HP Select Identity Software

Connector for Sun ONE Directory Server (Bidirectional LDAP Based)

Connector Version: 1.12

Installation and Configuration Guide

Document Release Date: September 2007
Software Release Date: September 2007

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

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Select Identity uses software from the Apache Jakarta Project including:

- Commons-beanutils
- Commons-collections
- Commons-logging
- Commons-digester
- Commons-httpclient
- Element Construction Set (ecs)
- Jakarta-poi
- Jakarta-regexp
- Logging Services (log4j)

Additional third party software used by Select Identity includes:

- JasperReports developed by SourceForge
- iText (for JasperReports) developed by SourceForge
- BeanShell
- Xalan from the Apache XML Project
- Xerces from the Apache XML Project
- Java API for XML Processing from the Apache XML Project
- SOAP developed by the Apache Software Foundation
- JavaMail from SUN Reference Implementation
- Java Secure Socket Extension (JSSE) from SUN Reference Implementation
- Java Cryptography Extension (JCE) from SUN Reference Implementation
- JavaBeans Activation Framework (JAF) from SUN Reference Implementation

- OpenSPML Toolkit from OpenSPML.org
- JGraph developed by JGraph
- Hibernate from Hibernate.org
- BouncyCastle engine for keystore management, bouncycastle.org

This product includes software developed by Teodor Danciu (http://jasperreports.sourceforge.net). Portions Copyright © 2001-2004 Teodor Danciu (teodord@users.sourceforge.net). All rights reserved.

Portions Copyright © 1994-2004 Sun Microsystems, Inc. All Rights Reserved.

This product includes software developed by the Waveset Technologies, Inc. (www.waveset.com). Portions Copyright © 2003 Waveset Technologies, Inc. 6034 West Courtyard Drive, Suite 210, Austin, Texas 78730. All rights reserved.

Portions Copyright © 2001-2004, Gaudenz Alder. All rights reserved.

Trademark Notices

AMD and the AMD logo are trademarks of Advanced Micro Devices, Inc.

Intel and Pentium are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

JAVA™ is a US trademark of Sun Microsystems, Inc.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California

UNIX® is a registered trademark of The Open Group.

Support

You can visit the HP software support web site at:

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

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

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

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

To find more information about support access levels, go to:

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

Contents

1 Documentation Map

This chapter describes the organization of HP Select Identity connector documentation and provides necessary information on how to use the documentation set to install and configure the connectors.

Figure 1 illustrates the documentation map for Select Identity connector. For a list of available product documentation, refer to the Table 1.

Figure 1 Documentation Map

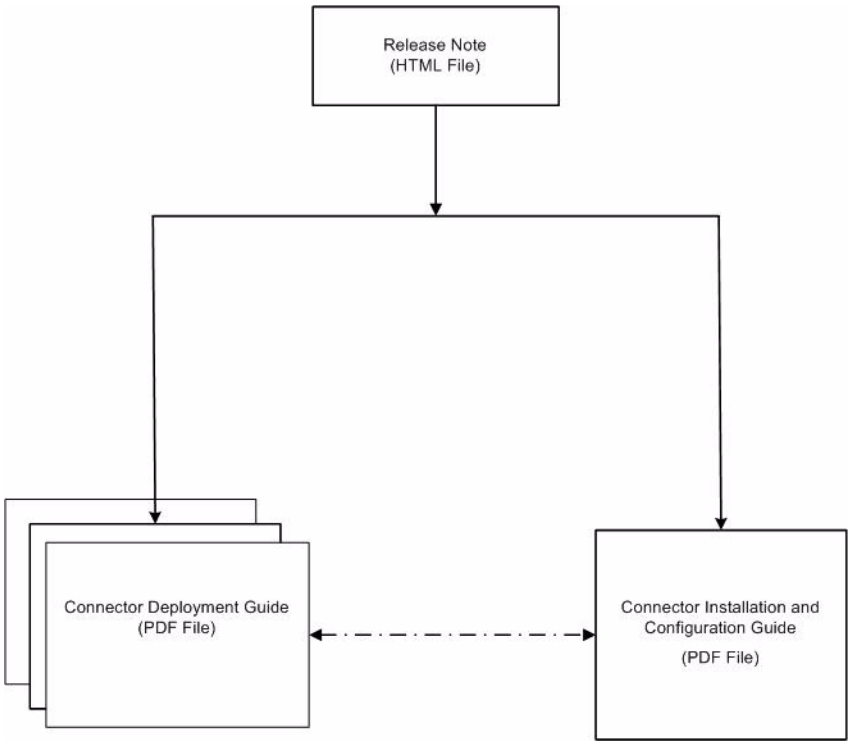


Table 1 Connector Documentation

Document Title and Filename	Contents	Location
Release Note `Sun ONE BiLDAP Connector v1.12 Release Note.htm`	This file contains necessary information on new features of the connector, enhancements, known problems or limitations, and support information.	`/Docs/` subdirectory under the connector directory.
Connector Deployment Guide (for Select Identity 4.20) `connector_deploy_SI4.20.pdf`	Connector deployment guides provide detailed information on: • Deploying a connector on an application server. • Configuring a connector with Select Identity. Refer to these guides when you need generic information on connector installation.	`/Docs/` root directory on the product's CD media.
Connector Deployment Guide (for Select Identity 4.10-4.13) `connector_deploy_SI4.13.pdf`		
Connector Deployment Guide (for Select Identity 4.0-4.01) `connector_deploy_SI4.pdf`		
Connector Installation and Configuration Guide `Sun ONE BiLDAP_guide.pdf`	Connector installation and configuration guide provides installation instructions for a specific connector. It contains resource specific configuration details.	`/Docs/` subdirectory under the connector directory.

2 Introduction

This chapter gives an overview of the HP Select Identity connector for Sun ONE Directory Server. An HP Select Identity connector for Sun ONE Directory Server enables you to provision users and manage identities on Sun ONE Directory Server. At the end of this chapter, you will be able to know about:

- The benefits of HP Select Identity.
- The role of a connector.
- The connector for Sun ONE Directory Server.

About HP Select Identity

HP Select Identity provides a new approach to identity management. Select Identity helps you automate the process of provisioning and managing user accounts and access privileges across platforms, applications, and corporate boundaries. Select Identity communicates with the enterprise information system through connectors, and automates the tasks of identity management. The enterprise information system, which is also referred to as **resource**, can be a database, a directory service, or an ERP package, among many others.

About Connectors

You can establish a connection between a resource and Select Identity by using a connector. A connector is resource specific. The combination of Select Identity and connector helps you perform a set of tasks on the resource to manage identity. A connector can be **unidirectional** or **bidirectional**. A unidirectional connector helps you manage identities from Select Identity, but if any change takes place in resource, it cannot communicate that back to Select Identity. On the other hand, a bidirectional connector can reflect the changes made on resource back to Select Identity. This property of bidirectional connectors is known as **reverse synchronization**.

About Sun ONE Bidirectional LDAP Connector

The bidirectional LDAP based connector for Sun ONE Directory Server — hereafter referred to as Sun ONE Bidirectional LDAP connector — enables Select Identity to perform the following tasks in Sun ONE Directory Server:

- Add, update, and remove users
- Retrieve user attributes

- Enable and disable users
- Verify a user's existence
- Change user passwords
- Reset user passwords
- Validate passwords
- Retrieve all entitlements
- Retrieve a list of supported user attributes
- Grant and revoke entitlements to and from users

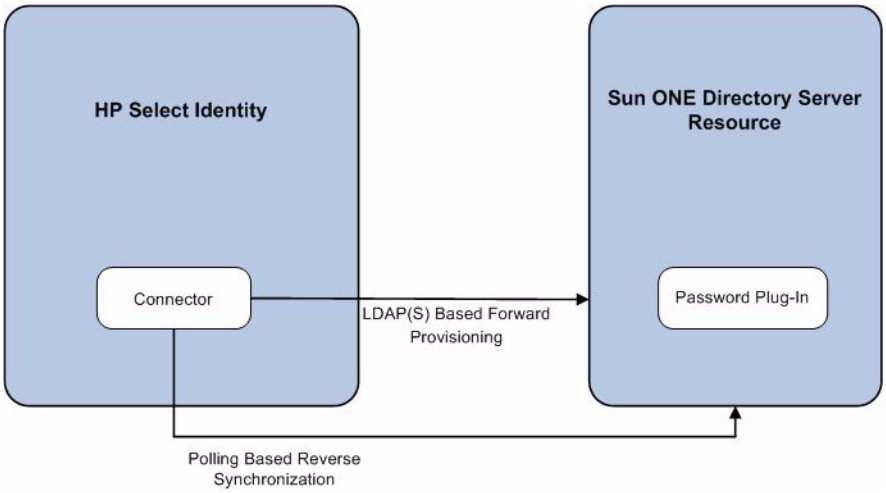
The Sun ONE Bidirectional LDAP connector is internationalized.

High-Level Architecture

Figure 2 illustrates a high-level architecture of Sun ONE Bidirectional LDAP connector. This is a bidirectional, Lightweight Directory Access Protocol Version 3 (LDAPv3) compliant connector that pushes changes made to user data in the Select Identity database to a target Sun ONE Directory Server. The connector uses the Java LDAP Application Program Interfaces (APIs) to provision users and their entitlements in the Sun ONE Directory Server (the LDAP server), which in turn pushes the data to the server.

A reverse synchronization feature reconciles user account changes made on the Sun ONE Directory Server resource with Select Identity. Select Identity periodically polls the Sun ONE Directory Server resource to retrieve changes through the connector.

Figure 2 High-Level Architecture of the Sun ONE Bidirectional LDAP Connector



The connector also has a Password Plug-In for password reconciliation..

This connector can be used with Select Identity 4.0-4.20.

Overview of Installation Tasks

Before you start installing the connector, you must ensure that system requirements and all the installation prerequisites are met. Refer to the Table 2 for an overview of installation tasks.

Table 2 Organization of Tasks

Task Number	Task Name	Reference
1	Install the connector on the Select Identity server.	See Installing the Connector on page 13.
	— Meet the system requirements.	See System Requirements on page 14.
	— Perform the pre-installation task: Install Sun ONE Directory Server certificate on the application server hosting Select Identity.	See Pre-Installation Task on page 14.
	— Install the Password Plug-In	See Installing Password Plug-In on page 18.
	— Configure Sun ONE Directory Server for reverse synchronization.	See Configuring Sun ONE Directory Server for Reverse Synchronization on page 20.
	— Extract contents of the Schema file (file that contains the mapping files for the connector) to a location on the Select Identity server.	See Extracting Contents of the Schema File on page 20.
	— Verify configurable parameters in the `SunONEConfig.poperties` file.	See Verifying Configurable Parameters on page 21.
	— Install the Resource Adapter Archive (RAR) of the connector on an application server.	See Installing the Connector RAR on page 22.
2	Configure the connector with the Select Identity server.	See Configuring the Connector with Select Identity on page 23.

3 Installing the Connector

This chapter elaborates the procedure to install Sun ONE Bidirectional LDAP on Select Identity server and agent on Sun ONE Directory Server. At the end of this chapter, you will know about

- Software requirements to install the Sun ONE Bidirectional LDAP connector.
- Prerequisite conditions to install Sun ONE Bidirectional LDAP connector.
- Procedure to install Sun ONE Bidirectional LDAP connector.

Sun ONE Bidirectional LDAP Connector Files

The Sun ONE Bidirectional LDAP connector is packaged in the following files, which are located in the `Bidirectional LDAP Connector - SunOne Directory` folder on the Select Identity Connector CD:

Table 3 Sun ONE Bidirectional LDAP Connector Files

Serial Number	File Name	Description
1	• `SunONEConnector_420.rar` for WebSphere • `SunONEConnector_420WL9.rar` for WebLogic	It contains the binaries for the connector. It contains binaries, implementation related Java class files, third party JAR files, and Sun ONE property files.
2	`SunONESchema.jar`	It contains the mapping file (`SunONE.xml`), which control how Select Identity fields are mapped to Sun ONE fields. It also contains the `SunONEConfig.properties` configuration files.
3	`postPassFilter.so`	This file is required to install password plug-in utility on a Solaris system.
4	`SunONEPassFilter.dll`	This file is required to install password plug-in utility on a Windows system.
5	`SunONEProperties.ini`	This file is required to install password plug-in utility.
6	`OpenSSLDLL.zip`	It contains the following dll files: • `libeay32.dll` • `libssl32.dll`

System Requirements

The Sun ONE Bidirectional LDAP connector is supported in the following environment:

Table 4 Platform Matrix for Sun ONE Bidirectional LDAP Connector

Select Identity Version	Application Server	Database
4.0-4.20	The Sun ONE Bidirectional LDAP connector is supported on all the platform configurations of Select Identity 4.0-4.20.	

The Sun ONE connector is supported for Sun ONE Directory Server version 5.2 on Windows and Solaris platforms.

The Sun ONE Bidirectional LDAP connector is internationalized and able to operate with languages that are supported by the Java Unicode specification. If you wish to use the connector on non-English platforms, make sure that the following prerequisites are met:

- The Select Identity server should be configured for internationalization. Refer to the *HP Select Identity Installation and Configuration Guide* for more information.
- The resource should be configured to support local language characters.

Pre-Installation Task

Before you start installing the connector, you must install the Sun ONE certificate on the application server on Select Identity system to enable the Secure Socket Layer (SSL) connectivity between the connector and the Sun ONE Directory Server:

- Install Sun ONE Certificate on Application Server
  - Install Sun ONE Certificate on Select Identity 4.0-4.13
  - Install Sun ONE Certificate on Select Identity 4.20

In order to enable the Select Identity to use different keys to connect to a resource, you also need to configure key rotation:

- Rotate Keys

Install Sun ONE Certificate on Application Server

If the connector is required to connect to SunONE through SSL-connection, then certificate configuration on Select Identity side is required.

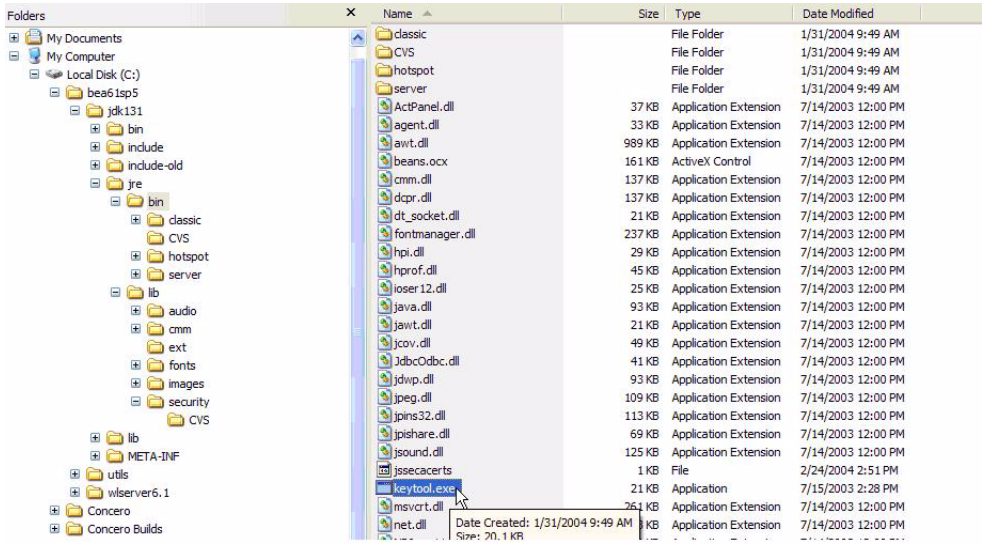
For Select Identity 4.0-4.13, only server certificate verification is supported. Certificate presenting SunONE resource or issuer of SunONE resource should be imported into `jssecacerts` file under `jre/lib/security` directory.

For Select Identity 4.20, Select Identity supports both one-way SSL authentication, in which only the server is authenticated, and two-way (mutual) SSL authentication, in which both the server and the client are authenticated. To connect through one-way SSL connection, the certificate presenting SunONE resource or issuer of SunONE resource should be imported

into Select Identity managed trust store. To connect through two-way SSL connection, in addition to importing the SunONE certificate into the trust store, it is also required to import certificate presenting Select Identity into the keystore managed by Select Identity.

Install Sun ONE Certificate on Select Identity 4.0-4.13

Before installing the Sun ONE Bidirectional LDAP certificate on the application server, verify if `keytool.exe` is available. To verify, go to Java home of application server's home directory, and locate the file `keytool.exe` in `jre\bin` subdirectory. If Select Identity is installed on Windows, in windows explorer, you can locate the file at *<Application Server Java Home>*/`jre/bin`..



Perform the following steps to install the Sun ONE Bidirectional LDAP certificate:

1. Copy the Sun ONE Bidirectional LDAP certificate file (*<certificate name>*`.cer`) to Select Identity system in the location *<Application Server Java Home>*`\jre\lib\security`.

   You must copy the certificate to all the application servers at the location *<Application Server Java Home>*`\jre\lib\security` for cluster setup.

2. From *<Application Server Java Home>*`jre\bin`, by using command prompt, run the command **`keytool -v -keystore jssecacerts -trustcacerts -import -file ..\lib\security\<certificate name>.cer`**.

3. When prompted for password, enter keystore password (the default password is **`changeit`**).

4. The keytool displays the following message:

```
Owner: CN=QA.hp.com, OU=QA, O="hp", L=abc, ST=efg, C=ab,
EmailAddress=qa@hp.com
Issuer: CN=QA.hp.com, OU=QA, O="hp", L=abc, ST=efg, C=ab,
EmailAddress=qa@hp.com
Serial number: 16bab38264ebda84f8011cf35d0ca6a
Valid from: Fri Jan 23 13:42:18 CST 2004 until: Fri Jan 23 13:50:22 CST
2009
Certificate fingerprints:
MD5:  60:72:A9:DD:C4:39:C4:8A:E7:42:56:0B:9E:5D:91:DB
SHA1: 38:D2:7F:33:FE:0A:AC:F3:D3:A0:2C:0F:A9:0C:6A:09:10:B5:EA:66
```

5 If the system displays `Trust this certificate? [no]:`, enter **yes**. The keytool displays the following message:

```
Certificate was added to keystore
[Saving jssecacerts]
```

6 Now copy the new `jssecacerts` file to the <*Application Server Java Home*>`\jre\lib\security` folder.

> You must copy the certificate (the `jssecacerts` file) to all the application servers at the location <*Application Server Java Home*>`\jre\lib\security` for cluster setup.

7 Restart the application server.

You can add additional certificates by using `alias` flag. For example, after performing the above mentioned steps, if you run **`keytool -v -keystore jssecacerts -trustcacerts -import -file ..\lib\security\cert-AD69.cer`**, you will get the message `keytool error: java.lang.Exception: Certificate not imported, alias <mykey> already exists.`

A listing of the `jssecacerts` shows the `mykey` alias as the default for the just-entered certificate:

```
mykey, Dec 22, 2004, trustedCertEntry,
Certificate fingerprint (MD5):B2:F6:42:F6:0C:88:65:EE:FB:38:3E:31:00:CA:DD:70
```

To add the additional certificate `cert-AD69.cer`, run the following command:

`keytool -v -keystore jssecacerts -trustcacerts -alias hp69trustca -import -file ..\lib\security\cert-AD69.cer`

The list of jssecacerts now includes:

```
hp69trustca, Dec 22, 2004, trustedCertEntry,
Certificate fingerprint (MD5):60:72:A9:DD:C4:39:C4:8A:E7:42:56:0B:9E:5D:91:DB
```

Install Sun ONE Certificate on Select Identity 4.20

Perform the following steps to install the Sun ONE Bidirectional LDAP certificate:

1 Create and configure Select Identity trust store and properties, if not already created.

a Create the trust store;

b Generate a properties file that is corresponding to the trust store file.

Refer to *Creating the Trust Store* section of *HP Select Identity Installation Guide* for detailed instructions on creating keystore, trust store, and properties.

2 Import certificate representing Sun ONE resource or issuer of Sun ONE resource to Select Identity trust store:

a Get Sun ONE certificate;

b Import the certificate into the trust store file you created in the previous step.

Refer to *Creating the Trust Store* section of *HP Select Identity Installation Guide* for detailed instructions on creating keystore, trust store, and properties.

3 If a resource requires a specific client certificate, you must either generate the client certificate or import the client certificate into the key store:

a Create the key store file;

b Generate the certificate that represents Select Identity server if no certificate available. Or, import the certificate that represents Select Identity server if a certificate already exists.

c Generate the properties file that is corresponding to the keystore.

For more information, refer to *Creating the Key Store and Key Pairs for Mutual Authentication and/or Secure Object Migration* section of *HP Select Identity Installation Guide*.

4 Register the key store and trust store and select the Select Identity client certificate, if not already done.

a Open the security setup tool in Select Identity;

b Register the keystore properties to Select Identity;

c Register the trust store properties to Select Identity;

d Select certificate represent Select Identity server if needed.

For detailed instructions, refer to *Configure System Security* topic in *HP Select Identity Administration Online Help*.

Rotate Keys

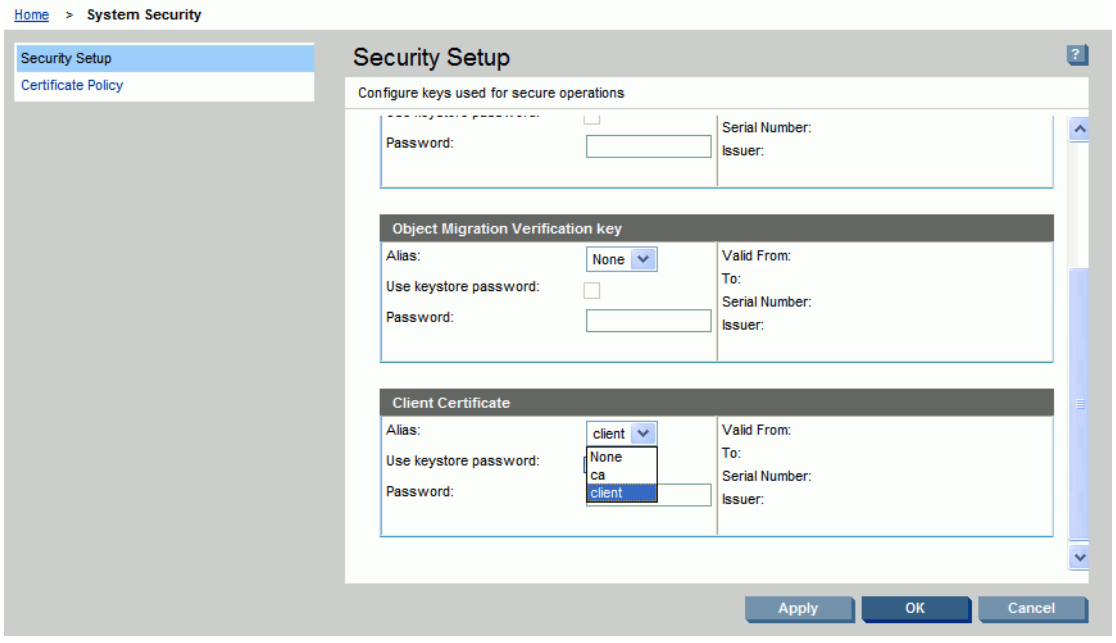
Key rotation is a process that Select Identity can use different keys to connect to a resource. The process is:

1 Generate new key pair in keystore.

For detailed instructions, refer to *Creating the Mutual Authentication Key store* section of *HP Select Identity Installation Guide*.

2 Change key alias in system security setup:

a From the Tools menu, select **System Security** → **Security Setup**. The Security Setup page displays.



b Under Client Certificate section, select the newly generated certificate.

Installing Password Plug-In

The password plug-in captures the password changes on the Sun ONE Directory Server and stores on Sun ONE Directory Server in an encrypted form. If the password plug-in is not installed, password changes cannot be reconciled to Select Identity. Perform the following steps (on Solaris or Windows platform) to install password plug-in.

Solaris

Before you start installing the Password Plug-In on Solaris platform, make sure that the following pre-requisites are met:

- OpenSSL (version 0.9.8a) must be installed on the system. You can download OpenSSL (version 0.9.8a) from **http://www.openssl.org**.
- GNU Compiler Collection (GCC) must be installed on the system. You can download GCC from **http://www.sunfreeware.com**.

Perform the following steps to install the Password Plug-In on Solaris platform:

1. Copy the file `postPassFilter.so` to a local subdirectory.
2. Copy the `SunONEProperties.ini` file to the following subdirectory:

   <SunOnebase directory home>`/ds5/bin/slapd/server`.

   Alternatively, create an environment variable named `SunOnePropertyPath` and provide the path where `SunONEProperties.ini` file is placed on mahine.
3. To configure the plug-in, add the following entry in `cn=plugins, cn=config` by using LDP.

```
Dn: cn=SUNONE FILTER,cn=plugins,cn=config
cn: SUNONE FILTER;
 objectClass: top; nsSlapdPlugin; extensibleObject;
 nsslapd-pluginPath:path where postPassFilter.so/postPassFilter.dll is
located on your machine ; for example <SunOnebase directory home>/mps/lib/
postPassFilter.so
nsslapd-pluginInitfunc: postop_init;
nsslapd-pluginType: postoperation;
nsslapd-pluginEnabled: on;
nsslapd-plugin-depends-on-type: database;
nsslapd-pluginId: SunOne-PwdFilter;
nsslapd-pluginVersion: 0.5;
nsslapd-pluginVendor: iPlanet;
nsslapd-pluginDescription: SunOne password filter post-operation plugin;
```

   Alternatively, Stop the directory server, edit the `dse.ldif` file (in the `<server_root>/slapd-<server_id>/config` directory) and add the following lines before restarting the server.

```
dn: cn=SUNONE FILTER,cn=plugins,cn=config
objectClass: top
objectClass: nsSlapdPlugin
objectClass: extensibleObject
cn: Test PostOp
nsslapd-pluginPath:path where postPassFilter.so/postPassFilter.dll is
located on your machine ;
nsslapd-pluginInitfunc: postop_init
```

```
nsslapd-pluginType: postoperation
nsslapd-pluginEnabled: on
nsslapd-plugin-depends-on-type: database
nsslapd-pluginId: SunOne-PwdFilter
```

4 Restart the server.

Windows

1 Extract contents of the `OpenSSLDLL.zip` file and copy the extracted contents to the location `<system root>\system 32` on resource machine. The contents of this file are:

- `libeay32.dll`
- `libssl32.dll`

2 Copy following files to the folder <*SystemRoot*>`\system32` (For example, `C:\WINNT\system32`)

a `SunONEPassFilter.dll`

b `SunONEProperties.ini`

3 To configure the plug-in, add the following entry in `cn=plugins, cn=config` by using LDP.

```
dn: cn=SUNONE FILTER,cn=plugins,cn=config
cn: SUNONE FILTER;
objectClass: top; nsSlapdPlugin; extensibleObject;
nsslapd-pluginPath:<SystemRoot>\system32\SunONEPassFilter.dll;
nsslapd-pluginInitfunc: postop_init;
nsslapd-pluginType: postoperation;
nsslapd-pluginEnabled: on;
nsslapd-plugin-depends-on-type: database;
nsslapd-pluginId: SunOne-PwdFilter;
nsslapd-pluginVersion: 0.5;
nsslapd-pluginVendor: iPlanet;
nsslapd-pluginDescription: SunOne password filter post-operation plugin;
```

Alternatively, Stop the directory server, edit the `dse.ldif` file (in the `<server_root>/slapd-<server_id>/config` directory) and add the following lines before restarting the server.

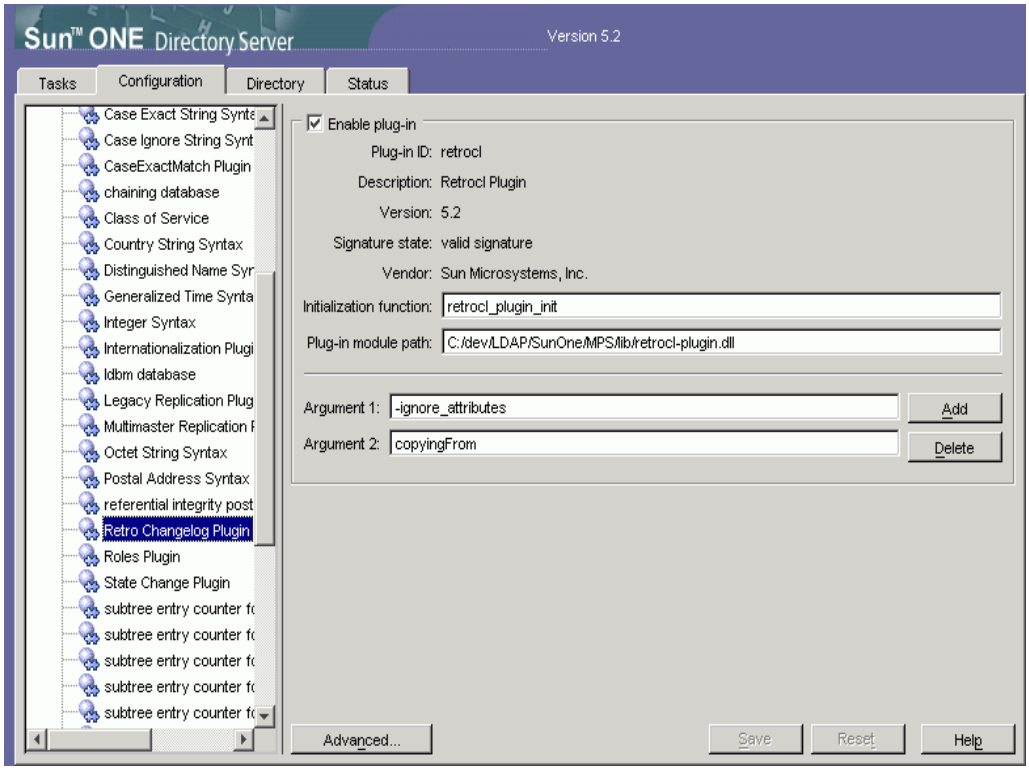
```
dn: cn=SUNONE FILTER,cn=plugins,cn=config
objectClass: top
objectClass: nsSlapdPlugin
objectClass: extensibleObject
cn: Test PostOp
nsslapd-pluginPath: <SystemRoot>\system32\SunONEPassFilter.dll;
nsslapd-pluginInitfunc: postop_init
nsslapd-pluginType: postoperation
nsslapd-pluginEnabled: on
nsslapd-plugin-depends-on-type: database
nsslapd-pluginId: SunOne-PwdFilter
```

4 Restart the server.

Configuring Sun ONE Directory Server for Reverse Synchronization

To enable reverse synchronization of the Sun ONE Bidirectional LDAP connector, you must perform the following steps:

1. Log on to the Sun ONE Directory Server with the administrative username.
2. Open the directory server and navigate to the Configurations tab.
3. Expand the Plugins folder.
4. Choose the Retro Changelog Plugin.
5. Select the Enable plug-in check box.



6. To activate the changelog, stop and restart the directory server.

Extracting Contents of the Schema File

The Schema file of the connector contains necessary mapping information to map resource attributes to Select Identity. Extract contents of the `SunONESchema.jar` file to a directory that is in the application server `CLASSPATH`. Refer to the *HP Select Identity Connector Deployment Guide* for detailed instruction to extract contents of the Schema file.

Verifying Configurable Parameters

The `SunONEConfig.properties` file, which is present in the `SunONESchema.jar` file, contains the following configurable parameters. These parameters can be changed manually. Before installing the connector, verify the parameter values and change the values if they don't match with the values mentioned below.

- `entitlement-delimiter=|`

  It contains the string delimiter that is displayed between an entitlement type and its name.

- `modify_replace=false`

  It is a configuration parameter that can be set to true or false. When it is set to false, Sun ONE Bidirectional LDAP Connector uses modify/add and modify/delete operations to support multivalued attribute. When it is set to true, Sun ONE Bidirectional LDAP Connector uses modify/replace operation to support multivalued attribute.

- `attributeValue-delimiter=|`

  It contains the string delimiter that is used to separate attribute values for multi valued attribute.

- `attribute-begins=[[`

  Begin parameter to wrap the special base64 encoded attribute values while sending to connector from Select Identity.

- `attribute-ends=]]`

  End parameter to wrap the special base64 encoded attribute values while sending to connector from Select Identity.

- `dualLink-support.`*<entity>* `= 0` where *<entity>* can be group, role, and so on.

  If the value is set to 0, bidirectional linking operation is performed (the user as well as the entity will contain the `Link` attribute).

  If the value is set to 1, only user-side linking operation is performed.

  If the value is set to 2, only entity-side linking operation is performed.

- `dualLink-support=0`

  This specifies whether a Link is a User Link or a Group Link. If it is 0, then it is User Link as well as Group Link.

- `multivalue-support=false`

  This specifies whether Select Identity supports multivalued attributes or not. This property is used in the reverse provisioning, when a mutlivalued attribute is detected in the replog during the polling, all the values of this multivalued attribute are combined as single valued string.

  If true - Select Identity supports multivalued attributes.
  If false - Select Identity does not support multivalued attributes.

- `unlink-before-terminate=false`

  If you want to unlink the entitlements while performing a terminate user operation, set this flag to false.

- `PSSync_ATTRIBUTE=description`

It must hold the name of Sun ONE Bidirectional LDAP attribute, where encrypted password is stored.

- `mergeChangeLog=true`.

  If multiple modifications are done at the resource on a user, all the modifications will be sent as a single reconciliation request when this parameter is set as `true`.

Installing the Connector RAR

To install the RAR file of the connector (such as `SunONEConnector_420.rar`) on the Select Identity server, you must copy the file to a local subdirectory on the Select Identity server, and then deploy on the application server. Refer to the *HP Select Identity Connector Deployment Guide* for detailed information on deploying a RAR file on an application server.

While deploying the RAR on WebSphere, enter the JNDI Pool Name as **`eis/SunONEConnector`**.

4 Configuring the Connector with Select Identity

This chapter describes the procedure to configure the Sun ONE Bidirectional LDAP connector with Select Identity and the connector specific parameters that you must provide while configuring the connector with Select Identity.

Configuration Procedure

After you deploy the connector RAR on application server, you must configure the connector with Select Identity. Perform the following steps to configure the Sun ONE Bidirectional LDAP connector with Select Identity.

1 Add a New Connector

2 Add a New Resource

3 Map Attributes

Add a New Connector

Add a new connector in Select Identity by using the user interface. While adding the connector, do the following:

- In the Connector Name text box, specify a name for the connector.
- In the Pool Name text box, enter **`eis/SunONEConnector`**.
- Select **`No`** for the Mapper Available section.

Refer to the *HP Select Identity Connector Deployment Guide* for detailed information on adding a new connector in Select Identity.

Add a New Resource

Add a new resource in Select Identity that uses the newly added connector. Refer to the *HP Select Identity Connector Deployment Guide* for detailed instruction on adding a resource in Select Identity.

Refer to the following table while entering the parameters in the Basic Information and the Access Information pages:

Table 5 Resource Configuration Parameters

Field Name	Sample Values	Description
Resource Name	ELDAPSUNONE	Name given to the resource.
Connector Name	Sun ONE	The newly deployed connector
Authoritative Source	Yes	Whether this resource is a system that is considered to be the authoritative source for user data in your environment. Specify Yes if the resource has to be authoritative.
Delete User	No	Specifies whether the user should be deleted from the resource when a DeleteServiceMembership operation is performed for the user in Select Identity.
Access URL	ldap://sidc:369 or ldaps://sidc:636	Resource connection URL - *protocaol:/ / hostname(or IP):port* Before using ldaps , the trusted root certificate has to be downloaded for Sun ONE machine and imported to the weblogic keystore.
Suffix	DC=hp,DC=com	Default root suffix.
Login Name	cn=Directory Manager	Admin User Login Name. To block cyclic request, you must use an exclusive login name with administrative privilege and you must not use this login name for any other operation on Sun ONE Directory Server.
Password	SUNONEPASSWORD	Password of the admin user.
Default User Suffix	ou=people	Suffix where all users exist.
Default Group Suffix	ou=Groups	Suffix where all groups exist.
Mapping File	SunONE.xml	Name of the file that specifies the attribute mappings. This file should exist in the classpath of the application server. Click **View** to open the file in a browser. If this file cannot be viewed, Select Identity could not locate it.

Table 5 Resource Configuration Parameters (cont'd)

Field Name	Sample Values	Description
Select Identity Locale	en_US	Locale-specific information. If Country = US and Language = English, current locale string is en_US.
CRL Flag	false	Indicates if the resource performs CRL check. This flag works with CRL check flag in **Tools** → **System Security** → **Security Setup** → **Certificate Policy** page. If these two flags are both true, the connector will perform CRL check.
Usage Flag	false	Indicates if the connector performs usage check. This flag works with usage check flag in **Tools** → **System Security** → **Security Setup** → **Certificate Policy** page. If these two flags are both true, the connector will perform Usage check.

Configuring Polling for Reverse Synchronization:

After entering the resource access information, User Reconciliation Policy page appears. On this page, do the following.

a. Check the Polling Enable checkbox. Set the polling interval to the desired value.

b. Under the Modify sections, set Reconciliation Workflow as Select Identity Recon User Enable Disable Workflow by using the drop-down box.

Keep all other default settings in this page.

Map Attributes

After successfully adding a resource for the Sun ONE Bidirectional LDAP connector, you must map the resource attributes to Select Identity attributes. Refer to the *HP Select Identity Connector Deployment Guide* for information on mapping and creating attributes. While mapping attributes, refer to the following table for resource specific mapping information.

Table 6 Sun ONE Bidirectional LDAP Mapping Information

Select Identity Resource Attribute	Connector Attribute	Attribute on Sun ONE Bidirectional LDAP	Description
postalAddress	postalAddress	postalAddress	
Email	Mail	mail	
UserName	uid	uid	*This attribute is mandatory for user creation.*
Zip	postalCode	postalCode	
PhBus	telephoneNumber	telephoneNumber	

Table 6 Sun ONE Bidirectional LDAP Mapping Information (cont'd)

Select Identity Resource Attribute	Connector Attribute	Attribute on Sun ONE Bidirectional LDAP	Description
Password	userPassword	userPassword	*This attribute is mandatory for user creation.*
Title	title	title	
LastName	sn	sn	*This attribute is mandatory for user creation.*
FirstName	givenName	givenName	*This attribute is mandatory for user creation.*
State	st	st	
Usersuffix	userSuffix	userSuffix	
City	l	l	
POBox	postOfficeBox	postOfficeBox	
nsAccountLock	nsAccountLock	nsAccountLock	While associating Sun ONE Directory Server resource to a service, do not add this attribute to the service.
roomNumber	roomNumber	roomNumber	
employeeNumber	employeeNumber	employeeNumber	

Configure Workflow External Call on Select Identity

To achieve reverse synchronization, you must configure the workflow external call for user enable/ disable operation for Sun ONE Bidirectional LDAP connector. Refer to *HP Select Identity Deployment Guide* for information on configuring user enable/disable workflow external call. While configuring, enter the parameters as given in Table 7 below.

Table 7 User Enable/Disable Parameters for Sun ONE Bidirectional LDAP Connector

Serial Number	Parameter Name	Parameter Value
1	AttributeName	nsAccountLock
2	EnableValue	false
3	DisableValue	true

Table 7 User Enable/Disable Parameters for Sun ONE Bidirectional LDAP Connector (cont'd)

Serial Number	Parameter Name	Parameter Value
4	UserName	Select Identity admin user name. For example, sisa.
5	Password	Select Identity admin password. For example, abc123.
6	Url	Select Identity web service url. For example: http://localhost:7001/lmz/webservice

While entering these parameters, check the Sensitive checkbox only in the case of Password.

After configuring the connector with Select Identity, you can use the connector to create a service, or you can associate the connector with an existing service. Refer to the *Service Studio* chapter of the *HP Select Identity Administration Online Help* for information on Select Identity services.

5 Uninstalling the Connector

If you want to uninstall the connector, perform the following steps:

- Remove all resource dependencies.
- Delete the connector from the Select Identity.
- Delete the connector from application server.

See *HP Select Identity Deployment Guide* for more information on deleting the connector from application server and Select Identity.

A Overview of Reverse Synchronization by Polling

Overview of Reverse Synchronization by Polling

Reverse synchronization in Sun ONE Bidirectional LDAP connector is achieved by polling. Each time the polling is invoked, the following sequences take place in the background:

1. The polling batch task is invoked
2. The polling batch task converts all the ChangeLogs into an SPML file, and the SPML file is converted to a request using the SPML parser and submitted to the Select Identity Reconciliation engine. Then ReconcilationHelper is called to execute all the Modify Requests.
3. In the provisioning stage of request execution, Select Identity is updated with the changes in the resource.

On Select Identity, if Sun ONE Bidirectional LDAP service view has some attributes as mandatory, all of them should exist on Sun ONE Bidirectional LDAP server and they should be sent when reverse add request comes from connector. That is, the only attributes that are coming in reverse add request can be mandatory in Select Identity Service view, if it is mandatory in view and it does not come in reverse add request, request will be rejected by Select Identity.

About Cyclic Request

The Sun ONE Bidirectional LDAP connector supports both forward provisioning and change detection. When a forward operation is performed on the resource, the next polling cycle of the connector may detect the operation as if it was performed directly on the Sun ONE Directory Server. This is called cyclic request. To block any cyclic request, during resource creation on Select Identity, you must use an exclusive administrative username/ login name of Sun ONE Directory Server and you must not use that username/ login name for any other operation on Sun ONE Directory Server.

B Troubleshooting

- While creating and trying to save a resource, you get error `The following resource failed to save: Reason: Unable to test connector.`

  Solution:

  Verify the following properties file are in the application server classpath while deploying the connector.

  `com\hp\ovsi\connector\bidirldap\sunone\SunONEConfig.properties`

- While creating and trying to save a resource, you get an error saying

  `The following resource failed to save: SunONE-2way. Reason: Copy failed.`

  Solution:

  Verify that the certificate to enable ldaps is installed in the application server.

- While creating and trying to save a resource, you get an error saying

  `Unable to find valid certification path to requested target.`

  Solution:

  Verify if the certificate of Sun ONE resource or issuer of Sun ONE resource has been imported into the truststore of Select Identity.

- While creating and trying to save a resource, you get an error saying

  `No trusted certificate found`

  Solution:

  Check the truststore managed by Select Identity, it seems that there is no trust key entry in the truststrore.

- While creating and trying to save a resource, you get an error saying

  `Bad certificate`

  Solution:

  Check the keystore managed by Select Identity to see if the certificate representing Select Identity is correct and trusted by the server.

- While creating and trying to save a resource, you get an error saying `error.securityfw.provider.cert.cn.not.found{16.157.133.80}`

  Cause:

  The cn field of server certificate is not equal to ldap URL in access information. For example, cn of certificate is machine name but using IP address in access information.

- While creating and trying to save a resource, you get an error saying

  `Cannot access key :null, maybe the password is incorrect or there is no private key.`

  Cause:

The keystore managed by Select Identity is corrupt, or no key in it, or the password is incorrect.

- While creating and trying to save a resource, you get an error saying `error.securityfw.provider.certificate.revoked{CN=sicf-dev-2.asiapacific.hpqcorp.net, OU=TISU, O=CarlTao.HP.com, ST=Shanghai, C=CN}`

  Cause:

  The certificate from Sun ONE server can not pass CRL (certificate revoke list) check.