HP OpenView Select Identity

Connector for Microsoft® Active Directory (unidirectional LDAP based)

Connector Version: 4.2

Installation and Configuration Guide

Document Release Date: March 2006
Software Release Date: March 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 Introduction

This chapter gives an overview of the HP OpenView Select Identity connector for Microsoft Active Directory server. An HP OpenView Select Identity connector allows you to provision users and manage identities on Microsoft Active Directory server. 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 Microsoft Active Directory server

About HP OpenView Select Identity

HP OpenView Select Identity (OVSI) provides a new approach to identity management. It helps you manage the entire identity lifecycle of an enterprise application. By using OVSI, you can automate the process of provisioning and managing user accounts and access privileges across platforms, applications, and corporate boundaries. OVSI 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 OVSI by using a connector. A connector is resource specific. It is installed on the system where OVSI is installed. The combination of OVSI 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 OVSI, but if any change takes place in resource, it cannot communicate that back to OVSI. On the other hand, a bidirectional connector can reflect the changes made on resource back to OVSI. This property of bidirectional connectors is known as **reverse synchronization**.

About Active Directory LDAP Connector

The connector for Microsoft Active Directory server version 5.2 — hereafter referred to as Active Directory LDAP connector — enables you to perform the following tasks on Microsoft Active Directory server by using OVSI.

- 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 Operating Units
- Change log retrieval
- Provision users over Secure Server Logon (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.

This connector can be used with OVSI version 4.0.

2 Installing the Connector

Active Directory LDAP connector is packaged with the following files.

Table 1 Active Directory LDAP Connector Files

Serial Number	File Name	Description
1.0	`TALDAPv3.rar`	It is the Resource Adapter Archive (RAR) file for the connector. It contains the connector binary files.
2.0	`schema.jar`	It contains the attribute mapping file (`ActiveDir40.xml`) for this system, which controls how the OVSI fields are mapped to Microsoft Active Directory server 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 2 Platform Matrix for Active Directory LDAP Connector

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)

Table 2 Platform Matrix for Active Directory LDAP Connector

Select Identity Version	Application Server	Database
3.3	WebLogic 8.1.4 on Windows 2003	SQL Server 2000
3.3.1	WebLogic 8.1.4 on Windows 2003	SQL Server 2000
	WebSphere 5.1.1 on HP-UX 11i	Oracle 9i
4.0	The Active Directory LDAP connector is supported on all the platform configurations of Select Identity 4.0.	

The connector is supported with Active Directory on Windows 2000 and Windows 2003. On Windows 2000, you can enable secure communication (LDAPS) for this connector. On Windows 2003, you *must* enable LDAPS. See Install Secure LDAP on page 10 for configuration details.

Installation Procedure

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.

Perform the following tasks to install the Active Directory LDAP connector on OVSI system.

1 Install Secure LDAP

2 Deploy the Connector on Application Server

3 Configure the Connector with OVSI

4 Configure the Connector with OVSI

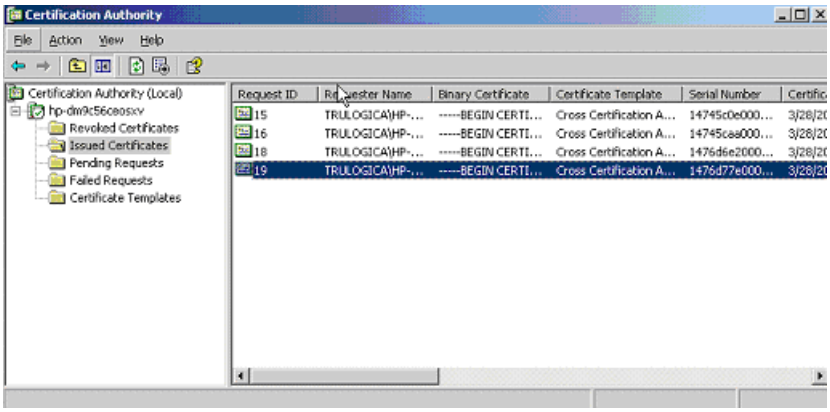
Install Secure LDAP

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.

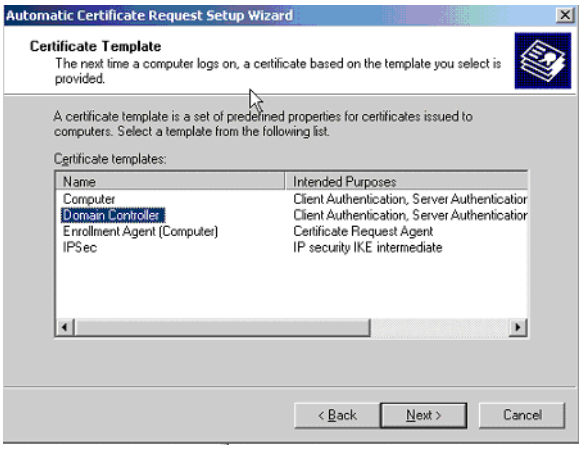
Complete the following steps to enable secure communication (LDAPS) on the Active Directory system:

1 Install the Certificate Services Component from the Windows CD.

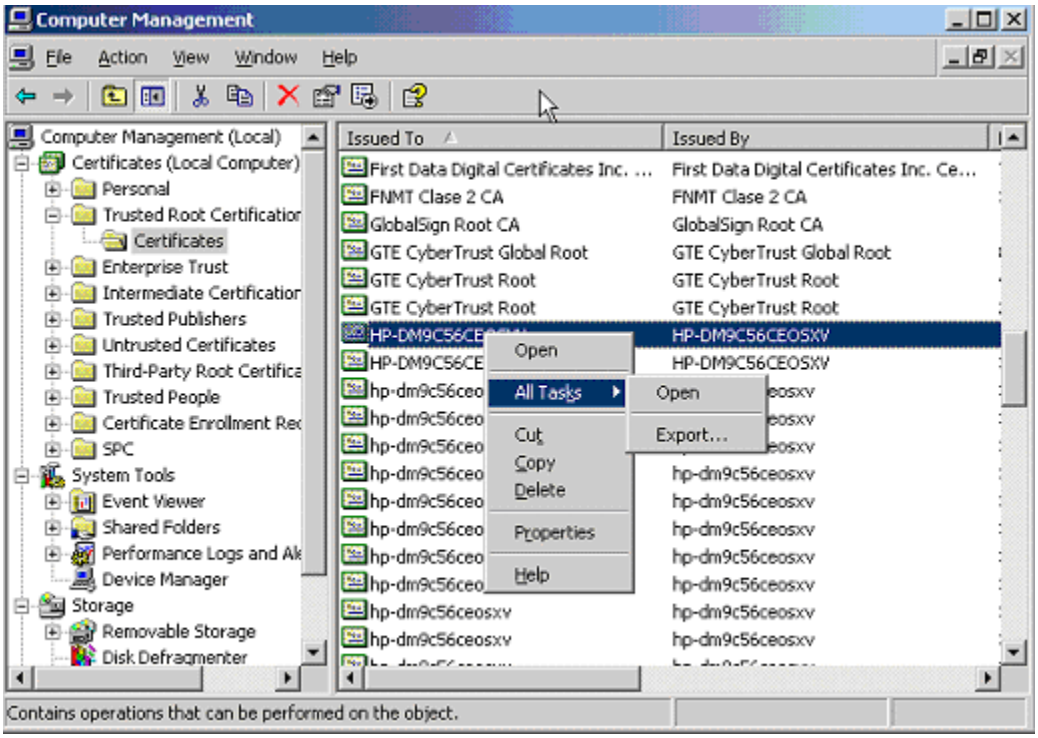
2 Configure HTTPS on the system. Create a Certificate Authority (from Administrative Tools → Certification Authority), which also creates a root certificate. The following shows the certificate after it is created on Windows 2003:



3 Create an Automatic Certificate Request (from Administrative Tools → Domain Controller Security Policy → Public Key Policies). When prompted, select **Domain Controller**, as shown here:



4 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.



5 Export the certificate and specify a file name with the extension **.cer**.

6 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.

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

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

It should display 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-DM9C56CEOSXV, DC=trulogica, DC=local
Issuer: CN=HP-DM9C56CEOSXV, 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
```

8 Install the certificate on the Select Identity server, as follows:

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.

9 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. See step 3 on page 18 for details.

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.

Extract the Contents of Schema File

Create a subdirectory in the OVSI home directory on OVSI system. Extract the contents of `schema.jar` file to this subdirectory. Ensure that the `CLASSPATH` environment variable in the application server startup script references this `Schema` subdirectory.

Deploy the Connector on Application Server

You must deploy the RAR file (`TALDAPv3.rar`) of the connector on an application server. Before deploying the RAR file, you must copy it to a local directory from the connector CD. Refer to *HP OpenView Select Identity Connector Deployment Guide* for more information on deploying a connector on an application server.

Configure the Connector with OVSI

After deploying the connector to an application server, you must configure it with OVSI. Before configuring the connector with OVSI, connect to the Lightweight Directory Access Protocol (LDAP) server by using an LDAP browser or any other utility. This can ensure that the LDAP resource is available and the correct parameters are known before deploying the resource in OVSI.

To configure the connector with OVSI, perform the following steps.

1 Add a new connector – Add a new connector on OVSI. Refer to *HP OpenView Select Identity Connector Deployment Guide* for information on adding a new connector. While adding the connector, under Current Resource Connectors section in Manage Connectors page, do the following:

— In the Connector Name text box, specify a name for the connector.

— In the Pool Name text box, enter **eis/LDAPv3**.

— Under Mapper Available section, select **No.**

2 Add a resource — You must add a resource to OVSI that uses the newly added connector. Refer to *HP OpenView Select Identity Connector Deployment Guide* for the instructions to achieve this. While entering the resource parameters for Active Directory LDAP connector, refer to the table below.

Table 3 Resource Configuration Parameters

Field Name	Sample Values	Description
Resource Name	*ActiveDirectory*	Name of the target resource.
Resource Type	*AD LDAP*	The connector that was deployed in step 1 on page 13.
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.
Associate to Group	*Selected*	Whether the system uses the concept of groups. For this LDAP connector, select this option.
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,user*	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 3 Resource Configuration Parameters

Field Name	Sample Values	Description
Group Object Class	*Top, group*	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.

This connector supports the addition of users to different OUs. To enable this, specify the appropriate values for the User Suffix and Group Suffix while creating the resource.

3 Map the attributes — You must map the OVSI attributes to the attributes of the resource. Refer to *HP OpenView Select Identity Connector Deployment Guide* for information on mapping attributes. While mapping the attributes, refer to the following table for resource specific mapping information.

Table 4 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	
Business Phone	telephoneNumber	
Home Phone	homePhone	

Table 4 Active Directory LDAP Mapping Information

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

Also, if you are using LDAP, not LDAPS, edit the following attribute in the mapping file:

<attributeDefinitionReference name="userAccountControl"
required="true" concero:tafield="546"...

to assign 512 to the tafield attribute:

```
<attributeDefinitionReference name="userAccountControl"
required="true" concero:tafield="512"...
```

This will create the account without a password, though the account will be disabled.

4 Associate the newly added resource to a service. Refer to the chapter *Service Studio* of *HP OpenView Select Identity Administrator Guide* for more information on service.

3 Uninstalling the Connector

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

1. Remove all resource dependencies.
2. Delete the connector from OVSI.
3. Delete the connector from application server.

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