# HP OpenView Select Federation

## Configuration and Administration Guide

**Software Version: 6.0**

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

**January 2005**

# 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 Trustgenix, Inc.
- BEA and WebLogic are registered trademarks of BEA Systems, Inc.
- IBM, Tivoli, WebSphere are trademarks of International Business Machines in the United States, other countries or both.
- Linux is a U.S. registered trademark of Linus Torvalds.
- Microsoft®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

- Oracle is a registered trademark of Oracle Corporation.  Various product and service names referenced herein may be trademarks of Oracle Corporation.
- Sun, Sun Microsystems, Solaris, and Java™ are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.
- All other trademarks, trade names, service marks, and logos referenced herein belong to their respective companies/owners.

## Support

Please visit the HP OpenView web site at:

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

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

You can also go directly to the support web site at:

http://support.openview.hp.com/

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 being able to:

- Search for knowledge documents of interest
- 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 log in.   Throughout the site, access levels are indicated by the following icons:

🔑 HP Passport

📝 Active contract

★ Premium contract

To find more information about access levels, go to the following URL:

http://support.openview.hp.com/access_level.jsp

To register for an HP Passport ID, go to the following URL:

https://passport.hp.com/hpp2/newuser.do

# Contents

1

# Introducing the Select Federation Configuration and Administration Guide

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 working knowledge of:

- Identity Management
- Federated Identity

## Chapters Summary

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

**Table 1-1: Contents Table**

| Chapter | Description |
|---|---|
| Chapter 1, Introducing the 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 2, Select Federation: Getting Started | This chapter describes what Select Federation does, and how to deploy and configure Select Federation for the initial use. This chapter provides the basic installation steps and is meant to be used in conjunction with the HTML installation instructions on the CD that holds the Select Federation software. This chapter includes directions on how to integrate Select Federation with Select Access. |
| Chapter 3, Select Federation: Systems Requirements | This chapter lists the systems requirements for Select Federation, including the hardware, software, operating systems that are supported by Select Federation. It also provides a list of third-party servers that can be used with Select Federation. |
| Chapter 4, Navigating the Select Federation Management Console | This chapter provides an overview of the Select Federation Management Console and details the features available to the root administrator. |
| Chapter 5, Setting Up Your Federations | This chapter provides detailed instructions on how to set up a federation for secure data exchange. It covers the concept of meta-data in federations, and how to create meta-data files that are sent to your partners in order to create your federation. |
| Chapter 6, Adding Trusted Partner Sites to Your Federation | This chapter explains how you will set up a new federation on your systems. Select Federation allows for Liberty ID-FF 1.1, Liberty ID-FF 1.2, SAML 1.0, and SAML 1.1 federation instances. This chapter details how to set up any of these federation instances and how to delete any existing federations. |
| Chapter 7, Editing Your Federation Parameters | This chapter explains how to change the parameters on your existing federations. |
| Chapter 8, Configuring the Profile Service | Select Federation allows you to transmit user attributes on every user authentication. This chapter provides an overview on Select Federation's Profile Service and explains how to configure the profile attribute exchange. |

| Chapter | Description |
|---|---|
| Chapter 9, Configuring the Privacy Manager | Select Federation allows the end-users to control the transmission of their personal attributes and preferences to other sites in the federation.  This chapter provides an overview of the Select Federation Privacy Manager and explains how to configure the Privacy Manager. |

2

# Select Federation: Getting Started

This chapter gives you a brief overview on Select Federation's capabilities. It also details the hardware, operating systems, and third party software that Select Federation supports.

## What does Select Federation Do?

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

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

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 websites that they use less frequently. Once these accounts are federated, users can access all the federated websites through their most frequently used account without having to log in each time.

## Select Federation: Systems Requirements

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

## Hardware Systems Requirements

Select Federation is qualified to run on any of the following hardware:

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

## Operating System Requirements

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

- HP-UX 11.20 or above
- Red Hat Linux version 7.3 or above
- Windows 2000 (server or professional) or Windows XP professional
- Sun Solaris 8 or above

## Java Software Requirements

Select Federation is qualified to run on any of the following Java Development Kits (JDKs):

- JDK 1.4.0
- JDK 1.4.1
- JDK 1.4.2 (**versions 1.4.2_04 and below only**)

## Supported Third-Party Servers

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

## Application Servers

Select Federation is qualified to run on any of the Application Servers shown in Table 2-1.

**Table 2-1: Applications Servers upon which Select Federation Runs**

| Server | Licensing Terms | Comments, if any |
|---|---|---|
| BEA Weblogic 7.0.1 | Free 90 day evaluation download available. | |
| BEA WebLogic 8.1 | Free 90 day evaluation download available | XML runtime libraries need to be replaced |
| IBM WebSphere 5.0.0 | Free 6-month trial download available | Requires manual addition of Sun RSA JCA crypto provider from JDK 1.3.1 |
| Apache / Jakarta Tomcat 4.1.10 | Free open-source | XML runtime libraries must be replaced as above |

## Database Servers

Select Federation is qualified to run on any of the database software shown in Table 2-2.

**Table 2-2: Database Servers upon which Select Federation Runs**

| Database | Licensing Terms | Comments, if any |
|---|---|---|
| Oracle 9i | Free development license available | |
| Apache Derby | Free open-source | Bundled with Select Federation, no need to install separately. |

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. The installation process requires a database instance name and a user name / password that can be used to create and drop tables, triggers, indexes, etc. in that instance.

## LDAP Servers

Select Federation is qualified to run on any of the LDAP Servers shown in Table 2-3.

**Table 2-3: Applications Servers upon which Select Federation Runs**

| LDAP Server | Licensing Terms | Comments, if any |
|---|---|---|
| Microsoft Active Directory | Included in Windows 2000 server | |

| LDAP Server | Licensing Terms | Comments, if any |
|---|---|---|
| OpenLDAP | Free open source software | Can be downloaded from www.openldap.org |
| Sun Java System Directory Server 5.1 | Free trial license available | |
| CA *e*Trust™ Directory 8.0 | Commercial license | Not supported in Select Access 6.0, but will be supported in Select Access 6.1 |

# Select Federation: Installation Overview

This chapter does not go into the details of each step of how to install Select Federation, but instead points the reader to the step that the user is required to go to. The installation of Select Federation has the following steps:

1. **Configuring Select Federation.** Running the configuration scripts that configures Select Federation for deployment.
2. **Integrating Select Access with Select Federation** explains how to configure policies in the Select Access Policy Builder for proper operation of Select Federation.
3. **Configuring Trusted Sites** Federation works between trusted sites, so the first step in creating an operational federation is setting up your trusted partner sites.
4. **Using the Application Helper** Select Federation has a special Application Helper that enables you to create URLs for embedding in your application.

## Using CD to Install Select Federation

For the initial installation, the installation instructions are in HTML form on the CD. To access the installation instructions, open the following file in a browser window:

```
<cd-base-directory>/docs/index.html
```

where the `<cd-base-directory>` is the location of the Select Federation distribution CD.

The installation instructions direct you to set the needed global attributes for your site policy. The root administrator can change the site attributes later if needed.

## Configuring Select Federation

The key to a successful Select Federation configuration requires that you copy and customize Select Federation's properties file. This file holds all the configuration information for Select Federation's setup.

### To Configure Select Federation

1. Copy the contents of the Select Federation CD to a hard-disk location. This location will become the home directory for Select Federation. In the rest of this chapter, we will refer generically to this location as the `${SF_HOME}` directory.
2. Open the `${SF_HOME}/` InstallSF.properties file in a text editor of your choosing. This is the file with which you configure Select Federation .
3. Open a browser and load the `${SF_HOME}/docs/index.html` file. This file contains the installation instructions for modifying this file.
4. Make changes to the file as required and save those changes.
5. Run the command-line installer. The command-line installer will generate tables in the database, generate the certificates and keys needed for Select Federation and configure output files that are used by the Select Federation server during run-time.

## Deploying Select Federation on an Application Server

You can deploy Select Federation on a variety of app-servers which implement the Servlet 2.3 specification which is a part of the Java 2 Enterprise Edition (J2EE) architecture. Examples of such products include: Jakarta Tomcat, BEA WebLogic, IBM WebSphere, etc.

The documentation included in the CD provides instructions for deployment on each of these servers. You will find these instructions in `docs/index.html` sub-topic "Deploying Select Federation."

## Integrating Select Access with Select Federation

Select Federation depends upon Select Access for authentication. Therefore, it is important to configure and set apropriate protection for the Select Federation resources in the Select Access Policy Builder. This section explains how to do that

Integrating Select Acces with Select Federation primarily centers around five tasks:

- **Configuring the Enforcer**: Since Select Federation uses the generic enforcer, it needs to be configured. The default name of the enforcer used by Select Federation is "servlet". Refer to the chapter titled "Configuring the Enforcer Plugins" in the *Select Access Installation Guide* for instructions on configuring a Generic 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 "Integrated Windows". For details see section "To Configure the Federation Authentication Server."

> Even if you are running on a non-Windows platform, this Authentication Server type needs to be created.

- **Logout rule:** To enable users to perform global logouts in a federated environment, a special logout rule needs to be created in Select Access. For details, see section "To Create a Logout Rule."
- **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. For details, see section "To Add Select Federation Resources to the Policy Matrix."
- **Access policies:** Select Federation assets need to be protected with the appropriate combination of access policies that authorize identity entitlements accordingly. For details, see section "To Authorize Identity Entitlements with Access Policies".

The following section documents how to configure this authentication service. If you already have configured and Integrated Windows 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.
3. Click **Add**. The **Authentication Servers** dialog appears.
4. Click the **Integrated Windows** option and name the server "`federation`".
5. Click **Ok**. The **New Integrated Windows 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 Select Federation Resources to the Policy Matrix

1. In the Select Access Policy Builder, create a new Select Federation service on the Resources Tree, and name it appropriately for your deployment. 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.

3 The resource list is automatically saved to *${SF_HOME}/config/sf-URLs.txt*.

4 The **sf-URLs.txt** 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*.

5 When you are finished you will have created entries that look like the Figure 3.1.

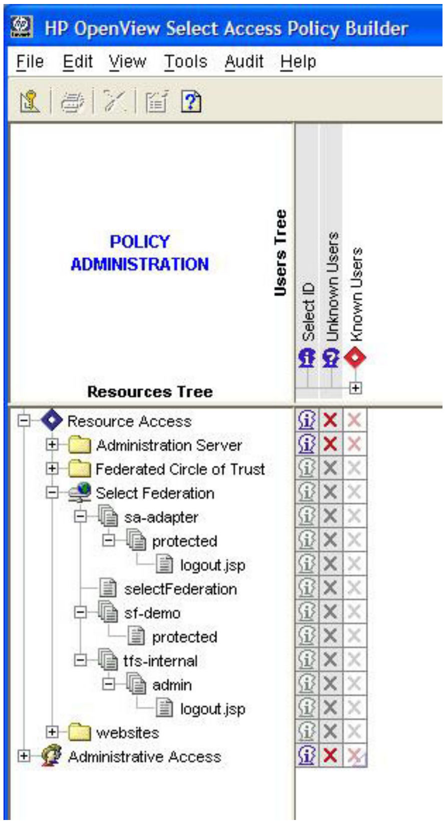


Figure 3-1: Nested Select Federation Resources

## To Authorize Identity Entitlements with Access Policies

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

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

3. In the **Select ID 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 ID column and the newly-created `logout.jsp` resource under `sa-adapter/protected` intersect.
7. From the popup menu click, **Disable Select ID**.
8. Right-click the cell where the Unknown Users 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.
11. Right-click the cell where the Select ID column and the newly-created `selectFederation` resource intersect.
12. From the popup menu click, **Enable Select ID**. The **Select ID Properties** dialog will appear.
13. In the **Select ID 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.
14. Right-click the cells where your federation-capable users and the newly-created `selectFederation` resource intersect. In this example, we will be enabling users in the IDP folder.
15. From the popup menu, click **Allow Access**.
16. Right-click the cell where the **Select ID** column and the newly-created `sf-demo` resource intersect.
17. From the popup menu click, **Enable Select ID**. The **Select ID Properties** dialog appears.
18. 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.
19. 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.

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

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

22 From the popup menu click, **Enable Select ID**. The **Select ID Properties** dialog appears.

23 Click **Add** to configure the authentication service that will be used to authenticate **Select Federation** administrators – you could use password, certificate, SecurID, Radius, etc.

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

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

26 Right-click all cells for users who are administrators and the newly-created admin resource intersect. In this example, we will be enabling the user in the IDP folder named "System Administrator".

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

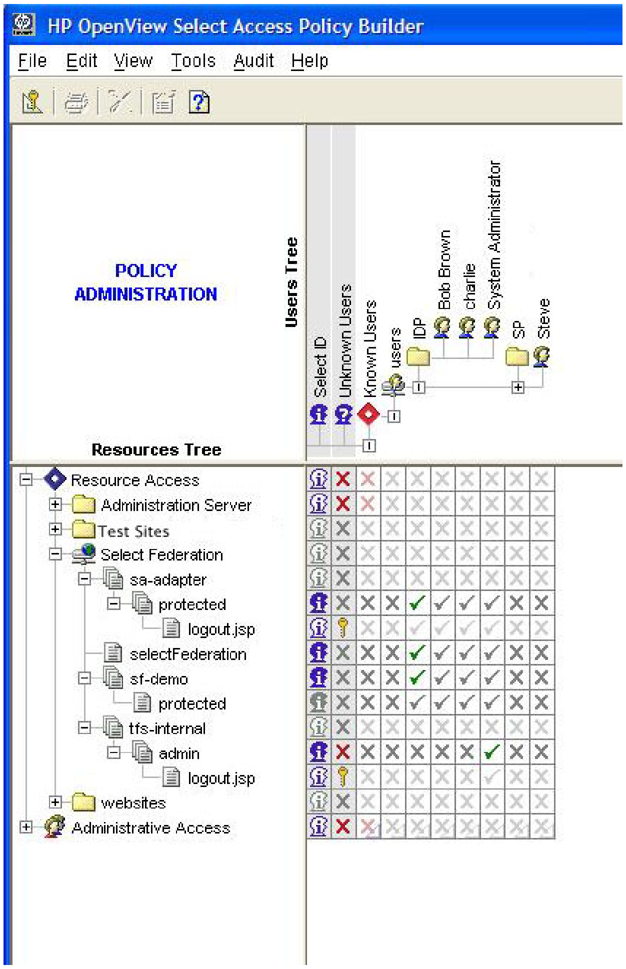
Alternatively, you can create a group for all identities with Select Federation administration entitlements. That way you only need to assign one cell an allow policy. For details on how to create groups, see chapter 4 of the *HP OpenView Select Access Policy Builder User's Guide*.

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

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

30 >From the popup menu click, **Conditional Access**. The **Conditional Rule Selection** dialog appears. Click the **Logout** rule you created earlier in this integration process.

31 When you are finished, your **Policy Matrix** should look similar to that shown in Figure 3-2.


HP OpenView Select Access Policy Builder
File Edit View Tools Audit Help
POLICY
ADMINISTRATION
Users Tree
Resources Tree

| | Select ID | Unknown Users | Known Users | users | IDP | Bob Brown | charlie | System Administrator | SP | Steve |
|---|---|---|---|---|---|---|---|---|---|---|
| Resource Access | ⓘ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Administration Server | ⓘ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Test Sites | ⓘ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Select Federation | ⓘ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| sa-adapter | ⓘ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| protected | ⓘ | ✗ | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ |
| logout.jsp | ⓘ | 🔑 | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ |
| selectFederation | ⓘ | ✗ | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ |
| sf-demo | ⓘ | ✗ | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ |
| protected | ⓘ | ✗ | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ |
| tfs-internal | ⓘ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| admin | ⓘ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| logout.jsp | ⓘ | 🔑 | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| websites | ⓘ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Administrative Access | ⓘ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

Figure 3-2: Completed Policy Matrix with Select Federation Resources

# Configuring Trusted Sites

Chapter 6 of this guide, entitled “ Adding Trusted Partner Sites to Your Federation,” describes how you can configure trusted sites. Select Federation can simultaneously act as a Liberty Service Provider, Liberty Identity Provider, SAML Consumer or SAML Provider. You can configure trusted partner sites to communicate over any of these protocols.

# Using the Application Helper

For ease of integration into your existing environment Select Federation provides a special Application Helper component. The Application helper is available 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 websites. 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.

4

# Navigating the Select Federation Management Console

Select Federation provides a Management Console that allows the root administrator to add and configure additional delegated administrators to Select Federation, and to monitor the activities of these delegated administrators and the enable end-users.

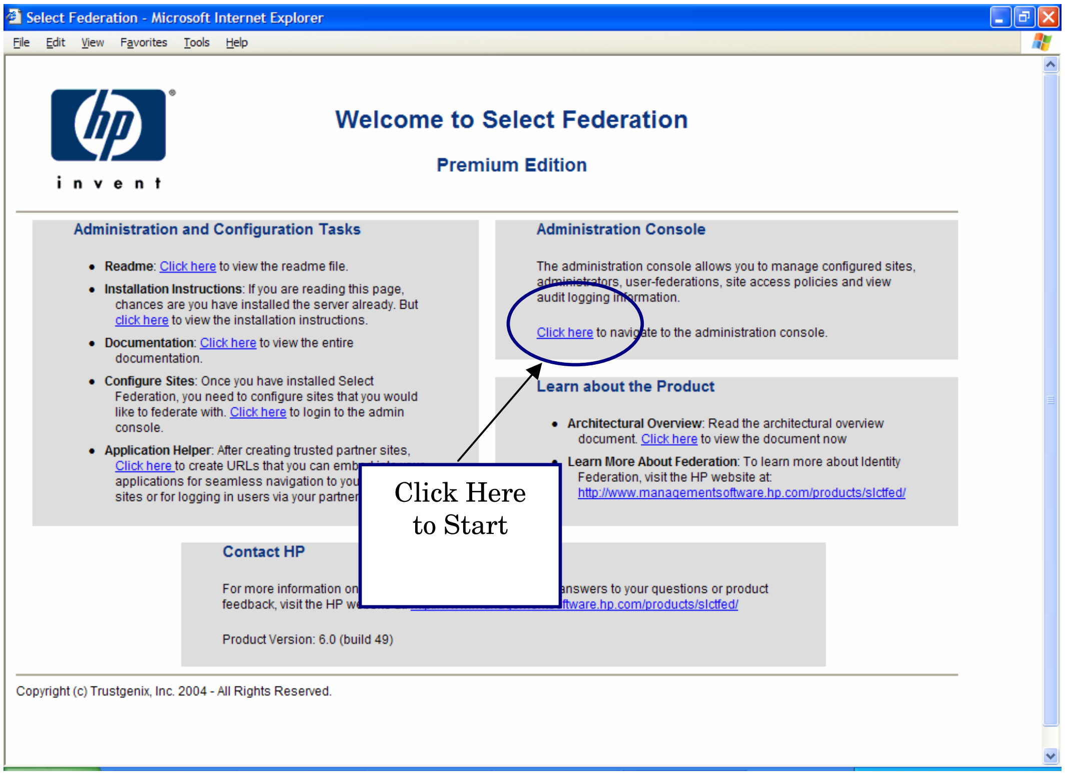
## Running the Management Console

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 welcome page that has pointers to the documentation and various resources.  It also includes a link to the “Administrative Console”, as shown in Figure 4-1.



## Welcome to Select Federation

Premium Edition

### Administration and Configuration Tasks

- **Readme**: Click here to view the readme file.
- **Installation Instructions**: If you are reading this page, chances are you have installed the server already. But click here to view the installation instructions.
- **Documentation**: Click here to view the entire documentation.
- **Configure Sites**: Once you have installed Select Federation, you need to configure sites that you would like to federate with. Click here to login to the admin console.
- **Application Helper**: After creating trusted partner sites, Click here to create URLs that you can emb
applications for seamless navigation to you
sites or for logging in users via your partner

### Administration Console

The administration console allows you to manage configured sites, administrators, user-federations, site access policies and view audit logging information.

Click here to navigate to the administration console.

### Learn about the Product

- **Architectural Overview**: Read the architectural overview document. Click here to view the document now
- **Learn More About Federation**: To learn more about Identity Federation, visit the HP website at: http://www.managementsoftware.hp.com/products/slctfed/

### Contact HP

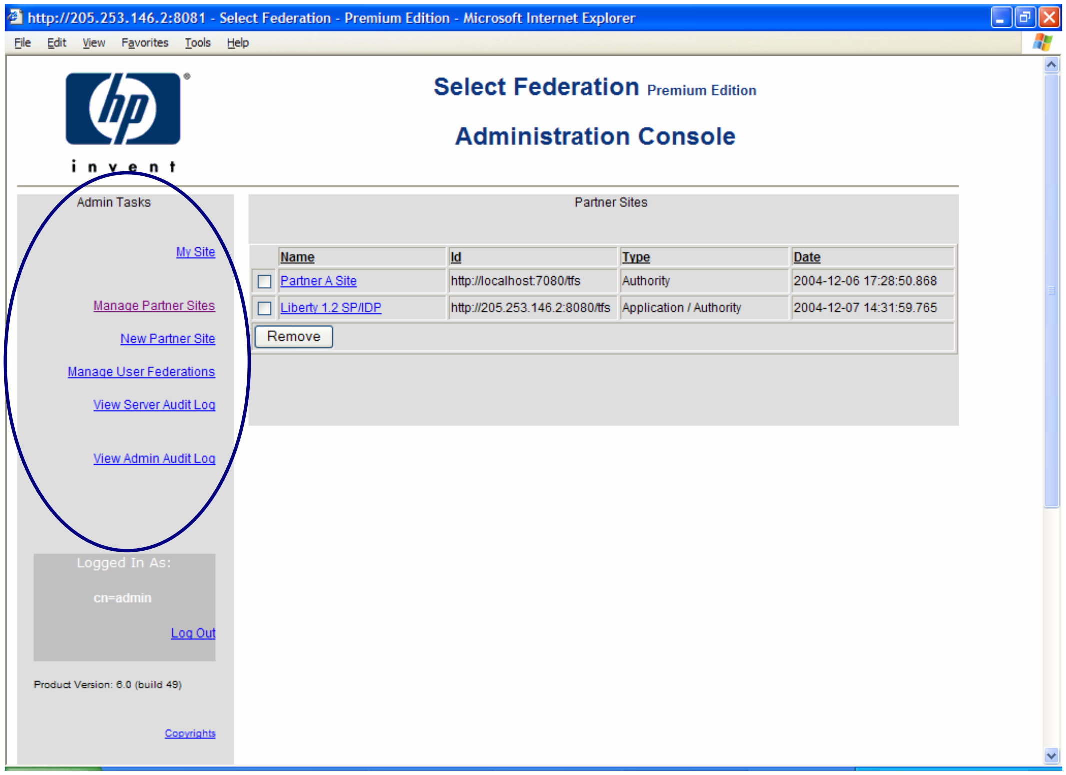
For more information on answers to your questions or product feedback, visit the HP w ftware.hp.com/products/slctfed/

Product Version: 6.0 (build 49)

Copyright (c) Trustgenix, Inc. 2004 - All Rights Reserved.

Click Here to Start

**Figure 4-1: Select Federation Welcome Page**



| | Name | Id | Type | Date |
|---|---|---|---|---|
| □ | Partner A Site | http://localhost:7080/tfs | Authority | 2004-12-06 17:28:50.868 |
| □ | Liberty 1.2 SP/IDP | http://205.253.146.2:8080/tfs | Application / Authority | 2004-12-07 14:31:59.765 |

**Figure 4-2: Select Federation Administration Console**

# Understanding Admin Tasks Sidebar Options

On the left-pane of the Management Console is the Admin Tasks Sidebar (see Figure 4-2) 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:

**My Site** - Allows you to describe your site to another site in order to set up a federation. A federation is a group of organizations that securely share user identity information outside of their firewalls using open standards protocols. A federation initially comprises of a corporation, and its external business partners, customers, and/or vendors. You may download the <meta-data> 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. For the SAML 1.0, SAML 1.1 and Liberty ID-FF 1.1 protocols, you may download the meta-data in any of the following formats.

- If you want your site to act as an Authority, download the meta-data for the Authority / IDP.
- If you want your site to act as an application, download the meta-data for the Application / SP.

The Liberty ID-FF 1.2 meta-data has an option to download both Application and Authority information in one file.

**Manage Partner Sites** – Allows you to view the details of each site with which you have a federation, edit the details of each site, and remove and/or change the configuration.

**New Partner Site** – Allows you to enter a new partner site with which you are creating a federation

**Manage User Federations** – Allows you to see all of the users that are federated with your sites. Search by user name or if you want to see all of your existing federations, leave the box blank and select the <Enter> key.

**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.

# Key Root Administrator Features

Select Federation has a number of helpful, simple-to-use monitoring 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 provider 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

## 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 provider 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

**To date** – Specified as MM-DD-YYYY

5

# Setting Up Your Federations

Your federation is the set of websites 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.

## 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 meta-data 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 as well as an 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 meta-data. 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 Meta-data on Federation

Meta-data 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, the meta-data 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 meta-data specification or just a convention in the community about how to define the meta-data. In Select Federation, the management console enables an administrator to publish the site's meta-data as well as import other sites' meta-data.

# Exchanging Meta-data with Your Partners

To add Trusted Partner sites to your federation, both you and your Trusted Partner need to upload each other's the meta-data. Meta-data exchange is mutual, so you need to ensure that the other site(s) has added your meta-data to its federation. The sections that follow describe how you can forward relevant data to your partner. For details on how to use meta-data forwarded to you from a partner, see Chapter 6.

As described in "Sending Your Meta-Data to Your Trusted Partner" below, you can download the meta-data into a meta-data file and send this file to your Trusted Partner, or send the partner the information for manual entry.

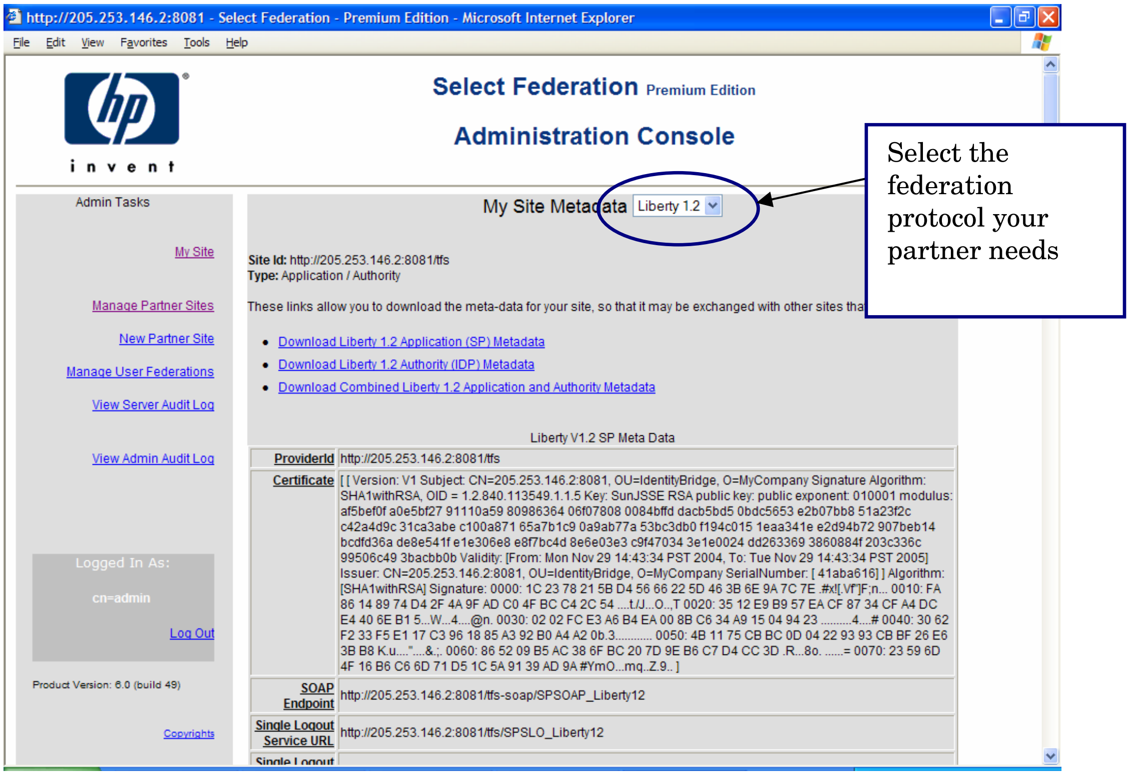
You will need to know the protocol and protocol version that the Trusted Partner site is capable of, i.e. you need to select the type of federation you would like to set up:

- For Liberty ID-FF 1.2, see "Downloading your Site's Meta-Data for a Liberty ID-FF 1.1 or ID-FF 1.2 Federation"
- For Liberty ID-FF 1.1, see "Downloading your Site's Meta-Data for a Liberty ID-FF 1.1 or ID-FF 1.2 Federation"
- For SAML 1.1, see "Downloading your Site's Meta-Data for a SAML 1.1 or SAML 1.0 Federation"
- For SAML 1.0, see "Downloading your Site's Meta-Data for a SAML 1.1 or SAML 1.0 Federation"

## Sending Your Meta-Data to Your Trusted Partner

Select Federation has simplified the process of obtaining your meta-data for all the popular federation protocols. With one click, you can download your site information into any of the needed 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 meta-data, simply click on the "My Site" link in the Admin Tasks Sidebar (left pane of the management console). You will be directed to a web page that looks like the one in Figure 5-1.  This page allows you to download the meta-data in the protocol format that your partner needs, and shows you the details of your site in the selected protocol.



**Site Id:** http://205.253.146.2:8081/tfs
**Type:** Application / Authority

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

- Download Liberty 1.2 Application (SP) Metadata
- Download Liberty 1.2 Authority (IDP) Metadata
- Download Combined Liberty 1.2 Application and Authority Metadata

Liberty V1.2 SP Meta Data

| | |
|---|---|
| ProviderId | http://205.253.146.2:8081/tfs |
| Certificate | [ [ Version: V1 Subject: CN=205.253.146.2:8081, OU=IdentityBridge, O=MyCompany Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5 Key: SunJSSE RSA public key: public exponent: 010001 modulus: af5bef0f a0e5bf27 91110a59 80986364 06f07808 0084bffd dacb5bd5 0bdc5653 e2b07bb8 51a23f2c c42a4d9c 31ca3abe c100a871 65a7b1c9 0a9ab77a 53bc3db0 f194c015 1eaa341e e2d94b72 907beb14 bcdfd36a de8e541f e1e306e8 e8f7bc4d 8e6e03e3 c9f47034 3e1e0024 dd263369 3860884f 203c336c 99506c49 3bacbb0b Validity: [From: Mon Nov 29 14:43:34 PST 2004, To: Tue Nov 29 14:43:34 PST 2005] Issuer: CN=205.253.146.2:8081, OU=IdentityBridge, O=MyCompany SerialNumber: [ 41aba616] ] Algorithm: [SHA1withRSA] Signature: 0000: 1C 23 78 21 5B D4 56 66 22 5D 46 3B 6E 9A 7C 7E .#x![.Vf"]F;n... 0010: FA 86 14 89 74 D4 2F 4A 9F AD C0 4F BC C4 2C 54 ....t./J...O..,T 0020: 35 12 E9 B9 57 EA CF 87 34 CF A4 DC E4 40 6E B1 5...W...4....@n. 0030: 02 02 FC E3 A6 B4 EA 00 8B C6 34 A9 15 04 94 23 ..........4....# 0040: 30 62 F2 33 F5 E1 17 C3 96 18 85 A3 92 B0 A4 A2 0b.3............ 0050: 4B 11 75 CB BC 0D 04 22 93 93 CB BF 26 E6 3B B8 K.u...."....&.;. 0060: 86 52 09 B5 AC 38 6F BC 20 7D 9E B6 C7 D4 CC 3D .R...8o. ......= 0070: 23 59 6D 4F 16 B6 C6 6D 71 D5 1C 5A 91 39 AD 9A #YmO...mq..Z.9.. ] |
| SOAP Endpoint | http://205.253.146.2:8081/tfs-soap/SPSOAP_Liberty12 |
| Single Logout Service URL | http://205.253.146.2:8081/tfs/SPSLO_Liberty12 |
| Single Logout | |

Select the federation protocol your partner needs

**Figure 5-1:  To Download Your Meta-Data to Send to Your Partner**

## Downloading your Site’s Meta-Data 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 meta-data file that will be sent to your trusted partner:

1 Click **My Site** 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 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**.

4 The ID-FF 1.2 protocol allows for both the Authority Site and Application Site to be described in one meta-data file.  To select this, click **Download Combined Liberty 1.2 Application and Authority Metadata**.

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 meta-data file.

## Downloading your Site's Meta-Data for a SAML 1.1 or SAML 1.0 Federation

Select Federation uses meta-data exchange with your trusted partner in order to set up the SAML federation. Only Select Federation and Trustgenix IdentityBridge™ have this easy configuration approach. SAML 1.0 and SAML 1.1 federation software from other identity management vendors does not have the meta-data capability and requires manual entry to set up the federation.

The SAML protocols (versions 1.1 and 1.0) do not support a meta-data format yet, but SAML 2.0 will support meta-data. Since SAML does not define a meta-data format, HP uses an extended form of the Liberty 1.2 meta-data to put the SAML specific information in a meta-data file.

### My Trusted Partner is Using Select Federation or Trustgenix IdentityBridge™ for SAML

If your partner is using Select Federation or Trustgenix IdentityBridge, you will be able to easily create and exchange your meta-data. You start by creating your meta-data file that will be sent to your trusted partner:

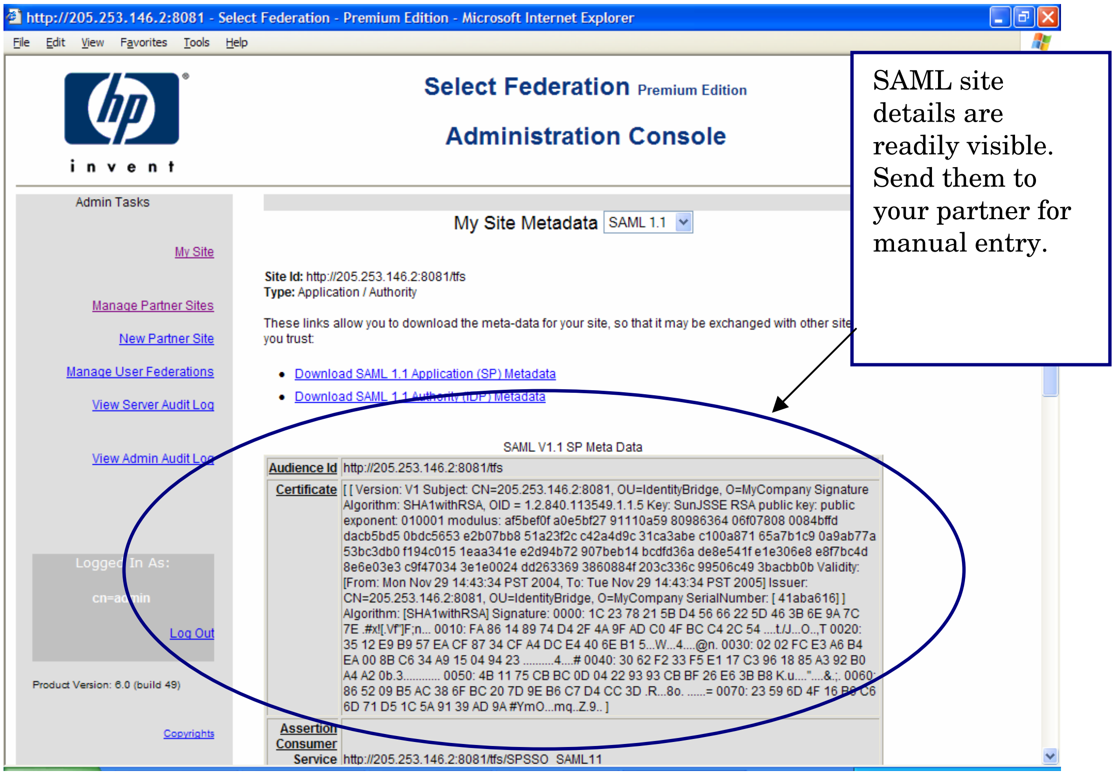
1. Click **My Site** under the Admin Tasks side bar.
2. Select the SAML protocol that you and your partner have agreed to use, either SAML 1.0 or SAML 1.1.
3. If your site will be the SAML Consumer or Application Site, click **Download SAML 1.X Application (SP) Metadata**. If your site will be the SAML Producer or Authority Site, click **Download SAML 1.X Authority (IDP) Metadata**.

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 meta-data file.

### My Trusted Partner is NOT Using Select Federation or Trustgenix IdentityBridge™ for SAML

Select Federation uses a modified version of the Liberty 1.2 meta-data format to encode information that unambiguously describes a SAML responder and can be automatically uploaded. Unfortunately, except for Select Federation and Trustgenix IdentityBridge™, the other federated identity management solutions do not support a meta-data format so the meta-data information needs to be entered in manually by your partner.

As shown in Figure 5-2, the web page shows the details of your SAML site such as the Issuer Id, Certificate, Source Id, Artifact Retrieval SOAP Endpoint, and Attribute Authority SOAP Endpoint. You will need to relay this site information to your Trusted Partner to manually enter into their federated identity management system.



http://205.253.146.2:8081 - Select Federation - Premium Edition - Microsoft Internet Explorer
File Edit View Favorites Tools Help
invent

Select Federation Premium Edition

Administration Console

My Site Metadata SAML 1.1

**Site Id:** http://205.253.146.2:8081/tfs
**Type:** Application / Authority

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

- Download SAML 1.1 Application (SP) Metadata
- Download SAML 1.1 Authority (IDP) Metadata

SAML V1.1 SP Meta Data

| | |
|---|---|
| **Audience Id** | http://205.253.146.2:8081/tfs |
| **Certificate** | [ [ Version: V1 Subject: CN=205.253.146.2:8081, OU=IdentityBridge, O=MyCompany Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5 Key: SunJSSE RSA public key: public exponent: 010001 modulus: af5bef0f a0e5bf27 91110a59 80986364 06f07808 0084bffd dacb5bd5 0bdc5653 e2b07bb8 51a23f2c c42a4d9c 31ca3abe c100a871 65a7b1c9 0a9ab77a 53bc3db0 f194c015 1eaa341e e2d94b72 907beb14 bcdfd36a de8e541f e1e306e8 e8f7bc4d 8e6e03e3 c9f47034 3e1e0024 dd263369 3860884f 203c336c 99506c49 3bacbb0b Validity: [From: Mon Nov 29 14:43:34 PST 2004, To: Tue Nov 29 14:43:34 PST 2005] Issuer: CN=205.253.146.2:8081, OU=IdentityBridge, O=MyCompany SerialNumber: [ 41aba616] ] Algorithm: [SHA1withRSA] Signature: 0000: 1C 23 78 21 5B D4 56 66 22 5D 46 3B 6E 9A 7C 7E .#x![.Vf"]F;n... 0010: FA 86 14 89 74 D4 2F 4A 9F AD C0 4F BC C4 2C 54 ....t./J...O..,T 0020: 35 12 E9 B9 57 EA CF 87 34 CF A4 DC E4 40 6E B1 5...W...4....@n. 0030: 02 02 FC E3 A6 B4 EA 00 8B C6 34 A9 15 04 94 23 ..........4....# 0040: 30 62 F2 33 F5 E1 17 C3 96 18 85 A3 92 B0 A4 A2 0b.3............ 0050: 4B 11 75 CB BC 0D 04 22 93 93 CB BF 26 E6 3B B8 K.u...."....&.;. 0060: 86 52 09 B5 AC 38 6F BC 20 7D 9E B6 C7 D4 CC 3D .R...8o. ......= 0070: 23 59 6D 4F 16 B0 C6 6D 71 D5 1C 5A 91 39 AD 9A #YmO...mq..Z.9.. ] |
| **Assertion Consumer Service** | http://205.253.146.2:8081/tfs/SPSSO_SAML11 |

SAML site details are readily visible. Send them to your partner for manual entry.

**Figure 5-2: SAML Site Details are Easily Visible to be Sent to Your Trusted Partner**

6

# Adding Trusted Partner Sites to Your Federation

To add Trusted Partner sites to your federation, you need to have the meta-data for those Trusted Partner sites. Meta-data exchange is mutual, so you need to ensure that the other site(s) has added your meta-data to its federation. For more information on meta-data, see “Understanding the Impact of Meta-data on Federation” in the previous chapter.

There are two ways to obtain data from your partners:

1 Download the meta-data of a site from a well-known URL.

2 Obtain them securely from the administrator of the peer site.

Irrespective of the method for obtaining meta-data you  use, you will also need to know the protocol and protocol version that the peer site is capable of. That is, Select Federation requires that you select the type of federation you would like to set up:

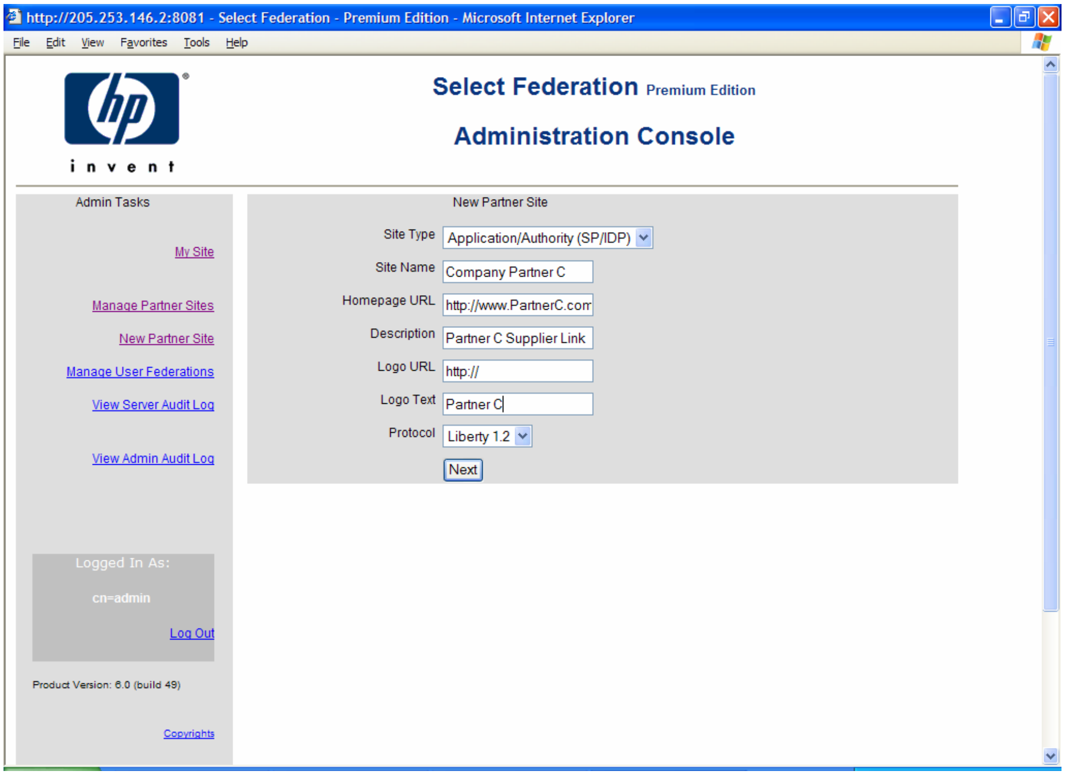
- For Liberty ID-FF 1.2, see ”To Set Up a New Federation Site Using Liberty ID-FF 1.1 or ID-FF 1.2.”
- For Liberty ID-FF 1.1, see “To Set Up a New Federation Site Using Liberty ID-FF 1.1 or ID-FF 1.2”
- For SAML 1.1, see “To Set Up a New Federation Site using SAML 1.1 or SAML 1.0”
- For SAML 1.0, see “To Set Up a New Federation Site using SAML 1.1 or SAML 1.0”

## To Set Up a New Federation Site Using Liberty ID-FF 1.1 or ID-FF 1.2

To create the new federation, you will need your partner’s meta-data file so that you can upload this information into your Select Federation. Once you have the meta-data file of your peer site, click **New Partner Site** on the Admin Tasks side bar and you will be directed to a web page that looks like the one in Figure 6-1.

1 First, select the role of your Trusted Partner's site under the **Site Type** – either an Application, Authority Site, or Both.

- If your site is an authority site or Identity Provider, then your Trusted Partner is the application site or the Service Provider. **Select Application (SP)** as the Site Type for the site you are adding.
- If your site is an application site or Service Provider, then specify **Authority (IDP)** as the Site Type for the Trusted Partner site you are adding.
- To import both authority site and application site data in the same meta-data file, you and your partner need to use the Liberty ID-FF 1.2 protocol. If your Partner is using this protocol, then you can select **Application/Authority (SP/IDP)** for the Trusted Partner site you are adding.



Site Type: Application/Authority (SP/IDP)

Site Name: Company Partner C

Homepage URL: http://www.PartnerC.com

Description: Partner C Supplier Link

Logo URL: http://

Logo Text: Partner C

Protocol: Liberty 1.2

**Figure 6-1: To Set up New Liberty Federation, Enter A Brief Description of Your Trusted Partner's Site**

2 In the **Site Name** field, you can assign any "friendly name" to describe your partner's site on your HP administration console. Enter the **Site Name** as you would like it to appear in your system. You must enter data into this field.

## Optional Fields

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.

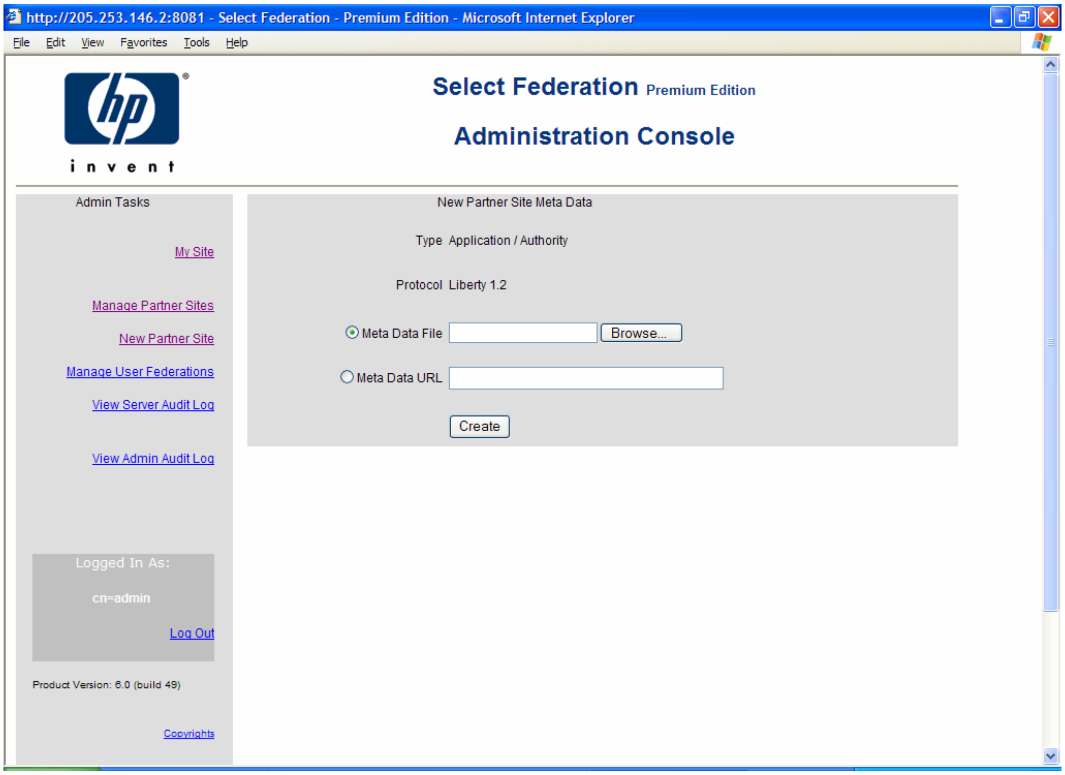
The **Homepage URL** is your partner's URL that users should be directed to when they use the federated link.

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 Trusted 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.

3 In the **Protocol** field, select the federation open standard that you and your partner agreed to use for this link – either Liberty 1.2 or Liberty 1.1. Click <Next> and you will be direct to the next web page (Figure 6-2).



http://205.253.146.2:8081 - Select Federation - Premium Edition - Microsoft Internet Explorer

Select Federation Premium Edition

Administration Console

New Partner Site Meta Data

Type Application / Authority

Protocol Liberty 1.2

● Meta Data File

○ Meta Data URL

Logged In As: cn=admin

Product Version: 6.0 (build 49)

**Figure 6-2: To Set up New Liberty Federation, Upload Your Partner's Meta-Data**

4 You can either upload your partner's meta-data file or get the information from a URL.

**Meta Data File**: Enter or browse to find the full path of the meta-data file that you received from your partner.

**Meta Data URL**: Enter the URL where the meta-data information from your partner. is stored.

5 Click **Create** to complete the creation of your federation link.

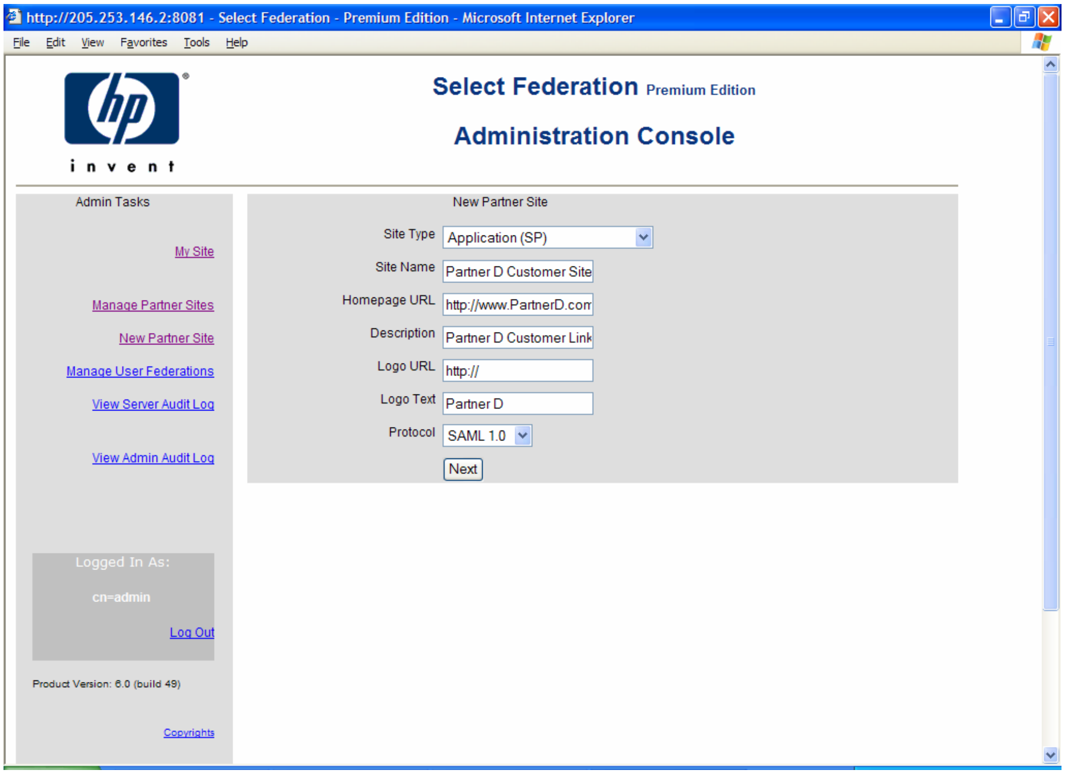
You will see a screen that shows the newly added site in the federation. To see or edit details of this new partner site, click the **Name** of the partner.

# To Set Up a New Federation Site using SAML 1.1 or SAML 1.0

As previously mentioned, SAML 1.1 and SAML 1.0 do not define a meta-data format. Select Federation uses an extended form of the Liberty 1.2 meta-data to put the SAML specific information in a meta-data file.

Only Select Federation and Trustgenix IdentityBridge™ have this easy configuration approach. SAML 1.0 and 1.1 federation software from other identity management vendors does not have the meta-data capability and requires manual entry to set up the federation.

To create the SAML federation in your system, click New Partner Site on the Admin Tasks side bar. You will be directed to a web page as shown in Figure 6-3.



New Partner Site

Site Type: Application (SP)

Site Name: Partner D Customer Site

Homepage URL: http://www.PartnerD.com

Description: Partner D Customer Link

Logo URL: http://

Logo Text: Partner D

Protocol: SAML 1.0

**Figure 6-3: Creating a New SAML Federation**

1 First, select the role of your Trusted Partner's site under the **Site Type** – either an Application or Authority Site.

- If your site is an authority site or SAML Producer, then your Trusted Partner is the application site or the SAML Consumer. Select Application (SP) as the Site Type for the site you are adding.
- If your site is an application site or SAML Consumer, then specify Authority (IDP) as the Site Type for the Trusted Partner site you are adding.

2 In the **Site Name** field, you can assign any “friendly name” to describe your partner’s site on your HP administration console. Enter the **Site Name** as you would like it to appear in your system. You must enter data into this field.

### Optional Fields

The rest of the text-fields are optional. However, if you fill in these optional fields, it will 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 **Homepage URL** is your partner’s URL that users should be directed to when they use the federated link.

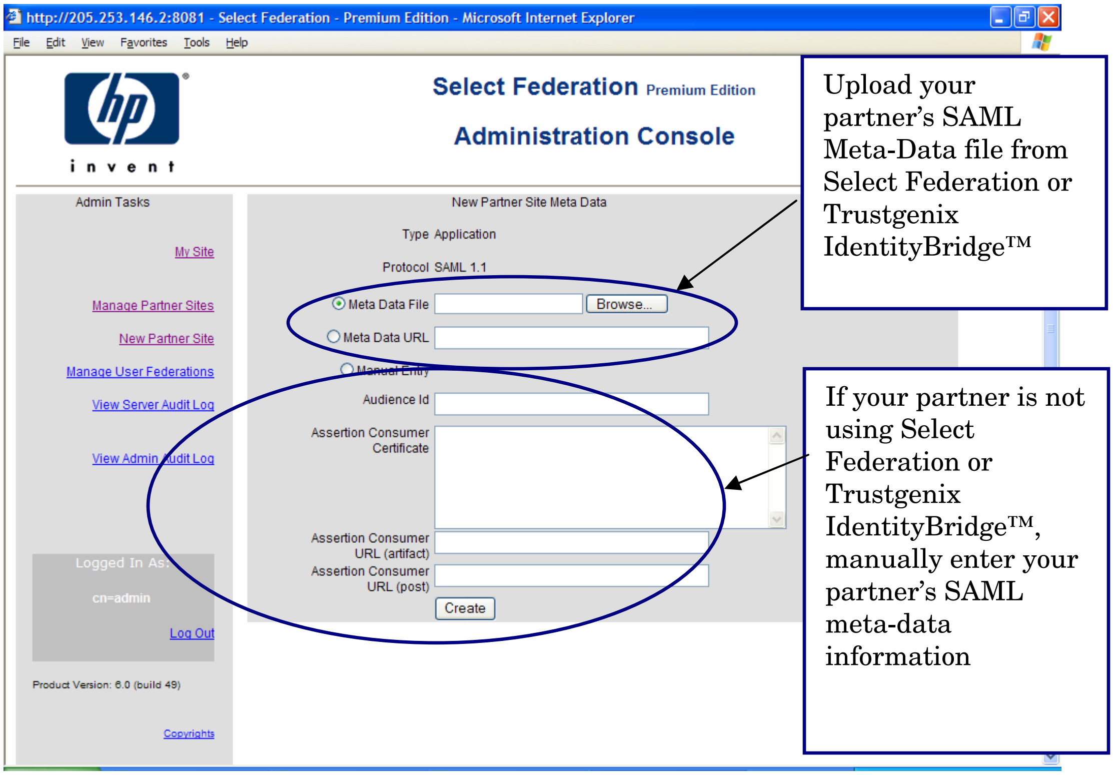
Enter a one-line **Description** of the Partner Site to which you are connecting. This is optional and can be left blank.

**Logo URL** is the logo that appears on your portal and represents the logo of the federation link you created. It can be your Trusted 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.

3 In the **Protocol** field, select the federation open standard that you and your partner agreed to use for this link – either SAML 1.0 or SAML 1.1.

4 Click <Next> and you will be direct to the next web page, which is shown in Figure 6-4.



New Partner Site 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)

Upload your partner's SAML Meta-Data file from Select Federation or Trustgenix IdentityBridge™

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

**Figure 6-4: Uploading or Entering Your Partner's Meta-Data for a New SAML Federation**

## My Trusted Partner is Using Select Federation or Trustgenix IdentityBridge™ for SAML

If your Trusted Partner is using Select Federation or Trustgenix IdentityBridge™, you can either upload your partner's meta-data file or get the information from a URL using the first or second field on the web page (see Figure 6.4).

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

Click **Create** to complete the creation of your federation link. You will see a screen that shows the newly added site in the federation.

To see or edit details of this new partner site, click the **Name** of the partner.

## My Trusted Partner is NOT Using Select Federation or Trustgenix IdentityBridge™ for SAML

If your Trusted Partner is not using Select Federation or Trustgenix IdentityBridge™, he will not be able to send you a meta-data file or a URL link. Instead, you will need to select **Manual Entry** as shown in Figure 6-4, and type in the SAML parameters for your partner's site. The parameters needed are:

- **Issuer Id**: The Unique ID that identifies this site within a list of sites trusted by your site.
- **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.

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

## Deleting Sites from Your Federation

To delete an existing federation:

1. Click **Manage Partner Sites** on the Admin Tasks sidebar to get a list of the existing federations.
2. Check the box next to the Partner name that you wish to delete.
3. Click <**Remove**>.

# Editing Your Federation Parameters

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

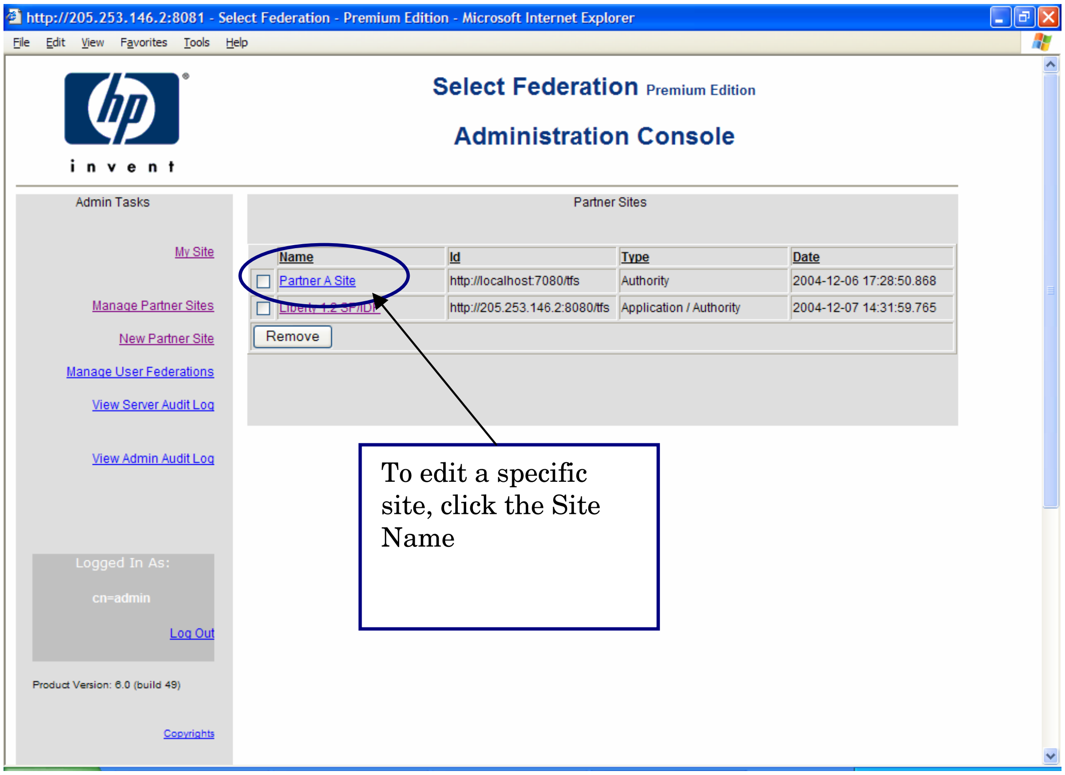
- Site Description: This describes how your partner's site appears in your system. For details, see "Editing Your Partner Site's Display Information."
- Site Federation Policy: These are the rules that you and your partner agreed to use in communicating between your sites. For details, see "Editing the Federation Policy of Your Authority Site."
- Protocol Policy: These are the actual protocol parameters, also known as meta-data, consisting of URLs for various protocol services, certificates, etc. For details, see "Updating Your Federation Protocol Policy and/or Meta-Data."

## Changing Your Site Policy

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

- View the details of each Trusted Partner site 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 7-1):



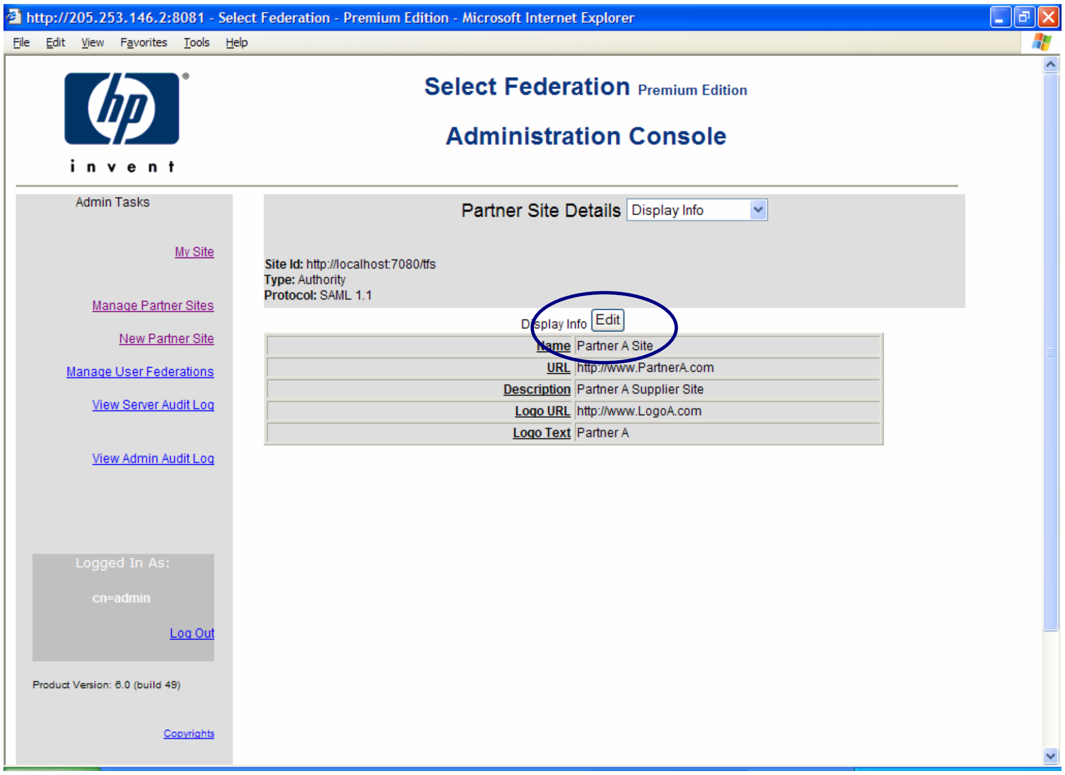
| | Name | Id | Type | Date |
|---|---|---|---|---|
| □ | Partner A Site | http://localhost:7080/tfs | Authority | 2004-12-06 17:28:50.868 |
| □ | Liberty 1.2 SP/IDP | http://205.253.146.2:8080/tfs | Application / Authority | 2004-12-07 14:31:59.765 |

To edit a specific site, click the Site Name

**Figure 7-1: Selecting the Federation to Edit**

You will be directed a web page (as shown in Figure 7-2) that has the basic information related to this Trusted Partner site:

- **Site Id** is the URL for the Trusted site with which you have a federation
- **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 1.1, SAML 1.0, Liberty 1.2, or Liberty 1.1.



Partner Site Details: Display Info

**Site Id:** http://localhost:7080/tfs
**Type:** Authority
**Protocol:** SAML 1.1

Display Info

| | |
|---|---|
| **Name** | Partner A Site |
| **URL** | http://www.PartnerA.com |
| **Description** | Partner A Supplier Site |
| **Logo URL** | http://www.LogoA.com |
| **Logo Text** | Partner A |

Logged In As:
cn=admin

Product Version: 6.0 (build 49)

**Figure 7-2: To Edit Partner Site Details**

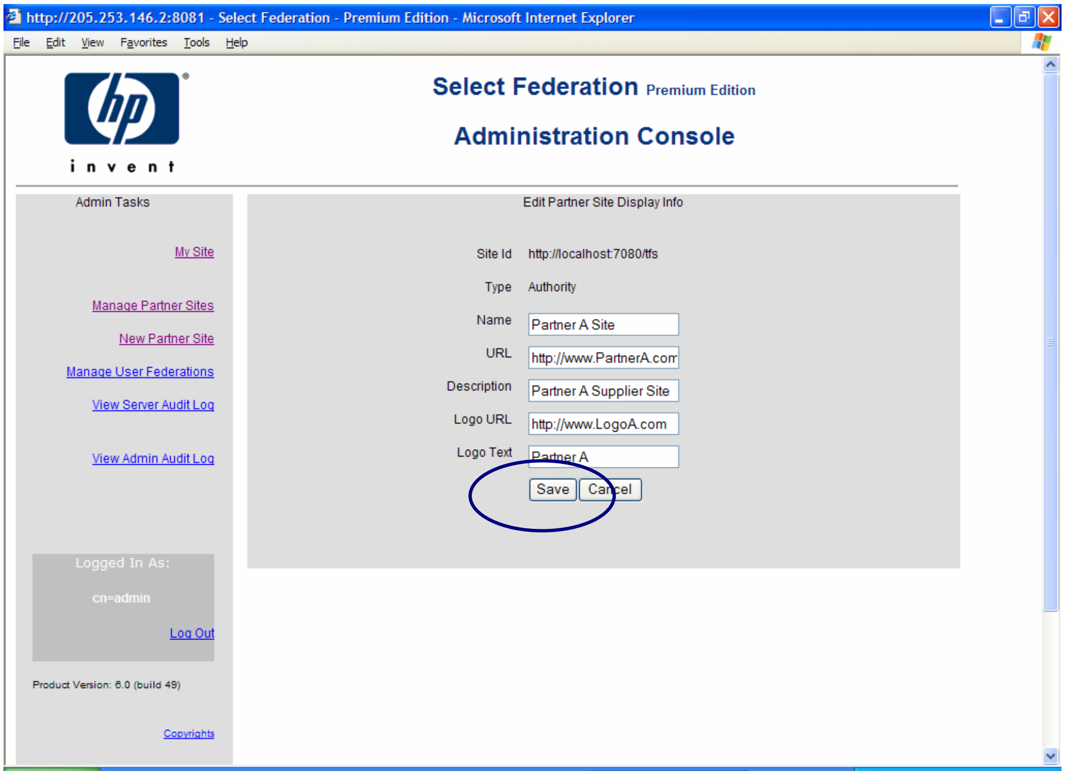
# Editing Your Partner Site's Display Information

Site Display information is the data that determine how your Trusted Partner site appears on your federation web page. This includes your partner's name, URL, and/or logo.

To change, click **Edit** button next to Display Info as shown in Figure 7-2.

- **Name** is the Site Name of your partner site, as you would like it to appear in your system.
- The **URL** is your partner's URL that you should be directed to when you use the federated link.
- Enter a one-line **Description** of the Partner Site 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 7-3) allows you to change the Name, URL, Description, Logo URL, and Logo Text that you use to distinguish your Partner site. The screen will be populated with the current partner site information. You can fill in any changes to the site information that you wish and click **Save**.



Site Id http://localhost:7080/tfs

Type Authority

Name Partner A Site

URL http://www.PartnerA.com

Description Partner A Supplier Site

Logo URL http://www.LogoA.com

Logo Text Partner A

**Figure 7-3: To Edit Site Details**

# Editing the Federation Policy of Your Authority Site

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

- **Name Federation** or the form of the user name,
- **User Consent**, and
- **Restricted Access to Group**, i.e. the User Groups that have access to this partner site are indicated with an LDAP Distinguished Name (LDAP DN).

## *Name Federation*

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

— **Local Names** are the names that the users are known by at the Identity Provider or Authority site. The Authority Site also may 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 also identifiers or tokens that are 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 Trusted Partner site, the same identifier is presented. The Service Provider or Application site will know that this user's activity at its site.

— **One Time Pseudonym** is an anonymous identifier or token (a long list of numbers) that is generated each time the user accesses a Trusted site. To keep the user anonymous to the Service Provider site, a different anonymous token is generated each time the link is used.

### *User Consent*

The first time a user goes to a new Trusted Partner Site, he has the option to consent to sending his personal information 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**.

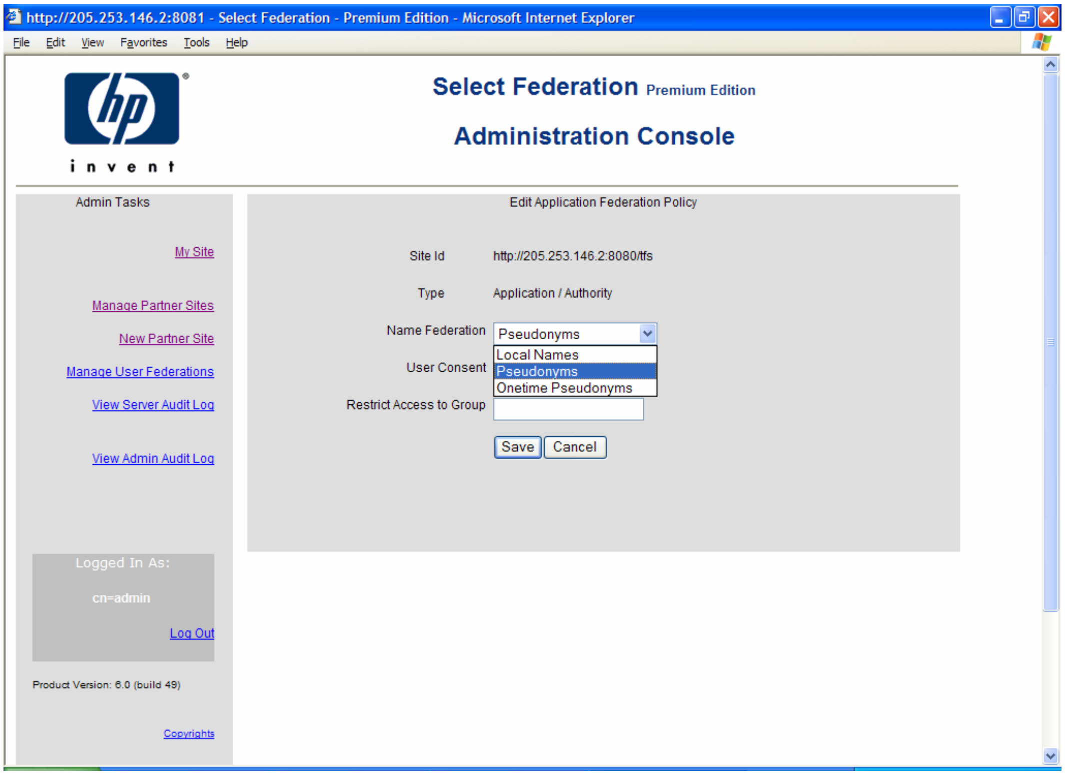
### *Restrict Access to Group*

The administrator can define an LDAP group of users who only have access to this Trusted Partner site. The user groups that have access to this partner site are indicated using an LDAP Distinguished Name (DN). This is the DN for the LDAP group of which the user must be a member in order to access that site. If you have specified a custom Directory Plugin, this parameter is passed verbatim to the `DirPlugin:isMember` method of the Directory Plugin.

> ➤ When using the Sun Directory Server, make sure that the type of group that you create in the directory is a "Role" and sets the `nsRole` attribute in the user object. Also change the value of the configuration parameter `ldapGroupMembershipAttr` to be `nsRole` in the `tfsconfig.properties` file.

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 next to **Partner Site Details**, select **Federation Policy** (as shown in Figure 7-2). 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 7-4. Make the needed changes to each of the fields and click **Save**.



Select Federation Premium Edition

Administration Console

Edit Application Federation Policy

Site Id http://205.253.146.2:8080/tfs

Type Application / Authority

Name Federation Pseudonyms

Local Names
Pseudonyms
Onetime Pseudonyms

User Consent

Restrict Access to Group

Logged In As:

cn=admin

Product Version: 6.0 (build 49)

**Figure 7-4: Edit Site Federation Policy**

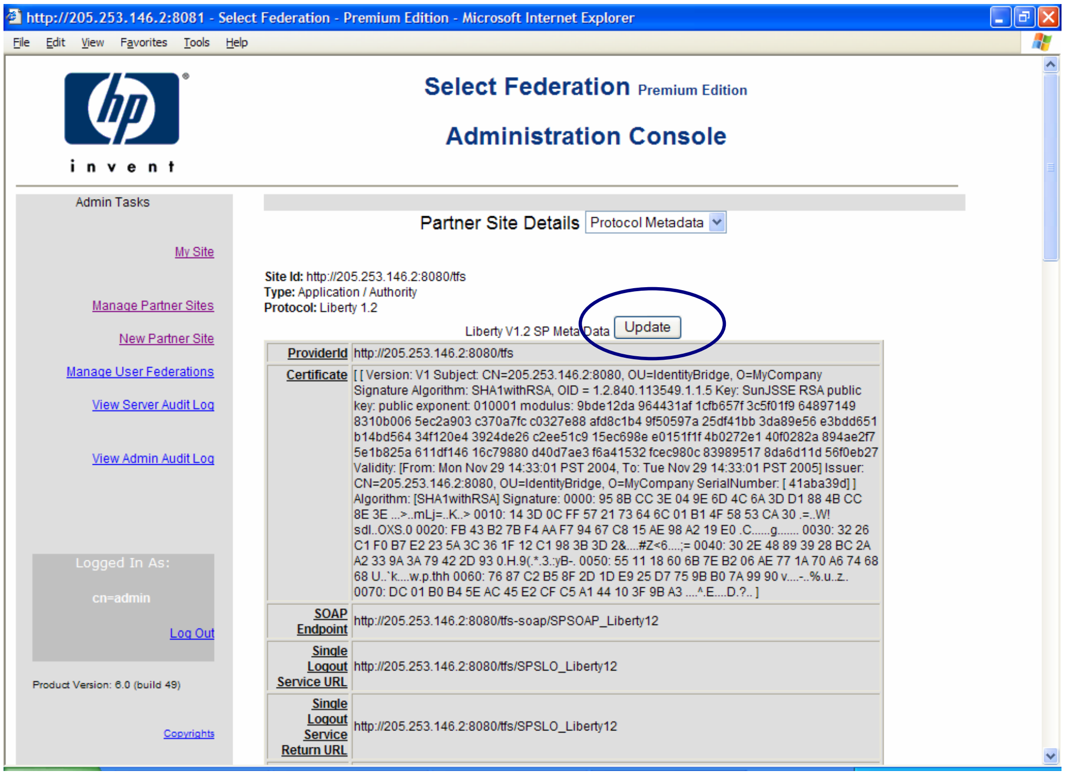
# Updating Your Federation Protocol Policy and/or Meta-Data

Select Federation makes it relatively easy to make changes to your federation's protocol policy and/or protocol meta-data. 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 Liberty Protocol Policy

Similar to setting up a new Liberty Trusted Partner, updating an existing Liberty protocol policy is relatively automated. Under Site Details (see Figure 7-2), 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 federation.

Changing any information in a Liberty federation is just a matter of uploading a new metadata file provided by your Trusted Partner. To change the metadata, click **Update** as shown in Figure 7-5.



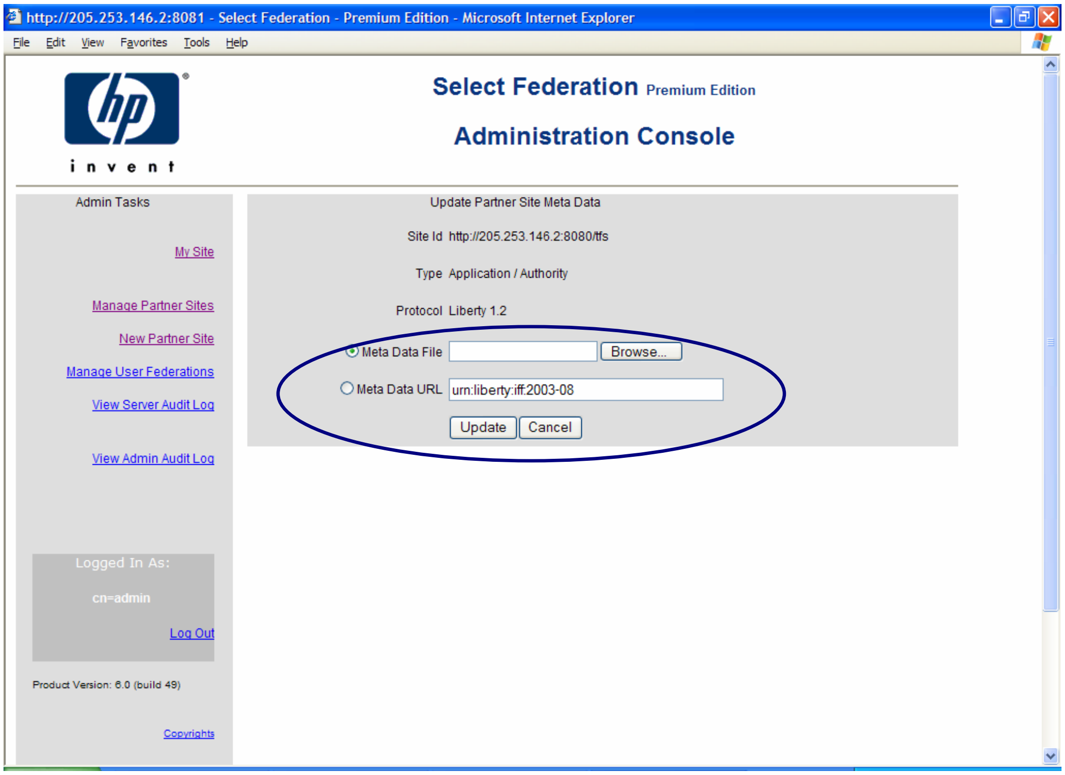
**Site Id:** http://205.253.146.2:8080/tfs
**Type:** Application / Authority
**Protocol:** Liberty 1.2

Liberty V1.2 SP Meta Data

| | |
|---|---|
| **ProviderId** | http://205.253.146.2:8080/tfs |
| **Certificate** | [ [ Version: V1 Subject: CN=205.253.146.2:8080, OU=IdentityBridge, O=MyCompany Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5 Key: SunJSSE RSA public key: public exponent: 010001 modulus: 9bde12da 964431af 1cfb657f 3c5f01f9 64897149 8310b006 5ec2a903 c370a7fc c0327e88 afd8c1b4 9f50597a 25df41bb 3da89e56 e3bdd651 b14bd564 34f120e4 3924de26 c2ee51c9 15ec698e e0151f1f 4b0272e1 40f0282a 894ae2f7 5e1b825a 611df146 16c79880 d40d7ae3 f6a41532 fcec980c 83989517 8da6d11d 56f0eb27 Validity: [From: Mon Nov 29 14:33:01 PST 2004, To: Tue Nov 29 14:33:01 PST 2005] Issuer: CN=205.253.146.2:8080, OU=IdentityBridge, O=MyCompany SerialNumber: [ 41aba39d] ] Algorithm: [SHA1withRSA] Signature: 0000: 95 8B CC 3E 04 9E 6D 4C 6A 3D D1 88 4B CC 8E 3E ...>..mLj=..K..> 0010: 14 3D 0C FF 57 21 73 64 6C 01 B1 4F 58 53 CA 30 .=..W! sdl..OXS.0 0020: FB 43 B2 7B F4 AA F7 94 67 C8 15 AE 98 A2 19 E0 .C......g....... 0030: 32 26 C1 F0 B7 E2 23 5A 3C 36 1F 12 C1 98 3B 3D 2&....#Z<6....;= 0040: 30 2E 48 89 39 28 BC 2A A2 33 9A 3A 79 42 2D 93 0.H.9(.*.3.:yB-. 0050: 55 11 18 60 6B 7E B2 06 AE 77 1A 70 A6 74 68 68 U..`k....w.p.thh 0060: 76 87 C2 B5 8F 2D 1D E9 25 D7 75 9B B0 7A 99 90 v....-..%.u..z.. 0070: DC 01 B0 B4 5E AC 45 E2 CF C5 A1 44 10 3F 9B A3 ....^.E....D.?.. ] |
| **SOAP Endpoint** | http://205.253.146.2:8080/tfs-soap/SPSOAP_Liberty12 |
| **Single Logout Service URL** | http://205.253.146.2:8080/tfs/SPSLO_Liberty12 |
| **Single Logout Service Return URL** | http://205.253.146.2:8080/tfs/SPSLO_Liberty12 |

**Figure 7-5: Changing the Metadata for a Liberty Federation**

You will then be directed to a web page as shown in Figure 7-6 where you can upload a new Liberty meta-data file by simply entering or browsing for the file path name. Alternatively, you can also enter the meta-data URL. Click **Update** when you are done.



http://205.253.146.2:8081 - Select Federation - Premium Edition - Microsoft Internet Explorer

Select Federation Premium Edition

Administration Console

Update Partner Site Meta Data

Site Id http://205.253.146.2:8080/tfs

Type Application / Authority

Protocol Liberty 1.2

● Meta Data File

○ Meta Data URL urn:liberty:iff:2003-08

Logged In As:

cn=admin

Product Version: 6.0 (build 49)

**Figure 7-6: To Update a Liberty Federation's Protocol Policy, Upload a Revised Meta Data File**

## Changing Your Partner's SAML Protocol Meta-Data and Policy

Similar to setting up a new SAML Trusted Partner, updating an existing SAML protocol policy and meta-data can be relatively automated if your Trusted Partner is using Select Federation or Trustgenix IdentityBridge™, or require manual entry of your Trusted Partner is using some other federated identity management product.

➤ Changing your SAML Protocol parameters can be a 2-step process if you need to make changed in both your Protocol Meta-Data and Protocol Policy. We recommend that you first update your Protocol Metadata, and then update your Protocol Policy.

### Updating Your SAML SP Partner's Protocol Metadata

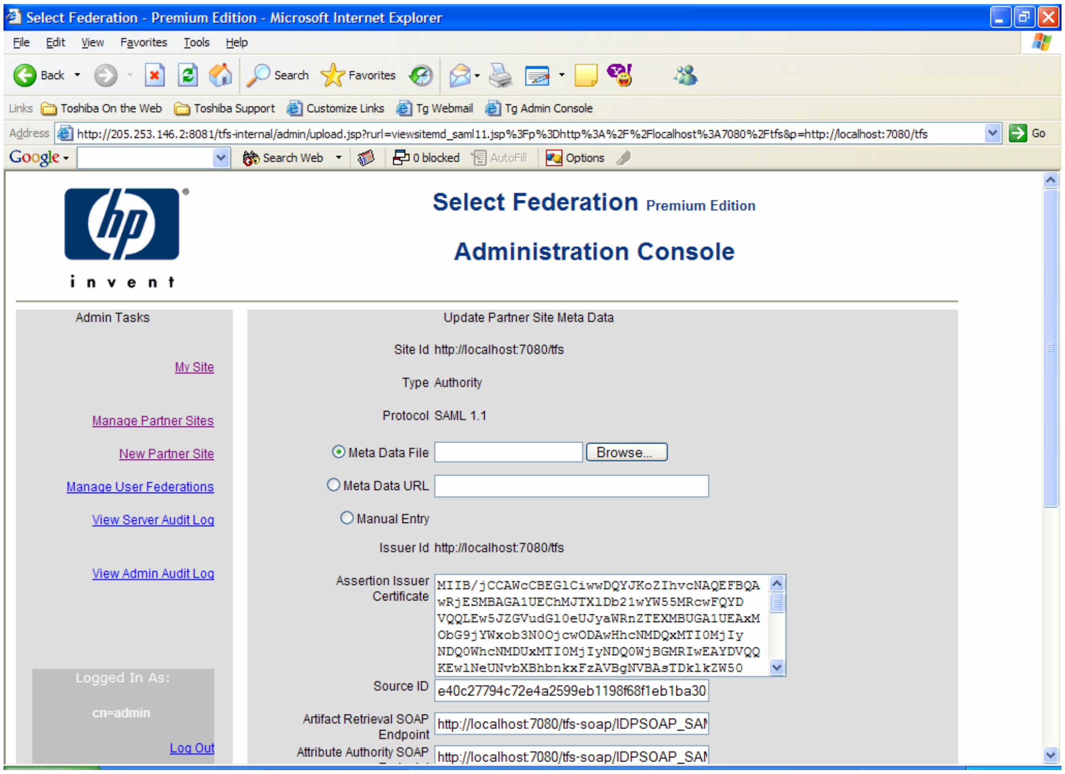
Under **Partner Site Details** (see Figure 7-2), select **Protocol Metadata**. You will be directed to a web page similar to the one in Figure 7-5 that delineates all the certificate information, protocol policy, and URLs that are needed for this SAML federation.

When you click **Update**, you will then be directed to a web page as shown in Figure 7-7 where you can update your Trusted Partner's SAML Consumer (Application Site or SP) policy information.

If your Trusted Partner is using Select Federation or Trustgenix IdentityBridge™, you can either upload your partner's meta-data file or get the information from a Meta Data URL using the first or second field on the web page as shown in Figure 7-7.

When your Trusted Partner is not using Select Federation or Trustgenix IdentityBridge™, due to the lack of meta-data usage in the SAML specifications, you will need to enter some data manually to update the SAML protocol policy. You will need to get the new protocol policy information from your Trusted Partner. For an application site (Figure 7-7), make any needed changes to the:

- **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. The
- **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



Update Partner Site Meta Data

Site Id http://localhost:7080/tfs

Type Authority

Protocol SAML 1.1

● Meta Data File [ ] Browse...

○ Meta Data URL [ ]

○ Manual Entry

Issuer Id http://localhost:7080/tfs

Assertion Issuer Certificate
```
MIIB/jCCAWcCBEG1CiwwDQYJKoZIhvcNAQEFBQA
wRjESMBAGA1UEChMJTX1Db21wYW55MRcwFQYD
VQQLEw5JZGVudG10eUJyaWRnZTEXMBUGA1UEAxM
ObG9jYWxob3N0OjcwODAwHhcNMDQxMTI0MjIy
NDQ0WhcNMDUxMTI0MjIyNDQ0WjBGMRIwEAYDVQQ
KEwlNeUNvbXBhbnkxFzAVBgNVBAsTDklkZW50
```

Source ID e40c27794c72e4a2599eb1198f68f1eb1ba30

Artifact Retrieval SOAP Endpoint http://localhost:7080/tfs-soap/IDPSOAP_SAI

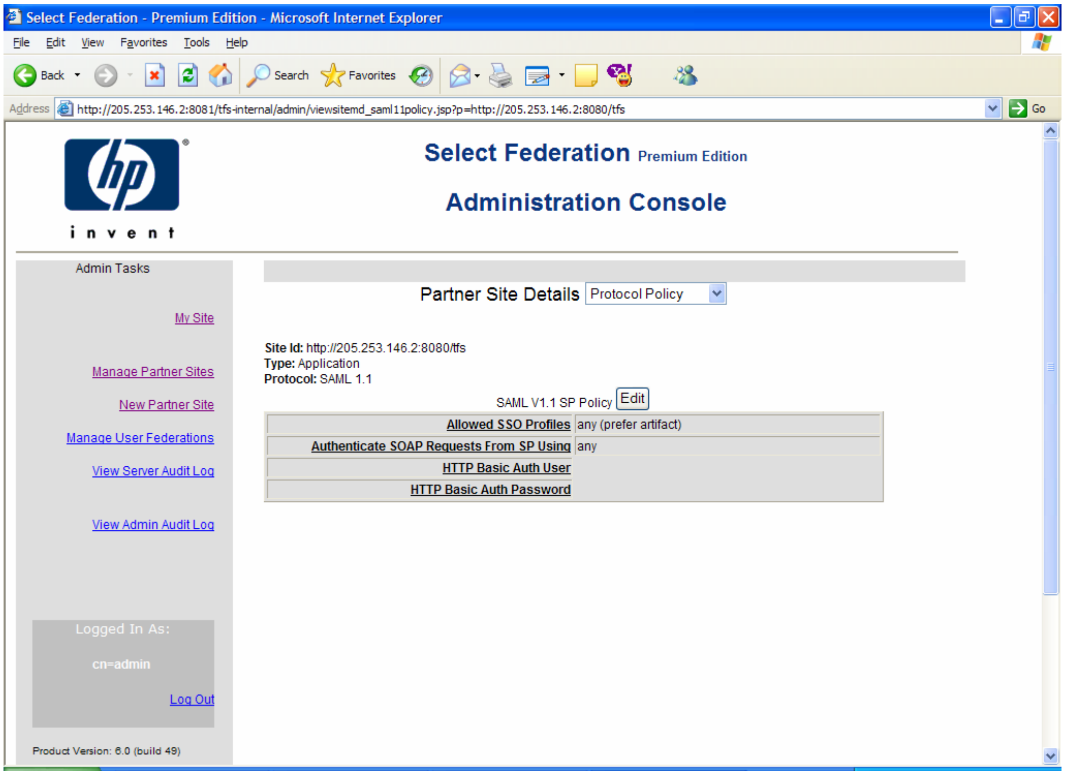
Attribute Authority SOAP http://localhost:7080/tfs-soap/IDPSOAP_SAI

**Figure 7-7: To Update a SAML Federation's Protocol Meta-Data**

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

## Updating Your SP Partner's SAML 1.x SP Policy

Select **Protocol Policy** under Partner Site Details as shown in Figure 7-2 for your SAML federation. You will be directed to a web page as shown in Figure 7-8. To make changes, click **Edit** and you will be directed to another web page as shown in Figure 7-9.



Address: http://205.253.146.2:8081/tfs-internal/admin/viewsitemd_saml11policy.jsp?p=http://205.253.146.2:8080/tfs

Partner Site Details: Protocol Policy

**Site Id:** http://205.253.146.2:8080/tfs
**Type:** Application
**Protocol:** SAML 1.1

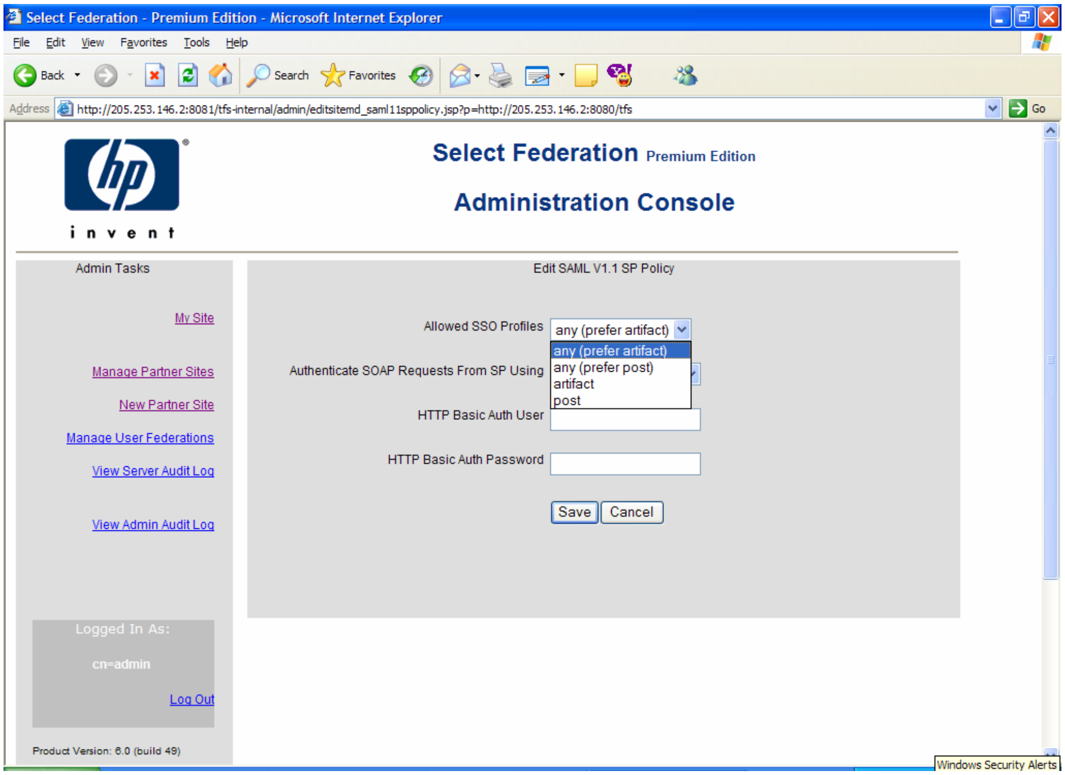
SAML V1.1 SP Policy

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

Logged In As:
cn=admin

Product Version: 6.0 (build 49)

**Figure 7-8: To Update a SAML Federation’s Protocol Policy for an Application (SP) Site**



Address: http://205.253.146.2:8081/tfs-internal/admin/editsitemd_saml11sppolicy.jsp?p=http://205.253.146.2:8080/tfs

Edit SAML V1.1 SP Policy

Allowed SSO Profiles: any (prefer artifact)

Authenticate SOAP Requests From SP Using

HTTP Basic Auth User

HTTP Basic Auth Password

Logged In As:

cn=admin

Product Version: 6.0 (build 49)

**Figure 7-9: Setting the Allowed SSO Profiles in your SAML SP Policy**

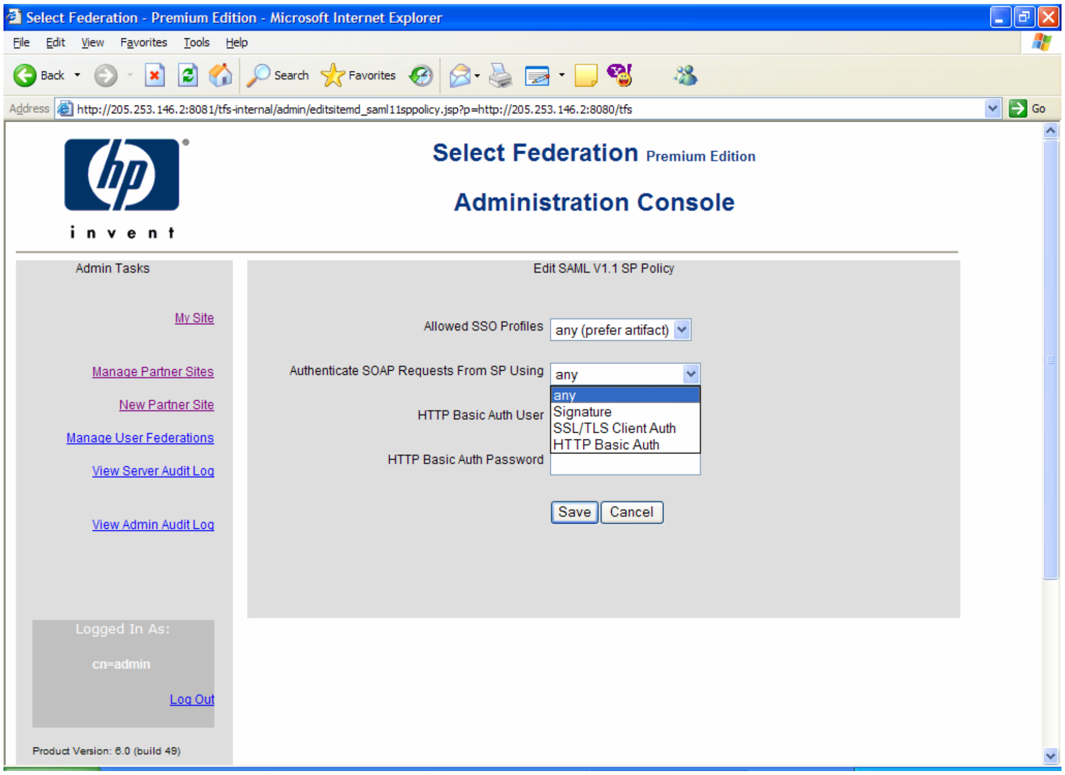
## Set the Allowed SSO Profile in Your SAML SP Policy

If your site is the SAML Producer (IDP) and you will receive artifacts from your SAML Consumer Partners (SP), you will need to set the single sign on parameters in this section of the web page (Figure 7-9). 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 (IDP) to the SAML Consumer (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 (SP) to the SAML Producer (IDP) using one of the four SOAP Authentication methods.



http://205.253.146.2:8081/tfs-internal/admin/editsitemd_saml11sppolicy.jsp?p=http://205.253.146.2:8080/tfs

Select Federation Premium Edition

Administration Console

Edit SAML V1.1 SP Policy

Allowed SSO Profiles: any (prefer artifact)

Authenticate SOAP Requests From SP Using: any

HTTP Basic Auth User

HTTP Basic Auth Password

Logged In As:

cn=admin

Product Version: 6.0 (build 49)

**Figure 7-10: Setting the SOAP Authentication Method in your SAML SP Policy**

As shown in Figure 7-10, you can **Authenticate SOAP Requests from SP Using**:

— **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 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 this authentication method, you will need to enter the desired user name and password in the fields **HTTP Basic Auth User** and **HTTP Basic Auth Password** as shown in Figure 7-10.

— **Any** of the above

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

## Updating Your SAML IDP Partner's Protocol Metadata

Under **Partner Site Details** (see Figure 7-2), select **Protocol Metadata**. You will be directed to a web page similar to the on in Figure 7-5 that delineates all the certificate information, protocol policy, and URLs that are needed for this SAML federation.

When you click **Update**, you will then be directed to a web page similar to the one shown in Figure 7-7 where you can update your Trusted Partner's SAML Producer (Authority Site or IDP) policy information.

If your Trusted Partner is using Select Federation or Trustgenix IdentityBridge™, you can either upload your partner's meta-data file or get the information from a Meta Data URL using the first or second field on the web page as shown in Figure 7-7.

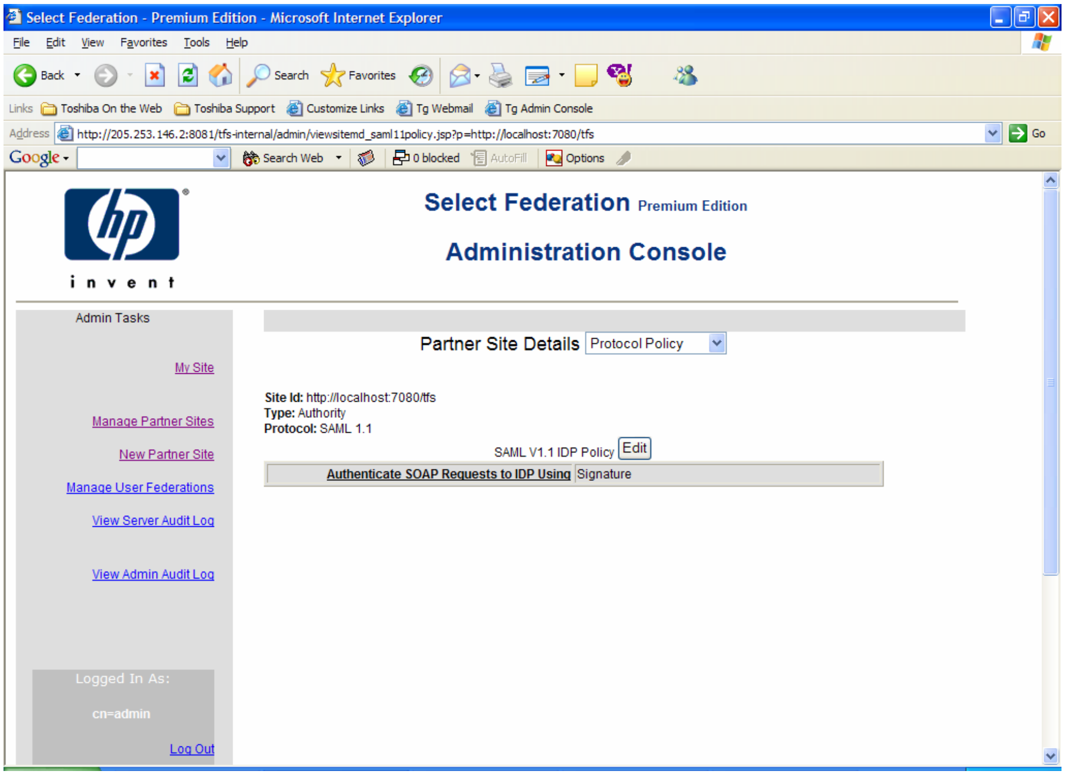
When your Trusted Partner is not using Select Federation or Trustgenix IdentityBridge™, due to the lack of meta-data usage in the SAML specifications, you will need to enter some data manually to update the SAML protocol policy. You will need to get the new protocol policy information from your Trusted Partner. For an application site (Figure 7-7), 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**.

## Updating Your IDP Partner's SAML 1.x IDP Policy

Select **Protocol Policy** under Partner Site Details (as shown in Figure 7-2) for your SAML federation. You will be directed to a web page as shown in Figure 7-11. To make changes, click **Edit** and you will be directed to another web page as shown in Figure 7-12.


Select Federation - Premium Edition - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Links Toshiba On the Web Toshiba Support Customize Links Tg Webmail Tg Admin Console
Address
Go
Google Search Web 0 blocked AutoFill Options
invent
Admin Tasks
My Site
Manage Partner Sites
New Partner Site
Manage User Federations
View Server Audit Log
View Admin Audit Log
Logged In As:
cn=admin
Log Out
Edit

http://205.253.146.2:8081/tfs-internal/admin/viewsitemd_saml11policy.jsp?p=http://localhost:7080/tfs

Select Federation Premium Edition

Administration Console

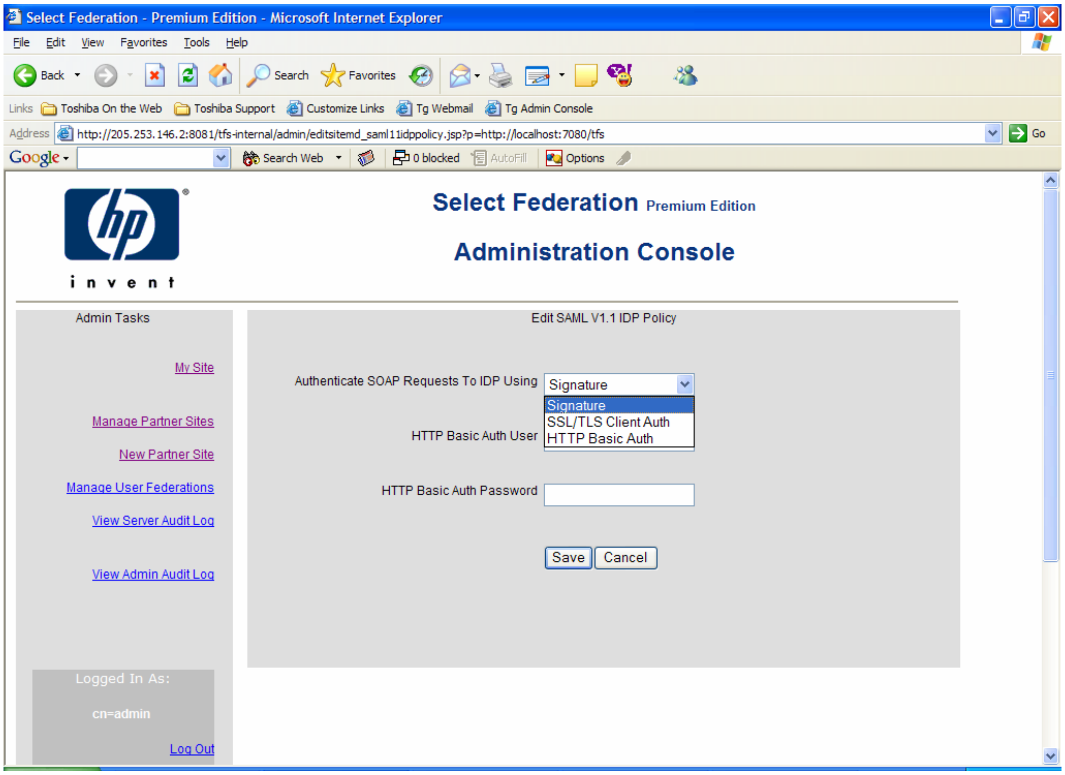
Partner Site Details: Protocol Policy

**Site Id:** http://localhost:7080/tfs
**Type:** Authority
**Protocol:** SAML 1.1

SAML V1.1 IDP Policy

| | |
|---|---|
| **Authenticate SOAP Requests to IDP Using** | Signature |

**Figure 7-11: To Update a SAML Federation’s Protocol Policy for an Authority (IDP) Site**



http://205.253.146.2:8081/tfs-internal/admin/editsitemd_saml11idppolicy.jsp?p=http://localhost:7080/tfs

Select Federation Premium Edition

Administration Console

Edit SAML V1.1 IDP Policy

Authenticate SOAP Requests To IDP Using: Signature

HTTP Basic Auth User

HTTP Basic Auth Password

**Figure 7-12: Setting the SOAP Authentication Method in your SAML IDP Policy**

If your site is a SAML Consumer (SP or Application Site) and you will be sending artifacts to the SAML Producer (IDP or Authority Site), you will need to set the single sign on parameters in this section of the web page as shown in Figure 7-12.

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 user name and password in the fields **HTTP Basic Auth User** and **HTTP Basic Auth Password** as shown in Figure 7-12.

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

8

# Configuring the Profile Service

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 Trusted Partner will need to agree on the attributes to be exchanged.

Attributes are configured in the Select Federation properties file and are fetched on every user authentication. Select Federation can further be configured to "push" attributes on every outbound user authentication when working as a SAML producer or IDP, further saving the overhead in fetching attributes about the user.

At a SAML producer, attribute values about a user are fetched from a user repository (typically an LDAP directory or an RDBMS). Select Federation provides an LDAP plugin that readily integrates with X.500 directories that support the LDAP v3 protocol. This includes Microsoft Active Directory, the Sun Java System Directory Server, and a number of other products.

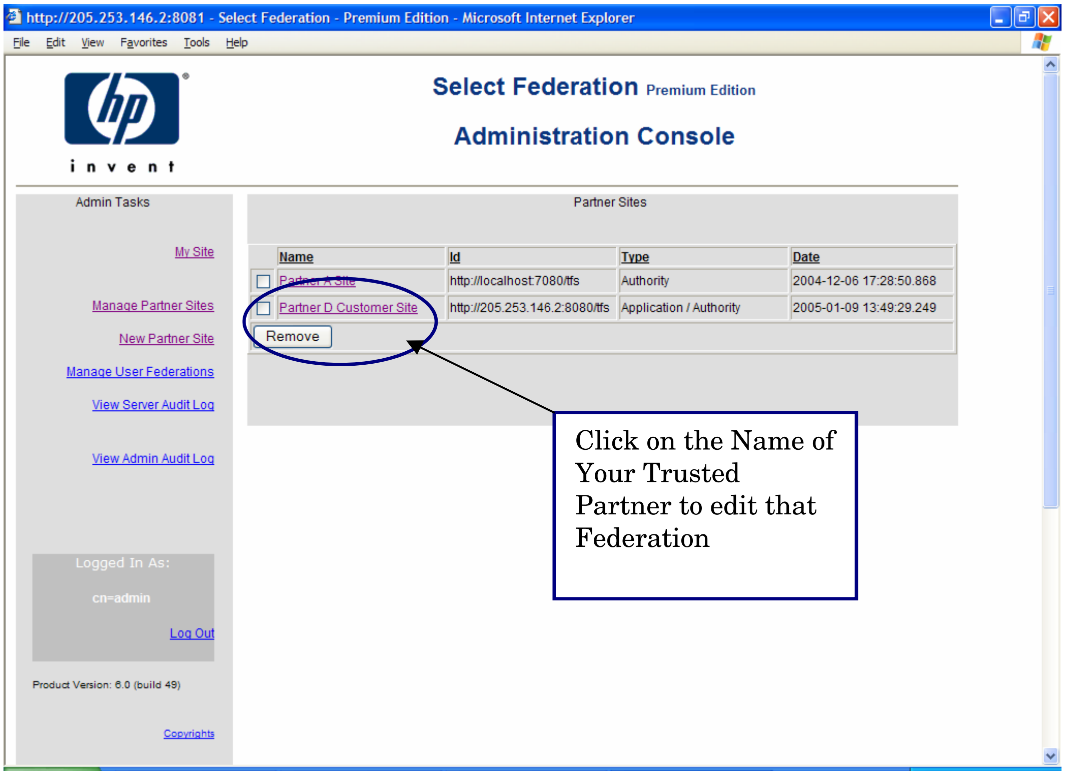
## Configuring Your Profile Attribute Exchange

Select Federation allows you to configure and change the user profile attribute exchange. To edit or set your profile attribute:

1 Click **Manage Partner Sites** on the **Admin Tasks** side bar. You will be directed a web page as shown in Figure 8-1.

2 Then click the **Name** of the site that you wish to edit. You will be directed a web page as shown in Figure 8-2.

3 In the dropdown menu next to **Partner Site Details**, select **Attribute Policy**. You will be directed to a web page as shown in Figure 8-3 that delineates all the existing attribute policy parameters, if any, for this Liberty federation.


http://205.253.146.2:8081 - Select Federation - Premium Edition - Microsoft Internet Explorer
File Edit View Favorites Tools Help
invent
Remove

Select Federation Premium Edition

Administration Console

Admin Tasks

My Site

Manage Partner Sites

New Partner Site

Manage User Federations

View Server Audit Log

View Admin Audit Log

Logged In As:

cn=admin

Log Out

Product Version: 6.0 (build 49)

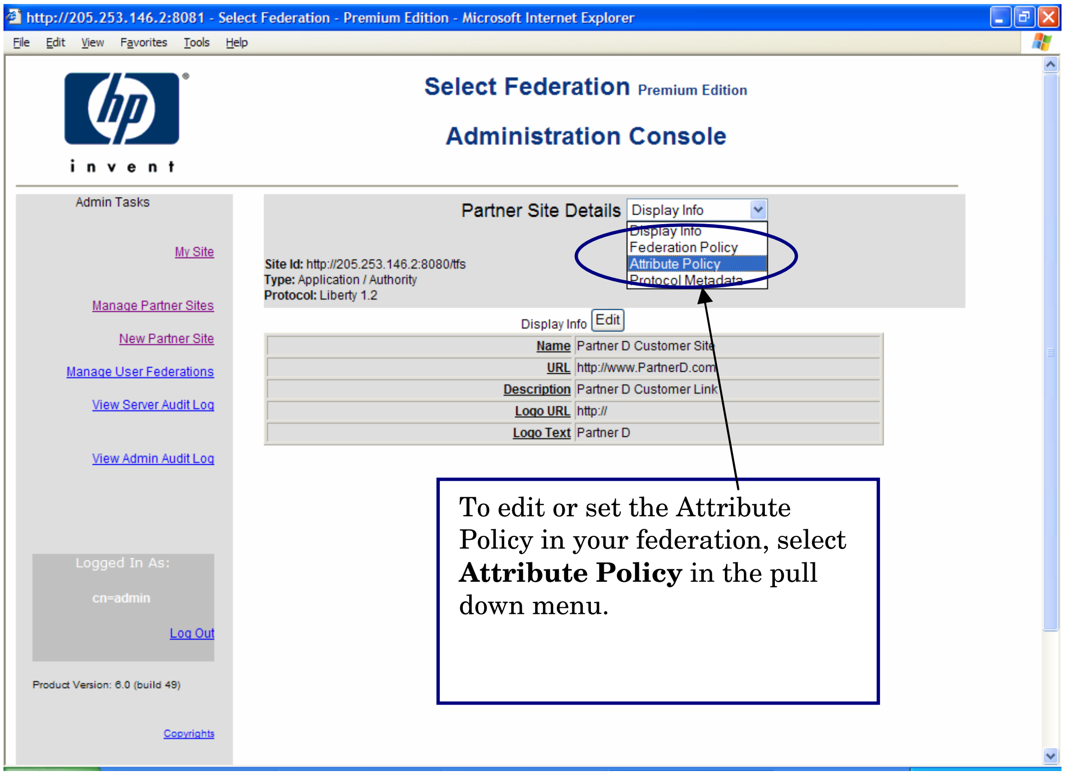
Copyrights

Partner Sites

| | Name | Id | Type | Date |
|---|---|---|---|---|
| □ | Partner A Site | http://localhost:7080/tfs | Authority | 2004-12-06 17:28:50.868 |
| □ | Partner D Customer Site | http://205.253.146.2:8080/tfs | Application / Authority | 2005-01-09 13:49:29.249 |

Click on the Name of Your Trusted Partner to edit that Federation

**Figure 8-1: Select the Federation that You Wish to Edit**



Select Federation Premium Edition

Administration Console

Partner Site Details: Display Info

Site Id: http://205.253.146.2:8080/tfs
Type: Application / Authority
Protocol: Liberty 1.2

Display Info

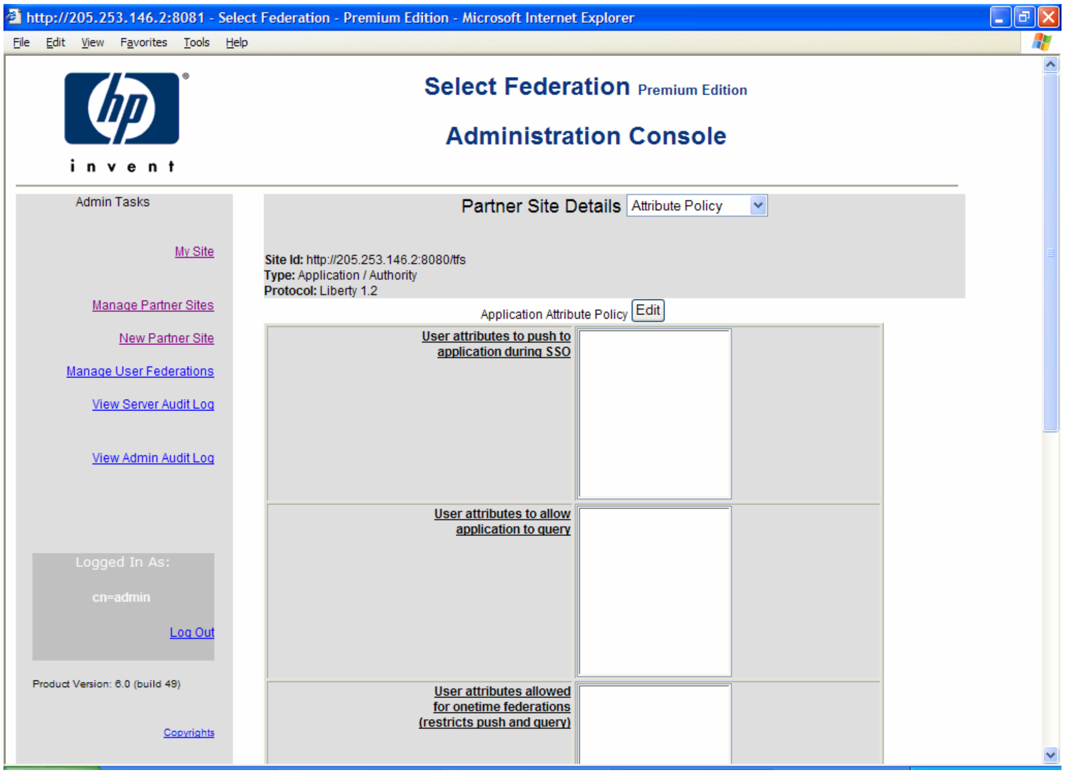
|  |  |
|---|---|
| Name | Partner D Customer Site |
| URL | http://www.PartnerD.com |
| Description | Partner D Customer Link |
| Logo URL | http:// |
| Logo Text | Partner D |

Logged In As: cn=admin

Product Version: 6.0 (build 49)

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

**Figure 8-2: To Edit the Profile Attribute Policy in Your Federation**



Select Federation Premium Edition

Administration Console

Partner Site Details: Attribute Policy

Site Id: http://205.253.146.2:8080/tfs
Type: Application / Authority
Protocol: Liberty 1.2

Application Attribute Policy

|  |  |
|---|---|
| User attributes to push to application during SSO |  |
| User attributes to allow application to query |  |
| User attributes allowed for onetime federations (restricts push and query) |  |

Logged In As: cn=admin

Product Version: 6.0 (build 49)

**Figure 8-3: Existing Attribute Policy Parameters of Your Federation, if Any.**

The attributes that may be conveyed at the time of single sign on from the Authority Site (IDP or SAML Producer) to the Application Site (SP or SAML Consumer) are as follows:

**Application Attribute Policy**

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

**User attributes to allow application to query**: The additional attributes that the Application Site is allowed to pull from the Authority Site. They are attributes that were not pushed by the Authority Site in the initial sign on. The Application Site 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 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**

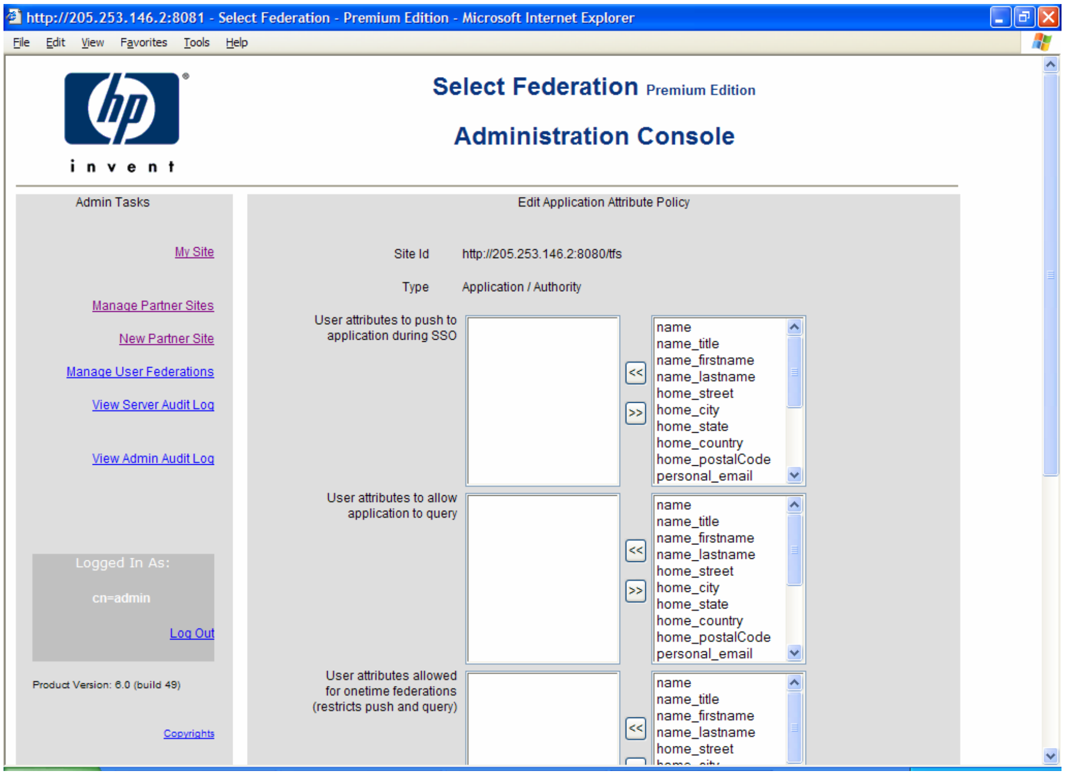
**User attributes to obtain from authority on each login:** Each time the user executes a transaction at the Application Site this user information is retrieved from the Authority Site.

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

4 To set or change your profile attribute policy, click **Edit.** You will be directed to a screen similar to the one shown in Figure 8-4. Select the user attributes that you would like to pass for each login.

5 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.

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



http://205.253.146.2:8081 - Select Federation - Premium Edition - Microsoft Internet Explorer
File Edit View Favorites Tools Help
invent
Select Federation Premium Edition
Administration Console
Admin Tasks
My Site
Manage Partner Sites
New Partner Site
Manage User Federations
View Server Audit Log
View Admin Audit Log
Logged In As:
cn=admin
Log Out
Product Version: 6.0 (build 49)
Copyrights
<<
>>

Edit Application Attribute Policy

Site Id http://205.253.146.2:8080/tfs

Type Application / Authority

User attributes to push to application during SSO

name
name_title
name_firstname
name_lastname
home_street
home_city
home_state
home_country
home_postalCode
personal_email

User attributes to allow application to query

name
name_title
name_firstname
name_lastname
home_street
home_city
home_state
home_country
home_postalCode
personal_email

User attributes allowed for onetime federations (restricts push and query)

name
name_title
name_firstname
name_lastname
home_street

**Figure 8-4: Editing Your Attribute Policy**

9

# Configuring the Privacy Manager

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

## Accessing the Privacy Manger

The Privacy Manager is located at the top-level URL:

`/PrivacyManager`

The Privacy Manager has two screens:

1 The Preference setting screen

2 The interaction / consent screen

Its look and feel can be completely controlled by providing a different style sheet than is supplied on the CD.

## Setting Up the Configuration File

The configuration file that contains all information regarding the Privacy Manager is the file "`pmconfig.properties`". The installer copies this file to the "`${SF_HOME}/config`" output sub directory. `SF_HOME` is the directory on your hard disk where you copied the CD and ran the installer script. This file is expected to be copied along with other files to the "`conf`" sub directory under the root of the application server.

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

1 First run the Select Federation installation script

2 Copy the configuration files as instructed in the installation instructions to the "conf" sub directory of the app-server.

3 Make a backup copy of the `pmconfig.properties` before editing it.

4 Edit the `pmconfig.properties` file in the "conf" sub directory of the app-server.

## Configuration File Contents

The configuration file contains the following parameters as shown in Table 9-1:

**Table 9-1: Configuration File Parameters**

| Parameter | Description | Default Value |
|---|---|---|
| `brandCSS` | The style sheet to be used for branding (URL) | `u/styles.css` |
| `brandLogo` | The logo URL to be embedded in the Privacy Manager screen (URL) | `u/logo.gif` |
| `brandLogoAlt` | The text to be displayed when the mouse hovers over the logo when the page is displayed in the browser | `HP` |
| `brandTitle` | The name of the Privacy Manager application as seen by the user | `HP OpenView Select Federation Privacy Manager` |
| `profileDispAttrs` | The order in which attribute values should be shown in the interaction screen if multiple attributes are requested at once | `name name_title name_firstname name_lastname home_street home_city home_state home_country home_postalCode personal_email personal_phone work_street work_city work_state work_country work_postalCode work_email work_phone` |
| `<*>.dispName` | The descriptive name to be used for each attribute | |

A

# Configuration Parameters

When you install Select Federation, you will see a file called tfsconfig.properties. This Appendix has the configuration parameters that can be manually typed into this tfsconfig.properties file in order to customize your installation.

## Types of Configuration Parameters

Table A-1 delineates the five types of configuration parameters that are possible when you are manually entering the data.

**Table A-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<br>param=1 | A Boolean has a value of 0 (false) or 1 (true). |
| Integer | param=123<br>param=-1 | An Integer value. |
| TimeDuration | param=1s<br>param=1h30m<br>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 A-2: Core Configuration File Parameters**

| Name | Type | Default (if not reqd) | Description |
|---|---|---|---|
| installMode | StringList | “sp idp” | Records installation mode. Controls options available in Admin Console for configuring and managing Circle-of-Trust. Must not be changed post-installation. |
| licenseFile | String | Required | Full path to customer’s license.xml file. |
| providerId | String | Required | Server’s Liberty ProviderID. Must be same as <providerBaseURL> to enable Liberty Metadata publishing. Must not be changed post-installation. |
| providerBaseURL | String | Required | URL for the server’s front-channel WAR. |
| providerBaseSOAPURL | String | Required | URL for the server’s back-channel (SOAP) WAR. |
| providerBaseTLSClientAuthSOAPURL | String | null | URL for the server’s back-channel (SOAP) WAR, as protected by TLS Client Auth. If null, no TLS Client Auth support is enabled. |
| errorURL | String | Required | URL to which front-channel protocols should redirect in the case of an unrecoverable error. |
| keystorePath | String | Required | Full path to keystore containing server’s signing key. |
| keystoreType | String | Required | Keystore type (e.g. JKS). |
| keystorePassword | String | Required | Keystore password. |
| certAlias | String | Required | Alias for signing certificate. |
| keyPassword | String | Required | Signing key password. |
| keyAlias | String | Required | Alias for signing key. |

| Name | Type | Default (if not reqd) | Description |
|---|---|---|---|
| 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. |
| 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. |

| Name | Type | Default (if not reqd) | Description |
|---|---|---|---|
| relayTimeout | TimeDuration | 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 | TimeDuration | 1h | Determines how often the runtime tables are purged of entries for abandoned sessions. Default is 1 hour. |

**Table A-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". |
| spEventPlugin | String | null | SPEventPlugin implementation class name. If non-null, the class will be instantiated and called for login and logout events. |
| spDefaultURL | String | Required | The default application URL to send users to following receipt of an unsolicited authentication assertion with no accompanying target URL. |

| Name | Type | Default (if not reqd) | Description |
|---|---|---|---|
| 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). |

**Table A-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. |
| 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. |
| authTimeout | TimeDurat ion | 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 | TimeDurat ion | 1s | Maximum age of an authentication that can satisfy a forced re-authentication request. Default is 1 second. |
| authnContextClassRef | StringList | Required | List of Liberty AuthnContextClassRef URIs supported by the configured idpAuthnPlugin or loginURL.• |

| Name | Type | Default (if not reqd) | Description |
|---|---|---|---|
| authnContextStatementRef | StringList | Required | List of Liberty AuthnContextStatementRefs corresponding to the AuthnContextClassRefs listed in authnContextClassRef (in order). |
| samlAuthMethod | StringList | Required | List of SAML 1.1 AuthenticationMethod URIs corresponding to the Liberty AuthnContextClassRefs listed in authnContextClassRef (in order). |
| rankedAuthnContextClassRefs | StringList | Required | List of Liberty AuthnContextClassRefs in comparison order according to local policy, from weakest to strongest. |
| rankedAuthnContextStatementRefs | StringList | Required | List of Liberty 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 group membership, and fetching user profile attributes. |
| <attralias>.ldapAttr | String | null | If non-null, the LDAP user attribute that maps to his profile attribute. |

**Table A-5: ID-FF Application Configuration File Parameters**

| Name | Type | Default (if not reqd) | Description |
|---|---|---|---|
| signAuthnRequests | Boolean | Required | If true, AuthnRequest messages will be signed. |
| spFederationTerminationNotificationProtocolProfiles | StringList | Required | List of Liberty protocol profile URIs to support for FT at the SP. |
| spRegisterNameIdentifierProtocolProfiles | StringList | Required | List of Liberty protocol profile URIs to support for RNI at the SP. |
| spSingleLogoutProtocolProfiles | StringList | Required | List of Liberty protocol profile URIs to support for SLO at the SP. |
| supportLECProfile | Boolean | false | 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. |

**Table A-6: ID-FF Authority Configuration File Parameters**

| Name | Type | Default (if not reqd) | Description |
|---|---|---|---|
| idpFederationTerminationNotificationProtocolProfiles | StringList | Required | List of Liberty protocol profile URIs to support for FT at the IDP. |
| idpRegisterNameIdentifierProtocolProfiles | StringList | Required | List of Liberty protocol profile URIs to support for RNI at the IDP. |
| idpSingleLogoutProtocolProfiles | StringList | Required | List of Liberty protocol profile URIs to support for SLO at the IDP. |
| idpSingleSignOnProtocolProfiles | StringList | Required | List of protocol profile URIs to support for SSO at the IDP. |
| idwsfSupportAttributeQuery | 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). |
| useSSOCookieWriter | Boolean | false | If true, the SSO service will use the configured cookie writer to update the Liberty common domain cookie. |
| cookieWriterServiceURL | String | null | The URL of the CookieWriterService to use. Required if useSSOCookieWriter is true. |
| 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. |

**Table A-7: SAML Authority Configuration File Parameters**

| Name | Type | Default (if not reqd) | Description |
|---|---|---|---|
| samlRequestAuth | StringList | “sign ssl http” | The list of SOAP authentication mechanisms configured for the SAML SOAP service. |
| samlIncludeAudienceRestrictionCondition | Boolean | false | If true, SAML SSO assertions include an audience restriction condition identifying the intended consumer. |
| samlIncludeSubjectIP | 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). |
| samlSupportAttributeQuery | Boolean | false | If true, attribute query requests will be accepted on the SAML SOAP endpoint. |

**Table A-8: 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. |
| 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. |

| Name | Type | Default (if not reqd) | Description |
|---|---|---|---|
| ldapUserBaseDN | String | Required | Base DN to use in constructing user DN from username and ldapUserAttr. User DN looks like <ldapUserAttr>=<username>,<ldapUserBaseDN>.• |
| ldapGroupMembershipAttr | String | null | LDAP attribute that enumerates a user group memberships (e.g. “memberOf” for AD, “ibm-allGroups” for IBM Directory Server, “nsRole” for Sun Directory Servier). |
| <attralias>.ldapAttr | String | null | If non-null, the LDAP user attribute that maps to his profile attribute. |

**Table A-9: 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 |

# spapiconfig.properties

**Table A-10: 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. |
| 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. |
| cookieReaderServiceURL | String | null | If non-null, the URL of the CookieReaderService to use. |

## idpapiconfig.properties

**Table A-11: 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. |
| 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. |

| Name | Type | Default (if not reqd) | Description |
|---|---|---|---|
| tfsSIDCookieDomain | 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. |
| cookieReaderService URL | String | null | If non-null, the URL of the CookieReaderService to use. |
| cookieWriterService URL | String | null | If non-null, the URL of the CookieWriterService to use. |

**Table A-12: 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. |
| idwsfDSTokenTimeout | TimeDuration | 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). |
| idwsfDSAllowUpdatesFrom | StringList | null | If non-null, discovery service updates will only be allowed from the listed SPs (identified by ProviderID). |

**Table A-13: LECP Service Configuration File Parameters**

| Name | Type | Default (if not reqd) | Description |
|---|---|---|---|
| lecpAllowIDPLocPrefixes | 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. |
| lecpDenyIDPLocPrefixes | 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. |
| lecpStripHeadersIDP | StringList | null | List of headers (received by the LECP service) that should not be forwarded in requests sent to IDPs. |
| lecpStripHeadersSP | StringList | null | List of headers (received by the LECP service) that should not be forwarded in requests sent to SPs. |

| Name | Type | Default (if not reqd) | Description |
|---|---|---|---|
| lecpSessionHdr | String | "X-LECPSession" | 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. |

## pmconfig.properties

**Table A-14: Privacy Manager Configuration File Parameters**

| Name | Type | Default (if not reqd) | Description |
|---|---|---|---|
| brandCSS | String | Required | URL of CSS stylesheet to use for branding in PrivacyManager screens. |
| brandLogo | String | Required | URL of logo image to use for branding in PrivacyManager screens. |
| brandLogoAlt | String | Required | Alt logo image text to use for branding in PrivacyManager screens. |
| brandTitle | String | Required | Title text to use for branding in PrivacyManager screens. |
| brandCopyright | String | Required | Copyright text to display in PrivacyManager screens. |
| profileDispAttrs | StringList | null | List of profile attributes to display in consent dialogs, if present in request. |
| <attralias>.dispName | String | Required | Display name for profile attribute. |