

HP OpenView Select Identity

Connector for OpenLDAP Directory Server (One-Way LDAP Based)

Connector Version: 1.0

Installation and Configuration Guide

Document Release Date: November 2006
Software Release Date: November 2006



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

© Copyright 2006 Hewlett-Packard Development Company, L.P.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>). Portions Copyright (c) 1999-2003 The Apache Software Foundation. All rights reserved.

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 (C) 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 (c) 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 OpenView Support web site at:

www.hp.com/managementsoftware/support

HP OpenView 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 a support contract.

To find more information about access levels, go to:

www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

www.managementsoftware.hp.com/passport-registration.html

Contents

1	Documentation Map	7
2	Introduction	9
	About HP OpenView Select Identity	9
	About Connectors	9
	About OpenLDAP Connector	9
	Overview of Installation Tasks	10
3	Installing the Connector	13
	OpenLDAP Connector Files	13
	System Requirements	13
	Pre-Installation Task	14
	Install OpenLDAP Directory Server Certificate on Application Server	14
	Extracting Contents of the Schema File	15
	Verifying Configurable Parameters	15
	Installing the Connector RAR	17
4	Configuring the Connector with Select Identity	19
	Configuration Procedure	19
	Add a New Connector	19
	Add a New Resource	19
	Map Attributes	21
5	Uninstalling the Connector	23

1 Documentation Map

This chapter describes the organization of HP OpenView 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 OpenView Select Identity connector. For a list of available product documentation, refer to the [Table 1](#).

Figure 1 Documentation Map

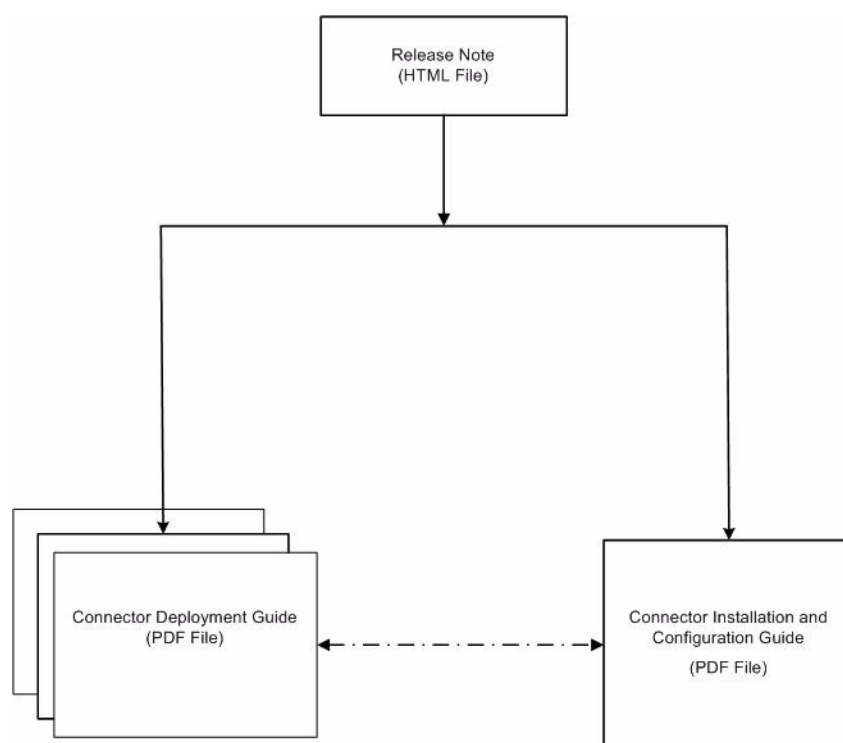


Table 1 Connector Documentation

Document Title and Filename	Contents	Location
<i>Release Note</i> OpenLDAP Connector v1.0 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.
<i>Connector Deployment Guide (for Select Identity 4.10)</i> connector_deploy_SI4.1.pdf	Connector deployment guides provide detailed information on: <ul style="list-style-type: none">• 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/ subdirectory under the connector directory.
<i>Connector Installation and Configuration Guide</i> OpenLDAP_install.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 OpenView Select Identity connector for OpenLDAP Directory Server. An HP OpenView Select Identity connector for OpenLDAP Directory Server enables you to provision users and manage identities on OpenLDAP Directory Server. At the end of this chapter, you will be able to know about:

- The benefits of the HP OpenView Select Identity.
- The role of a connector.
- The connector for OpenLDAP Directory Server.

About HP OpenView Select Identity

HP OpenView 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 OpenLDAP Connector

The connector for OpenLDAP Directory Server — hereafter referred to as the OpenLDAP connector — is a unidirectional connector and it enables Select Identity to perform the following tasks on OpenLDAP 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



This connector can be used with Select Identity 4.10.

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 OpenLDAP 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 19.
	— Verify configurable parameters in the <code>OpenLDAPConfig.properties</code> file.	See Verifying Configurable Parameters on page 19.
	— Install the Resource Adapter Archive (RAR) of the connector on an application server.	See Installing the Connector RAR on page 20.
2	Configure the connector with the Select Identity server.	See Configuring the Connector with Select Identity on page 21.

3 Installing the Connector

This chapter elaborates the procedure to install OpenLDAP connector on Select Identity server. At the end of this chapter, you will know about

- Software requirements to install the OpenLDAP connector.
- Procedure to install OpenLDAP connector.

OpenLDAP Connector Files

The OpenLDAPP connector is packaged in the following files, which are located in the LDAP OpenLDAP directory of the Select Identity Connector CD:

Table 3 OpenLDAP Connector Files

Serial Number	File Name	Description
1	OpenLDAPConnector.rar	It contains the binaries for the connector.
2	OpenLDAPSchema.jar	It contains the mapping file (OpenLDAP.xml), which control how Select Identity fields are mapped to OpenLDAP Directory Server fields. It also contains the OpenLDAPConfig.properties configuration files.

System Requirements

The OpenLDAP connector is supported in the following environment:

Table 4 Platform Matrix for OpenLDAP Connector

Select Identity Version	Application Server	Database
4.10	The OpenLDAP connector is supported on all the platform configurations of Select Identity 4.10.	

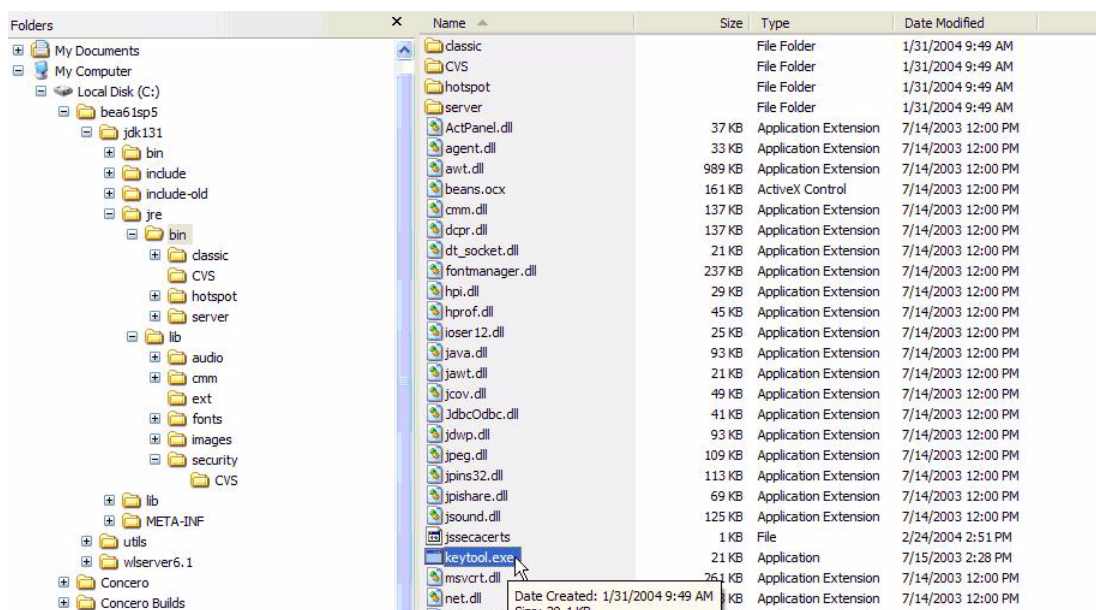
The OpenLDAP connector is supported on OpenLDAP Directory Server 2.3.24 and above.

Pre-Installation Task


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

Install OpenLDAP Directory Server Certificate on Application Server

Before installing the OpenLDAP 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*.



Perform the following steps to install the OpenLDAP certificate.

- 1 Copy the OpenLDAP 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 as **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
```

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 OpenLDAPSchema.jar file to a directory that is in the application server CLASSPATH. Refer to the *HP OpenView Select Identity Connector Deployment Guide* for detailed instruction to extract contents of the Schema file.

Verifying Configurable Parameters

The OpenLDAPConfig.properties file, which is present in the OpenLDAPSchema.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, OpenLDAP Connector uses modify/add and modify/delete operations to support multivalued attribute. When it is set to true, OpenLDAP 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 multivalued attribute is detected in the relog 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 OpenLDAP attribute, where encrypted password is stored.

Installing the Connector RAR

To install the RAR file of the connector (`OpenLDAPConnector.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 OpenView 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/OpenLDAPConnector**.

4 Configuring the Connector with Select Identity

This chapter describes the procedure to configure the OpenLDAP 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 OpenLDAP 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/OpenLDAPConnector**.
- Select **No** for the Mapper Available section.

Refer to the *HP OpenView 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 OpenView 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	OpenLDAP	Name given to the resource.
Connector Name	OpenLDAP	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:389 or ldaps://sidc:636	Resource connection URL - IP:port
Suffix	dc=hpit,dc=com	Default root suffix.
Login Name	cn=Manager,dc=hpit,dc=com	Admin User Login Name.
Password	Abc123	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	OpenLDAP.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.
SI Locale	en_US	Locale-specific information. If Country = US and Language = English, current locale string is en_US.

Map Attributes

After successfully adding a resource for the OpenLDAP connector, you must map the resource attributes to Select Identity attributes. Refer to the *HP OpenView 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 OpenLDAP Mapping Information

Select Identity Resource Attribute	Connector Attribute	Attribute on OpenLDAP	Description
postalAddress	postalAddress	postalAddress	
Email	Mail	mail	
UserName	uid	uid	<i>This attribute is mandatory for user creation.</i>
CN	cn	cn	<i>This attribute is mandatory for user creation.</i>
Zip	postalCode	postalCode	
PhBus	telephoneNumber	telephoneNumber	
Password	userPassword	userPassword	<i>This attribute is mandatory for user creation.</i>
Title	title	title	
LastName	sn	sn	<i>This attribute is mandatory for user creation.</i>
FirstName	givenName	givenName	<i>This attribute is mandatory for user creation.</i>
State	st	st	
Usersuffix	userSuffix	userSuffix	
City	l	l	
POBox	postOfficeBox	postOfficeBox	
roomNumber	roomNumber	roomNumber	While associating OpenLDAP resource to a service, do not add this attribute to the service.
employeeNumber	employeeNumber	employeeNumber	

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

