HP OpenView Select Identity

Connector for Microsoft® Active Directory (Bidirectional LDAP Based)

Connector Version: 1.0

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. An HP OpenView Select Identity connector allows you to provision users and manage identities on Active Directory system. 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

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 Connector

The bidirectional LDAP based connector for Microsoft Active Directory server — hereafter referred to as Active Directory connector — enables OVSI to perform the following tasks in Active Directory server:

- Add, update, and remove users

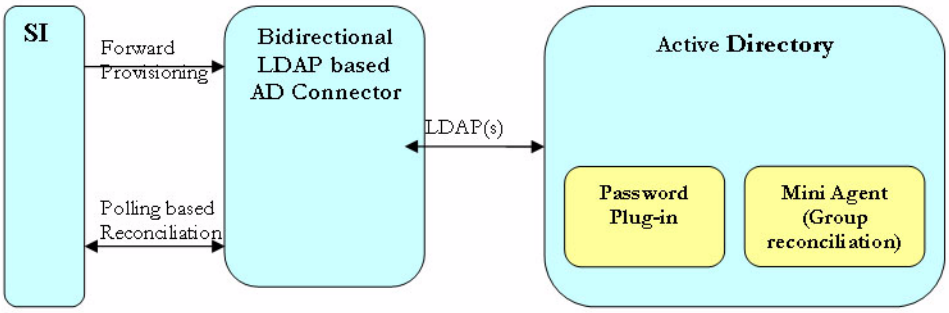
- Retrieve user attributes
- Enable and disable users
- Verify a user's existence
- Change user passwords
- Reset user passwords
- Expire passwords
- Validate passwords
- Retrieve all entitlements
- Retrieve a list of supported user attributes
- Grant and revoke entitlements to and from users

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

A reverse synchronization feature reconciles user account changes made on the Active Directory resource with OVSI. OVSI periodically polls the Active Directory resource to retrieve changes through the connector.

This connector can be used with OVSI 4.0 and 3.3.1.

Figure 1 High Level Architecture of the Connector



The connector also has two agents, namely Password plug-in for password reconciliation and Mini Agent for group reconciliation which sits on the resource (AD) box.

Password Plug-in:

The purpose of the password plug-in is to capture the password changes on the Active Directory and store it in encrypted form in Active Directory itself so that it can be picked up during next Polling by the connector. This agent only updates Active Directory and does not directly interact with SI web service. The password plug-in is optional and if it is not installed, password changes won't be reconciled to OVSI.

Mini Agent: (Group Reconciliation):

The purpose of the mini agent is to allow reconciliation of entitlement changesfor a user. This agent only updates Active Directory and does not directly interact with OVSI web service. The mini agent is optional and if it is not installed, entitlement changes for a user will not be reconciled to OVSI, but the changes in any other attribute will be picked up the Connector in the succeeding cycles.

2 Installing the Connector

Active Directory connector is packaged with the following files.

Table 1 Active Directory Connector Files

Serial Number	File Name	Description
1.0	`ActiveDirConnector.rar`	It is the Resource Adapter Archive (RAR) file of the connector. It contains binaries, implementation related Java class files, third party JAR files, and Active Directory property files.
2.0	`ActiveDirSchema.jar`	It contains the `ActiveDir.xml` file, which maps attributes from Active Directory to OVSI. It also contains configuration files – `ActiveDirParamResources.properties` and `ActiveDirConfig.properties`.
3.0	`AD_Password_Plugin.zip`	It contains the files required to install password synchronization plug-in, which are: • `ADProperties.ini` • `ADPassfilt.dll` • `libeay32.dll` • `libssl32.dll`
4.0	`KeyGenUtility.zip`	This file contains the keygen utility.
5.0	`cbc_config.zip`	It contains the DDL files to configure the database to block cyclic request.
6.0	`TLNotify.exe`	This is the mini agent file.

These files are located in the `ActiveDirectory_ELDAP` directory on the Select Identity Connector CD.

System Requirements

The Active Directory connector is supported in the following environment:

Table 2 Platform Matrix for Active Directory connector

Select Identity Version	Application Server	Database
3.3.1	WebLogic 8.1.4 on RedHat Enterprise Linux AS Release 3.0	Oracle 10g
	WebLogic 8.1.4 on Windows 2003 Server.	MS SQL 2000
4.0	The Active Directory connector is supported on all the platform configurations of Select Identity 4.0	

Configurable Parameters

The `ActiveDirConfig.properties` file, which is present in the `ActiveDirSchema.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, Active Directory Connector uses modify/add and modify/delete operations to support multivalued attribute. When it is set to true, Active Directory 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 OVSI.

- `attribute-ends=]]`

  End parameter to wrap the special base64 encoded attribute values while sending to connector from OVSI.

- `dualLink-support=2`

  This specifies whether a Link is a User Link or a Group Link. If it is 1, then it is a User Link. If it is 2, then it is a Group Link.

- `multivalue-support=false`

  This specifies whether SI supports multivalued attributes or not. This property is used in the reverse provisioning, when a mutlivalued attribute is detected in the replog during the polling, all the values of this multivalued attribute are combined as single valued string.

  If true - SI supports multivalued attributes.
  If false - SI 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.

- `Add PSSync_ATTRIBUTE=description`

  It must hold the name of Active Directory attribute, where encrypted password is stored.

Installation Procedure

Perform the following tasks to achieve successful installation of Active Directory connector.

1. Configure the Database on OVSI system
2. Install Password Synchronization Plug-In on Resource
3. Install Certificate on Application Server
4. Deploy the Connector on Application Server
5. Extract the Contents of Schema File
6. Configure the Connector with OVSI
7. Configure Workflow External Call on OVSI

Configure the Database on OVSI system

This is a bidirectional connector. At the time of forward provisioning, it tends to send reconciliation request to OVSI from the resource. This is called cyclic request. To block the cyclic request, perform the following steps on the database for OVSI.

1. Create a new table on OVSI database.
2. Execute the DDL file (`mssql_cbc_ddl.sql` for MS SQL database or `Oracle_cbc_ddl.sql` for Oracle database), which are available in `cbc_config.zip`.
3. Create a Connection Pool by using Oracle or MSSQL in Application Server.
4. Configure a new JDBC Data Source, and use the Connection Pool created above.
5. Add/Modify two parameters in `Config.properties` file

   `CBCDatasource-JNDIName=jdbc/LdapAD`

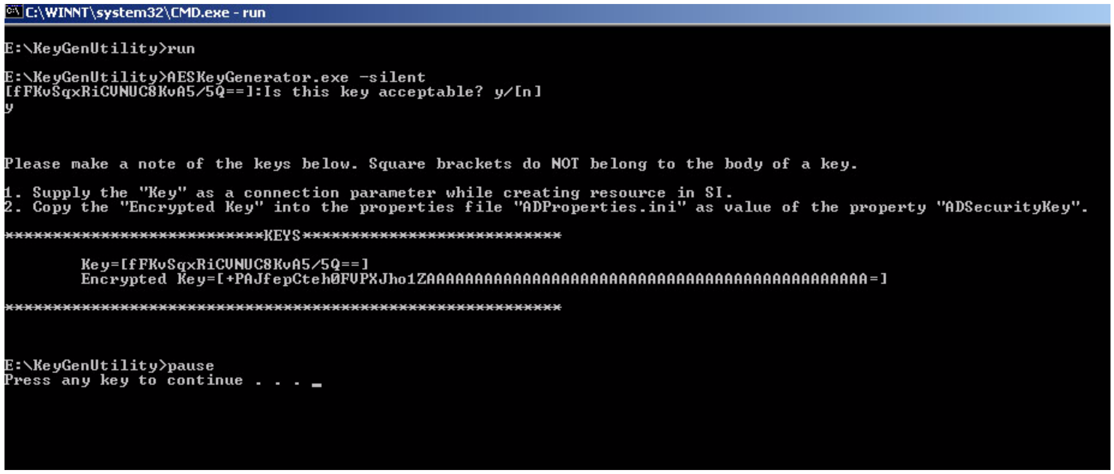
   `CBCDatasource-Repository=`*database name*
   where database name can be oracle or MsSQL depending on type of the database.

   CBCDatasource-JNDIName of JDBC Data Source.

Install Password Synchronization Plug-In on Resource

You must install server specific plug-ins on the Active Directory resource system. It is avilable in `AD_Password_Plugin.zip`. Perform the following steps to install it.

1. Execute the `KeyGenUtility` to generate `Key` and `Encrypted Key`. Perform the following steps to execute it.
   a. Extract `KeyGenUtility.zip`.
   b. To run the utility, open on command prompt the folder `KeyGenUtility` and type `run.cmd`. For verbose mode, run`Verbose.cmd` instead of `run.cmd`. In verbose mode, the utility generates more information, which is useful for debugging later on. The extra information is stored in a file and not shown on the console. Hence on console both modes appear almost the same.
   c. When executed, the utility shows a series of keys (one by one) and asks the user if the key currently shown is acceptable to the user. If user selects the key, the utility further shows result, which comprises of the key, its encryption key, and a helpful message on where each of the two keys has to go. The encrypted key has to be copied into the properties file of the agent `ADProperties.ini` as value of the property `ADSecurityKey`. The key is to be provided as a value of encryptionKey parameter while configuring resource parameter for connector.



In the above image, Key and Encrypted Key are the strings within the brackets.

2 Install password filter on resource machine. To do this, perform the following steps.

a Click **Start** → **Settings** → **Control Panel**. Control Panel window appears.

b Click **Administrative Tools** → **Domain Security Policy** →**Account Policies** → **Password Policy** → **Passwords must meet complexity requirements.**

c Copy the following files, to the location `<system root>\system32` on resource machine.

– `ADPassfilt.dll`

– `ADProperties.ini`

– `libeay32.dll`(this is a password encrytion dll file, supplied by OpenSSL)

– `libssl32.dll` (this is a password encrytion dll file, supplied by OpenSSL)

d Verify if `ADProperties.ini` has the properties as mentioned below. Make changes if necessary. The properties are:

– `PSLog_Path`: The folder name (not filename) under which log file is created

– `PSSync_Password_Suffix`: Suffix on the directory where user entry is located. (For example, DC=openview2k3,DC=hp,DC=co,DC=in)

– `PSSync_Server_Name`: Name of the Active directory server (For example, 2k3ps2227.openview2k3.hp.co.in)

– `PSSync_Server_Port`: Server port for Active directory service (For example 389)

– `PSSync_Admin_Dn`: Name of administrator user on Active Directory (For example, Administrator@DomainName)

– `PSSync_Admin_Password`: Password of administrator user on Active Directory in encrypted format. To encrypt the password for Active Directory admin user, copy `PasswordEncryptionUtility.exe` provided with the zip file to a folder, and run `PasswordEncryptionUtility` *`<admin_password>`* from that location by using command prompt.

– `PSSync_ATTRIBUTE`: Name of the user attribute where user will store encrypted password value in the Active Directory. The field which are mentioned should have the capacity of holding more than 180 characters. Otherwise AD will not be able to hold the encrypted password.

– ADSecurityKey: Encrypted key generated by the KeyGenUtility.

A sample ADProperties.ini looks like the following texts.

```
PSLog_Path=C:\ADPasswordLogs
PSSync_Password_Suffix=DC=si,DC=hp,DC=com
PSSync_Server_Name=sint22.si.hp.com
PSSync_Server_Port=389
PSSync_Admin_Dn=Administrator@si.hp.com
PSSync_Admin_Password=aLpdS+aoGv5YuLp6MlbIudFeySx5ofxC6FsrzT8TPS+FccvH
u+EcQr44pSErKzooh9CI2zsFblDU5k0LNfdkLVwKLX36nc9dWgxYoKEqdGQE9AraG4JjN+
TglPgPGivv8t4xwqvdMGC5ZHl7SiAzt+pAuGWJzuoVOz5mGtsC4WE=
PSSync_ATTRIBUTE=description
PSSync_Modifier_Name=admin123
ADSecurityKey=ivmoNHPzD0Ds9WdTuZi4dwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAA=
```

Make sure that the path mentioned for the property PSLog_Path is available.

e Open the Registry Editor (regedit.exe) and locate the following registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

f Modify the Notification Packages multi-string value of the above key and add your Password Filter file name (ADPassfilt) without the .dll extension.

g Close Registry Editor and restart your machine.

3 Perform the following steps on OVSI system, where connector is being installed.

a Modify PSSync_ATTRIBUTE property of ActiveDirConfig.properties file. Set the this attribute as the name, which was mentioned in the ADProperties.ini file.

b Restart the application server.

Install Mini Agent

The mini agent detects the link/unlink operations for a user and it changes the uSNChanged attribute for that user by modifying the value of a dummy attribute with the same value.

Perform the following steps to deploy the mini agent on resource system.

1 Copy TLNotify.exe file to the location <*system root*>\system32 on resource machine. ADProperties.ini file must also be present at <*system root*>\system32.

2 Set the parameters PSSync_ATTRIBUTE and PSSync_Modifier_Name in ADProperties.ini file as described below.:

PSSync_ATTRIBUTE: The Name of an AD attribute having only string value. This is used to modify the uSNChanged attribute for that user by modifying the value of a dummy attribute given in the ADProperties.ini file (PSSync_ATTRIBUTE) with the same value.

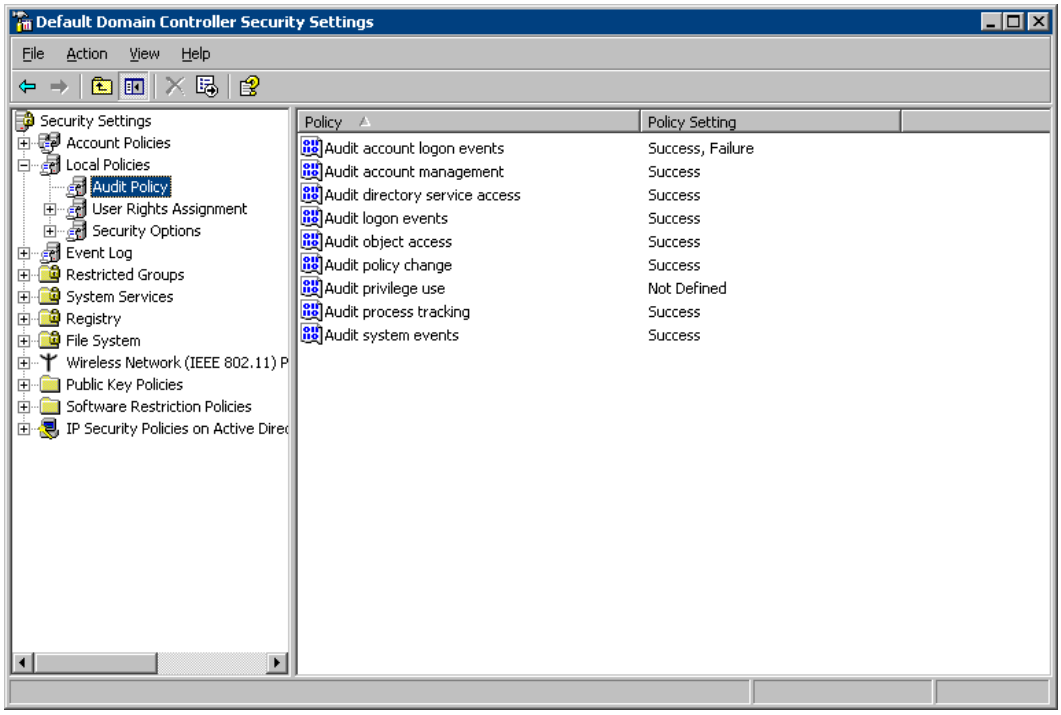
PSSync_Modifier_Name: Create a new user ID on Active Directory with administration privilege, and provide that name as attribute value of PSSync_Modifier_Name. This helps Active Directory block cyclic requests. You must not log in to Active Directory by using this newly created user ID.

For example:

```
PSSync_ATTRIBUTE=description
PSSync_Modifier_Name=admin123
```

The agent blocks the detection of any link/unlink operation if `PSSync_Modifier_Name=Administrator`.

3 Set the security event settings, at the location **Start** → **Settings** →**Control Panel** → **Administrative Tools** →**Default Domain Controller Security Policy**, to detect the changes on Active Directory as shown in the following screen shot:

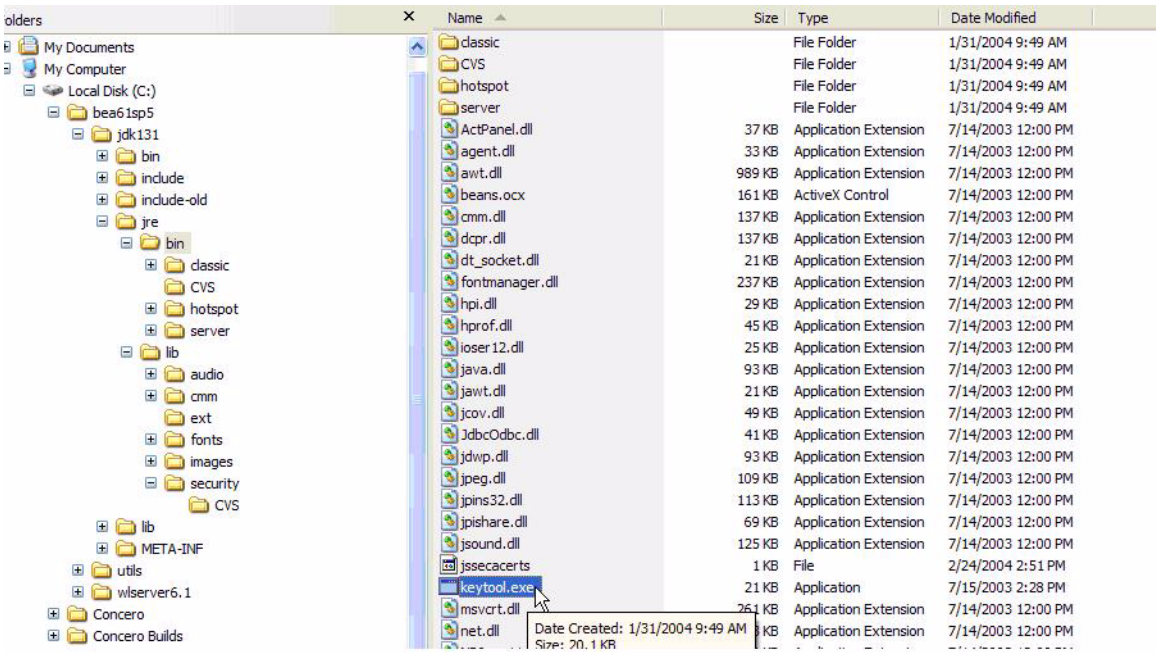


4 Start the mini-agent by double-clicking the `TLNotify.exe`.

5 You can verify if the event logs are getting generated at the location **My Computer** →**Manage**→**Event Viewer**.

Install Certificate on Application Server

Before installing the Active Directory certificate on application server, verify if `keytool.exe` is available. To verify, go to Java home of application server's home directory, and locate the file `keytool.exe` in `jre\bin` subdirectory. If OVSI 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 Active Directory certificate.

1 Copy the Active Directory certificate file (`<certificate-name>.cer`) to OVSI 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.trulogica.com, OU=QA, O="TruLogica, Inc.", L=Plano, ST=TX,
C=US, EmailAddress=qa@trulogica.com
Issuer: CN=QA.trulogica.com, OU=QA, O="TruLogica, Inc.", L=Plano, ST=TX,
C=US, EmailAddress=qa@trulogica.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 this file because there is already a `jssecacerts` file in the security folder that needs to be overridden by this one.

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
```

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

Extract the Contents of Schema File

Create a subdirectory in the OVSI home directory on OVSI system. Extract the contents of `ActiveDirSchema.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 (`ActiveDirConnector.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 Select Identity. 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/ActiveDirConnector`**
   - Under Mapper Available section, select **Yes.**
2. Add a new resource – You must add a new resource to OVSI that uses the newly added connector. Refer to *HP OpenView Select Identity Connector Deployment Guide* for the instruction to add a new resource to OVSI. While entering the resource parameters for Active Directory connector, refer to the table below.

Table 3 Resource Configuration Parameters

Field Name	Sample Values	Description
Resource Name	*ELDAPAD*	Name given to the resource.
Access URL	*ldaps://sidc:636*	Resource connection URL - IP:port Before using ldaps , the trusted root certificate has to be downloaded for Active Directory machine and imported to the weblogic keystore.
Suffix	*DC=sis,DC=com*	Default root suffix.
Login Name	*CN=Administrator, CN=Users,DC=sis, DC=com*	Admin User Login Name.
Password	*ADPASSWORD*	Password of the admin user.
Default User Suffix	*CN=Users*	Suffix where all users exist.
passPluginSuffix	*DC=sis,Dc=com*	Password Plug-in Suffix, where te encrypted password will stored for reconciliation
Default Group Suffix	*CN=Builtin*	Suffix where all groups exist.
Mapping File	`ActiveDir.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.

Table 3 Resource Configuration Parameters

Field Name	Sample Values	Description
GCAccess URL:	*ldap://openview2k:3268*	This is not a mandatory field. This URL if specified will be used for Global Catalog Search operations. If the GC Access URL is not known, please leave it empty.
SI Locale	*en_US*	Locale-specific information. If Country = US and Language = English, current locale string is en_US.
encryptionKey	*6PqwwkfRTxaEJgW/cFuIUA==*	Copy the key generated by KeyGenUtility

Configuring Polling for Reverse Synchronization:

After entering the resource access information, User Reconciliation Policy page appears. On this page, do the following.

a. Check the Polling Enable checkbox. Set the polling interval as one hour.

b. Under both Add and Modify sections, set Reconciliation Workflow as SI Recon User Enable Disable Workflow by using the drop-down box.

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 Mapping Information

Select Identity Resource Attribute	Connector Attribute	Attribute on Active Directory	Description
Street	streetAddress	streetAddress	
PhHome	homePhone	homePhone	
Email	Mail	mail	
PhMobile	mobile	mobile	
UserName	sAMAccountName	sAMAccountName	*This attribute is mandatory for user creation.*
CN	cn	Cn	*This attribute is mandatory for user creation.*
Zip	postalCode	postalCode	
PhBus	telephoneNumber	telephoneNumber	
Password	unicodePwd	unicodePwd	*This attribute is mandatory for user creation.*

Table 4 Active Directory Mapping Information

Select Identity Resource Attribute	Connector Attribute	Attribute on Active Directory	Description
Title	title	title	
DisplayName	displayName	displayName	
LastName	sn	Sn	*This attribute is mandatory for user creation.*
ObjectGUID	objectGUID	objectGUID	While associating Active Directory resource to a service, do not add this attribute to the service.
Groups	memberOf	memberOf	
FirstName	givenName	givenName	
UserPrincipalName	userPrincipalName	userPrincipalName	
State	st	St	
Usersuffix	userSuffix	userSuffix	
City	l	L	
POBox	postOfficeBox	postOfficeBox	
userAccount Control	userAccount Control	userAccount Control	While associating Active Directory resource to a service, do not add this attribute to the service.

Map the following attributes, if you want to provision users in Exchange mailbox.

Table 4A Exchange Mapping Information

Select Identity Resource Attribute	Connector Attribute	Attribute on Active Directory	Description
Email	Mail	mail	
MailBoxStore	homeMDB	homeMDB	
mailNickName	mailNickname	mailNickname	

Table 4A Exchange Mapping Information

Select Identity Resource Attribute	Connector Attribute	Attribute on Active Directory	Description
AlternateRecipient	altRecipient	altRecipient	
HomeDirectory	homeDirectory	homeDirectory	
AddressBook	showInAddressBook	showInAddressBook	

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

Configure Workflow External Call on OVSI

To achieve reverse synchronization, you must configure the workflow external call for user enable/ disable operation for Active Directory connector. Refer to *HP OpenView Select Identity Deployment Guide* for information on configuring user enable/disable workflow external call. While configuring, enter the parameters as given in Table 5 below.

Table 5 User Enable/Disable Parameters for Active Directory Connector

Serial Number	Parameter Name	Parameter Value
1.0	AttributeName	userAccountControl
2.0	EnableValue	512
3.0	DisableValue	514
4.0	UserName	OVSI admin user name. For example, sisa.
5.0	Password	OVSI admin password. For example, abc123.
6.0	Url	SI webservice url. For example: http://localhost:7001/lmz/webservice

While entering these parameters, check the Sensitive checkbox only in the case of Password.

Configuring the Exchange Related Attributes

You can provision users in Exchange mailbox by using this connector. To be able to do that, you must map the exchange related attributes. These attributes are described below with example attribute values, which has to be entered during user provisioning.

- `Mail` — This is the Email Address for the user. For example, *user01@sitest.com*

- `homeMDB` — This is the ExchangeFolderDN and is a concatenation of several server values. For example, Example:

  CN=Mailbox Store (TLNT3),CN=First Storage Group,CN=InformationStore,CN=TLNT3,CN=Servers,CN=First Administrative Group,CN=Administrative Groups,CN=SITestOrg,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=sitest,DC=com

  This is a test DN. You must give an equivalent value.

- `mailNickname` – This nick name can be `User name` or `sAMAccountName`. For example:

  User01nick

  While adding user if you enter this value, email id of the user becomes - *User01nick@sitest.com*

- `altRecipient` — This is DN of any other User entry and used for forwarding mails from User01 to User02. For example, *CN=User02,CN=Users,DC=sitest,DC=com*.

  If you configure this attribute, then any mail that is sent to User01 will be forwarded to User02.

- `homeDirectory` — This is the virtual home folder. This is the location on which the Exchange User home directory will be stored. For example: *D:\temp*

  This folder is just shown as the User attribute and the folder is not created physically on the server.

- `showInAddressBook` — This is a concatenation of several server values. For example,

  CN=All Users,CN=All Address Lists,CN=Address Lists Container,CN=SITestOrg,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=sitest,DC=com|CN=Default Global Address List,CN=All Global Address Lists,CN=Address Lists Container,CN=SITestOrg,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=sitest,DC=com

  This is a test value, you must give an equivalent value.

3 Uninstalling the Connector

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

- Remove all resource dependencies.
- Delete the connector from the OVSI.
- Delete the connector from application server.
- Uninstall the mini agent from Active Directory resource. To uninstall the mini agent, perform the following steps.
  a. Go to the agent console and stop the mini agent by **Ctrl+C**.
  b. Delete the `TLNotify.exe` file.
  c. Delete the following files.
     - `ADProperties.ini`
     - `ADPassfilt.dll`
     - `libeay32.dll`
     - `libssl32.dll`

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

A Overview of Reverse Synchronization by Polling

Reverse synchronization in Active Directory connector is achieved by polling. Each time the polling is invoked, the following sequences take place in the background:

1. The polling batch task is invoked
2. The polling batch task converts all the ChangeLogs into an SPML files, and the SPML file is converted to a request using the SPML parser and submitted to the Select Identity Reconciliation engine. Then ReconcilationHelper is called to execute all the Modify Requests.
3. In the provisioning stage of request execution, Select Identity is updated with the changes in the resource.

On Select Identity, if Active Directory service view has some attributes as mandatory, all of them should exist on Active Directory server and they should be sent when reverse add request comes from connector. That is, the only attributes that are coming in reverse add request can be mandatory in Select Identity Service view, if it is mandatory in view and it does not come in reverse add request, request will be rejected by Select Identity.

B Troubleshooting

- While creating the user if the password is not set and an exception with `5003` code is thrown

  Solution:

  Verify whether the password sent to the user meets the password policy.

  For example, the default password policy should accept a password with 8 or 9 characters with atleast one uppercase and a numeric value (Password1).

- While creating and trying to save a resource, you get error `The following resource failed to save: Reason: Unable to test connector.`

  Solution:

  Verify the following config files are in the application server classpath while deploying the connector.

  — `com\trulogica\truaccess\connector\ldapv3\ActiveDirConfig.properties`

  — `com\trulogica\truaccess\connector\ldapv3\ActiveDirParamResources.properties`