

# **HP OpenView Select Identity**

**Connector for iPlanet LDAP Servers**

**Installation and Configuration Guide**

**Connector Version: 3.3**  
**Select Identity Version: 3.3**



**April 2005**

© 2005 Hewlett-Packard Development Company, L.P.

## Legal Notices

### Warranty

*Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.*

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

### Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company  
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

### Copyright Notices

© 2005 Hewlett-Packard Development Company, L.P.

No part of this document may be copied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

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](http://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

HP OpenView Select Identity is a trademark of Hewlett-Packard Development Company, L.P. Microsoft, Windows, the Windows logo, and SQL Server are trademarks or registered trademarks of Microsoft Corporation.

Sun™ workstation, Solaris Operating Environment™ software, SPARCstation™ 20 system, Java technology, and Sun RPC are registered trademarks or trademarks of Sun Microsystems, Inc. JavaScript is a trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

This product includes the Sun Java Runtime. This product includes code licensed from RSA Security, Inc. Some portions licensed from IBM are available at <http://oss.software.ibm.com/icu4j/>.

IBM, DB2 Universal Database, DB2, WebSphere, and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

This product includes software provided by the World Wide Web Consortium. This software includes xml-apis. Copyright © 1994-2000 World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. <http://www.w3.org/Consortium/Legal/>

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

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

BEA and WebLogic are registered trademarks of BEA Systems, Inc.

VeriSign is a registered trademark of VeriSign, Inc. Copyright © 2001 VeriSign, Inc. All rights reserved.

All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

## Support

Please visit the HP OpenView web site at:

**<http://www.managementsoftware.hp.com/>**

This web site provides contact information and details about the products, services, and support that HP OpenView offers.

You can also go directly to the support web site at:

**<http://support.openview.hp.com/>**

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valuable support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter 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 log in. Many also require a support contract.

To find more information about access levels, go to:

**[http://support.openview.hp.com/access\\_level.jsp](http://support.openview.hp.com/access_level.jsp)**

To register for an HP Passport ID, go to:

**<https://passport.hp.com/hpp2/newuser.do>**

# contents

<b>Chapter 1</b>	<b>Installing the Connector</b> .....	7
	System Requirements. ....	8
	Deploying on the Web Application Server. ....	9
	Installing the Change Detection Utility .....	11
	Installation and Configuration. ....	12
	The resourceagent.properties File .....	13
<b>Chapter 2</b>	<b>Understanding the Mapping File</b> .....	15
	General Information. ....	16
	iPlanet LDAP Mapping Information. ....	19
<b>Chapter 3</b>	<b>Configuring the Connector</b> .....	22
<b>Chapter 4</b>	<b>Uninstalling the Connector</b> .....	27
	On WebLogic. ....	27
	On WebSphere .....	28

# Installing the Connector

The iPlanet LDAP connector enables HP OpenView Select Identity to perform the following tasks on an iPlanet LDAP server:

- 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
- Assign and unassign entitlements to and from users

A utility is also provided with this connector that detects changes made to Sun ONE iPlanet 5.2 systems. The utility generates an SPML file that contains the changes and sends a reconciliation request to the Select Identity server. See [Installing the Change Detection Utility on page 11](#) for information about enabling this feature.

The iPlanet LDAP connector is a one-way connector and pushes changes made to user data in the Select Identity database to a target iPlanet server. The mapping file controls how Select Identity fields are mapped to LDAP fields.



This connector is supported on non-US platforms. This connector relies on the JNDI (LDAP's resource provider interface) to exchange data with LDAP.

The iPlanet LDAP connector is packaged in the following files, which are located in the LDAP iPlanet directory on the Select Identity Connector CD:

- `schema.jar` — contains the attribute mapping file for this system
- `TALDAPv3.rar` — contains the connector's binary files

## System Requirements

The iPlanet LDAP connector is supported in the following environment:

Select Identity Version	Application Server	Database
3.0.2	WebLogic 8.1.2 on Windows 2003	SQL Server 2000
	WebLogic 8.1.2 on Solaris 9	Oracle 9i
	WebLogic 8.1.2 on HP-UX 11i	Oracle 9i
	WebSphere 5.1.1 on Solaris 9	DB2 8.2 (or DB2 8.1 Service Pack 7)
3.3	WebLogic 8.1.4 on Windows 2003	SQL Server 2000

This connector is supported with Sun ONE iPlanet 5.0 and 5.2 on Windows 2000 and Solaris 9.



# Deploying on the Web Application Server

To install the iPlanet LDAP connector on the Select Identity server, complete these steps:

- 1 Create a subdirectory in the Select Identity home directory where the connector's RAR file will reside. For example, you could create the `C:\Select_Identity\connectors` folder on Windows. (A connector subdirectory may already exist.)
- 2 Copy the `TALDAPv3.rar` file from the Select Identity Connector CD to the connector subdirectory.
- 3 If deploying the connector on WebLogic, complete the following steps. If deploying on WebSphere, skip to [Step 4 on page 10](#).
  - a Create a schema subdirectory in the Select Identity home directory where the connector's mapping file(s) will reside. For example, you could create the `C:\Select_Identity\schema` folder. (This subdirectory may already exist.)
  - b Extract the contents of the `schema.jar` file (on the Select Identity Connector CD) to the schema subdirectory.
  - c Ensure that the `CLASSPATH` environment variable in the WebLogic server startup script references the schema subdirectory.
  - d Start the application server if it is not currently running.
  - e Log on to the WebLogic Server Console.
  - f Navigate to **My\_domain** → **Deployments** → **Connector Modules**.
  - g Click **Deploy a New Connector Module**.
  - h Locate and select the `TALDAPv3.rar` file from the list. It is stored in the connector subdirectory.
  - i Click **Target Module**.
  - j Select the **My Server** (your server instance) check box.
  - k Click **Continue**. Review your settings.
  - l Keep all default settings and click **Deploy**. The Status of Last Action column should display Success.

- 4 If deploying the connector on WebSphere, complete the following steps:
  - a Stop the application server.
  - b Extract the contents of the `schema.jar` file (on the Select Identity Connector CD) to the `WebSphere\AppServer\lib\ext` directory.
  - c Start the application server.
  - d Log on to the WebSphere Application Server Console.
  - e Navigate to **Resources** → **Resource Adapters**.
  - f Click **Install RAR**.
  - g In the Server path field, enter the path to the `TALDAPv3.rar` file. It is stored in the subdirectory created in [Step 1](#).
  - h Click **Next**.
  - i In the Name field, enter a name for the connector.
  - j Click **OK**.
  - k Click the **Save** link (at the top of the page).
  - l On the Save to Master Configuraton dialog, click the **Save** button.
  - m Click **Resources** → **Resource Adapters**.
  - n Click the new connector.
  - o Click **J2C Connection Factories** in the Additional Properties table.
  - p Click **New**.
  - q In the Name field, enter the name of the factory for the connector. For the SQL connector, enter **eis/LDAPv3**.
  - r Click **OK**.
  - s Click the **Save** link.
  - t On the Save to Master Configuraton dialog, click the **Save** button.
  - u Restart WebSphere.
- 5 Modify the mapping file, if necessary. See [Understanding the Mapping File on page 15](#) for details.

After installing the connector, see [Configuring the Connector on page 22](#) for information about registering and configuring the connector in Select Identity.

# Installing the Change Detection Utility

The Change Detection utility detects the changes made on the LDAP server and generates an SPML file for reconciliation with Select Identity. This utility works with Sun ONE iPlanet 5.2. The following files are provided:

- `runagent.bat`  
A Windows batch file that runs the utility once based on the settings in the `resourceagent.properties` file. The `JAVA_HOME` variable is required to change according to the installation on the target host.
- `runagent.sh`  
A UNIX shell script that runs the utility once based on the settings in the `resourceagent.properties` file. The `JAVA_HOME` variable is required to change according to the installation on the target host.
- `ldapagent.jar`  
The utility executables.
- `ldapjdk.jar`  
The NetScape LDAP JDK executables.
- `resourceagent.properties`  
The configuration file.
- `fieldmapping.properties`  
The mapping files that provides a mapping between LDAP resource and Select Identity resource attribute names.

Also, keep the following in mind:

- The SPML file is user oriented. When the utility detects a group change on the LDAP server, the SPML file is created such that one group contains multiple users. Each user must be specified in an individual SPML request containing only one group.
- When all members of a group are removed, the Retro Plugin does not provide a list of user IDs that were removed. (The utility relies on the Retro Plugin to interact with the LDAP server.) Thus, a request to remove the empty group is not generated. To avoid this and workaround this limitation, it is recommended that you leave a user in a group or delete the least significant user from a group last.
- The password in the change log that is generated is encrypted. The utility cannot decode the password and does not provide the password field as part of the SPML file.

## Installation and Configuration

Complete the following steps to install, configure, and run the utility on the LDAP server:

- 1 Enable the LDAP server to log changes by enabling the Retro ChangeLog Plugin:
  - a Launch LDAP Directory Server.
  - a Click the **Configuration** tab.
  - a Select **Plugins**.
  - a Locate the Retro Changelog Plugin and select **Enable plug-in**.
  - b Save the changes.
- 2 Copy the utility's files from the `ldapagent` directory on the CD to a directory on the LDAP server. All of the files must reside in the same directory.
- 3 Make sure that the JRE (version 1.3.3+) is installed properly and included in the path on the LDAP server.
- 4 Edit the `runagent.bat` or `runagent.sh` file to specify the Java home directory on the server.
- 5 Edit the configuration file. The file is described in [The resourceagent.properties File on page 13](#).
- 6 Run the `runagent.bat` or `runagent.sh` file. It is recommended that you execute the utility as a scheduled job.

The utility generates an SPML file that contains the user information that has changed. If the SPML file is formatted for Select Identity reconciliation through a file upload, upload the file using the Select Identity reconciliation page. Refer to the *HP OpenView Select Identity Administrator Guide* for more information. If the file is formatted for Select Identity reconciliation through Web Services, send the file to Select Identity as specified in the *HP OpenView Select Identity Web Service Developer Guide*.

## The resourceagent.properties File

The following are the parameters provided by the `resourceagent.properties` file and required for reconciliation with Select Identity. All parameters are required. However, only those parameters that you can modify are explained here. *Do not modify parameters not listed here.*

- `debug`  
The audit flag, which enables you to generate debug statements. In general, set this property to **false**.
- `ldap_host`  
The name of the LDAP server.
- `ldap_port`  
The LDAP server's port.
- `ldap_user`  
The user name of the LDAP server; the utility will use this to log in and retrieve changes.
- `ldap_pass`  
The password of the LDAP server user.
- `s_filter`  
The filter DN for the LDAP server.
- `t_checkperiod`  
The frequency (in minutes) to check for changes in LDAP.
- `method`  
The method used to send the reconciliation request (the SPML file) to the Select Identity server. Based on this setting, the SPML will vary slightly. Specify **fileupload** or **webservice**.
- `resourcename`  
The Select Identity resource name for the LDAP server.
- `resource_key_field`  
The attribute that uniquely identifies the user on the resource.
- `si_username_field`  
The user name that will be used to log in to Select Identity.

- `si_ws_userid`  
The user name that enables the Web Service to log in to Select Identity. Set this property only if you specified **webservice** for the `method` property.
- `si_ws_password`  
The password of the user specified by `si_ws_userid`.
- `workingdir`  
The directory where the SPML files will be stored.
- `extension`  
The extension of the generated SPML files.

## Understanding the Mapping File

The iPlanet LDAP connector is deployed with the `iplanet.xml` mapping file, which describes the attributes required by the system. The file is created in XML, according to SPML standards, and is bundled in a JAR file called `schema.jar`. The mapping file is used to map user account additions and modifications from Select Identity to the system resource. When you deploy a resource using the Resources page of the Select Identity client, you can review this file.

You can create attributes that are specific to Select Identity using the Attributes page in the Select Identity client. These attributes can be used to associate Select Identity user accounts with system resources by editing the connector mapping file described in this chapter. This process becomes necessary because, for example, a single attribute “username” can have a different name on different resources, such as “login” for UNIX, “UID” for a database, and “userID” on a Windows server.

This file does not need to be edited unless you want to map additional attributes to your resource. If attributes and values are not defined in this mapping file, they cannot be saved to the resource through Select Identity.

## General Information

The following operations can be performed in the mapping file:

- Add a new attribute mapping
- Delete an existing attribute mapping
- Modify attribute mappings

Here is an explanation of the elements in the XML mapping files provided by the iPlanet LDAP connector:

- **<Schema>**, **<providerID>**, and **<schemaID>**

Provides standard elements for header information.

- **<objectClassDefinition>**

Defines the actions that can be performed on the specified object as defined by that name attribute (in the **<properties>** element block) and the Select Identity-to-resource field mappings for the object (in the **<memberAttributes>** block). For example, the object class definition for users defines that users can be created, read, updated, deleted, reset, and expired in LDAP.

- **<properties>**

Defines the operations that are supported on the object. This can be used to control the operations that are performed through Select Identity. The following operations can be controlled:

- Create (CREATE)
- Read (READ)
- Update (UPDATE)
- Delete (DELETE)
- Enable (ENABLE)
- Disable (DISABLE)
- Reset password (RESET\_PASSWORD)
- Expire password (EXPIRE\_PASSWORD)
- Change password (CHANGE\_PASSWORD)



The operation is assigned as the name of the <attr> element and access to the operation is assigned to a corresponding <value> element. You can set the values as follows:

- true — the operation is supported by the connector
- false — the operation is not supported by the connector and will throw `PermissionException`
- bypass — the operation is not supported by the connector but will not throw any exception; the operation is simply bypassed

Here is an example:

```
<objectClassDefinition name="User" description="iPlanet
User">
  <properties>
    <attr name="CREATE">
      <value>true</value>
    </attr>
    <attr name="READ">
      <value>true</value>
    </attr>
```

- **<memberAttributes>**

Defines the attribute mappings. This element contains <attributeDefinitionReference> elements that describe the mapping for each attribute. Each <attributeDefinitionReference> must be followed by an <attributeDefinition> element that specifies details such as minimum length, maximum length, and so on.

Each <attributeDefinitionReference> element contains the following attributes:

- Name — the name of the reference.
- Required— if this attribute is required in the provisioning (set to true or false).
- Conzero:tafield — the name of the Select Identity resource attribute.
- Conzero:resfield — the name of the physical resource attribute from the resource schema. If the resource does not support an explicit schema (such as UNIX), this can be a tag field that indicates a resource attribute mapping.

- **Concero:isKey** — An optional attribute that, when set to true, specifies that this is the key field to identify the object on the resource. Only one `<attributeDefinitionReference>` can be specified where `isKey="true"`. This key field does not need to be the same as the key field of the identity object in Select Identity.
- **Concero:init** — An optional attribute that identifies that the attribute is initialized with the value of the attribute passed in from Select Identity.

Here is an example:

```
<memberAttributes>
  <attributeDefinitionReference name="User Name"
    required="true" concero:tafield="[User Name]"
    concero:resfield="cn" concero:isKey="true"
    concero:init="true" />
```

The interpretation of the mapping between the connector field (as specified by the `Concero:tafield` attribute) and the resource field (as specified by the `Concero:resfield` attribute) is determined by the connector. The iPlanet LDAP connector has code to interpret the mappings in one way, as follows:

- The connector attribute names are specified in square braces, like this: `[xyz]`. The value of attribute `xyz` is taken from the `UserModel` during provisioning.
- Composite attributes can be specified in the iPlanet LDAP connector mapping file. To do this, specify `[attr1] xxxx [attr2]` as the connector attribute. This specifies that the value of the `attr1` and `attr2` attributes should be combined with the string `xxxx` to form a mapping for the specified resource field. iPlanet LDAP connector has code to handle these composite mappings.

- **<attributeDefinition>**

Defines the properties of each object's attribute. For example, the attribute definition for the `HomeDir` attribute defines that it must be between zero and 100 characters in length and can contain the following letters, numbers, and characters: `a-z`, `A-Z`, `0-9`, `@`, `+`, and a space.

Here is an excerpt from the `iplanet.xml` file:

```
<attributeDefinition name="HomeDir" description="User Home
directory" type="xsd:string" >
  <properties>
```

```

    <attr name="minLength">
      <value>0</value>
    </attr>
    <attr name="maxLength">
      <value>128</value>
    </attr>
    <attr name="pattern">
      <value><![CDATA[[a-zA-Z0-9@+]]> </value>
    </attr>
  </properties>
</attributeDefinition>

```

- **<concerro:entitlementMappingDefinition>**  
Defines how entitlements are mapped to users.
- **<concerro:objectStatus>**  
Defines how to assign status to a user.
- **<concerro:relationshipDefinition>**  
Defines how to create relationships between users.

## iPlanet LDAP Mapping Information

The following are the attribute mappings supported for iPlanet. These are listed in the `iplanet.xml` mapping file. You can add, modify, or delete attributes once you are familiar with the contents of this file. You can edit the Select Identity resource attributes; they reflect the identity information as seen in Select Identity. The physical resource attributes are literal attributes of user accounts on the iPlanet LDAP server. These attributes cannot be changed. See the *HP OpenView Select Identity Connector Developer Guide* for more information about attributes and mapping information.

Select Identity Resource Attribute	iPlanet LDAP Attribute	Description
UserName	uid	Key field on the resource
Password	userpassword	
Email	mail	

<b>Select Identity Resource Attribute</b>	<b>iPlanet LDAP Attribute</b>	<b>Description</b>
FirstName	givenname	
LastName	sn	
FirstName + LastName	cn	
Address 1	postalAddress	
Address 2	roomNumber	
City	l	
State	st	
Zip	postalCode	
Title	title	
Employee ID	employeenumber	
Business Phone	telephoneNumber	
Disable Function	Description="disabled"	Marks the user as disabled
Enable Function	Description="enabled"	Marks the user as enabled
mailHost	mailHost	Mail-related attributes
maildeliveryoption	mailDeliveryOption	
mailQuota	mailQuota	
nslicensedfor	nslicensedfor	
mailAlternateAddress	mailAlternateAddress	
mailForwardingAddress	mailForwardingAddress	
nscalorgunit2	nscalorgunit2	Calendar-related attributes
nscalpasswordrequired	nscalpasswordrequired	
nscalxitemid	nscalxitemid	
nscalflags	nscalflags	

<b>Select Identity Resource Attribute</b>	<b>iPlanet LDAP Attribute</b>	<b>Description</b>
nscallanguageid	nscallanguageid	
nscalsysopcanwrite password	nscalsysopcanwrite password	
nscaldefaultnotereminder	nscaldefaultnotereminder	

## Configuring the Connector

After you deploy the connector on the application server, you must configure Select Identity to use the connector by deploying it in the Select Identity client. The following provides an overview of the procedures you must complete in order to deploy your connector. It also provides connector-specific information you must provide when configuring Select Identity to use the connector.

- 1 Before deploying the connector in Select Identity, connect to LDAP using an LDAP browser or another utility. This will help ensure that the LDAP resource is available and the correct parameters are known before deploying the resource in Select Identity.
- 2 Register the connector with Select Identity by clicking the **Deploy New Connector** button on the Connectors home page. Complete this procedure as described in the “Connectors” chapter of the *HP OpenView Select Identity Administrator Guide*.

After you deploy the connector, the connector properties will look similar to this:

> [Home](#) > [Connectors](#) : LDAP

Connector Information	
* Connector Name:	LDAP
* Pool Name:	eis/LDAPv3

- 3 Deploy a resource that uses the newly created connector. On the Resources home page, click the **Deploy New Resource** button. When configuring the resource, refer to the following table for parameters specific to this connector:

Field Name	Sample Values	Description
Resource Name	local_ipplanet	Name of the target resource.
Resource Type	iPlanet LDAP	The connector that was deployed in <a href="#">Step 2 on page 22</a> .
Authoritative Source	No	Whether this resource is a system that is considered to be the authoritative source for user data in your environment. You must specify <b>No</b> because the connector cannot synchronize account data with the Select Identity server.
Associate to Group	Selected	Whether the system uses the concept of groups. For the iPlanet LDAP connector, select this option.
Access URL	ldap://localhost:389	URL access to the resource.
Suffix	dc=india, dc=hp	The domain(s) to which the users will be provisioned.
Login Name	cn=Directory Manager uid=hp_admin,dc=Directory Administrators, dc=trulogica,dc=com	Login account with administrative privileges to add and delete users. This is required to log in to the resource.  If an ID other than Directory Manager was created, use the full DN, as in the second sample value here.
Password	Password123	Password corresponding to the login account.

Field Name	Sample Values	Description
User Suffix	ou=people	Suffix of user's distinguished name. This is the location in the tree where the users will be provisioned.
User Object Class	top, person, organizationalPerson, inetorgPerson	Object class of users.
Group Suffix	ou=groups	Suffix part of group's distinguished name. This is the location in the tree where the user groups will be provisioned.
Group Object Class	top, groupofuniquenames	Object class of user groups.
Mapping File	iplanet.xml	Location of the connector mapping file, which is used to map resource attributes to Select Identity attributes.

Complete the steps in this procedure as described in the “Resources” chapter of the *HP OpenView Select Identity Administrator Guide*.

After you deploy the resource, the Access Info properties for the resource will look similar to this:

> [Home](#) > [Resources](#) > [View Resource](#) : LDAP66

Resource Access Information	
* Resource Name:	LDAP66
Access URL:	ldap://16.73.17.66:389
Suffix:	dc=qa,dc=trulogica,dc=com
Login Name:	cn=Directory Manager
Password:	*****
* User Suffix:	ou=people
* User Object Class:	top,person,organizationalPerson,inetorgperson
* Group Suffix:	ou=Groups
* Group Object Class:	top,groupofuniquenames
* Mapping File:	iplanet.xml



- 4 Create attributes that link Select Identity to the connector. For each mapping in the connector's mapping file, create an attribute using the Attributes capability on the Select Identity client.

Refer to the "Attributes" chapter in the *HP OpenView Select Identity Administrator Guide* for more information. After you create the attributes for the iPlanet Active Directory connector, the View Attributes page for the resource will look similar to this:

(Resource Name=LDAP70)				
<< Page 1 of 1 >>				Total Records:28
Name	Min Length	Max Length	Attribute Mapped To	Authorative
Address 1	1	128	Addr1	N
Address 2	1	128		
Business Phone	1	50		
City	1	128	Info	N
Email	1	128		
Employee ID	1	128	Company	N
FirstName	1	128	FirstName	N
LastName	1	128	LastName	N
LDAP70_ENTITLEMENTS	1	255	LDAP70_ENTITLEMENTS	Y
LDAP70_KEY	1	255	LDAP70_KEY	Y
mailAlternateAddress	1	128		
maildeliveryoption	1	128		
mailForwardingAddress	1	128		
mailHost	1	128		
mailQuota	1	10		
nscaldefaultnotereminder	1	8		
nscallflags	1	8		
nscallanguageid	1	8		
nscalorgunit2	1	8		
nscalpasswordrequired	1	8		
nscalsysopcanwritepassword	1	8		
nscalxitemid	1	8		
nslicensedfor	1	10		
Password	1	128	Password	N
State	1	128	State	N
Title	1	50		
UserName	1	128	UserName	N
Zip	1	50	Zip	N

- 5 Create a Service that will use the newly created resource. To do so, click the **Deploy New Service** button on the Services home page. Complete this procedure as described in “Services” of the *HP OpenView Select Identity Administrator Guide*. You will reference your new resource created in [Step 3](#) while creating this service.

# Uninstalling the Connector

If you need to uninstall a connector from Select Identity, make sure that the following are performed:

- All resource dependencies are removed.
- The connector is deleted using the Select Identity client Connectors pages.

## On WebLogic

Perform the following to delete a connector:

- 1 Log on to the WebLogic Server Console.
- 2 Navigate to ***My\_Domain*** → **Deployments** → **Connector Module**.
- 3 Click the delete icon next to the connector that you want to uninstall.
- 4 Click **Yes** to confirm the deletion.
- 5 Click **Continue**.

## On WebSphere

Complete the following steps to uninstall the connector on WebSphere:

- 1 Log on to the WebSphere Application Server Console.
- 2 Navigate to **Resources** → **Resource Adapters**.
- 3 Select the connector to uninstall.
- 4 Click **Delete**.
- 5 Click the **Save** link (at the top of the page).
- 6 On the Save to Master Configuraton dialog, click the **Save** button.