HP Select Federation

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

Software Version: 7.01

Oracle COREid 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

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 guide's title page contains the following identifying information:

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

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

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

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

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

Changes to this Document

Chapter	Changes
Documentation Updates	Updated the documentation URL.
Support	Updated this section's information and URLs.
Chapter 2, Deploying the Select Federation Oracle COREid Connector	Updated Software Requirements on page 13. Updated Select Federation Oracle COREid Connector Logging on page 15.
Appendix A, Troubleshooting	Updated the introductory paragraph.

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

The Select Federation Oracle COREid Connector integrates with Select Federation IDP and SP sites, and the Administration Console and Privacy Manager.

This chapter describes the Oracle COREid connector integration with Select Federation in the following topics:

- Select Federation Oracle COREid Connector components
- Prerequisites
- Using the COREid connector with Select Federation

Select Federation Oracle COREid Connector Components

The Select Federation Oracle COREid Connector consists of the following components:

- IDP side component, which includes the Oracle COREid-protected Select Federation Administration Console and Privacy Manager.
- SP side component, which includes the Oracle COREid-protected Select Federation Administration Console and Privacy Manager.

The Select Federation Oracle COREid Connector provides the ability to integrate Select Federation SP and IDP sites with Oracle COREid 7.0.4/10.1.2/10.1.4.

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

Prerequisites

This document assumes you have knowledge of the following:

- HP Select Federation (installation, configuration, concepts and so on)
- Oracle COREid Access 7.0.4/10.1.4 (installation, configuration, concepts and so on)
- Web application servers: Select Federation's built-in server (Tomcat 5.5.23), WebLogic 8.1, 9.1 and 9.2, and WebSphere 6.0.2 (installation, configuration, concepts, and so on)

Using the Select Federation Oracle COREid Connector

Many organizations may already have third-party Access Management systems deployed such as Oracle COREid. These organizations may also assume the role of an identity provider (IDP) or service provider (SP). Select Federation integrates with Oracle COREid out-of-the-box.

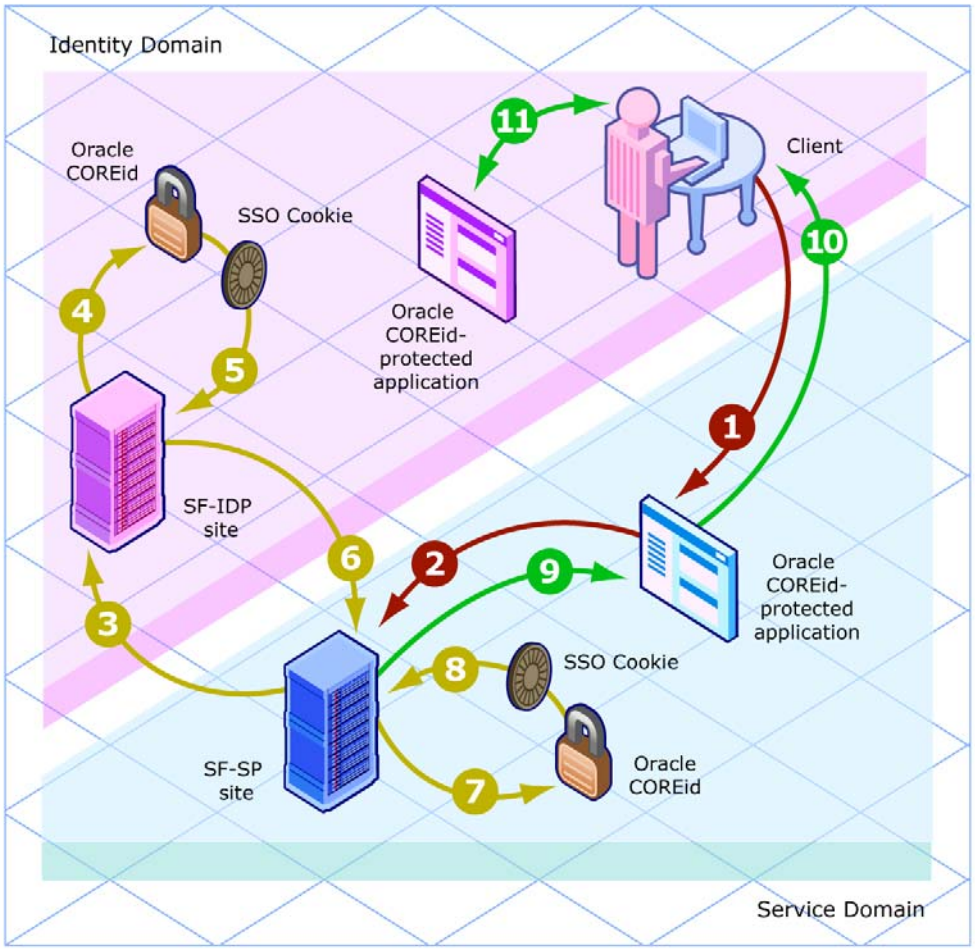
You can choose to integrate Oracle COREid with Select Federation both as an IDP and SP. When you integrate Oracle COREid with an SP or IDP, the Select Federation Administration Console and Privacy Manager are protected by Oracle COREid.

Using Oracle COREid with SP and IDP Integration

The advantage of integrating Oracle COREid with a Select Federation SP and/or IDP site is that once a user is authorized to access an Oracle COREid-protected application in the Service Domain and/or Identity Domain, the user is no longer challenged for credentials and the user has full access each time.

Figure 1 illustrates the process of authorizing a user to access an Oracle COREid-protected application both in the Service and Identity Domains.

Figure 1 Authorization Flow to Access an Oracle COREid-Protected Application



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

1. An unauthenticated user begins at a client, such as a browser, and tries to access an Oracle COREid-protected application in the Service Domain that is integrated with Oracle COREid.
2. The application redirects the user to the SF-SP site.
3. The SF-SP site redirects the user to the SF-IDP site, which is integrated with Oracle COREid for authentication.
4. During the authentication process, the SF-IDP site presents the user with a login page, collects the credentials and calls to the Oracle COREid to generate an Oracle COREid SSO Cookie.
5. Oracle COREid replies with an Oracle COREid SSO cookie for the Identity domain.
6. The SF-IDP returns the user to the SF-SP site after processing the request, to generate an assertion and an Oracle COREid SSO Cookie.
7. The SF-SP site calls out to Oracle COREid to generate an Oracle COREid SSO Cookie for the user using the assertion.
8. Oracle COREid returns the Oracle COREid SSO Cookie for the Service Domain.

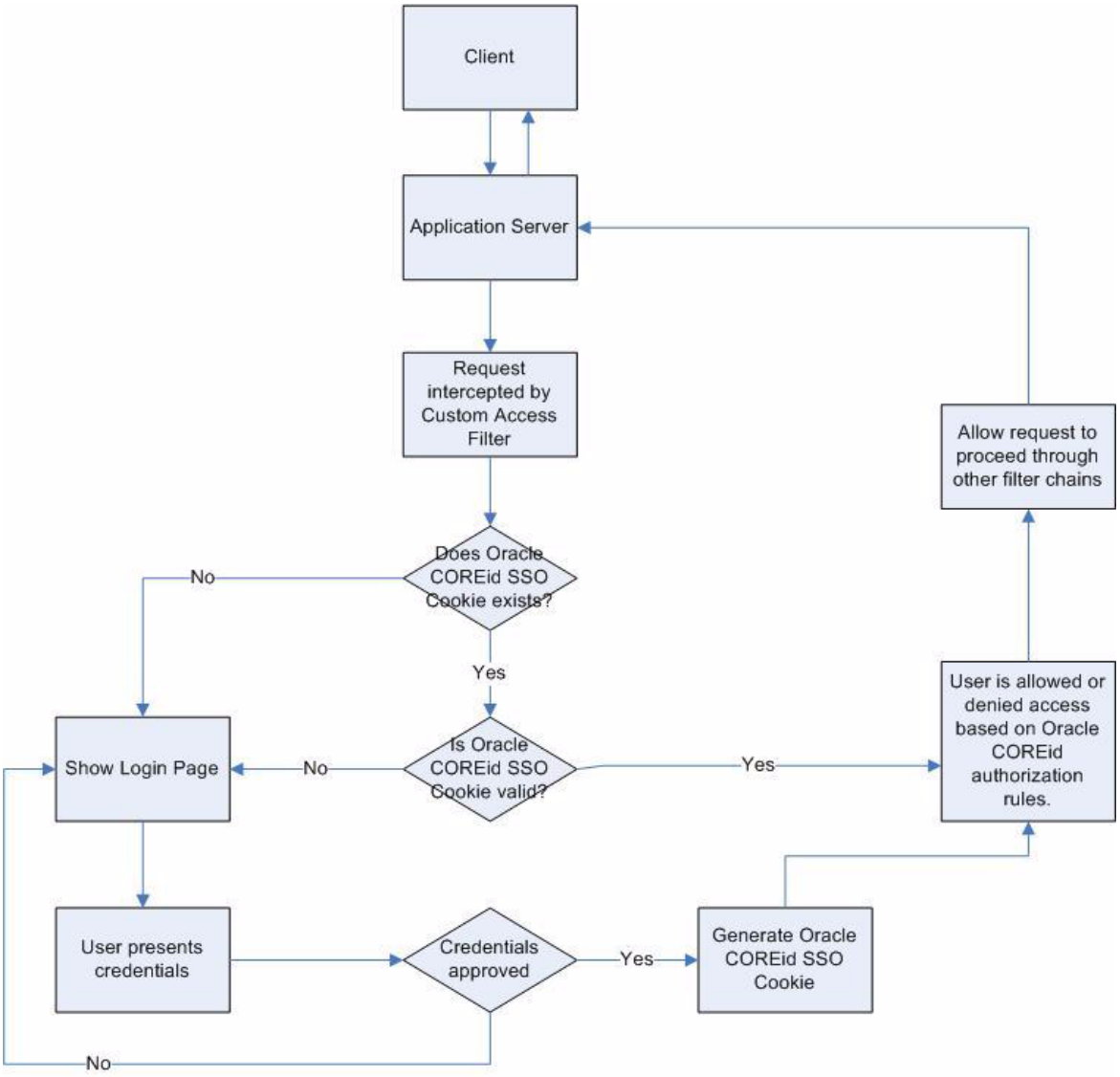
   The user is now authenticated.
9. The SF-SP site returns control to the application in the Service Domain.
10. The application is then presented to the client for the user to access.

    Since the Oracle COREid SSO cookie has been generated for both the Service Domain and Identity Domain, the user is not challenged for credentials again. The user now has access to any application protected by Oracle COREid within both Domains.
11. The user is able to access the application in the Identity Domain without being challenged.

Using Oracle COREid with the Select Federation Administration Console/Privacy Manager

Select Federation Administration console and Privacy Manager are protected with Oracle COREid using an access filter. Figure 2 illustrates a user request flow to an Oracle COREid-protected Administration console.

Figure 2 Flow Diagram of the Administration Console Protected by Oracle COREid



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

1 The user tries to access the Select Federation Administration console on an Application server, from a client such as a browser.

2 The Select Federation Access Filter intercepts the request and checks if a valid Oracle COREid SSO Cookie exists.

3 If a valid Oracle COREid SSO Cookie exists, the Access Filter either allows or denies access to the Administration console and Privacy Manager interfaces.

The decision to allow or deny access is based on the authorization policies configured in Oracle COREid and if the request is allowed. Processing continues to other filters in the chain.

4 If no Oracle COREid SSO Cookie exists or the cookie is not valid, the user is presented with a login page.

5 Once the user presents the credentials, the credentials are validated.

6 If the credentials are valid, the Oracle COREid SSO Cookie is generated, and step 3 is performed.

7 If the credentials are invalid, the user is taken to step 4.

2 Deploying the Select Federation Oracle COREid Connector

This chapter includes the following topics:

System Requirements

Software Requirements

The following software must be installed and configured:

- Select Federation 7.00 plus 7.01 Patch — see the *HP Select Federation Installation Guide* for installation instructions
- Oracle COREid Access Manager 7.0.4 or 10.1.4
- Oracle COREid Access SDK 7.0.4 or 10.1.4

Platform Requirements

The Select Federation Oracle COREid Connector can work on any Select Federation platform that is compatible with the Oracle COREid Access SDK. For every Select Federation install that you want to integrate with Oracle COREid, you must install the Oracle COREid Access SDK on the same machine.

Deploying the Select Federation Oracle COREid Connector

When Select Federation is installed, the following Select Federation Oracle COREid Connector files are automatically deployed in the `<SF_INSTALL_DIR>/connectors/coreid/` directory:

- `COREidConnector.jar`
- `docs/COREid.pdf`

This section provides the basic steps for deploying the Select Federation Oracle COREid Connector files on any application server. For application server-specific instructions, see the application server's documentation.

Perform the following steps to complete the deployment of the Select Federation Oracle COREid Connector:

1 Set the Oracle COREid Access Server SDK environment variables (such as `OBACCESS_INSTALL_DIR`, `PATH`, `CLASSPATH`).

The variables should be set so that they are visible to the application server on which Select Federation is running. See the Oracle Access Server SDK README files for details on which variables need to be set.

2 Depending on whether your site is an IDP or SP, integrate the Select Federation Oracle COREid Connector with one or both of the following areas of Select Federation:

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

See Chapter 3, Integrating the Select Federation Oracle COREid Connector with Select Federation for complete integration and configuration instructions.

3 Restart the application server.

Rolling Back the Select Federation Oracle COREid Connector

You can roll back the Select Federation Oracle COREid Connector from the Select Federation installation. To do this, remove or comment out all Oracle COREid-specific configuration parameters from the `<SF_INSTALL_DIR>/conf/tfsconfig.properties` file you added.

This section describes how to roll back the Select Federation Oracle COREid Connector from the following areas of integration:

- IDP site
- SP site

Rolling Back the Select Federation Oracle COREid Connector From the IDP Integration

Perform the following steps to roll back the Select Federation Oracle COREid Connector from the IDP integration:

1 Comment out the following lines in the `tfsconfig.properties` file:

```
idpAuthnPlugin=myAuthPlugin
myAuthPlugin.class=com.hp.selectfederation.COREidAuthnPlugin
myAuthPlugin.jar=<SF_INSTALL_DIR>/connectors/coreid/COREidConnector.jar
coreidConfigDir=<Access_server_sdk_install>
amPlugin=myAdminPlugin
myAdminPlugin.jar=<SF_INSTALL_DIR>/connectors/coreid/COREidConnector.jar
myAdminPlugin.class=com.hp.selectfederation.coreid.COREidAMPlugin
```

2 Uncomment or add the following line where `<user-base-dn>` is your User repository Base DN and `user-id-attr` is your User ID attribute name:

```
idpAuthnPlugin=com.trustgenix.tfsIDP.util.IDPAuthnPlugin_Dir
ldapUserBaseDN=<user-base-dn>
ldapUserAttr=<user-id-attr>
```

3 Comment out or remove any of the parameters from the table in Integrating the Select Federation Oracle COREid Connector with an IDP Site on page 17 that were added for the Oracle COREid Access Manager integration.

Rolling Back the Select Federation Oracle COREid Connector From the SP Integration

Perform the following steps to roll back the Select Federation Oracle COREid Connector from the SP integration:

1 Comment out the following lines in the `tfsconfig.properties` file:

```
spEventPlugin=myEventPlugin
myEventPlugin.class=com.hp.selectfederation.COREidEventPlugin
myEventPlugin.jar=<SF_INSTALL_DIR>/connectors/coreid/COREidConnector.jar
coreidConfigDir=<Access_server_sdk_install>
amPlugin=myAdminPlugin
myAdminPlugin.jar=<SF_INSTALL_DIR>/connectors/coreid/COREidConnector.jar
myAdminPlugin.class=com.hp.selectfederation.coreid.COREidAMPlugin
```

2 Comment out or remove any of the parameters from the table in Integrating the Select Federation Oracle COREid Connector with an SP Site on page 25 that were added for the Oracle COREid Access Manager integration.

Select Federation Oracle COREid Connector Logging

The Select Federation Oracle COREid connector errors are logged based on settings in the Select Federation `log4j.properties` file in the `<SF_INSTALL_DIR>/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 Oracle COREid Connector with Select Federation

You can integrate the Select Federation Oracle COREid Connector with one or both of the following Select Federation areas:

- SP side
- IDP side

This chapter provides instructions for integrating and configuring the Select Federation Oracle COREid Connector with these Select Federation areas. The instructions assume knowledge of Oracle COREid Access Manager terminology and configuration setup. For more details on how to configure the authentication scheme or configure resources to be protected, see the Oracle COREid Access Manager documentation.

The figures shown in the following sections are examples from the Oracle COREid Access Manager 7.0.4/10.1.2. If you are using Oracle Access Manager 10.1.4, navigate to the equivalent locations to perform these operations.

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

Integrating the Select Federation Oracle COREid Connector with an IDP Site

Overview

Integrating the Select Federation Oracle COREid Connector with an IDP site requires that you configure the Oracle COREid Access Manager and Select Federation. When you integrate the Select Federation Oracle COREid Connector with an IDP site, the Select Federation Administration Console and Privacy Manager are also integrated with Oracle COREid.

There are two integration mechanisms possible for the IDP site:

- Using a Login URL — A resource protected by Oracle COREid WebGates.
- Using a dummy resource — Using a parameter value such as `/selectFederation`, and using the Oracle COREid Access SDK to do the authentication/authorization. The authentication mechanism in this case is limited to password validation.

Using a Login URL

You can use the `coreidLoginURL` login parameter in the `<SF_INSTALL_DIR>/conf/tfsconfig.properties` file. The value for this parameter is a resource that exists on the Web Server. This resource must be protected by the Oracle COREid Access Manager. Based on

the deployment requirements, Oracle COREid Access Manager administrators can configure the authentication mechanism for this resource. Oracle Access Manager administrators can also give access permission to this resource based on the users who are allowed to federate.

The resource being protected by Oracle COREid Access Manager WebGates must be able to read the "RURL" parameter which is passed to it by the login URL, and redirect the user to the value of the "RURL" parameter. For example, a sample-login.jsp protected by Oracle COREid Access Manager WebGate can be as simple as the following code:

```
<%

        String redirectURL = request.getParameter("RURL");
        if (redirectURL != null) {
        response.sendRedirect(redirectURL);
        }
%>
```

Using the Dummy Resource Mechanism

You can configure a dummy resource such as /selectFederation. In this mechanism the authentication scheme is limited to password authentication. This mechanism uses the Oracle COREid Access SDK for authentication.

Configuring the Oracle COREid Access Manager for the IDP Integration

Complete the following basic tasks to configure the Oracle COREid Access Manager for the IDP side integration. For more details on using the Oracle COREid Access Manager, see the Oracle COREid Access Manager documentation.

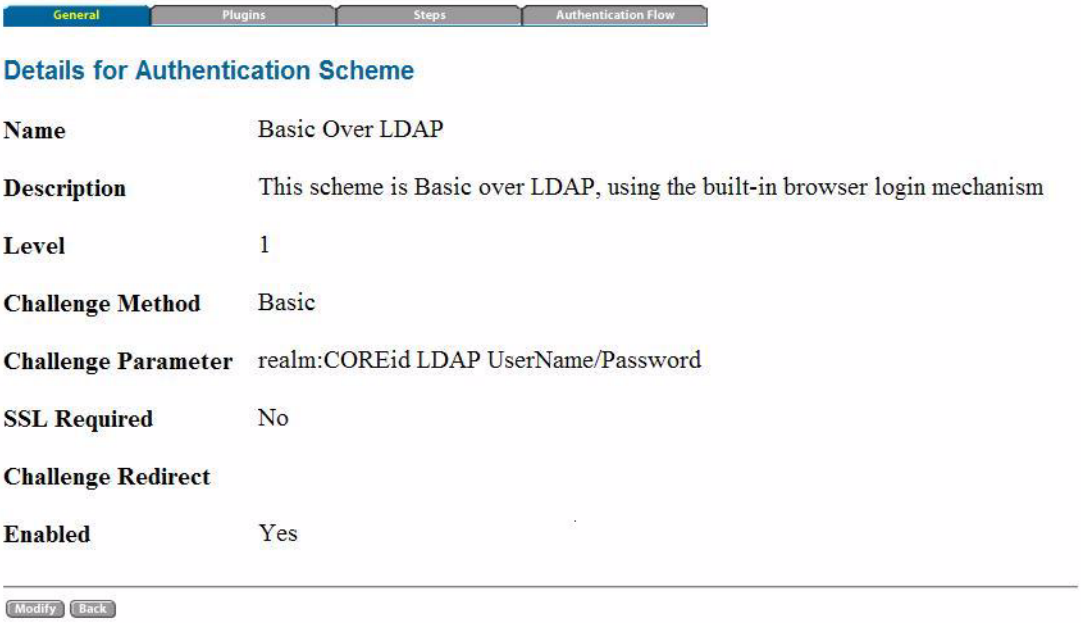
Task 1: Configure the Authentication Scheme

- If you are using the Login URL mechanism for integration, you can configure your resource to be protected by any authentication scheme. Make sure you set the cookieDomain on Oracle COREid WebGate and in the <SF_INSTALL_DIR>/conf/tfsconfig.properties file appropriately.
- If you are using a dummy resource integration mechanism, only the basic challenge method is supported.

Based on your integration mechanism, perform the following steps to add an authentication scheme with necessary plugins, steps and authentication flow.

1. Log in to the Oracle COREid Access Manager System console.
2. Click **Access System Configuration**.
3. Click **Authentication Management** on the left navigation bar.
4. Click **Add** in the right pane to add a new authentication scheme.
5. Fill in the general information for an authentication scheme.

   Following is an example:



6 Add the plugins associated with the authentication scheme.

Following is an example of plugins:

Plugin Name	Plugin Parameters
Credential mapping	`obMappingBase="dc=americas,dc=hpqcorp,dc=net",obMappingFilter=(&(objectclass=inetorgpersonuid=%userid%))"`
validate password	`obCredentialPassword="password"`

7 Enter the **Step Name** to set up the steps for the Authentication scheme.

For example: **Default Step**.

8 Create a flow for the Authentication scheme.

Following is an example:

Task 2: Configure a resource to be protected

Perform the following steps to configure a protected resource:

1 Log in to the Oracle COREid Access Manager.

2 Click **Create Policy Domain** on the left navigation bar of your Oracle COREid Access Manager.

3 Enter the **Policy Domain Name** and **Description**.

4 Add resources to be protected by this policy domain.

5 Add the Authorization rule and the authorization success actions for the Authorization rule.

The figure below shows the variable name and value of the authorization success actions in the **On Success** area of the Authorization Rules.

6 Add the authentication rule and the authorization expression under default rules.

7 Enable your policy domain once you have finished configuring your resource.

Following is an example of the "view as page" mode of the IDP Integration policy domain. You can also define host identifiers in your environment and add resources to be protected appropriately based on your host identifiers.

IDP Integration

Name IDP Integration
Description Oracle Access Manager and Select Federation IDP integration domain
Enabled Yes

Resources

Resource Type	Host Identifiers	URL Prefix	Description
http	hostid	/test	
http	hostid	/selectFederation	

Authorization Rules

Name Allow all
Description
Enabled Yes
Allow takes precedence Yes

On Success
HTTP Header Variable

Type	Name	Return Attribute
HeaderVar	FIRST_NAME	cn
HeaderVar	LAST_NAME	sn

HTTP Header Variable
Allow Access
Role Any one

Default Rules

Authentication Rule

Name Basic
Description Basic
Authentication Scheme Basic Over LDAP

Authorization Expression

Expression *Allow all*

Duplicate Actions No policy defined for this Authorization Expression. The Access System level default policy for dealing with duplicate action headers will be employed.

By default, the COREid Connector sets the User's DN as the federation name in the assertion.

8 If you wish to set another profile attribute instead of the user's DN, add an authorization success action to your IDP Policy Domain in your COREid Access Manager console with the following information:

```
Type : HeaderVar
Name : USER_ID
Return Attribute : <attr>
```

`<attr>` is the profile attribute you want to configure for the `uid`. Following is an example of the authorization success actions:

IDP Integration

Name IDP Integration
Description Oracle Access Manager and Select Federation IDP integration domain
Enabled Yes

Resources

Resource Type	Host Identifiers	URL Prefix	Description
http	hostid	/test	
http	hostid	/selectFederation	

Authorization Rules

Name Allow all
Description
Enabled Yes
Allow takes precedence Yes

On Success
HTTP Header Variable

Type	Name	Return Attribute
HeaderVar	FIRST_NAME	cn
HeaderVar	LAST_NAME	sn
HeaderVar	USER_ID	uid

HTTP Header Variable
Allow Access
Role Any one

Default Rules

Authentication Rule

Name Basic
Description Basic
Authentication Scheme Basic Over LDAP

Authorization Expression

Expression *Allow all*

Duplicate Actions No policy defined for this Authorization

Configuring Select Federation for the IDP Integration

Perform the following steps to configure the `<SF_INSTALL_DIR>/conf/tfsconfig.properties` file for the Oracle COREid integration with the IDP site:

1. Comment out the following line, if it is not already commented out:

   ```
   idpAuthnPlugin=com.trustgenix.tfsIDP.util.IDPAuthnPlugin_Dir
   ```

2. Add the following required lines:

   ```
   idpAuthnPlugin=myAuthPlugin
   myAuthPlugin.class=com.hp.selectfederation.coreid.COREidAuthnPlugin
   myAuthPlugin.jar=<SF_INSTALL_DIR>/connectors/coreid/COREidConnector.jar
   coreidConfigDir=<Access_server_sdk_install>
   amPlugin=myAdminPlugin
   myAdminPlugin.jar=<SF_INSTALL_DIR>/connectors/coreid/COREidConnector.jar
   myAdminPlugin.class=com.hp.selectfederation.coreid.COREidAMPlugin
   ```

   Make the following substitutions in these lines:

   - `<SF_INSTALL_DIR>` = Your IDP Select Federation install directory. For example:

     ```
     c:/test-area/idp/inst7501
     ```

   - `<Access_server_sdk_install>` = Your Oracle COREid Access Server SDK install directory. For example:

     ```
     c:/test-area/orcl/1014/asdk1/AccessServerSDK/
     ```

3. Add and configure the following Oracle COREid parameters that do not have default values, to the `tfsconfig.properties` file.
4. Add and configure required and optional Oracle COREid parameters in the `tfsconfig.properties` file.

All parameters with default values are required. You only need to add them if you want to change the default value. Some parameters without default values are also required. The following table lists and describes the Oracle COREid parameters for an IDP integration:

Parameter Name	Parameter Value	Description	Example	Required/ Optional (default value)
`coreidLoginURL`	URL which is protected by Oracle COREid	Value for this parameter is the URL protected by Oracle COREid Access. This page has the ability to redirect the user back to the originally requested URL. The originally requested URL is appended as a parameter called "`RURL`" to `coreidLoginURL`. This parameter must be set if you are using the login URL mechanism for integration.	**http://idp.company.net:82/test/sample-login.jsp**	Optional (None)

Parameter Name	Parameter Value	Description	Example	Required/ Optional (default value)
coreidConfigDir	Oracle COREid Access SDK install directory	Oracle COREid Access SDK install directory.	C:/test-area/orcl/704/asdk/AccessServerSDK	Required (None)
coreidResrcType	Resource Type	Resource Type of the dummy resource protected by Oracle COREid	http	Required (http)
coreidResrcURL	Resource URL	Dummy Resource URL. If you have host identifiers specified in your Oracle COREid Access Manager, you need to specify the host identifiers as well in the resource. For example, if no host identifiers are defined, your resource may be /selectFederation. If the host identifier is defined as idp, specify your resource as //idp/selectFederation.	/selectFederation	Required (/selectFederation)
coreidResrcMethod	Resource Method	Method to access dummy URL	GET	Required (GET)
coreidCookieDomain	Cookie Domain	Cookie Domain for Oracle COREid SSO Cookie. When you use the coreidLoginURL mechanism for integration, make sure that the cookie domain configuration on the Oracle COREid WebGate allows cookies to be received by the Select Federation IDP.	.domain.com	Optional (None)
coreidBaseURL	Application Server host and port.	Root URL of your application server.	**http://idp.company.net:6500**	Required (None)

5 Configure the Select Federation Directory Plugin settings in the `tfsconfig.properties` file to get user attribute information, as follows:

a Set the `ldapURL`, `ldapPrincipal`, and `ldapPassword` properties. For example:

```
ldapURL=ldap://idp.company.net:400
ldapPrincipal=cn=Directory Manager
ldapPassword=password
```

b Make sure that `ldapUserBaseDN` and `ldapUserAttr` are commented out.

Integrating the Select Federation Oracle COREid Connector with an SP Site

Overview

Integrating the Select Federation Oracle COREid Connector with an SP site requires that you configure the Oracle COREid Access Manager and Select Federation. You can protect your SP Select Federation Administration Console or Privacy Manager with Oracle COREid by using one of the following mechanisms:

- Login URL — A resource protected by Oracle COREid WebGates.
- Dummy resource — Using a parameter value such as `/selectFederation`, and using the Oracle `COREidAccessSDK` to do the authentication/authorization. The authentication mechanism in this case is limited to password validation.

Using a Login URL

You can use the `coreidLoginURL` login parameter in the `<SF_INSTALL_DIR>/conf/tfsconfig.properties` file. The value for this parameter is a resource that exists on the web server. This resource must be protected by the Oracle COREid WebGate. Based on the deployment requirements, Oracle Access Manager administrators can configure the authentication mechanism for this resource. Oracle Access Manager administrators can also give access permission to this resource based on the users who are allowed to access the Select Federation Administration Console.

The resource being protected by Oracle COREid WebGates must be able to read the `"RURL"` parameter which is passed to it by the login URL and redirect the user to the value of the `"RURL"` parameter. For example, a `sample-login.jsp` protected by Oracle COREid WebGate can be as simple as the following code:

```
<%

String redirectURL = request.getParameter("RURL");
if (redirectURL != null) {
response.sendRedirect(redirectURL);
}
%>
```

Using the Dummy Resource Mechanism

You can configure a dummy resource such as `/selectFederation`. In this mechanism, the authentication scheme is limited to password authentication. This mechanism uses the Oracle `COREidAccessSDK` for authentication.

Configuring the Oracle COREid Access Manager for the SP Integration

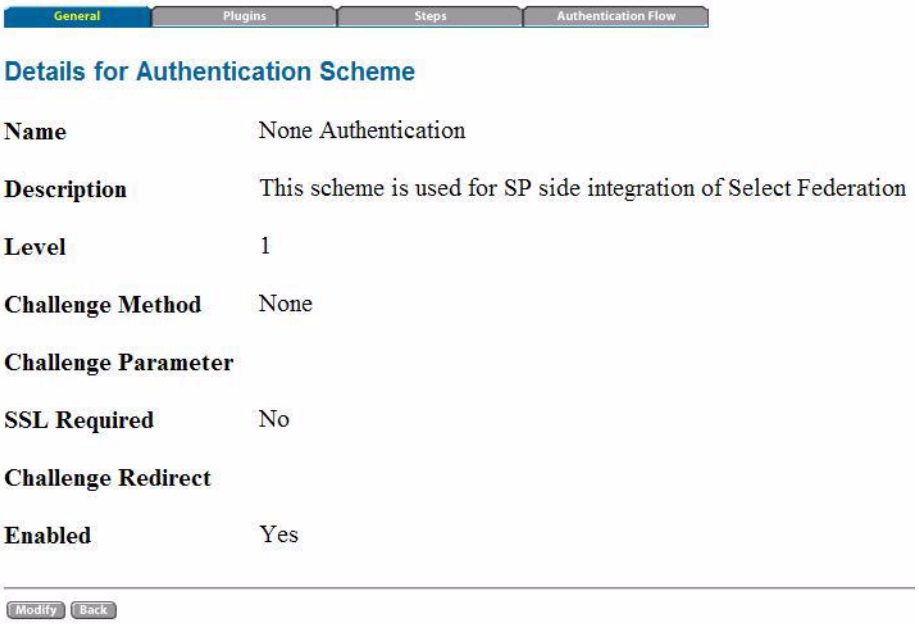
Complete the following basic tasks to configure the Oracle COREid Access Manager for the SP integration. For more details on using the Oracle COREid Access Manager, see the Oracle COREid Access Manager documentation.

Task 1: Configure Authentication Scheme

1. Log in to the Oracle COREid Access Manager System Console.
2. Click **Access System Configuration**.
3. Click **Authentication Management** on the left navigation bar.
4. Click **Add** in the right pane to add a new Authentication scheme.

   For the SP integration, the Challenge Method must **None**.
5. Fill in the general information for an Authentication scheme.

   Following is an example:



6. Add the plugins associated with the scheme.

Following is an example of plugins:

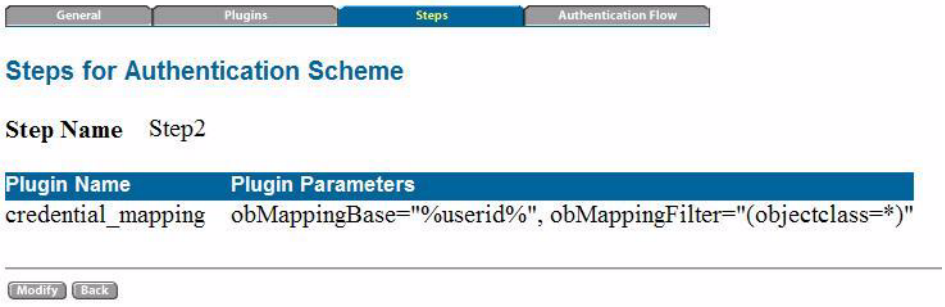
Plugin Name	Plugin Parameters
credential_mapping	obMappingBase="dc=americas,dc=hpqcorp,dc=net",obMappingFilter="(&(objectclass=inetorgperson)(uid=%userid%))"
credential_mapping	obMappingBase="%userid%",obMappingFilter="(objectclass=*)"

7 Set up two steps for the authentication scheme.

Following is an example:

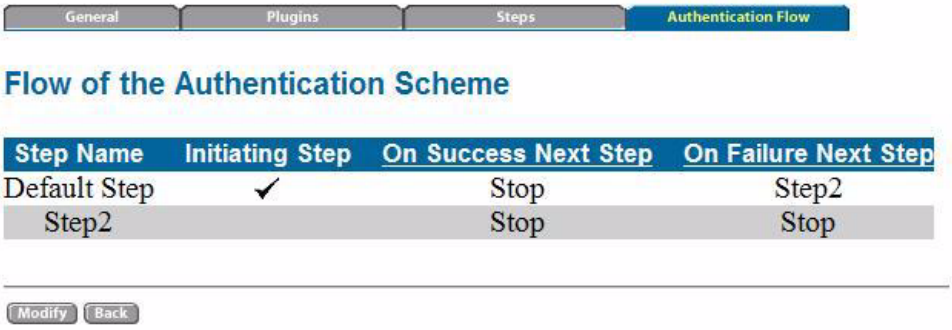
Following is an example of the Default Step definition:

Following is an example of the Step2 definition:



8 Create a flow for the authentication scheme.

Following is an example:

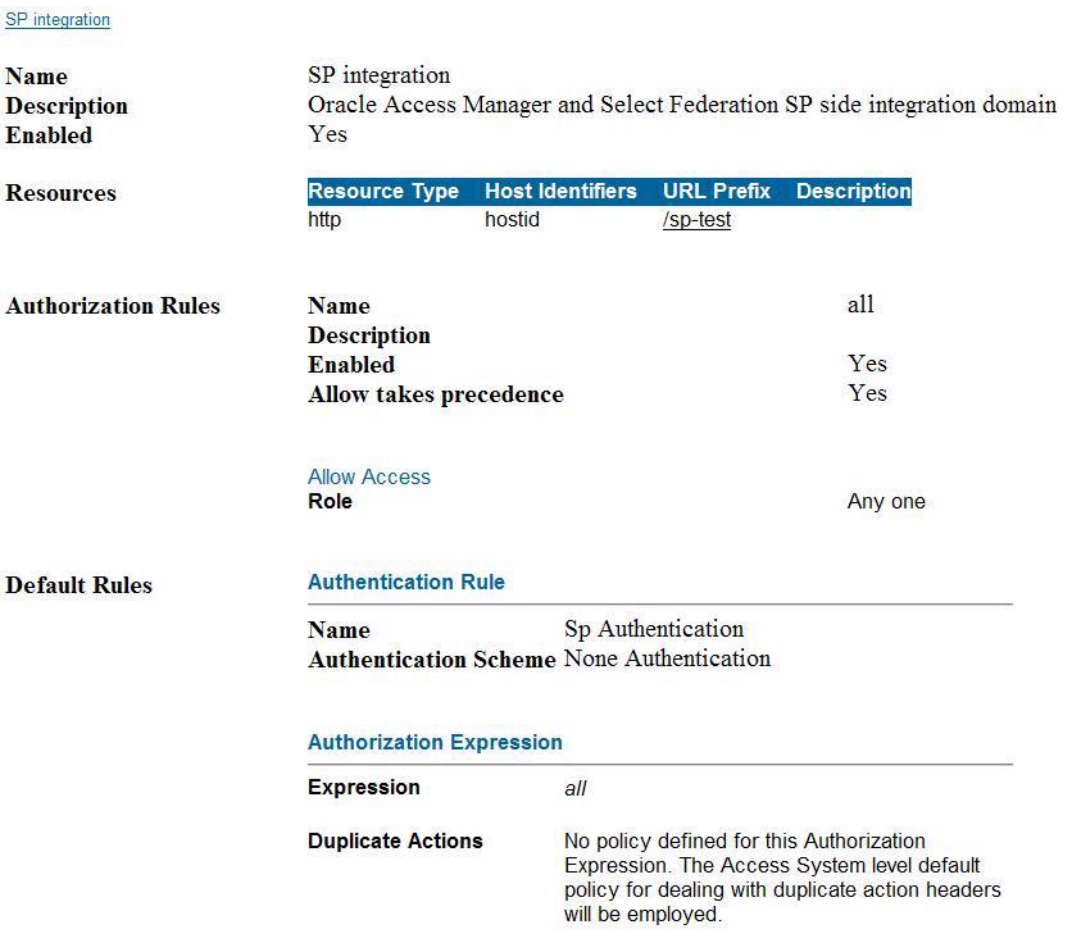


Task 2: Configure the resource to be protected for the SP integration.

Perform the following steps to configure the resource to be protected:

1. Log in to Oracle COREid Access Manager.
2. Click **Create Policy Domain** on the left navigation bar of your Oracle COREid Access Manager.
3. Enter the **Policy Domain Name** and **Description**.
4. Add resources to be protected by this policy domain.
5. Add the authorization rule.
6. Add the authentication rule and the authorization expression under default rules.
7. Enable your policy domain once you have finished configuring your resource.

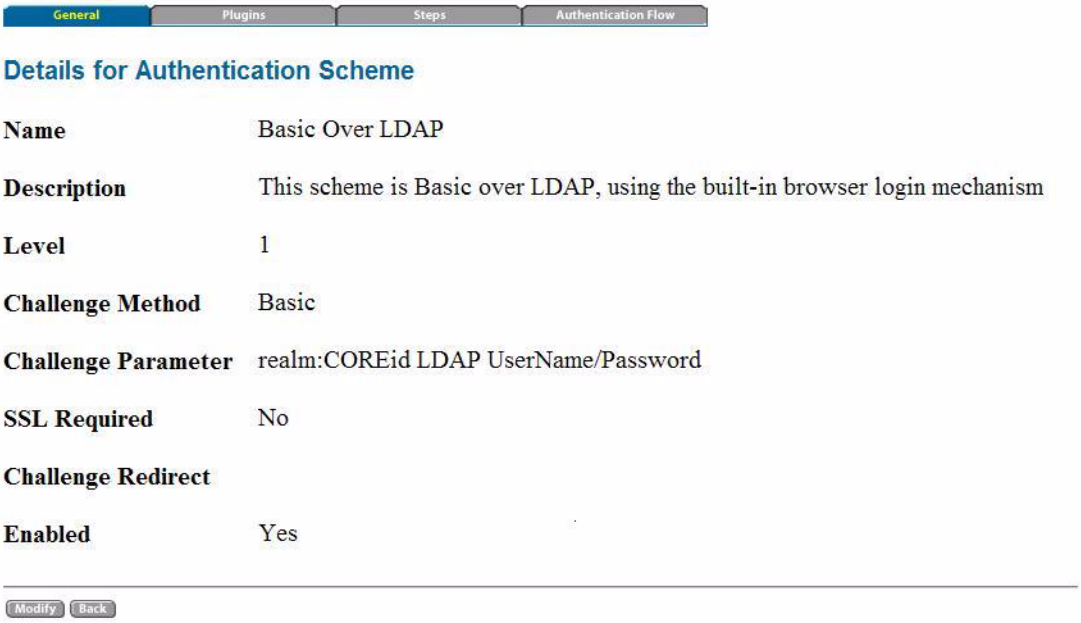
   Following is an example of the “view as page” mode of the SP Integration policy domain. You can also define host identifiers in your environment and add resources to be protected appropriately based on your host identifiers.



Task 3: Configure the Authentication scheme to be used by the Select Federation Administration console and Privacy Manager.

1. Log in to the Oracle COREid Access Manager System Console.
2. Click **Access System Configuration**.
3. Click **Authentication Management** on the left navigation bar.
4. Click **Add** in the right pane to add a new Authentication scheme.
5. Fill in the general information for an Authentication scheme.

   Following is an example:



6 Add the plugins associated with the authentication scheme.

Following is an example of plugins:

Plugin Name	Plugin Parameters
Credential mapping	`obMappingBase="dc=americas,dc=hpqcorp,dc=net",obMappingFilter=(&(objectclass=inetorgpersonuid=%userid%))"`
validate password	`obCredentialPassword="password"`

7 Enter the **Step Name** to set up the steps for the Authentication scheme.

For example: **Default Step**.

8 Create a flow for the Authentication scheme.

Following is an example:

Task 4: Configure a resource to be protected for the Administration console and Privacy Manager integration

Perform the following steps to configure the resource to be protected:

1 Log in to Oracle COREid Access Manager.

2 Click **Create Policy Domain** on the left navigation bar of your Oracle COREid Access Manager.

3 Enter the **Policy Domain Name** and **Description**.

4 Add resources to be protected by this policy domain.

5 Add the Authorization rule and the authorization success actions for the Authorization rule.

The figure below shows the variable name and value of the authorization success actions in the **On Success** area of the Authorization Rules.

6 Add the authentication rule and the authorization expression under default rules.

7 Enable your policy domain once you have finished configuring your resource.

Following is an example of the "view as page" mode of the Administration Console Integration policy domain. You can also define host identifiers in your environment and add resources to be protected appropriately based on your host identifiers.

Admin Console and SF-Demo Integration

Name Admin Console and SF-Demo Integration
Description Oracle Access Manager and Select Federation Admin Console and SF-Demo integration domain
Enabled Yes

Resources

Resource Type	Host Identifiers	URL Prefix	Description
http	hostid	/test	
http	hostid	/selectFederation	

Authorization Rules

Name Allow all
Description
Enabled Yes
Allow takes precedence Yes

On Success
HTTP Header Variable

Type	Name	Return Attribute
HeaderVar	FIRST_NAME	cn
HeaderVar	LAST_NAME	sn

HTTP Header Variable
Allow Access
Role Any one

Default Rules

Authentication Rule

Name Basic
Description Basic
Authentication Scheme Basic Over LDAP

Authorization Expression

Expression *Allow all*

Duplicate Actions No policy defined for this Authorization Expression. The Access System level default policy for dealing with duplicate action headers will be employed.

Configuring Select Federation for the SP Integration

Perform the following steps to configure Select Federation for the SP integration:

1. Add the following required lines to the Select Federation `<SF_INSTALL_DIR>/conf/tfsconfig.properties` file:

   ```
   spEventPlugin=myEventPlugin
   myEventPlugin.class=com.hp.selectfederation.coreid.COREidEventPlugin
   myEventPlugin.jar=<SF_INSTALL_DIR>/connectors/coreid/COREidConnector.jar
   amPlugin=myAdminPlugin
   myAdminPlugin.jar=<SF_INSTALL_DIR>/connectors/coreid/COREidConnector.jar
   myAdminPlugin.class=com.hp.selectfederation.coreid.COREidAMPlugin
   coreidConfigDir=<Access_server_sdk_install>
   ```

   Make the following substitutions in these lines:

   - `<SF_INSTALL_DIR>` = Your SP Select Federation install directory. For example:

     `c:/test-area/sp/inst7501`

   - `<Access_server_sdk_install>` = Your Oracle COREid Access Server SDK install directory. For example:

     `c:/test-area/orcl/704/asdk1/AccessServerSDK/`

2. Add and configure required and optional Oracle COREid parameters in the `tfsconfig.properties` file.

All parameters with default values are required. You only need to add them if you want to change the default value. Some parameters without default values are also required. The following table lists and describes the Oracle COREid parameters:

Parameter Name	Parameter Value	Description	Example	Required/ Optional (default value)
coreidLoginURL	URL which is protected by Oracle COREid and is used for the Select Federation Administration Console and Privacy Manager.	Value for this parameter is the URL protected by Oracle COREid Access. This page can redirect the user back to the originally requested URL. The originally requested URL is appended as a parameter called "RURL" to coreidLoginURL.	**http://sp.company.net:82/test/sample-login.jsp**	Optional (None)
coreidConfigDir	Oracle COREid Access SDK install Directory	Oracle COREid Access SDK install directory.	C:/test-area/orcl/704/asdk/AccessServerSDK	Required (None)
coreidResrcType	Resource Type	Resource Type of the dummy resource protected by Oracle COREid, which is used to protect the Select Federation Administration Console and Privacy Manager.	http	Required (http)
coreidResrcURL	Resource URL used for Oracle COREid Login	Resource URL protected by Oracle COREid, which is used to protect the Select Federation Administration Console and Privacy Manager.	/selectFederation	Required (/selectFederation)

Parameter Name	Parameter Value	Description	Example	Required/ Optional (default value)
coreidCookieDomain	Cookie Domain	Cookie Domain for Oracle COREid SSO Cookie. When you use the coreidLoginURL mechanism for integration, make sure that the cookie domain configuration on the Oracle COREid WebGate allows cookies to be received by the Select Federation SP.	.domain.com	Optional (None)
coreidResrcMethod	Resource method	Method to access dummy URL, which is used to protect the Select Federation Administration Console and Privacy Manager.	GET	Required (GET)
coreidSPResrcType	Resource type	Resource type of the resource protected by the None Authentication Scheme in Oracle COREid.	http	Required (http)
coreidSPResrcMethod	Resource method	Resource method of the resource protected by the None Authentication Scheme in Oracle COREid.	GET	Required (GET)
coreidSPResrcURL	Resource URL	Resource URL of the resource protected by the None Authentication Scheme in Oracle COREid.	/selectFederation	Required (/selectFederation)
coreidBaseURL	Application Server host and port	Root URL of your application server.	**http://sp.company.net:6500**	Required (None)

Setting User Profile Attributes and tfssessionId as a Cookie

On the SP side integration, the incoming user profile information from the IDP can be set as a profile cookie.

Perform the following steps to set the user profile attributes and to set `tfssessionId` as a cookie:

1 Add the following lines to the `<SF_INSTALL_DIR>/conf/tfsconfig.properties` file.

Add Profile Attribute Event Plugin to the sp event plugin chain:

```
spEventPlugin=myEventPlugin profileCookieEP
profileCookieEP.class=
com.trustgenix.tfsSP.util.SPEventPlugin_ProfileCookie
```

2 Optionally, add and configure the following parameters that do not have default values, in the `tfsconfig.properties` file.

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 `tfsSessionId`.	`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)

User Activation

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 Oracle COREid Connector assumes that the user is activated and the `localUserId` of the user is set when the control reaches the Select

Federation Oracle COREid 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 COREid environment. See the “Event Plugins” chapter in the *HP Select Federation Configuration and Administration Guide* for more information.

Editing the tfsconfig.properties File to Configure Select Federation

Configuring Select Federation to set up a unique identity mapping between incoming federated users and the users in your COREid environment, requires that you edit your SP's `<SF_INSTALL_DIR>\conf\tfsconfig.properties` file. When you edit the `tfsconfig.properties` file, be sure to do the following:

1. Make a backup copy of the `tfsconfig.properties` file before editing it.
2. Edit the `tfsconfig.properties` file in the configuration directory of the Application Server — the directory in which the configuration files was copied.
3. Restart the Application Server.

Demo Activation Page for Testing

A demo activation page has been bundled for testing purposes. It shows how an activation page fulfills its responsibilities by mapping the user's identity. In this particular case the user is prompted to provide the user name and password that will allow for a successful ID-mapping against a file plugin. You need to make sure that this user also exists in your COREid environment.

Following is an example configuration in the `tfsconfig.properties` file for a Select Federation SP. This configuration uses the Redirect URL Activation Plugin and sample `activate-demo.jsp` file which is shipped with the product. This example uses the Directory Plugin File. Using the Activate URL EventPlugin results in a redirect to a URL specified by you, thus hooking you into the workflow. This allows you to present and/or execute your own identity-mapping logic to the user.

Do not use `activate-demo.jsp` in your deployments. This is for demo purposes only. Replace the activation plugin with your deployment-specific activation plugin.

Following is the sample configuration:

```
#######################
### DEMO PURPOSES ONLY
#######################
##
## COREid Configurations
spEventPlugin=myActivatePlugin profileCookieEP myEventPlugin
##
myActivatePlugin.class=com.trustgenix.tfsSP.util.SPEventPlugin_ActivateURL
SPEventPlugin_ActivateURL.spActivateURL=http://sp.vm.net:2001/sf-demo/
activate-demo.jsp
##
## settings for File based directory plugin
dirPlugin=com.trustgenix.tfsIDP.util.DirPlugin_File
DirPlugin_File.filePath=C:\\test-area\\sp\\inst2001\\properties\\users.properties

profileCookieEP.class=com.trustgenix.tfsSP.util.SPEventPlugin_ProfileCookie
```

```
myEventPlugin.class=com.hp.selectfederation.coreid.COREidEventPlugin
myEventPlugin.jar=<SF_INSTALL_DIR>/connectors/coreid/COREidConnector.jar
amPlugin=myAdminPlugin
myAdminPlugin.jar=<SF_INSTALL_DIR>/connectors/coreid/COREidConnector.jar
myAdminPlugin.class=com.hp.selectfederation.coreid.COREidAMPlugin
coreidConfigDir=<Access_server_sdk_install>
coreidLoginURL=http://me.vm.net/test/sample-login.jsp
coreidResrcURL=/sf-admin
coreidCookieDomain=.vm.net
coreidSPResrcURL=/spsf
coreidBaseURL=http://sp.vm.net:2001
```

4 Error Messages

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

Error Message Terminology

The following terminology is used in the COREid error messages:

- `COREidAMPlugin` – Module used for Select Federation Administration console and Privacy Manager integration.
- `COREidAuthnPlugin` – Module used for IDP side integration of Select Federation with Oracle COREid.
- `COREidEventPlugin` – Module used for SP side integration of Select Federation with Oracle COREid.
- `COREidUtil` – Utility Module used for COREid integration.
- `XXXException` – Exception message from Exception class.
- `XXX` – Represents parameter substitutions.

Error Messages and Descriptions

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

COREidAMPlugin Error Messages

The following table lists the COREidAMPlugin error messages and explanations:

Table 1 COREidAMPlugin Error Messages

Error Message	Explanation
`Unable to create COREidUtil class`	`Error occurred when creating Utility class coreidUtil.`
`authnAndAuthz returned an exception: XXXException`	Details of exception are included in the `XXXException` message.
`Error cleaning COREid session: XXXException`	Error when deleting COREid session during logout. Details included in the `XXXException` message.

COREidAuthnPlugin Error Messages

The following table lists the COREidAuthnPlugin error messages and explanations:

Table 2 COREidAuthnPlugin Error Messages

Error Message	Explanation
`Unable to create COREidUtil class`	`Error occurred when creating Utility class coreidUtil.`
`Exception when processing authenticateUser request: XXXException`	Details of exception are included in the `XXXException` message.
`Error cleaning COREid session: XXXException`	Error when deleting COREid session during logout. Details included in the `XXXException` message.

COREidEventPlugin Error Messages

The following table lists the COREidEventPlugin error messages and explanations:

Table 3 COREidEventPlugin Error Messages

Error Message	Explanation
`Unable to create COREidUtil class`	`Error occurred when creating Utility class coreidUtil.`
`Error when creating COREid session: XXXException`	Error creating COREid session. Details included in the `XXXException` message.
`Error cleaning COREid session: XXXException`	Error when deleting COREid session during logout/deactivation. Details included in the `XXXException` message.
`User not activated. Please configure an activation event plugin:`	Activation exception in `COREidEventPlugin`. Configure the activation plugin. The user is expected to be activated before control reaches COREid.

COREidUtil Error Messages

The following table lists the COREidUtil error messages and explanations:

Table 4 COREidUtil Error Messages

Error Message	Explanation
`Failed to initialize COREid Access SDK: XXXException`	Failed to initialize COREid libraries. Details included in the `XXXException` message.
`Cannot URL-encode with UTF-8: XXXException`	URL encoding failed. Details included in the `XXXException` message.
`Error redirecting to login url: XXXException`	Error redirecting to Login URL. Details included in the `XXXException` message.
`Failed to create new COREid resource request`	Unable to create COREid resource request.
`Resource XXX : XXX is unprotected`	Resource not protected by COREid.
`COREid returned exception : XXXException`	Exception returned from COREid APIs. Details included in the `XXXException` message.
`Exception returned in isAuthz : XXXException`	Details included in the `XXXException` message.

Error Message	Explanation
`Unable to create COREid User Session`	Unable to create COREid session.
`Could not create COREid Session : XXXException`	Unable to create COREid session. Details included in the `XXXException` message.
`Got error while writing to printWriter: XXXException`	Error showing login page. Details included in the `XXXException` message.

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 due to incorrect syntax or configuration. Following are some common problems:

Error

```
com.trustgenix.tfs.ModuleLoader - com/oblix/access/ObAccessException
java.lang.reflect.InvocationTargetException
com.trustgenix.tfs.ConfigException: com/oblix/access/ObAccessException
```

Problem

Your application server CLASSPATH does not contain Oracle COREid jars needed for the integration.

Solution

Check the Oracle COREid Access Server SDK README to determine which jars 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

```
Failed to create new user session
```

Problem

Your Oracle COREid Access Server or LDAP Server is down.

Solution

Start all components of the Oracle COREid Access Manager and your Select Federation application server.

Error

```
com.oblix.access.ObAccessException: The NetPoint AccessGate is unable to
contact any NetPoint Access Servers
```

Problem

Your Oracle COREid Access Server is down.

Solution

Start your Oracle COREid Access Server.

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 bytecore 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

I

L

O

P

R

S

T

U


invent


Java™
COMPATIBLE