installation parameters



HP OpenView Select Federation 6.5 Premium Edition

Enter HP OpenView Select Federation 6.5 Premium Edition installation parameters

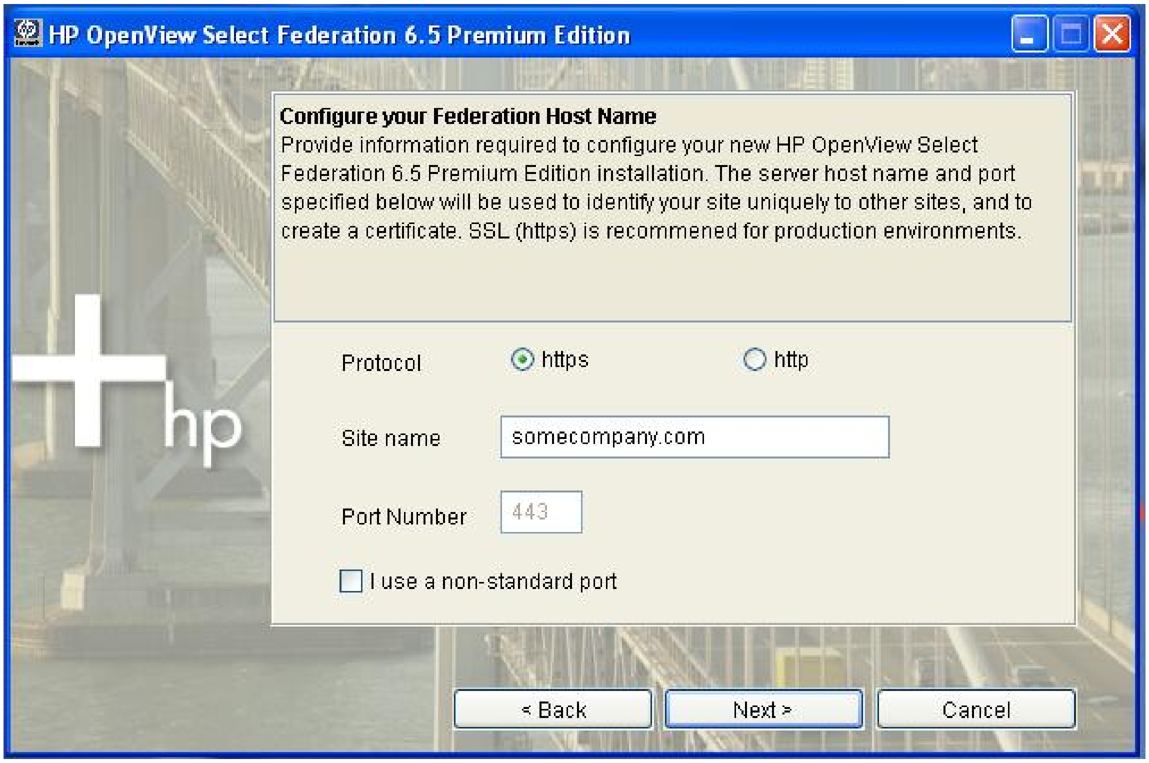
HP OpenView Select Federation 6.5 Premium Edition will be installed on the built-in application server. This server will not be visible on the Internet. Choose a different port if you have any other applications running on 8080 (the default port).

□ I would like to install the server on a different port

8080

b **Existing application server.** The server host name and port specified will be used to identify your site uniquely to other sites, and to create a signing certificate. SSL (https) is recommended for **production** environments. See Figure 7. Click **Next** to continue.

Figure 7 Configure your Federation host name



Configure your Federation Host Name

Provide information required to configure your new HP OpenView Select Federation 6.5 Premium Edition installation. The server host name and port specified below will be used to identify your site uniquely to other sites, and to create a certificate. SSL (https) is recommened for production environments.

Protocol ● https ○ http

Site name: somecompany.com

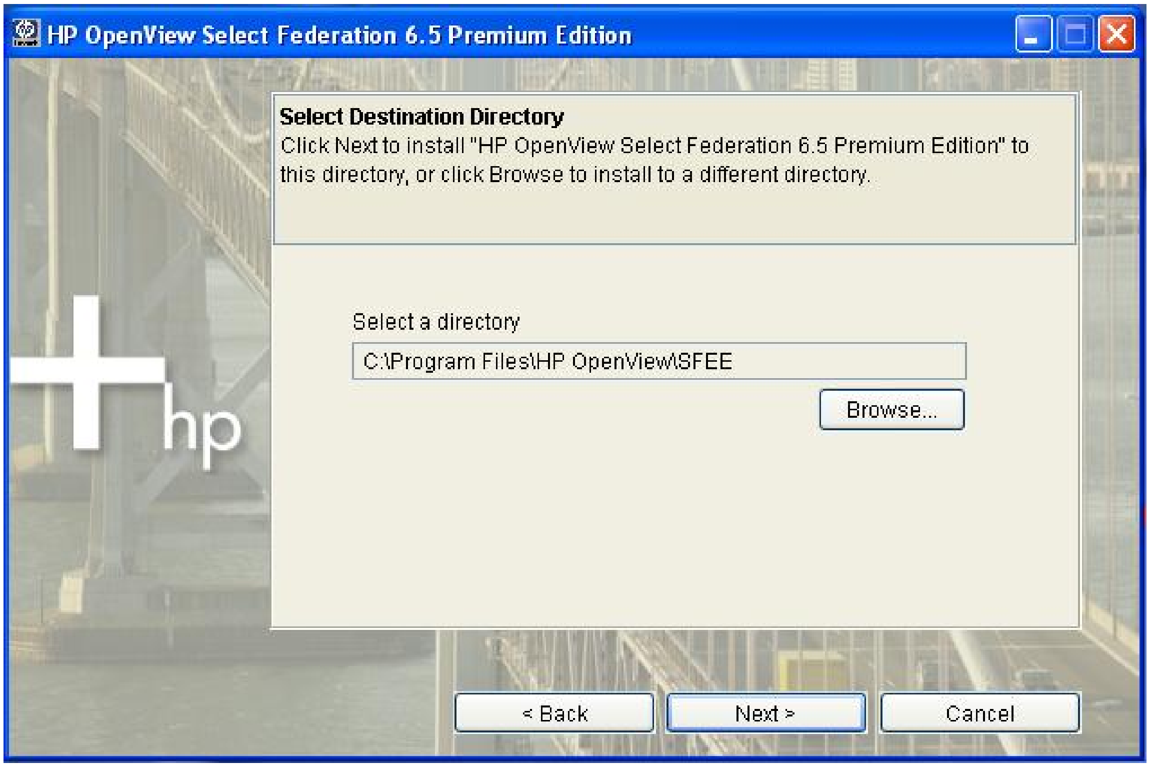
Port Number: 443

□ I use a non-standard port

6 **Select destination directory.** Use the **Browse** button to define the installation destination directory or enter the path information on the indicated space. If you have chosen to use the bundled application server, the specified path will be the home (base) of the application server. If you are instead using an existing WebLogic or WebSphere server in your environment, please 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 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. So if you had created a domain called sf65 in your Windows system, the installation directory that you specify should look something like: `C:\bea\user_projects\domains\sf65.` Please refer to the documentation of the particular application server in question for additional help. See Figure 8. Click **Next** to continue.

If you have previously installed Select Federation, you need to 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 Un-installer, but if you have not used the uninstaller or if the uninstaller did not complete successfully, you will have to verify this manually.

Figure 8 Select destination directory



Select Destination Directory

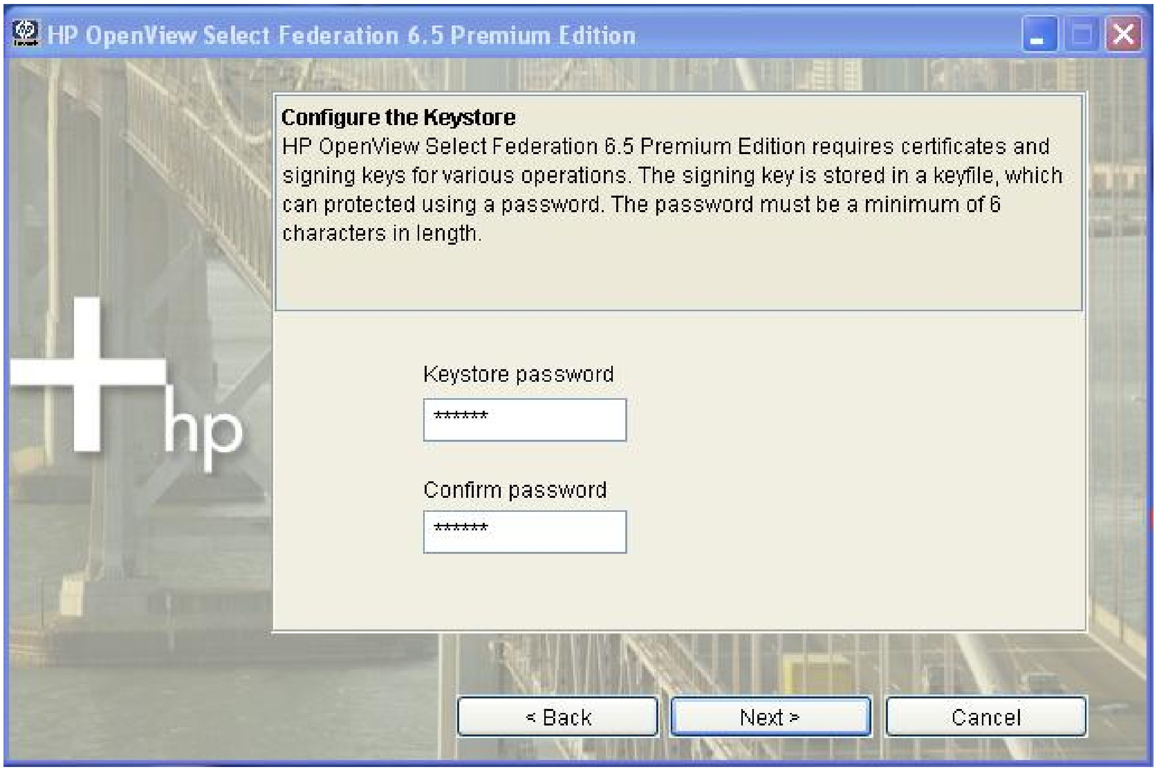
Click Next to install "HP OpenView Select Federation 6.5 Premium Edition" to this directory, or click Browse to install to a different directory.

Select a directory

C:\Program Files\HP OpenView\SFEE

7 **Configure the Select Federation keystore.** Enter the keystore password twice to create and open the keyfile that stores the signing key. The **password** cannot be left blank and should be at least 6 characters long. See Figure 9. Click **Next** to continue.

Figure 9 Configure the keystore



Configure the Keystore

HP OpenView Select Federation 6.5 Premium Edition requires certificates and signing keys for various operations. The signing key is stored in a keyfile, which can protected using a password. The password must be a minimum of 6 characters in length.

Keystore password

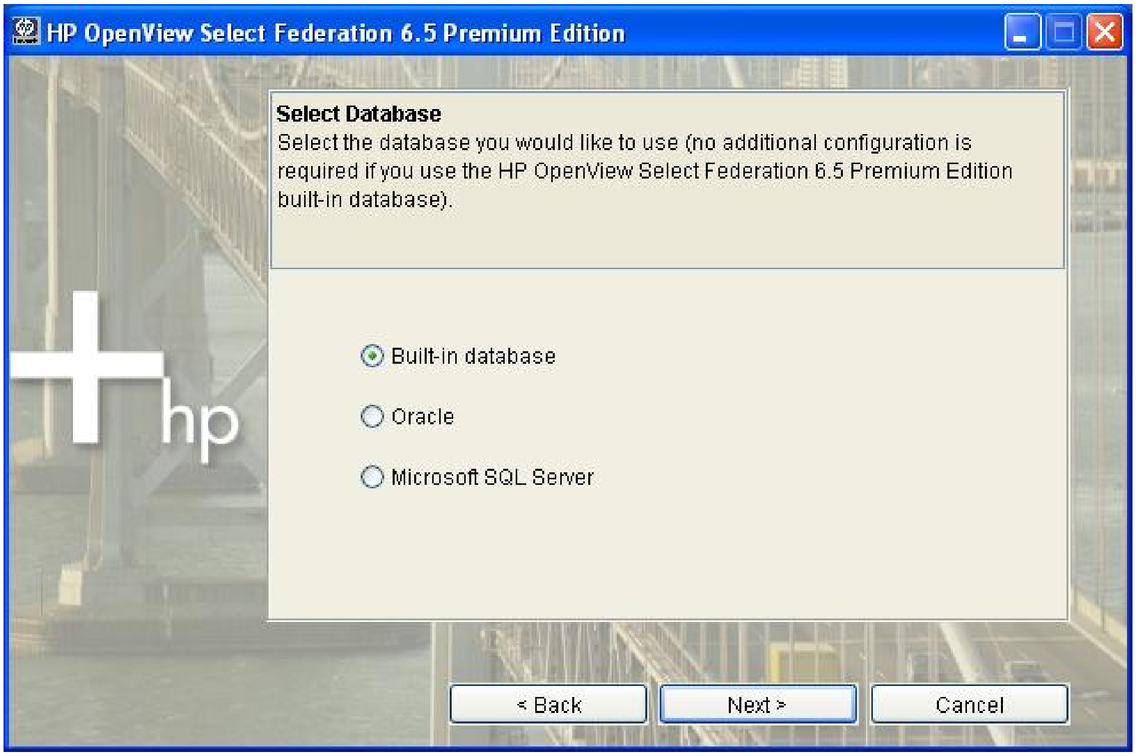
******

Confirm password

******

8 **Select database.** Choose the database you would like to use. If you choose the HP OpenView built-in database, no further database configuration is necessary. Otherwise, choose your database and click **Next** to see the configuration options. After you enter the database details, the Installer will be establishing 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. Please take appropriate corrective action in such an event. See Figure 10, Figure 11 and Figure 12. Click **Next** to continue.

Figure 10 Select database



Select Database

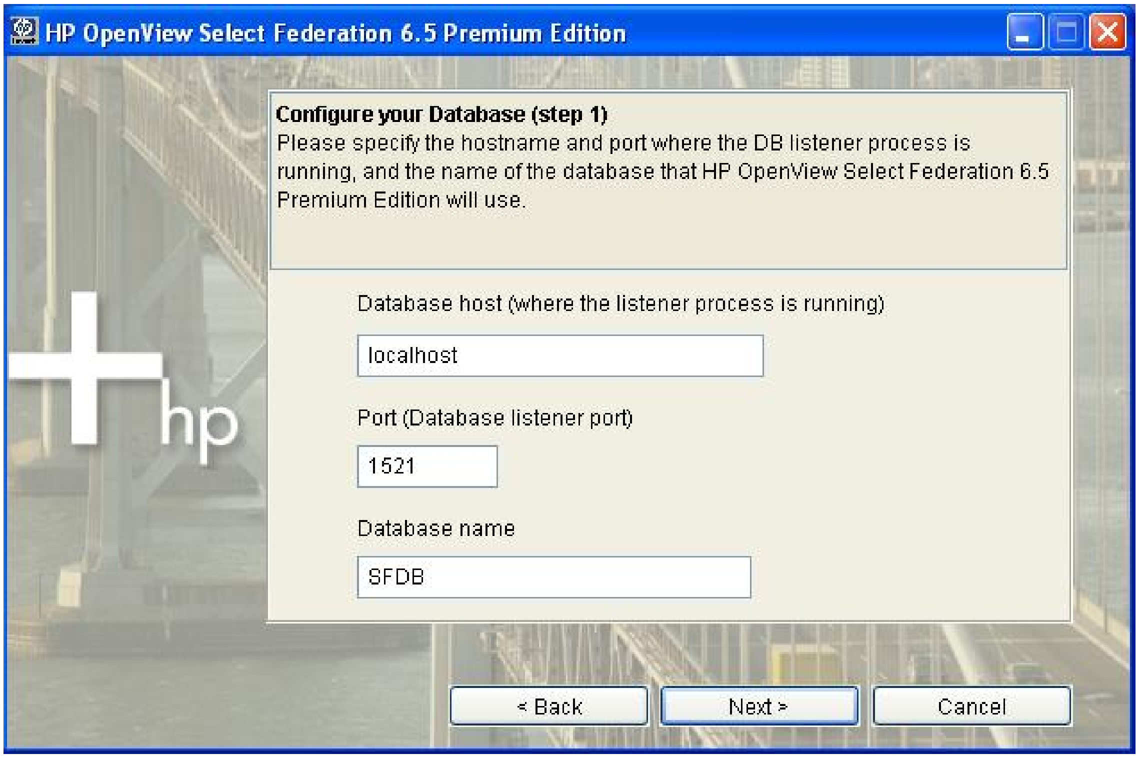
Select the database you would like to use (no additional configuration is required if you use the HP OpenView Select Federation 6.5 Premium Edition built-in database).

● Built-in database

○ Oracle

○ Microsoft SQL Server

Figure 11 Configure your database (step1)



Configure your Database (step 1)
Please specify the hostname and port where the DB listener process is running, and the name of the database that HP OpenView Select Federation 6.5 Premium Edition will use.

Database host (where the listener process is running)

localhost

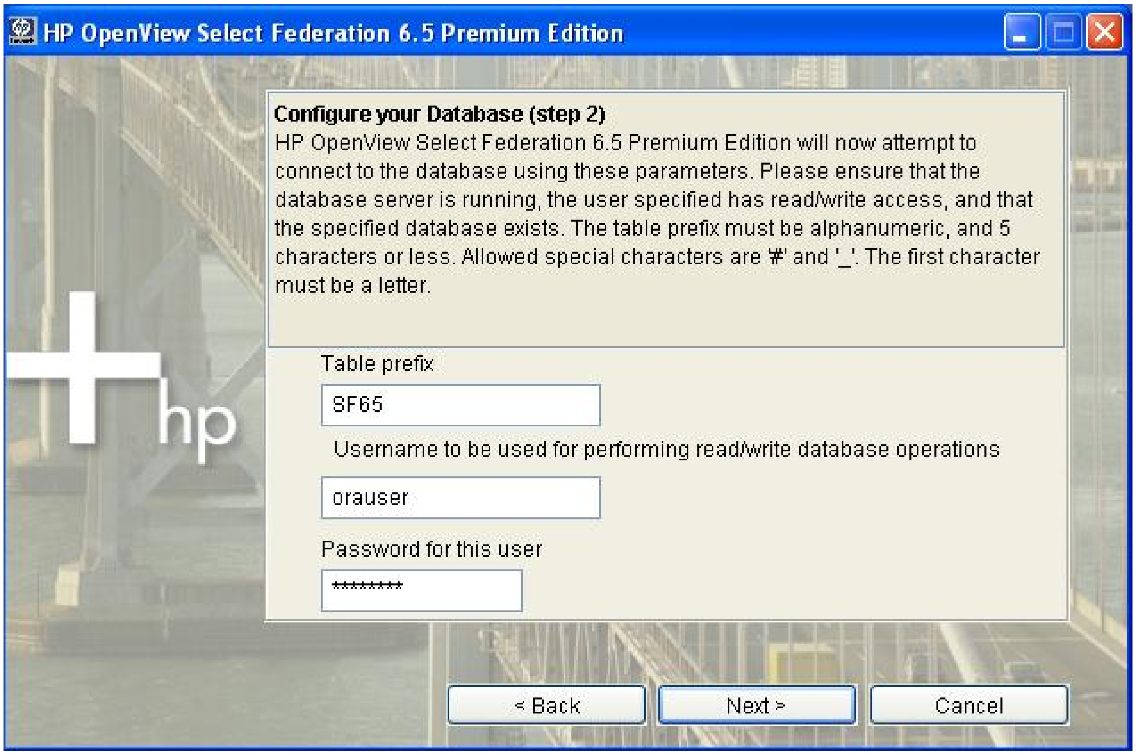
Port (Database listener port)

1521

Database name

SFDB

Figure 12 Configure your database (step2)



Configure your Database (step 2)
HP OpenView Select Federation 6.5 Premium Edition will now attempt to connect to the database using these parameters. Please ensure that the database server is running, the user specified has read/write access, and that the specified database exists. The table prefix must be alphanumeric, and 5 characters or less. Allowed special characters are '#' and '_'. The first character must be a letter.

Table prefix

SF65

Username to be used for performing read/write database operations

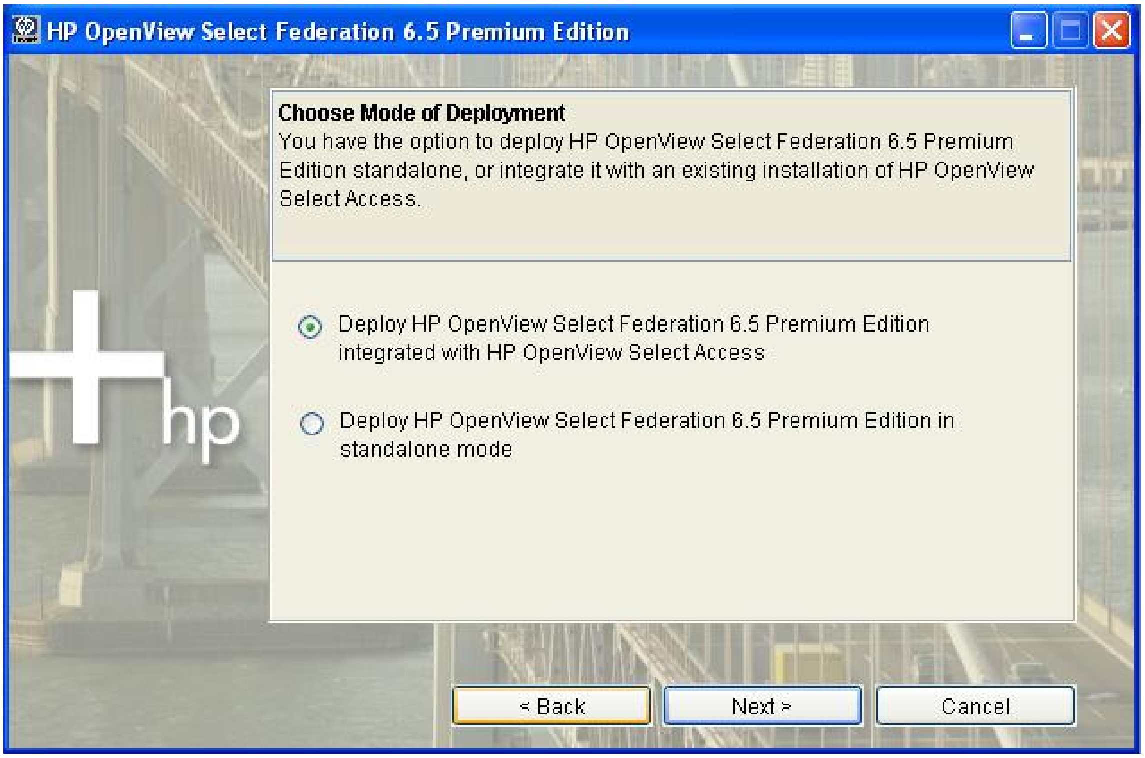
orauser

Password for this user

****

9 **Choose mode of deployment.** Using the radio buttons, choose to deploy Select Federation in standalone mode or integrated with HP OpenView Select Access. See Figure 13.

Figure 13 Choose mode of deployment



HP OpenView Select Federation 6.5 Premium Edition

Choose Mode of Deployment

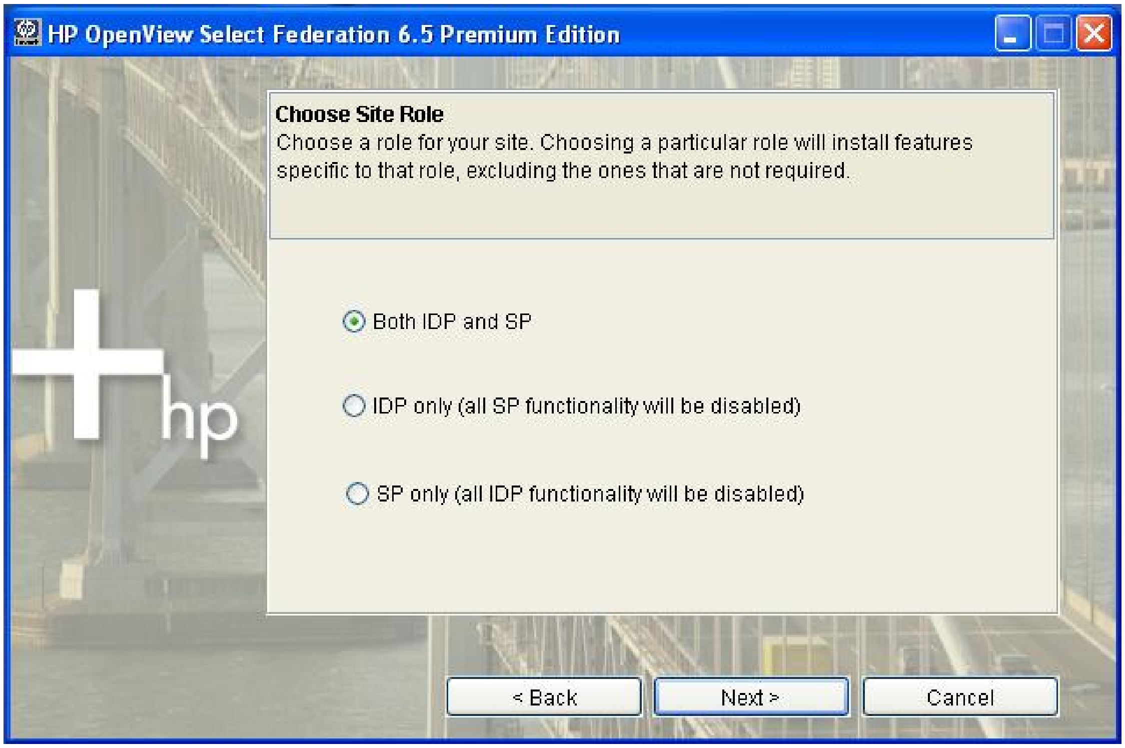
You have the option to deploy HP OpenView Select Federation 6.5 Premium Edition standalone, or integrate it with an existing installation of HP OpenView Select Access.

● Deploy HP OpenView Select Federation 6.5 Premium Edition integrated with HP OpenView Select Access

○ Deploy HP OpenView Select Federation 6.5 Premium Edition in standalone mode

10 **Choose site role.** Using the radio buttons, 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 will enable functionality specific to that role. See Figure 14. Click **Next** to continue.

Figure 14 Choose site role



HP OpenView Select Federation 6.5 Premium Edition

Choose Site Role

Choose a role for your site. Choosing a particular role will install features specific to that role, excluding the ones that are not required.

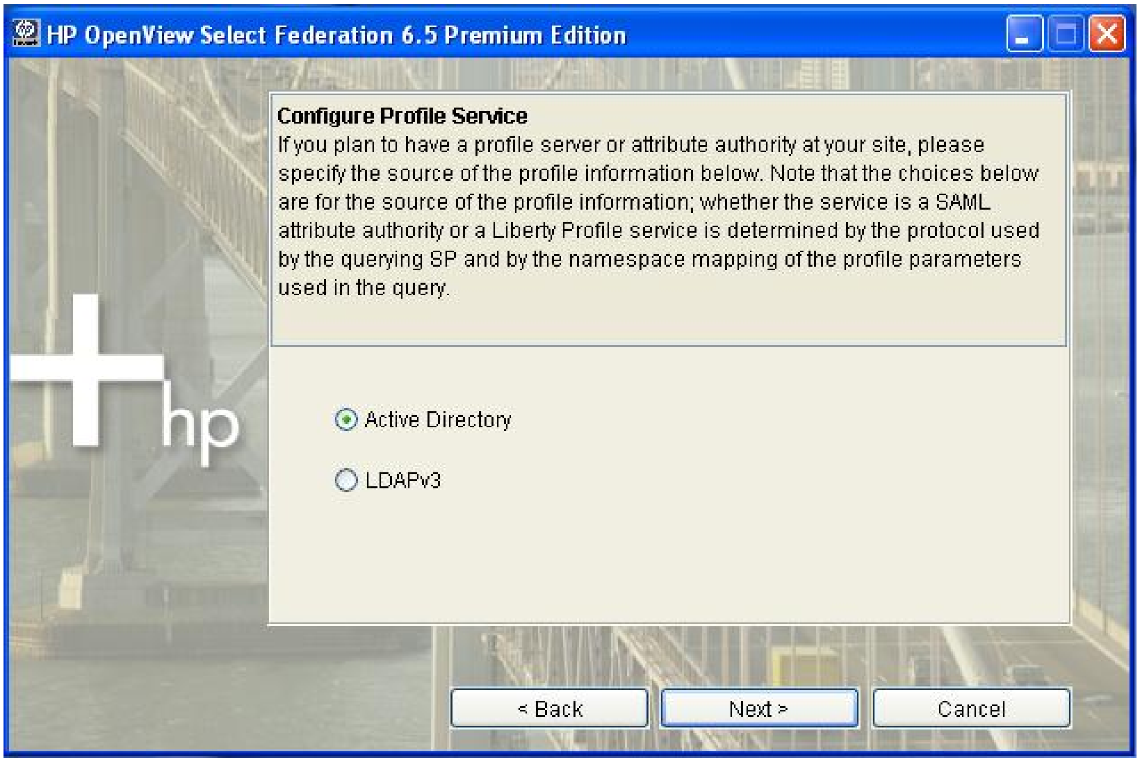
● Both IDP and SP

○ IDP only (all SP functionality will be disabled)

○ SP only (all IDP functionality will be disabled)

11 **Configure profile service.** Using the radio buttons, choose the profile service that you wish to configure. You are asked to choose the source of the profile information. This is directory server that will be integrated with Select Federation and serve as the source for the user attribute information. See Figure 15 and Figure 16. Click **Next** to continue. Depending on your choice, you will be asked to provide configuration details about either your ADS installation or any other LDAPv3 server like SunOne. The administrator name should be provided with the full DN suffix, e.g.: *Administrator name:* cn=administrator,cn=users,dc=hp,dc=net. The Base DN entry is the location where new users will be created for this instance of Select Federation. If you would like Select Federation to use SSL to communicate with the directory server, select the checkbox at the bottom of the configuration screen. Note that this would require SSL to be previously setup on the directory server. See the next step for more information.

Figure 15 Configure profile service



HP OpenView Select Federation 6.5 Premium Edition

Configure Profile Service

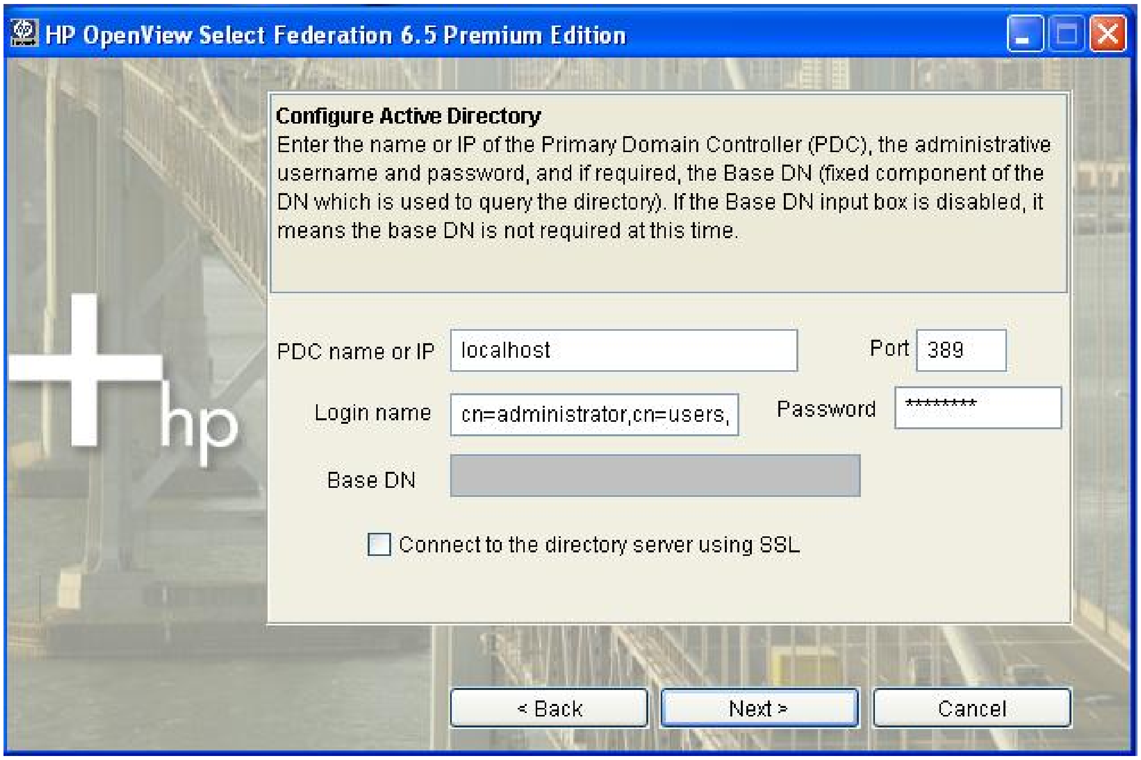
If you plan to have a profile server or attribute authority at your site, please specify the source of the profile information below. Note that the choices below are for the source of the profile information; whether the service is a SAML attribute authority or a Liberty Profile service is determined by the protocol used by the querying SP and by the namespace mapping of the profile parameters used in the query.

● Active Directory

○ LDAPv3

If you are using Active Directory, then you must make sure the Base DN you specify can have "Organizational Unit" or OU entries under it.

Figure 16 Configure profile service (continued)



Configure Active Directory

Enter the name or IP of the Primary Domain Controller (PDC), the administrative username and password, and if required, the Base DN (fixed component of the DN which is used to query the directory). If the Base DN input box is disabled, it means the base DN is not required at this time.

PDC name or IP: localhost

Port: 389

Login name: cn=administrator,cn=users,

Password: ********

Base DN:

□ Connect to the directory server using SSL

12 For LDAP configuration, you will see the following, depending on the provider type and deployment chosen:

Provider type "IDP and SP", deploying with HP OpenView Select Access

- Profile service screen (choose Active Directory/LDAPv3), see Figure 17, followed by:
  - LDAP connection information screen for the IDP, see Figure 18. We do not need the Base DN information for the IDP in this case.
  - SP LDAP Base DN, see Figure 19. Note that we do not need to prompt for other connection parameters, since that information is available from the previous IDP dialog.

Provider type "IDP and SP", deploying without HP OpenView Select Access

- Profile service screen (choose Active Directory/LDAPv3), see Figure 17, followed by:
  - LDAP connection information screen for the IDP, see Figure 20.

Provider type "IDP only", deploying with HP OpenView Select Access

- Profile service screen (choose Active Directory /LDAPv3), see Figure 17, followed by:
  - LDAP connection information screen for the IDP, see Figure 18. We do not need the Base DN information for the IDP in this case.

Provider type "IDP only", deploying without HP OpenView Select Access

- Profile service screen (choose Active Directory /LDAPv3), see Figure 17, followed by:
  - LDAP connection information screen for the IDP, see Figure 20.

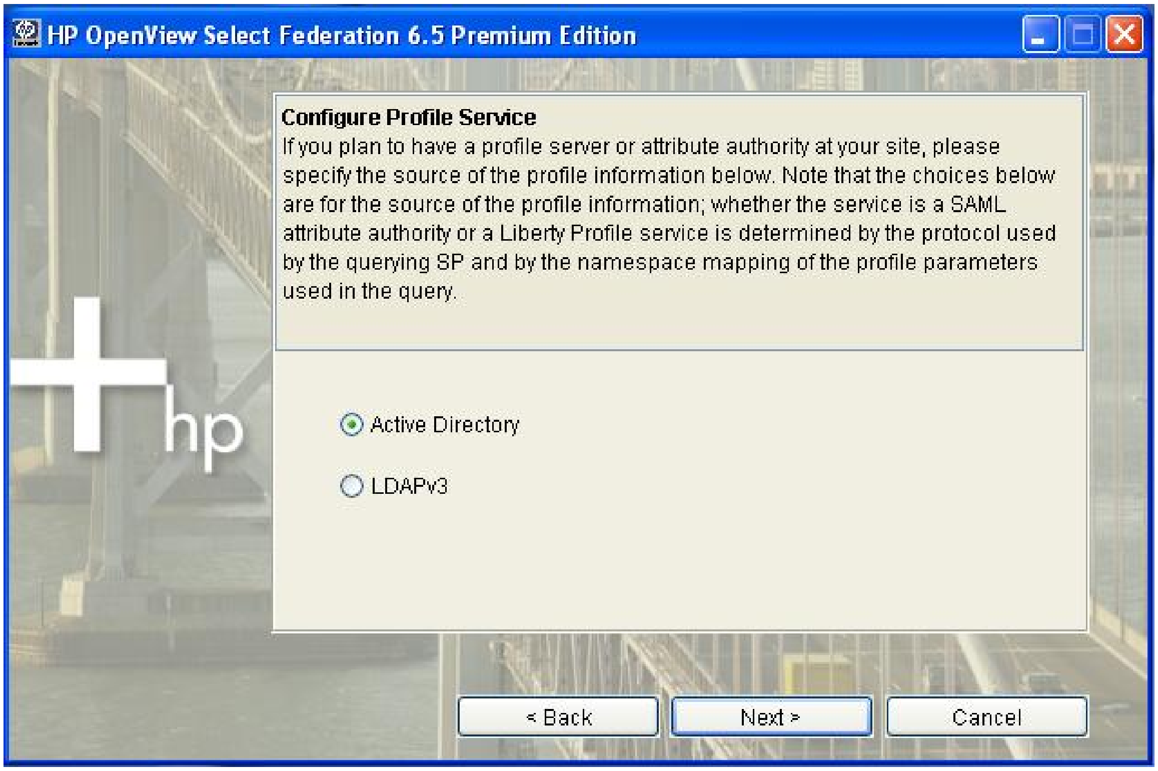
Provider type "SP", deploying with HP OpenView Select Access

- Profile service screen (choose Active Directory /LDAPv3), see Figure 17, followed by:
  - LDAP connection information screen for the SP, see Figure 21, which is used for incoming IDP authenticated users.

Provider type "SP", deploying without HP OpenView Select Access

- No LDAP configuration is required.

Figure 17 Configure profile service



HP OpenView Select Federation 6.5 Premium Edition

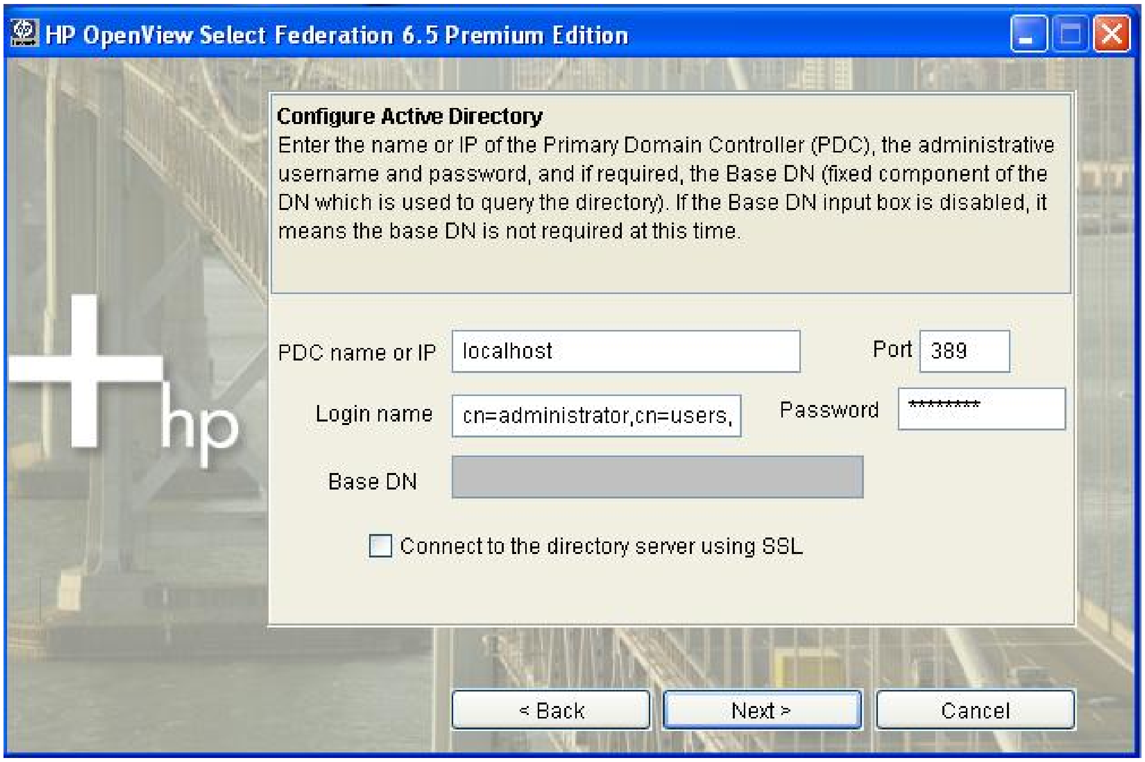
Configure Profile Service

If you plan to have a profile server or attribute authority at your site, please specify the source of the profile information below. Note that the choices below are for the source of the profile information; whether the service is a SAML attribute authority or a Liberty Profile service is determined by the protocol used by the querying SP and by the namespace mapping of the profile parameters used in the query.

● Active Directory

○ LDAPv3

Figure 18 Configure LDAP directory



Configure Active Directory

Enter the name or IP of the Primary Domain Controller (PDC), the administrative username and password, and if required, the Base DN (fixed component of the DN which is used to query the directory). If the Base DN input box is disabled, it means the base DN is not required at this time.

PDC name or IP: localhost

Port: 389

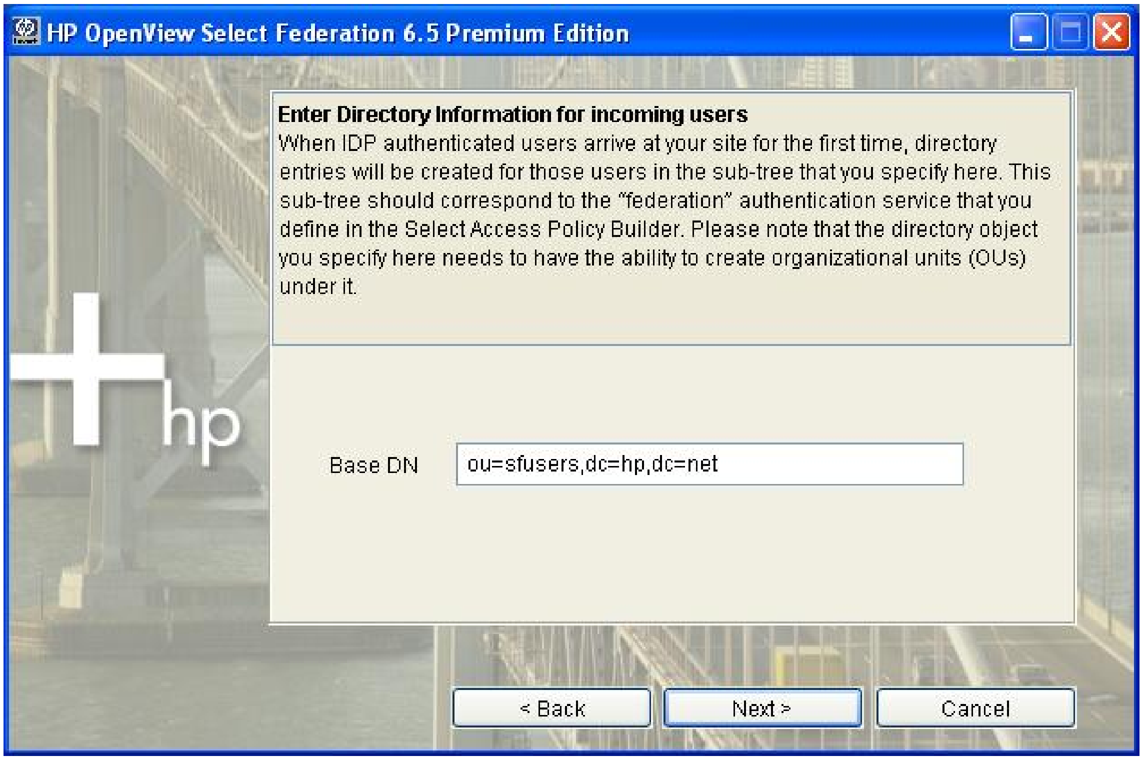
Login name: cn=administrator,cn=users,

Password: *********

Base DN:

□ Connect to the directory server using SSL

Figure 19 Enter directory information for incoming users

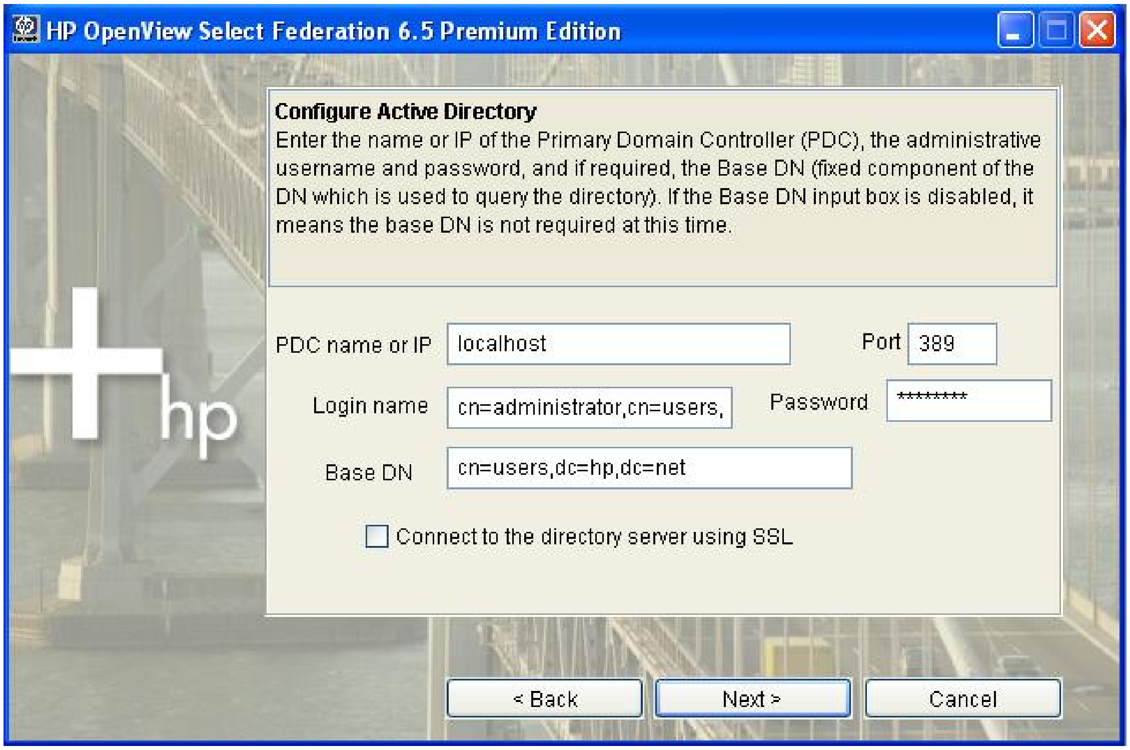


Enter Directory Information for incoming users

When IDP authenticated users arrive at your site for the first time, directory entries will be created for those users in the sub-tree that you specify here. This sub-tree should correspond to the "federation" authentication service that you define in the Select Access Policy Builder. Please note that the directory object you specify here needs to have the ability to create organizational units (OUs) under it.

Base DN: ou=sfusers,dc=hp,dc=net

Figure 20 Configure LDAP directory



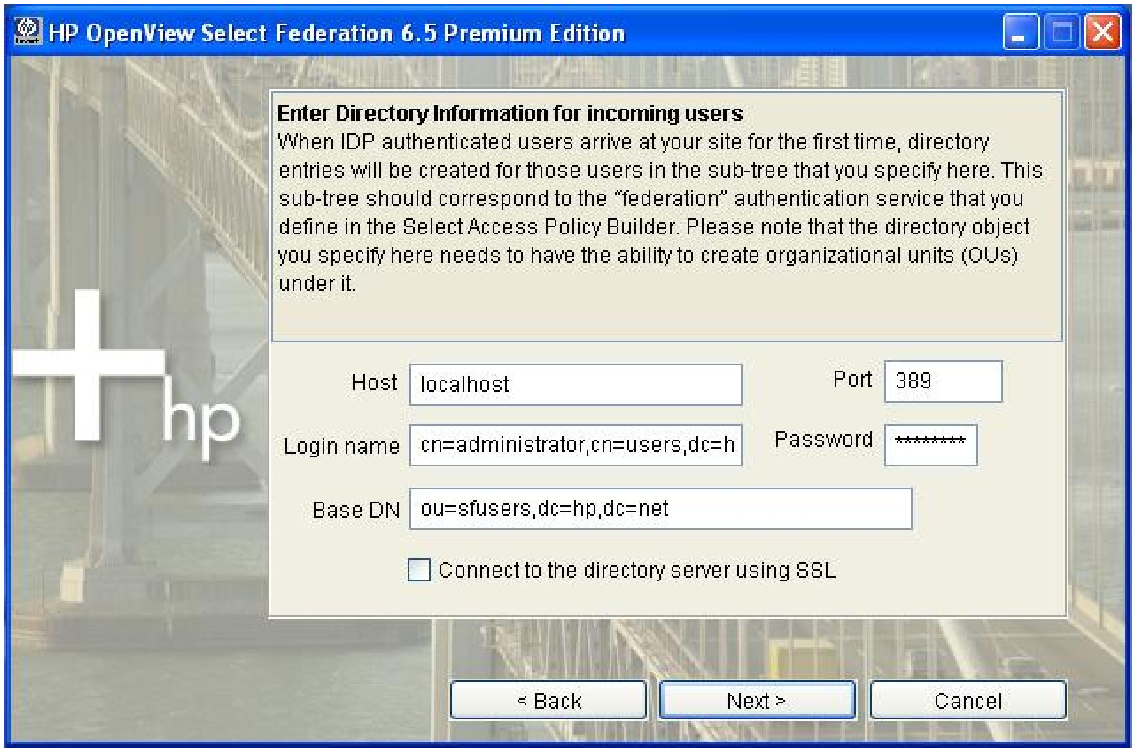
Configure Active Directory

Enter the name or IP of the Primary Domain Controller (PDC), the administrative username and password, and if required, the Base DN (fixed component of the DN which is used to query the directory). If the Base DN input box is disabled, it means the base DN is not required at this time.

PDC name or IP: localhost
Port: 389
Login name: cn=administrator,cn=users,
Password: *********
Base DN: cn=users,dc=hp,dc=net

□ Connect to the directory server using SSL

Figure 21 Enter directory information for incoming users



Enter Directory Information for incoming users

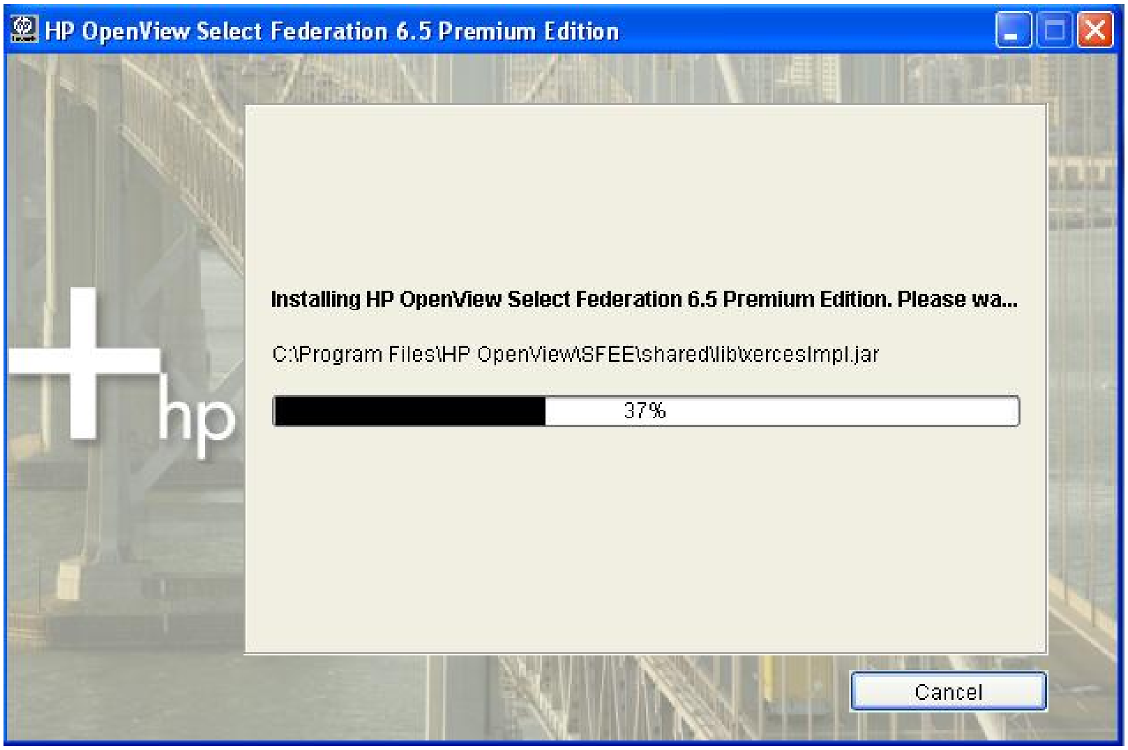
When IDP authenticated users arrive at your site for the first time, directory entries will be created for those users in the sub-tree that you specify here. This sub-tree should correspond to the “federation” authentication service that you define in the Select Access Policy Builder. Please note that the directory object you specify here needs to have the ability to create organizational units (OUs) under it.

Host: localhost
Port: 389
Login name: cn=administrator,cn=users,dc=h
Password: *********
Base DN: ou=sfusers,dc=hp,dc=net

□ Connect to the directory server using SSL

13 **Summary information.** Verify that the installation information is correct and click **Install**. Installation progress is shown in a progress bar and as completed percentage. See Figure 22.

Figure 22 Installation progress



HP OpenView Select Federation 6.5 Premium Edition

Installing HP OpenView Select Federation 6.5 Premium Edition. Please wa...

C:\Program Files\HP OpenView\SFEE\shared\lib\xercesImpl.jar

37%

14 **Ending installation.** Verify that the installation has been successful by reading the summary information. Click **Finish**. The installer will launch a browser window to your site and closes itself.

Finishing Installation

If you chose the option of deploying on an existing application server, there are a few simple steps required to complete the installation process. Please follow the links and steps below.

1 Deploying HP OpenView Select Federation on an existing server:

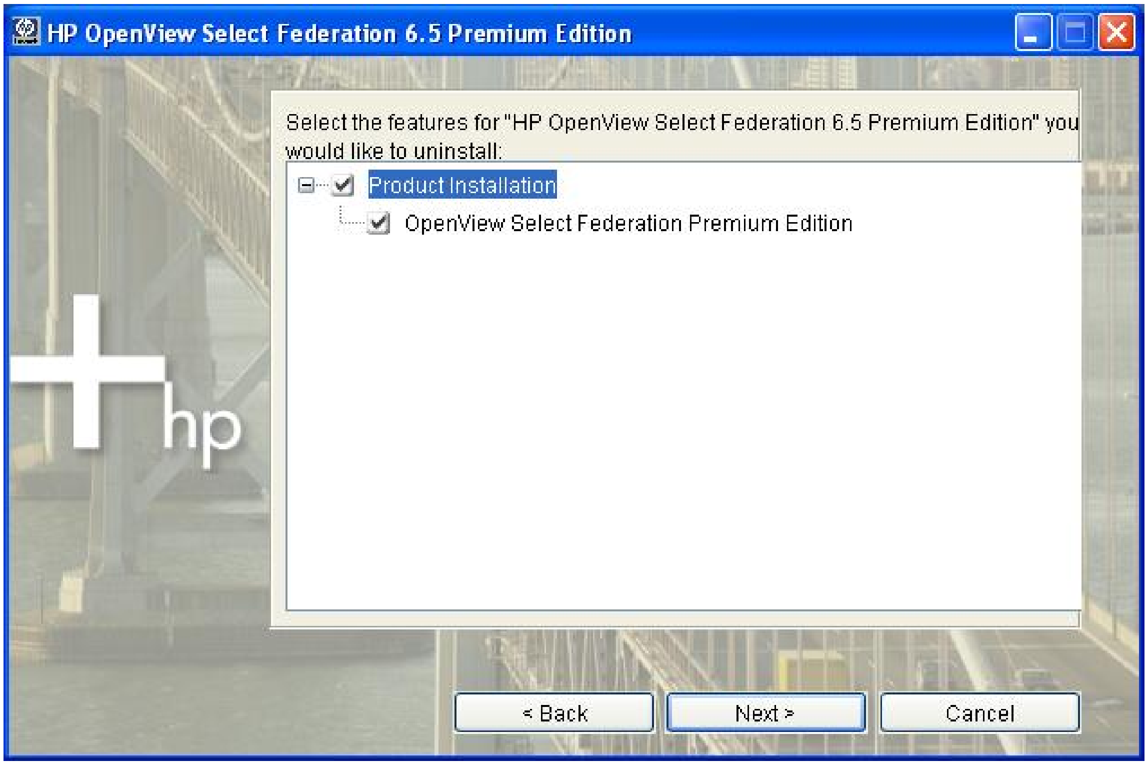
- See *Deployment instructions for BEA WebLogic server version 8.1* on page 39 or
- See *Enabling Logging* on page 42.

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

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 23. The following screen capture is given for a Microsoft Windows® installation, Premium Edition. Uninstallation on other supported operating systems, or for the Enterprise Edition, is the same for all practical purposes.

Figure 23 Uninstallation



Select the features for "HP OpenView Select Federation 6.5 Premium Edition" you would like to uninstall:

☑ Product Installation
- ☑ OpenView Select Federation Premium Edition

Further Configuration

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

Considerations for a Production Deployment

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

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*)
- 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, HP OpenView 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. Hence 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.

Security

Security is an important aspect of a production deployment. HP OpenView 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 in a DMZ.
- 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 HP OpenView Select Access is used for authentication, the Select Access policies should be setup in such a way that only authorized administrators have access.

Deploying HP OpenView Select Federation on an Existing Application Server

The HP OpenView Select Federation Installer can install a built-in application server during the installation procedure. If you choose not to use this built-in application server installation, but instead want to use an existing application server, follow the instructions below.

Deploying the server consists of three steps:

1. Refer to the configuration file from the WARs.
2. Deploy the configured EAR.
3. Run the EAR.

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 below.

Deployment instructions for BEA WebLogic server version 8.1

Step 1. Verify configuration

The Select Federation installer would have generated certain configuration files and copied them over to the WebLogic server domain that was specified as the destination directory during installation. Please verify that a directory named “conf” should have been created with the required configuration files.

Step 2. Recommended JDK

BEA WebLogic comes bundled with two JDKs:

- the JRockit JDK
- the Sun JDK.

We recommend using the Sun JDK for the server domain where Select Federation is installed.

Step 3. Ensuring JDBC Driver is in the classpath

Since Select Federation relies on a database, you need to make sure the appropriate JDBC driver is available to the application server. All the required drivers can be found under the /database/drivers sub-directory of the installation. You can also obtain the latest versions of the respective drivers from the vendor’s web site. To ensure that the appropriate JDBC driver is available to the application server, add the appropriate file to the BEA WebLogic server’s classpath.

If you are using Oracle 10g, you can download the Oracle 10g JDBC driver from: http://otn.oracle.com/software/tech/java/sqlj_jdbc/index.html. If this driver (ojdbc14.jar) is already present in the server's classpath, you will not need to do anything. Otherwise, you will have to add this driver to the classpath.

If you are using the built-in database, the required driver file is called derby.jar, which will also have to be copied to the classpath.

If you are using Microsoft SQL server as your database, the driver is called jtds-1.1.jar. In this case, you will have to manually edit the server startup file (startWebLogic.sh or startWebLogic.cmd depending on your OS) to include the MSSQL driver in the server classpath.

Step 4. (Windows only) Modify the server classpath

If you are deploying Select Federation on the windows platform, you must add several jar files to the BEA WebLogic server's classpath. This extra step is not required on UNIX platforms.

The Select Federation package is a J2EE "Enterprise Archive" or EAR located at `$SF_HOME/sf_ear/tfs.ear` in the distribution. To unpack the EAR, first create a new directory (staging in the example below) in a working area and then explode the EAR there by using the commands below:

```
% mkdir staging
% cd staging
% jar xf $SF_HOME/sf_ear/tfs.ear
```

The staging directory will now contain a number of files, some with the extension "`.jar`", others with the extension "`.war`" and a `META-INF` directory.

Add the following files to the server classpath:

- `commons-logging.jar`
- `derby.jar`, OR `ojdbc.jar`, OR `jtds-1.1.jar` (depending on the database being used)
- `log4j-1.2.5.jar`
- `xalan.jar`
- `xercesImpl.jar`
- `xml-apis.jar`
- `xmlParserAPIs.jar`

When integrating with HP OpenView Select Access, the following JAR files need to be added to the BEA WebLogic classpath:

- `bcprov-jdk14-125.jar`
- `castor-0.9.3.19-xml.jar`
- `EnforcerAPI.jar`
- `jakarta-oro-2_0.jar`
- `jdom.jar`
- `ldapjdk.jar`
- `mail.jar`
- `msgsresources.jar`
- `protomatter.jar`
- `servletenforcer.jar`
- `shared.jar`
- `xml.jar`
- `xmlsec.jar`

If your WebLogic server is running, you need to restart the WebLogic server process.

Step 5. Deploy the configured EAR on BEA WebLogic

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.

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

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:

- Upload the `$SF_HOME/sf_ear/tfs.ear`.
- Select the `tfs.ear` in the list seen at the bottom of the screen.

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**.

Viewing Select Federation Debug/Error Logs on WebLogic:

Select Federation uses Log4j and errors are logged to the console. You should be able to see DEBUG messages since the log4j configuration file was added to the classpath in Step 4. If anything goes wrong in running Select Federation, you will see it mentioned in the logs.

Enabling logging

To enable logging, add the directory containing the `log4j.properties` file (`$SF_HOME\properties`) to the the server classpath. The classpath can be found within the server startup script – `startWebLogic.cmd` for Windows and `startWebLogic.sh` for UNIX.

For example, the entries can be added as shown below:

```
set CLASSPATH=<existing entries>;
set SF_HOME=<Destination directory chosen during installation>
set SF_JARS=<path to the staging directory created above>
%SF_HOME%\properties;%SF_JARS%\commons-logging.jar;<entries for all the
other jars>
```

Deploying on IBM WebSphere Server version 6.0.2

Step 1. Verify configuration

The Select Federation installer would have generated certain configuration files and copied them over to your WebSphere server profile that was specified as the destination directory during installation. Please verify that a directory named “`conf`” should have been created with the required configuration files.

Step 2. Copying the JDBC driver

Since Select Federation relies on a database, you need to make sure the appropriate JDBC driver is available to the application server. All the required drivers can be found under the `/database/drivers` subdirectory of the installation. You can also obtain the latest versions of the respective drivers from the vendor's web site.

If you are using Oracle 10g, you can download the Oracle 10g JDBC driver from: `http://otn.oracle.com/software/tech/java/sqlj_jdbc/index.html`.

If you are using the built-in database, the required driver file is called `derby.jar`. If instead, you are using Microsoft SQL server as your database, the driver is called `jtds-1.1.jar`.

To ensure that the appropriate JDBC driver is available to the application server, add the appropriate file to the IBM WebSphere server's classpath. For example, if you are using Oracle, copy the file `ojdbc14.jar` to the WebSphere server's `/Appserver/lib` directory.

Step 3. Deploy the configured EAR on IBM 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), simply 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. You will see the new Select Federation as **Select Federation** in the list in the right pane.
8. Check the box next to the line corresponding to Select Federation and click **Start**.
9. When the server starts, you will see a green arrow in the right pane.

Step 4. Running Select Federation and viewing logs

The Select Federation will be running after the deployment as shown in the steps above.

Select Federation uses Log4j for diagnostic logging. These messages will be seen in the server console, and also get written to a log file under `<profile>\logs\server1\SystemOut.txt`.

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`. You will see a Welcome page. Follow the link in the section titled **Administration Console** on the welcome screen to login to the management console.

Integrating HP OpenView Select Access with HP OpenView Select Federation

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

It is important to configure and set apropriate 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.

To Configure the Federation Authentication Server

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.

To Create a Logout Rule

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 type 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.

To Add HP OpenView Select Federation Resources to the Policy Matrix

1. In the Select Access Policy Builder, create a new service on the Resources Tree, and name it appropriately for your deployment, e.g. “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 Chapter 4 of the *HP OpenView Select Access Policy Builder User’s Guide*.

2. To create Select Federation resources in Select Access, import the resource list provided for this purpose.

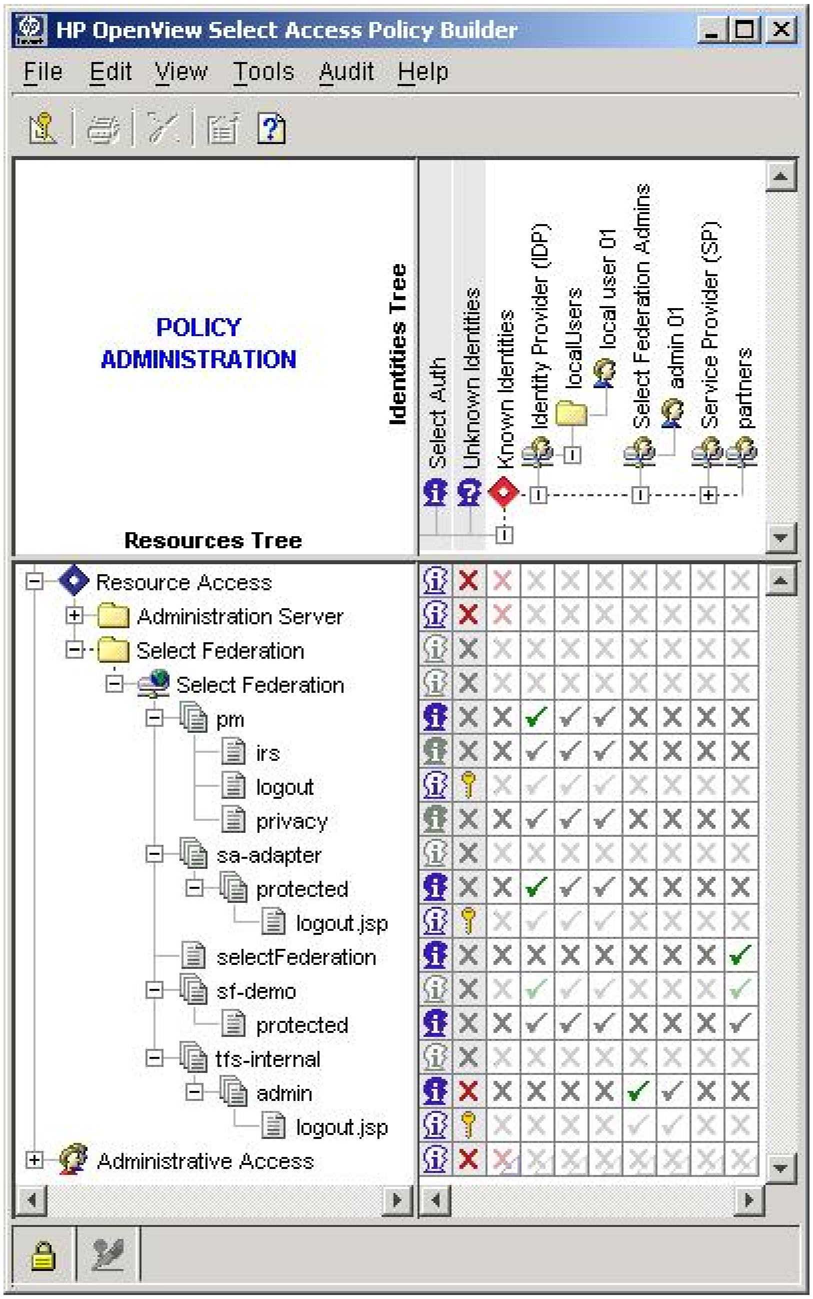
   The resource list is automatically saved to `/config/sf-URLs.txt`.

   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 resources, see Chapter 4, Building Your Users and Resources Tree, of the *HP OpenView Select Access Policy Builder User’s Guide*.

3. When you are finished you will have created entries that look like Figure 24.

Figure 24 Nested Select Federation resources



Authorize Entitlements with Access Policies

Configure each resource as follows:

pm

The pm resource is only included in HP OpenView Select Federation Premium Edition and is only needed for an installation that acts as an authority.

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, we will be 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, we will be 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, we will be 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, etc.)
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 HP OpenView Select Audit with HP OpenView Select Federation

In HP OpenView Select Audit integration, the system sends operational and administrative events to HP OpenView Select Audit (not the entries that end up in the log files). Add the following entries to `tfsconfig.properties` in order to use it:

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

```
auditDataProvider=com.trustgenix.hpsf.selectaudit.AuditDataProvider_Sel
ectAudit
```

Uncommenting the following line will ensure concurrent logging to the default AuditDataProvider:

```
AuditDataProvider_SelectAudit.auditToHPSF=1
```

4 Navigating the HP OpenView Select Federation Administration Console

HP OpenView Select Federation provides an Administration Console that allows the root administrator to add and configure additional delegated administrators to Select Federation, and to monitor the activities of these delegated administrators and end users.

Running the Administration Console

The Select Federation management console is typically deployed at:

```
http://<base-url>/tfs-internal
```

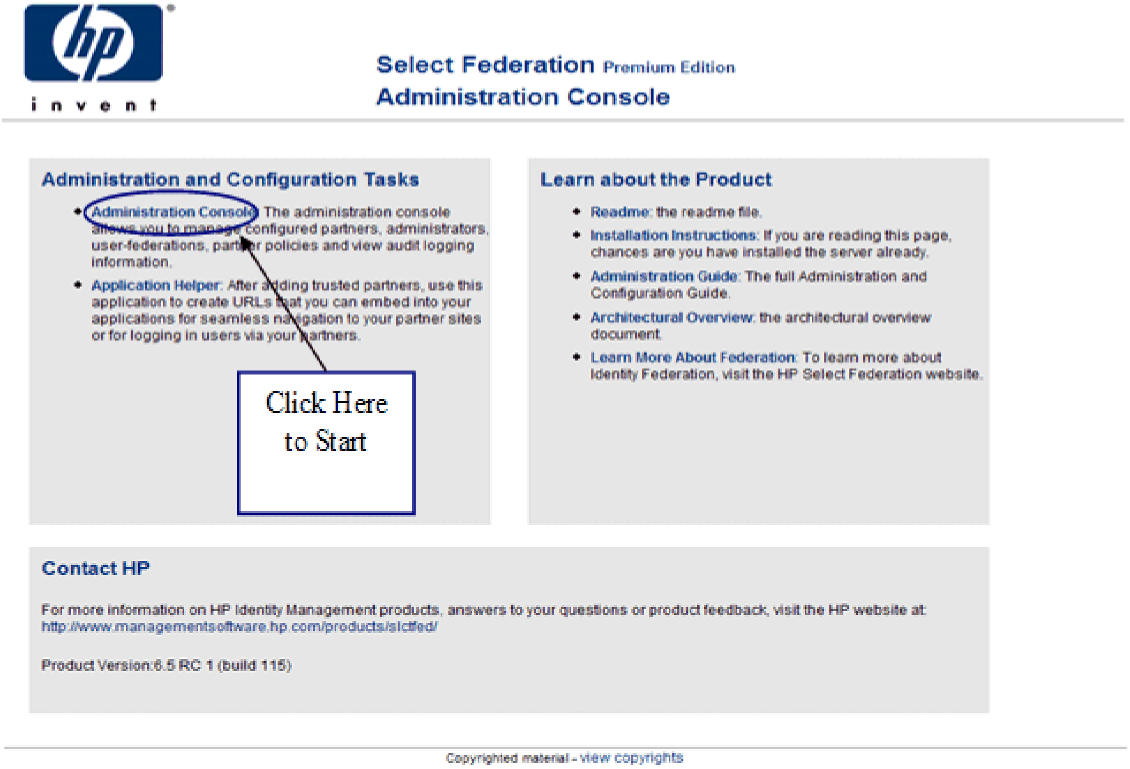
where *base-url* is the root of the application server on which you have deployed Select Federation.

After you install Select Federation, you will find a Select Federation Administration Console startup page that has links to the documentation and various resources. It also includes a link to the Administration Console, as shown in Figure 25.

If HP OpenView Select Access is not used, the default Admin account is “`admin`” and the default password is “`tgadmin`”.

➤ You should change the default password immediately after installing Select Federation.

Figure 25 Select Federation Startup page



Select Federation Premium Edition
Administration Console

Administration and Configuration Tasks

- Administration Console: The administration console allows you to manage configured partners, administrators, user-federations, partner policies and view audit logging information.
- Application Helper: After adding trusted partners, use this application to create URLs that you can embed into your applications for seamless navigation to your partner sites or for logging in users via your partners.

Click Here to Start

Learn about the Product

- Readme: the readme file.
- Installation Instructions: If you are reading this page, chances are you have installed the server already.
- Administration Guide: The full Administration and Configuration Guide.
- Architectural Overview: the architectural overview document.
- Learn More About Federation: To learn more about Identity Federation, visit the HP Select Federation website.

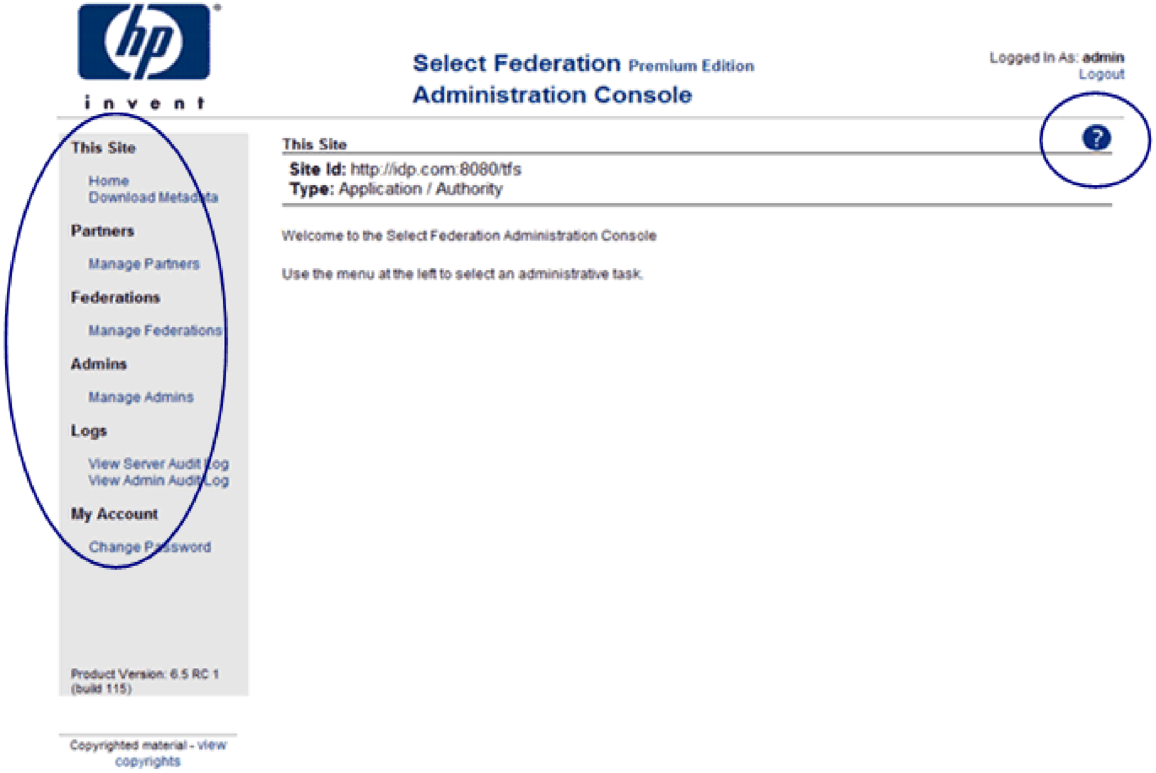
Contact HP

For more information on HP Identity Management products, answers to your questions or product feedback, visit the HP website at: http://www.managementsoftware.hp.com/products/slctfed/

Product Version:6.5 RC 1 (build 115)

Copyrighted material - view copyrights

Figure 26 Select Federation Administration Console



Select Federation Premium Edition
Administration Console

Logged In As: admin
Logout

This Site

Site Id: http://idp.com:8080/tfs
Type: Application / Authority

Welcome to the Select Federation Administration Console

Use the menu at the left to select an administrative task.

Product Version: 6.5 RC 1 (build 115)

Copyrighted material - view copyrights

Understanding Menu Sidebar Options

On the left-pane of the Administration Console is the Menu Sidebar (see Figure 26) that links the administrator to all the features of this product. Here is a brief summary of each link, more details on how to use these features follow this summary:

Home – Clicking **Home** will bring you back to the Administration Console Welcome page showing you site ID and type.

Download Metadata – You may download the metadata from your site as a file so that it can be uploaded into other sites that you trust, or you may just view the parameters of your site.

Manage Partners – Allows you to create or remove Partner Groups, to view the details of each Partner Group and Partners with which you have federations, to edit the details of each Group or Partner and remove and/or change the configuration.

Manage Federations – Allows you to see all of the users that are federated with your Partners. You can also perform a search with a single user name.

Manage Admins – Allows you to add and remove new administrators. Only available when running in Standalone mode.

View Server Audit Log – This page allows the administrator to view all the activities of each user.

View Admin Audit Log – This page allows the root administrator to view all the activities of each delegated administrator.

Change Password – Allows you to change the administration password. Only available when running in Standalone mode.

You can always get context-sensitive Help by clicking the circular question mark button on the upper right-hand corner.

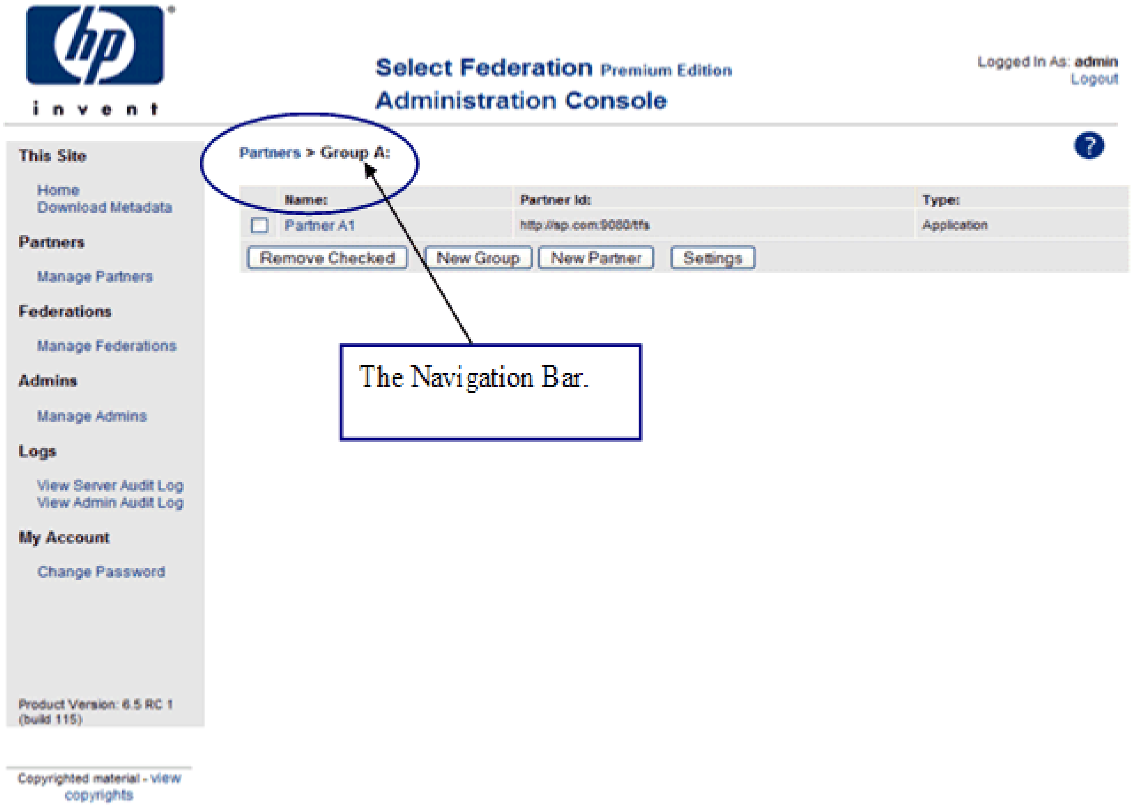
Navigation Bar

The Navigation Bar or “bread crumbs” (see Figure 27) shows the current Group or Partner that you are viewing. Using the Navigation Bar’s hyperlinks, you can use it to move back in the hierarchical group structure and to make sure that you are viewing the right Group or Partner.

The buttons **New Group, New Partner** and **Settings** operate on the last item shown in the Navigation Bar. The **Remove Checked** button operates on the checked items in the current group shown below the Navigation Bar.

Note that

Figure 27 Using the Navigation Bar



Select Federation Premium Edition
Administration Console

Logged In As: admin
Logout

Partners > Group A:

	Name:	Partner Id:	Type:
□	Partner A1	http://sp.com:9080/tfs	Application

Product Version: 6.5 RC 1 (build 115)

Copyrighted material - view copyrights

The Navigation Bar.

5 Setting Up Partnerships

Your federation is the set of web sites that you would like common users to have a seamless login experience. A federation is an open standards connection you create with a trusted site (your Trusted Partner) in order to get single sign-on, provisioning and privilege management without having to centralize all your data stores.

The basic advantage of federation is that your enterprise can quickly provide the benefits of a centralized identity management system to a larger set of users than is possible with a centralized identity management system. This larger set of users can be within your enterprise and/or from other organizations. They can also be customers, users of your extranet, users of your supply chain, or other external users that you share with your partner companies.

This chapter explains how to get the metadata of the Select Federation installation to your Partners. For more information on how to add Partners to your installation, see *Adding Partners to Your Installation.*

Benefits of Using Open Standard Federation Protocols

The two most popular open standard federation standards today are Security Assertion Markup Language (SAML) and Liberty Alliance. In order to create a federated link with your partner, you need to decide which open standard protocol you and your partner will use. You then exchange metadata with each other. To setup a federation, you first have to decide whether your site is going to be an Authority Site [also called a SAML Producer or Identity Provider (IDP) Site] or an Application Site [also called a SAML Consumer or Service Provider (SP) Site], or both an Authority and Application Site.

This typically means that for some set of users, you are hosting an application but are not authenticating those users. For another independent set of users, you are providing the authentication but allowing them to seamlessly use other application sites in your federation.

Once you have decided the role of your site, the first step is to download the metadata. HP OpenView Select Federation is unique in that it supports all of the popular open federation standards. This makes it easier to connect to multiple partners that may not have selected the same standards or conventional identity management solution.

Understanding the Impact of Metadata on Federation

Metadata in federation is a description of the Trusted Partner site with which you want to link. It is an on-line exact description of a site in a federation that describes the various URLs at which different site services (such as single sign-on, logout) are available, and its public-key certificates so that sites receiving messages from that site can confirm that those messages are signed by it and have not been tampered with.

In some federation standards such as Liberty 1.2 or SAML 2.0, the metadata specification is a conformant part of interoperability certification. In other specifications such as SAML 1.0, SAML 1.1, and Liberty 1.1, there is either just an informal metadata specification or just a convention in the community about how to define the metadata. In Select Federation, the management console enables an administrator to publish the site’s metadata as well as import other sites’ metadata.

Exchanging Metadata with Your Partners

To add Trusted Partner sites to your federation, both you and your Trusted Partner need to upload each other’s the metadata. Metadata exchange is mutual, so you need to ensure that the other site has added your metadata to its federation. The sections that follow describe how you can forward relevant data to your partner. For details on how to use metadata forwarded to you from a partner, see *Adding Partners*.

You can download the metadata into a metadata file and send this file to your Trusted Partner, or send the partner the information for manual entry.

You will need to know the protocol and protocol version that the Trusted Partner site is capable of, i.e. you need to select the type of federation you would like to setup:

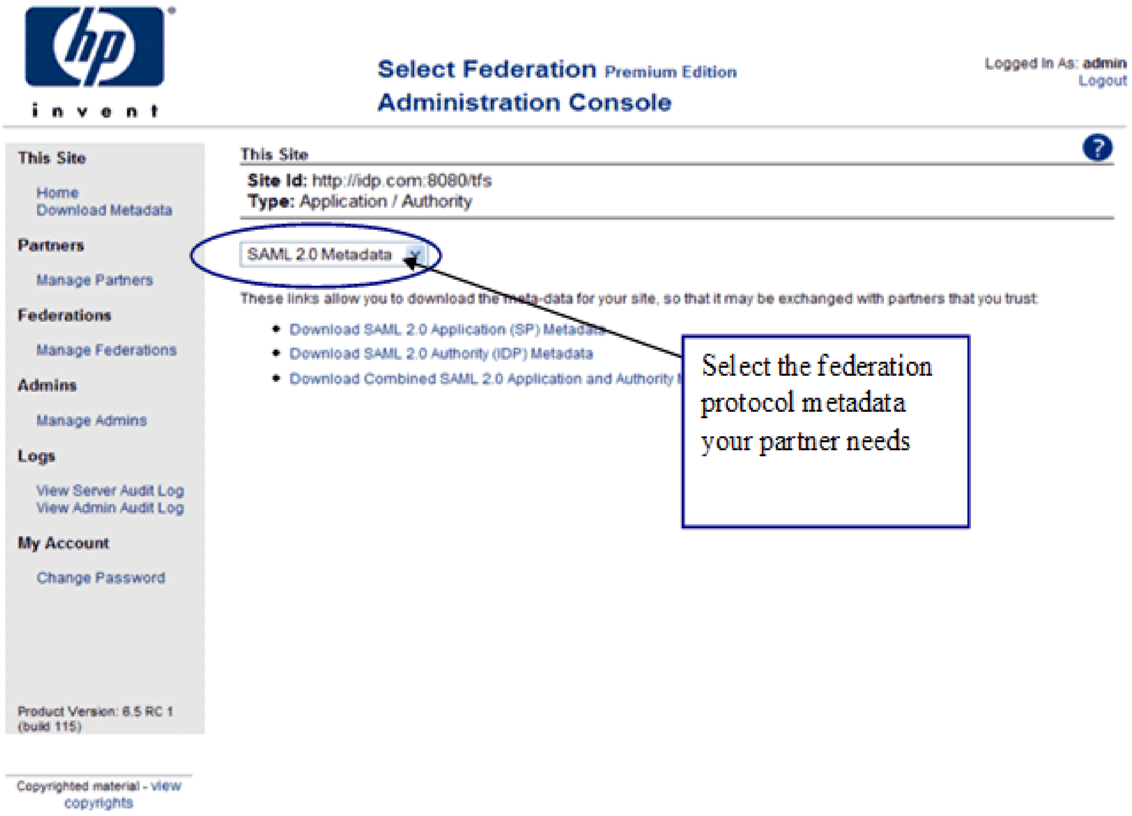
- For SAML 2.0, see *Downloading Your Site’s Metadata for a SAML 2.0 Federation*
- For SAML 1.1, see *Downloading your Site’s Metadata for a SAML 1.0 or SAML 1.1*
- For SAML 1.0, see *Downloading your Site’s Metadata for a SAML 1.0 or SAML 1.1*
- For Liberty ID-FF 1.2, see *Downloading Your Site’s Metadata for a Liberty ID-FF 1.1 or ID-FF 1.2 Federation*
- For Liberty ID-FF 1.1, see *Downloading Your Site’s Metadata for a Liberty ID-FF 1.1 or ID-FF 1.2 Federation*

Sending Your Metadata to Your Trusted Partner

HP OpenView Select Federation has simplified the process of obtaining your metadata for all the popular federation protocols. With one click, you can download your site information into any of the needed formats. Alternatively, if your partner prefers the information in text format, all information is readily available on the web page so that you can cut and paste the text.

To download the metadata, simply click on the **Download Metadata** link in the Menu Sidebar (left pane of the Administrator Console). You will be directed to a web page that looks like the one in Figure 28. This page allows you to download the metadata in the protocol format that your partner needs, and shows you the details of your site in the selected protocol.

Figure 28 Download your metadata to send to your partner



Site Id: http://idp.com:8080/tfs
Type: Application / Authority

SAML 2.0 Metadata

These links allow you to download the meta-data for your site, so that it may be exchanged with partners that you trust:

- Download SAML 2.0 Application (SP) Metadata
- Download SAML 2.0 Authority (IDP) Metadata
- Download Combined SAML 2.0 Application and Authority M

Select the federation protocol metadata your partner needs

Downloading Your Site's Metadata for a SAML 2.0 Federation

HP OpenView Select Federation uses metadata exchange with your Trusted Partner in order to setup the SAML federation. You start by creating your metadata file that will be sent to your Trusted Partner:

1. Click **Download Metadata** under the Admin Tasks side bar.
2. Select the SAML 2.0 protocol.
3. Do one of the following:
   - If your site will be the SAML Consumer or Application Site, click **Download SAML 2.0 Application (SP) Metadata**.
   - If your site will be the SAML Producer or Authority Site, click **Download SAML 2.0 Authority (IDP) Metadata**.
   - To describe both the Authority Site and Application Site one metadata file, click **Download Combined SAML 2.0 Application and Authority Metadata**.
4. Send this file to your partner so that they can upload it into their Select Federation or Trustgenix IdentityBridge™ software. Follow instructions in the next section to upload your partner's metadata file.

Downloading your Site's Metadata for a SAML 1.0 or SAML 1.1

Federation software from other vendors that does not support SAML 2.0 typically does not recognize SAML 1.0 or 1.1. metadata. Only SAML2.0 specified a format for metadata for SAML protocols. Earlier versions of HP OpenView Select Federation (and Trustgenix IdentityBridge™) supported a proprietary format for SAML 1.0 and 1.1. metadata that is still supported in HP OpenView Select Federation 6.5.

The SAML 1.X metadata format is specified by Oasis (see `http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security`). This format is based on the SAML 2.0 metadata specification.

You start by creating your metadata file that will be sent to your Trusted Partner:

1 Click **Download Metadata** under the Admin Tasks side bar.

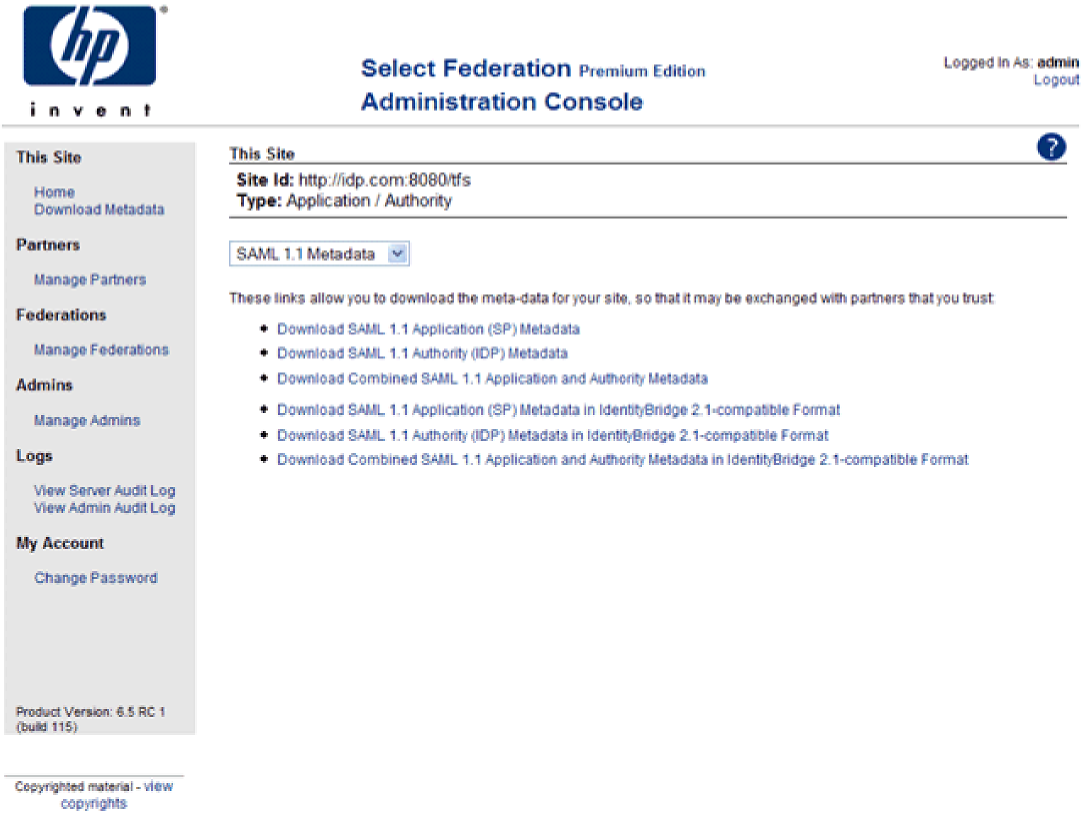
2 Select the SAML protocol that you and your partner have agreed to use, either SAML 1.0 or SAML 1.1.

3 Do one of the following:

- If your site will be the SAML Consumer or Application Site, click **Download SAML 1.X Application (SP) Metadata**.
- If your site will be the SAML Producer or Authority Site, click **Download SAML 1.X Authority (IDP) Metadata**.
- If your site will be both an Application and Authority Site, click **Download Combined SAML 1.X Application and Authority Metadata**.

If your Partner is using HP OpenView Select Federation 6.0 or Trustgenix IdentityBridge™ 2.1, you can choose to download the metadata in **IdentityBridge™ 2.1 compatible format** for an Application, Authority or both Application and authority Sites. See Figure 29.

Figure 29 Downloading your site’s metadata for SAML 1.X



This Site

Site Id: http://idp.com:8080/tfs
Type: Application / Authority

SAML 1.1 Metadata

These links allow you to download the meta-data for your site, so that it may be exchanged with partners that you trust

- Download SAML 1.1 Application (SP) Metadata
- Download SAML 1.1 Authority (IDP) Metadata
- Download Combined SAML 1.1 Application and Authority Metadata
- Download SAML 1.1 Application (SP) Metadata in IdentityBridge 2.1-compatible Format
- Download SAML 1.1 Authority (IDP) Metadata in IdentityBridge 2.1-compatible Format
- Download Combined SAML 1.1 Application and Authority Metadata in IdentityBridge 2.1-compatible Format

4 Send this file to your partner so that they can upload it into their HP OpenView Select Federation or Trustgenix IdentityBridge™ software. Follow instructions in the next section to upload your partner’s metadata file.

Downloading Your Site’s Metadata for a Liberty ID-FF 1.1 or ID-FF 1.2 Federation

You start by creating your Liberty ID-FF 1.1 or ID-FF 1.2 metadata file that will be sent to your trusted partner:

1 Click **Download Metadata** under the Admin Tasks side bar.

2 Select the Liberty protocol that you and your partner have agreed to use, either Liberty ID-FF 1.1 or ID-FF 1.2. If your partner is also using Select Federation, it may be desirable to choose Liberty 1.2. However, all protocols will work between two instances of Select Federation.

3 Do one of the following:

- If your site will be the Authority Site, click **Download Liberty 1.X Authority (IDP) Metadata**.
- If your site will be the Application Site, click **Download Liberty 1.X Application (SP) Metadata**.
- To describe both the Authority Site and Application Site in one metadata file, click **Download Combined Liberty 1.2 Application and Authority Metadata**.

4 Send this file to your partner so that they can upload it into their Liberty Certified Compliant federation software. Follow instructions in the next section to upload your partner's metadata file.

Metadata URLs

The metadata URL for your installation is its "ProviderId", with a value of

```
https://<site-base-URL>/tfs
```

Note that the metadata format under this URL can be specified by the `defaultMetadata` system configuration entry, which can have one of the following values:

- `liberty12`
- `liberty11idp`
- `liberty11sp`
- `saml10`
- `saml11`
- `saml20`

The default value is `saml20`.

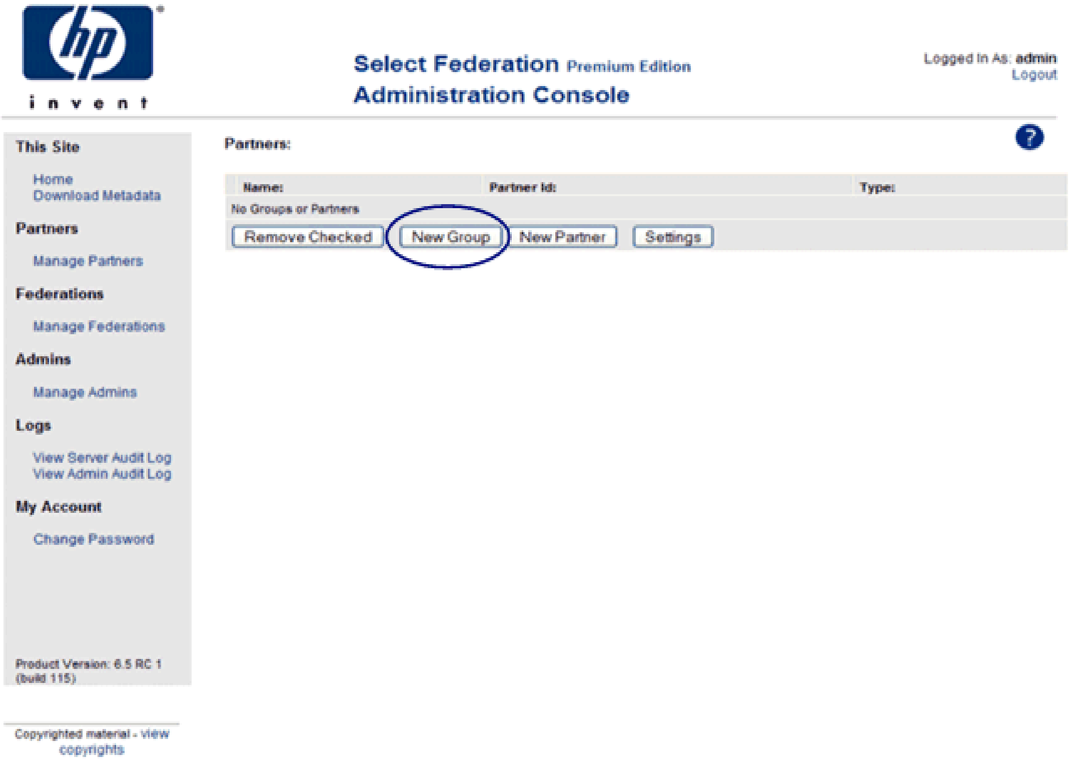
6 Adding Partners to Your Installation

Adding Groups

In HP OpenView Select Federation it is possible to create Groups for your various Partners. This gives you the benefit of better organization between different types of Partners and it will also make Partner configuration easier, since you can make the Partner inherit its configuration from the parent group. You should note that the metadata is always partner-specific; Groups do not have metadata of their own.

1 First, click **Manage Partners** on the Admin Tasks side bar and you will be directed to a web page that looks like the one in Figure 30.

Figure 30 Adding groups



Name:	Partner Id:	Type:
No Groups or Partners		

2 Click on **New Group** and give a name for your Group in the Group Name field. Click **Create** to finish. You will automatically be directed to a new web page showing you the contents of the Group you just created.

You can create subgroups easily by navigating to the Group of your choice and performing Step 2 again.

Adding Partners

To add Partners to your federation, you need to have the metadata for those Partners. Metadata exchange is mutual, so you need to ensure that the other Partner has added your metadata to its federation. For more information on metadata, see *Understanding the Impact of Metadata on Federation*.

There are two ways to obtain data from your partners:

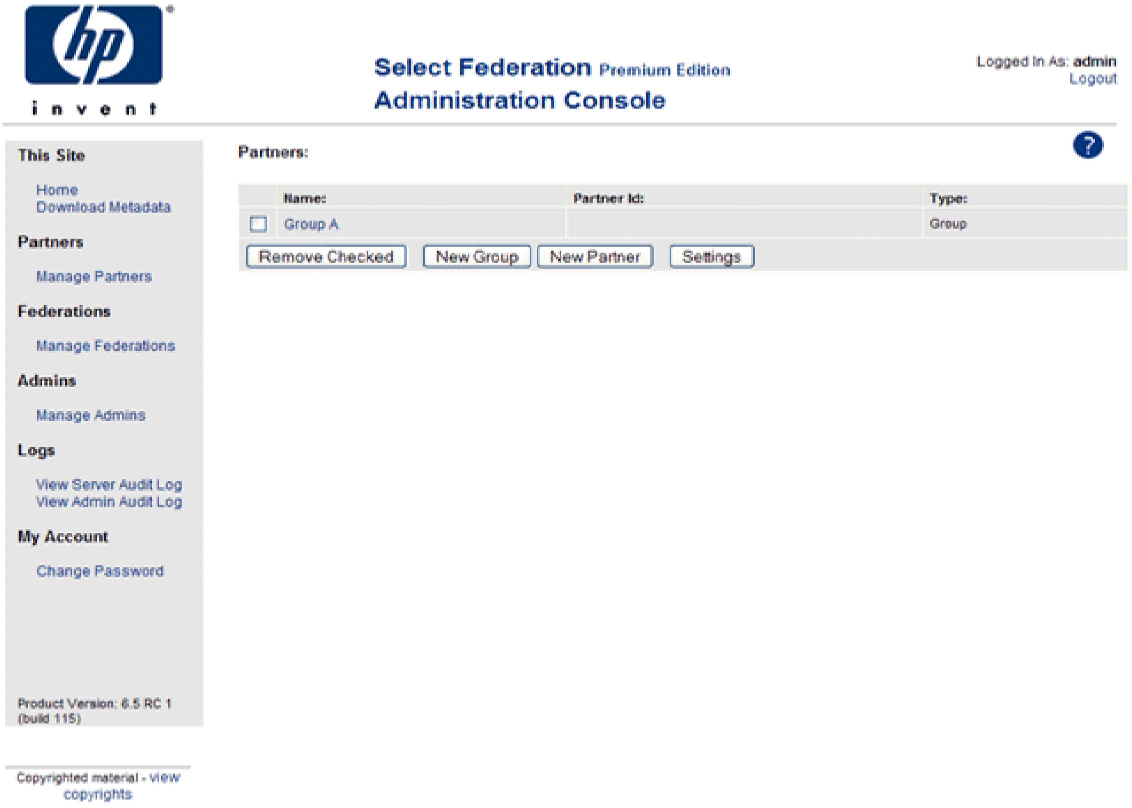
1. Download the Partner's metadata from a well-known URL.
2. Obtain the metadata securely from the administrator of the Partner.
3. If a metadata file or download is NOT available, see *My Partner is using SAML 1.X and metadata is NOT available as a file or a download.*

HP OpenView Select Federation can detect the protocol used by the Partner from the metadata provided by that Partner. However it is recommended to obtain knowledge about and agreement upon the protocol used for federation.

Adding a Partner for which metadata is available

To create the new federation, you will need your partner's metadata file so that you can upload this information into your Select Federation. Once you have your Partner's metadata file, click **Manage Partners** on the Admin Tasks side bar and you will be directed to a web page that looks like the one in Figure 31.

Figure 31 Adding a new Partner (part 1)



	Name:	Partner Id:	Type:
□	Group A		Group

1 Navigate to the Group where you want to create the Partner by clicking the name of the group. Click **New Partner** and a new page opens (see Figure 32). Select a name for your Trusted Partner site. In the **Partner Name** field, you can assign any “friendly name” to describe your partner’s site on your HP administration console. Enter the **Partner Name** as you would like it to appear in your system.

➤ You must enter data into this field.

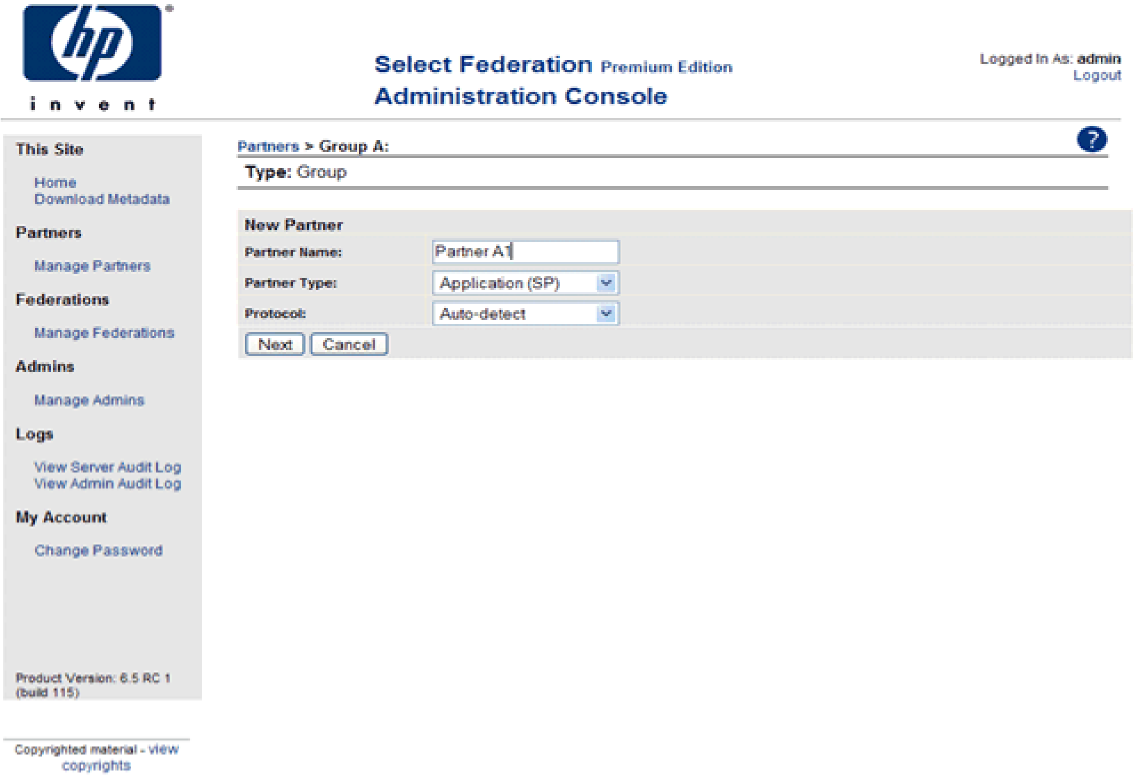
➤ This name is also visible to the end users.

2 Select the role of your Partner under the **Partner Type** – either an Application, Authority Site, or both.

- If your site is an authority site or Identity Provider, then your Partner is the application site or the Service Provider. **Select Application (SP)** as the Site Type for the Partner you are adding.
- If your site is an application site or Service Provider, then specify **Authority (IDP)** as the Site Type for the Partner you are adding.
- To import both authority site and application site data in the same metadata file, select **Application/Authority (SP/IDP)** for the Partner you are adding.

3 In the **Protocol** field, select **Auto-detect** and click **Next** and you will be direct to a next web page (Figure 33). Clicking **Cancel** will cancel the creation of a new Partner.

Figure 32 Adding a new Partner (part 2)



Select Federation Premium Edition
Administration Console

Logged In As: admin

Partners > Group A:

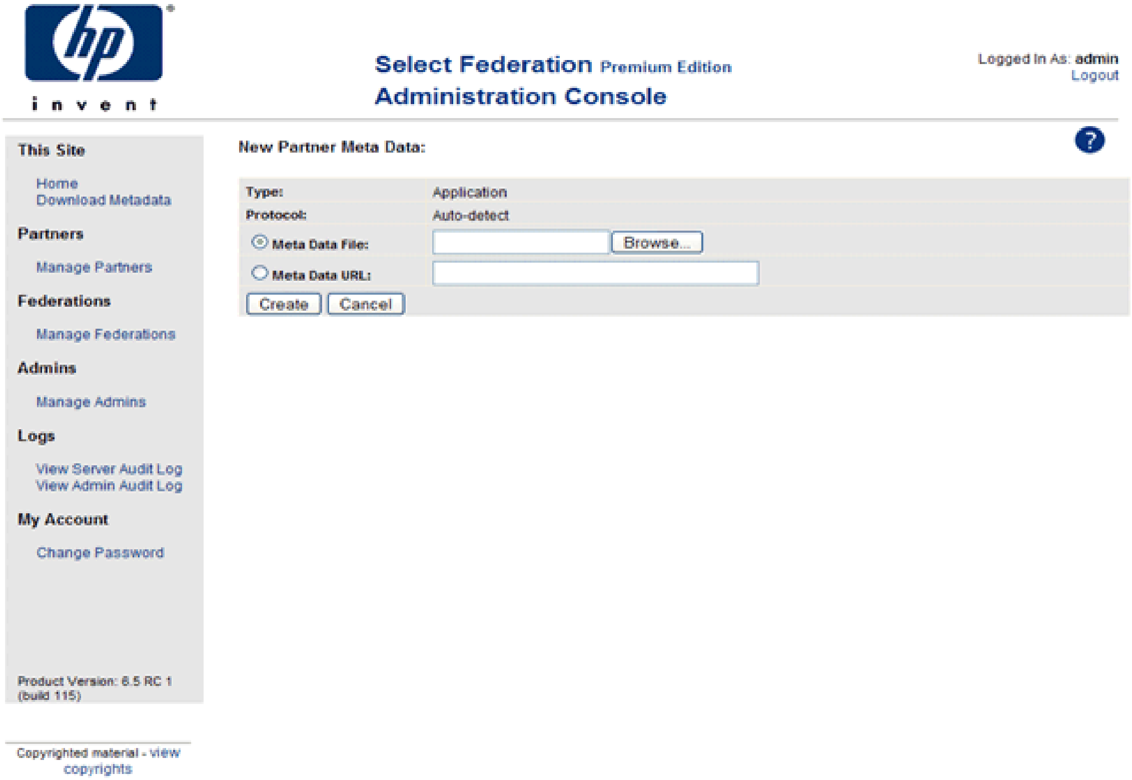
Type: Group

New Partner

Partner Name:	Partner A1
Partner Type:	Application (SP)
Protocol:	Auto-detect

Product Version: 6.5 RC 1 (build 115)

Figure 33 Setup new federation, upload your Partner’s metadata



New Partner Meta Data:

Type: Application

Protocol: Auto-detect

● Meta Data File: [   ] Browse...

○ Meta Data URL: [   ]

Create Cancel

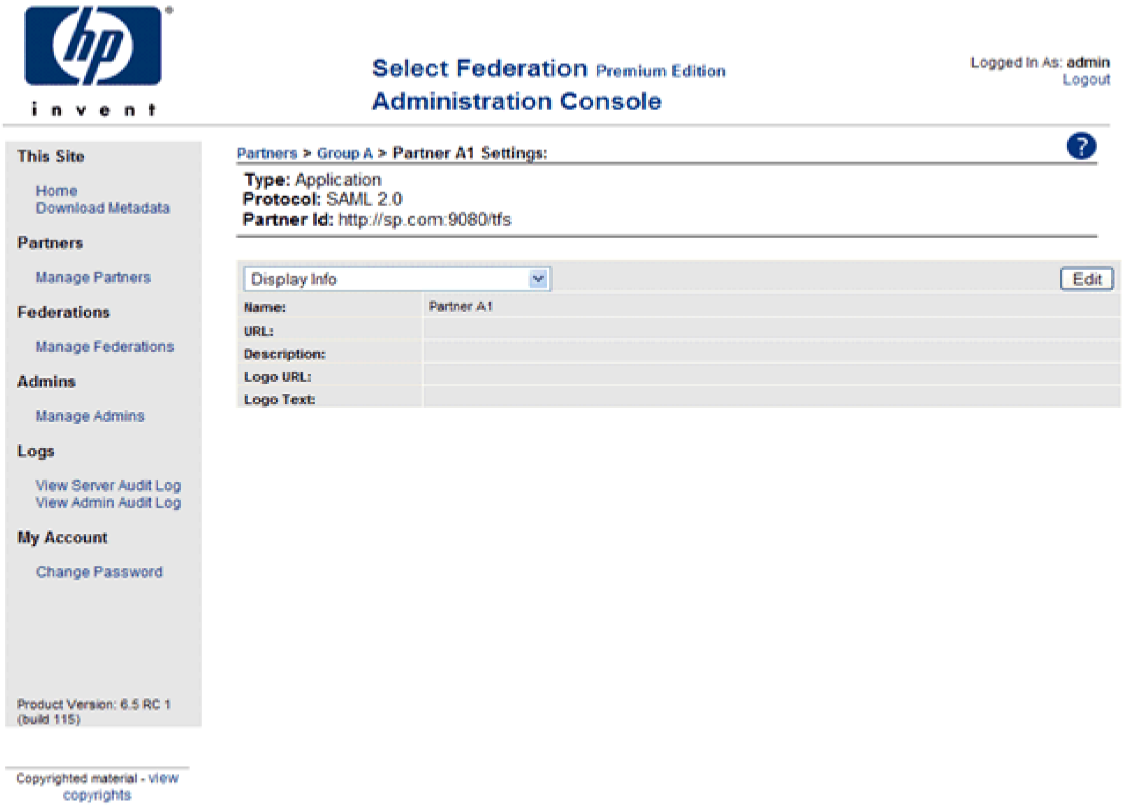
4 You can either upload your Partner’s metadata file or get the information from a URL.

- **Metadata File**: Enter or browse to find the full path of the metadata file that you received from your partner.
- **Metadata URL**: Enter the URL where the metadata information from your partner is stored.

5 Click **Create** to complete the creation of your federation link. Clicking **Cancel** will cancel the creation of a new Partner.

You will see a screen that shows the newly added Partner in the federation. To edit the details of the new Partner, click **Edit**. See Figure 34.

Figure 34 Newly added Partner



Type: Application
Protocol: SAML 2.0
Partner Id: http://sp.com:9080/tfs

Name:	Partner A1
URL:	
Description:	
Logo URL:	
Logo Text:	

The **Name** field is mandatory, but the rest of the text fields are optional, however, filling in these optional fields help the look-and-feel of the applications that process your federation information. These optional fields allow you to import your Partner's logo and link directly to your Partner's web page.

The **URL** is the default application that the Partner makes available for single sign-on to users of your installation. This is mainly useful if you want to add the a single-sing-on link to that partners application to a portal (see also *Enabling Applications*).

This URL is NOT a link to the Partner's ProviderId.

Enter a one-line **Description** of the Partner site to which you are connecting. This is optional and can be left blank.

Logo URL is the logo that appears on your portal and represents the logo of the federation link you created. It can be your Partner's logo. This field is optional.

Logo Text is the text that appears in the bubble when you put your mouse over the Logo URL. This field is optional.

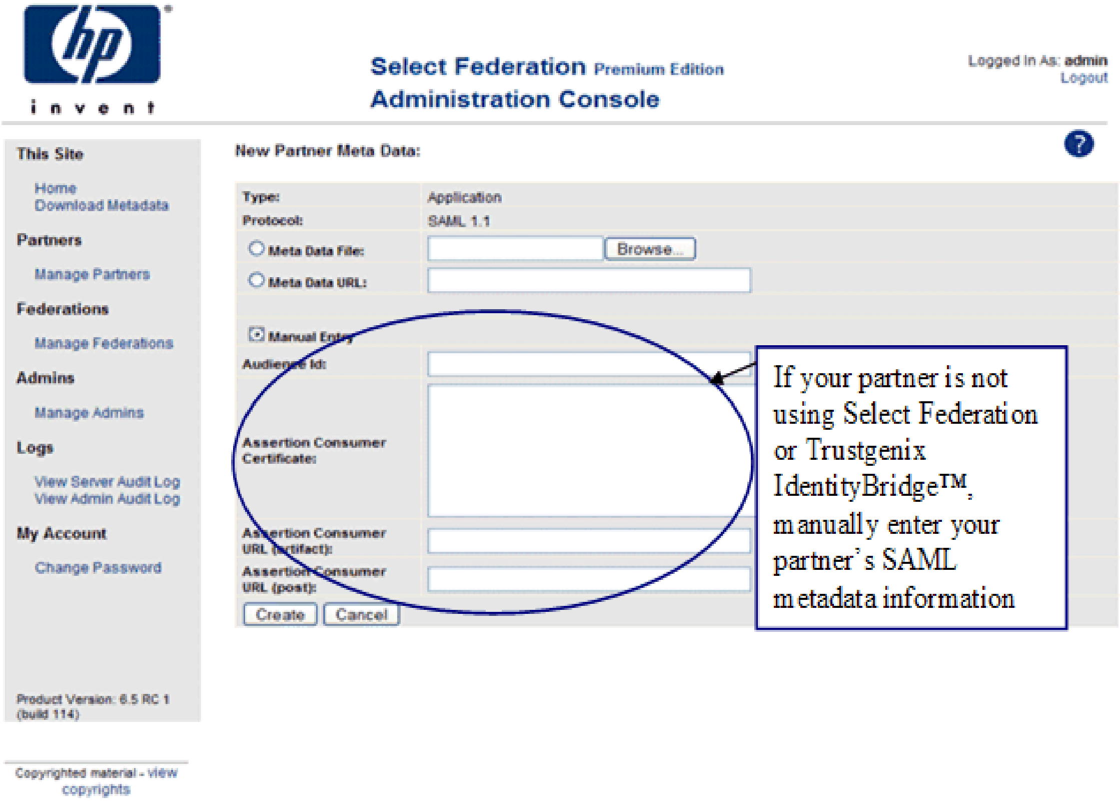
6 Click **Save** to save the changes you have made. Clicking **Cancel** will cancel the changes.

My Partner is using SAML 1.X and metadata is NOT available as a file or a download

If your Trusted Partner uses SAML 1.0 or SAML 1.1, it is possible that no metadata file or a URL link is available. Instead, you will need to select **Manual Entry** as shown in Figure 35, and type in the SAML parameters for your Partner's site.

If your Trusted Partner is not using HP OpenView Select Federation 6.0 or Trustgenix IdentityBridge™ 2.1, your partner can make metadata available in the proprietary IdentityBridge 2.1 format and you can follow the procedure in the previous section.

Figure 35 Uploading or entering your Partner's metadata for a new SAML federation



New Partner Meta Data:

Type: Application
Protocol: SAML 1.1
○ Meta Data File:
○ Meta Data URL:
● Manual Entry
Audience Id:
Assertion Consumer Certificate:
Assertion Consumer URL (artifact):
Assertion Consumer URL (post):

If your partner is not using Select Federation or Trustgenix IdentityBridge™, manually enter your partner's SAML metadata information

The parameters needed when adding an authority are:

- **Issuer Id**: The identifier that the partner site includes in the issuer field in the assertions that it generates.
- **Assertion Issuer Certificate**: This certificate is required if the partner site signs the assertions that it issues, but not otherwise.
- **Source Id**: A 20-byte hex encoded or base64 encoded binary value placed in artifacts that the partner site generates, when using the artifact profile. It is not something that can be chosen by the administrator adding the partner.
- **Artifact Retrieval SOAP Endpoint**: This is the location of the SAML responder's SOAP service used for artifact pickup.
- **Attribute Authority SOAP Endpoint:** This is the URL where your site will invoke the partner's attribute authority service over SOAP for obtaining user attributes.
- **Intersite Transfer URL:** This field is optional. This is the SAML Inter-site Transfer Service URL used to navigate to your partner site in the federation.

The parameters needed when adding an application are:

- **Audience Id:** The identifier for the Partner site.
- **Assertion Consumer Certificate:** This certificate is used by the Assertion Consumer to authenticate to the SAML Producer for picking up the SAML Assertion Artifact and it is required if the partner site signs the authentication requests that it issues, but not otherwise.
- **Assertion Consumer URL** (artifact)**:** This is the URL to which your site sends assertion artifacts.
- **Assertion Consumer URL** (post): This is the URL to which the user is redirected from your site to the SAML consumer site when using the SAML POST profile.

Click **Create** to complete the creation of your federation link. You will see a screen that shows the newly added site in the federation. Clicking **Cancel** will cancel the creation of a new site. To edit the details of the new partner site, click **Edit**.

Optional Fields

The name field is mandatory, but the rest of the text-fields are optional, however, filling in these optional fields help the look-and-feel of the applications that process your federation information. These optional fields allow you to import your Partner's logo and link directly to your Partner's web page.

- The **URL** is your Partner's URL that users may use as a homepage, if this site acts as an IDP portal.
- Enter a one-line **Description** of the Partner Site to which you are connecting. This is optional and can be left blank.
- **Logo URL** is the logo that appears on your portal and represents the logo of the federation link you created. It can be your Partner's logo. This field is optional.
- **Logo Text** is the text that appears in the bubble when you put your mouse over the Logo URL. This field is optional.

Click **Save** to save the changes you have made. Clicking **Cancel** will cancel the changes.

Removing Partners and Groups from Your Installation

Follow these steps to remove an existing Partner or Group:

1. Click **Manage Partners** on the Menu sidebar to get a list of the existing federations.
2. Navigate to the Partner that you want to remove by clicking the name of the group that your Partner belongs to (if you have created a group for your Partner).
3. Check the box next to the name of the Partner that you wish to remove.
4. Click **Remove Checked**. A confirmation dialog opens up asking if you really wish to remove existing federations. If this is correct, click **OK**.

7 Editing Partner Settings

HP OpenView Select Federation allows you to make changes to all the parameters of your existing federations, including your:

- **Display Info**: This describes how your Partner appears in your system. For details, see *Configuring the Display Information*.
- **Federation Policy**: These are the rules that you and your partner agreed to use in communicating between your sites. For details, see *Configuring the Federation Policy*.
- **Attribute policy**: Select Federation allows you to configure and change the user profile attribute exchange. For details, see *Configuring the Attribute Policy*.
- **Protocol Policy**: These are the actual protocol parameters, also known as metadata, consisting of URLs for various protocol services, certificates, etc. For details, see *Configuring the Protocol Policy and Metadata*.

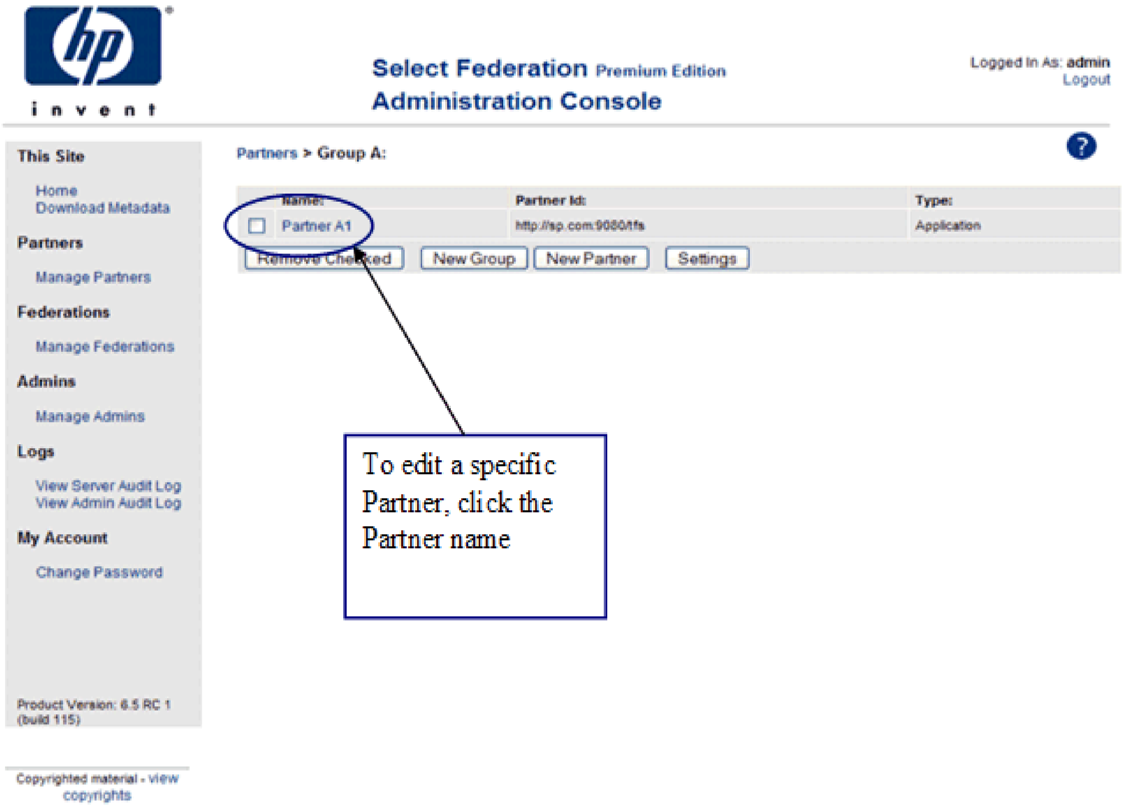
Changing Settings for a Partner

To edit on any of the federations you have in your system, click **Manage Partners** on the Admin Tasks side bar. Select Federation's **Manage Partners** page allows you to:

- View the details of each Partner with which you have a federation
- Edit the details of each site
- Remove, and/or change the configuration

Click the **Name** of the site with which you have a federation that you wish to edit (see Figure 36):

Figure 36 Selecting a Partner to edit



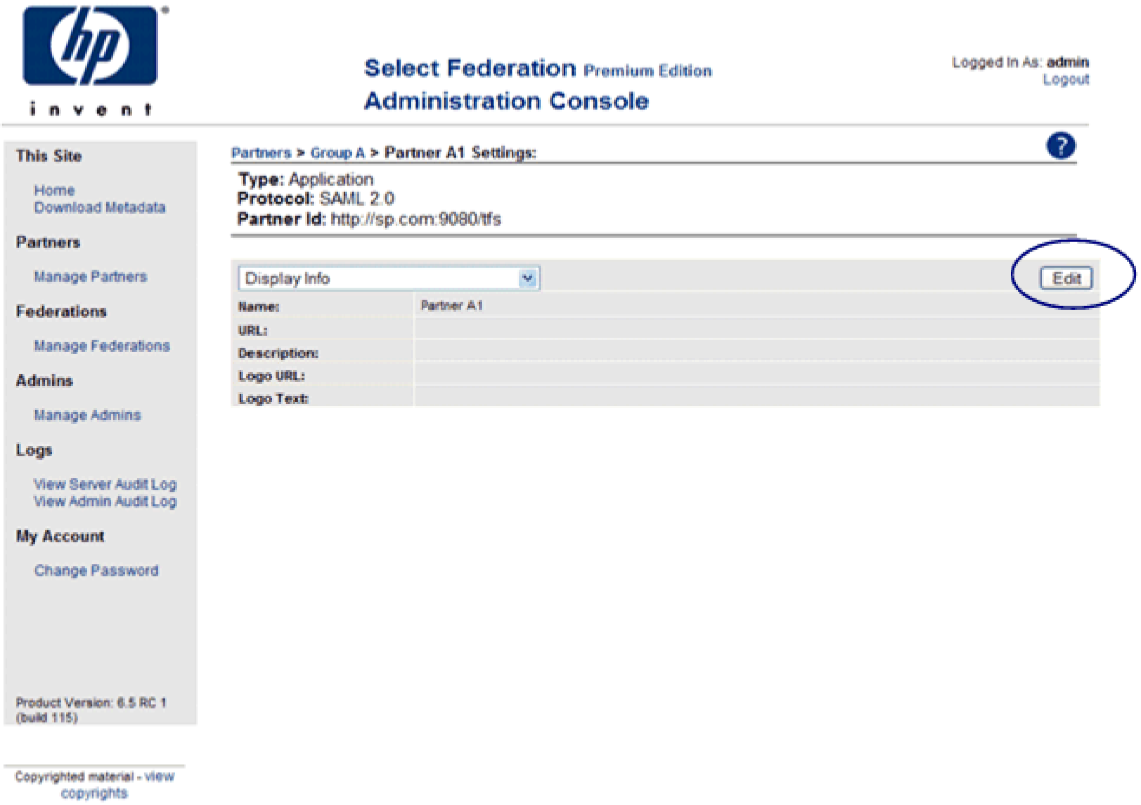
Name:	Partner Id:	Type:
□ Partner A1	http://sp.com:9080/tfs	Application

To edit a specific Partner, click the Partner name

You will be directed a web page (as shown in Figure 37) that has the basic information related to this Partner:

- **Type** is either an Authority/identity provider site or an Application/service provider site.
- **Protocol** is the open standards protocol that this federation used. It can be SAML 2.0, SAML 1.1, SAML 1.0, Liberty 1.2 or Liberty 1.1.
- **Partner Id** is the URL for the Trusted site with which you have a federation.

Figure 37 To edit Partner details, click the Edit button



Partners > Group A > Partner A1 Settings:

Type: Application
Protocol: SAML 2.0
Partner Id: http://sp.com:9080/tfs

Display Info

Name:	Partner A1
URL:	
Description:	
Logo URL:	
Logo Text:	

Configuring the Display Information

Display Information is the data that determine how your Partner appears on your federation web page. This includes your Partner’s name, URL, and/or logo.

To change, click **Edit** next to Display Info as shown in Figure 37.

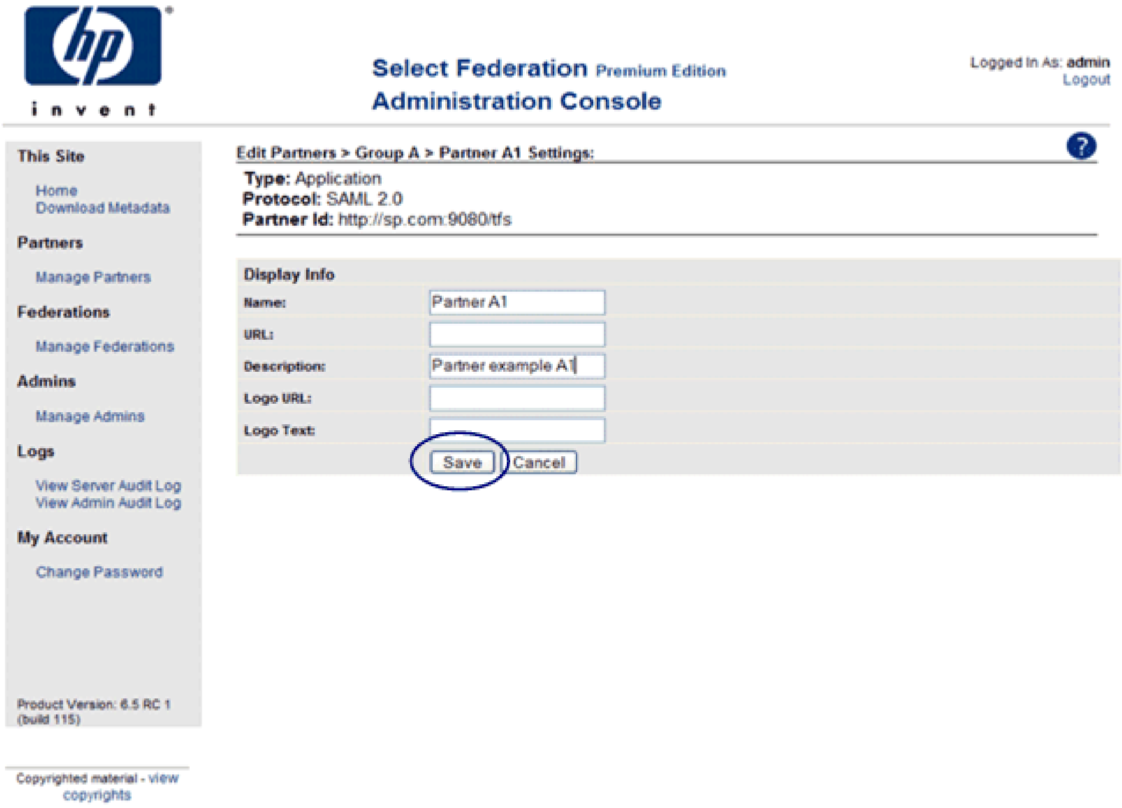
- **Name** is your Partner’s Site Name, as you would like it to appear in your system.
- The **URL** is the URL to your Partner’s application that you should be directed to when you use the federated link.

  ➤ This URL is NOT a link to the Partner’s ProviderId.

- Enter a one-line **Description** of the Partner to which you are connecting.
- **Logo URL** is the Logo that will appear on your portal which represents the logo of the federation link you have created. It can be your Partner’s logo.
- **Logo Text** is the text that appears in the bubble when you put your mouse over the Logo URL.

The web page that follows (as shown in Figure 38) allows you to change the Name, URL, Description, Logo URL, and Logo Text that you use to distinguish your Partner. The screen will be populated with the current Partner information. You can fill in any changes to the Partner information that you wish and click **Save**.

Figure 38 After editing Partner details, click Save



Edit Partners > Group A > Partner A1 Settings:

Type: Application
Protocol: SAML 2.0
Partner Id: http://sp.com:9080/tfs

Display Info

Name:	Partner A1
URL:	
Description:	Partner example A1
Logo URL:	
Logo Text:	

Configuring the Federation Policy

The federation policy is the set of rules that both you and your Partner agreed to use in communicating between the sites. These rules comprised of:

- **Name Federation** or the form of the user name
- **User Consent**

Name Federation

HP OpenView Select Federation allows users to connect to Partner web sites in three ways: using the user's local name which has identifiable user information, using a unique identifier that does not reveal the users' identities to outside sites, or total anonymity. This is accomplished through:

- **Local Names** are the names (or identifiers) that the users are known by at the Identity Provider or Authority site. The Authority Site may also elect to pass some user information to the Service Provider. One Time Pseudonyms and Pseudonyms are generated and used in place of the Local Name.
- **Pseudonyms** are identifiers that are randomly generated to keep the user's local identity unknown to the Service Provider. However, unlike the One Time Pseudonym, each time the user goes to the Partner site, the same identifier is presented. The Service Provider or Application site will know that this user has been active at its site.

- **One Time Pseudonyms** are identifiers that are randomly generated each time the user accesses a Trusted site, providing the strongest privacy to users.

  If you are using the one-time pseudonym name federation policy, you will not be able to link accounts on an IDP / Authority to an existing account on an SP / Application. This is because the linked account at the SP will refer to a federated identifier that will never be repeated by the IDP, so a user navigating to the SP for a second time will not be recognized as a returning user.

User Consent

The first time a user goes to a new Trusted Partner Site, he has the option to consent to sending his federated name identifier to this Trusted Site. The type and level of user information that would be transmitted are determined by the Authority Site (or Identity Provider or SAML Producer). The administrator decides whether User Consent is **Required** or **Not Required**. To enable attribute consent, see *Configuring use of end user privacy policies (PE only).*

If your site is the Authority Site, you can edit the site federation policy for each Application Site in your federation. From the drop-down menu below **Partner Site Details**, select **Application Federation Policy** (as shown in Figure 37). You will be directed to a web page that shows the current entries in your Federation Policy.

To change your Federation Policy, click **Edit**, and you will be directed to a web page as shown in Figure 38.

Initially the Application Federation Policy is inherited from the parent Group where the Partner resides. You can either edit the parent Group's Application Federation Policy to affect all Partner's under the Group in the same way or override the Group Policy and edit the Partner's Policy by itself.

Check the Override checkbox if you want to edit your Partner's Application Federation Policy irrespective to the Group policy. Make the needed changes to each of the fields and click **Save**.

Configuring the Attribute Policy

Applications typically need attributes about the authenticated users. In a federated system, the most recent values for these user attributes are at the original source of the authentication, i.e. the Identity Provider or SAML Producer. The Profile Service is a module in Select Federation that allows you to transmit user attributes on every user authentication.

Introduction

Using the Liberty Profile Services (Personal Profile Service – ID-PP or Employee Profile Service – ID-EP) or the SAML Attribute Authority, Select Federation provides these user attributes to the application residing at the federated site, i.e. the Service Provider or SAML Consumer. You and your Partner will need to agree on the attributes to be exchanged.

An Application must be configured with the attributes it "requests" from its Authority partners whereas an Authority must be configured with the attributes it is "willing to consider for release" to its Application partners. The set of attributes to request or release is called an Attribute Policy. The remainder of the chapter explains how to configure Attribute Policies.

HP OpenView Select Federation has a built-in profile service that uses the system configuration to determine the sources of attribute information. This is explained in more detail in *Configuring Attributes*. An Application does not use the profile service of its own installation but requests attributes from its Authority partners. The release of profile attributes to applications can be subject to end user consent (see *Configuring Privacy Manager*).

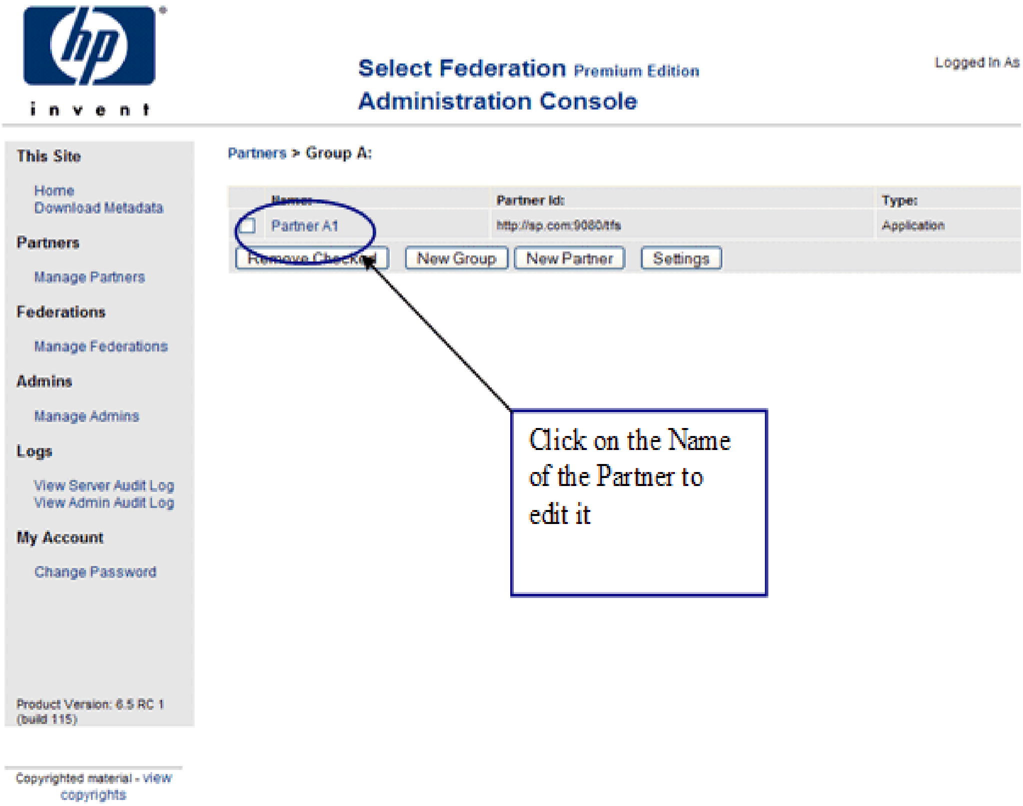
Configuring Your Attribute Policy

HP OpenView Select Federation allows you to configure and change the user profile attribute exchange for Groups and Partners. Partners can inherit their Application Attribute Policy from a Group if so desired. This can be helpful when many Partners share a similar configuration. To edit or set your profile attribute:

1. Click **Manage Partners** on the Menu side bar. You will be directed to a web page as shown in Figure 39.
2. Click the **Name** of the Group or Partner that you wish to edit. You will be directed to a web page as shown in Figure 40.
3. In the drop-down menu under the **Partner Details**, select **Application Attribute Policy**. You will be directed to a web page as shown in Figure 41 that delineates all the existing attribute policy parameters, if any, for this Liberty federation.

   ➤ Initially the Application Attribute Policy is inherited from the parent Group where the Partner resides. You can either edit the parent Group’s Application Attribute Policy to affect all Partner’s under the Group in the same way or override the Group Policy and edit the Partner’s Policy by itself.

Figure 39 Select the Partner that you wish to edit



Select Federation Premium Edition
Administration Console

Logged In As

Partners > Group A:

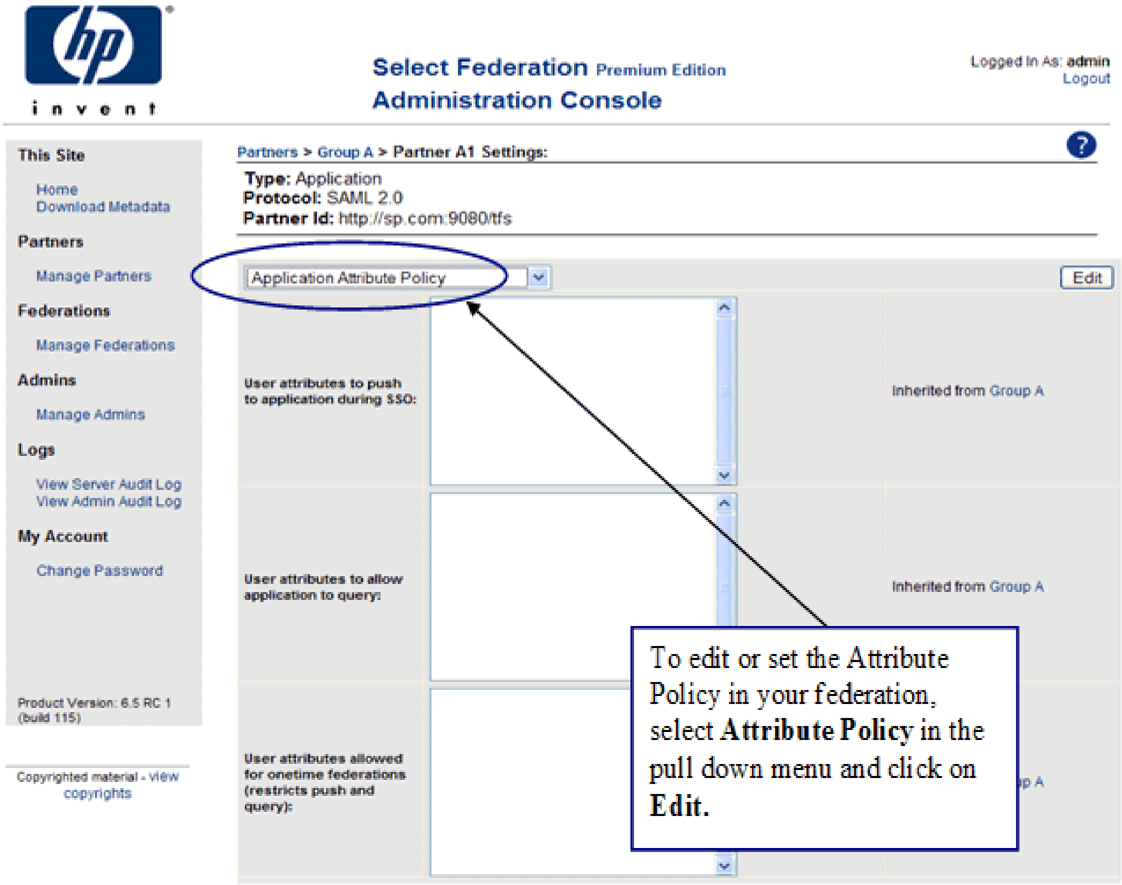
	Name:	Partner Id:	Type:
□	Partner A1	http://sp.com:9080/tfs	Application

Click on the Name of the Partner to edit it

Product Version: 6.5 RC 1 (build 115)

Copyrighted material - view copyrights

Figure 40 Edit the Application Attribute Policy in your federation



Type: Application
Protocol: SAML 2.0
Partner Id: http://sp.com:9080/tfs

User attributes to push to application during SSO: Inherited from Group A

User attributes to allow application to query: Inherited from Group A

User attributes allowed for onetime federations (restricts push and query): ...p A

To edit or set the Attribute Policy in your federation, select **Attribute Policy** in the pull down menu and click on **Edit.**

The attributes that may be conveyed at the time of single sign on from the Authority Partner (IDP or SAML Producer) to the Application Partner (SP or SAML Consumer) are given below.

Application Attribute Policy

User attributes to push to application during SSO: The attributes that are pushed from the Authority Partner to the Application Partner each time users log in to the application.

User attributes to allow application to query: The additional attributes that the Application Partner is allowed to pull from the Authority Partner. They are attributes that were not pushed by the Authority Partner in the initial sign on. The Application Partner queries the Liberty Profile Service or SAML Attribute Authority for this information.

➤ When using Liberty 1.2, the Profile Service is only available for the HP OpenView Select Federation Premium Edition. Therefore, the attribute query functionality will not have any effect in the Enterprise Edition.

User attributes allowed for one time federations (restricts push and query): If the Federation Policy is set for anonymous logins using the One Time Pseudonyms, you can set user attributes for the one-time logins, if desired.

Authority Attribute Policy

User attributes to obtain from authority on each login: Each time the user executes a transaction at the Application Partner this user information is retrieved from the Authority Partner.

Additional user attributes to obtain from authority on activation: The first time a new user accesses the Application Partner, these are the user attributes that the Application Partner needs from the Authority Partner to active the user account.

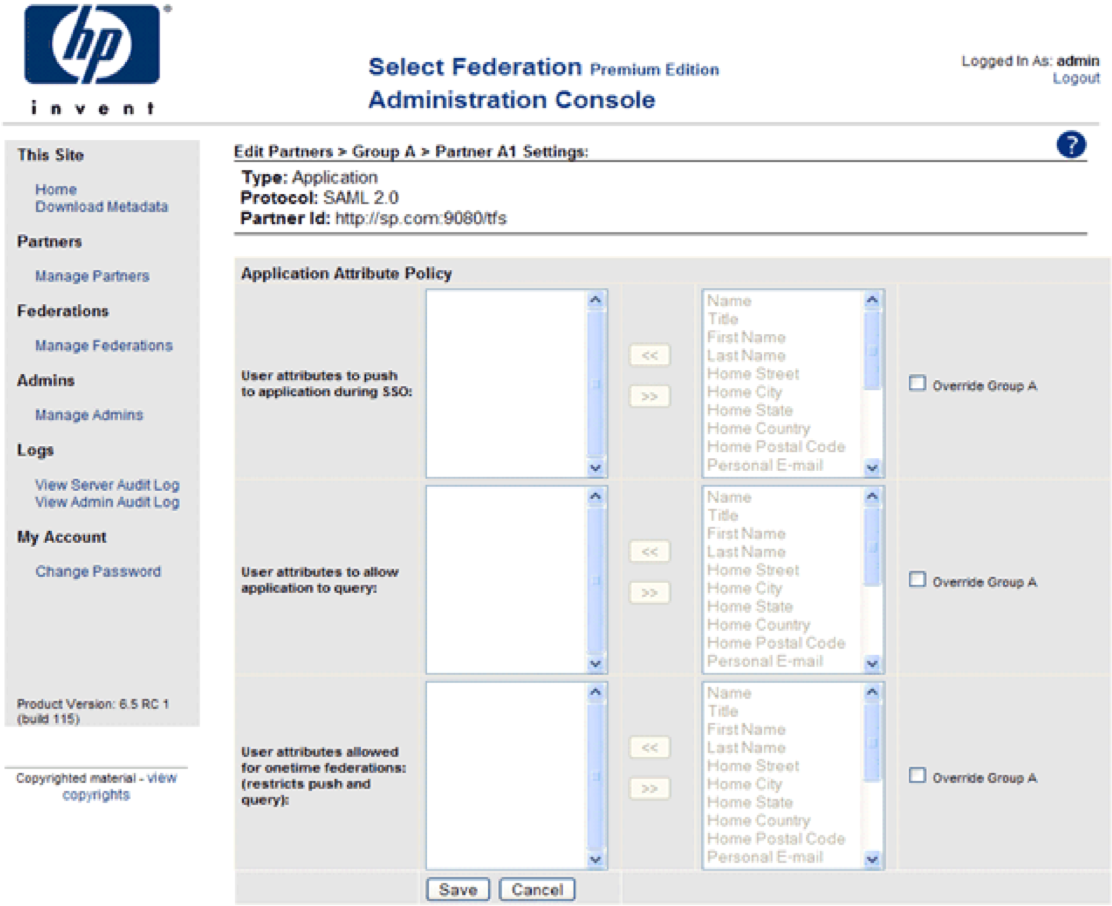
Setting Attribute Policies

1 To set or change your profile attribute policy, click **Edit.** You will be directed to a screen similar to the one shown in Figure 41. Check the **Override** checkbox if you want to edit your Partner's Application Attribute Policy irrespective to the Group policy.

2 Select the user attributes that you would like to pass for each login. If you wish to select more than one attribute in each category, you can use the **<Ctrl>** key on your keyboard to select multiple options, or the **<Shift>** key on your keyboard to select a range of options.

3 When you are done, click **Save**.

Figure 41 Editing your Attribute Policy



Edit Partners > Group A > Partner A1 Settings:

Type: Application
Protocol: SAML 2.0
Partner Id: http://sp.com:9080/tfs

Application Attribute Policy

User attributes to push to application during SSO:		<< >>	Name Title First Name Last Name Home Street Home City Home State Home Country Home Postal Code Personal E-mail	□ Override Group A
User attributes to allow application to query:		<< >>	Name Title First Name Last Name Home Street Home City Home State Home Country Home Postal Code Personal E-mail	□ Override Group A
User attributes allowed for onetime federations: (restricts push and query):		<< >>	Name Title First Name Last Name Home Street Home City Home State Home Country Home Postal Code Personal E-mail	□ Override Group A

Configuring the Protocol Policy and Metadata

HP OpenView Select Federation makes it relatively easy to make changes to your Partner's protocol policy and/or protocol metadata. Due to the differences between the Liberty and SAML specifications, the way to update existing federation links differs as explained in the following sections.

Changing your SAML Protocol parameters can be a two-step process if you need to make changes in both your Protocol Metadata and Protocol Policy. We recommend that you first update your Protocol Metadata, and then update your Protocol Policy.

Updating Your SAML Application Partner Protocol Metadata

Under partner details in the drop-down menu, select **Protocol Metadata**. You will be directed to a web page similar to the one in Figure 42 that delineates all the certificate information, protocol policy, and URLs that are needed for this SAML Partner.

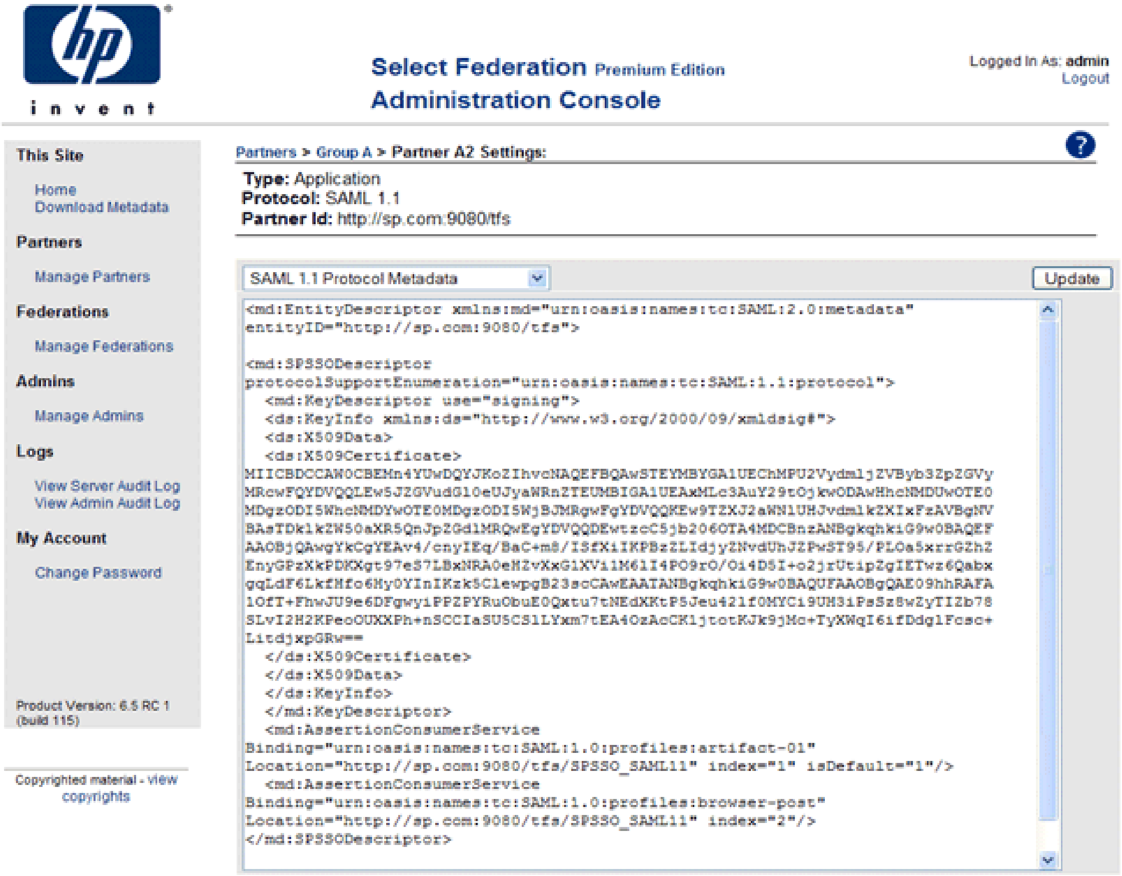
When you click **Update**, you will then be directed to a web page as shown in Figure 46 where you can update your Partner's SAML Consumer (Application Partner or SP) policy information.

If your Trusted Partner uses SAML 1.X, it is possible that no metadata file or a URL link is available. In this case you will need to enter the updated information manually.

For the Partner metadata, make any needed changes to the following:

- **Assertion Consumer Certificate**: The Assertion Consumer Certificate is the certificate used by the Assertion Consumer to authenticate to the SAML Producer for picking up the SAML Assertion Artifact.
- **Assertion Consumer URL** (artifact): The URL to which the user is redirected from your site to the SAML consumer site when using the SAML Artifact profile.
- **Assertion Consumer URL** (post): The URL to which the user is redirected from your site to the SAML consumer site when using the SAML POST profile.

Figure 42 To update a SAML Partner's protocol metadata, click Update



Type: Application
Protocol: SAML 1.1
Partner Id: http://sp.com:9080/tfs

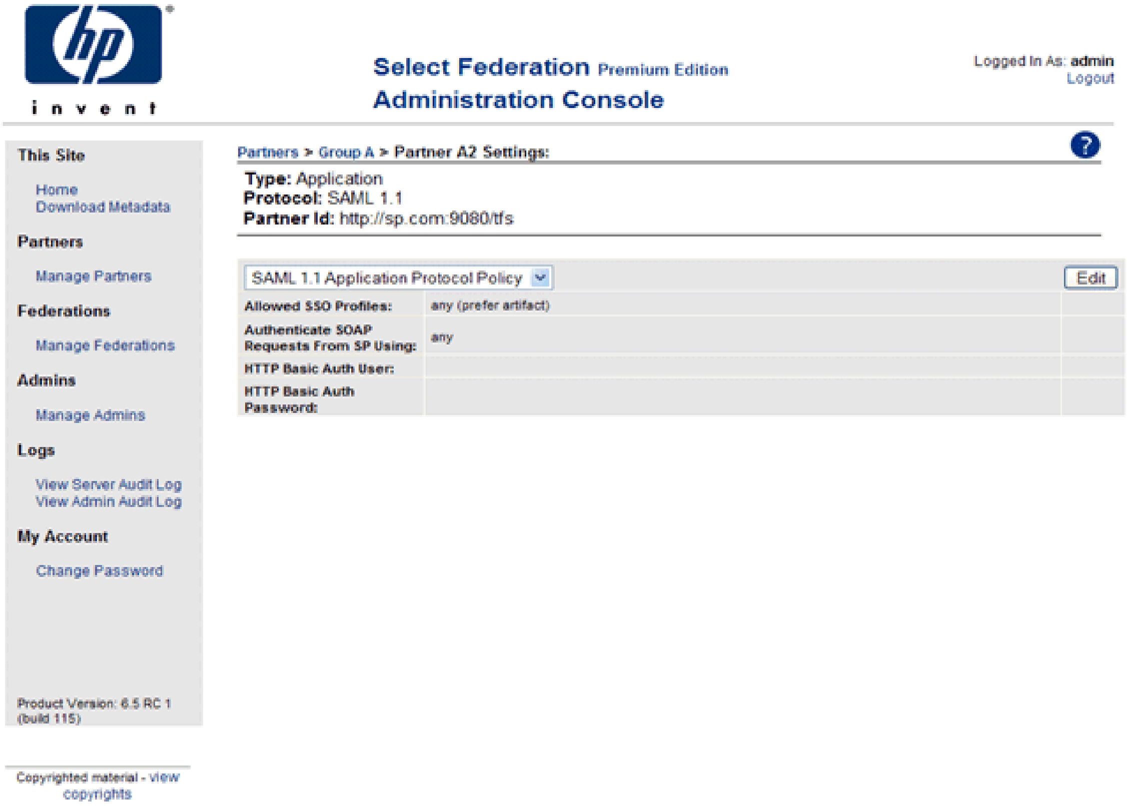
```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="http://sp.com:9080/tfs">

<md:SPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol">
  <md:KeyDescriptor use="signing">
  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:X509Data>
  <ds:X509Certificate>
MIICBDCCAW0CBEMn4YUwDQYJKoZIhvcNAQEFBQAwSTEYMBYGA1UEChMPU2VydmljZVByb3ZpZGVy
MRcwFQYDVQQLEw5JZGVudGl0eUJyaWRnZTEUMBIGA1UEAxMLc3AuY29tOjkwODAwHhcNMDUwOTE0
MDgzODI5WhcNMDYwOTE0MDgzODI5WjBJMRgwFgYDVQQKEw9TZXJ2aWN1UHJvdmlkZXIxFzAVBgNV
BAsTDk1kZW50aXR5QnJpZGdlMRQwEgYDVQQDEwtzcC5jb206OTA4MDCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEAv4/cnyIEq/BaC+m8/ISfXiIKPBzZLIdjyZNvdUhJZPwST95/PLOa5xrrGZhZ
EnyGPzXkPDKXgt97eS7LBxNRA0eMZvXxG1XVi1M61I4PO9rO/Oi4D5I+o2jrUtipZgIETwz6Qabx
gqLdF6LkfMfo6My0YInIKzk5ClewpgB23scCAwEAATANBgkqhkiG9w0BAQUFAAOBgQAE09hhRAFA
1OfT+FhwJU9e6DFgwyiPPZPYRuObuE0Qxtu7tNEdXKtP5Jeu421f0MYCi9UM3iPsSz8wZyTIZb78
SLvI2H2KPeoOUXXPh+nSCCIaSU5CS1LYxm7tEA4OzAcCK1jtotKJk9jMc+TyXWqI6ifDdglFcsc+
LitdjxpGRw==
  </ds:X509Certificate>
  </ds:X509Data>
  </ds:KeyInfo>
  </md:KeyDescriptor>
  <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:1.0:profiles:artifact-01"
Location="http://sp.com:9080/tfs/SPSSO_SAML11" index="1" isDefault="1"/>
  <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post"
Location="http://sp.com:9080/tfs/SPSSO_SAML11" index="2"/>
</md:SPSSODescriptor>
```

Do not forget to save your changes by clicking **Update**.

Editing SAML Application Partner Protocol Policy

Select **Protocol Policy** under partner details in the drop-down menu as shown in Figure 43. To make changes, click **Edit** and you will be directed to another web page as shown in Figure 44.

Figure 43 To update a SAML Partner’s protocol policy for an Application (SP) Partner



Partners > Group A > Partner A2 Settings:

Type: Application
Protocol: SAML 1.1
Partner Id: http://sp.com:9080/tfs

SAML 1.1 Application Protocol Policy

Allowed SSO Profiles:	any (prefer artifact)
Authenticate SOAP Requests From SP Using:	any
HTTP Basic Auth User:	
HTTP Basic Auth Password:	

Product Version: 6.5 RC 1 (build 115)

Set the Allowed SSO Profile in Your SAML SP Policy

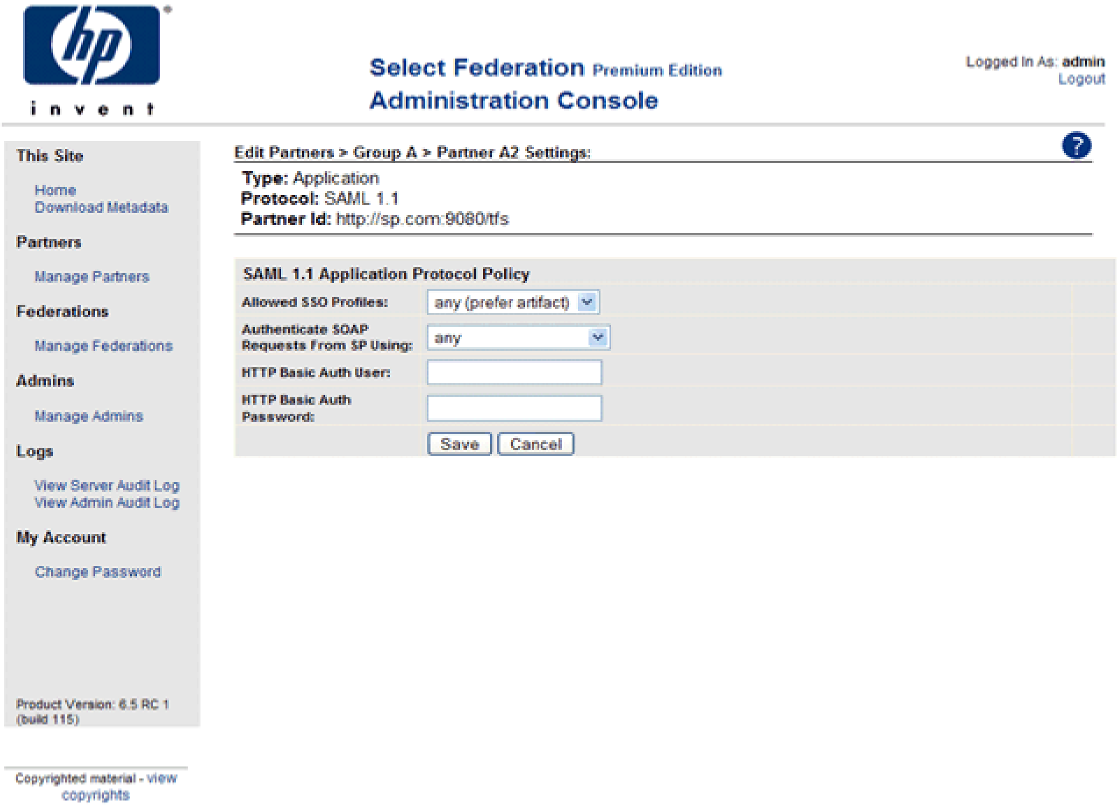
If your site is the SAML Producer (Authority or IDP) and you will receive authentication requests from your SAML Consumer Partners (Application or SP), you will need to set the single sign-on parameters in this section of the web page (Figure 44). The **Allowed SSO Profiles** are:

- **Any (prefer artifact)**: Your system will accept any SSO profile, but will prefer artifact.
- **Any (prefer post)**: Your system will accept any SSO profile, but will prefer post.
- **Artifact**: Your system will only accept artifact profiles.
- **Post**: Your system will only accept post profiles.

Set the SOAP Authentication Method in Your SAML SP Policy

In the post profile, a SAML assertion is sent from the SAML Producer (Authority or IDP) to the SAML Consumer (Application or SP) via the browser only and SOAP requests are not used. In the artifact profile, a pointer is sent from the IDP to the SP via the browser and a SOAP call is set from the SAML Consumer (Application or SP) to the SAML Producer (Authority or IDP) using one of the four SOAP Authentication methods.

Figure 44 Setting the SOAP Authentication Method in your SAML SP policy



Edit Partners > Group A > Partner A2 Settings:

Type: Application
Protocol: SAML 1.1
Partner Id: http://sp.com:9080/tfs

SAML 1.1 Application Protocol Policy

Allowed SSO Profiles:	any (prefer artifact)
Authenticate SOAP Requests From SP Using:	any
HTTP Basic Auth User:	
HTTP Basic Auth Password:	

Figure 44 shows the current screen. You can **Authenticate SOAP Requests from SP Using**:

- **Signature**: SAML Digital Signature-based Authentication

  > The **Signature** authentication method will not work for SAML 1.0 due to a limitation in the protocol specification; therefore, it is important to configure the authentication method for SAML 1.0 to be anything other than **Signature**.

- **SSL/TLS Client Authentication** Certificate-based authentication for authenticating the SAML consumer to the SAML producer. The SAML consumer presents an SSL client certificate in order to successfully establish a secure SSL / TLS channel for picking up the SAML artifact.

  > Using the client authentication method requires both partners to be using the HTTPS protocol.

- **HTTP Basic Authentication** using a username and password. If you select this authentication method, you will need to enter the desired username and password in the fields **HTTP Basic Auth User** and **HTTP Basic Auth Password** as shown in Figure 44.
- **Any** of the above

Do not forget to save your changes by clicking **Save**.

Updating Your SAML Authority Partner Protocol Metadata

Under partner details in the drop-down menu, select **Protocol Metadata**. You will be directed to a web page similar to the one in Figure 45 that delineates all the certificate information, protocol policy, and URLs that are needed for this SAML Partner.

When you click **Update**, you will then be directed to a web page similar to the one shown in Figure 46 where you can update your Partner's SAML Producer (Authority or IDP) policy information.

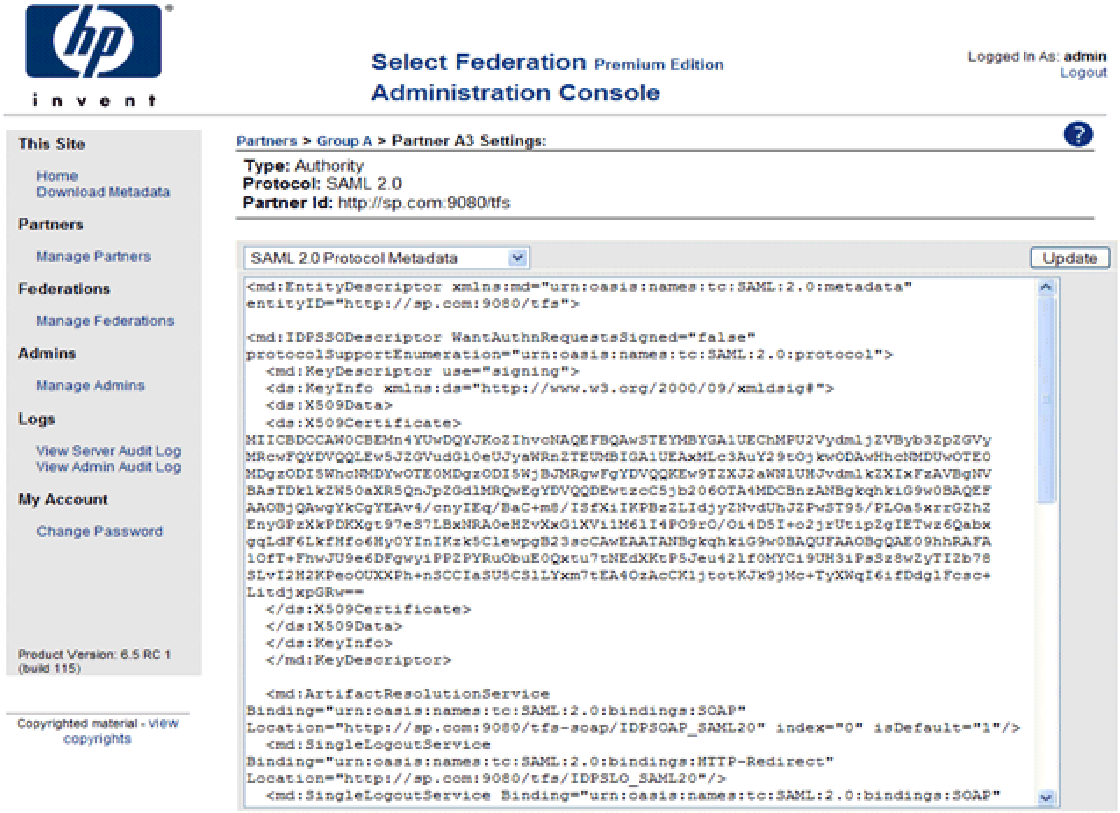
If your Trusted Partner uses SAML 1.X, it is possible that no metadata file or a URL link is available. In this case you will need to enter the updated information manually.

For the Partner metadata, make any needed changes to the:

- **Assertion Issuer Certificate**: This certificate is required for verifying SAML assertions received from that site. This field is only needed for SAML 1.1.
- **Source Id**: A 20 byte hex encoded or base64 encoded binary value that the Authority includes in artifacts that it generates. It uniquely identifies this site in your federation to Select Federation. Choose a unique name for each site you are adding.
- **Artifact Retrieval SOAP Endpoint**: This is the location of the SAML responder's SOAP service used for artifact pickup.
- **Attribute Authority SOAP Endpoint:** If your site is a SAML consumer and the Partner site is a SAML producer, then this is the URL where your site will invoke the Partner's attribute authority service over SOAP for obtaining user attributes.
- **Intersite Transfer URL:** This field is optional. This is the SAML Inter-site Transfer Service URL used to navigate to your Partner site in the federation.

Do not forget to save your changes by clicking **Update**.

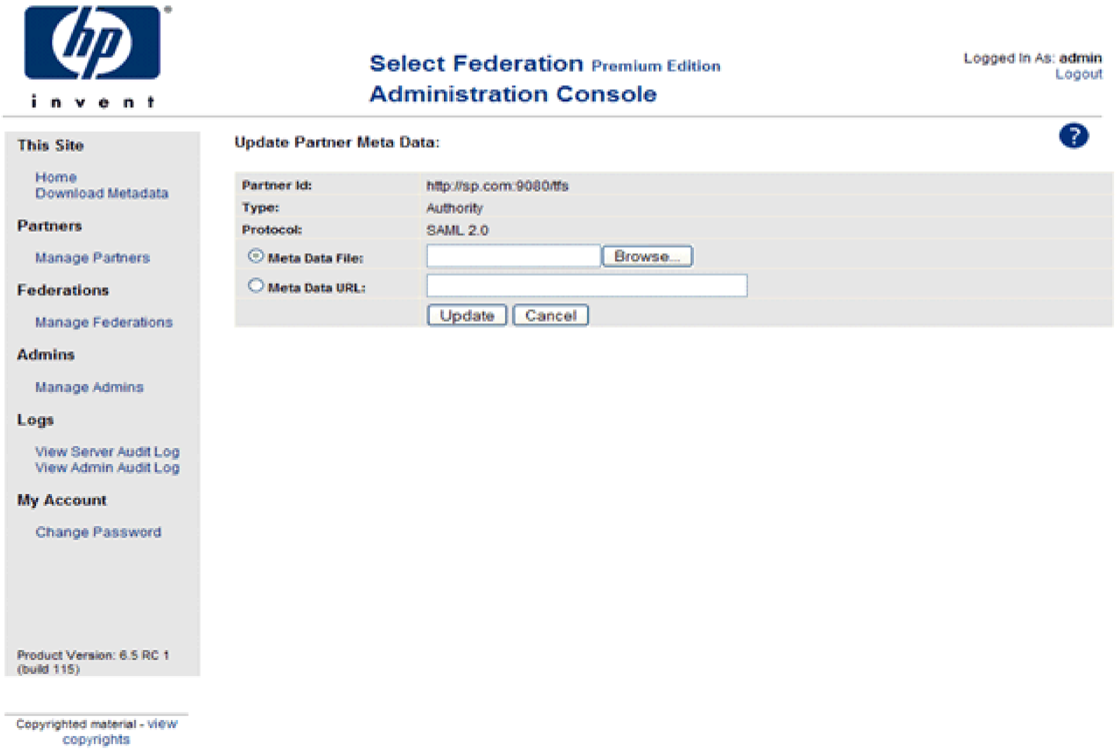
Figure 45 Updating a SAML Protocol metadata for an Authority Partner



Type: Authority
Protocol: SAML 2.0
Partner Id: http://sp.com:9080/tfs

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="http://sp.com:9080/tfs">

<md:IDPSSODescriptor WantAuthnRequestsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
   <md:KeyDescriptor use="signing">
   <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   <ds:X509Data>
   <ds:X509Certificate>
MIICBDCCAW0CBEMn4YUwDQYJKoZIhvcNAQEFBQAwSTEYMBYGA1UEChMPU2VydmljZVByb3ZpZGVy
MRcwFQYDVQQLEw5JZGVudGl0eUJyaWRnZTEUMBIGA1UEAxMLc3AuY29tOjkwODAwHhcNMDUwOTE0
MDgzODI5WhcNMDYwOTE0MDgzODI5WjBJMRgwFgYDVQQKEw9TZXJ2aWNlUHJvdmlkZXIxFzAVBgNV
BAsTDklkZW50aXR5QnJpZGdlMRQwEgYDVQQDEwtzcC5jb206OTA4MDCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEAv4/cnyIEq/BaC+m8/ISfXiIKPBzZLIdjyZNvdUhJZPwST95/PLOa5xrrGZhZ
EnyGPzXkPDKXgt97eS7LBxNRA0eHZvXxG1XVi1M61I4PO9rO/Oi4D5I+o2jrUtip2gIETwz6Qabx
gqLdF6LkfMfo6My0YInIKzk5ClewpgB23scCAwEAATANBgkqhkiG9w0BAQUFAAOBgQAE09hhRAFA
1OfT+FhwJU9e6DFgwyiPPZPYRuObuE0Qxtu7tNEdXKtP5Jeu421f0MYCi9UH3iPsSz8wZyTIZb78
SLvI2M2KPeoOUXXPh+nSCCIaSU5CS1LYxm7tEA4OzAcCK1jtotKJk9jMc+TyXWqI6ifDdg1Fcsc+
LitdjxpGRw==
   </ds:X509Certificate>
   </ds:X509Data>
   </ds:KeyInfo>
   </md:KeyDescriptor>

   <md:ArtifactResolutionService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="http://sp.com:9080/tfs-soap/IDPSOAP_SAML20" index="0" isDefault="1"/>
   <md:SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="http://sp.com:9080/tfs/IDPSLO_SAML20"/>
   <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
```

Figure 46 Uploading Partner metadata



Update Partner Meta Data:

Partner Id:	http://sp.com:9080/tfs
Type:	Authority
Protocol:	SAML 2.0
◉ Meta Data File:	
○ Meta Data URL:	

Updating Your Authority Partner SAML Protocol Policy

Under partner details in the drop-down menu, select **Protocol Policy**. You will be directed to a web page as shown in Figure 43. To make changes, click **Edit** and you will be directed to another web page as shown in Figure 44.

If your site is a SAML Consumer (Application or SP) and you will be sending artifacts to the SAML Producer (Authority or IDP), you will need to set the single sign-on parameters on this web page.

Select one of the three SOAP Authentication methods that your site will use to **Authenticate SOAP Requests to the IDP**.

- **Signature**: SAML Digital Signature-based Authentication.
- **SSL/TLS Client Authentication**: Certificate-based authentication for authenticating the SAML consumer to the SAML producer. The SAML consumer presents an SSL client certificate (see “Assertion Consumer Certificate” above) in order to successfully establish a secure SSL / TLS channel for picking up the SAML artifact.
- **HTTP Basic Authentication** using a username and password. If you select HTTP Basic Authentication, you will need to enter in the username and password in the fields **HTTP Basic Auth User** and **HTTP Basic Auth Password** as shown in Figure 44.

Do not forget to **Save** your changes.

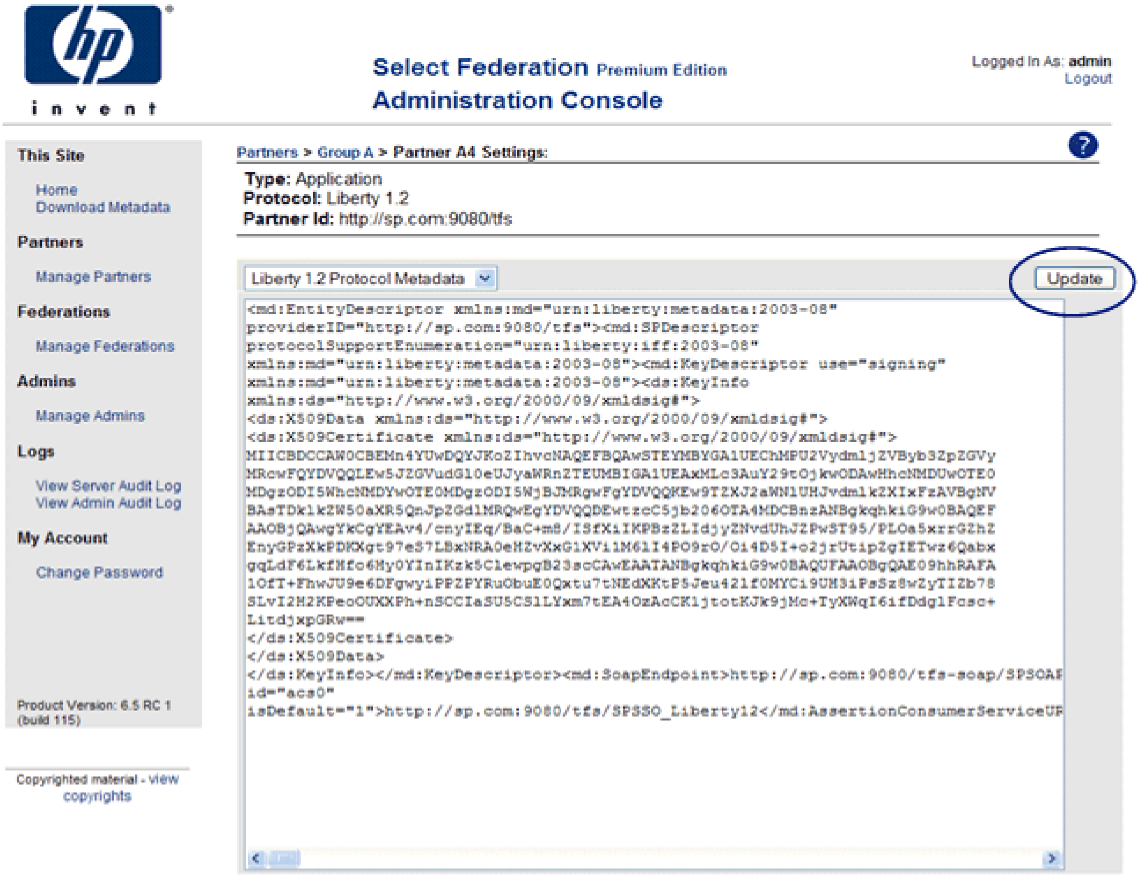
Updating Your Liberty Protocol Metadata

Similar to setting up a new Liberty Partner, updating an existing Liberty protocol metadata is relatively automated. Under partner details in the drop-down menu, select **Protocol**

Metadata. You will be directed to a web page that delineates all the certificate information, protocol policy, and URLs that are needed for this Liberty Partner.

Changing any information for a Liberty Partner is just a matter of uploading a new metadata file provided by your Partner. To change the metadata, click **Update** as shown in Figure 47.

Figure 47 Changing the metadata for a Liberty Partner

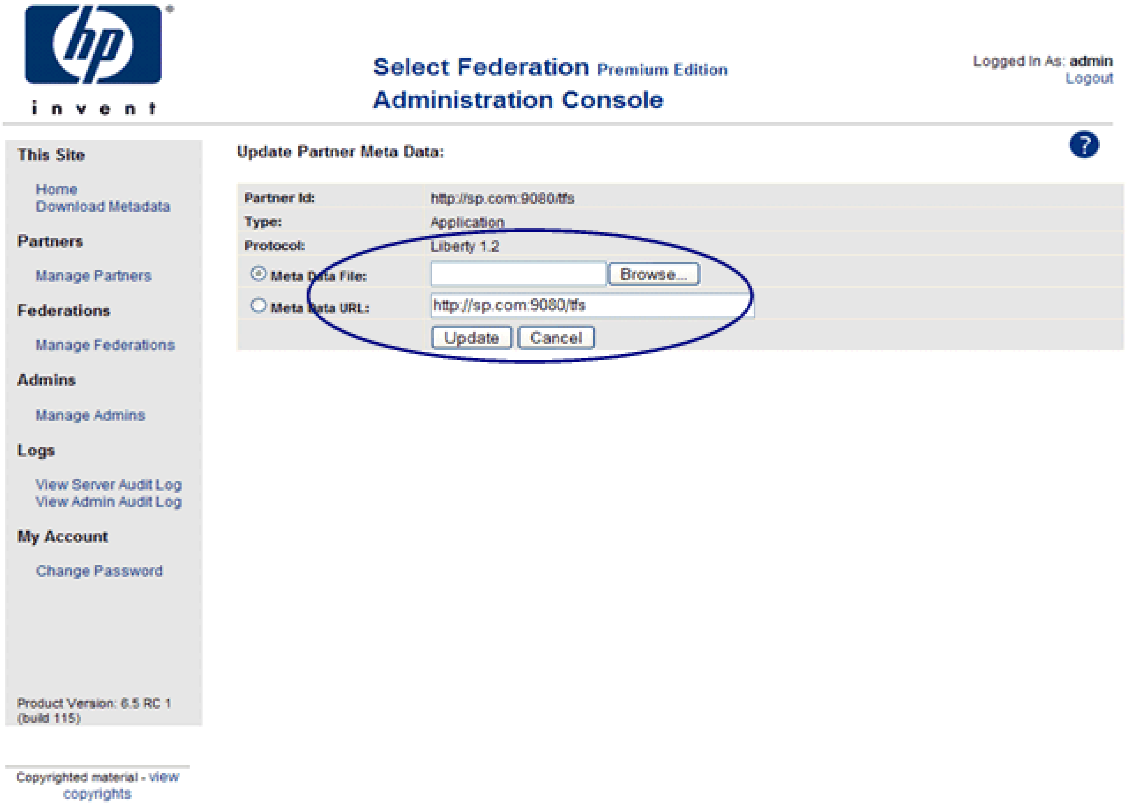


Type: Application
Protocol: Liberty 1.2
Partner Id: http://sp.com:9080/tfs

```
<md:EntityDescriptor xmlns:md="urn:liberty:metadata:2003-08"
providerID="http://sp.com:9080/tfs"><md:SPDescriptor
protocolSupportEnumeration="urn:liberty:iff:2003-08"
xmlns:md="urn:liberty:metadata:2003-08"><md:KeyDescriptor use="signing"
xmlns:md="urn:liberty:metadata:2003-08"><ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Certificate xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
MIICBDCCAW0CBEMn4YUwDQYJKoZIhvcNAQEFBQAwSTEYMBYGA1UEChMPU2VydmljZVByb3ZpZGVy
MRcwFQYDVQQLEw5JZGVudG10eUJyaWRnZTEUMBIGA1UEAxMLc3AuY29tOjkwODAwHhcNMDUwOTE0
MDgzODI5WhcNMDYwOTE0MDgzODI5WjBJMRgwFgYDVQQKEw9TZXJ2aWN1UHJvdmlkZXIxFzAVBgNV
BAsTDk1kZW50aXR5QnJpZGd1MRQwEgYDVQQDEwtzcC5jb206OTA4MDCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEAv4/cnyIEq/BaC+m8/ISfXiIKPBzZLIdjyZNvdUhJZPwST95/PLOa5xrrGZhZ
EnyGPzXkPDKXgt97eS7LBxNRA0eHZvXxG1XVi1M61I4PO9rO/Oi4D5I+o2jrUtipZgIETwz6Qabx
gqLdF6LkfHfo6My0YInIKzk5ClewpgB23scCAwEAATANBgkqhkiG9w0BAQUFAAOBgQAE09hhRAFA
1OfT+FhwJU9e6DFgwyiPPZPYRuObuE0Qxtu7tNEdXKtP5Jeu421f0MYCi9UH3iPsSz8wZyTIZb78
SLvI2H2KPeoOUXXPh+nSCCIaSU5CS1LYxm7tEA4OzAcCK1jtotKJk9jMc+TyXWqI6ifDdglFcsc+
LitdjxpGRw==
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo></md:KeyDescriptor><md:SoapEndpoint>http://sp.com:9080/tfs-soap/SPSOAP
id="acs0"
isDefault="1">http://sp.com:9080/tfs/SPSSO_Liberty12</md:AssertionConsumerServiceUR
```

You will then be directed to a web page as shown in Figure 48 where you can upload a new Liberty metadata file by simply entering or browsing for the file path name. Alternatively, you can also enter the metadata URL. Click **Update** when you are done.

Figure 48 Update a Liberty Partner’s Protocol Policy, upload a revised metadata file



Update Partner Meta Data:

Partner Id:	http://sp.com:9080/tfs
Type:	Application
Protocol:	Liberty 1.2
● Meta Data File:	
○ Meta Data URL:	http://sp.com:9080/tfs

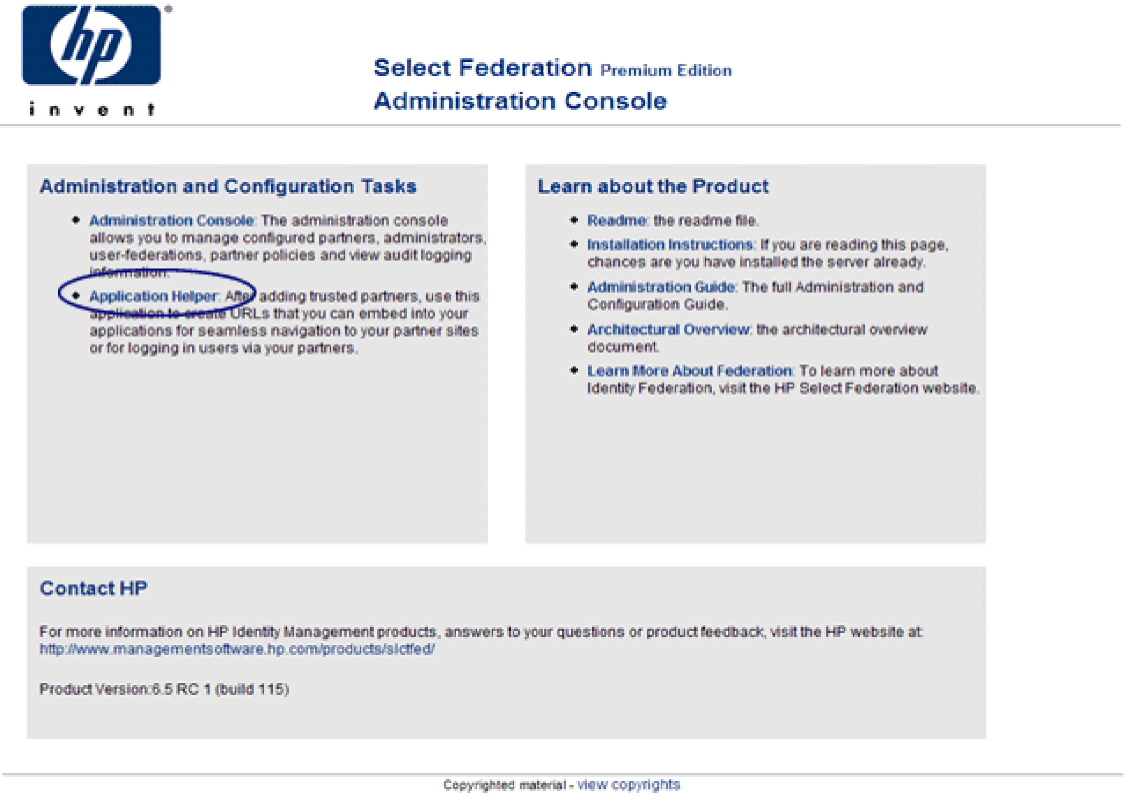
8 Enabling Applications

This chapter gives a short description on how to enable applications to work with HP OpenView Select Federation. For more detailed instructions, see the *HP OpenView Select Federation Programmers Guide* which is provided on the Select Federation SDK CD.

Using the Application Helper

For ease of integration into your existing environment Select Federation provides a special Application Helper component. There is a link to the Application helper in the Administration Console startup page (see Figure 49).

Figure 49 Select Federation Administration Console



Select Federation Premium Edition
Administration Console

Administration and Configuration Tasks

- Administration Console: The administration console allows you to manage configured partners, administrators, user-federations, partner policies and view audit logging information.
- Application Helper: After adding trusted partners, use this application to create URLs that you can embed into your applications for seamless navigation to your partner sites or for logging in users via your partners.

Learn about the Product

- Readme: the readme file.
- Installation Instructions: If you are reading this page, chances are you have installed the server already.
- Administration Guide: The full Administration and Configuration Guide.
- Architectural Overview: the architectural overview document.
- Learn More About Federation: To learn more about Identity Federation, visit the HP Select Federation website.

Contact HP

For more information on HP Identity Management products, answers to your questions or product feedback, visit the HP website at: http://www.managementsoftware.hp.com/products/slctfed/

Product Version:6.5 RC 1 (build 115)

Copyrighted material - view copyrights

You can also navigate to the Application Helper using the following address at the top-level URL:

```
<base-url>/tfs-internal/helperMain.html
```

The Application Helper can help you configure URLs in your application for seamless navigation to Service Provider (SAML Consumer) sites or for authentication via Identity Provider (SAML Producer) sites.

There are two useful pages in the Application Helper:

- `idphelper.jsp:` This helps you construct URLs to embed in your application that allow your users to seamlessly navigate to trusted third-party web sites. You may want users to go to a particular URL at that site, which you can enter on this page, or you can leave the target URL field blank, in which case the third-party site will navigate the user to an default URL after verifying the trust between the sites.
- `sphelper.jsp:` This shows how to construct login URLs that enable you to let users login, federate and de-federate via a trusted Identity Provider (IDP). It also provides a way of constructing "global logout" URLs that you can use to initiate a global logout for a user that has been authenticated at your site. Please note that the global logout and federation / defederation features are available only when using the Liberty protocol.

9 Regular Administration Tasks

Managing Federations

Clicking **Manage Federations** on Menu Sidebar of the Administration Console allows you to see all of the users that are federated with your Partners. You can search in three different ways:

- Enter the **Partner ID** on the corresponding field and click **Lookup** to find information about that specific user's federations.
- Enter the **Group ID** on the corresponding field and click **Lookup** to find information about that specific Partner's user federations.
- Click on **Lookup** without entering any information to search for all users and their federations.

Server and Admin Auditing

HP OpenView Select Federation has two helpful, simple-to-use auditing and administrative tools. These tools are the:

- Server Audit Log
- Admin Audit Log

Select Federation tracks all federation logins and logouts in the database that can be searched by most of its parameters.

Viewing the Server Audit Log

All administrators can view the server log for their department or region to see the activities of their enabled users. You can view Server Audit Log by specifying initial substrings for any or all of the search criteria for viewing the audit logs. All the fields are optional. If you leave a field blank, you will search for all the entries in that category. If you want to see a list of all enabled users, leave the field blank and click **Lookup**.

By event type – Event type is a federation event such as "Logged In" or "Received Logout Request", "Logged Out", etc.

By user Id – The local user ID of the user can be used to search the logs.

By request Id – Each federation request has a particular request ID that can be used to correlate logs at different sites. This field allows you to search the logs by this request ID.

By partner Id – Each site in a federation is uniquely identified by its provider ID. Use this field to search for all messages exchanged with a particular site.

By origin IP – Origin IP is the IP address of the authentication request.

From date – Specified as MM-DD-YYYY.

To date – Specified as MM-DD-YYYY.

When viewing the Server Audit log, the Partner IDs show up as friendly name hyperlinks whenever that Group/Partner ID is still in use.

Viewing the Admin Audit Log

The Root Admin can view all the federated identity activities of the delegated administrators. You can view Admin Audit Log by specifying initial substrings for any or all of the search criteria for viewing the audit logs. All the fields are optional. If you leave a field blank, you will search for all the entries in that category. For example, if you want to see a list of all enabled administrators, leave the field blank and click **Lookup**.

By event type – Event type is an administrator action such as "Viewed Audit Log" or "Logged In", etc.

By admin Id – The user ID of the administrator.

By user Id – The user ID of the user whose entries have been referenced / manipulated by the administrator.

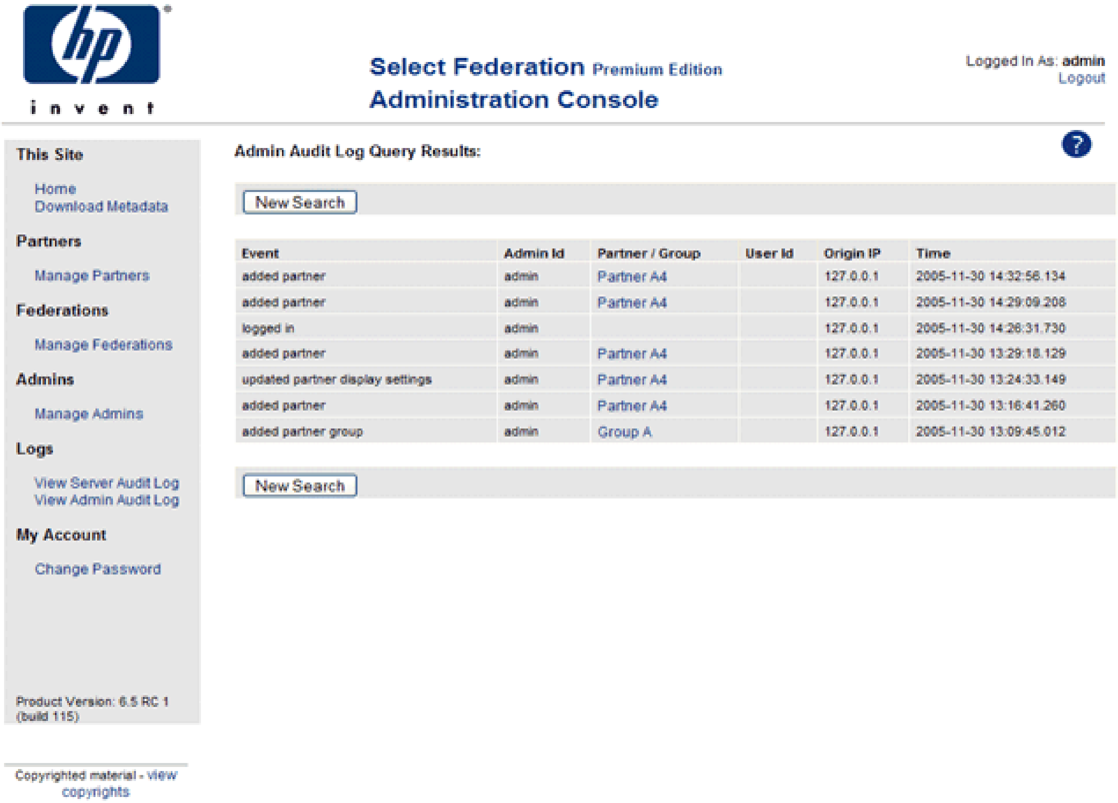
By partner Id – The unique ID of the partner site.

By origin IP – Origin IP is the IP address of the authentication request.

From date – Specified as MM-DD-YYYY.

When viewing the Admin Audit log, the Partner IDs show up as friendly name hyperlinks whenever that Group/Partner ID is still in use. See Figure 50.

Figure 50 Viewing the Admin Audit Log



Admin Audit Log Query Results:

Event	Admin Id	Partner / Group	User Id	Origin IP	Time
added partner	admin	Partner A4		127.0.0.1	2005-11-30 14:32:56.134
added partner	admin	Partner A4		127.0.0.1	2005-11-30 14:29:09.208
logged in	admin			127.0.0.1	2005-11-30 14:26:31.730
added partner	admin	Partner A4		127.0.0.1	2005-11-30 13:29:18.129
updated partner display settings	admin	Partner A4		127.0.0.1	2005-11-30 13:24:33.149
added partner	admin	Partner A4		127.0.0.1	2005-11-30 13:16:41.260
added partner group	admin	Group A		127.0.0.1	2005-11-30 13:09:45.012

Product Version: 6.5 RC 1 (build 115)

Copyrighted material - view copyrights

10 Configuring Attributes

Introduction

Attributes are often important for a useful federation setup. Installations that act as authorities provide attributes to application partners. Attributes are conveyed using the various federation protocols; these protocols require that attributes have designated names. Authorities that provide attributes need to fetch these attributes from a data source. HP OpenView Select Federation comes with built in support for LDAP directories, and relational databases as attribute sources. In addition, a plugin interface (see DirPlugin in the SDK) is available that enables development plugins that fetch or compute attributes from alternative sources.

The remainder of this chapter describes how the attributes that are used in HP OpenView Select Federation are defined in the system configuration (the `tfsconfig.properties` file).

Configuration of an attribute

The system configuration has an entry "`userAttrs`", a space separated list of keys for the attributes that are available to the system. For each listed key a corresponding attribute should be configured. For example, if there is:

```
userAttrs=name_title name_firstname
```

then the system configuration should have entries for the attributes "`name_title`" and "`name_firstname`". The entries for `name_firstname` could look like:

```
name_firstname.dstSvc=pp
name_firstname.dstSelect=/pp:PP/pp:CommonName/pp:AnalyzedName/pp:FN

name_firstname.samlAttr=name_firstname

name_firstname.samlAttrNS=http://schemas.trustgenix.com/samlattr

name_firstname.saml2Attr=name_firstname

name_firstname.saml2AttrFormat=urn:oasis:names:tc:SAML:2.0:attrname-

format:basic

name_firstname.ldapAttr=givenName
```

Each entry starts with the "key" and is followed by a dot. For each attribute the recognized subentries are:

- **`dstSvc`**: the key to a DST (Liberty ID-WSF Data Services Template) service. This means that the attribute will be available through the named DST service. The service name should have a corresponding entry with its namespace, e.g. `pp.dstNS=urn:liberty:id-sis-pp:2003-08`.
- **`dstSelect`**: the Select statement for the given attribute as specified by the DST service in question.

The presence of `dstSvcC` and `dstSelect` indicate that the attribute is available through an ID-WSF DST type of service.

- **`samlAttr`**: the name of the attribute in SAML 1 attribute statements. This name has to be agreed upon with partners.
- **`samlAttrNS`**: the namespace of name of the SAML attribute. This namespace has to be agreed upon with partners.
- **`saml2Attr`**: the name of the attribute in SAML 2 attribute statements. This name has to be agreed upon with partners.
- **`saml2AttrFormat`**: the identifier of the format of the attribute name in SAML 2.0 attribute statements. SAML 2.0 profiles specify a number of these format identifiers. Partners may agree upon other identifiers too.

The presence of the `samlAttr` or `saml2Attr` means that the attribute can be pushed in assertions, and is available for SAML attribute queries; subject to per partner settings for attributes (see *Editing Partner Settings*) and possibly subject to end user policy (see *Configuring Privacy Manager*).

- **`dispName`**: the name shown to end user by the Privacy Manager. If absent, the attribute "key" is used. Note that the dictionaries for internationalization may have entries based upon attribute keys, display names or both. So the final text presented to the user may not be the display name that is in the system configuration.
- **`ldapAttr`**: At an authority site (IDP site), the name of the LDAP attribute that is used to find the value of the configured attribute. This is only used when an LDAP is used to resolve attribute queries. If Select Federation is configured to work with Select Access, then at an application site (SP site), the ldapAttr value is used to populate the destination LDAP directory.

> In order for federation to work successfully, you need to make sure that every attribute that is used to populate the LDAP directory can be created in the destination LDAP directory.

In general, an authority installation obtains attributes from a DirPlugin implementation. HP OpenView Select Federation ships with implementations for relational databases and LDAP directories as well as with an implementation for a simple file-based user database. The DirPlugin implementation is set using the "`dirPlugin`" configuration entry, which is set during installation. See the `tfsconfig.properties` file and Appendix A for alternative values. Also note that it is possible to develop custom DirPlugin implementations, see *Programmers Guide* which is provided on the Select Federation SDK CD.

Using Multiple Directory Plugins

It is possible to setup multiple directory plugin implementations, such that a particular plugin is responsible for one or more designated attributes. Multiple plugins can be set using these steps:

1. Add the "`directory`" entry to one or more attributes, e.g.:

   `someAttribute.directory=2ndPlugin`.

2. Add at least a "`class`" entry for the additional plugin to the system configuration, e.g.:

   `2ndPlugin.class=myPlugin`.

In addition it is then possible to add a "`jarFile`" entry and plugin specific entries., e.g.:

```
2ndPlugin.jarFile=/home/ib/newDirPlugin.jar
```

```
2ndPlugin.someEntry=foo.
```

When the system instantiates the plugin it will be provided with the configuration parameters, e.g. with "`someEntry=foo`".

For each attribute the responisble plugin can be given in the "`directory`" subentry for that attribute, e.g.:

```
newAttr.directory=2ndPlugin.
```

When the "`directory`" subentry is absent the DirPlugin that is configued with "`dirPlugin`" is used. It is possible to configure all attributes with an explicity responsible directory plugin but it is strongly recommended to have a default plugin configured with "`dirPlugin=`". This as some authentication plugins authenticate against the configured default plugin.

11 Configuring Privacy Manager

Overview

HP OpenView Select Federation Privacy Manager is a unique feature that empowers end users to control the exchange of their personal attributes and their preferences about exchanging such information between trusted sites.

The Privacy Manager is used by Select Federation to interact with end users to ask for permission to link accounts (federate), to ask for permission to release attributes to partners, etc. In Select Federation *Premium Edition* (only) the Privacy Manager allows for end users to have the system remember privacy decisions as privacy policy rules. In this case, the Privacy Manager also offers a facility to end users to review such privacy policy rules. In all cases, the Privacy Manager uses a presentation engine to render pages to users. This presentation engine allows for localization on a per user basis, can adapt to various browsers that end users may have, and enables branding of the pages.

Configuring Privacy Manager

Privacy Manager configuration is performed by changing settings in the `tfsconfig.properties` file.

Enabling the use of Privacy Manager for ID-WSF services (PE only)

If ID-WSF services such as the Personal Profile are used, one should also enable the ID-WSF interaction redirect service, one of the components of the Privacy Manager. This is performed by uncommenting the following line in `tfsconfig.properties`:

```
## Location of interaction redirect service used by
## ID-WSF WSPs deployed here
userInteractionURL=https://{BASE_URL}/pm/irs
```

where `{BASE_URL}` is the URL of your installation.

Configuring use of end user privacy policies (PE only)

By default the use of end user privacy policies is disabled. Enabling such policies will allow end users to ask the system to remember privacy decisions, and to review the thus constructed policies. To enable privacy policy rules changes this line in `tfsconfig.properties`:

```
# Uncomment/edit following line to allow use of user
# specific policies for the listed services
userPolicy.services=profile
```

This line accepts a list of space separated service names; "profile" is the build in service name for the set of SAML and ID-WSF attribute services (see *Configuring the Attribute Policy*).

For the profile service it is now possible to set some parameters related to pages that users may encounter. The name of the service as displayed to user (before localization) is set by:

`profile.name=Personal Profile`.

The possible outcomes of user privacy policy rules are governed by this line:

`profile.possibleDecisions=DENY PROMPT GRANT`.

For example to allow users only to create rules that deny access to certain profile attributes and, hence ensure positive explicit consent before attribute release, the line could read:

`profile.possibleDecisions=DENY`.

DENY, PROMPT and GRANT are all keywords that should be used as is. The actual text shown to end users is subject to localization and branding.

End users can review their policies by visiting this URL:

`https:{BASE_URL}/pm/privacy`.

Branding the end user pages

The Privacy Manager uses the Select Federation presentation engine to render pages to end users; both the pages that ask for consent as well as the pages that enable viewing and modification of the user privacy rules. The presentation engine allows for branding of these pages in two ways. First, changes in titles, logo and colors and to some degree layout are possible by changing configuration entries. A second level of modification is possible by changing or replacing the XSLT stylesheets.

Branding by configuration settings

The following configuration entries can be used to influence the pages:

```
## CSS stylesheet reference, that controls colors and layout
#presentation.css-url=/styles/users.css
## Logo source
#presentation.logo-src=/styles/logo.gif
## Logo alternative text
#presentation.logo-text=HP
## Logo hyperlink, this is the page users will go when they
## click the logo
#presentation.logo-href=http://www.hp.com
```

The logo-text is also used for some page titles. The CSS stylesheet can be used to make quite drastic changes. Note that color changes are easy and "safe" whereas layout changes will require careful testing.

Branding by XSLT stylesheets

The presentation engine uses XSLT stylesheets to transform semantic XML documents into browser pages. These stylesheets provide ultimate control over the end user look and feel, but modifying these is recommended only to experts. A good reason to modify these files is to allow for better localization.

The stylesheets are located in a subdirectory of the "conf" directory of the installation. The files are structured in a hierarchy according to locale and browser type. The names of the XSLT stylesheets and the directory structure should *not* be changed. Most layout changes can be achieved by changing those stylesheets that have names ending in "`-layout.xsl`".

12 Authentication Contexts

The Liberty ID-FF and the SAML 2.0 standard suites have the notion of an "Authentication Context". An authentication context is a description of a particular method for authenticating users, such as verifying a password. An application may require that a user be authenticated in a manner that is consistent with a particular authentication context and likewise an authority informs an application about the actual authentication context that was used. Authentication contexts need to be agreed upon between partners. This chapter describes how to configure authentication contexts in HP OpenView Select Federation.

In many cases no changes are required. Making changes is not recommended unless the administrator has a thorough understanding of both the standards as well as the policy that the partnership wants to deploy.

Statements and classes

Authentication context descriptions are typically fairly large (XML) documents that contain details about e.g. password length, verification of photo IDs, etc. It would be impractical to always move these large documents around over the network. Also, there are a number of widely-used authentication methods that are well understood even if details are slightly different between different implementations. Hence, there are Authentication Context Classes, which represent such well-known methods such as "password over a protected transport". Authentication Context Statements however, are actual description documents that define the details of the authentication context, e.g. the number of bits in the password. As there rarely is a need to move actual authentication context documents around, references are used.

Relative order of authentication context

Without mutual agreement between partners a particular authentication context classes cannot be interpreted as referring to "stronger" authentication as another. When partners agree about relative ordering of authentication contexts, it becomes possible for an application partner to request an authority for authentication of a user at "at least" a given authentication context. The ID-FF and SAML 2.0 protocols allow for this notion, but as explained it requires agreement between partners.

Configuring authentication context statements and references

The system configuration contains information about the authentication contexts. The authentication context classes and statements that are supported by the currently configured authentication plugin (or page) can be configured. These are set by the parameters:

- **`authnContextClassRef`**: the space separated references to the supported authentication context classes; used for processing Liberty ID-FF authentication requests.
- **`authnContextStatementRef`**: the space separated references to the corresponding authentication context statements that are supported.
- **`saml2AuthnContextClassRef`**: the space separated references to the supported authentication context classes; used for processing SAML 2.0 authentication requests.
- **`saml2AuthnContextStatementRef`**: the space separated references to the corresponding authentication context statements that are supported.
- **`samlAuthMethod`**: the space separated identifiers of the supported authentication methods according to the SAML 1 specifications.

The relative ordering of authentication contexts is set by the parameters:

- **`rankedAuthnContextClassRefs`**: space separated list of references to authentication context classes; from weak to strong, weakest first.
- **`rankedAuthnContextStatementRefs`**: space separated list of references to authentication context statements; from weak to strong, weakest first.

➤ These are the Liberty ID-FF classes / statements. Normally the set of supported authentication contexts is a subset of the ranked contexts.

13 Configuring Liberty Introduction Service

A common problem in a federated system is that when a user is about to login to a service provider site, how can that site help the user identify which site he can login from. This is the IDP Selection problem.

The Liberty Alliance Standard has a specialized mechanism for addressing this issue called the Introduction Protocol. This is done by the all the IDPs and the SP setting up a common DNS Domain that hosts a server from each one of the sites. Thus if an “Extranet” acting as an SP site and several “Portals” acting as IDPs form a circle-of-trust, to use the introductions protocol, they need to define a common DNS domain, say `commondomain.com`.

Each site gets a sub DNS address such as `extranet.commondomain.com` and `portal1.commondomain.com`, for each participant in the circle of trust. An IDP is expected to write a cookie in this common domain by redirecting its users to its server in the common domain. The cookie domain is set to the entire common domain `commondomain.com` so that it may be read by any web server in this domain.

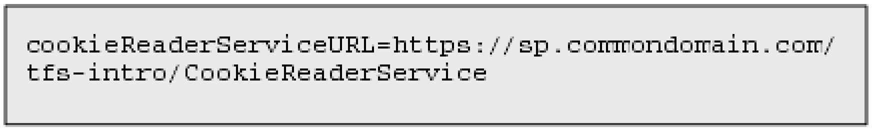
When the user then navigates to the SP, the SP redirects the user to the common domain and finds out if any IDP has stored a cookie in the common domain. If it has, then the SP redirects the user to that IDP in order to sign-on the user.

Configuration and Usage

HP OpenView Select Federation provides certified interoperable support for the introduction protocol. The WAR file to be hosted on the introductions server is `tfs-intro.war`.

In order to use the Introduction service, you need to setup DNS appropriately and then run the `tfs-intro.war` on the server in the common DNS domain. This WAR requires the configuration file `tfsconfig.properties`. In addition, the Select Federation operational WAR, `tfs.war`. needs to know where the introduction service is located.

At an IDP Site, the `tfs.war` requires the following variables:

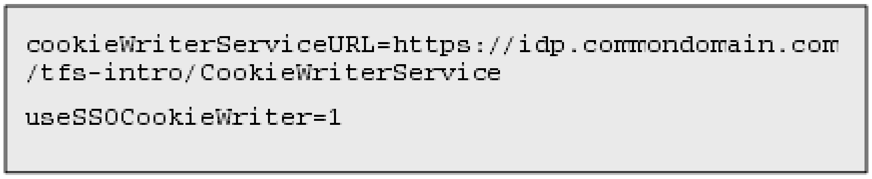


```
cookieReaderServiceURL=https://sp.commondomain.com/
tfs-intro/CookieReaderService
```

The value of the `cookieWriterServiceURL` variable is the URL of the common domain cookie writer. The `useSSOCookieWriter` variable turns the introduction functionality on or off. The value of this variable should be “1” in order to use the introduction service.

Currently, HP OpenView Select Federation only supports the use of the Cookie Writer Service when using the artifact profile.

At an SP Site, the `tfs.war` requires the following variables:



```
cookieWriterServiceURL=https://idp.commondomain.com
/tfs-intro/CookieWriterService

useSSOCookieWriter=1
```

14 Certificate Management

Using a signing certificate issued by a 3rd party CA

The Select Federation installer generates a self-signed certificate for use in signing and TLS client authentication. If you have a certificate issued by a certificate authority (CA), it may be used instead by following these instructions.

Prerequisites

- Java keystore with your private key and the matching certificate issued by a CA
- File with CA certificate in PEM format:

  ```
  -----BEGIN CERTIFICATE-----
  ```

  and

  ```
  -----END CERTIFICATE-----
  ```

Installation

1 Edit the `tfsconfig.properties` file generated by the Select Federation installer and change the following lines:

```
keystoreType=JKS
keystorePath=<path to your keystore.jks>
keystorePassword=<password for your keystore>
certAlias=<alias for your certificate in the keystore>
keyAlias=<alias for your key in the keystore>
keyPassword=<password for your key in the keystore>
```

2 If you have a certificate issued by a private CA that is not included in the default Java trust list, you will need to install the CA's certificate in your Java cacerts file using the Java keytool. The default paths are as follows:

- **WebLogic:** `BEA_HOME/jdk142_05/jre/lib/security/cacerts`
- **WebSphere:** `IBMWS_HOME/java/jre/lib/security/cacerts`
- **Built-in application server:** `SF_HOME/_jvm/lib/security/cacerts`

15 Localizing and Customizing HP OpenView Select Federation

This chapter deals with customization and localization of the end user visible pages of Select Federation. These pages are mainly the Privacy Manager and the federation consent page. Customization of these pages refers to changing the look and feel – the styles, logos, colors, etc. Localization refers to changing anything about these pages such that they are rendered effectively in a particular locale (language and country).

Customizing Select Federation

Simple Customization

Most common requirements for customization, such as changing the styles used for various visual elements, logos, colors, etc. can be met by simply adding a few variables to the Select Federation configuration file `tfsconfig.properties`. The variables are:

Name	**Type**	**Description**
`presentation.css-url`	String	The URL of the style sheet to be used for rendering Privacy Manager pages.
`presentation.logo-src`	String	The URL of the logo to be displayed on the Privacy Manager pages.
`presentation.logo-text`	String	Alternative text to be displayed when the mouse is hovered over the logo.
`presentation.logo-href`	String	The URL to which the user is navigated upon clicking the logo.

Advanced Customization

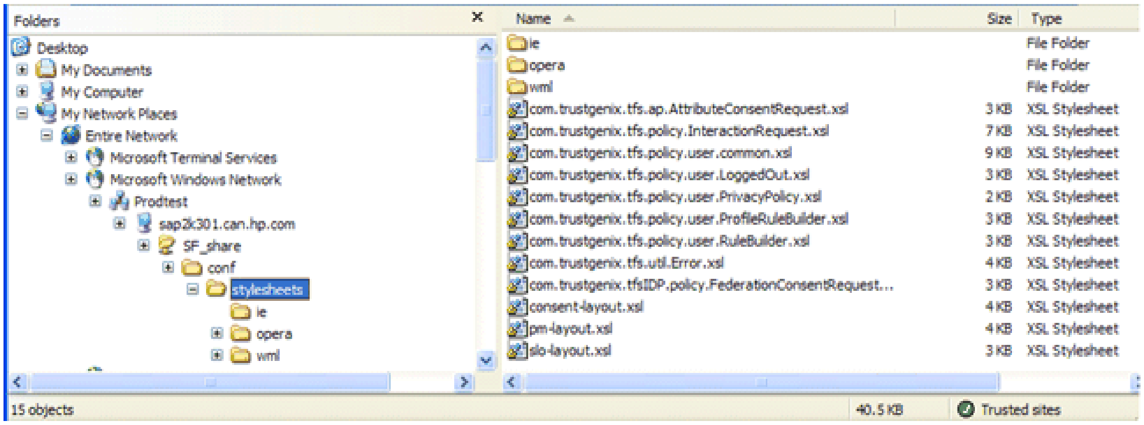
If the above customization parameters do not meet your requirements for customization of the Privacy Manager, then further customization can be done by modifying the XSLT files that are used to render the pages. The original XSLT files are typically in the `conf/stylesheets` subdirectory relative to the current working directory of the JVM (i.e. the directory from where the application server is launched).

It is also possible to create XSLT files that are specific to a particular user agent. This requires you to define possible user-agent aliases in the `tfsconfig.properties` file as follows:

```
presentation.browsers=wml ie mogw

presentation.mogw=MOGW

presentation.ie=MSIE Internet%20Explorer
presentation.wml=wml
```

As you can see above, the `presentation.browsers` variable indicates the complete list of defined browser types. Subsequently, for each browser type defined, a user-agent search string is defined. Select Federation will determine if the user-agent string presented by the browser contains the string defined above. If so, it will use the first matching browser type. The resulting directory structure is shown below:

Figure 51 Directory for XSLT template files



Name	Size	Type
ie		File Folder
opera		File Folder
wml		File Folder
com.trustgenix.tfs.ap.AttributeConsentRequest.xsl	3 KB	XSL Stylesheet
com.trustgenix.tfs.policy.InteractionRequest.xsl	7 KB	XSL Stylesheet
com.trustgenix.tfs.policy.user.common.xsl	9 KB	XSL Stylesheet
com.trustgenix.tfs.policy.user.LoggedOut.xsl	3 KB	XSL Stylesheet
com.trustgenix.tfs.policy.user.PrivacyPolicy.xsl	2 KB	XSL Stylesheet
com.trustgenix.tfs.policy.user.ProfileRuleBuilder.xsl	3 KB	XSL Stylesheet
com.trustgenix.tfs.policy.user.RuleBuilder.xsl	3 KB	XSL Stylesheet
com.trustgenix.tfs.util.Error.xsl	4 KB	XSL Stylesheet
com.trustgenix.tfsIDP.policy.FederationConsentRequest...	3 KB	XSL Stylesheet
consent-layout.xsl	4 KB	XSL Stylesheet
pm-layout.xsl	4 KB	XSL Stylesheet
slo-layout.xsl	3 KB	XSL Stylesheet

Localizing Select Federation

International Character Support

If you would like your installation to have support for international characters for user attributes exchanged between federated sites, it is strongly recommended to set the default locale of the systems on which HPSF is installed such that the character encoding is "UTF-8". Alternatively, most Java runtime implementations can be forced into UTF-8 by starting the JVM with the option: `-Dfile.encoding=UTF-8`.

Simple Localization

As with customization, most of the needs for localization to a particular language and country combination can be met by simply creating a resource bundle specific to that language, and if required to a country specific version of it. This resource bundle then needs to be added to the system classpath before starting the application server. The base name of the Java class for which you can create locale specific resource bundles is `com.trustgenix.tfs.i18n.User`. Sample locale specific resource bundles are provided on the SDK CD under the `localization` top-level directory.

Advanced Localization

In case you need to localize the end user pages (modify formatting or look and feel elements or alter layouts), you can create locale (language and country) specific subdirectories to the `conf/stylesheets` subdirectory. The name of the language specific subdirectory is the two letter **ISO Language Code** optionally followed by an underscore followed by the two letter **ISO Country Code**. For example, you may create a directory for the Swedish language as:

`conf/stylesheets/sv`.

Or create a directory for the Finland country specific variant of Swedish as:

`conf/stylesheets/sv_FI`.

Select Federation will attempt to find a locale specific directory for the XSLT for any end user facing page by matching the locale specification supplied by the browser. If the user agent specifies a country specific language variant, Select Federation will attempt to find the country specific and language specific subdirectory, but if it does not find that, Select Federation will attempt to find the generic language specific language subdirectory. If neither is not found, it will load the generic XSLTs at the top-level `conf/stylesheets` subdirectory.

16 Troubleshooting

Use the Tomcat log file (`catalina.out`) to view logged messages. You would have use the UNIX shell script (`startup.sh`) instead of the DOS batch script so that this log file gets generated. There could be some exceptions caused due to incorrect syntax or configuration. Here are some common problems:

Why do I get the error “schema does not exist”?

The current schema for any connection defaults to a schema corresponding to the user name. If no user name is supplied then the user name (and hence current schema) defaults to APP. However, even though the current schema is set to the user name, that schema may not exist. A schema is only created by CREATE SCHEMA or creating an object (table etc.) in that schema (this is implicit schema creation). **The one exception to this is the APP schema, which is always created**, though applications should not depend on that. This is the reason why the userid and password have been set to “APP”.

“Userid length, 0, is not allowed”

The DB2 driver *requires* that a user ID be specified when establishing a connection. Not specifying a user ID or leaving it blank will result in this error.

The Select Federation installer reported an issue with the directory server SSL certificate. How do I fix this?

There are several possibilities which might have generated this warning, e.g., a name mismatch or an expired certificate. However, the most common scenario is that of an "untrusted certificate", when the CA that issued this certificate is unknown to the Select Federation Java trust store. You could use a simple utility like **keytool** to install the CA's certificate in your Java cacerts file. In the case of the bundled application server, the cacerts file would be located in the `_jvm\lib\security` sub-directory of the install location. If you installed Select Federation on an existing application server in your environment, locate the cacerts file for the JDK that is being used by the application server. You can then issue a command (example given below) for importing your CA cert:

```
% keytool -import -trustcacerts -alias MyCA -file <CA certificate file> -
keystore <path to your Java installation>/lib/security/cacerts -storepass
<default value is "changeit">
```

In Select Access integrated mode, browser is stuck after federated login at IDP

This can happen when you are using Internet Explorer, and Select Access and Select Federation are running on different ports of the same computer. This happens due to a known issue with the Microsoft Internet Explorer browser which causes wrong URLs to be generated during the redirect from Select Federation to Select Access.

A Configuration Parameters

HP OpenView Select Federation configuration is mainly performed by editing the `tfsconfig.properties` file. This appendix has the configuration parameters that can be manually typed into the `tfsconfig.properties` file in order to customize your installation. The parameters related to several topics are explained in more detail in the following chapters.

If you would like to edit the `tsfconfig.properties`, you should:

1. Make a backup copy of the `tfsconfig.properties` before editing it.
2. Edit the `tfsconfig.properties` file in the configuration directory of the application server (i.e. the directory where the configuration files were copied to).

Types of Configuration Parameters

There are five types of configuration parameters that are possible when you are manually entering the data.

Table 1 Types of Configuration File Parameters

Type	Example	Format
String	param=value	A String value. See Java Properties documentation for the list of special characters that require escaping.
StringList	param=value1 value2	A StringList is a space-separated list of String values (spaces appearing in values, if allowed, must be escaped).

Boolean	param=0
	param=1
		A Boolean has a value of 0 (false) or 1 (true).

Integer	param=123
	param=-1
		An Integer value.

TimeDuration	param=1s
	param=1h30m
	param=500
		A TimeDuration is a measure of time in days, hours, minutes, seconds (and milliseconds). Use the unit suffix ‘d’ or ‘D’ for days, ‘h’ or ‘H’ for hours, ‘m’ or ‘M’ for minutes, and ‘s’ or ‘S’ for seconds. A number without a unit suffix is treated as milliseconds.

tfsconfig.properties

Table 2 Core Configuration File Parameters

Name	Type	Default (if not reqd)	Description
jdbcDataSource	String	null	JNDI name of J2EE Data Source to use, by default, for connections to the database. If this option is provided then jdbcAddr/Driver/User/Password are ignored..
jdbcAddr	String	null	JDBC address to use, by default, for connections to the database.
jdbcDriver	String	null	JDBC driver to use, by default, for connections to the database.
jdbcUser	String	null	JDBC user to use, by default, for connections to the database.
jdbcPassword	String	null	JDBC password to use, by default, for connections to the database.
tblPrefix	String	"tfs"	Prefix to use, by default, for database tables.
userAttrs	StringList	null	List of user profile attributes to support.
<attralias>.dstSelect	String	null	If non-null, the DST select expression that maps to this profile attribute.
<attralias>.dstNS	String	null	The DST service namespace for this profile attribute.
<attralias>.samlAttr	String	null	If non-null, the SAML attribute that maps to his profile attribute.
<attralias>.samlAttrNS	String	null	The SAML attribute namespace for this profile attribute.
relayTimeout	Time Duration	20m	The time to allow for messages to be relayed through user agent (browser) connections. Determines various cache lifetimes and notOnOrAfter values in SAML assertions. Default is 20 minutes.
purgeInterval	Time Duration	1h	Determines how often the runtime tables are purged of entries for abandoned sessions. Default is 1 hour.
auditPrune	Time Duration	0	Audit logs are pruned of all entries older than auditPrune. If auditPrune is 0, logs are not pruned.

Name	Type	Default (if not reqd)	Description
adminEventPlugin	String	null	Specifies the `com.trustgenix.tfsAdmin.plugin.AdminEventPlugin` to be used.
defaultMetadata	String	“saml20”	Specifies the format of the metadata available at the providerId of the installation. It can be one of: liberty12, liberty11idp, liberty11sp, saml10, saml11, saml20.
preferFrontChannel	Boolean	false	Indicates that protocols should prefer front-channel browser profiles (such as SAML POST) instead of back-channel profiles (such as SAML Artifact).
presentation.defaultLanguage	String	“en”	Indicates the language of the top-level XSLT files in the `conf/stylesheet` directory.
presentation.stylesheetDir	String	“conf/stylesheets”	Sets the directory with the XSLT files that control the presentation of end user pages. The default directory is where the installer copies these files.
presentation.css-url	String	“/styles/users.css”	The URL to the CSS stylesheet that will be used by the XSLT files of the presentation service.
presentation.logo-src	String	“/styles/logo.gif”	The logo is used for the top-left logo in pages served by the presentation service.
presentation.logo-text	String	“HP”	Used as an alternative text for the logo used by the presentation service. The same string is also used in some titles and headers.
presentation.logo-href	String	“http://www.hp.com”	Link to the page users will go when they click the logo rendered by the presentation service.
useSelectAccess	Boolean	true	Indicates if HP OpenView Select Access is used together with this HP OpenView Select Federation installation.
useSLOGetProfile	Boolean	false	This is set to true by the installer and indicates that the GET based method for Single Logout is to be used. If true, checkmarkURL should be set too.

Name	Type	Default (if not reqd)	Description
checkmarkURL	String		An optional String that typically points to a picture that should be shown upon successful logout of a partner. The installer sets this to `<baseURL>/tfs/checkmark.gif`. This entry is required if useSLOGetProfile is true.
auditDataProvider	String	com.trustgenix.tfs.util.AuditDataProvider_JDBC	This parameter can be set to com.trustgenix.hpsf.selectaudit.AuditDataProvider_SelectAudit in case HP OpenView Select Audit should be used for auditing system events.
AuditDataProvider_SelectAudit.auditToHPSF	Boolean	False	If HP OpenView Select Audit is used for auditing and this entry is true, system events will be logged to both Select Audit and Select Federation databases.
AuditDataProvider_SelectAudit.port	String	<Select Access default connector port>	The port number of the Select Access connector can be found in the *HP OpenView Select Access Installation Guide*.

Table 3 Application Configuration File Parameters

Name	Type	Default (if not reqd)	Description
defaultIDP	String	null	Default IDP to use when authenticating users.
spAutoGenerateLocalUserId	Boolean	false	If true, new users are assigned an automatically generated unique local identifier, bypassing the activation process. This is equivalent to specifying the F_AUTOGENERATELOCALID flag in the SPAPI.loginUser call.
includeSAMLAssertionInProfile	Boolean	false	If true, the SAML Assertion will be included in the SPAPI profile as an XML string under the key "_samlAssertion".
includeSAMLSubjectNameInProfile	Boolean	false	If true, the SAML Assertion Subject Name will be included in the SPAPI profile as three strings under the keys: "_samlSubjectName", "_samlSubjectNameQualifier", and "_samlSubjectNameFormat".

Name	Type	Default (if not reqd)	Description
spEventPlugin	String	null	SPEventPlugin implementation class name. If non-null, the class will be instantiated and called for login and logout events. If installation is used to host Applications that are to be protected by HP OpenView Select Access, this should be set to "`com.hp.ov.selectfederation.HPSA_SPEventPlugin`".
spDefaultURL	String	Required	The default application URL to send users to following receipt of an unsolicited authentication assertion with no accompanying target URL.
spProxyReturn	Boolean	false	If true, the server will act as a proxy to load the return URL for authenticated users during the login process. This eliminates a user agent redirect, but requires that the return URL is re-written to include any needed session IDs (since cookies will not be available).
signAuthnRequests	Boolean	Required	If true, AuthnRequest messages will be signed.
spFederation Termination NotificationProtocol Profiles	StringList	Required	List of Liberty protocol profile URIs to support for FT at the SP.
spRegisterName IdentifierProtocol Profiles	StringList	Required	List of Liberty protocol profile URIs to support for RNI at the SP.
spSingleLogout ProtocolProfiles	StringList	Required	List of Liberty protocol profile URIs to support for SLO at the SP.
supportLECProfile	Boolean	true	If true, AuthnRequests will be sent using the LECP profile whenever a compatible Liberty-Enabled header is detected.
lecpIDPs	StringList	null	If non-null, the list of IDPs (identified by ProviderID) to include in the AuthnRequestEnvelope IDPList.
useSSOCookie Writer	Boolean	false	If true, the SSO service will use the configured cookie writer to update the Liberty common domain cookie.
cookieWriter ServiceURL	String	null	The URL of the CookieWriterService to use. Required if useSSOCookieWriter is true.

Name	Type	Default (if not reqd)	Description
spAuthTimeout	String	Value of authTimeout	If the IDP sends a **reauthOnOrAfter** which is later than what the SP configuration dictates or for absent values, the SP will use its own, stricter, value. If **spAuthTimeout** is set to 0, the SP uses the IDP provided timestamps as is, even if null (never expire). Hence when Select Federation is being used with Select Access, **spAuthTimeout** should never be set to 0.

Table 4 Authority Configuration File Parameters

Name	Type	Default (if not reqd)	Description
idpAuthnPlugin	String	null	IDPAuthnPlugin implementation class name. If non-null, the class will be instantiated and called to authenticate users and invalidate login sessions. If null, loginURL will be used.
idpAuthnPlugin. characterEncoding	String	“UTF-8”	idpAuthnPlugin.characterEncoding can be set to indicate the character encoding used by a login page. This may be needed if an IDPAuthnPlugin is used (by setting idpAuthnPlugin=..). The default value is "UTF-8" and it is strongly recommended that all login pages use "UTF-8" for forms (e.g. like this: <form action="..." accept-charset="utf-8" method="post">.
loginURL	String	null	If idpAuthnPlugin is null, users are redirected to this URL for authentication. The page at this URL must use the IDPAPI to record the user authentication.
logoutURL	String	null	If idpAuthnPlugin is null, and logoutURL is non-null, users are redirected to this URL during logout processing.
consentURL	String	null	If non-null, users are redirected to this URL to provide consent for new federations.

Name	Type	Default (if not reqd)	Description
authTimeout	Time Duration	0	Default timeout for user authentications at the IDP, within a browser session. After this time, the user is required to re-authenticate. A value of 0 disables expiration of user authentications.
reauthMaxAge	TimeDuration	1s	Maximum age of an authentication that can satisfy a forced re-authentication request. Default is 1 second.
authnContext ClassRef	StringList	Required	List of Liberty AuthnContextClassRef URIs supported by the configured idpAuthnPlugin or loginURL.
authnContext StatementRef	StringList	Required	List of Liberty AuthnContextStatementRefs corresponding to the AuthnContextClassRefs listed in authnContextClassRef (in order).
saml2Authn ContextClassRef	StringList	Required	List of SAML 2.0 AuthnContextClassRefURIs supported by the configured idpAuthnPlugin or loginURL.
saml2Authn ContextStatementRef	StringList	Required	List of SAML 2.0 AuthnContextStatementRefs corresponding to the AuthnContextClassRefs listed in saml2AuthnContextClassRef (in order).
samlAuthMethod	StringList	Required	List of SAML 1.1 AuthenticationMethod URIs corresponding to the Liberty AuthnContextClassRefs listed in authnContextClassRef (in order).
rankedAuthn ContextClassRefs	StringList	Required	List of AuthnContextClassRefs in comparison order according to local policy, from weakest to strongest.
rankedAuthn ContextStatement Refs	StringList	Required	List of AuthnContextStatementRefs in comparision order according to local policy, from weakest to strongest.
dirPlugin	String	null	DirPlugin implementation class. If non-null, the class will be instantiated and called to perform directory operations such as verifying passwords and fetching user profile attributes.

Name	Type	Default (if not reqd)	Description
dirPlugin_File.file Path	String	Required if dirplugin =com. trustgenix .tfsIDP. util. DirPlugin _FIle	The file path for the properties file used by the file based DirPlugin.
dirPlugin_File. valueSep	String	";"	A configurable value separator that is used to split attribute properties into multiple values. For example, "`user.foo=one;two;three`". The default is semicolon. If valueSep is set to an empty value, then attribute properties will NOT be split into multiple values (each attribute will have only one value).
<attralias>.ldap Attr	String	null	If non-null, the LDAP user attribute that maps to his profile attribute.
idpFederation Termination NotificationProtocol Profiles	StringList	Required	List of Liberty protocol profile URIs to support for FT at the IDP.
idpRegisterName IdentifierProtocol Profiles	StringList	Required	List of Liberty protocol profile URIs to support for RNI at the IDP.
idpSingleLogout ProtocolProfiles	StringList	Required	List of Liberty protocol profile URIs to support for SLO at the IDP.
idpSingleSignOn ProtocolProfiles	StringList	Required	List of protocol profile URIs to support for SSO at the IDP.
idwsfSupport AttributeQuery	Boolean	false	If true, the built-in ID-WSF profile service front-end to the dirPlugin is enabled and advertised via the DiscoveryResourceOffering attribute in ID-FF assertions. The DS is also enabled in read-only mode to advertise the profile service(s).
useSSOCookie Writer	Boolean	false	If true, the SSO service will use the configured cookie writer to update the Liberty common domain cookie.
cookieWriter ServiceURL	String	null	The URL of the CookieWriterService to use. Required if useSSOCookieWriter is true.

Name	Type	Default (if not reqd)	Description
cookieDomain	String	null	If non-null, the CookieWriterService is enabled to write Liberty introduction cookies in the specified domain (e.g. ".cot.com").
cookieMaxAge	Integer	0	If zero, the default, introduction cookies are created as session cookies. If greater than zero, introduction cookies are created as persistent cookies with the specified lifetime.
cookieSecure	Boolean	true	If true, introduction cookies are flagged as secure.
samlRequest Auth	StringList	"sign ssl http"	The list of SOAP authentication mechanisms configured for the SAML SOAP service.
samlInclude Audience Restriction Condition	Boolean	false	If true, SAML SSO assertions include an audience restriction condition identifying the intended consumer.
samlIncludeSubject IP	Boolean	false	If true, SAML SSO assertions include the authenticated user's IP address (as determined by examining the network connection over which the user is authenticated).
samlSupport AttributeQuery	Boolean	false	If true, attribute query requests will be accepted on the SAML SOAP endpoint.
wantAuthn RequestsSigned	Boolean	false	If set to 1, authentication requests from all partners are expected to be signed, irrespective of the partner specific setting for the Application Protocol Policy.
workaroundCookie Quotes	Boolean	false	Enables a workaround for a bug in Tomcat cookie handling, explicitly adding quotes around the cookie value.

Table 5 DirPlugin_LDAP Plugin Configuration File Parameters

Name	Type	Default (if not reqd)	Description
ldapURL	String	Required	LDAP URL to use, by default, for connections to the directory.
ldapPrincipal	String	null	LDAP user to use, by default, for connections to the directory.
ldapPassword	String	null	LDAP password to use, by default, for connections to the directory.

Name	Type	Default (if not reqd)	Description
ldapAuthentication	String	"simple"	LDAP authentication mode to use, by default, for connections to the directory (see JNDI documentation for possible values; “GSSAPI” is supported for Kerberos v4 authentication to AD).
ldapUserAttr	String	Required	LDAP attribute to use for username in constructing user DN.
ldapUserBaseDN	String	Required	Base DN to use in constructing user DN from username and ldapUserAttr. User DN looks like `<ldapUserAttr>=<username>,<ldapUserBaseDN>.`
<attralias>.ldapAttr	String	null	If non-null, the LDAP user attribute that maps to his profile attribute.

Table 6 HPSA Adapter Configuration File Parameters

Name	Type	Default (if not reqd)	Description
hpsf.debugLevel	String	`null`	Debugging level for enforcer.
hpsf.enforcerName	String	`null`	Name of the enforcer used by Select Federation.
hpsf.enforcerPath	String	`/selectFederation`	The path at which the enforcer is used.
hpsf.serviceURL	String	Automatically computed	The base URL of the server at which the enforcer is running. This is automatically set by select Federation, but can be overridden by this variable.
hpsf.spLogoutURL	String		The URL at an SP to which Select Federation redirects when it receives a logout request from an IDP.
hpsf.ldapServerType	String		This can be either “ads” for active directory or “sun” for all other.
hpsf.ldapUserAttr	String		The attribute for creating the full path to the user object in the LDAP directory.
hpsf.ldapUserBaseDN	String		The base DN within which the LDAP path will be created.
hpsf.enforcerConf	String	null	Adds a path to a HP OpenView Select Access enforcer config file (`enforcer-servlet.xml).` This is useful to overcome the SA bug in Linux with the default SA enforcer config path.

Table 7 Privacy Manager Configuration File Parameters

Name	Type	Default (if not reqd)	Description
profileDispAttrs	StringList	null	List of profile attributes to display in consent dialogs, if present in request.
<attralias>.disp Name	String		Display name for profile attribute.
userPolicy.services	String	“profile”	Allows use of user-specific policies for the listed services. For listed services, user consent will be required. Select Federation Premium Edition only.
userInteraction URL	String	null	Location of interaction redirect service used by ID-WSF WSPs. Should be set to the base URL followed by `/pm/irs` . Select Federation Premium Edition only.
userPolicyData Provider	String	“com. trustgenix .tfs.policy. user. Policy Data Provider_ JDBC”	User privacy store type. It can be either “com.trustgenix.tfs.policy.user.PolicyDataProvider_JDBC” (for relational databases), “com.trustgenix.tfs.policy.user.PolicyDataProvider_Dir” (when storing policies in the configured directory) or “com.trustgenix.tfs.policy.user.PolicyDataProvider_File” (for storing policies as XML documents in a file system directory).
PolicyDataProvider _File.cache	Integer	10	File-based PolicyDataProvider file cache size.
PolicyDataProvider _File.directoryPath	String	“properties”	Directory where user privacy files will be stored.
PolicyDataProvider _Dir.policy AttributeName	String	“privacypolicy”	The name of the single valued LDAP attribute that will hold a user privacy policy as a blob.
profile.name	String	Required	The label for the tabbed page that shows user privacy rules for the profile service. The installer sets it to “Personal Profile”.
profile.default ConsentRequired	Boolean	true	Reserved for future usage. If set to false, end user consent will not be required for attribute release. Has the same effect as removing “profile” from the value of userPolicy.services.
profile.possible Decisions	StringList	“DENY, GRANT”	The possible decisions that rules about attribute release can state. The installer sets it to “DENY PROMPT GRANT”.

Name	Type	Default (if not reqd)	Description
profile.showValues InConsentRequest	Boolean	false	If true values of attributes that are about to be released are presented to the end user.
federation.name	String	Required	The label for the tabbed page that shows user privacy rules for the federation consent. The installer sets it to “Single Sign-on”.
federation.possible Decisions	StringList	“DENY, GRANT”	The possible decisions that rules about federation consent can state.
privacy.invalid RuleDeleteDelay	Time Duration	24h	Controls how long rules in user privacy policies that are no longer valid (e.g. because of reference to partners that no longer exist) remain in the policy before being removed. Note that rules are only marked as invalid, and only removed when users log in to the Privacy Manager.

spapiconfig.properties

Table 8 Application Configuration File Parameters

Name	Type	Default (if not reqd)	Description
providerId	String	Required	Server’s Liberty ProviderID.
providerBaseURL	String	Required	URL for the server’s front-channel WAR.
jdbcProvider	String	Required	Database-specific JDBC provider to use, by default, for connections to the database (e.g. “com.trustgenix.tfs.JDBCProvider_ Oracle”).
jdbcDataSource	String	null	JNDI name of J2EE Data Source to use, by default, for connections to the database. If this option is provided then jdbcAddr/Driver/User/Password are ignored.
jdbcAddr	String	null	JDBC address to use, by default, for connections to the database.
jdbcDriver	String	null	JDBC driver to use, by default, for connections to the database.

Name	Type	Default (if not reqd)	Description
jdbcUser	String	null	JDBC user to use, by default, for connections to the database.
jdbcPassword	String	null	JDBC password to use, by default, for connections to the database.
tblPrefix	String	"tfs"	Prefix to use, by default, for database tables.
cookieReader ServiceURL	String	null	If non-null, the URL of the CookieReaderService to use.

idpapiconfig.properties

Table 9 Authority Configuration File Parameters

Name	Type	Default (if not reqd)	Description
providerId	String	Required	Server's Liberty ProviderID.
providerBaseURL	String	Required	URL for the server's front-channel WAR.
jdbcProvider	String	Required	Database-specific JDBC provider to use, by default, for connections to the database (e.g. "com.trustgenix.tfs.JDBCProvider_ Oracle").
jdbcDataSource	String	null	JNDI name of J2EE Data Source to use, by default, for connections to the database. If this option is provided then jdbcAddr/Driver/User/Password are ignored.
jdbcAddr	String	null	JDBC address to use, by default, for connections to the database.
jdbcDriver	String	null	JDBC driver to use, by default, for connections to the database.
jdbcUser	String	null	JDBC user to use, by default, for connections to the database.
jdbcPassword	String	null	JDBC password to use, by default, for connections to the database.
tblPrefix	String	"tfs"	Prefix to use, by default, for database tables.

Name	Type	Default (if not reqd)	Description
timeOutSeconds	Integer	0	If greater than zero, determines the reauthenticateOnOrAfter time in assertions (overriding the value established by authTimeout in server). It is preferable to use the authTimeout parameter in the server. This parameter should only be used to override the authTimeout setting in the server with a shorter time, if needed.
tfsSIDCookie Domain	String	null	If non-null, the cookie domain used for the tfsSID cookie that records the user's IDP session. Can be used to share the tfsSID cookie between IDP web applications.
cookieReader ServiceURL	String	null	If non-null, the URL of the CookieReaderService to use.
cookieWriter ServiceURL	String	null	If non-null, the URL of the CookieWriterService to use.
cookieReader ReturnPrefixes	String	null	If non-null, the list of prefixes for allowed cookie reader return URLs.

Table 10 ID-WSF DS Configuration File Parameters

Name	Type	Default (if not reqd)	Description
idwsfSupportDS	Boolean	false	If true, the DS is enabled.
idwsfDSSecMechId	StringList	null	List of ID-WSF security mechanism URNs to support on DS endpoint. If null, defaults to urn:liberty:security:2003-08:TLS:X509, if providerBaseSOAPURL starts with https and urn:liberty:security:2003-08:null:X509 otherwise. If the AS is supported, the default security mechanisms will also include urn:liberty:security:2004-04:TLS:Bearer or urn:liberty:security:2004-04:null:Bearer, as appropriate based on providerBaseSOAPURL.
idwsfDSToken Timeout	Time Duration	0	Timeout for credential tokens issued by the DS. A value of 0 causes the value of authTimeout to be used (if authTimeout is also 0, credential tokens issued by the DS do not expire).

Name	Type	Default (if not reqd)	Description
idwsfDSAllow UpdatesFrom	StringList	null	If non-null, discovery service updates will only be allowed from the listed SPs (identified by ProviderID).

Table 11 LECP Service Configuration File Parameters

Name	Type	Default (if not reqd)	Description
lecpAllowIDPLoc Prefixes	StringList	null	If non-null, the LECP service will only consider IDPList entries (in a received AuthnRequestEnvelope) with locations that have a match in this list of URL prefixes.
lecpDenyIDPLoc Prefixes	StringList	null	If non-null, the LECP service will ignore IDPList entries (in a received AuthnRequestEnvelope) with locations that have a match in this list of URL prefixes.
lecpDefaultIDPLoc	String	null	The location of the IDP to use by default, when no IDPList is provided.
lecpDefaultIDPLoc_ Liberty11	String	null	The location of the IDP to use by default for Liberty 1.1 requests, when no IDPList is provided. This overrides lecpDefaultIDPLoc for Liberty 1.1 requests.
lecpDefaultIDPLoc_ Liberty12	String	null	The location of the IDP to use by default for Liberty 1.2 requests, when no IDPList is provided. This overrides lecpDefaultIDPLoc for Liberty 1.2 requests.
lecpStripHeaders IDP	StringList	null	List of headers (received by the LECP service) that should not be forwarded in requests sent to IDPs.
lecpStripHeaders SP	StringList	null	List of headers (received by the LECP service) that should not be forwarded in requests sent to SPs.
lecpSessionHdr	String	“X-LECP Session”	If non-null, identifies the header (received by the LECP service) that should be used to track the user’s session. See LECP Service manual for more information.

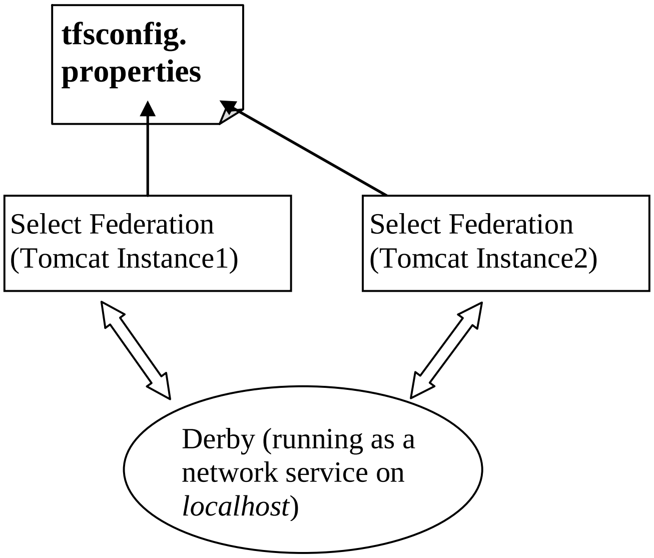
B Running Apache Derby as a Network Service

Summary

HP OpenView Select Federation uses Apache Derby as an embedded database. The database used by the system can be selected during the installation (see *Installation Procedure*).

This appendix describes the steps for running Apache Derby as a network service, rather than using it in embedded mode. This is especially useful in production environments, when multiple (possibly replicated) instances of Select Federation will have to share a database over the network.

Test scenario


tfsconfig. properties
Select Federation (Tomcat Instance1)
Select Federation (Tomcat Instance2)
Derby (running as a network service on *localhost*)

The experimental setup above shows 2 instances of Select Federation deployed on Tomcat 4.1. The host platform is WinXP. Derby will run as a network service on the host. The aim is to get both Select Federation instances to share the database available on the network.

Instructions

Download the Apache Derby binary

Go to the “Distributions” section on the *download page*.

Get the “jar” files required for the Derby server and client

On the server side (these are part of the Derby installation package in /lib):

- `derby.jar`
- `derbynet.jar`

On the client side (these are available *here*):

- `db2jcc.jar`
- `db2jcc_license_c.jar`

Set the CLASSPATH

Ensure that the classpath includes these jars. For example, on the server side, you would have to edit your classpath to include the following:

```
C:\<derbyhome>\lib\derby.jar;C:\<derbyhome>\lib\derbytools.jar;C:\<derb
yhome>\lib\derbynet.jar;%CLASSPATH%
```

The client jars should be copied to the “`/shared/lib`” subdirectory for all Tomcat instances that will be connecting to Derby.

Starting and shutting down derby through the command line

Startup command:

```
java org.apache.derby.drda.NetworkServerControl start -h localhost
-p 1527
```

Shutdown command:

```
java org.apache.derby.drda.NetworkServerControl shutdown -h localhost -
p 1527
```

Its convenient to put these commands in batch files under the Derby home directory (`startup.bat` and `shutdown.bat`). On successfully starting up the Derby server, you should see the following message:

```
Server is ready to accept connections on port 1527.
```

Edit tfsconfig.properties

Use the following syntax for the JDBC connection parameters when using a Derby network driver.

```
jdbcProvider=com.trustgenix.tfs.JDBCProvider_Derby

jdbcDriver=com.ibm.db2.jcc.DB2Driver

jdbcAddr=jdbc:derby:net://localhost:1527/"c:/ib-
cd/TFSDB":user=APP;password=APP;retrieveMessagesFromServerOnGetMessage=
true;
```

Comment out the properties `jdbcUser` and `jdbcPassword.` Note that the address string above is with the database authentication turned off. Refer to the troubleshooting and references section for additional information on the syntax.

Modify the deployment descriptor of the 2nd Select Federation instance

Edit the `web.xml` of the "tfs-internal" web-app of the 2nd Select Federation instance so that it points to the `tfsconfig.properties` of the 1st instance. This file can be found under `webapps\tfs-internal\WEB-INF` in the Tomcat installation directory.

```
<web-app>

…………..

<env-entry>

 <env-entry-name>com.trustgenix.tfs.propFile</env-entry-name>

 <env-entry-value>../<Select Federation 1st

 instance>/conf/tfsconfig.properties</env-entry-value>

 <env-entry-type>java.lang.String</env-entry-type>

</env-entry>

…………….

</web-app>
```

Start the Derby server and the Select Federation instances

Use the startup scripts to start Derby and both the Tomcat instances. Navigate to the admin console (`tfs-internal`) and login. This completes the setup.

Additional references

1 The Derby documentation is fairly good. Several manuals are available (look under `doc/manuals/index.html` in your Derby installation). These manuals are also available *online*.

2 *Accessing the Network Server using the DB2 Universal Driver* (contains syntactical notations and examples for accessing the network server).

3 Note on using *authentication and encryption* with Derby.

4 Setting Derby *system-wide properties*.

5 IBM *Cloudscape documentation*.

Index