HP Select Identity Software

Connector for Oracle® Internet Directory Server (Bidirectional LDAP Based)

Connector Version: 1.02

Installation and Configuration Guide

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

Legal Notices

Warranty

Restricted Rights Legend

Copyright Notices

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

Trademark Notices

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 7

2 Introduction 9

About HP Select Identity 9

About Connectors 9

About Oracle Internet Directory Bidirectional LDAP Connector 9

Overview of Installation Tasks 11

3 Installing the Connector 13

Oracle Internet Directory Bidirectional LDAP Connector Files 13

System Requirements 13

Pre-Installation Task 14

Install Oracle Internet Directory Certificate on Application Server 14

WebLogic 14

WebSphere 6.1 16

Extracting Contents of the Schema File 20

Verifying Configurable Parameters 20

Installing the Connector RAR 21

4 Configuring the Connector with Select Identity 23

Configuration Procedure 23

Add a New Connector 23

Add a New Resource 23

Map Attributes 25

Configure Workflow External Call on Select Identity 26

5 Uninstalling the Connector 27

A Overview of Reverse Synchronization by Polling 29

Overview of Reverse Synchronization by Polling 29

About Cyclic Request 29

B Troubleshooting 31

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 HP Select Identity connector. For a list of available product documentation, refer to the Table 1.

Figure 1 Documentation Map

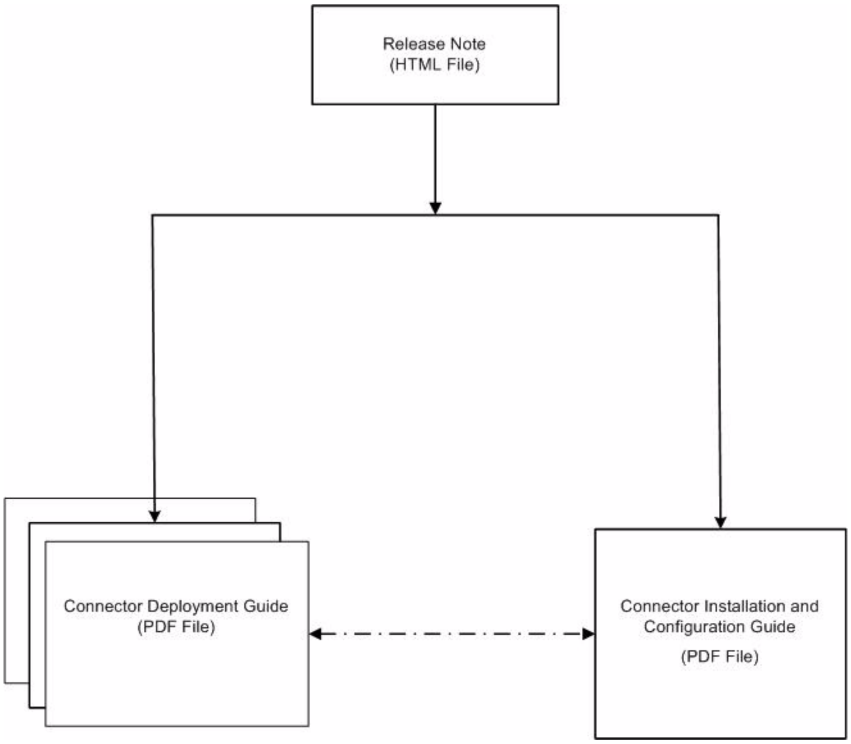

Release Note
(HTML File)
Connector Deployment Guide
(PDF File)
Connector Installation and Configuration Guide
(PDF File)

Table 1 Connector Documentation

Document Title and Filename	Contents	Location
Release Note `Oracle Internet Directory BiLDAP Connector v1.02 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 `Oracle Internet Directory 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 Oracle Internet Directory. An HP Select Identity connector for Oracle Internet Directory enables you to provision users and manage identities on Oracle Internet 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 Oracle Internet Directory.

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 Oracle Internet Directory Bidirectional LDAP Connector

The bidirectional LDAP based connector for Oracle Internet Directory server — hereafter referred to as Oracle Internet Directory Bidirectional LDAP connector — enables Select Identity to perform the following tasks in Oracle Internet Directory:

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

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

This is a Lightweight Directory Access Protocol Version 3 (LDAPv3) compliant connector that pushes changes made to user data in the Select Identity database to a target Oracle Internet Directory. The connector uses the Java LDAP Application Program Interfaces (APIs) to provision users and their entitlements in the LDAP server, which in turn pushes the data to the Oracle Internet Directory.

The reverse synchronization feature reconciles user account changes made on the Oracle Internet Directory resource with Select Identity. Select Identity periodically polls the Oracle Internet Directory resource to retrieve changes through the connector.

This connector can be used with Select Identity 4.01-4.20.

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 13.
	— Perform the pre-installation task: Install Oracle Internet Directory server certificate on the application server hosting Select Identity.	See Pre-Installation Task on page 14.
	— 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 `OIDConfig.properties` file.	See Verifying Configurable Parameters on page 20.
	— Install the Resource Adapter Archive (RAR) of the connector on an application server.	See Installing the Connector RAR on page 21.
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 Oracle Internet Directory Bidirectional LDAP connector on Select Identity server. At the end of this chapter, you will know about

- Software requirements to install the Oracle Internet Directory Bidirectional LDAP connector.
- Procedure to install Oracle Internet Directory Bidirectional LDAP connector.

Oracle Internet Directory Bidirectional LDAP Connector Files

The Oracle Internet Directory Bidirectional LDAP connector is packaged in the following files, which are located in the `Bidirectional LDAP Connector - Oracle Internet Directory` directory of the Select Identity Connector CD:

Table 3 Oracle Internet Directory Bidirectional LDAP Connector Files

Serial Number	File Name	Description
1	• `OIDConnector_420.rar` for WebSphere • `OIDConnector_420WL9.rar` for WebLogic	It contains the binaries for the connector.
2	`OIDSchema.jar`	It contains the mapping file (`OID.xml`), which control how Select Identity fields are mapped to Oracle Internet Directory server fields. It also contains the `OIDConfig.properties` configuration files.

System Requirements

The Oracle Internet Directory Bidirectional LDAP connector is supported in the following environment:

Table 4 Platform Matrix for Oracle Internet Directory Bidirectional LDAP Connector

Select Identity Version	Application Server	Database
4.01-4.20	The Oracle Internet Directory Bidirectional LDAP connector is supported on all the platform configurations of Select Identity 4.01-4.20.	

The Oracle Internet Directory Bidirectional LDAP connector is supported with Oracle Internet Directory 9.0.2 on Windows 2000.

The Oracle Internet Directory 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

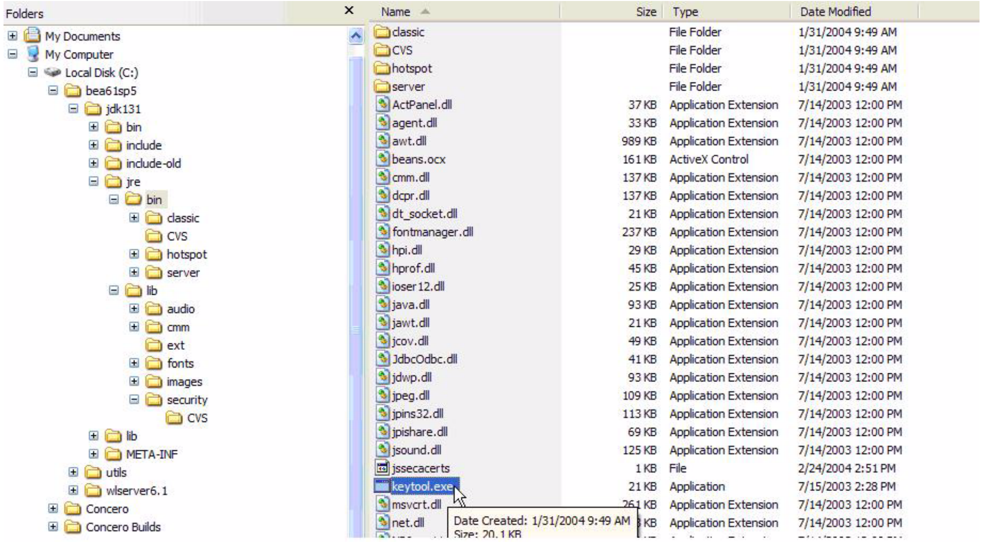
Before you start installing the connector, you must install the Oracle Internet Directory certificate on the application server on Select Identity system to enable the Secure Socket Layer (SSL) connectivity between the connector and the Oracle Internet Directory:

- Install Oracle Internet Directory Certificate on Application Server
  - WebLogic
  - WebSphere 6.1

Install Oracle Internet Directory Certificate on Application Server

WebLogic

Before installing the Oracle Internet Directory certificate on 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`.



Name	Size	Type	Date Modified
classic		File Folder	1/31/2004 9:49 AM
CVS		File Folder	1/31/2004 9:49 AM
hotspot		File Folder	1/31/2004 9:49 AM
server		File Folder	1/31/2004 9:49 AM
ActPanel.dll	37 KB	Application Extension	7/14/2003 12:00 PM
agent.dll	33 KB	Application Extension	7/14/2003 12:00 PM
awt.dll	989 KB	Application Extension	7/14/2003 12:00 PM
beans.ocx	161 KB	ActiveX Control	7/14/2003 12:00 PM
cmm.dll	137 KB	Application Extension	7/14/2003 12:00 PM
dcpr.dll	137 KB	Application Extension	7/14/2003 12:00 PM
dt_socket.dll	21 KB	Application Extension	7/14/2003 12:00 PM
fontmanager.dll	237 KB	Application Extension	7/14/2003 12:00 PM
hpi.dll	29 KB	Application Extension	7/14/2003 12:00 PM
hprof.dll	45 KB	Application Extension	7/14/2003 12:00 PM
ioser12.dll	25 KB	Application Extension	7/14/2003 12:00 PM
java.dll	93 KB	Application Extension	7/14/2003 12:00 PM
jawt.dll	21 KB	Application Extension	7/14/2003 12:00 PM
jcov.dll	49 KB	Application Extension	7/14/2003 12:00 PM
JdbcOdbc.dll	41 KB	Application Extension	7/14/2003 12:00 PM
jdwp.dll	93 KB	Application Extension	7/14/2003 12:00 PM
jpeg.dll	109 KB	Application Extension	7/14/2003 12:00 PM
jpins32.dll	113 KB	Application Extension	7/14/2003 12:00 PM
jpishare.dll	69 KB	Application Extension	7/14/2003 12:00 PM
jsound.dll	125 KB	Application Extension	7/14/2003 12:00 PM
jssecacerts	1 KB	File	2/24/2004 2:51 PM
keytool.exe	21 KB	Application	7/15/2003 2:28 PM
msvcrt.dll	261 KB	Application Extension	7/14/2003 12:00 PM
net.dll	[illegible] KB	Application Extension	7/14/2003 12:00 PM

Date Created: 1/31/2004 9:49 AM
Size: 20.1 KB

Perform the following steps to install the Oracle Internet Directory certificate.

1. Copy the Oracle Internet Directory 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 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
```

WebSphere 6.1

Perform the following steps to create keystore file and configure WebShpere 6.1 to use the newly created keystore:

Create Keystore File

1 Copy the LDAP certificate file (`<certificate name>.cer`) to Select Identity system under `<certificate path>`.

2 Run the command **`keytool -v -keystore <keystore name>  -import -file <certificate path>/<certificate name>.cer`**.

3 When prompted for password, enter your keystore password.

4 The keytool displays a message similar to the following:

```
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:

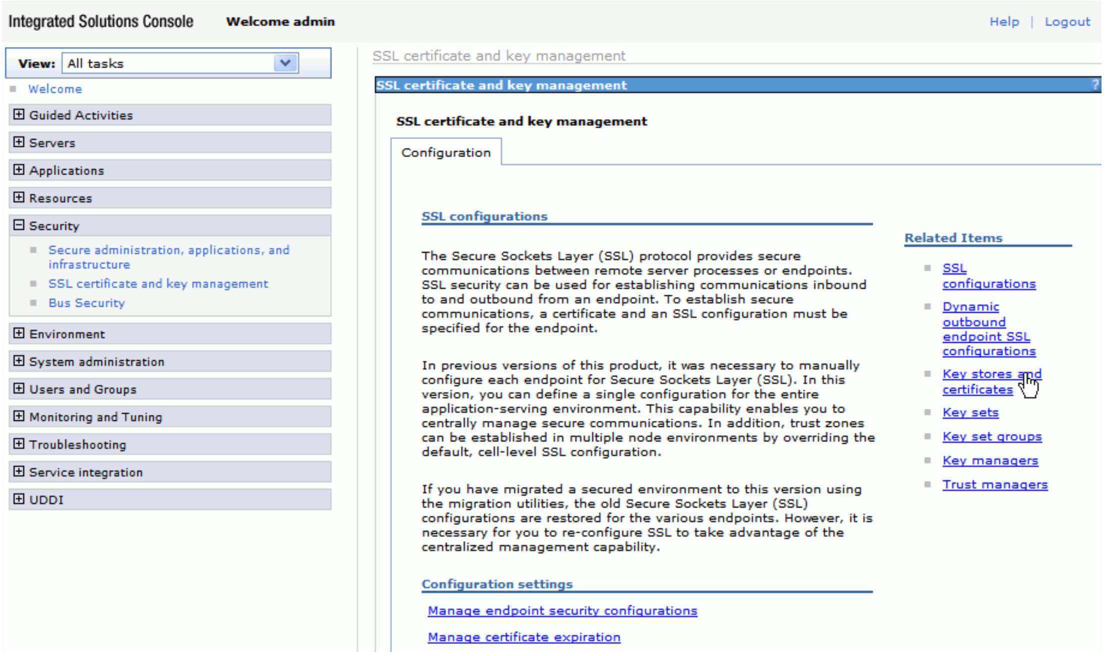
```
Certificate was added to keystore
```

Configure WebSphere 6.1 to Use the Newly Created Keystore

1 Sign on into WebSphere application server console.

2 In the navigation pane, click **Security** → **SSL certificate and key management**. The SSl certificate and key management page displays.

3 Under **Related Items** section, click **Key Stores and certificates**. The Key stores and certificates page displays, this is where you can define logical key store that points to the key store file you previously created.



SSL certificate and key management

SSL configurations

The Secure Sockets Layer (SSL) protocol provides secure communications between remote server processes or endpoints. SSL security can be used for establishing communications inbound to and outbound from an endpoint. To establish secure communications, a certificate and an SSL configuration must be specified for the endpoint.

In previous versions of this product, it was necessary to manually configure each endpoint for Secure Sockets Layer (SSL). In this version, you can define a single configuration for the entire application-serving environment. This capability enables you to centrally manage secure communications. In addition, trust zones can be established in multiple node environments by overriding the default, cell-level SSL configuration.

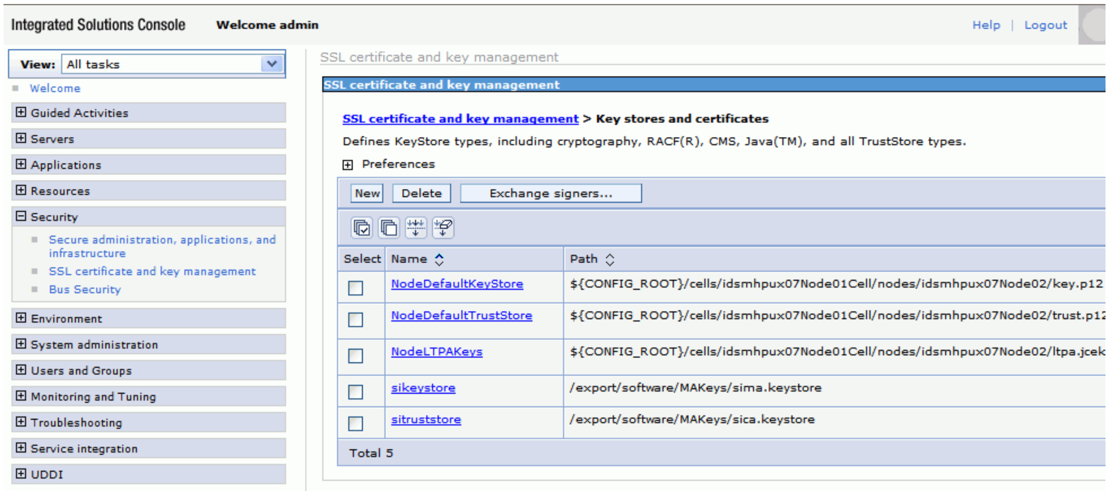
If you have migrated a secured environment to this version using the migration utilities, the old Secure Sockets Layer (SSL) configurations are restored for the various endpoints. However, it is necessary for you to re-configure SSL to take advantage of the centralized management capability.

Configuration settings

Manage endpoint security configurations

Manage certificate expiration

4 To create logical trust stores, click **New**.



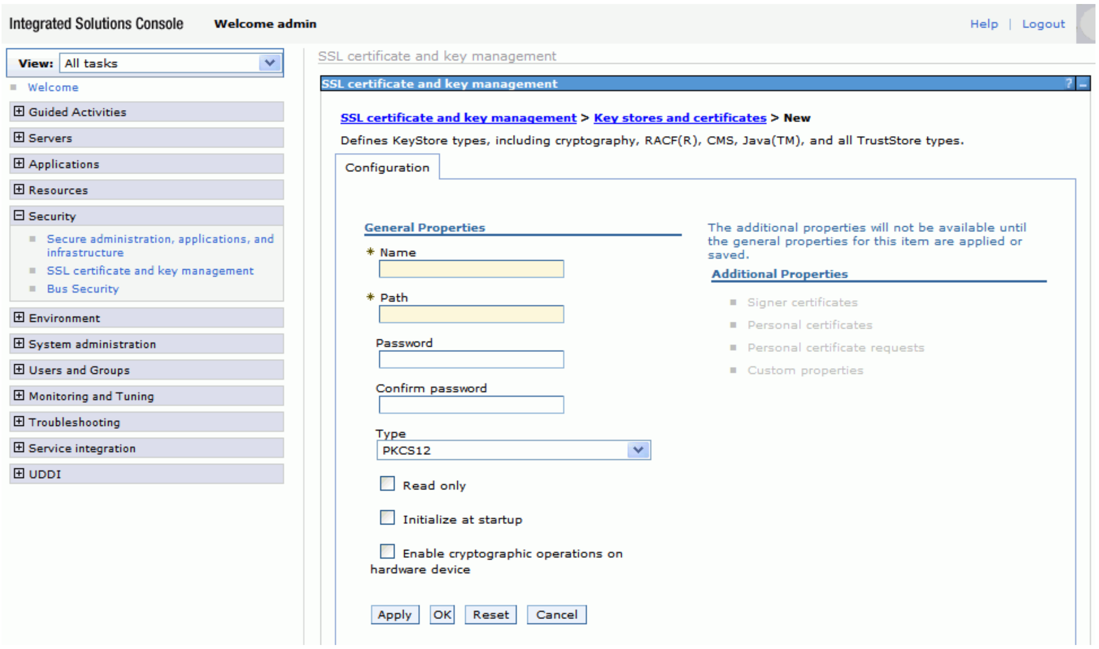
SSL certificate and key management > Key stores and certificates

Defines KeyStore types, including cryptography, RACF(R), CMS, Java(TM), and all TrustStore types.

Select	Name	Path
□	NodeDefaultKeyStore	${CONFIG_ROOT}/cells/idsmhpux07Node01Cell/nodes/idsmhpux07Node02/key.p12
□	NodeDefaultTrustStore	${CONFIG_ROOT}/cells/idsmhpux07Node01Cell/nodes/idsmhpux07Node02/trust.p12
□	NodeLTPAKeys	${CONFIG_ROOT}/cells/idsmhpux07Node01Cell/nodes/idsmhpux07Node02/ltpa.jcek
□	sikeystore	/export/software/MAKeys/sima.keystore
□	sitruststore	/export/software/MAKeys/sica.keystore

Total 5

5 Input a key store name, key store path (point to the key store file you previously created), password and key store type (should be JKS) for your logical trust store.



SSL certificate and key management > Key stores and certificates > New

Defines KeyStore types, including cryptography, RACF(R), CMS, Java(TM), and all TrustStore types.

The additional properties will not be available until the general properties for this item are applied or saved.

* Name

* Path

Password

Confirm password

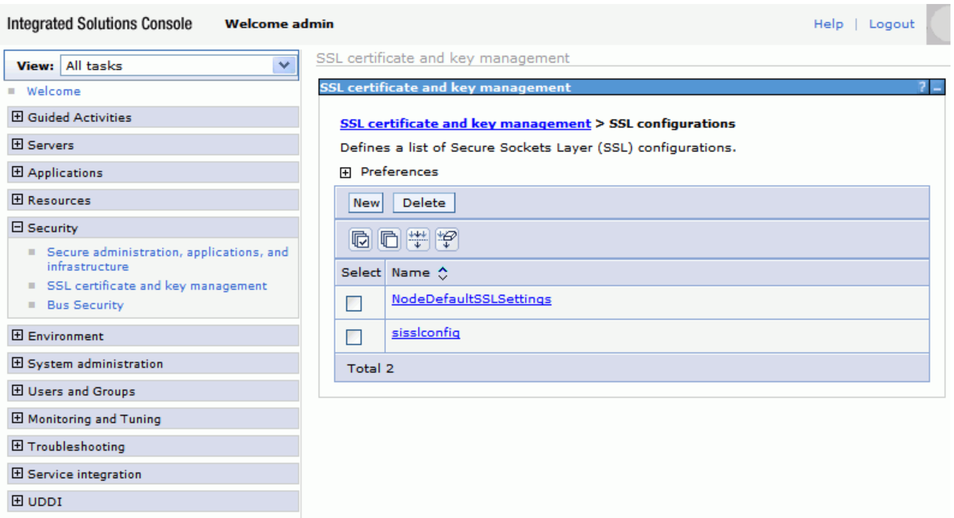
Type: PKCS12

□ Read only

□ Initialize at startup

□ Enable cryptographic operations on hardware device

6 Go back to SSL certificate and key management page, click **SSL configurations** in **Related Items** section. The SSL configuration page displays.

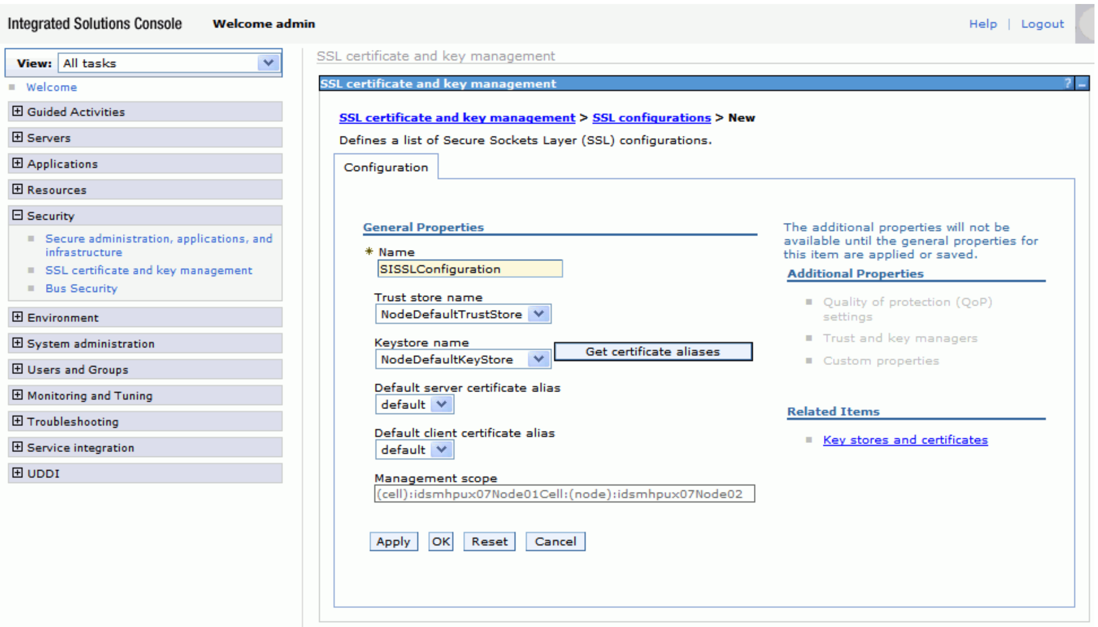


SSL certificate and key management > SSL configurations

Defines a list of Secure Sockets Layer (SSL) configurations.

Select	Name
□	NodeDefaultSSLSettings
□	sisslconfig
Total 2	

7 Click **New.** Define a new SSL configuration that fits your need. Your SSL configuration points to the new logical trust store you defined earlier.



SSL certificate and key management > SSL configurations > New

Defines a list of Secure Sockets Layer (SSL) configurations.

General Properties

* Name: SISSLConfiguration

Trust store name: NodeDefaultTrustStore

Keystore name: NodeDefaultKeyStore

Default server certificate alias: default

Default client certificate alias: default

Management scope: (cell):idsmhpux07Node01Cell:(node):idsmhpux07Node02

The additional properties will not be available until the general properties for this item are applied or saved.

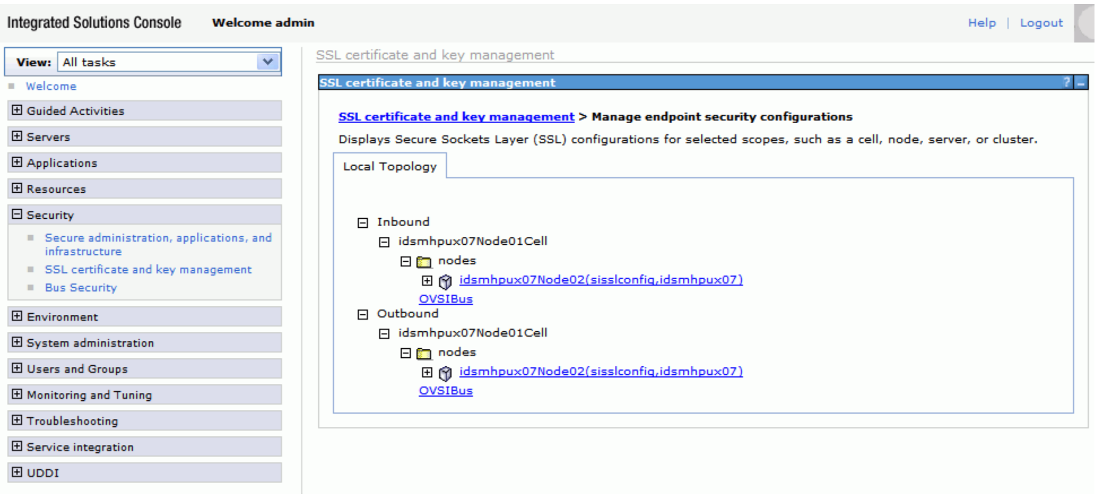
Additional Properties

- Quality of protection (QoP) settings
- Trust and key managers
- Custom properties

Related Items

- Key stores and certificates

8 Go back to SSL certificate and key management page, click **Manage endpoint security configurations** under **Configuration settings** section, then expand **Outbound**.

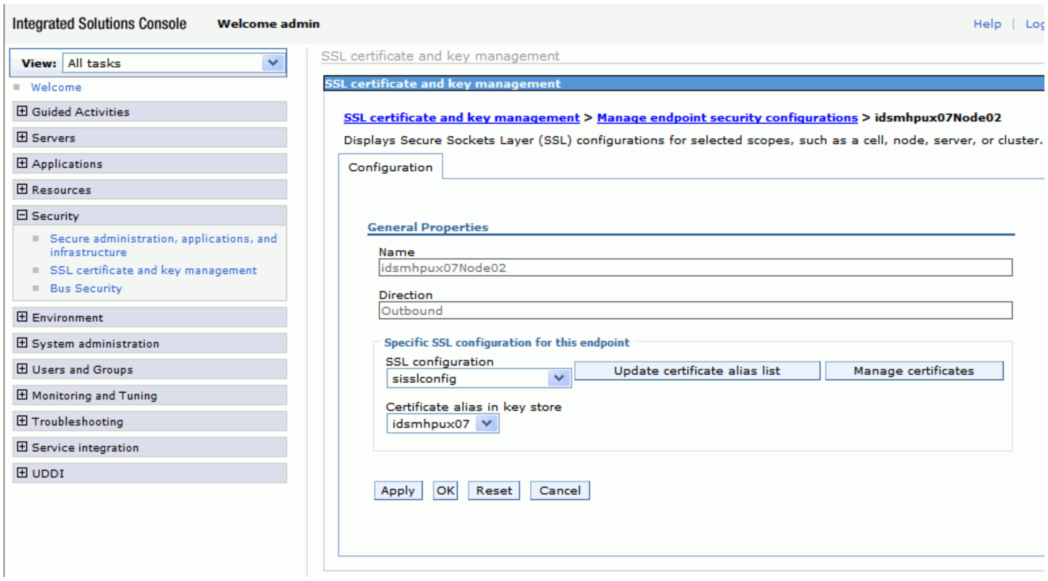


SSL certificate and key management > Manage endpoint security configurations

Displays Secure Sockets Layer (SSL) configurations for selected scopes, such as a cell, node, server, or cluster.

```
⊟ Inbound
   ⊟ idsmhpux07Node01Cell
      ⊟ nodes
         ⊞ idsmhpux07Node02(sisslconfig,idsmhpux07)
   OVSIBus
⊟ Outbound
   ⊟ idsmhpux07Node01Cell
      ⊟ nodes
         ⊞ idsmhpux07Node02(sisslconfig,idsmhpux07)
   OVSIBus
```

9 Select your SSL configuration and certificate alias.



SSL certificate and key management

SSL certificate and key management > Manage endpoint security configurations > idsmhpux07Node02

Displays Secure Sockets Layer (SSL) configurations for selected scopes, such as a cell, node, server, or cluster.

General Properties

Name: idsmhpux07Node02

Direction: Outbound

Specific SSL configuration for this endpoint

SSL configuration: sisslconfig

Certificate alias in key store: idsmhpux07

10 Apply your changes and make sure your setting is saved by WebSphere.

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 `OIDSchema.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 `OIDConfig.properties` file, which is present in the `OIDSchema.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, Oracle Internet Directory Bidirectional LDAP connector uses modify/add and modify/delete operations to support multivalued attribute. When it is set to true, Oracle Internet Directory 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.

- `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 `OIDConnector_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.

4 Configuring the Connector with Select Identity

This chapter describes the procedure to configure the Oracle Internet Directory Bidirectional LDAP 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 Oracle Internet Directory 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/OIDConnector`**.
- 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	ELDAPOID	Name given to the resource.
Connector Name	OID	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:3060 and ldaps://sidc:3130	Resource connection URL - IP:port
Suffix	DC=hp,DC=com	Default root suffix.
Login Name	cn=orcladmin	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 Oracle Internet Directory server.
Password	OIDPASSWORD	Password of the admin user.
Default User Suffix	CN=Users	Suffix where all users exist.
Default Group Suffix	CN=Groups,CN=OracleContext	Suffix where all groups exist.
Mapping File	`OID.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.
Select Identity Locale	en_US	Locale-specific information. If Country = US and Language = English, current locale string is en_US.

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 section, 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 Oracle Internet Directory 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 Oracle Internet Directory Bidirectional LDAP Mapping Information

Select Identity Resource Attribute	Connector Attribute	Attribute on Oracle Internet Directory server	Description
Addr1	Address1	postalAddress	
Addr2	Address2	roomNumber	
Email	Email	mail	
UserName	UserName	uid	*This attribute is mandatory for user creation.*
cn	cn	cn	*This attribute is mandatory for user creation.*
DN	DN	DN	
Zip	Zip	postalCode	
PhBus	BusinessPhone	telephoneNumber	
Password	Password	userPassword	*This attribute is mandatory for user creation.*
Title	Title	Title	
LastName	LastName	sn	*This attribute is mandatory for user creation.*
FirstName	FirstName	givenName	
EmployeeID	EmployeeID	employeeNumber	
State	State	st	
userSuffix	userSuffix	userSuffix	
City	City	l	
orclIsEnabled	orclIsEnabled	orclIsEnabled	While associating the resource to a service, do not add this attribute to the service.

➤ If you modify the mapping file (`OID.xml`), make sure that resource key is set to `uid`.

Configure Workflow External Call on Select Identity

To achieve reverse synchronization, you must configure the workflow external call for user enable/ disable operation for Oracle Internet Directory 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 Oracle Internet Directory Bidirectional LDAP Connector

Serial Number	Parameter Name	Parameter Value
1	AttributeName	orclIsEnabled
2	EnableValue	Enabled
3	DisableValue	Disabled
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, select the Sensitive checkbox only in 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 Oracle Internet Directory 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 Oracle Internet Directory Bidirectional LDAP service view has some attributes as mandatory, all of them should exist on Oracle Internet Directory 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 Oracle Internet Directory 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 Oracle Internet 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 Oracle Internet Directory server and you must not use that username/ login name for any other operation on Oracle Internet 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\oid\
  OIDConfig.properties
  ```