

HP Select Federation

For the HP-UX, Linux, Solaris and Windows® operating systems

Software Version: 7.01

CA SiteMinder Connector Guide

Document Release Date: March 2008

Software Release Date: March 2008



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

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

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

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

Trademark Notices

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

Documentation Updates

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

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

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

<http://h20230.www2.hp.com/selfsolve/manuals>

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

Support

You can visit the HP Software Support web site at:

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

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

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

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

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

For more information about HP Passport, go to:

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

Contents

1	Introduction	9
	Prerequisites	9
	How an SF-IDP with CA SiteMinder Connector Integration Works with SiteMinder	10
	How an SF-SP with CA SiteMinder Connector Integration Works with SiteMinder	11
	How an SF-SP&IDP with CA SiteMinder Connector Integration Works with SiteMinder	11
	How Select Federation Applications Work with SiteMinder	11
2	Deploying the Select Federation CA SiteMinder Connector	13
	System Requirements	13
	Software Requirements	13
	Platform Requirements	13
	Deploying the Select Federation CA SiteMinder Connector	14
	Deploying on the SiteMinder Policy Server	14
	Deploying on the Select Federation Application Server	14
	Rolling Back the Select Federation CA SiteMinder Connector	15
	Select Federation CA SiteMinder Connector Logging	15
3	Integrating the Select Federation CA SiteMinder Connector with an IDP Site	17
	Requirements	17
	CA SiteMinder Connector Integration with an SF-IDP	17
	Step 1: Prepare the Environment for Federated Applications	18
	Step 2: Integrate the Select Federation Agent	20
	Step 3: Authenticate SiteMinder Domain-Local Users	26
	Authenticating the SiteMinder Domain-Local Users Through the Select Federation Agent	26
	Authenticating the SiteMinder Domain-Local Users Through a Login URL	29
	Step 4: Configure Select Federation SF-IDP Applications	32
	Configuring the Administration Console when Authenticating Through the Select Federation Agent	32
	Configuring the Privacy Manager when Authenticating Through the Select Federation Agent ..	33
	Configuring the Administration Console when Authenticating Through a Login URL	34
	Configuring the Privacy Manager when Authenticating Through a Login URL	35
	Step 5: Configure Profile-Attribute-Fetching for Federated Users	36
	Step 6: (Optionally) Test the CA SiteMinder Connector Integration with the Demonstration Application	36
	Setting Up an Environment for the Demonstration Application	37
	Configuring the Demonstration Application	37
	Running the Demonstration Application	39
4	Integrating the Select Federation CA SiteMinder Connector with an SP Site	41
	Requirements	41

CA SiteMinder Connector Integration with an SF-SP	41
Step 1: Determine a User Activation Scheme	42
Configuring Select Federation	42
Using the Activate LDAP Plugin for the User Activation Scheme	43
Step 2: (Optionally) Set User Profile Attributes as a Cookie	43
Step 3: Integrate the Select Federation Agent	44
Step 4: Enable Incoming Federated Users	50
Step 5: Update Application Policies	53
Step 6: Authenticate SiteMinder Domain-Local Users	53
Authenticating the SiteMinder Domain-Local Users Through the Select Federation Agent	53
Authenticating the SiteMinder Domain-Local Users Through a Login URL	56
Step 7: Configure Select Federation SF-SP Applications	59
Configuring the Administration Console when Authenticating Through the Select Federation Agent	59
Configuring the Administration Console when Authenticating Through a Login URL	60
Step 8: (Optionally) Test the CA SiteMinder Connector Integration with the Demonstration Application	61
Setting Up an Environment for the Demonstration Application	61
Configuring the Demonstration Application	61
Running the Demonstration Application	64
5 Integrating the Select Federation CA SiteMinder Connector with SP and IDP Sites	65
Requirements	65
CA SiteMinder Connector Integration with an SF-SP&IDP	65
Step 1: Prepare the Environment for Federated Applications	66
Step 2: Determine a User Activation Scheme	67
Step 3: (Optionally) Set User Profile Attributes as a Cookie	67
Step 4: Integrate the Select Federation Agent	67
Step 5: Enable Incoming Federated Users	67
Step 6: Authenticate SiteMinder Domain-Local Users	67
Step 7: Configure Select Federation Applications	68
Step 8: Configure Profile Attributes for Federated Users	68
Step 9: (Optionally) Test the CA SiteMinder Connector Integration with the Demonstration Application	68
Setting Up an Environment for the Demonstration Application	69
Configuring the Demonstration Application	69
Running the Demonstration Application	71
6 Error Messages	73
Error Message Terminology	73
Error Messages and Descriptions	73
CASM_AMPlugin Error Messages	73
CASM_IDPAuthnPlugin Error Messages	74
CASM_SPEventPlugin Error Messages	74
SFAgentModule Error Messages	75
A Troubleshooting	77
Glossary	79

Index 89

1 Introduction

This guide describes how to deploy, integrate and configure the CA SiteMinder connector. It provides a solution for the following use-cases:

- A self-sufficient enterprise that manages its users and applications through CA SiteMinder needs to enable its users to seamlessly access any federated applications offered by its enterprise partners. An IDP-only mode installation of Select Federation (SF-IDP) can be integrated with SiteMinder through the CA SiteMinder connector to accomplish this goal.
- A self-sufficient enterprise that manages its users and applications through CA SiteMinder needs to enable federated users to access its domain-local applications. An SP-only mode installation of Select Federation (SF-SP) can be integrated with SiteMinder through the CA SiteMinder connector to accomplish this goal.
- A self-sufficient enterprise that manages its users and applications through CA SiteMinder needs to (a) enable its users to seamlessly access any federated applications offered by its enterprise partners, and (b) enable federated users to access its domain-local applications. An SP and IDP mode installation of Select Federation (SF-SP&IDP) can be integrated with SiteMinder through the CA SiteMinder connector to accomplish this goal.

Instructions are also included to integrate any Select Federation application, such as the Administration console, into your access management system.



Select Federation can only be integrated with one access management system at a time.

This chapter includes the following topics:

- [Prerequisites](#)
- [How an SF-IDP with CA SiteMinder Connector Integration Works with SiteMinder](#)
- [How an SF-SP with CA SiteMinder Connector Integration Works with SiteMinder](#)
- [How an SF-SP&IDP with CA SiteMinder Connector Integration Works with SiteMinder](#)
- [How Select Federation Applications Work with SiteMinder](#)

Prerequisites

- HP Select Federation 7.00 + Patch 7.01 (installation, configuration, concepts and so on)
- CA SiteMinder Policy Server 6.0.x.x (installation, configuration, concepts and so on)
- CA SiteMinder SDK 6.0.x.x (installation and configuration) — The following table lists the base versions of the SiteMinder SDK for every platform where the CA SiteMinder Connector can be integrated with Select Federation:

Table 1 Base SiteMinder SDK Versions for Select Federation Supported Platforms

Base SiteMinder SDK Version	Platform
SDK 6.0	<ul style="list-style-type: none"> Windows 2003 (32-bit) Solaris 9, 10 (32-bit)
SDK 6.0 SP5 CR4	<ul style="list-style-type: none"> HP-UX 11.23 PA-RISC and Itanium (64-bit)
SDK 6.0 SP5 CR5	<ul style="list-style-type: none"> Windows 2003 R2 (64-bit) HP-UX 11.23 PA-RISC (32-bit) Red Hat Linux AS 3.0 Update 5 and 4.0 (32-bit)
SDK 6.0 QMR1	<ul style="list-style-type: none"> Red Hat Linux AS 3.0 Update 5 (32-bit)
SDK 6.0 QMR4	<ul style="list-style-type: none"> Red Hat Linux AS 4.0 (32-bit)

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

- Web application servers: Select Federation’s Built-in application server (Tomcat 5.5.23), WebLogic 9.2, and WebSphere 6.0.2 (installation, configuration, concepts, and so on)

How an SF-IDP with CA SiteMinder Connector Integration Works with SiteMinder

When you integrate an SF-IDP with the CA SiteMinder connector, SiteMinder can continue to authenticate and authorize users who should have access to Select Federation applications. From the user’s perspective, this makes accessing a federated application as seamless as accessing a SiteMinder domain-local application.

Following is a step-by-step explanation:

- 1 An unauthenticated user in the SiteMinder domain begins at a client, such as a browser, and wants to access a federated application.
 - a The unauthenticated user can successfully perform Single Sign-On (SSO) to a SiteMinder domain-local application such as an enterprise portal, and then navigate to a link for the federated application.
 - b If the unauthenticated user had bookmarked the link for a federated application and attempts to navigate directly to it, the user is prompted for authentication. The user can then perform SSO using SiteMinder credentials.
- 2 An authorization check is performed against the CA SiteMinder Policy Server.

▶ Since the ultimate authorization decision is performed by the federated applications at the partner, the domain-local policies do not attempt to authorize outgoing users based on the application they are headed to.
- 3 The SF-IDP registers the user, populates the user's profile attributes, and sends the user to the federated application with an assertion generated on the user's behalf.

How an SF-SP with CA SiteMinder Connector Integration Works with SiteMinder

When you integrate an SF-SP with the CA SiteMinder connector, SiteMinder can manage the incoming federated users as seamlessly as SiteMinder domain-local users.

Following is a step-by-step explanation:

- 1 A federated user comes in from a trusted partner to the SF-SP in the SiteMinder domain.
- 2 The Activation Event Plugin successfully identifies the user within the SiteMinder domain or provisions the user as required by the enterprise. See [Step 1: Determine a User Activation Scheme](#) on page 42 for more details.
- 3 The Event Plugin provided by the CA SiteMinder connector calls upon SiteMinder to generate a SiteMinder SSO Cookie for the user.
- 4 The user is sent to the application.
- 5 If the policies in the SiteMinder domain are set properly for that user, then the user can access the application.

How an SF-SP&IDP with CA SiteMinder Connector Integration Works with SiteMinder

When you integrate an SF-SP&IDP with the CA SiteMinder connector, SiteMinder can do the following:

- Continue to authenticate and authorize users who should become federation-capable
- Manage the incoming federated users as seamlessly as SiteMinder domain-local users.

For a step-by-step explanation of the workflow for each site role, see [How an SF-IDP with CA SiteMinder Connector Integration Works with SiteMinder](#) on page 10 and [How an SF-SP with CA SiteMinder Connector Integration Works with SiteMinder](#) on page 11.

How Select Federation Applications Work with SiteMinder

When you integrate Select Federation applications, such as Administration console or Privacy Manager, with the CA SiteMinder connector, SiteMinder can manage these applications like any other SiteMinder domain-local applications.

Following is a step-by-step explanation:

- 1 The SiteMinder user tries to access a Select Federation application using a client such as a browser.
- 2 The Select Federation Access Filter intercepts the request and checks if a SiteMinder SSO Cookie exists. If not then the user is asked to authenticate.

- 3 If the SiteMinder SSO Cookie exists, the Access Filter either allows or denies access, based on the authorization policies set in SiteMinder.
- 4 If the user is authorized, then the user can access the Select Federation application.
- 5 If the user is not authorized, an error message is displayed.

2 Deploying the Select Federation CA SiteMinder Connector

This chapter includes the following topics:

- System Requirements
- Deploying the Select Federation CA SiteMinder Connector
- Select Federation CA SiteMinder Connector Logging

System Requirements

Software Requirements

The following software must be installed and configured:

- Select Federation 7.00 and the 7.01 Patch — See the *HP Select Federation Installation Guide* for installation instructions.
- CA SiteMinder Policy Server 6.0 — See the CA SiteMinder documentation for installation instructions.
- CA SiteMinder SDK 6.0 — Install the SiteMinder SDK on the same machine where Select Federation is installed. Be sure to install the correct SDK for the corresponding platform (see [Prerequisites](#) on page 9 for the version requirement for your platform).



If you want your installation to support international characters, be sure you have properly set up the following to support these characters:

- Platforms on which Select Federation and CA SiteMinder are installed
- Databases and/or LDAP directories used by Select Federation and CA SiteMinder

Platform Requirements

The Select Federation CA SiteMinder connector can work on any Select Federation platform that is compatible with the CA SiteMinder SDK and offers support for the V6.0 Agent APIs. For every Select Federation install that you want to integrate with CA SiteMinder, you must install the CA SiteMinder SDK on the same machine. See [Prerequisites](#) on page 9 for the SiteMinder SDK version requirement for your platform.

Deploying the Select Federation CA SiteMinder Connector

This section provides the basic steps for deploying the Select Federation CA SiteMinder connector on the SiteMinder Policy Server and any application server on which Select Federation is installed. For detailed instructions on application server-specific tasks, see the application server's documentation.

Deploying on the SiteMinder Policy Server

Perform the following steps on the machine or machines where the CA SiteMinder Policy Server or Policy Servers are installed:

- 1 Copy the `$SF_PATCH/connectors/siteminder/SFAuthnModule.jar` file to a local directory where the SiteMinder Policy Server is installed, such as `$SMPS_INSTALL/bin/jars/`.
- 2 Go to the `$SMPS_INSTALL/config/` directory and open the `JVMOptions.txt` file.
- 3 Add the `SFAuthnModule.jar` path to the `-Djava.class.path` parameter, as follows:
`-Djava.class.path=<other files>;$SMPS_INSTALL/bin/jars/SFAuthnModule.jar`
- 4 Restart the SiteMinder Policy Server.

Deploying on the Select Federation Application Server

After the Select Federation patch has been applied, and the CA SiteMinder SDK has been installed, perform the following steps to deploy the Select Federation CA SiteMinder connector files:

- 1 Copy the following files from the `$SF_PATCH/connectors/siteminder/` directory to the `$SF_HOME/connectors/siteminder/` directory:
 - `CASMConnector.jar`
 - `/docs/siteminder.pdf`
- 2 Make sure that your application server's class path is pointing to the `smjavaagentapi.jar` file from your SiteMinder SDK. Specify the full path for the `.jar` file, including the `jar` file name.

For example:

```
set CLASSPATH=<path_to_SM_SDK>\<DIR_with_jar_files>\smjavaagentapi.jar;%CLASSPATH%
```

See the application server's documentation for instructions on how to set its class path.

- 3 Set the CA SiteMinder SDK-related variables (such as `LD_LIBRARY_PATH`, `PATH`, `LIBPATH`, or `SHLIB_PATH`) so that the system can find the JNI support library. Specify the directory as the value of the variable.

For example:

```
set PATH=<path_to_SM_SDK>\<DIR_with_jni_files>;%PATH%
```

See the instructions for setting these SDK-related variables in the CA SiteMinder guide for Java developers.

- 4 Restart the application server.

All the variables should be set so that they are visible to the application server on which Select Federation is running. You may check the application server's logs to make sure that all the variables and their values have been picked-up by the application server.

- 5 Integrate the Select Federation CA SiteMinder connector with one or both of the following Select Federation site roles:

- ▶ Before you begin, make a backup copy of the `$SF_Home/conf/tfsconfig.properties` file. You can use this backup copy to roll back the CA SiteMinder connector integration. See [Rolling Back the Select Federation CA SiteMinder Connector](#) on page 15 for details.
- Identity Provider (IDP) site — see [Chapter 3, Integrating the Select Federation CA SiteMinder Connector with an IDP Site](#) for complete integration and configuration instructions.
- Service Provider (SP) site — see [Chapter 4, Integrating the Select Federation CA SiteMinder Connector with an SP Site](#) for complete integration and configuration instructions.
- IDP and SP site — see [Chapter 5, Integrating the Select Federation CA SiteMinder Connector with SP and IDP Sites](#) for complete integration and configuration instructions.
- ▶ When you start up Select Federation, be sure at least one SiteMinder Policy Server is running so that the CA SiteMinder connector can be initialized properly.

Rolling Back the Select Federation CA SiteMinder Connector

You can roll back the Select Federation CA SiteMinder connector integration from the Select Federation installation. To do this, copy your backed up version of the `$SF_Home/conf/tfsconfig.properties` file over the existing `tfsconfig.properties` file.

- ▶ If you did not back up the Select Federation installation `tfsconfig.properties` file, then remove or comment out all CA SiteMinder-specific configuration parameters in the existing `tfsconfig.properties` file.

Select Federation CA SiteMinder Connector Logging

The Select Federation CA SiteMinder connector errors are logged based on settings in the Select Federation `log4j.properties` file in the `$SF_HOME/properties` directory. Use the Select Federation log file to view logged messages. The location of the log file depends on the application server on which you have Select Federation installed.

For WebLogic and WebSphere, you need to enable logging, if you have not done so already. Logging is already enabled for the built-in server.

- For instructions on enabling logging for WebLogic, see “Deploying Select Federation on the BEA WebLogic Server” in the *HP Select Federation Installation Guide*.
- For instructions on enabling logging for WebSphere, see “Deploying Select Federation on the IBM WebSphere 6.0.2 Server” in the *HP Select Federation Installation Guide*.

3 Integrating the Select Federation CA SiteMinder Connector with an IDP Site

This chapter provides instructions for integrating and configuring the Select Federation CA SiteMinder connector with a Select Federation IDP site. The instructions assume knowledge of CA SiteMinder Policy Server terminology and configuration setup. For more details on how to configure authentication schemes, web agents or resources to be protected, see the CA SiteMinder Policy Server Configuration Guide.

The figures shown in this chapter are examples from the CA SiteMinder Policy Server 6.0.5.10. If you are using a slightly different CA SiteMinder Policy Server 6.0.x.x, navigate to the equivalent locations to perform these operations.

It is important to configure and set appropriate protection for the Select Federation resources in CA SiteMinder.

Requirements

The following requirements must be met before integrating the CA SiteMinder connector with an SF-IDP:

- HP Select Federation 7.00 + Patch 7.01 is installed
- CA SiteMinder Policy Server 6.0.x.x is installed
- CA SiteMinder SDK 6.0.x.x is installed (see [Prerequisites](#) on page 9 for the version requirement for your platform)
- CA SiteMinder connector is deployed

CA SiteMinder Connector Integration with an SF-IDP

When you integrate the CA SiteMinder connector with an SF-IDP, a self-sufficient enterprise that manages its users and applications through CA SiteMinder can enable its SiteMinder domain-local users to seamlessly access any federated applications offered by its enterprise partners.

Complete the following main steps to integrate the CA SiteMinder connector with an SF-IDP (see each step for instructions):

- [Step 1: Prepare the Environment for Federated Applications](#)

For ease of integration into your existing environment, Select Federation provides a special Application Helper component. You can use the Application Helper to generate the URLs for federated applications and then place them at meaningful locations such as Enterprise Portals for users to access.

► If you do not have your existing environment set up for a federation yet, you can set up a dummy environment as described in [Step 6: \(Optionally\) Test the CA SiteMinder Connector Integration with the Demonstration Application](#) on page 36, and then complete the following steps.

- [Step 2: Integrate the Select Federation Agent](#)

Configure the SF-IDP and the CA SiteMinder Policy Server to use the Select Federation Agent. This component is primarily used for performing authorization. Optionally, it can also be used for authentication.

- [Step 3: Authenticate SiteMinder Domain-Local Users](#)

You can authenticate SiteMinder domain-local users who should become federation capable either through the Select Federation Agent or through a Login URL.

- [Step 4: Configure Select Federation SF-IDP Applications](#)

The configuration that is used to integrate the SF-IDP with CA SiteMinder for authentication (either the Select Federation Agent or the login URL), is also used to authenticate users to access any Select Federation applications (such as the Administration console and Privacy Manager). You also need to set policies for these applications to configure users who are authorized to access them.

- [Step 5: Configure Profile-Attribute-Fetching for Federated Users](#)

SF-IDP installations provide user attributes contained in a data source to application partners. You need to configure Select Federation to use your data source to populate user attributes for outgoing federated users.

- [Step 6: \(Optionally\) Test the CA SiteMinder Connector Integration with the Demonstration Application](#)

You can use the Select Federation Demonstration application to test your integration.

Step 1: Prepare the Environment for Federated Applications

The Application Helper is a unique feature of Select Federation that simplifies the way in which you initiate federation actions such as federated login and global logout. Using the Application Helper, you enter a “target URL” that you would like your users to go to after a federated login. The Application Helper will return a transformed URL that you can paste into your portal for your users to click on. When the users click on this transformed URL, they will arrive seamlessly at the target URL using their domain-local credentials.

To use the Application Helper to generate URLs to federated applications, perform the following steps:

- 1 Navigate to the Select Federation Administration console landing page.

The landing page is usually deployed at:

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

or

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

`<base-url>` is the root of the application server on which you have deployed Select Federation. Replace `<base-url>` with your `hostname:port`.

The landing page opens as shown in the following figure:

Select Federation Administration Console

Administration and Configuration Tasks

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

Learn about the Product

- [Release Notes](#): To see the release notes, visit the HP Software Product Manuals web site and select Select Federation.
- [Installation Instructions](#): The full Installation Guide. If you are reading this page, chances are you have installed the server already.
- [Administration Guide](#): The full Configuration and Administration Guide.
- [Architectural Overview](#): Chapter 2, "Select Federation Architecture" in the Configuration and Administration Guide.
- [Learn More About Federation](#): To learn more about Identity Federation, visit the HP Select Federation website.

Contact HP

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

- 2 Click the **Application Helper** link.

The Federation Application Helper page opens:

hp invent

Select Federation Federation Application Helper

The pages below help you create URLs that you can embed into your applications

If your site is an Authority Site, SAML Producer or Liberty Identity Provider, you can obtain the appropriate URLs by visiting this page:	idphelper.jsp
If your site is an Application Site, SAML Consumer or Liberty Service Provider, you can obtain the appropriate URLs by visiting this page:	sphelper.jsp

- 3 Select **idphelper.jsp**.

The IDP Portal Helper page opens.



Select Federation IDP Portal Helper

Construct URLs for seamless access to trusted partners	
This page helps you create a URL that you can paste into your application such as a portal so that your users can click that link to seamlessly navigate to your trusted partners.	
Select a partner	<input type="text" value="▼"/>
Enter a URL that you want to embed in your portal	<input type="text"/>
<input type="button" value="Construct URL"/>	

- 4 Select a partner in the list and enter the target URL that you want your users to go to after a federated logon.

➤ If the partners list is empty, you need to first exchange metadata with your trusted partners and add your partners through the Select Federation Administration console. Then the partners list on this page will be populated with the partners you added.

Following is an example of a partner and URL:

Partner: HealthCare

URL: <https://www.healthcare.com/myBenefitsApp>

- 5 Click **Construct URL**.

A transformed URL is returned that you can paste into your portal for your users to click on. By clicking this URL, a user can arrive seamlessly at the target URL by using their domain-local credentials.

Step 2: Integrate the Select Federation Agent

The Select Federation Agent is primarily used for performing authorization. Optionally, it can be used for authentication. You need to configure the SF-IDP and CA SiteMinder Policy Server to use the Select Federation Agent.

Complete the following tasks to integrate the Select Federation Agent:

Task 1: Enable the Select Federation Agent at the SF-IDP.

- 1 Add the following required lines in the `$SF_HOME/conf/tfsconfig.properties` file, at the SF-IDP:

➤ Be sure to backup all configuration files. Also, when configuring, search the file and comment out any older configuration values for the parameters that you happen to be working with.

```
# For Windows platforms
SFAgentModule.jar=$SF_HOME\connectors\siteminder\CASMConnector.jar
# For Unix flavored platforms
SFAgentModule.jar=$SF_HOME/connectors/siteminder/CASMConnector.jar
```

```
# SF Agent reads/writes the SM SSO Cookie from/to this domain.
# This is needed because (a) Authentication may have been
# performed by another SiteMinder Web Agent in the domain,
# (b) Other SiteMinder Web Agents may accept third-party cookies.
# Note that the value begins with a dot, for example: .smdomain.com
SFAgentModule.cookieDomain=
# The shared secret that will be configured at the SM Policy Server
# Whatever value is used for agentSecret, the same value must be used
# at all the policy servers that the agent can talk to.
SFAgentModule.agentSecret=
# The SM Policy Server(s) to contact
SFAgentModule.policyServers=myPolicyServer
# The IP of the SM Policy Server to contact
myPolicyServer.ip=
```

- ▶ When you start up Select Federation, be sure at least one SiteMinder Policy Server is running so that the CA SiteMinder connector can be initialized properly.

Task 2: Add and configure other optional parameters in the `tfconfig.properties` file.

All parameters with default values are optional. You only need to add them if you want to change the default value.

- ▶ To see mock configurations that demonstrate how to use the parameters in the following table, see the `$SF_PATCH/connectors/siteminder/samples` directory.

The following table lists and describes the CA SiteMinder connector parameters that are optional. This table includes parameters for which you would specify values for any of the following reasons:

- to change the default value
- to use additional functionality

- ▶ Required parameters are shown in the previous step, and therefore are not listed in this table.

The following table lists and describes the CA SiteMinder connector parameters:

Table 2 Select Federation CA SiteMinder Connector Parameters

Parameter Name	Parameter Value	Description	Example	Required/Optional (default value)
SFAgentModule.agentName	String	Name of the Select Federation Agent, which should be registered at the SiteMinder Policy Server(s).	sfagentmodule	Optional (sfagentmodule)
SFAgentModule.cookieName	String	Name of the SiteMinder SSO cookie that the Select Federation Agent reads-from/writes-to the cookie domain.	SMSESSION	Optional (SMSESSION)
SFAgentModule.policyServers	String List	Space-separated list of CA SiteMinder Policy Servers which the SF Agent can contact.	psA psB psC	Required
<policyServer>.ip	String	Part of the contact information about the SiteMinder Policy server: IP address of a policy server.	11.12.13.14	Required
<policyServer>.connectionMin	Integer	Part of the contact information about the SiteMinder Policy server: Number of initial connections. See the SiteMinder documentation and/or the Policy Server configuration to provide this information.	1	Optional (1)
<policyServer>.connectionMax	Integer	Part of the contact information about the SiteMinder Policy server: Maximum number of connections. See the SiteMinder documentation and/or the Policy Server configuration to provide this information.	3	Optional (3)

Table 2 Select Federation CA SiteMinder Connector Parameters

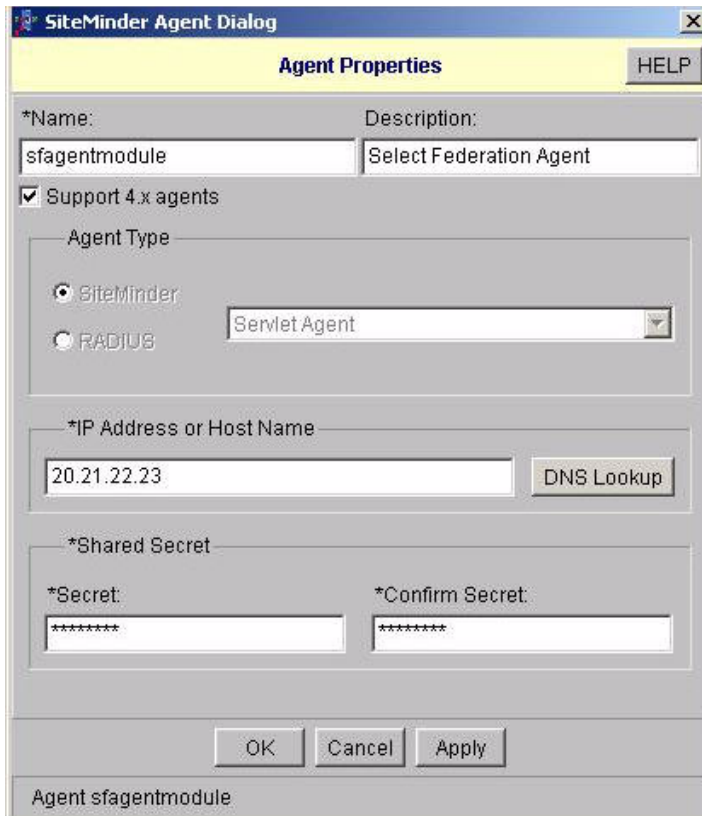
Parameter Name	Parameter Value	Description	Example	Required/ Optional (default value)
<policyServer> .connectionStep	Integer	Part of the contact information about the SiteMinder Policy server: Number of connections to allocate when out of connections. See the SiteMinder documentation and/or the Policy Server configuration to provide this information.	1	Optional (1)
<policyServer> .timeout	Integer	Part of the contact information about the SiteMinder Policy server: Connection timeout in seconds. You may refer to your SiteMinder documentation and/or the Policy Server configuration to provide this information.	75	Optional (75)
<policyServer> .accountingPort	Integer	Part of the contact information about the SiteMinder Policy server: Authentication server port (use 0 for none).	44441	Optional (44441)
<policyServer> .authenticationPort	Integer	Part of the contact information about the SiteMinder Policy server: Authentication server port (use 0 for none) for a SiteMinder policy server.	44442	Optional (44442)
<policyServer> .authorizationPort	Integer	Part of the contact information about the SiteMinder Policy server: Accounting server port (use 0 for none) for a SiteMinder policy server.	44443	Optional (44443)

Task 3: Create and configure a Response.

- 1 Expand the **Select Federation** domain in the **Domains** tab.
- 2 Right-click **Responses** under the *Select Federation* domain.
- 3 Click **Create Response** in the pop-up window.
The SiteMinder Response Dialog opens.
- 4 Fill in the necessary information, including the following required information:
 - **Agent Type:** SiteMinder Servlet Agent.
- 5 Click **Create**.
The SiteMinder Response Attribute Editor opens.
- 6 Fill in the necessary information, including the following required information:
 - **Attribute:** must be **ServletAgent-HTTP-Header-Variable**.
- 7 Select the **Attribute Setup** tab.
- 8 Fill in the necessary information, including the following required information:
 - **Attribute Kind:** must be **User Attribute**.
 - **Variable Name:** must be **SM_USERLOGINNAME**.
 - **Attribute Name:** must be **SM_USERLOGINNAME**.
- 9 Click **OK** to close the SiteMinder Response Attribute Editor.
- 10 Click **OK** to close the SiteMinder Response Dialog.

Task 4: Enable the Select Federation Agent at CA SiteMinder Policy Servers.

- 1 Create and configure a Custom Agent.
 - a Log on to the CA SiteMinder Policy Server Administration console.
 - b Select the **System** tab.
 - c Right-click on **Agents**.
 - d Click **Create Agent** in the pop-up window.
The Agent Properties dialog opens as shown in the following example:

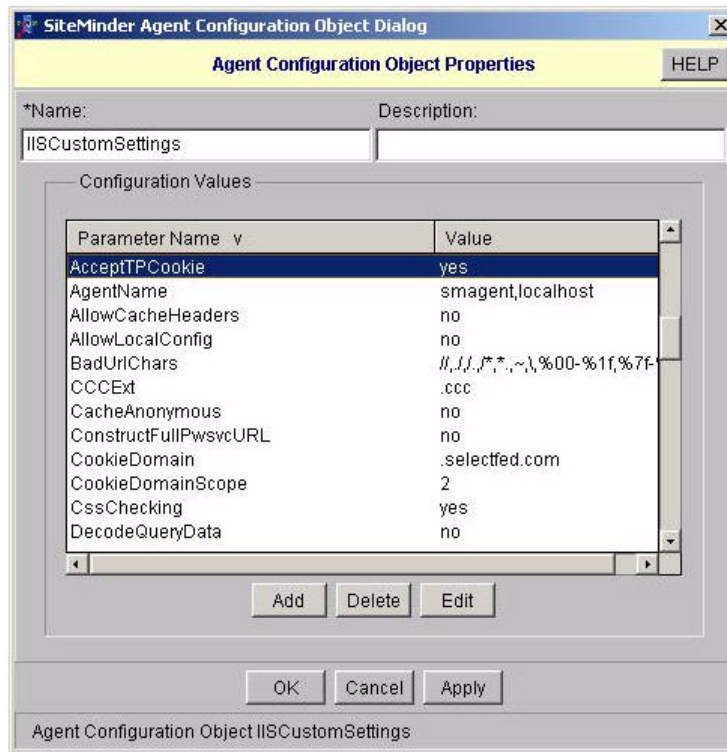


- e Fill in the necessary information, including the following required information, then click **OK**:
 - **Name:** recommended to be **sfagentmodule** unless there are naming conflicts. If there are naming conflicts, you must also make configuration changes in the `tfscnfig.properties` file. See the `SFAgentModule.agentName` parameter in [Table 2](#) on page 22.
 - **Support 4.x agents:** check box must be selected.
 - **Agent Type:** must be a SiteMinder Servlet Agent.
 - **IP Address or HostName:** should point to the machine on which Select Federation is installed.
 - **Shared Secret:** fields must match the value you will provide the Agent that sits with Select Federation. You should have configured the value for the `SFAgentModule.agentSecret` parameter.
- 2 Configure existing Agents to work with the Custom Agent.

Perform the following instructions only for the Agent or Agents that host a SiteMinder domain-local application, which should be accessible to federated users.

- a Select **Agent Conf Objects** in the **System** tab.
- b Double-click the agent configuration object from the **Agent Conf Object List** that applies to your Agent.

The Agent Configuration Object Properties dialog opens as shown in the following example:



- c Click **Add** and set the **AcceptTPCookie** parameter to **yes**.
- For Agents to work together, the cookie domain used by them must be the same.
- d Click **OK**.

Step 3: Authenticate SiteMinder Domain-Local Users

You can perform authentication for SiteMinder domain-local users with the CA SiteMinder Policy Server in one of two ways:

- [Authenticating the SiteMinder Domain-Local Users Through the Select Federation Agent](#) — The Select Federation Agent is limited to CA SiteMinder's Basic Authentication Scheme.
- [Authenticating the SiteMinder Domain-Local Users Through a Login URL](#) — The login URL can be used to point to a resource protected by any SiteMinder Agent, which allows that agent to perform the authentication. This gives you the flexibility to use any Authentication scheme offered by CA SiteMinder Web Agents.

The following sections describe how to configure the SF-IDP and CA SiteMinder Policy Server to perform authentication through the Select Federation Agent and the Login URL. Choose one of these ways to perform your authentication.

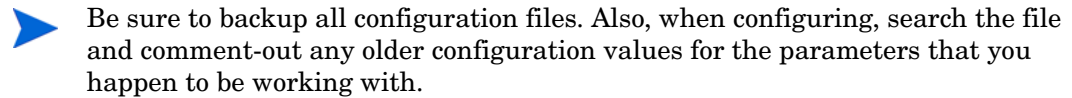
Authenticating the SiteMinder Domain-Local Users Through the Select Federation Agent

In this configuration, the authentication scheme is limited to password authentication. This scheme uses the CA SiteMinder SDK for authentication.

Task 1: Configure the SF-IDP to authenticate the CA SiteMinder domain-local users.

Perform the following steps to edit the `$SF_HOME/conf/tfsconfig.properties` file at the SF-IDP:

- 1 Comment out any previous configurations for the `idpAuthnPlugin` parameter.



- 2 Add the following required lines:

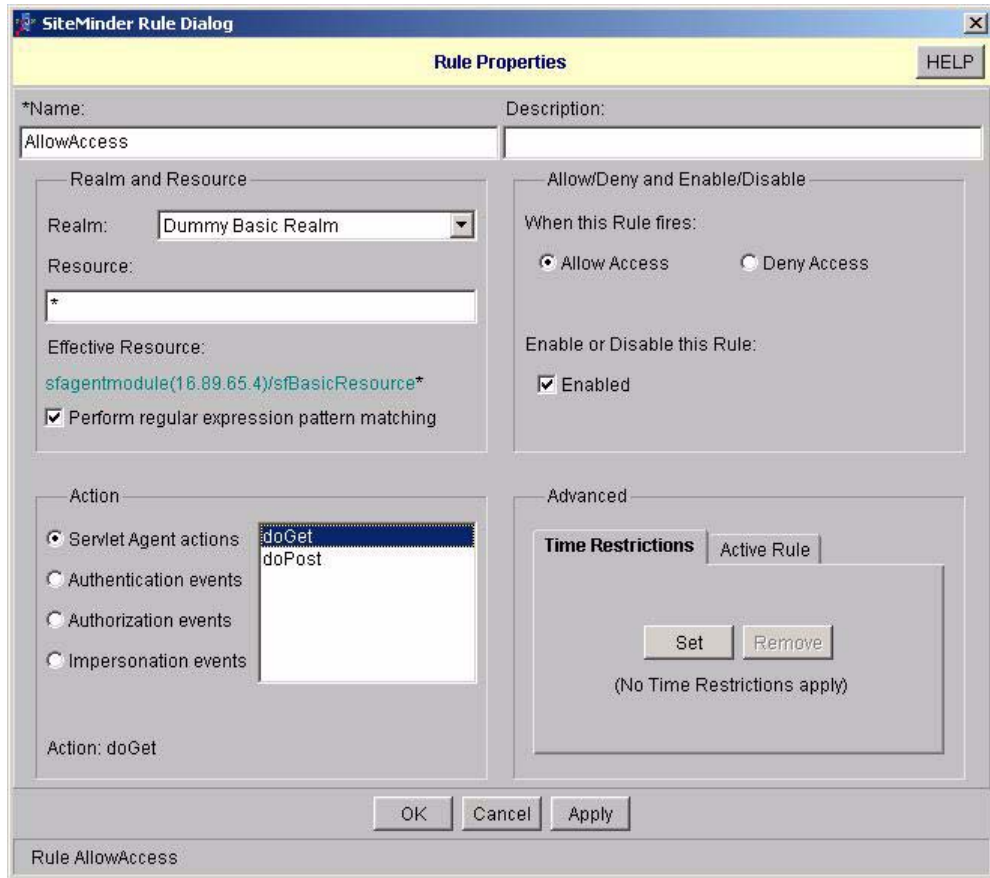
```
amPlugin=myAMPlugin
myAMPlugin.class=com.hp.selectfederation.siteminder.CASM_AMPlugin
# For Windows platforms
myAMPlugin.jar=$SF_HOME\\connectors\\siteminder\\CASMConnector.jar
# For Unix flavored platforms
myAMPlugin.jar=$SF_HOME/connectors/siteminder/CASMConnector.jar

idpAuthnPlugin=myAuthnPlugin
myAuthnPlugin.class=com.hp.selectfederation.siteminder.CASM_IDPAuthnPlugin
# For Windows platforms
myAuthnPlugin.jar=$SF_HOME\\connectors\\siteminder\\CASMConnector.jar
# FOR UNIX platforms
myAuthnPlugin.jar=$SF_HOME/connectors/siteminder/CASMConnector.jar
```

Task 2: Configure SiteMinder Policy Servers to authenticate the CA SiteMinder domain-local users.

Perform the following steps to configure the CA SiteMinder Policy Server for authentication through the Select Federation Agent:

- 1 Create and configure a Dummy Basic Realm:
 - a Expand the **Select Federation** domain in the **Domains** tab.
 - b Right-click **Realms** under the Select Federation domain.
 - c Click **Create Realm** in the pop-up window.
The Realm Properties dialog opens.
 - d Fill in the necessary information, including the following required information, then click **OK**:
 - **Agent:** must be the custom agent, **sagentmodule**.
 - **Resource Filter:** must be **/sfBasicResource**.
 - **Authentication Scheme:** must be **Basic**.
 - **Default Resource Protection:** must be set to **Protected**.
- 2 Create and configure a Rule for the Dummy Basic Realm:
 - a Expand **Realms** under the **Select Federation** domain.
 - b Right-click the **dummy Basic Realm** on the left navigation bar.
 - c Click **Create Rule under Realm** in the pop-up window.
The Rule Properties dialog opens as shown in the following example:



- d Fill in the necessary information, including the following required information, then click **OK**:
 - Resource: must be * (star).
 - **Perform regular expression pattern matching**: must be selected.
- 3 Create and configure a Select Federation AM (Access Management) Integrator Realm:
 - a Expand the **Select Federation** domain in the **Domains** tab.
 - b Right-click **Realms** under the Select Federation domain.
 - c Click **Create Realm** in the pop-up window.
The Realm Properties dialog opens.
 - d Fill in the necessary information, including the following required information, then click **OK**:
 - **Agent**: must be the custom agent, **sfagentmodule**.
 - **Resource Filter**: must be **/hpamintegrator/protected**.
 - **Authentication Scheme**: must be **Basic**.
 - **Default Resource Protection**: must be set to **Protected**.
- 4 Create and configure a Rule for the Select Federation AM Integrator Realm:
 - a Expand **Realms** under the **Select Federation** domain.
 - b Right-click the **SF AM Integrator Realm** on the left navigation bar.

- c Click **Create Rule under Realm** in the pop-up window.
The Rule Properties dialog opens.
 - d Fill in the necessary information, including the following required information, then click **OK**:
 - Resource: must be /* (slash star).
 - **Perform regular expression pattern matching**: must be selected.
- 5 Create and configure a Policy for the Dummy Basic Realm and the SF AM Integrator Realm:
- a Right-click **Policies** under the **Select Federation** domain.
 - b Click **Create Policy** in the pop-up window.
The Policy Properties dialog opens.
 - c Fill in the necessary information, including the following required information, then click **OK**:
 - Under the **Rules** tab, add the rules you created earlier for the Dummy Basic Realm and the SF AM Integrator Realm as follows:
 - 1 Select the **Rule(s)** you added and click **Set Response**.
 - 2 Select the **Response** you created earlier and click **OK**.
 - Under the **Users** tab, add all the users who should be authenticated through the Select federation Agent.
 - ▶ • Add all users who should be able to seamlessly access the federated applications offered by trusted partners, using their domain-local credentials.
 - Add users who should be able to access any Select Federation applications such as the Administration console using their domain-local credentials.

Authenticating the SiteMinder Domain-Local Users Through a Login URL

Perform the following tasks to allow any Web Server plus CA SiteMinder Web Agent installation to perform the authentication:

Task 1: Add and configure a redirect-resource.

- 1 Choose the Web Server that has the CA SiteMinder Web Agent of interest installed on it.
- 2 Add a redirect-resource to the Web Server that can do the following:
 - Read the value of a parameter named "E" and if the value is set to 1 then inform the user that an error has occurred.
 - Read the value of a parameter named "RURL" and redirect the user to the parameter.

For a simple sample to use as a guide to create your redirect-resource, see the `$SF-Patch/connectors/siteminder/samples` directory.

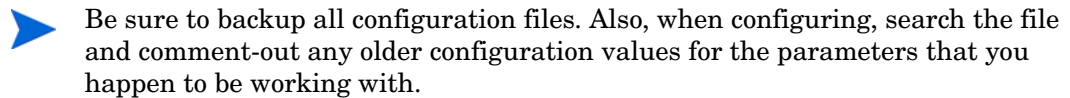
- 3 You must configure the CA SiteMinder Policy Server so that the following requirements are met:
 - CA SiteMinder Web Agent and Authentication Scheme protect the newly added redirect-resource.
 - Policies needed to allow access to the redirect-resource are set.

- Custom authentication scheme (Federation) that you configured earlier, has a value for the **Protection Level** that is equal to or greater than the value for the **Protection Level** of the authentication scheme used to protect the redirect-resource.

Task 2: Configure the SF-IDP.

Perform the following steps to edit the `$SF_HOME/conf/tfsconfig.properties` file at the SF-IDP:

- 1 Comment-out any previous configurations for the `idpAuthnPlugin` parameter.



- 2 Add the following required lines:

```
amPlugin=myAMPlugin
myAMPlugin.class=com.hp.selectfederation.siteminder.CASM_AMPlugin
# For Windows platforms
myAMPlugin.jar=$SF_HOME\\connectors\\siteminder\\CASMConnector.jar
# For Unix flavored platforms
myAMPlugin.jar=$SF_HOME/connectors/siteminder/CASMConnector.jar

idpAuthnPlugin=myAuthnPlugin
myAuthnPlugin.class=com.hp.selectfederation.siteminder.CASM_IDPAuthnPlugin
# For Windows platforms
myAuthnPlugin.jar=$SF_HOME\\connectors\\siteminder\\CASMConnector.jar
# FOR UNIX platforms
myAuthnPlugin.jar=$SF_HOME/connectors/siteminder/CASMConnector.jar
# This must point to the redirect-resource you created and configured
myAuthnPlugin.loginURL=https://my.webserver.com/path/to/redirect-resource
```

Task 3: Configure the SiteMinder Policy Server.

Perform the following steps to configure the CA SiteMinder Policy Server for authentication through a login URL:

- 1 Create and Configure a Dummy Login URL Realm:
 - a Expand the **Select Federation** domain in the **Domains** tab.
 - b Right-click **Realms** under the **Select Federation** domain.
 - c Click **Create Realm** in the pop-up window.
The Realm Properties dialog opens.
 - d Fill in the necessary information, including the following required information, then click **OK**:
 - **Agent:** must be the custom agent, **sfagentmodule**.
 - **Resource Filter:** must be **/sfLoginUriResource**.
 - **Authentication Scheme:** must be the same as the scheme used by the Web Agent that protects the redirect-resource.
 - **Default Resource Protection:** must be set to **Protected**.
- 2 Create and configure a Rule for the Dummy Login URL Realm.
 - a Expand **Realms** under the **Select Federation** domain.
 - b Right-click the **Dummy Login URL Realm** on the left navigation bar.

- c Click **Create Rule under Realm** in the pop-up window.
The Rule Properties dialog opens.
 - d Fill in the necessary information, including the following required information, then click **OK**:
 - **Resource**: must be * (star).
 - **Perform regular expression pattern matching**: must be selected.
- 3 Create and configure a Select Federation AM Integrator Realm:
- a Expand the **Select Federation** domain in the **Domains** tab.
 - b Right-click **Realms** under the Select Federation domain.
 - c Click **Create Realm** in the pop-up window.
The Realm Properties dialog opens.
 - d Fill in the necessary information, including the following required information, then click **OK**:
 - **Agent**: must be the custom agent, **sfagentmodule**.
 - **Resource Filter**: must be **/hpamintegrator/protected**.
 - **Authentication Scheme**: must be a scheme that has a value for the **Protection Level** that is less than or equal to the value for the **Protection Level** of the authentication scheme used to protect the redirect-resource.
 - **Default Resource Protection**: must be set to **Protected**.
- 4 Create and configure a Rule for the Select Federation AM Integrator Realm:
- a Expand **Realms** under the **Select Federation** domain.
 - b Right-click the **SF AM Integrator Realm** on the left navigation bar.
 - c Click **Create Rule under Realm** in the pop-up window.
The Rule Properties dialog opens.
 - d Fill in the necessary information, including the following required information, then click **OK**:
 - **Resource**: must be /* (slash star).
 - **Perform regular expression pattern matching**: must be selected.
- 5 Create and configure a Policy for the Dummy Login URL Realm and the SF AM Integrator Realm:
- a Right-click **Policies** under the **Select Federation** domain.
 - b Click **Create Policy** in the pop-up window.
The Policy Properties dialog opens.
 - c Fill in the necessary information, including the following required information, then click **OK**:
 - Under the **Rules** tab, add the rules you created earlier for the Dummy Login URL Realm and the SF AM Integrator Realm, as follows.
 - 1 Select the **Rule(s)** you added and click **Set Response**.
 - 2 Select the **Response** you created earlier and click **OK**.

- Under the **Users** tab, add all the users who should be authenticated through the login URL.
- ▶
 - Add all users who should be able to seamlessly access the federated applications offered by trusted partners, using their domain-local credentials.
 - Add users who should be able to access any Select Federation applications such as the Administration console using their domain-local credentials.

Step 4: Configure Select Federation SF-IDP Applications

The following sections describe how to configure the Select Federation Administration console and Privacy Manager using either authentication mechanism:

- [Configuring the Administration Console when Authenticating Through the Select Federation Agent](#)
- [Configuring the Privacy Manager when Authenticating Through the Select Federation Agent](#)
- [Configuring the Administration Console when Authenticating Through a Login URL](#)
- [Configuring the Privacy Manager when Authenticating Through a Login URL](#)

Configuring the Administration Console when Authenticating Through the Select Federation Agent

Perform the following tasks to configure the Administration console when authenticating users through the Select Federation Agent:

Task 1: [Create and configure a Realm for the Select Federation Administration console.](#)

- 1 Right-click **Realms** under the **Select Federation** domain.
- 2 Click **Create Realm** in the pop-up window.
The Realm Properties dialog opens.
- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - **Agent:** must be the custom agent, **sagentmodule**.
 - **Resource Filter:** must be **/tfs-internal/admin**.
 - **Authentication Scheme:** must be **Basic**.
 - **Default Resource Protection:** must be set to **Protected**.

Task 2: [Create and configure a Rule for the Select Federation Administration console.](#)

- 1 Expand **Realms** under the **Select Federation** domain.
- 2 Right-click the **Realm** for the Administration console on the left navigation bar.
- 3 Click **Create Rule under Realm** in the pop-up window.
The Rule Properties dialog opens.
- 4 Fill in the necessary information, including the following required information, then click **OK**:
 - **Resource:** must be **/*** (slash star).

- **Perform regular expression pattern matching:** must be selected.

Task 3: [Create and configure a Policy for the Select Federation Administration console.](#)

- 1 Right-click **Policies** under the **Select Federation** domain.
- 2 Click **Create Policy** in the pop-up window.
The Policy Properties dialog opens.
- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - Under the **Users** tab, add all the users who should have access to the Select Federation Administration console.
 - Under the **Rules** tab, add the **Rule** from the Realm for Administration console as follows:
 - 1 Select the **Rule(s)** you added and click **Set Response**.
 - 2 Select the **Response** you created earlier and click **OK**.

Configuring the Privacy Manager when Authenticating Through the Select Federation Agent

For information on how to enable the Privacy Manager, see the “Privacy Manager” chapter in the *HP Select Federation Configuration and Administration Guide*. The following instructions only cover the authentication for the application once it is enabled.

Perform the following tasks to configure the Select Federation Privacy Manager when authenticating users through the Select Federation Agent:

Task 1: [Create and configure a Realm for the Select Federation Privacy Manager.](#)

- 1 Right-click **Realms** under the **Select Federation** domain.
- 2 Click **Create Realm** in the pop-up window.
The Realm Properties dialog opens.
- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - **Agent:** must be the custom agent, **sfagentmodule**.
 - **Resource Filter:** must be **/pm**.
 - **Authentication Scheme:** must be **Basic**.
 - **Default Resource Protection:** must be set to **Protected**.

Task 2: [Create and configure a Rule for the Select Federation Privacy Manager.](#)

- 1 Expand **Realms** under the **Select Federation** domain.
- 2 Right-click the **Realm** for the Privacy Manager.
- 3 Click **Create Rule under Realm** in the pop-up window.
The Rule Properties dialog opens.
- 4 Fill in the necessary information, including the following required information, then click **OK**:

- **Resource:** must be /* (slash star).
- **Perform regular expression pattern matching:** must be selected.

Task 3: Create and configure a Policy for the Select Federation Privacy Manager.

- 1 Right-click **Policies** under the **Select Federation** domain.
- 2 Click **Create Policy** in the pop-up window.
The Policy Properties dialog opens.
- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - Under the **Users** tab, add all the users who should have access to the Select Federation Privacy Manager.
 - ▶ This would usually be all the users that should have access to federated applications.
 - Under the **Rules** tab, add the Rule from the Realm for Privacy Manager.
 - 1 Select the **Rule(s)** you added and click **Set Response**.
 - 2 Select the **Response** you created earlier and click **OK**.

Configuring the Administration Console when Authenticating Through a Login URL

Perform the following tasks to configure the Administration console when authenticating users through the login URL:

Task 1: Create and configure a Realm for the Select Federation Administration console.

- 1 Right-click **Realms** under the **Select Federation** domain.
- 2 Click **Create Realm** in the pop-up window.
The Realm Properties dialog opens.
- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - **Agent:** must be the custom agent, **sfagentmodule**.
 - **Resource Filter:** must be **/tfs-internal/admin**.
 - **Authentication Scheme:** must be a scheme that has a value for the **Protection Level** that is less than or equal to the value for the **Protection Level** of the authentication scheme used to protect the redirect-resource.
 - **Default Resource Protection:** must be set to **Protected**.

Task 2: Create and configure a Rule for the Select Federation Administration console.

- 1 Expand **Realms** under the **Select Federation** domain.
- 2 Right-click the **Realm** for the Administration console.
- 3 Click **Create Rule under Realm** in the pop-up window.
The Rule Properties dialog opens.
- 4 Fill in the necessary information, including the following required information, then click **OK**:

- **Resource:** must be /* (slash star).
- **Perform regular expression pattern matching:** must be selected.

Task 3: Create and configure a Policy for the Select Federation Administration console.

- 1 **Policies** under the **Select Federation** domain.
- 2 Click **Create Policy** in the pop-up window.
The Policy Properties dialog opens.
- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - Under the **Users** tab, add all the users who should have access to the Select Federation Administration console.
 - Under the **Rules** tab, add the Rule from the Realm for Administration console.
 - 1 Select the **Rule(s)** you added and click **Set Response**.
 - 2 Select the **Response** you created earlier and click **OK**.

Configuring the Privacy Manager when Authenticating Through a Login URL

For information on how to enable the Privacy Manager, see the “Privacy Manager” chapter in the *HP Select Federation Configuration and Administration Guide*. The following instructions only cover the authentication for the application once it is enabled.

Perform the following tasks to configure the Select Federation Privacy Manager when authentication users through the login URL:

Task 1: Create and configure a Realm for the Select Federation Privacy Manager.

- 1 Right-click **Realms** under the **Select Federation** domain.
- 2 Click **Create Realm** in the pop-up window.
The Realm Properties dialog opens.
- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - **Agent:** must be the custom agent, **sagentmodule**.
 - **Resource Filter:** must be **/pm**.
 - **Authentication Scheme:** must be a scheme that has a value for the **Protection Level** that is less than or equal to the value for the **Protection Level** of the authentication scheme used to protect the redirect-resource.
 - **Default Resource Protection:** must be set to **Protected**.

Task 2: Create and configure a Rule for the Select Federation Privacy Manager.

- 1 Expand **Realms** under the **Select Federation** domain.
- 2 Right-click the **Realm** for the Privacy Manager on the left navigation bar.
- 3 Click **Create Rule under Realm** in the pop-up window.
The Rule Properties dialog opens.
- 4 Fill in the necessary information, including the following required information, then click **OK**:

- **Resource:** must be /* (slash star).
- **Perform regular expression pattern matching:** must be selected.

Task 3: [Create and configure a Policy for the Select Federation Privacy Manager.](#)

- 1 Right-click **Policies** under the **Select Federation** domain.
- 2 Click **Create Policy** in the pop-up window.
The Policy Properties dialog opens.
- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - Under the **Users** tab, add all the users who should have access to the Select Federation Privacy Manager.
 - Under the **Rules** tab, add the **Rule** from the Realm for Privacy Manager.
 - 1 Select the **Rule(s)** you added and click **Set Response**.
 - 2 Select the **Response** you created earlier and click **OK**.

Step 5: Configure Profile-Attribute-Fetching for Federated Users

Installations that act as authorities (SF-IDP) provide attributes to application partners. Authorities that provide attributes need to fetch these attributes from a data source (referred to as User Directory in SiteMinder). Select Federation includes built-in support for profile-attribute-fetching from LDAP directories, and relational databases as attribute sources.

You need to configure profile-attribute-fetching in Select Federation so that it uses your SiteMinder data source to populate user attributes for outgoing federated users.



The data source that you configure for getting attributes in Select Federation must be the same as the data source used by the SiteMinder Policy Server.

To perform this configuration, go to the “Configuring Attributes” chapter in the HP Select Federation Configuration and Administration Guide for instructions.

Step 6: (Optionally) Test the CA SiteMinder Connector Integration with the Demonstration Application

As a convenience, a Demonstration application is provided with Select Federation that you can use to test your integration. It is meant to emulate a portal page with a list of all the federated applications that are accessible to SiteMinder domain-local users. It is not meant for production use and should only be used for sanity-testing the connector integration.

To use the Demonstration application, complete the instructions in the following sections:

- [Setting Up an Environment for the Demonstration Application](#)
- [Configuring the Demonstration Application](#)
- [Running the Demonstration Application](#)

Setting Up an Environment for the Demonstration Application

Following is a bare-minimum setup for the purposes of testing with the Demonstration application:

- 1 Set up different machines with different site roles:
 - One Select Federation install with the IDP role (which is integrated with CA SiteMinder): SF-IDP
 - One Select Federation install with the SP role: SF-SP.
- 2 Exchange metadata between the following sites:
 - SF-IDP with SF-SP.

If you are not familiar with setting up site roles or exchanging metadata, see the *HP Select Federation Administration and Configuration Guide* for detailed instructions.

Configuring the Demonstration Application

You can configure the Demonstration application in one of two ways

- [Configure the Demonstration Application when Authenticating Through the Select Federation Agent](#)
- [Configure the Demonstration Application when Authenticating Through a Login URL](#)

[Configure the Demonstration Application when Authenticating Through the Select Federation Agent](#)

When you use the Select Federation Agent for authentication, you are limited to CA SiteMinder's Basic Authentication Scheme.

Perform the following tasks to configure the Demonstration application when authenticating through the Select Federation Agent:

Task 1: [Create and configure a Realm for the Select Federation Demonstration Application:](#)

- 1 Right-click **Realms** under the **Select Federation** domain.
- 2 Click **Create Realm** in the pop-up window.
The Realm Properties dialog opens.
- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - **Agent:** must be the custom agent, **sfagentmodule**.
 - **Resource Filter:** must be **/sf-demo/protected**.
 - **Authentication Scheme:** must be **Basic**.
 - **Default Resource Protection:** must be set to **Protected**.

Task 2: [Create and configure a Rule for the Select Federation Demonstration Application.](#)

- 1 Under the **Select Federation** domain, expand **Realms**.
- 2 Right-click the **Realm** for the Demonstration application on the left navigation bar.
- 3 Click **Create Rule under Realm** in the pop-up window.
The Rule Properties dialog opens.

- 4 Fill in the necessary information, including the following required information, then click **OK**:
 - **Resource**: must be /* (slash star).
 - **Perform regular expression pattern matching**: must be selected.

Task 3: Create and configure a Policy for the Select Federation Demonstration Application.

- 1 Right-click **Policies** under the **Select Federation** domain.
- 2 Click **Create Policy** in the pop-up window.
The Policy Properties dialog opens.
- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - Under the **Users** tab, add all the users who should have access to the Select Federation Demonstration Application.
 - ▶ This would usually be all the users that should have access to the federated applications.
 - Under the **Rules** tab, add the Rule from the Realm for Demonstration Application.
 - 1 Select the **Rule(s)** you added and click **Set Response**.
 - 2 Select the **Response** you created earlier and click **OK**.

Configure the Demonstration Application when Authenticating Through a Login URL

The login URL gives you the flexibility to use any Authentication schemes offered by SiteMinder Web Agents. You can use the login URL to point to a resource protected by any SiteMinder Agent, which allows any SiteMinder agent to perform the authentication.

Perform the following tasks to use the login URL to allow any existing SiteMinder Web Agents to perform the authentication:


Task 1: Create and configure a Realm for the Select Federation Demonstration Application.

- 1 Right-click **Realms** under the **Select Federation** domain.
- 2 Click **Create Realm** in the pop-up window.
The Realm Properties dialog opens.
- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - **Agent**: must be the custom agent, **sagentmodule**.
 - **Resource Filter**: must be **/sf-demo/protected**.
 - **Authentication Scheme**: must be a scheme that has a value for the **Protection Level** that is less than or equal to the value for the **Protection Level** of the authentication scheme used to protect the redirect-resource.
 - ▶ It is assumed that the custom authentication scheme (Federation) that you configured earlier, has a value for the **Protection Level** that is equal to or greater than the value for the **Protection Level** of the authentication scheme used to protect the redirect-resource.
 - **Default Resource Protection**: must be set to **Protected**.

Task 2: Create and configure a Rule for the Select Federation Demonstration Application.

- 1 Expand **Realms** under the **Select Federation** domain.
- 2 Right-click the **Realm** for the Demonstration Application on the left navigation bar.
- 3 Click **Create Rule under Realm** in the pop-up window.
The Rule Properties dialog opens.
- 4 Fill in the necessary information, including the following required information, then click **OK**:
 - **Resource**: must be /* (slash star).
 - **Perform regular expression pattern matching**: must be selected.

Task 3: Create and configure a Policy for the Select Federation Demonstration Application.

- 1 Right-click **Policies** under the **Select Federation** domain.
- 2 Click **Create Policy** in the pop-up window.
The Policy Properties dialog opens.
- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - Under the **Users** tab, add all the users who should have access to the Select Federation Demonstration Application.
 This would usually be all the users that should have access to the federated applications.
 - Under the **Rules** tab, add the Rule from the Realm for Demonstration Application.
 - 1 Select the **Rule(s)** you added and click **Set Response**.
 - 2 Select the **Response** you created earlier and click **OK**.

Running the Demonstration Application

To test the SF-IDP with the SF-SP, perform the following steps:

- 1 Navigate to the Demonstration application using the following URL:
`https://<sf-idp-url>:<port>/sf-demo`
The Demonstration application landing page opens.
- 2 Select **Login locally to demo IDP application**.
The Login authentication page opens.
- 3 Enter your domain-local credentials.
The IDP Demonstration page opens.
- 4 Select an available link to the configured SF-SP.

You can now access the application at the SF-IDP as stated in [How an SF-IDP with CA SiteMinder Connector Integration Works with SiteMinder](#) on page 10.

4 Integrating the Select Federation CA SiteMinder Connector with an SP Site

This chapter provides instructions for integrating and configuring the Select Federation CA SiteMinder connector with an SP-only mode installation of Select Federation (SF-SP). The instructions assume knowledge of CA SiteMinder Policy Server terminology and configuration setup. For more details on how to configure authentication schemes, web agents or resources to be protected, see the SiteMinder Policy Server Configuration Guide.

The figures shown in this chapter are examples from the CA SiteMinder Policy Server 6.0.5.10. If you are using a slightly different CA SiteMinder Policy Server 6.0.x.x, navigate to the equivalent locations to perform these operations.

It is important to configure and set appropriate protection for the Select Federation resources in CA SiteMinder.

Requirements

The following requirements must be met before integrating the CA SiteMinder connector with an SF-SP:

- HP Select Federation 7.00 + Patch 7.01 is installed
- CA SiteMinder Policy Server 6.0.x.x is installed
- CA SiteMinder SDK 6.0.x.x is installed (see [Prerequisites](#) on page 9 for the version requirement for your platform)
- CA SiteMinder connector is deployed

CA SiteMinder Connector Integration with an SF-SP

When you integrate the CA SiteMinder connector with an SF-SP, a self-sufficient enterprise that manages its users and applications through CA SiteMinder can enable federated users to access its domain-local applications.

Complete the following main steps to integrate the CA SiteMinder connector with an SF-SP (see each step for instructions):

- [Step 1: Determine a User Activation Scheme](#)
Plug the User Activation scheme into the SF-SP so that it runs before the CA SiteMinder connector runs.
- [Step 2: \(Optionally\) Set User Profile Attributes as a Cookie](#)
Configure the incoming user profile information from an Authority (IDP) partner to be set as a profile cookie.
- [Step 3: Integrate the Select Federation Agent](#)

Configure the SF-SP and the CA SiteMinder Policy Server to use the Select Federation Agent. This component is primarily used for performing authorization. Optionally, it can also be used for authentication.

- **Step 4: Enable Incoming Federated Users**

SSO tokens are issued for the incoming federated users that have been activated.

- **Step 5: Update Application Policies**

Update the policies for the applications that should be accessible to/by federated users.

- **Step 6: Authenticate SiteMinder Domain-Local Users**

You can authenticate SiteMinder domain-local users to have access to Select Federation applications, either through the Select Federation Agent or through a Login URL.

- **Step 7: Configure Select Federation SF-SP Applications**

You need to set policies for the Select Federation applications to configure users who are authorized to access them.

- **Step 8: (Optionally) Test the CA SiteMinder Connector Integration with the Demonstration Application**

You can use the Select Federation Demonstration application to test your integration.

Step 1: Determine a User Activation Scheme

On the SP side when a new user arrives, you need to configure an Activation Event Plugin to activate the new user. The Select Federation CA SiteMinder connector assumes that the user is activated and the `localUserId` of the user is set when the control reaches the Select Federation CA SiteMinder connector in the processing logic. Based on your mapping requirements, there are different ways to configure Select Federation to set up a unique identity mapping between incoming federated users and the users in your SiteMinder environment. See the “Event Plugins” chapter in the *HP Select Federation Configuration and Administration Guide* for more information.

Configuring Select Federation

You need to configure Select Federation in your SP's `$SF_HOME\conf\tfsconfig.properties` file to set up a unique identity mapping between incoming federated users and the users in your CA SiteMinder environment.

To configure Select Federation, perform the following steps to edit the `tfsconfig.properties` file:

- 1 Make a backup copy of the `tfsconfig.properties` file before editing it.
- 2 Edit the `tfsconfig.properties` file according to the Activation Event Plugin for your deployment.

As an example, see [Using the Activate LDAP Plugin for the User Activation Scheme](#) on page 43, which demonstrates how to use one of the event plugins from the “Event Plugins” chapter in the *HP Select Federation Configuration and Administration Guide*.

- 3 Restart the application server.

Using the Activate LDAP Plugin for the User Activation Scheme

These instructions are only for the Activate LDAP Event Plugin. If this Event Plugin does not meet your deployment-specific activation needs, then you should replace it with another one that does.

The following example configuration assumes that the User Activation Scheme is sufficient for your needs. In this case, the user is successfully mapped if an attribute from the incoming federated user's profile can be used to locate a unique user in the directory server.



The Authority (IDP) for the federated user needs to be configured to provide the attribute as part of the user's profile. See the “Configuring the Application Attribute Policy” section in the *HP Select Federation Configuration and Administration Guide* for more information.

This configuration uses the Activate LDAP Event Plugin which is shipped with the product. For more details, see the “Event Plugins” chapter in the *HP Select Federation Configuration and Administration Guide*.

```
#####
### SAMPLE CONFIGURATION
#####
##
## Always be careful and back-up the file.
## Also, search the file to comment-out or remove any older
## configurations for the parameters that you happen to be working with.
##
spEventPlugin=outOfBoxActivationEventPlugin
## The class for the activation event plugin
outOfBoxActivationEventPlugin.class=com.trustgenix.tfsSP.util.SPEventPlugin_ActivateLDAP
teLDAP
## You do not want any random IDs
spAutoGenerateLocalUserId=0
## Your LDAP directory information
ldapURL=ldap://localhost:389
ldapPrincipal=cn=Directory Manager
ldapPassword=password
ldapUserBaseDN=dc=selectfed,dc=com
## The name of the attribute whose value should be
## picked up from the user's profile attributes
## in order to perform a search.
## The federated user's IDP will have to be configured
## to provide this as part of the user's profile.
SPEventPlugin_ActivateLDAP.userProfileAttr=personal_email
## The attribute-name in your LDAP directory that will
## have a unique match when a search is performed using
## the value received from the user's profile attributes.
personal_email.ldapAttr=mail
## The attribute-name in your LDAP directory whose value
## should be set as the id of the activated user
ldapUserAttr=cn
```

Step 2: (Optionally) Set User Profile Attributes as a Cookie

On the SP side integration, any incoming user profile information for a federated user from an Authority (IDP) partner can be set as a profile cookie.

Perform the following steps to set the user profile attributes and to set `tfssessionid` as a cookie in the `$SF_HOME/conf/tfsconfig.properties` file:

- 1 Add the following lines:

Add the Profile Attribute Event Plugin to the SP Event Plugin chain:

```
spEventPlugin=<activation_event_plugin> profileCookieEP
profileCookieEP.class=
com.trustgenix.tfsSP.util.SPEventPlugin_ProfileCookie
```

- 2 Optionally, add and configure the optional parameters in the following table that do not have default values.

For parameters with default values, you only need to add them if you want to change the default value.

Parameter Name	Description	Example	Required/ Optional (default value)
ProfileCookieEP.cookieDomain	Cookie Domain	Domain.com	Optional (None)
ProfileCookieEP.cookieName	Profile Cookie Name	HPSFProfileAttrCookie	Optional (HPSFProfileAttrCookie)
ProfileCookieEP.cookiePath	Profile Cookie Path	/	Optional (/)
ProfileCookieEP.tfsSessionIdStrName	Attribute Name within the Cookie which will contain the <code>tfssessionid</code> .	hpSFSessionId	Optional (hpSFSessionId)
ProfileCookieEP.setUserInfoFromIDP	Determines if all information about the user from the IDP is to be set in the cookie. Value=1 sets all user information in the cookie.	1	Optional (0)

Step 3: Integrate the Select Federation Agent

The Select Federation Agent is primarily used for performing authorization. Optionally, it can be used for authentication. You need to configure the SF-SP and CA SiteMinder Policy Server to use the Select Federation Agent.

Complete the following tasks to integrate the Select Federation Agent:

Task 1: Enable the Select Federation Agent at the SF-SP.

- 1 Add the following required lines in the `$SF_HOME/conf/tfsconfig.properties` file, at the SF-SP:

➤ Be sure to backup all configuration files. Also, when configuring, search the file and comment-out any older configuration values for the parameters that you happen to be working with.

```
spEventPlugin=<activation_event_plugin> <profile_cookie_plugin> casmPlugin
casmPlugin.class=com.hp.selectfederation.siteminder.CASM_SPEventPlugin
# For Windows platforms
casmPlugin.jar=$SF_HOME\\connectors\\siteminder\\CASMConnector.jar
# For UNIX platforms
casmPlugin.jar=$SF_HOME/connectors/siteminder/CASMConnector.jar
# SF Agent reads/writes the SM SSO Cookie from/to this domain.
# This is needed because (a) Authentication may have been
# performed by another SiteMinder Web Agent in the domain,
# (b) Other SiteMinder Web Agents may accept third-party cookies.
# Note that the value begins with a dot, for example: .smdomain.com
SFAgentModule.cookieDomain=
# The shared secret that will be configured at the SM Policy Server
# Whatever value is used for agentSecret, the same value must be used
# at all the policy servers that the agent can talk to.
SFAgentModule.agentSecret=
# For Windows platforms
SFAgentModule.jar=$SF_HOME\\connectors\\siteminder\\CASMConnector.jar
# For Unix flavored platforms
SFAgentModule.jar=$SF_HOME/connectors/siteminder/CASMConnector.jar
# The SM Policy Server(s) to contact
SFAgentModule.policyServers=myPolicyServer
# The IP of the SM Policy Server to contact
myPolicyServer.ip=
```

➤ When you start up Select Federation, be sure at least one SiteMinder Policy Server is running so that the CA SiteMinder connector can be initialized properly.

Task 2: Add and configure other optional parameters in the `tfsconfig.properties` file.

All parameters with default values are optional. You only need to add them if you want to change the default value.

➤ To see mock configurations that demonstrate how to use the parameters in the following table, see the `$SF_PATCH/connectors/siteminder/samples` directory.

The following table lists and describes the CA SiteMinder connector parameters that are optional. This table includes parameters for which you would specify values for any of the following reasons:

- to change the default value
- to use additional functionality

➤ Required parameters are shown in the previous step, and therefore are not listed in this table.

Table 3 Select Federation CA SiteMinder Connector Parameters

Parameter Name	Parameter Value	Description	Example	Required/Optional (default value)
SFAgentModule.agentName	String	Name of the Select Federation Agent, which should be registered at the SiteMinder Policy Server(s).	sfagentmodule	Optional (sfagentmodule)
SFAgentModule.cookieName	String	Name of the SiteMinder SSO cookie that the Select Federation Agent reads-from/writes-to the cookie domain.	SMSESSION	Optional (SMSESSION)
SFAgentModule.policyServers	String List	Space-separated list of CA SiteMinder Policy Servers which the SF Agent can contact.	psA psB psC	Required
<policyServer>.ip	String	Part of the contact information about the SiteMinder Policy server: IP address of a policy server.	11.12.13.14	Required
<policyServer>.connectionMin	Integer	Part of the contact information about the SiteMinder Policy server: Number of initial connections. See the SiteMinder documentation and/or the Policy Server configuration to provide this information.	1	Optional (1)
<policyServer>.connectionMax	Integer	Part of the contact information about the SiteMinder Policy server: Maximum number of connections. See the SiteMinder documentation and/or the Policy Server configuration to provide this information.	3	Optional (3)

Table 3 Select Federation CA SiteMinder Connector Parameters

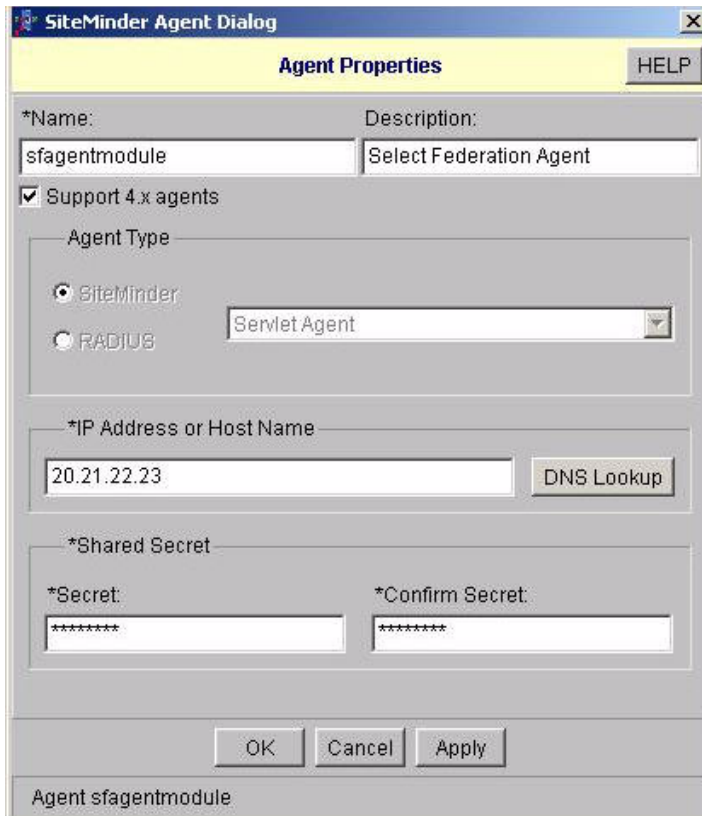
Parameter Name	Parameter Value	Description	Example	Required/ Optional (default value)
<policyServer> .connectionStep	Integer	Part of the contact information about the SiteMinder Policy server: Number of connections to allocate when out of connections. See the SiteMinder documentation and/or the Policy Server configuration to provide this information.	1	Optional (1)
<policyServer> .timeout	Integer	Part of the contact information about the SiteMinder Policy server: Connection timeout in seconds. You may refer to your SiteMinder documentation and/or the Policy Server configuration to provide this information.	75	Optional (75)
<policyServer> .accountingPort	Integer	Part of the contact information about the SiteMinder Policy server: Authentication server port (use 0 for none).	44441	Optional (44441)
<policyServer> .authenticationPort	Integer	Part of the contact information about the SiteMinder Policy server: Authentication server port (use 0 for none) for a SiteMinder policy server.	44442	Optional (44442)
<policyServer> .authorizationPort	Integer	Part of the contact information about the SiteMinder Policy server: Accounting server port (use 0 for none) for a SiteMinder policy server.	44443	Optional (44443)

Task 3: Create and configure a Response.

- 1 Expand the **Select Federation** domain in the **Domains** tab.
- 2 Right-click **Responses** under the *Select Federation* domain.
- 3 Click **Create Response** in the pop-up window.
The SiteMinder Response Dialog opens.
- 4 Fill in the necessary information, including the following required information:
 - **Agent Type:** SiteMinder Servlet Agent.
- 5 Click **Create**.
The SiteMinder Response Attribute Editor opens.
- 6 Fill in the necessary information, including the following required information:
 - **Attribute:** must be **ServletAgent-HTTP-Header-Variable**.
- 7 Select the **Attribute Setup** tab.
- 8 Fill in the necessary information, including the following required information:
 - **Attribute Kind:** must be **User Attribute**.
 - **Variable Name:** must be **SM_USERLOGINNAME**.
 - **Attribute Name:** must be **SM_USERLOGINNAME**.
- 9 Click **OK** to close the SiteMinder Response Attribute Editor.
- 10 Click **OK** to close the SiteMinder Response Dialog.

Task 4: Enable the Select Federation Agent at CA SiteMinder Policy Servers.

- 1 Create and configure a Custom Agent.
 - a Log on to the CA SiteMinder Policy Server Administration console.
 - b Select the **System** tab.
 - c Right-click on **Agents**.
 - d Click **Create Agent** in the pop-up window.
The Agent Properties dialog opens as shown in the following example:

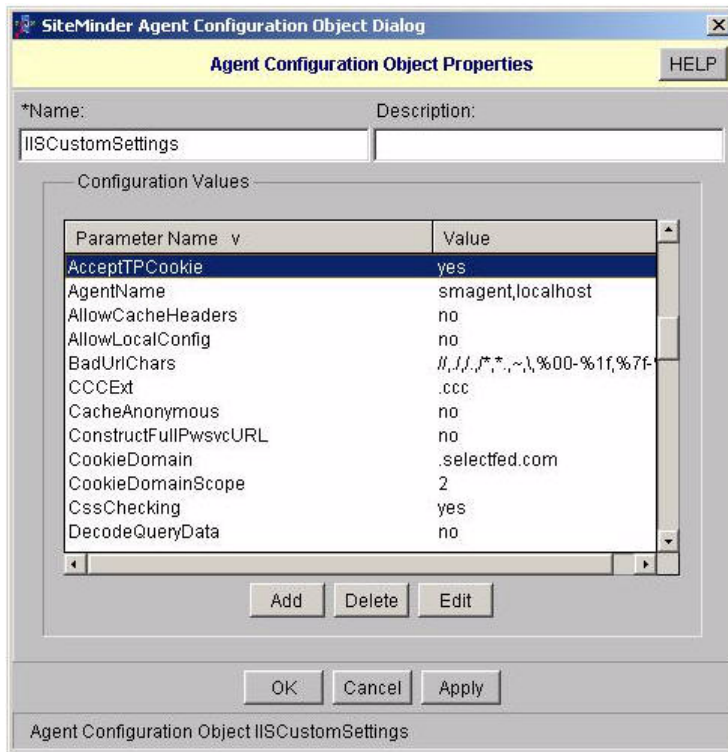


- e Fill in the necessary information, including the following required information, then click **OK**:
 - **Name:** recommended to be **sfagentmodule** unless there are naming conflicts. If there are naming conflicts, you must also make configuration changes in the `tfscnfig.properties` file. See the `SFAgentModule.agentName` parameter in [Table 3](#) on page 46.
 - **Support 4.x agents:** check box must be selected.
 - **Agent Type:** must be a SiteMinder Servlet Agent.
 - **IP Address or HostName:** should point to the machine on which Select Federation is installed.
 - **Shared Secret:** fields must match the value you will provide the Agent that sits with Select Federation. You should have configured the value for the `SFAgentModule.agentSecret` parameter.
- 2 Configure existing Agents to work with the Custom Agent.

Perform the following instructions only for the Agent or Agents that host a SiteMinder domain-local application, which should be accessible to federated users.

- a Select **Agent Conf Objects** in the **System** tab.
- b Double-click the agent configuration object from the **Agent Conf Object List** that applies to your Agent.

The Agent Configuration Object Properties dialog opens as shown in the following example:



- c Click **Add** and set the **AcceptTPCookie** parameter to **yes**.
 - For Agents to work together, the cookie domain used by them must be the same.
- d Click **OK**.

Step 4: Enable Incoming Federated Users

Complete the following tasks to configure the SF-SP and CA SiteMinder Policy Server so that SSO tokens can be issued for the incoming federated users that have been activated. For details on any tasks related to using the CA SiteMinder Policy Server, see the CA SiteMinder Policy Server documentation.

Task 1: Create and configure a Custom (Federation) Authentication Scheme.

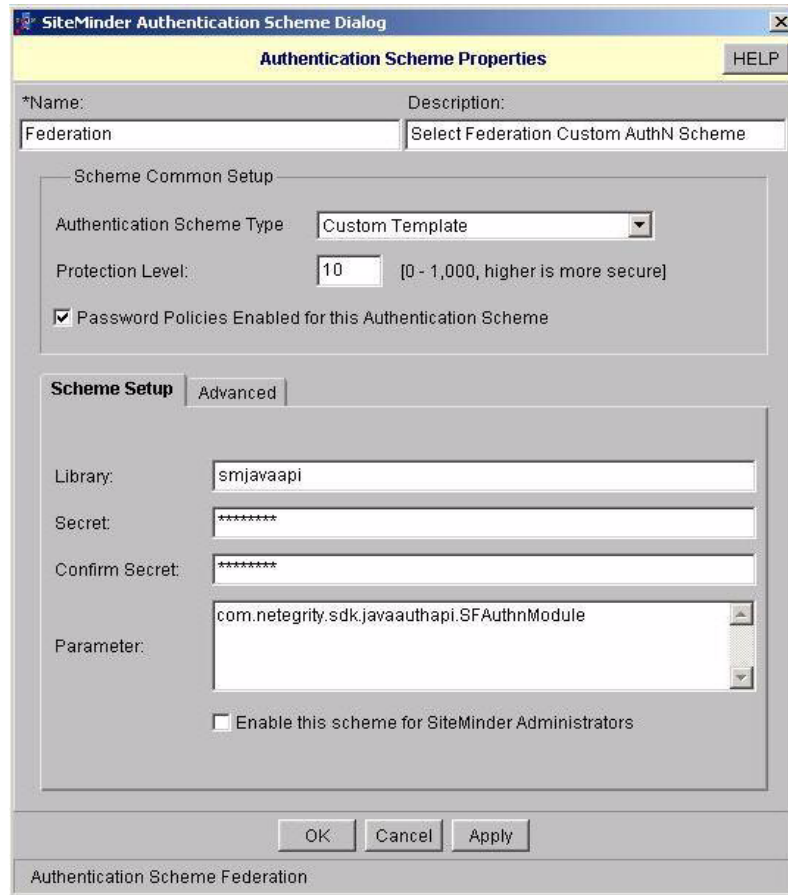
Task 2: Create and configure a domain for Select Federation.

Task 3: Configure a dummy resource for the Custom (Federation) Authentication Scheme.

Task 1: Create and configure a Custom (Federation) Authentication Scheme.

- 1 Right-click **Authentication Schemes** in the **System** tab.
- 2 Click **Create Authentication Scheme** in the pop-up window.

The Authentication Scheme Properties dialog opens as shown in the following example:



- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - **Name:** recommended to be **Federation** unless there are naming conflicts.
 - **Authentication Scheme Type:** must be **Custom Template**.
 - **Protection Level:** must be equal to or higher than any other authentication scheme that you expect federated users to access.
 - **Library:** must be **smjavaapi**.
 - **Parameter:** must be **com.netegrity.sdk.javaauthapi.SFAuthnModule**.

Task 2: Create and configure a domain for Select Federation.

- 1 Select the **Domains** tab.
- 2 Right-click **Domains** on the left navigation bar.
- 3 Click **Create Domain** in the pop-up window.
The Domain Properties dialog opens.
- 4 Fill in the necessary information, including the following required information, then click **OK**:
 - **Name:** recommended to be **SelectFederation** unless there are naming conflicts.

- **User Directories:** add all directories that can disambiguate the users (see the SiteMinder documentation for more information) according to your custom Activation and/or Provisioning implementation of the SP Event Plugin (see [Step 1: Determine a User Activation Scheme](#) on page 42).

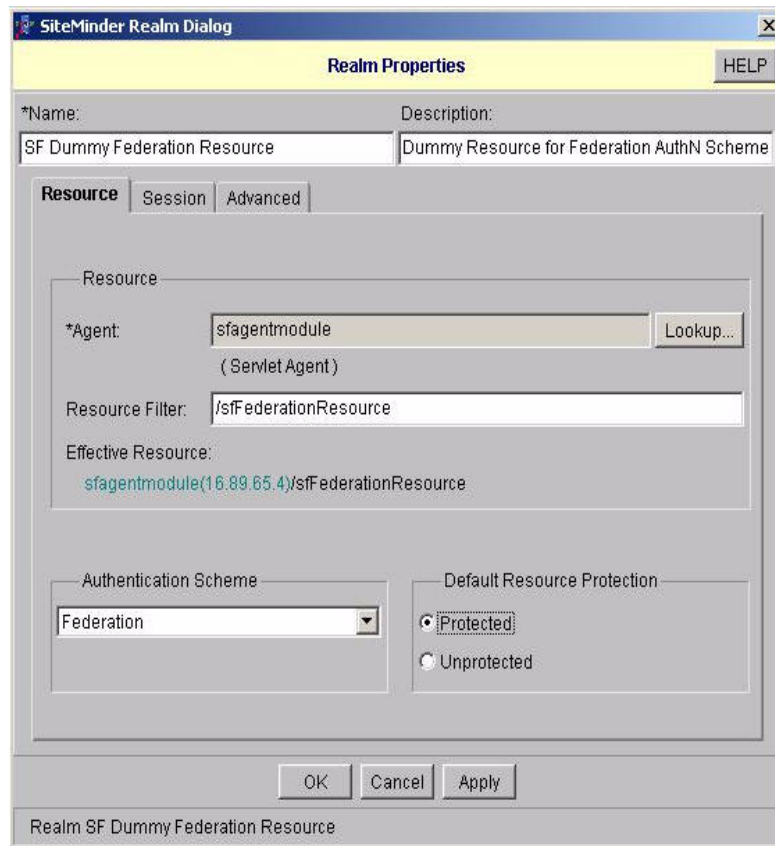
For example, if your User Activation Scheme activates a federated user as `CN=ID-From-Login,OU=smUsers,DC=smDomain,DC=com` then an **LDAP User DN Lookup** such as `(&(objectclass=user)(cn=ID-From-Login))` can be set in your **User Directory Properties** to disambiguate the user.

Task 3: Configure a dummy resource for the Custom (Federation) Authentication Scheme.

To configure the Select Federation Dummy resource, you need to create and configure a Realm as shown in the following steps:

- 1 Expand the **Select Federation** domain in the **Domains** tab.
- 2 Right-click **Realms** under the Select Federation domain.
- 3 Click **Create Realm** in the pop-up window.

The Realm Properties dialog opens as shown in the following example:



- 4 Fill in the necessary information, including the following required information, then click **OK**:
 - **Agent:** must be the custom agent, **sfagentmodule**.
 - **Resource Filter:** must be **/sfFederationResource**.
 - **Authentication Scheme:** must be the custom authentication scheme, **Federation**.

- **Default Resource Protection:** must be set to **Protected**.

Step 5: Update Application Policies

The SiteMinder Web Agents authorize the domain-local application users with the SiteMinder Policy Server. Therefore, you need to update the policies at the SiteMinder Policy Server to give federated users access to the domain-local applications. Once the policies are updated, the SiteMinder Web Agents can authorize the federated users as well. For an example of updating policies for a domain-local application to become accessible to federated users, see [Task 3: Create and configure a Policy for the Select Federation Demonstration Application](#).

Step 6: Authenticate SiteMinder Domain-Local Users

You can perform authentication for SiteMinder domain-local users with the CA SiteMinder Policy Server in one of two ways:

- [Authenticating the SiteMinder Domain-Local Users Through the Select Federation Agent](#) — The Select Federation Agent is limited to CA SiteMinder’s Basic Authentication Scheme.
- [Authenticating the SiteMinder Domain-Local Users Through a Login URL](#) — The login URL can be used to point to a resource protected by any SiteMinder Agent, which allows that agent to perform the authentication. This gives you the flexibility to use any Authentication scheme offered by CA SiteMinder Web Agents.

The following sections describe how to configure the SF-SP and CA SiteMinder Policy Server to perform authentication through the Select Federation Agent and the login URL. Choose one of these ways to perform the authentication for access to Select Federation applications.

Authenticating the SiteMinder Domain-Local Users Through the Select Federation Agent

In this configuration, the authentication scheme is limited to password authentication. This scheme uses the CA SiteMinder SDK for authentication.

Task 1: Configure the SF-SP to authenticate the CA SiteMinder domain-local users.

Perform the following steps to edit the `$SF_HOME/conf/tfsconfig.properties` file at the SF-SP:

- 1 Comment out any previous configurations for the `idpAuthnPlugin` parameter.
 - ▶ Be sure to backup all configuration files. Also, when configuring, search the file and comment-out any older configuration values for the parameters that you happen to be working with.

- 2 Add the following required lines:

```
amPlugin=myAMPlugin
myAMPlugin.class=com.hp.selectfederation.siteminder.CASM_AMPlugin
# For Windows platforms
myAMPlugin.jar=$SF_HOME\\connectors\\siteminder\\CASMConnector.jar
# For UNIX platforms
myAMPlugin.jar=$SF_HOME/connectors/siteminder/CASMConnector.jar

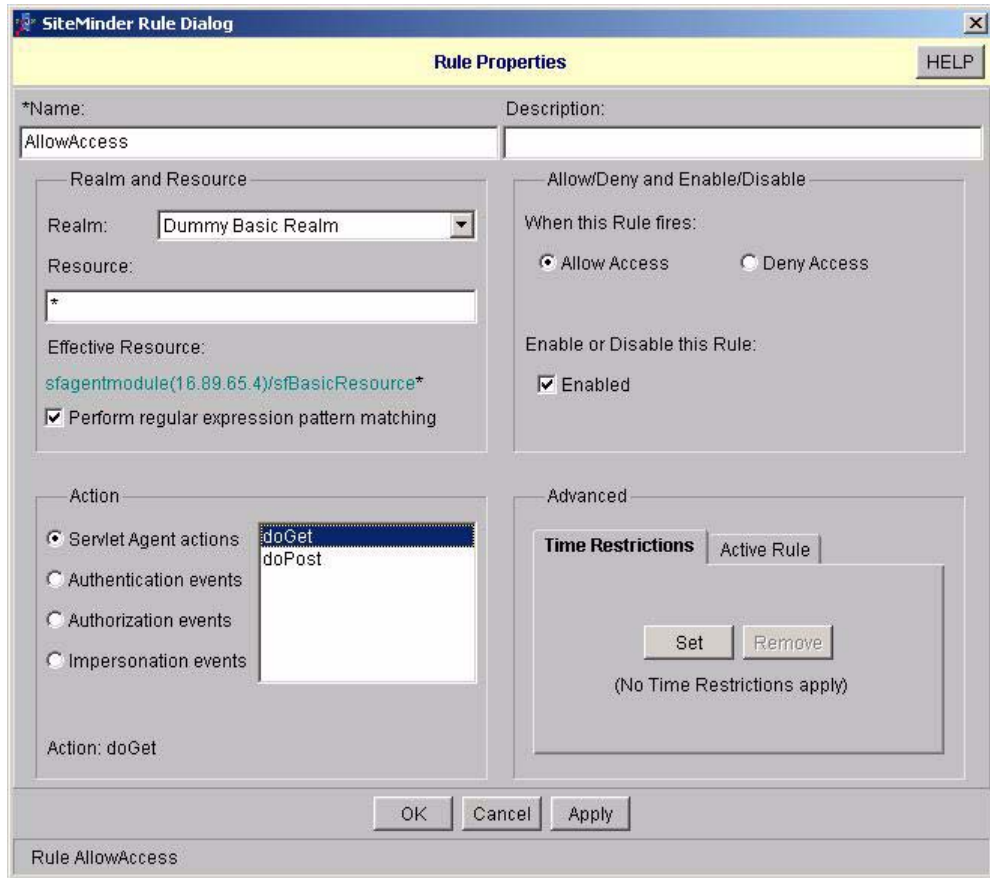
idpAuthnPlugin=myAuthnPlugin
myAuthnPlugin.class=com.hp.selectfederation.siteminder.CASM_IDPAuthnPlugin
```

```
# For Windows platforms
myAuthnPlugin.jar=$SF_HOME\\connectors\\siteminder\\CASMConnector.jar
# FOR UNIX platforms
myAuthnPlugin.jar=$SF_HOME/connectors/siteminder/CASMConnector.jar
```


Task 2: Configure CA SiteMinder Policy Server.

Perform the following steps to configure the CA SiteMinder Policy Server for authentication through the Select Federation Agent:

- 1 Create and configure a Dummy Basic Realm:
 - a Expand the **Select Federation** domain in the **Domains** tab.
 - b Right-click **Realms** under the Select Federation domain.
 - c Click **Create Realm** in the pop-up window.
The Realm Properties dialog opens.
 - d Fill in the necessary information, including the following required information, then click **OK**:
 - **Agent:** must be the custom agent, **sagentmodule**.
 - **Resource Filter:** must be **/sfBasicResource**.
 - **Authentication Scheme:** must be **Basic**.
 - **Default Resource Protection:** must be set to **Protected**.
- 2 Create and configure a Rule for the Dummy Basic Realm:
 - a Expand **Realms** under the **Select Federation** domain.
 - b Right-click the **dummy Basic Realm** on the left navigation bar.
 - c Click **Create Rule under Realm** in the pop-up window.
The Rule Properties dialog opens as shown in the following example:



- d Fill in the necessary information, including the following required information, then click **OK**:
 - Resource: must be * (star).
 - **Perform regular expression pattern matching**: must be selected.
- 3 Create and configure a Select Federation AM (Access Management) Integrator Realm:
 - a Expand the **Select Federation** domain in the **Domains** tab.
 - b Right-click **Realms** under the Select Federation domain.
 - c Click **Create Realm** in the pop-up window.
The Realm Properties dialog opens.
 - d Fill in the necessary information, including the following required information, then click **OK**:
 - **Agent**: must be the custom agent, **sfagentmodule**.
 - **Resource Filter**: must be **/hpamintegrator/protected**.
 - **Authentication Scheme**: must be **Basic**.
 - **Default Resource Protection**: must be set to **Protected**.
- 4 Create and configure a Rule for the Select Federation AM Integrator Realm:
 - a Expand **Realms** under the **Select Federation** domain.
 - b Right-click the **SF AM Integrator Realm** on the left navigation bar.

- c Click **Create Rule under Realm** in the pop-up window.
The Rule Properties dialog opens.
 - d Fill in the necessary information, including the following required information, then click **OK**:
 - Resource: must be /* (slash star).
 - **Perform regular expression pattern matching**: must be selected.
- 5 Create and configure a Policy for the Dummy Basic Realm and the SF AM Integrator Realm:
- a Right-click **Policies** under the **Select Federation** domain.
 - b Click **Create Policy** in the pop-up window.
The Policy Properties dialog opens.
 - c Fill in the necessary information, including the following required information, then click **OK**:
 - Under the **Rules** tab, add the rules you created earlier for the Dummy Basic Realm and the SF AM Integrator Realm.:
 - 1 Select the **Rule(s)** you added and click **Set Response**.
 - 2 Select the **Response** you created earlier and click **OK**.
 - Under the **Users** tab, add all the users who should be authenticated through the Select federation Agent.
-  Add users who should be able to access any Select Federation applications, such as the Administration console, using their domain-local credentials.

Authenticating the SiteMinder Domain-Local Users Through a Login URL

Perform the following tasks to allow any Web Server plus CA SiteMinder Web Agent installation to perform the authentication:

Task 1: Add and configure a redirect-resource.

- 1 Choose the Web Server that has the CA SiteMinder Web Agent of interest installed on it.
- 2 Add a redirect-resource to the Web Server that can do the following:
 - Read the value of a parameter named "E" and if the value is set to 1 then inform the user that an error has occurred.
 - Read the value of a parameter named "RURL" and redirect the user to the parameter.

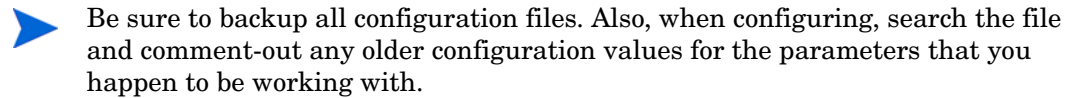
For a simple sample to use as a guide to create your redirect-resource, see the `$SF-Patch/connectors/siteminder/samples` directory.

- 3 You must configure the CA SiteMinder Policy Server so that the following requirements are met:
 - CA SiteMinder Web Agent and Authentication Scheme protect the newly added redirect-resource.
 - Policies needed to allow access to the redirect-resource are set.
 - Custom authentication scheme (Federation) that you configured earlier, has a value for the **Protection Level** that is equal to or greater than the value for the **Protection Level** of the authentication scheme used to protect the redirect-resource.

Task 2: Configure the SF-SP.

Perform the following steps to edit the `$SF_HOME/conf/tfsconfig.properties` file at the SF-SP:

- 1 Comment out any previous configurations for the `idpAuthnPlugin` parameter.



- 2 Add the following required lines:

```
amPlugin=myAMPlugin
myAMPlugin.class=com.hp.selectfederation.siteminder.CASM_AMPlugin
# For Windows platforms
myAMPlugin.jar=$SF_HOME\\connectors\\siteminder\\CASMConnector.jar
# For UNIX platforms
myAMPlugin.jar=$SF_HOME/connectors/siteminder/CASMConnector.jar

idpAuthnPlugin=myAuthnPlugin
myAuthnPlugin.class=com.hp.selectfederation.siteminder.CASM_IDPAuthnPlugin
# For Windows platforms
myAuthnPlugin.jar=$SF_HOME\\connectors\\siteminder\\CASMConnector.jar
# For UNIX platforms
myAuthnPlugin.jar=$SF_HOME/connectors/siteminder/CASMConnector.jar
# This must point to the redirect-resource you created and configured
myAuthnPlugin.loginURL=https://my.webserver.com/path/to/redirect-resource
```

Task 3: Configure the SiteMinder Policy Server.

Perform the following steps to configure the CA SiteMinder Policy Server for authentication through a login URL:

- 1 Create and Configure a Dummy Login URL Realm:
 - a Expand the **Select Federation** domain in the **Domains** tab.
 - b Right-click **Realms** under the **Select Federation** domain.
 - c Click **Create Realm** in the pop-up window.
The Realm Properties dialog opens.
 - d Fill in the necessary information, including the following required information, then click **OK**:
 - **Agent:** must be the custom agent, **sfagentmodule**.
 - **Resource Filter:** must be **/sfLoginUriResource**.
 - **Authentication Scheme:** must be the same as the scheme used by the Web Agent that protects the redirect-resource.
 - **Default Resource Protection:** must be set to **Protected**.
- 2 Create and configure a Rule for the Dummy Login URL Realm.
 - a Expand **Realms** under the **Select Federation** domain.
 - b Right-click the **Dummy Login URL Realm** on the left navigation bar.
 - c Click **Create Rule under Realm** in the pop-up window.
The Rule Properties dialog opens.

- d Fill in the necessary information, including the following required information, then click **OK**:
 - **Resource**: must be * (star).
 - **Perform regular expression pattern matching**: must be selected.
- 3 Create and configure a Select Federation AM Integrator Realm:
 - a Expand the **Select Federation** domain in the **Domains** tab.
 - b Right-click **Realms** under the Select Federation domain.
 - c Click **Create Realm** in the pop-up window.

The Realm Properties dialog opens.
 - d Fill in the necessary information, including the following required information, then click **OK**:
 - **Agent**: must be the custom agent, **sfagentmodule**.
 - **Resource Filter**: must be **/hpamintegrator/protected**.
 - **Authentication Scheme**: must be a scheme that has a value for the **Protection Level** that is less than or equal to the value for the **Protection Level** of the authentication scheme used to protect the redirect-resource.
 - **Default Resource Protection**: must be set to **Protected**.
- 4 Create and configure a Rule for the Select Federation AM Integrator Realm:
 - a Expand **Realms** under the **Select Federation** domain.
 - b Right-click the **SF AM Integrator Realm** on the left navigation bar.
 - c Click **Create Rule under Realm** in the pop-up window.

The Rule Properties dialog opens.
 - d Fill in the necessary information, including the following required information, then click **OK**:
 - **Resource**: must be /* (slash star).
 - **Perform regular expression pattern matching**: must be selected.
- 5 Create and configure a Policy for the Dummy Login URL Realm and the SF AM Integrator Realm:
 - a Right-click **Policies** under the **Select Federation** domain.
 - b Click **Create Policy** in the pop-up window.

The Policy Properties dialog opens.
 - c Fill in the necessary information, including the following required information, then click **OK**:
 - Under the **Rules** tab, add the rules you created earlier for the Dummy Login URL Realm and the SF AM Integrator Realm.:
 - 1 Select the **Rule(s)** you added and click **Set Response**.
 - 2 Select the **Response** you created earlier and click **OK**.

- Under the **Users** tab, add all the users who should be authenticated through the login URL.
- Add users who should be able to access any Select Federation applications such as the Administration console using their domain-local credentials.

Step 7: Configure Select Federation SF-SP Applications

The following sections describe how to configure the Select Federation Administration console using either of the following authentication mechanisms:

- [Configuring the Administration Console when Authenticating Through the Select Federation Agent](#)
- [Configuring the Administration Console when Authenticating Through a Login URL](#)

Configuring the Administration Console when Authenticating Through the Select Federation Agent

Perform the following tasks to configure the Administration console when authenticating users through the Select Federation Agent:

Task 1: [Create and configure a Realm for the Select Federation Administration console.](#)

- 1 Right-click **Realms** under the **Select Federation** domain.
- 2 Click **Create Realm** in the pop-up window.
The Realm Properties dialog opens.
- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - **Agent:** must be the custom agent, **sfagentmodule**.
 - **Resource Filter:** must be **/tfs-internal/admin**.
 - **Authentication Scheme:** must be **Basic**.
 - **Default Resource Protection:** must be set to **Protected**.

Task 2: [Create and configure a Rule for the Select Federation Administration console.](#)

- 1 Expand **Realms** under the **Select Federation** domain.
- 2 Right-click the **Realm** for the Administration console on the left navigation bar.
- 3 Click **Create Rule under Realm** in the pop-up window.
The Rule Properties dialog opens.
- 4 Fill in the necessary information, including the following required information, then click **OK**:
 - **Resource:** must be **/*** (slash star).
 - **Perform regular expression pattern matching:** must be selected.

Task 3: [Create and configure a Policy for the Select Federation Administration console.](#)

- 1 Right-click **Policies** under the **Select Federation** domain.
- 2 Click **Create Policy** in the pop-up window.

The Policy Properties dialog opens.

- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - Under the **Users** tab, add all the users who should have access to the Select Federation Administration console.
 - Under the **Rules** tab, add the Rule from the Realm for Administration console.
 - 1 Select the **Rule(s)** you added and click **Set Response**.
 - 2 Select the **Response** you created earlier and click **OK**.

Configuring the Administration Console when Authenticating Through a Login URL

Perform the following tasks to configure the Administration console when authenticating users through the login URL:

Task 1: Create and configure a Realm for the Select Federation Administration console.

- 1 Right-click **Realms** under the **Select Federation** domain.
- 2 Click **Create Realm** in the pop-up window.

The Realm Properties dialog opens.
- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - **Agent:** must be the custom agent, **sfagentmodule**.
 - **Resource Filter:** must be **/tfs-internal/admin**.
 - **Authentication Scheme:** must be a scheme that has a value for the **Protection Level** that is less than or equal to the value for the **Protection Level** of the authentication scheme used to protect the redirect-resource.
 - **Default Resource Protection:** must be set to **Protected**.

Task 2: Create and configure a Rule for the Select Federation Administration console.

- 1 Expand **Realms** under the **Select Federation** domain.
- 2 Right-click the **Realm** for the Administration console.
- 3 Click **Create Rule under Realm** in the pop-up window.

The Rule Properties dialog opens.
- 4 Fill in the necessary information, including the following required information, then click **OK**:
 - **Resource:** must be **/*** (slash star).
 - **Perform regular expression pattern matching:** must be selected.

Task 3: Create and configure a Policy for the Select Federation Administration console.

- 1 **Policies** under the **Select Federation** domain.
- 2 Click **Create Policy** in the pop-up window.

The Policy Properties dialog opens.

- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - Under the **Users** tab, add all the users who should have access to the Select Federation Administration console.
 - Under the **Rules** tab, add the Rule from the Realm for Administration console.
 - 1 Select the **Rule(s)** you added and click **Set Response**.
 - 2 Select the **Response** you created earlier and click **OK**.

Step 8: (Optionally) Test the CA SiteMinder Connector Integration with the Demonstration Application

As a convenience, a Demonstration application is provided with Select Federation that you can use to test your integration. It is meant to emulate a domain-local application that will be made available to federated users as well. It is not meant for production use and should only be used for sanity-testing the connector integration.

To use the Demonstration application, complete the instructions in the following sections:

- [Setting Up an Environment for the Demonstration Application](#)
- [Configuring the Demonstration Application](#)
- [Running the Demonstration Application](#)

Setting Up an Environment for the Demonstration Application

Following is a bare-minimum setup for the purposes of testing with the Demonstration application:

- 1 Set up different machines with different site roles:
 - One Select Federation install with the SP role (which is integrated with CA SiteMinder): SF-SP
 - One Select Federation install with the IDP role: SF-IDP.
- 2 Exchange metadata between the following sites:
 - SF-SP with SF-IDP.

If you are not familiar with setting up site roles or exchanging metadata, see the *HP Select Federation Administration and Configuration Guide* for detailed instructions.

Configuring the Demonstration Application

You can configure the Demonstration application in one of two ways

- [Configure the Demonstration Application when Authenticating Through the Select Federation Agent](#)
- [Configure the Demonstration Application when Authenticating Through a Login URL](#)

[Configure the Demonstration Application when Authenticating Through the Select Federation Agent](#)

When you use the Select Federation Agent for authentication, you are limited to CA SiteMinder's Basic Authentication Scheme.

Perform the following tasks to configure the Demonstration application when authenticating through the Select Federation Agent:

Task 1: Create and configure a Realm for the Select Federation Demonstration Application:

- 1 Right-click **Realms** under the **Select Federation** domain.
- 2 Click **Create Realm** in the pop-up window.
The Realm Properties dialog opens.
- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - **Agent:** must be the custom agent, **sfagentmodule**.
 - **Resource Filter:** must be **/sf-demo/protected**.
 - **Authentication Scheme:** must be **Basic**.
 - **Default Resource Protection:** must be set to **Protected**.

Task 2: Create and configure a Rule for the Select Federation Demonstration Application.

- 1 Under the **Select Federation** domain, expand **Realms**.
- 2 Right-click the **Realm** for the Demonstration application on the left navigation bar.
- 3 Click **Create Rule under Realm** in the pop-up window.
The Rule Properties dialog opens.
- 4 Fill in the necessary information, including the following required information, then click **OK**:
 - **Resource:** must be **/*** (slash star).
 - **Perform regular expression pattern matching:** must be selected.

Task 3: Create and configure a Policy for the Select Federation Demonstration Application.

- 1 Right-click **Policies** under the **Select Federation** domain.
- 2 Click **Create Policy** in the pop-up window.
The Policy Properties dialog opens.
- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - Under the **Users** tab, add all the users who should have access to the Select Federation Demonstration Application.
 - ▶ Normally, any pre-existing domain-local application already has the domain-local users assigned to it. Since you are setting up the Demonstration application (sf-demo) to emulate a domain-local application, you need to do the following:
 - Add some domain-local users.
 - Add the federated users who will have access to what was previously a domain-local application.
 - Under the **Rules** tab, add the Rule from the Realm for Demonstration Application.
 - 1 Select the **Rule(s)** you added and click **Set Response**.
 - 2 Select the **Response** you created earlier and click **OK**.


Configure the Demonstration Application when Authenticating Through a Login URL

The login URL gives you the flexibility to use any Authentication schemes offered by SiteMinder Web Agents. You can use the login URL to point to a resource protected by any SiteMinder Agent, which allows any SiteMinder agent to perform the authentication.

Perform the following tasks to use the login URL to allow any existing SiteMinder Web Agents to perform the authentication:

Task 1: Create and configure a Realm for the Select Federation Demonstration Application.

- 1 Right-click **Realms** under the **Select Federation** domain.
- 2 Click **Create Realm** in the pop-up window.
The Realm Properties dialog opens.
- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - **Agent:** must be the custom agent, **sfagentmodule**.
 - **Resource Filter:** must be **/sf-demo/protected**.
 - **Authentication Scheme:** must be a scheme that has a value for the **Protection Level** that is less than or equal to the value for the **Protection Level** of the authentication scheme used to protect the redirect-resource.

 An assumption being made is that the custom authentication scheme (Federation) that you configured earlier, has a value for the **Protection Level** that is equal to or greater than the value for the **Protection Level** of the authentication scheme used to protect the redirect-resource.

 - **Default Resource Protection:** must be set to **Protected**.

Task 2: Create and configure a Rule for the Select Federation Demonstration Application.

- 1 Expand **Realms** under the **Select Federation** domain.
- 2 Right-click the **Realm** for the Demonstration Application on the left navigation bar.
- 3 Click **Create Rule under Realm** in the pop-up window.
The Rule Properties dialog opens.
- 4 Fill in the necessary information, including the following required information, then click **OK**:
 - **Resource:** must be **/*** (slash star).
 - **Perform regular expression pattern matching:** must be selected.

Task 3: Create and configure a Policy for the Select Federation Demonstration Application.

- 1 Right-click **Policies** under the **Select Federation** domain.
- 2 Click **Create Policy** in the pop-up window.
The Policy Properties dialog opens.
- 3 Fill in the necessary information, including the following required information, then click **OK**:

- Under the **Users** tab, add all the users who should have access to the Select Federation Demonstration Application.
- ▶ Normally, any pre-existing domain-local application already has the domain-local users assigned to it. Since you are setting up the Demonstration application (sf-demo) to emulate a domain-local application, you need to do the following:
 - Add some domain-local users.
 - Add the federated users who will have access to what was previously a domain-local application.
- Under the **Rules** tab, add the Rule from the Realm for Demonstration Application.
 - 1 Select the **Rule(s)** you added and click **Set Response**.
 - 2 Select the **Response** you created earlier and click **OK**.

Running the Demonstration Application

To run the Demonstration application, perform the following steps:

- 1 Navigate to the Demonstration application using the following URL:

```
https://<sf-idp-url>:<port>/sf-demo
```

The Demonstration application landing page opens.

- 2 Select **Login locally to demo IDP application**.

The Login authentication page opens.

- 3 Enter a user name and password that can be validated against the directory server that was configured during the installation process.

The IDP Demonstration page opens.

- 4 Select an available link to the configured SF-SP.

You can now access the application as stated in [How an SF-SP with CA SiteMinder Connector Integration Works with SiteMinder](#) on page 11.

5 Integrating the Select Federation CA SiteMinder Connector with SP and IDP Sites

This chapter provides instructions for integrating and configuring the Select Federation CA SiteMinder connector with a Select Federation SP and IDP site (SF-SP&IDP). The instructions assume knowledge of CA SiteMinder Policy Server terminology and configuration setup. For more details on how to configure authentication schemes, web agents or resources to be protected, see the CA SiteMinder Policy Server Configuration Guide.

The figures shown in this chapter are examples from the CA SiteMinder Policy Server 6.0.5.10. If you are using a slightly different CA SiteMinder Policy Server 6.0.x.x, navigate to the equivalent locations to perform these operations.

It is important to configure and set appropriate protection for the Select Federation resources in CA SiteMinder.

Requirements

The following requirements must be met before integrating the CA SiteMinder connector with an SF-SP&IDP:

- HP Select Federation 7.00 + Patch 7.01 is installed
- CA SiteMinder Policy Server 6.0.x.x is installed
- CA SiteMinder SDK 6.0.x.x is installed (see [Prerequisites](#) on page 9 for the version requirement for your platform)
- CA SiteMinder connector is deployed

CA SiteMinder Connector Integration with an SF-SP&IDP

When you integrate the CA SiteMinder connector with an SF-SP&IDP, a self-sufficient enterprise that manages its users and applications through CA SiteMinder can do the following:

- Enable federated users from trusted partners to access the SiteMinder domain-local applications.
- Enable its SiteMinder domain-local users to seamlessly access any federated applications offered by its trusted partners.

Complete the following main steps to integrate the CA SiteMinder connector with an SF-SP&IDP (see each step for instructions):

- [Step 1: Prepare the Environment for Federated Applications](#)

For ease of integration into your existing environment, Select Federation provides a special Application Helper component for IDP sites. You can use the Application Helper to generate the URLs for federated applications and then place them at meaningful locations such as Enterprise Portals for users to access.

▶ If you do not have your existing environment set up for a federation yet, you can set up a dummy environment as described in [Step 9: \(Optionally\) Test the CA SiteMinder Connector Integration with the Demonstration Application](#) on page 68, and then complete the following steps.

- [Step 2: Determine a User Activation Scheme](#)
Plug the User Activation scheme into the SF-SP&IDP so that it runs before the CA SiteMinder connector runs.
- [Step 3: \(Optionally\) Set User Profile Attributes as a Cookie](#)
Configure the incoming user profile information from an Authority (IDP) partner to be set as a profile cookie.
- [Step 4: Integrate the Select Federation Agent](#)
Configure the SF-SP&IDP and the CA SiteMinder Policy Server to use the Select Federation Agent. This component is primarily used for performing authorization. Optionally, it can also be used for authentication.
- [Step 5: Enable Incoming Federated Users](#)
SSO tokens are issued for the incoming federated users that have been activated.
- [Step 6: Authenticate SiteMinder Domain-Local Users](#)
You can authenticate SiteMinder domain-local users who should become federation capable either through the Select Federation Agent or through a Login URL.
- [Step 7: Configure Select Federation Applications](#)
The configuration that is used to integrate the SF-SP&IDP with CA SiteMinder for authentication (either the Select Federation Agent or the login URL), is also used to authenticate users to access any Select Federation applications (such as the Administration console and Privacy Manager). You also need to set policies for these applications to configure users who are authorized to access them.
- [Step 8: Configure Profile Attributes for Federated Users](#)
SF-SP&IDP installations provide user attributes contained in a data source to application partners. You need to configure Select Federation to use your data source to populate user attributes for outgoing federated users.
- [Step 9: \(Optionally\) Test the CA SiteMinder Connector Integration with the Demonstration Application](#)
You can use the Select Federation Demonstration application to test your integration.

Step 1: Prepare the Environment for Federated Applications

The Application Helper is a unique feature of Select Federation that simplifies the way in which you initiate federation actions such as federated login and global logout. Use the Application Helper at the SF-SP&IDP to enter a “target URL” that you would like your users to go to after a federated login. The Application Helper will return a transformed URL that you can paste into your portal for your users to click on. When users click on this transformed

URL, they will arrive seamlessly at the target URL using their SiteMinder domain-local credentials. See [Step 1: Prepare the Environment for Federated Applications](#) on page 18 for instructions on preparing the environment for federated applications.

Step 2: Determine a User Activation Scheme

You need to configure an Activation Event Plugin to activate any new federated users that arrive at the SF-SP&IDP from trusted partners. The Select Federation CA SiteMinder connector assumes that the user is activated and the `localUserId` of the user is set when the control reaches the Select Federation CA SiteMinder connector in the processing logic. Based on your mapping requirements, there are different ways to configure Select Federation to set up a unique identity mapping between incoming federated users and the users in your SiteMinder environment. See the “Event Plugins” chapter in the *HP Select Federation Configuration and Administration Guide* for more information on Event Plugins.

For guidelines on how to configure the user activation scheme, see [Configuring Select Federation](#) on page 42.

Step 3: (Optionally) Set User Profile Attributes as a Cookie

On the SF-SP&IDP, any incoming user profile information for a federated user from an Authority (IDP) partner can be set as a profile cookie. This cookie is meant to be used by any domain-local applications, which are being accessed by federated users from truster partners. Follow the instructions in [Step 2: \(Optionally\) Set User Profile Attributes as a Cookie](#) on page 43 to complete this step.

Step 4: Integrate the Select Federation Agent

The Select Federation Agent is primarily used for performing authorization. Optionally, it can be used for authentication. You need to configure the SF-SP&IDP and CA SiteMinder Policy Server to use the Select Federation Agent.

See [Step 3: Integrate the Select Federation Agent](#) on page 44 for instructions.

Step 5: Enable Incoming Federated Users

Configure the SF-SP&IDP and CA SiteMinder Policy Server so that SSO tokens can be issued for the incoming federated users that have been activated. For instructions on enabling incoming federated users, see [Step 4: Enable Incoming Federated Users](#) on page 50.

Step 6: Authenticate SiteMinder Domain-Local Users

CA SiteMinder Policy Server can perform authentication for SiteMinder domain-local users in one of two ways:

- Through the Select Federation Agent — The Select Federation Agent is limited to CA SiteMinder’s Basic Authentication Scheme.
- Through a Login URL — The login URL can be used to point to a resource protected by any SiteMinder Agent, which allows that agent to perform the authentication. This gives you the flexibility to use any Authentication scheme offered by CA SiteMinder Web Agents.

See [Step 3: Authenticate SiteMinder Domain-Local Users](#) on page 26 for instructions on performing authentication through both ways. Choose one of these ways to perform your authentication.

Step 7: Configure Select Federation Applications

The configuration that is used to integrate the SF-SP&IDP with CA SiteMinder for authentication (either the Select Federation Agent or the login URL), is also used to authenticate users to access any Select Federation applications (such as the Administration console and Privacy Manager).

You can configure the Select Federation applications using either of the following authentication mechanisms:

- Select Federation Agent
- Login URL

See [Step 4: Configure Select Federation SF-IDP Applications](#) on page 32 for instructions on configuring the Administration console and Privacy Manager through both mechanisms.

Step 8: Configure Profile Attributes for Federated Users

Installations that act as Authorities (IDP) provide attributes to application partners. Authorities that provide attributes need to get these attributes from a data source. Select Federation includes built-in support for LDAP directories and relational databases as attribute sources. See the “Configuring Attributes” chapter in the *HP Select Federation Configuration and Administration Guide* for instructions on how to configure the SF-SP&IDP to use your data source to populate user attributes for any and all outgoing federated users.

Step 9: (Optionally) Test the CA SiteMinder Connector Integration with the Demonstration Application

As a convenience, a Demonstration application is provided with Select Federation that you can use to test your integration. It is meant to do the following:

- Emulate a portal page with a list of all the federated applications that are accessible to SiteMinder domain-local users.
- Emulate a domain-local application that will be made available to federated users.

The Demonstration application is not meant for production use and should only be used for sanity-testing the connector integration.

To use the Demonstration application, complete the instructions in the following sections:

- [Setting Up an Environment for the Demonstration Application](#)
- [Configuring the Demonstration Application](#)
- [Running the Demonstration Application](#)

Setting Up an Environment for the Demonstration Application

Following is a bare-minimum setup for the purposes of testing with the Demonstration application:

- 1 Set up different machines with different site roles:
 - One Select Federation install with the SP and IDP role (which is integrated with CA SiteMinder): SF-SP&IDP
 - One Select Federation install with the SP role: SF-SP.
 - One Select Federation install with the IDP role: SF-IDP.
- 2 Exchange metadata between the following sites:
 - SF-SP&IDP with SF-SP.
 - SF-SP&IDP with SF-IDP.

If you are not familiar with setting up site roles or exchanging metadata, see the *HP Select Federation Administration and Configuration Guide* for detailed instructions.

Configuring the Demonstration Application

You can configure the Demonstration application in one of two ways

- [Configure the Demonstration Application when Authenticating Through the Select Federation Agent](#)
- [Configure the Demonstration Application when Authenticating Through a Login URL](#)

[Configure the Demonstration Application when Authenticating Through the Select Federation Agent](#)

When you use the Select Federation Agent for authentication, you are limited to CA SiteMinder's Basic Authentication Scheme.

Perform the following tasks to configure the Demonstration application when authenticating through the Select Federation Agent:

Task 1: [Create and configure a Realm for the Select Federation Demonstration Application:](#)

- 1 Right-click **Realms** under the **Select Federation** domain.
- 2 Click **Create Realm** in the pop-up window.
The Realm Properties dialog opens.
- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - **Agent:** must be the custom agent, **sfagentmodule**.
 - **Resource Filter:** must be **/sf-demo/protected**.
 - **Authentication Scheme:** must be **Basic**.
 - **Default Resource Protection:** must be set to **Protected**.

Task 2: [Create and configure a Rule for the Select Federation Demonstration Application.](#)

- 1 Under the **Select Federation** domain, expand **Realms**.
- 2 Right-click the **Realm** for the Demonstration application on the left navigation bar.
- 3 Click **Create Rule** under **Realm** in the pop-up window.

The Rule Properties dialog opens.

- 4 Fill in the necessary information, including the following required information, then click **OK**:
 - **Resource**: must be /* (slash star).
 - **Perform regular expression pattern matching**: must be selected.

Task 3: [Create and configure a Policy for the Select Federation Demonstration Application.](#)

- 1 Right-click **Policies** under the **Select Federation** domain.
- 2 Click **Create Policy** in the pop-up window.

The Policy Properties dialog opens.

- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - Under the **Users** tab, add all the users who should have access to the Select Federation Demonstration Application.
 - ▶ Normally, any pre-existing domain-local application already has the domain-local users assigned to it. Since you are setting up the Demonstration application (`sf-demo`) to emulate a domain-local application, you need to do the following:
 - Add some domain-local users.
 - Add the federated users who will have access to what was previously a domain-local application.
 - Under the **Rules** tab, add the Rule from the Realm for Demonstration Application.
 - 1 Select the **Rule(s)** you added and click **Set Response**.
 - 2 Select the **Response** you created earlier and click **OK**.

[Configure the Demonstration Application when Authenticating Through a Login URL](#)

The login URL gives you the flexibility to use any Authentication schemes offered by SiteMinder Web Agents. You can use the login URL to point to a resource protected by any SiteMinder Agent, which allows any SiteMinder agent to perform the authentication.

Perform the following tasks to use the login URL to allow any existing SiteMinder Web Agents to perform the authentication:

Task 1: [Create and configure a Realm for the Select Federation Demonstration Application.](#)

- 1 Right-click **Realms** under the **Select Federation** domain.
- 2 Click **Create Realm** in the pop-up window.

The Realm Properties dialog opens.

- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - **Agent**: must be the custom agent, **sfagentmodule**.
 - **Resource Filter**: must be **/sf-demo/protected**.

- **Authentication Scheme:** must be a scheme that has a value for the **Protection Level** that is less than or equal to the value for the **Protection Level** of the authentication scheme used to protect the redirect-resource.
- It is assumed that the custom authentication scheme (Federation) that you configured earlier, has a value for the **Protection Level** that is equal to or greater than the value for the **Protection Level** of the authentication scheme used to protect the redirect-resource.
- **Default Resource Protection:** must be set to **Protected**.

Task 2: Create and configure a Rule for the Select Federation Demonstration Application.

- 1 Expand **Realms** under the **Select Federation** domain.
- 2 Right-click the **Realm** for the Demonstration Application on the left navigation bar.
- 3 Click **Create Rule** under **Realm** in the pop-up window.
The Rule Properties dialog opens.
- 4 Fill in the necessary information, including the following required information, then click **OK**:
 - **Resource:** must be /* (slash star).
 - **Perform regular expression pattern matching:** must be selected.

Task 3: Create and configure a Policy for the Select Federation Demonstration Application.

- 1 Right-click **Policies** under the **Select Federation** domain.
- 2 Click **Create Policy** in the pop-up window.
The Policy Properties dialog opens.
- 3 Fill in the necessary information, including the following required information, then click **OK**:
 - Under the **Users** tab, add all the users who should have access to the Select Federation Demonstration Application.

➤ Normally, any pre-existing domain-local application already has the domain-local users assigned to it. Since you are setting up the Demonstration application (sf-demo) to emulate a domain-local application, you need to do the following:

 - Add some domain-local users.
 - Add the federated users who will have access to what was previously a domain-local application.
 - Under the **Rules** tab, add the Rule from the Realm for Demonstration Application.
 - 1 Select the **Rule(s)** you added and click **Set Response**.
 - 2 Select the **Response** you created earlier and click **OK**.

Running the Demonstration Application

Test the SF-SP&IDP with the SF-SP

To test the SF-SP&IDP with the SF-SP, perform the following steps:

- 1 Navigate to the Demonstration application using the following URL:

`https://<sf-sp&idp-url>:<port>/sf-demo`

The Demonstration application landing page opens.

- 2 Select **Login locally to demo IDP application.**

The Login authentication page opens.

- 3 Enter your domain-local credentials.

The IDP Demonstration page opens.

- 4 Select an available link to the configured SF-SP.

You can now access the application at the SF-SP&IDP as stated in [How an SF-IDP with CA SiteMinder Connector Integration Works with SiteMinder](#) on page 10.

Test the SF-SP&IDP with the SF-IDP

To test the SF-SP&IDP with the SF-IDP, perform the following steps:

- 1 Navigate to the Demonstration application using the following URL:

`https://<sf-idp-url>:<port>/sf-demo`

The Demonstration application landing page opens.

- 2 Select **Login locally to demo IDP application.**

The Login authentication page opens.

- 3 Enter a user name and password that can be validated against the directory server that was configured during the installation process.

The IDP Demonstration page opens.

- 4 Select an available link to the configured SF-SP&IDP.

You can now access the application at the SF-SP&IDP as stated in [How an SF-SP with CA SiteMinder Connector Integration Works with SiteMinder](#) on page 11.

6 Error Messages

This chapter lists error messages that are reported by the Select Federation CA SiteMinder Connector. The exact wording may change.

Error Message Terminology

The following terminology is used in the CA SiteMinder connector error messages:

- `CASM_AMPlugin` — Module used for managing access to Select Federation Applications such as Administration console and Privacy Manager.
- `CASM_IDPAuthnPlugin` — Module used for authenticating CA SiteMinder domain-local users.
- `CASM_SPEventPlugin` — Module used for introducing federated users into a CA SiteMinder domain.
- `SFAgentModule` — Module used for conversing with CA SiteMinder Policy Server(s).
- `XXXException` — Exception message from Exception class.
- `XXX` — Represents parameter substitutions.

Error Messages and Descriptions

The CA SiteMinder connector reports error messages for the following plugin modules and utility:

- [CASM_AMPlugin Error Messages](#)
- [CASM_IDPAuthnPlugin Error Messages](#)
- [CASM_SPEventPlugin Error Messages](#)
- [SFAgentModule Error Messages](#)

CASM_AMPlugin Error Messages

The following table lists the `CASM_AMPlugin` error messages and explanations:

Table 4 CASM_AMPlugin Error Messages

Error Message	Explanation
An error occurred: XXXException	An error occurred. Details included in the XXXException message.

CASM_IDPAuthnPlugin Error Messages

The following table lists the CASM_IDPAuthnPlugin error messages and explanations:

Table 5 CASM_IDPAuthnPlugin Error Messages

Error Message	Explanation
User: XXX is not authorized to access the resource: XXX. Please check your SM Policy Server Configuration...	This happens when the user's SSO token has not been issued by the Select Federation Agent. To consider users as authenticated based on a third-party token, they must have access to the XXX resource. This configuration can be corrected at the Policy Server(s).
Cannot URL-encode with UTF-8. XXXException	Details of exception are included in the XXXException message.
Error redirecting to login url. XXXException	Details included in the XXXException message.

CASM_SPEventPlugin Error Messages

The following table lists the CASM_SPEventPlugin error messages and explanations:

Table 6 CASM_SPEventPlugin Error Messages

Error Message	Explanation
User not activated. Please configure an activation event plugin:	Activation exception in CASM_SPEventPlugin. Configure the activation plugin. The user is expected to be activated before control reaches this plugin.

SFAgentModule Error Messages

The following table lists the SFAgentModule error messages and explanations:

Table 7 SFAgentModule Error Message

Error Message	Explanation
Incorrect shared secret: XXX and/or agent name: XXX	The values are inconsistent for the agentSecret and/or agentName parameters configured in the tfconfig.properties file and the fields for the Custom Agent configured at the Policy Server(s).
Login failed, failed to authenticate user: XXX	Invalid credentials.
Logout failed, user was not logged out.	The request to the Policy Server(s) to log the user out failed. It is useful to look at the trace logs on the Policy Server to determine the cause of failure.
Authorization failed, failed to retrieve the user session.	The authorization operation failed because the user session could not be retrieved.
Authorization failed, failed to retrieve <SM_USERLOGINNAME>.	The authorization operation failed because the user's login name could not be retrieved. Check your policies in the SiteMinder Policy Server to make sure that you are returning an appropriate response.
XXX failed, the resource XXX is not protected by this agent, please check your settings at the SM Policy server...	The XXX operation failed because the resource XXX was not configured to be protected by the Select Federation Agent at the Policy Server(s).
XXX failed, could not connect to a Policy Server.	The XXX operation failed because a connection to the Policy Server(s) could not be established. This may happen between Policy Server failovers or if all the Policy Servers happen to be down.

Table 7 SFAgentModule Error Message

Error Message	Explanation
XXX failed, connection timed out.	The XXX operation failed because the connection to the Policy Server timed out. This may happen between failovers, or due to network latency or a heavy load on a Policy Server.
XXX failed, call to XXX() failed, please make sure the Policy Server(s) is/are up and running.	The XXX operation failed at a call to the XXX () method of the SiteMinder SDK. In addition to checking the health of the Policy Server(s), it is also useful to look at the trace logs on the Policy Server to determine any alternate cause(s) of failure.
XXX failed, call to XXX() failed, retcode: XXX	The XXX operation failed at a call to the XXX () method of the SiteMinder SDK with a return code of XXX. It is useful to look at the trace logs on the Policy Server to determine the cause of failure.
Call to XXX() failed, please make sure the Policy Server(s) is/are up and running.	A call to the XXX () method of the SiteMinder SDK failed. In addition to checking the health of the Policy Server(s), it is also useful to look at the trace logs on the Policy Server to determine any alternate cause(s) of failure.
Call to XXX() failed, could not connect to the Policy Server.	A call to the XXX () method of the SiteMinder SDK failed because a connection to the Policy Server(s) could not be established. This may happen between Policy Server failovers or if all the Policy Servers happen to be down.
Call to XXX() failed, retcode: XXX	A call to the XXX () method of the SiteMinder SDK failed with a return code of XXX. It is useful to look at the trace logs on the Policy Server to determine the cause of failure.

A Troubleshooting

Use the Select Federation `log` file to view logged messages. The location of the log file depends on the application server on which you have Select Federation installed. There could be some exceptions caused due to incorrect syntax or configuration. Following are some common problems:

Error

```
com.trustgenix.tfs.TFSEException: netegrity/siteminder/javaagent/AgentAPI
```

Problem

Your application server `CLASSPATH` does not contain SiteMinder SDK `jar` files needed for the integration.

Solution

Check the SiteMinder SDK documentation to determine which `jar` files (hint: `smjavaagentapi.jar`) need to be set in the application server `CLASSPATH`. For details of how to set the `CLASSPATH` for your application server, see your application server documentation.

Error

```
FATAL ERROR: Exception from System.loadLibrary(smjavaagentapi)
java.lang.UnsatisfiedLinkError: no smjavaagentapi in java.library.path

FATAL ERROR: Exception from AgentAPI.initialize()
java.lang.UnsatisfiedLinkError: initialize

com.trustgenix.tfs.ModuleLoader - error instantiating
com.hp.selectfederation.siteminder.CASM_AMPlugin

com.trustgenix.tfs.ModuleLoader - javaagent_api_init
```

Problem

Your system cannot find the SiteMinder SDK's JNI support library when the Java Virtual Machine (JVM) is invoked.

Solution

Check the CA SiteMinder SDK documentation to determine which environment/system variables (hint: `PATH`, `LD_LIBRARY_PATH`, `LIBPATH`, `SHLIB_PATH`) need to be set on your machine, to point to the SDK directory containing the JNI support library. Be sure that your application server can pick up the variables and their values.

Error

com.hp.selectfederation.siteminder.SFAgentModule - The resource is not protected by this agent. Please check your SiteMinder Policy Server configuration...

com.trustgenix.tfs.TFSEException: Internal error, agent failed to obtain realm definition

Problem

The Realm for the CA SiteMinder connector integration was incorrectly configured on the CA SiteMinder Policy Server.

Solution

Double-check your CA SiteMinder Policy Server settings as follows:

- Make sure that you configured the Select Federation Dummy Realm and chose the appropriate Custom Agent module to protect that Realm.
- Make sure that the setting for the Realm indicates that it is protected.

Error

N/A

Problem

Setting the `AcceptTPCookie` to **yes** and restarting the Web Server for the Web Agent configuration changes to take effect, does not seem to help.

Solution

This may happen when the Web Server is restarted too soon. There is a process called LLAWP that shuts down slower than your web server. Make sure that this process has also shut down after shutting down your Web Server and then restart the Web Server.

Error

N/A

Problem

After configuring the CA SiteMinder connector, when attempting to access the Administration console, an empty browser window is displayed after authentication.

Solution

You may not have applied the patch updates. You must update the files (such as the EAR) on the application server as part of the patch. See the HP Select Federation 7.01 Patch Release Notes for instructions.

Glossary

Access Control

The authorization policies and conditions that regulate identity access to resources with a goal towards preventing unauthorized use or use in an unauthorized manner.

Access Management

The process of authentication and authorization.

Activation

Process of setting up mapping from a federated name identifier to a local user ID.

Active Directory Federation Services (ADFS) (WS-Federation 1.0)

A feature of Microsoft Windows 2003 Server R2, which allows a federation with Active Directory-based users, by using the WS-Federation 1.0 protocol.

Active Server Pages (ASP)

Microsoft pages, which log users in by invoking the IDP-FSS over a secure channel. See also [Identity Provider Filter-Support Service \(IDP-FSS\)](#).

ADAM

Active Directory Application Mode

ADFS

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

Administrator

An identity with full permission to manage Select Federation.

API

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

Application Helper

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

Application Program Interface (API)

An interface that enables programmatic access to an application.

Application Site Role

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

Artifact Binding

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

ASP

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

Attribute

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

Authentication

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

Authority Site Role

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

Authorization

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

Bindings

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

CA

Certificate Authority

CardSpace

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

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

Certificate Revocation Checking

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

Context

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

CSR

Certificate Service Request

Delegated Administrator

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

Domain-Local Users

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

DS

Discover Service

DST

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

Edge Router

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

Event

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

Event Plugin Chain

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

Federation

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

Federation Router

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

Filter-Support

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

Filter-Support Service (FSS)

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

FSS

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

GMT

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

Greenwich Mean Time (GMT)

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

Group

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

Identity Mapping

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

Identity Provider Filter-Support Service (IDP-FSS)

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

Identity Provider (IDP)

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

Identity Web Services Framework (ID-WSF)

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

IDP

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

IDP-FSS

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

ID-WSF

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

IE

Internet Explorer

IIS

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

Impersonation Token

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

Inbound Windows Integration (IWI)

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

Integrated Windows Authentication (IWA)

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

Internet Information Server (IIS)

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

IWA

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

IWI

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

JAVA

Object-oriented programming language.

JVM

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

Keystore

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

LDAP

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

LECP

Liberty Enabled Client/Proxy Service.

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

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

Liberty Identity Federation Framework (ID-FF)

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

Lightweight Directory Access Protocol (LDAP)

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

LUAD-WSC

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

Metadata

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

Microsoft Management Console (MMC)

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

MIME

Multipurpose Internet Mail Extension

MMC

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

NTLM (NT LAN Manager)

Default network authentication protocol for Windows NT 4.0.

OCSP

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

Online Certificate Status Protocol (OCSP)

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

Partner

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

Passive URLs

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

PDC

Primary Domain Controller

Plugin

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

POST Binding

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

Presence Service

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

Privacy Manager

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

Protected URLs

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

Protocol

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

Root Administrator

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

SAML

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

Secure Sockets Layer (SSL)

A handshake protocol, which supports server and client authentication.

Service Provider (SP)

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

Single Logout (SLO)

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

Single Sign-On (SSO)

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

Site Role

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

SLO

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

SOAP

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

SP

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

SSC

Self Signed Certificate

SSL

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

SSO

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

TLS

Transport Layer Security

Universal Coordinated Time (UTC)

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

Unprotected URLs

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

UPN

User Principal Name

UTC

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

WAP

Wireless Application Protocol

Web Service Consumer (WSC)

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

Web Service Provider (WSP)

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

WSC

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

WSP

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

Index

A

Administration console

- configuring a Policy at the SF-IDP using the Select Federation agent, 33
- configuring a Policy at the SF-SP using the Select Federation agent, 59
- configuring a Realm at the SF-IDP using the Select Federation agent, 32
- configuring a Realm at the SF-SP using the Select Federation agent, 59
- configuring a Rule at the SF-IDP using the Select Federation agent, 32
- configuring a Rule at the SF-SP using the Select Federation agent, 59
- configuring when authenticating through the SF-IDP Select Federation agent, 32
- configuring when authenticating through the SF-SP Select Federation agent, 59

Application Helper

- idphelper.jsp link to IDP Portal Helper page, 19
- landing page, 19
- using for IDP federated applications, 18
- using for SP&IDP integration, 66

authenticating SiteMinder users

- through the SF-IDP Login URL, 29
- through the SF-IDP Select Federation agent, 26
- through the SF-SP Login URL, 56
- through the SF-SP Select Federation agent, 53

authorization

- Select Federation agent for an SF-IDP integration, 20

C

CA SiteMinder

- logging, 15

CASM_AMPlugin error messages, 73

CASM_IDPAuthnPlugin error messages, 74

CASM_SPEventPlugin error messages, 74

configuring

- Response for the SF-IDP Select Federation agent, 24
- Response for the SF-SP Select Federation agent, 48

custom authentication scheme

- configuring a dummy resource, 52
- creating and configuring for incoming federated users, 50

D

demo activation page, 43

- sample configuration, 43

Demonstration application

- testing the SiteMinder connector integration with an SF-IDP overview, 36
- testing the SiteMinder connector integration with an SF-SP overview, 61
- using to test SiteMinder connector for the SP&IDP integration, 68

deploying

- CA SiteMinder connector, 14
- on the Select Federation application server, 14
- on the SiteMinder Policy Server, 14
- SiteMinder connector files, 14
- SiteMinder Policy Server, 14

dummy resource

- configuring for a custom authentication scheme, 52

E

error messages

- CASM_AMPlugin, 73
- CASM_IDPAuthnPlugin, 74
- CASM_SPEventPlugin, 74
- SFAgentModule, 75
- terminology, 73

I

- IDP integration
 - authenticating SiteMinder domain-local users, 26
 - configuring profile-attribute-fetching, 36
 - configuring SF-IDP applications, 32
 - how the IDP works with the SiteMinder connector, 10
 - integrating Select Federation agent for authorization, 20
 - main steps for the SiteMinder connector integration, 17
 - preparing the environment, 18
 - required lines for `tfsconfig.properties` to enable the Select Federation agent, 20
 - requirements, 17
 - testing with the Demonstration application, 36
- incoming federated users, 50
 - configuring a dummy resource for the custom authentication scheme, 52
 - configuring a Select Federation domain, 51
 - creating and configuring a custom authentication scheme, 50
- introduction, this guide, 9

L

- logging, 15
- Login URL
 - authenticating SiteMinder users at the SF-IDP, 29
 - authenticating SiteMinder users at the SF-SP, 56
 - configuring a redirect-resource at the SF-IDP, 29
 - configuring a redirect-resource at the SF-SP, 56
 - configuring the SF-IDP, 30
 - configuring the SF-SP, 57
 - configuring the SiteMinder Policy Server at the SF-IDP, 30
 - configuring the SiteMinder Policy Server at the SF-SP, 57

P

- parameters
 - CA SiteMinder with SP integration, 44
 - optional for the SF-IDP Select Federation agent, 21
 - optional for the SF-SP Select Federation agent, 45
 - required for the SF-IDP Select Federation agent, 20
 - required for the SF-SP Select Federation agent, 45
 - `SFAgentModule.agentName`, 46
 - `SFAgentModule.cookieName`, 46
 - `SFAgentModule.policyServers`, 46
- passive URLs, 85
- platform requirements, 13
- policies
 - updating for SF-SP applications, 53
- Policy
 - configuring for the SF-IDP Administration console using the Select Federation agent, 33
 - configuring for the SF-SP Administration console using the Select Federation agent, 59
- preparing the environment, for SF-IDP federation applications, 18
- prerequisites, 9, 41

R

- Realm
 - configuring for the SF-IDP Administration console using the Select Federation agent, 32
 - configuring for the SF-SP Administration console using the Select Federation agent, 59
- requirements
 - IDP integration, 17
 - SP&IDP integration, 65
- rolling back, 15
- Rule
 - configuring for the SF-IDP Administration console using the Select Federation agent, 32
 - configuring for the SF-SP Administration console using the Select Federation agent, 59

S

- sample demo activation configuration, 43
- Select Federation
 - configuring a domain for incoming federation users, 51

- Select Federation agent
 - authenticating SiteMinder users at an SF-IDP, 26
 - authenticating SiteMinder users at an SF-SP, 53
 - configuring the SF-IDP to authenticate SiteMinder users, 27
 - configuring the SF-SP to authenticate SiteMinder users, 53
 - configuring the SiteMinder Policy Server at the SF-IDP, 27
 - configuring the SiteMinder Policy Server at the SF-SP, 54
 - creating and configuring a Response at the SF-IDP, 24
 - creating and configuring a Response at the SF-SP, 48
 - enabling at SiteMinder Policy Servers at an SF-IDP, 24
 - enabling at SiteMinder Policy Servers at an SF-SP, 48
 - enabling at the SF-IDP, 20
 - enabling at the SF-SP, 45
 - integrating for an SF-SP, 44
 - integrating for authorization, 20
 - optional parameters for the SF-IDP integration, 21
 - optional parameters for the SF-SP integration, 45
 - required lines for tfsconfig.properties at the SF-IDP, 20
 - required lines for tfsconfig.properties at the SF-SP, 45
 - SP&IDP integration, 67
- Select Federation applications
 - how these applications work with SiteMinder, 11
- SFAgentModule.agentName parameter, 46
- SFAgentModule.cookieName parameter, 46
- SFAgentModule.policyServers parameter, 46
- SFAgentModule error messages, 75
- SiteMinder connector
 - deploying, 14
 - deploying connector files, 14
 - deploying on the Select Federation application server, 14
 - deploying on the SiteMinder Policy Server, 14
- SiteMinder connector integration
 - main steps for an SF-IDP, 17
 - main steps for an SF-SP, 41
 - using Application Helper for an SF-IDP, 18
- SiteMinder Policy Server
 - configuring for authentication through the SF-IDP Select Federation agent, 27
 - configuring for authentication through the SF-SP Select Federation agent, 54
 - configuring for the SF-IDP Login URL, 30
 - configuring for the SF-SP Login URL, 57
 - deploying, 14
- SiteMinder Policy Servers
 - enabling the SF-IDP Select Federation agent, 24
 - enabling the SF-SP Select Federation agent, 48
- SiteMinder SDK
 - versions for supported platforms, 10
- SiteMinder Web Agents
 - authenticating federated users at an SF-IDP, 29
 - authorizing federated users at an SF-SP, 53
- SP&IDP integration
 - authenticating SiteMinder domain-local users, 67
 - configuring profile attributes for federated users, 68
 - configuring Select Federation applications, 68
 - enabling incoming federated users, 67
 - how the SF-SP&IDP works with the SiteMinder connector, 11
 - integrating the Select Federation agent, 67
 - main steps, 65
 - preparing the environment for federated applications, 66
 - requirements, 65
 - setting user profile attributes as a cookie, 67
 - testing the SiteMinder connector integration, 68
 - user activation, 67
 - using the Application Helper, 66
- SP integration
 - authenticating SiteMinder domain-local users, 53
 - CA SiteMinder parameters, 44
 - configuring SF-SP applications, 59
 - enabling incoming federated users, 50
 - how the SP works with the SiteMinder connector, 11
 - integrating Select Federation agent, 44
 - main steps for the SiteMinder connector integration, 41
 - required lines for tfsconfig.properties to enable the Select Federation agent, 45
 - testing with the Demonstration application, 61
 - updating application policies, 53
- system requirements
 - platform, 13
 - software, 13

T

terminology, error messages, 73

testing

- SiteMinder connector with an SF-IDP integration, 36

- SiteMinder connector with an SF-SP integration, 61

tfsconfig.properties file

- edit for user activation, 42

- required lines to enable SF_IDP Select Federation agent, 20

- required lines to enable the SF_SP Select Federation agent, 45

troubleshooting, 77

U

URL classes

- passive, 85

user activation, 42

- configuring Select Federation, 42

- demo activation page for testing, 43

- SP&IDP integration, 67

