HP OpenView Select Identity

Connector for Windows® Active Directory (One-Way LDAP Based)

Software Version: 4.3

Installation and Configuration Guide

Document Release Date: July 2006
Software Release Date: July 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

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

Please visit the HP OpenView support web site at:

http://www.hp.com/managementsoftware/support

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

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 enhancement requests online
- Download software patches
- 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://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

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

Contents

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

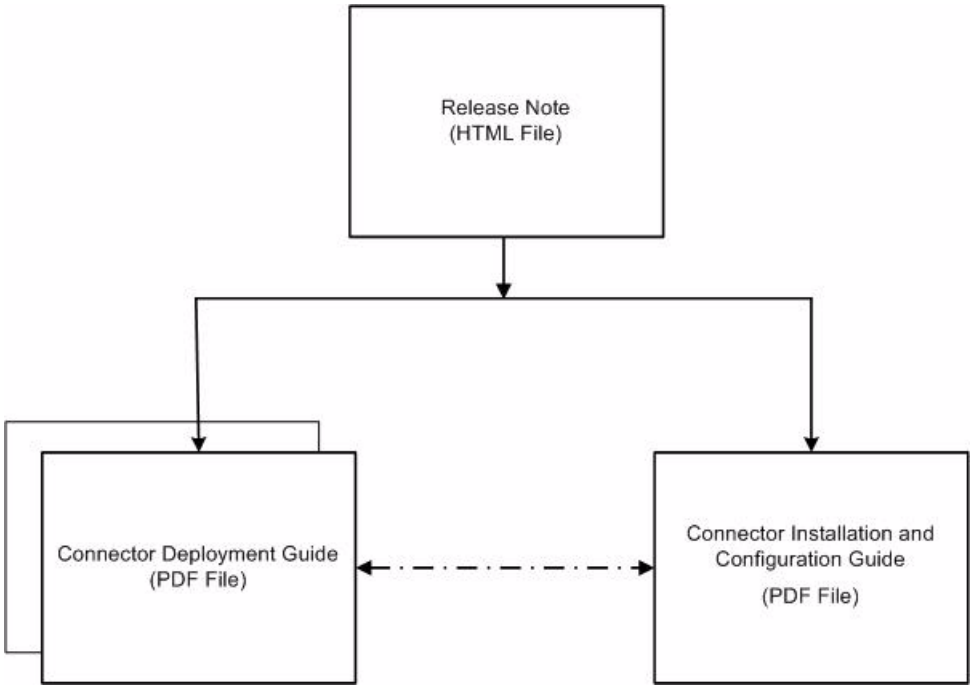


Table 1 Connector Documentation

Document Title and Filename	Contents	Location
Release Note `Active Directory LDAP Connector v4.3 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 4.0/4.01.000) `connector_deploy_SI4.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/` subdirectory under the connector directory.
Connector Installation and Configuration Guide `Active Directory LDAP_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 Active Directory. An HP OpenView Select Identity connector enables you to provision users and manage identities on Active Directory. At the end of this chapter, you will be able to know about:

- The benefits of HP OpenView Select Identity.
- The role of a connector.
- The connector for Active Directory.

About HP OpenView Select Identity

HP OpenView Select Identity provides a new approach to identity management. It helps you manage the entire identity lifecycle of an enterprise application. 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. It is installed on the system where Select Identity is installed. 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 Active Directory LDAP Connector

The one-way LDAP based connector for Active Directory — hereafter referred to as Active Directory LDAP connector — enables HP OpenView Select Identity to Select Identity to perform the following operations on Active 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
- Retrieve all entitlements
- Retrieve a list of supported user attributes
- Grant and revoke entitlements to and from users, including the addition of users to multiple OUs.
- Provision users over SSL.

When the connector adds a user to the Active Directory LDAP resource, the user is assigned to a default group called "Domain User." Do not use this group as an entitlement; you cannot remove this group from the user.

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

This connector can be used with Select Identity 4.01.000 and 4.0.

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.
	— Enable secure LDAP communication	See Pre-Installation Task: Enabling Secure LDAP on page 14.
	— Extract contents of the Schema file (file that contains the mapping files for the connector) to location on the Select Identity server.	See Extracting Contents of the Schema File on page 16.
	— Install the Resource Adapter Archive (RAR) of the connector on an application server.	See Installing the Connector RAR on page 17.
2	Configure the connector with the Select Identity server.	See Configuring the Connector with Select Identity on page 19.

3 Installing the Connector

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

- Software requirements to install the Active Directory LDAP connector.
- Prerequisite conditions to install Active Directory LDAP connector.
- Procedure to install Active Directory LDAP connector.

Active Directory LDAP Connector Files

Active Directory LDAP connector is packaged with the following files.

Table 3 Active Directory LDAP Connector Files

Serial Number	File Name	Description
1	`TALDAPv3.rar`	The connector RAR file (the binaries).
2	`schema.jar`	It contains the attribute mapping file (`activedir40.xml`) for this system, which control how Select Identity fields are mapped to Active Directory LDAP fields.

These files are located in the `LDAP Active Dir` directory on the Select Identity Connector CD.

System Requirements

The Active Directory LDAP connector is supported in the following environment:

Table 4 Platform Matrix for the Active Directory LDAP Connector

Select Identity Version	Application Server	Database
4.0/4.01.000	The Active Directory LDAP connector is supported on all the platform configurations of Select Identity 4.0 and 4.01.000.	

This connector is supported with Active Directory on Windows 2000 and Windows 2003

The Active Directory 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:

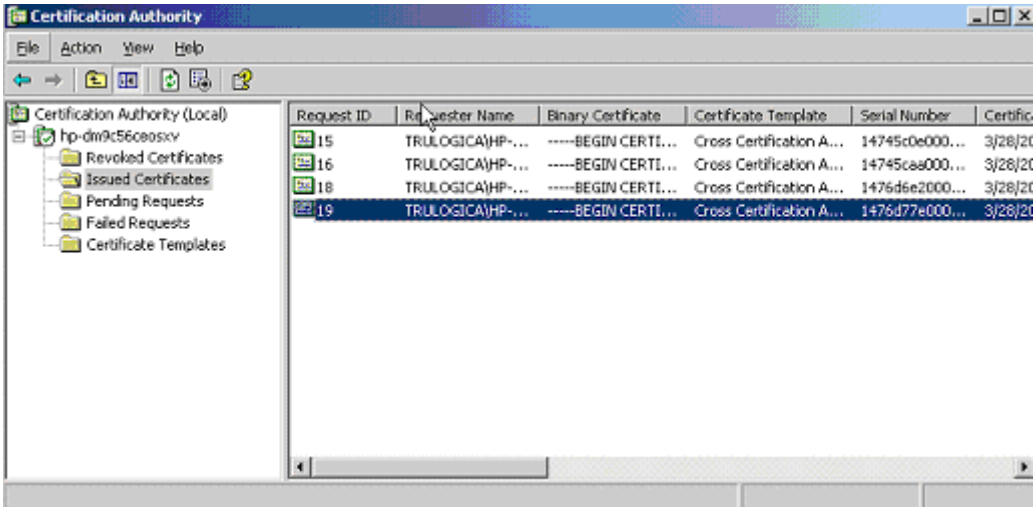
- The Select Identity server should be configured for internationalization. Refer to the *HP OpenView Select Identity Installation and Configuration Guide* for more information.
- The resource should be configured to support local language characters.

Pre-Installation Task: Enabling Secure LDAP

You must use secure LDAP (LDAPS) to connect to Windows Active Directory for user password changes. Without this, the Active Directory LDAP connector cannot update passwords in Active Directory. Also, for Active Directory on Windows 2003, you must use LDAPS for all tasks.

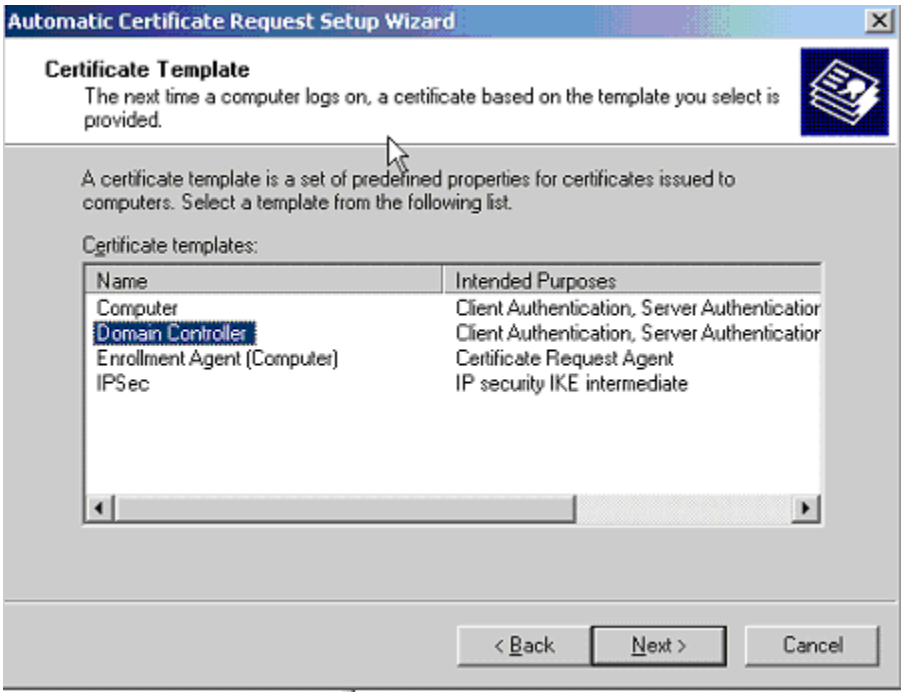
Perform the following steps to enable secure communication (LDAPS) on the Active Directory system:

1. Install the Certificate Services Component from the Windows CD.
2. Configure HTTPS on the system.
3. Create a Certificate Authority (from Administrative Tools ¨ Certification Authority), which also creates a root certificate. The following shows the certificate after it is created on Windows 2003:

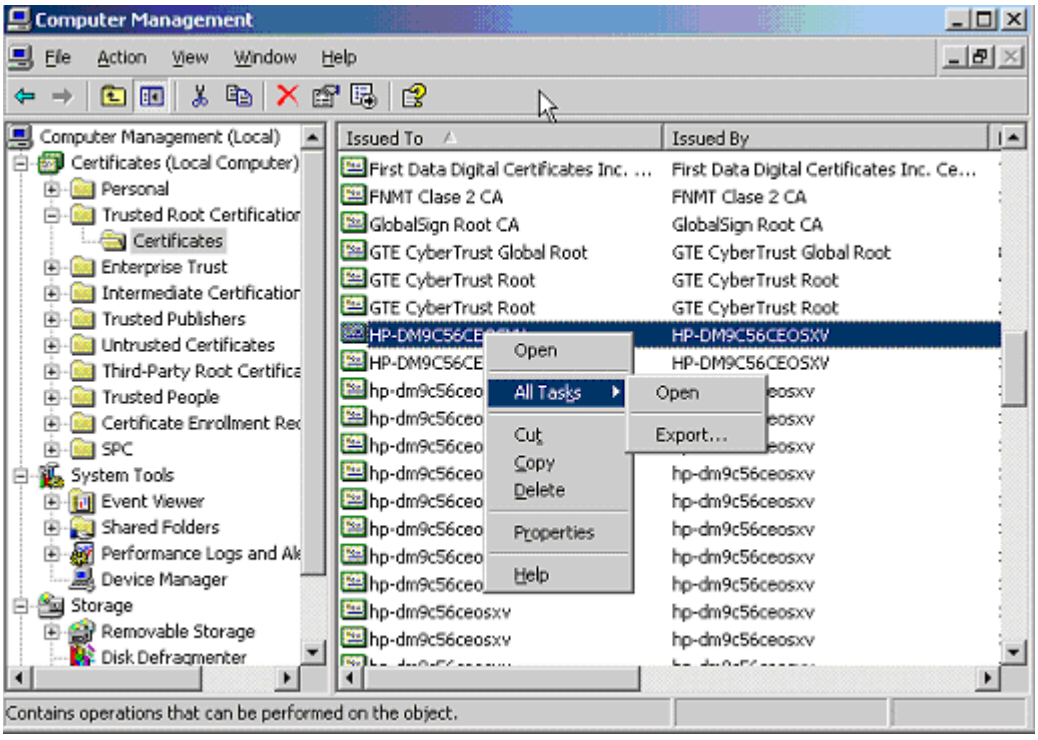


4. Create an Automatic Certificate Request (from **Administrative Tools → Domain Controller Security Policy→ Public Key Policies**).

When prompted, select **Domain Controller**, as shown here:



5 After the new entries are displayed in Administrative Tools → Certification Authority → Issued Certificates, open the certificate (using the snap-in from mmc), which is located under Trusted Root Certification Authorities → Certificates and has the same name as the CA.



6 Export the certificate and specify a file name with the extension `.cer`.

7 Download the certificate to the Select Identity server from the Active Directory server by loading the following URL in a browser on the Select Identity server:

http://AD_host/certsrv

Specify the login credentials for the Active Directory server when prompted. Be sure to download the certificate to the *%JAVA_HOME%*`\jre\lib\security` directory.

You can also copy the certificate to the Select Identity server.

8 From the command line, change directories to the %JAVA_HOME%\jre\bin directory and verify the certificate by printing it by using the following command:

```
keytool -printcert -v -file filename.cer
```

It should display an output similar to this:

```
C:\>cd bea\jdk142_05\jre\lib\security

C:\bea\jdk142_05\jre\lib\security>keytool -printcert -v -file AD_03_28_1.cer
Owner: CN=HP-DM9C56CEOSXU, DC=trulogica, DC=local
Issuer: CN=HP-DM9C56CEOSXU, DC=trulogica, DC=local
Serial number: 7f08ce59f430a6884a09f8ad7aaabcbf
Valid from: Fri Dec 10 14:13:35 CST 2004 until: Thu Dec 10 14:17:47 CST 2009
Certificate fingerprints:
         MD5:  5B:BB:F6:A7:ED:4D:43:52:21:67:06:13:02:96:6A:98
         SHA1: 7B:97:6C:5F:81:53:2D:FF:DB:3F:89:67:6B:83:D8:9B:C3:48:E8:6E
```

9 Perform the following steps to install the certificate on the Select Identity server:

a Import the certificate into the cacerts keystore using this keytool command:

```
keytool -import -v -trustcacerts -alias alias -file filename.cer
-keystore cacerts
```

b When challenged, enter the keystore password.

c Specify yes when prompted to trust the certificate.

d Ensure that the certificate is imported by listing it:

```
keytool -list -alias CA123 -keystore file_name
```

e Copy the keystore file to the *%JAVA_HOME%*`\jre\lib\security` directory, which may overwrite an existing file.

f Restart the application server.

10 To verify that the Select Identity server can connect to the Active Directory server using a secure connection (LDAPS), specify **ldaps://AD_host:636** for the Access URL when you create a resource for the connector.

Refer to the white paper *Provisioning to AD with HP OpenView Select Identity using LDAP over SSL* for more information on configuring Active Directory with certificate.

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 `schema.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.

Installing the Connector RAR

To install the RAR file of the connector (`TALDAPv3.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/LDAPv3`**.

After deploying the connector RAR on application server, you must configure Active Directory LDAP connector with Select Identity. Refer to Configuring the Connector with Select Identity on page 19 for configuration steps.

4 Configuring the Connector with Select Identity

This chapter describes the procedure to configure the Active Directory LDAP connector with Select Identity. At the end of this chapter, you will know the procedure to configure the Active Directory 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 Active Directory 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/LDAPv3`**.
- 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 instructions 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	ActiveDirectory	Name of the target resource.
Connector Name	AD LDAP	The newly deployed connector.
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 **No** because the connector cannot synchronize account data with the Select Identity server.
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://136.168.1.20:389 ldaps://192.168.1.19:636	URL to access the resource. If using secure LDAP (ldaps) for password changes, specify **ldaps** as the protocol and **636** as the port.
Suffix	dc=qa, dc=hp, dc=com	The domain(s) to which the users will be provisioned.
Login Name	cn=Administrator, cn=Users, dc=qa, dc=hp, dc=com	Login account with administrative privileges to add and delete users. This is required to log in to the resource.
Password	Password123	Password corresponding to the login account.
User Suffix*	cn=users	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 for the users.
Group Suffix*	cn=users	Suffix part of group's distinguished name. This is the location in the tree where the user groups will be provisioned. This parameter is optional (you can leave this field blank).

Table 5 Resource Configuration Parameters

Field Name	Sample Values	Description
Group Object Class	top, groupofuniquenames	Object class of user groups.
Mapping File	`activedir40.xml`	Location of the connector mapping file, which is used to map resource attributes to Select Identity attributes.
Cleanup Groups	Selected	Whether to delete the user's entitlements when the user is deleted from Select Identity.

*Instead of creating an authoritative resource, you can create authoritative attributes (in the next step) for the attributes that will be synchronized. Entitlements are authoritative by default in a non-authoritative resource but other attributes are not.

Map Attributes

After successfully adding a resource for the Active Directory LDAP 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 Active Directory LDAP Mapping Information

Select Identity Resource Attribute	Active Directory LDAP Attribute	Description
User Name	cn	Key field on the resource
Password	UnicodePwd	
First Name	givenname	
Last Name	sn	
User Name	samaccountname	
FirstName + LastName	displayname	
Directory	homeDirectory	
Last Name + First Name	userPrincipalName	
Address 1	streetAddress	
Address 2	postOfficeBox	
City	l	
State	st	
Zip	postalCode	
Title	title	

Table 6 Active Directory LDAP Mapping Information

Select Identity Resource Attribute	Active Directory LDAP Attribute	Description
Business Phone	telephoneNumber	
Home Phone	homePhone	
Profile Path	profilePath	
Script Path	scriptPath	
Description	description	
Disable function	userAccountControl=514	Disables a user
Enable function	userAccountControl=512	Enables a user

After mapping the attributes, 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 Administrator Guide* for information on Select Identity services.

5 Uninstalling the Connector

If you want to uninstall a connector from Select Identity, perform the following steps:

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

See *HP OpenView Select Identity Deployment Guide* to for information on deleting a connector from Select Identity and application server.