HP OpenView Select Identity

Connector for Windows® Active Directory (Bidirectional LDAP Based)

Connector Version: 1.1

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

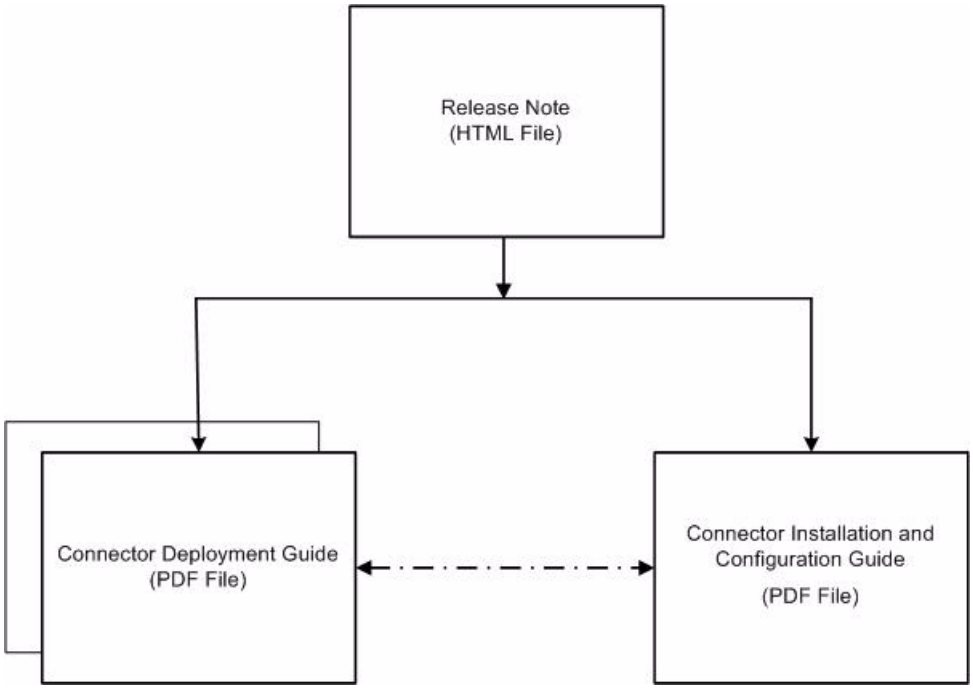


Table 1 Connector Documentation

Document Title and Filename	Contents	Location
Release Note `Active Directory Bidirectional LDAP Connector v1.1 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)
`connector_deploy_SI4.pdf`
Connector Deployment Guide (for Select Identity 3.3.1)
`connector_deploy_SI3.3.1.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 Bidirectional 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 Bidirectional LDAP Connector

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

- Add, update, and remove users

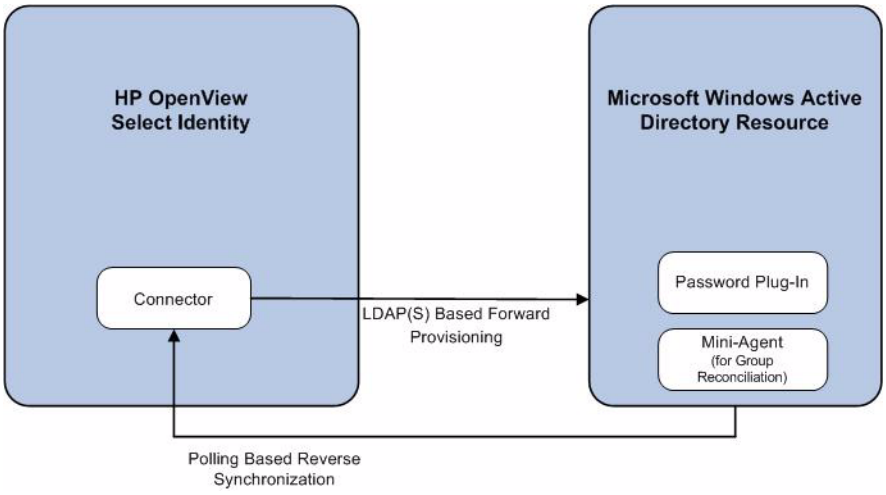
- Retrieve user attributes
- Enable and disable users
- Verify a user's existence
- Change user passwords
- Reset user passwords
- Expire user passwords
- Retrieve all entitlements
- Retrieve a list of supported user attributes
- Grant and revoke entitlements to and from users

High-Level Architecture

Figure 2 illustrates a high-level architecture of Active Directory Bidirectional LDAP connector. This 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 Select Identity. Select Identity periodically polls the Active Directory resource to retrieve changes through the connector.

Figure 2 High-Level Architecture of the Active Directory Bidirectional LDAP Connector



The connector also has two agents; a Password Plug-In for password reconciliation and a Mini-Agent for group reconciliation which resides on the resource (Active Directory).

This connector can be used with Select Identity 4.01.000, 4.0, and 3.3.1.

Password Plug-In

The Password Plug-In captures the password changes in Active Directory and stores the changed password in encrypted form on Active Directory system. The change is picked up by the connector during next polling operation. This agent only updates Active Directory and does not directly interact with Select Identity web service. The Password Plug-In is optional and if it is not installed, password changes will not be reconciled to Select Identity.

Mini-Agent

The Mini-Agent enables reconciliation of entitlement changes for a user. Like Password Plug-In, this agent also updates Active Directory and does not directly interact with Select Identity web service. If the Mini-Agent is not installed, entitlement changes for a user will not be reconciled to Select Identity, but the changes in any other attribute will be picked up the connector in the succeeding polling cycles.

Overview of Installation Tasks

Before you start installing the connector, you must ensure that system requirements and all the installation prerequisites are met. Refer to the Table 2 for an overview of installation tasks.

Table 2 Organization of Tasks

Task Number	Task Name	Reference
1	Install the connector on the Select Identity server.	See Installing the Connector on page 13.
	— Meet the system requirements.	See System Requirements on page 14.
	— Perform the pre-installation task: Install Active Directory certificate on the application server hosting Select Identity.	See Pre-Installation Task on page 14.
	— Extract contents of the Schema file (file that contains the mapping files for the connector) to a location on the Select Identity server.	See Extracting Contents of the Schema File on page 18.
	— Verify configurable parameters in the `ActiveDirconfig.properties` file.	See Verifying Configurable Parameters on page 18.
	— Install the Resource Adapter Archive (RAR) of the connector on an application server.	See Installing the Connector RAR on page 19.
	— Configure Select Identity database to block cyclic request.	See Configuring the Database on Select Identity System on page 20.

Table 2 Organization of Tasks

Task Number	Task Name	Reference
2	Installing agent modules for Active Directory Bidirectional LDAP connector.	See Installing Agents on page 21.
3	Configure the connector with the Select Identity server.	See Configuring the Connector with Select Identity on page 29.
	— Add a new connector to Select Identity.	See Add a New Connector on page 29.
	— Add a new resource to Select Identity.	See Add a New Resource on page 29.
	— Map Active Directory attributes to Select Identity attributes.	See Map Attributes on page 31.
	— Configure Workflow External Call.	See Configure Workflow External Call on Select Identity on page 33.
	— Configure polling on Select Identity 3.3.1 (Perform this task only if you install the connector on Select Identity 3.3.1.	See Configure Polling for Reverse Provisioning on Select Identity 3.3.1 on page 34.

3 Installing the Connector

This chapter elaborates the procedure to install Active Directory Bidirectional 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 Bidirectional LDAP connector.
- Prerequisite conditions to install Active Directory Bidirectional LDAP connector.
- Procedure to install Active Directory Bidirectional LDAP connector.

Active Directory Bidirectional LDAP Connector Files

The Active Directory Bidirectional LDAP connector is packaged in the following files, which are located in the `Bidirectional LDAP Connector - Active Directory` folder on the Select Identity Connector CD:

Table 3 Active Directory Bidirectional LDAP Connector Files

Serial Number	File Name	Description
1	`ActiveDirConnector.rar`	It contains the binaries for the connector.
2	`ActiveDirSchema.jar`	It contains the mapping file (`ActiveDir.xml`), which control how Select Identity fields are mapped to Active Directory fields. It also contains the following properties files: `ActiveDirConfig.properties`
3	`OpenSSLDLL.zip`	It contains the dll files: • `libeay32.dll` • `libssl32.dll`
4	`cbc_config.zip`	It contains the DDL files to configure the database to block cyclic request.
5	`MiniAgent_Password_Installer.zip`	It contains the installation executable for the agent.

System Requirements

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

Table 4 Platform Matrix for Active Directory Bidirectional LDAP Connector

Select Identity Version	Application Server and Operating System	Database
3.3.1	WebLogic 8.1.4 on Windows 2003 Server.	Microsoft SQL 2000
	WebSphere 5.1.1.7 on Windows 2003	Oracle 9i
4.0/4.01.000	The Active Directory Bidirectional LDAP connector is supported on all the platform configurations of Select Identity 4.0 and 4.01.000.	

The Active Directory Bidirectional LDAP connector is supported on Microsoft Windows Server 2000 and Microsoft Windows Server 2003 with Service Pack 1.

Pre-Installation Task

To provision users directly to LDAP store, the connector must communicate with the Active Directory resource over a secure channel (LDAPS). To enable a secure communication between the connector and Active Directory, you must perform the following tasks:

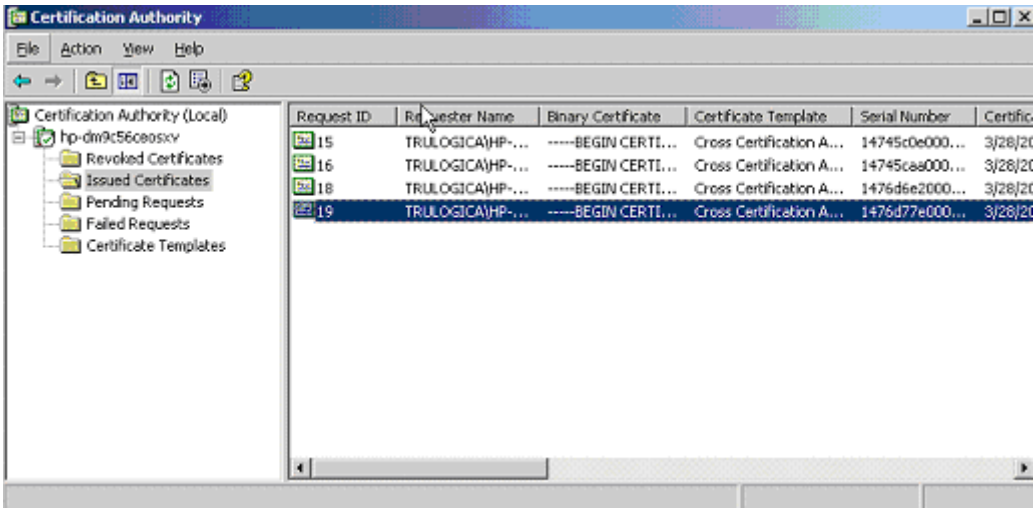
- Generate a root CA certificate on Active Directory server.
- Deploy the certificate with keystore.

Generate Root CA Certificate on Active Directory

Perform the following steps to generate a Root CA Certificate on Active Directory:

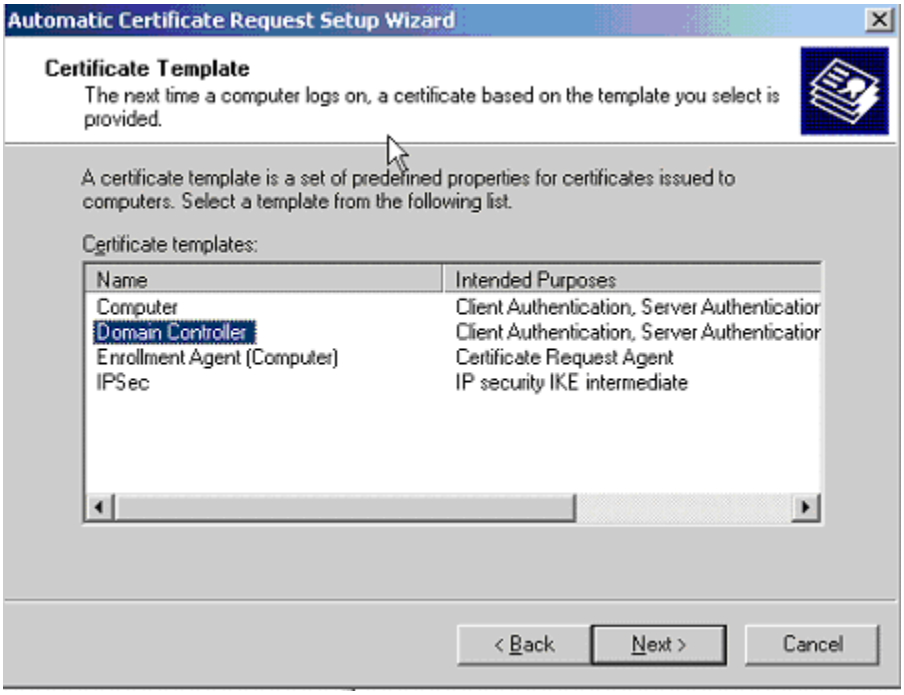
1. Install the Certificate Services Component from the Windows CD.
2. Configure HTTPS on the system.

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:

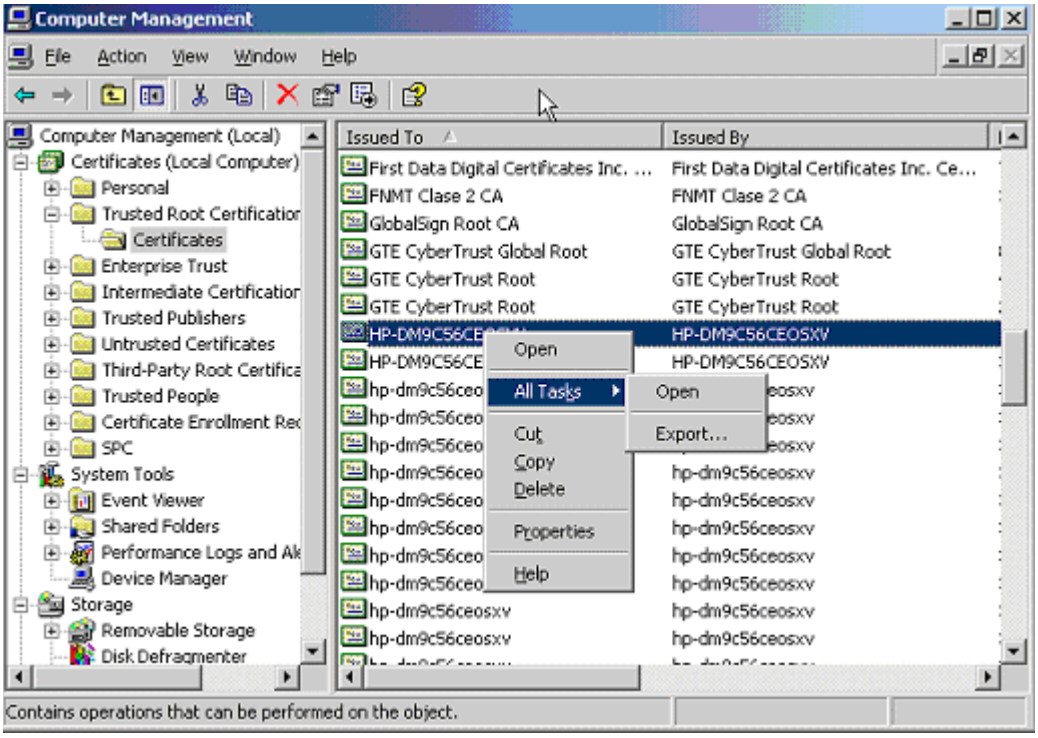


4 Create an Automatic Certificate Request (from **Administrative Tools → Domain Controller Security Policy → Public Key Policies**).

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 (by 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

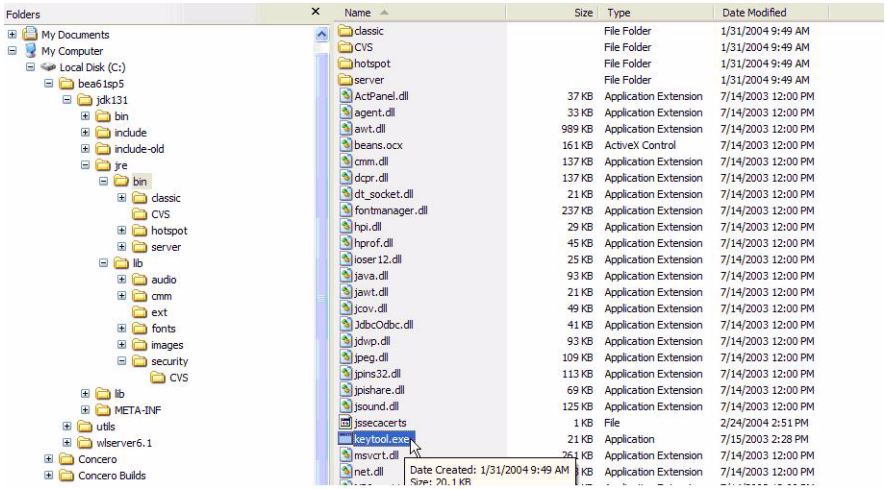
Specify the login credentials for the Active Directory server when prompted. You must download the certificate to the <*Application Server Java Home*>`\jre\lib\security` directory.

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

Deploy the Certificate with Keystore

Perform the following steps to deploy the certificate:

1 Go to the Java home of the application server and verify if the `keytool.exe` file is available in <*Application Server Java Home*>`/jre/bin` subdirectory. If Select Identity is installed on Windows, you can locate the file at <*Application Server Java Home*>`/jre/bin` by using Windows explorer.



2 Make sure that the Active Directory certificate file (<*certificate-name*>`.cer`) resides in the location <*Application Server Java Home*>`\jre\lib\security` on the Select Identity system.

> You must copy the certificate to the location <*Application Server Java Home*>`\jre\lib\security` on all the application servers for cluster setup.

3 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>`**.

4 When prompted for password, enter keystore password as **`changeit`**.

5 The keytool displays the following message:

```
Owner: CN=QA.hp.com, OU=QA, O="hp", L=abc, ST=xyz, C=mno,
EmailAddress=qa@hp.com
Issuer: CN=QA.hp.com, OU=QA, O="hp", L=abc, ST=xyz, C=mno,
EmailAddress=qa@hp.com
Serial number: 16bab38264ebda84f8011cf35d0ca6a
Valid from: Fri Jan 23 13:42:18 CST 2004 until: Fri Jan 23 13:50:22 CST
2009
Certificate fingerprints:
MD5:  60:72:A9:DD:C4:39:C4:8A:E7:42:56:0B:9E:5D:91:DB
SHA1: 38:D2:7F:33:FE:0A:AC:F3:D3:A0:2C:0F:A9:0C:6A:09:10:B5:EA:66
```

6 If the system displays `Trust this certificate? [no]:`, enter **`yes`**. The keytool displays the following message:

```
Certificate was added to keystore
[Saving jssecacerts]
```

7 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.

8 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*.

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

Verifying Configurable Parameters

The `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 Bidirectional LDAP Connector uses modify/add and modify/delete operations to support multivalued attribute. When it is set to true, Active Directory Bidirectional LDAP Connector uses modify/replace operation to support multivalued attribute.

- `attributeValue-delimiter=|`

  It contains the string delimiter that is used to separate attribute values for multi valued attribute.

- `attribute-begins=[[`

  Begin parameter to wrap the special base64 encoded attribute values while sending to connector from Select Identity.

- `attribute-ends=]]`

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

- `dualLink-support=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 Select Identity 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 - Select Identity supports multivalued attributes.
  If false - Select Identity does not support multivalued attributes.

- `unlink-before-terminate=false`

  If you want to unlink the entitlements while performing a terminate user operation, set this flag to false.

- `Add PSSync_ATTRIBUTE=description`

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

- `null-entitlement-support=true`

  Set this parameters to `true` for Select Identity 4.0/4.01.000 and to `false` for Select Identity 3.3.1.

Installing the Connector RAR

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

Configuring the Database on Select Identity System

The Active Directory Bidirectional LDAP connector supports both forward provisioning and change detection. When a forward operation is performed on the resource, the next polling cycle of the connector may detect the operation as if it was performed directly on the Active Directory system. This is called cyclic request. To block any cyclic request, you must configure the database of Select Identity.

Perform the following steps to block cyclic request.

1. Create a new table on Select Identity database.
2. Execute the DDL file (`mssql_cbc_ddl.sql` for Microsoft 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 Microsoft SQL in Application Server.
4. Configure a new JDBC Data Source, and use the Connection Pool created above.
5. Add/Modify two parameters in `ActiveDirConfig.properties` file

   `CBCDatasource` — `JNDIName=jdbc/LdapAD`
   This is the JNDI name of JDBC Data Source.

   `CBCDatasource` — `Repository=`*database name*
   where database name can be Oracle or Microsoft SQL depending on type of the database.

4 Installing Agents

This chapter gives an overview of agents for Active Directory Bidirectional LDAP connector and the procedure to install these agents on an Active Directory server. At the end of the chapter, you will be able to know about:

- The role of an agent.
- The procedure to install the agent.

About Agents

The Active Directory Bidirectional LDAP connector is packaged with two agent modules—Password Plug-In and Mini-Agent. The Password Plug-In detects any change in password on the Active Directory system. The Mini-Agent detects entitlement changes of users on Active Directory. You can install the agent modules on the Active Directory server by using the agent installation wizard.

Installing Password Plug-In and Mini-Agent

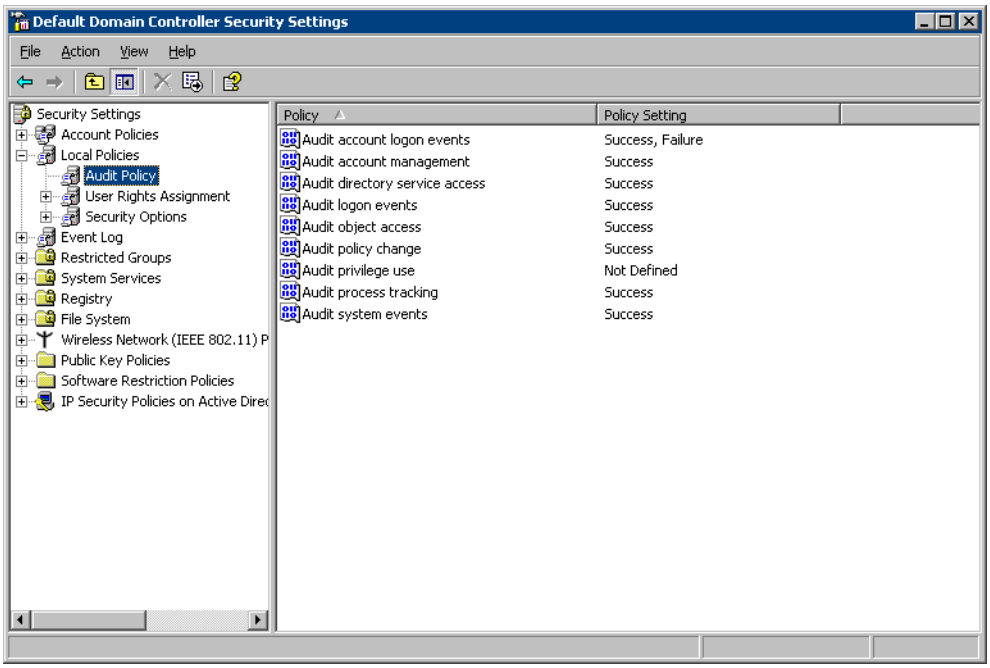
You can install the agent modules on the Active Directory server by using the agent installation wizard.

Pre-Installation Tasks

Before you start the installer, perform these steps.

1. Extract the contents of `OpenSSLDLL.zip` file and copy them to <*system root*>`\system 32` on resource machine. The contents of this file are:
   - `libeay32.dll`
   - `libssl32.dll`

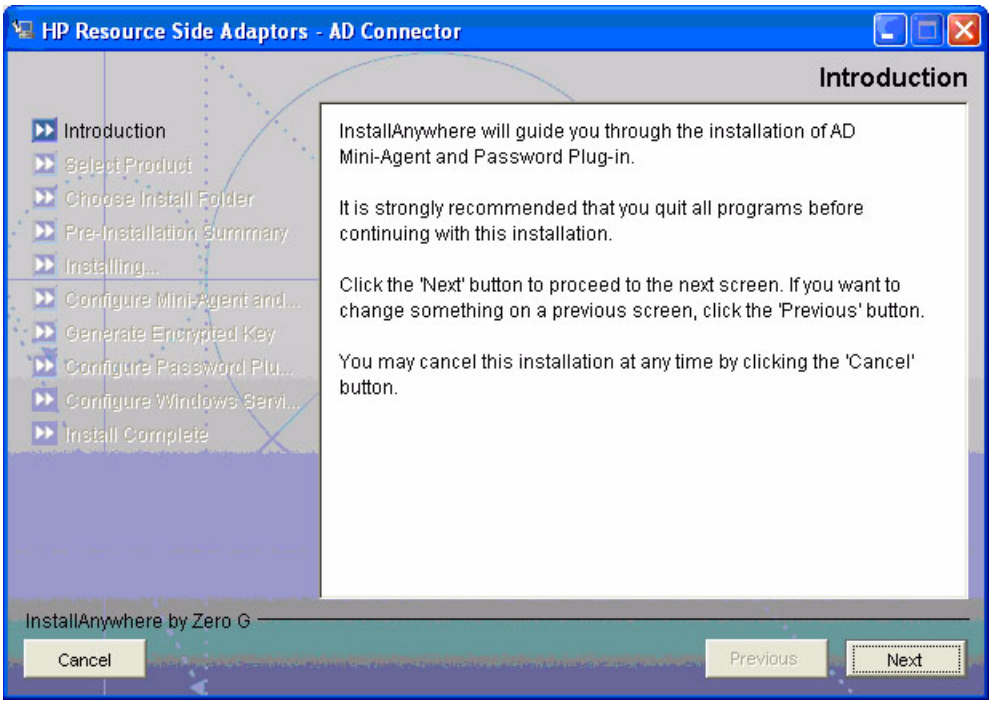
   these are password encryption dll files, supplied by OpenSSL.
2. Create a new user, for example, Admin1234 at the resource. This user must have administrator privileges.
3. Extract the contents of the file `MiniAgent_Password_Installer.zip` to a local directory (*<Installer Dir>)* on the Active Directory system. The automatic installer program `setup.exe` is stored in *<Installer Dir>*`\Disk1\InstData\NoVM`.
4. 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 image below:



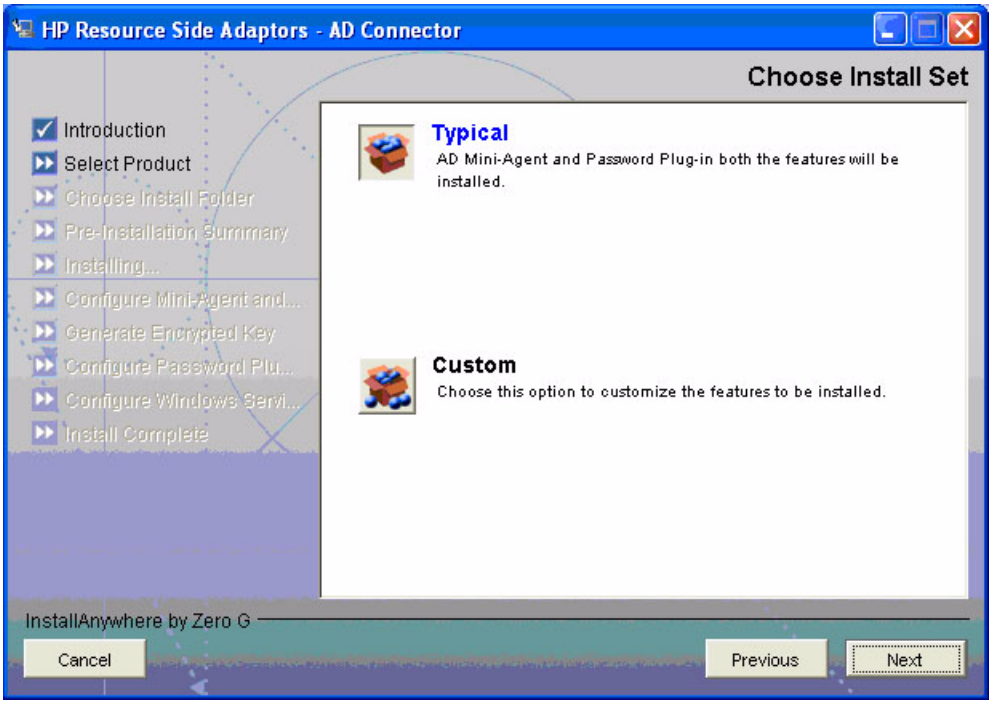
Installation Procedure

Perform the following steps to install mini agent and password plug-in with the help of the wizard:.

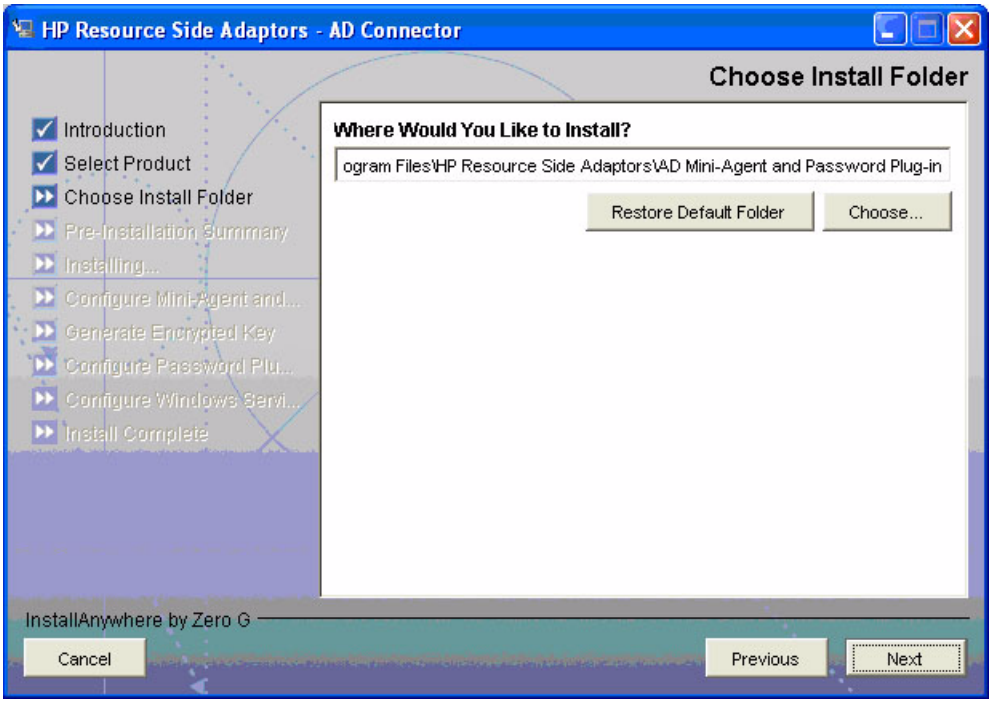
1 Run the file `setup.exe`, which is placed in the location <*Installer Dir*>`\Disk1\InstData\NoVM` on resource system. The installation wizard appears.



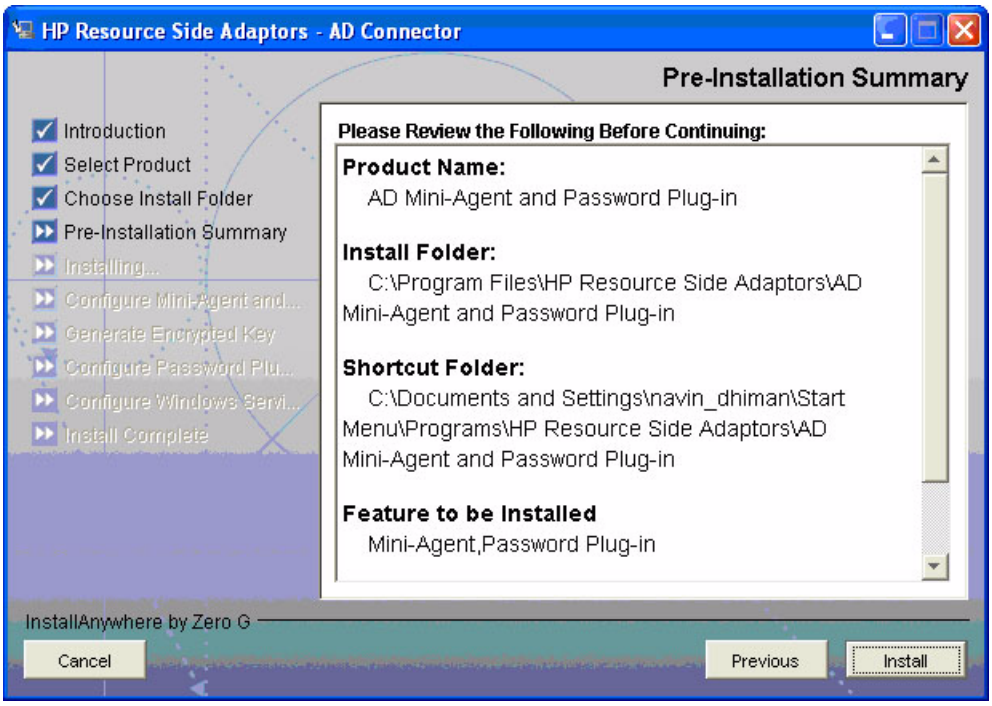
2 Click **Next** to begin installation. Choose Install Set screen appears.



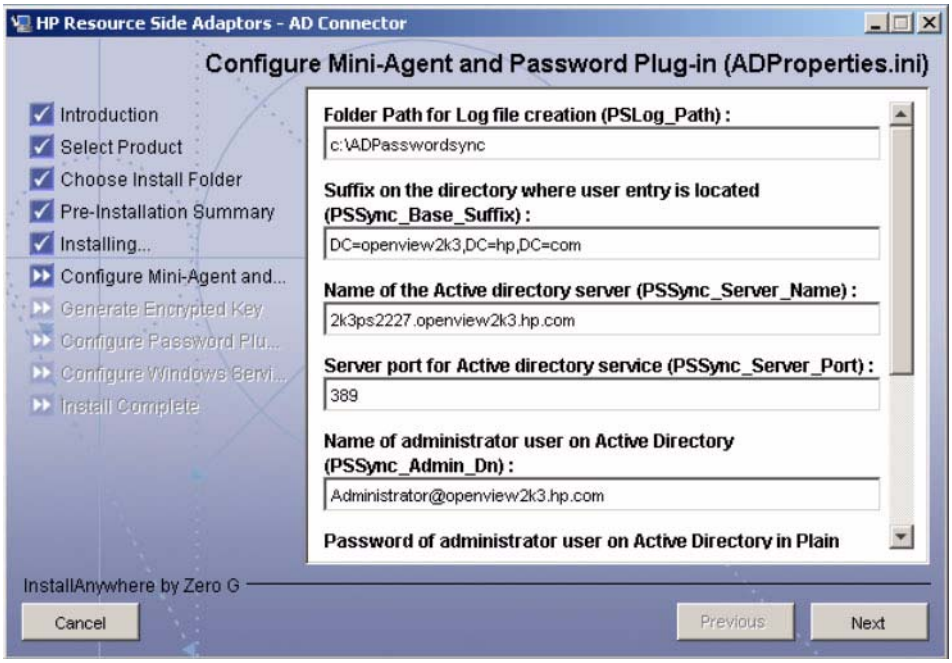
3 Choose Typical install set, and then click **Next**. Choose Install Folder screen appears. If you select Custom, installer gives you the option to install either mini agent or password plug-in.

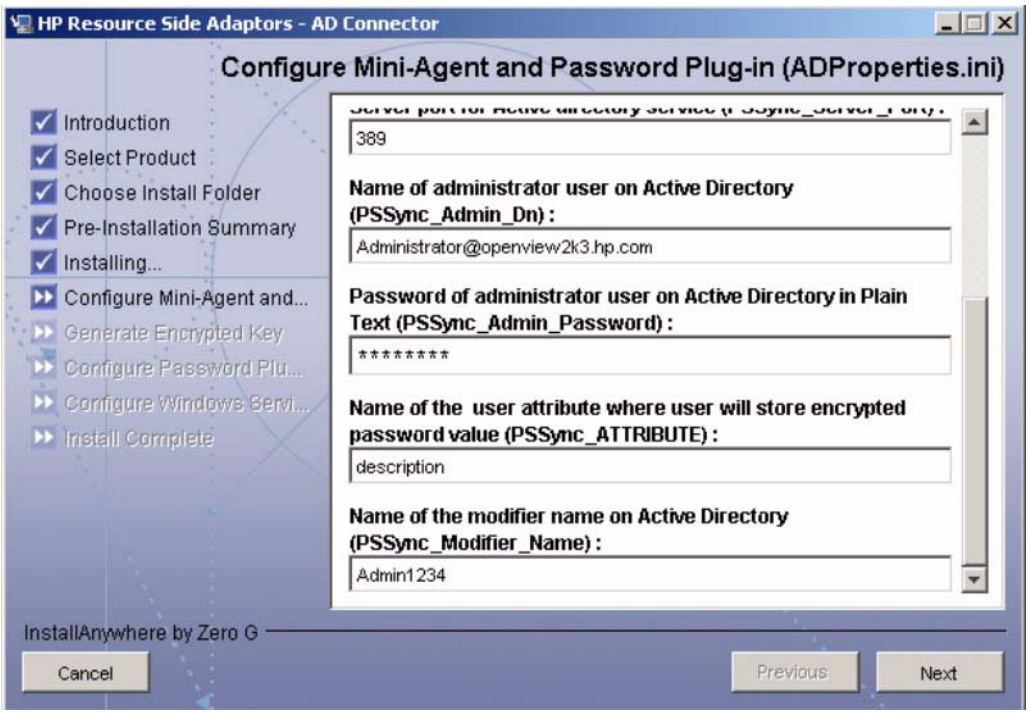


4 Specify the location for mini agent and password plug-in, and then click **Next**. Pre-Installation Summary screen appears.



5 Review the summary and click **Install** to beign installation. The Configure Mini-Agent and Password Plug-in (ADProperties.ini) screen appears.





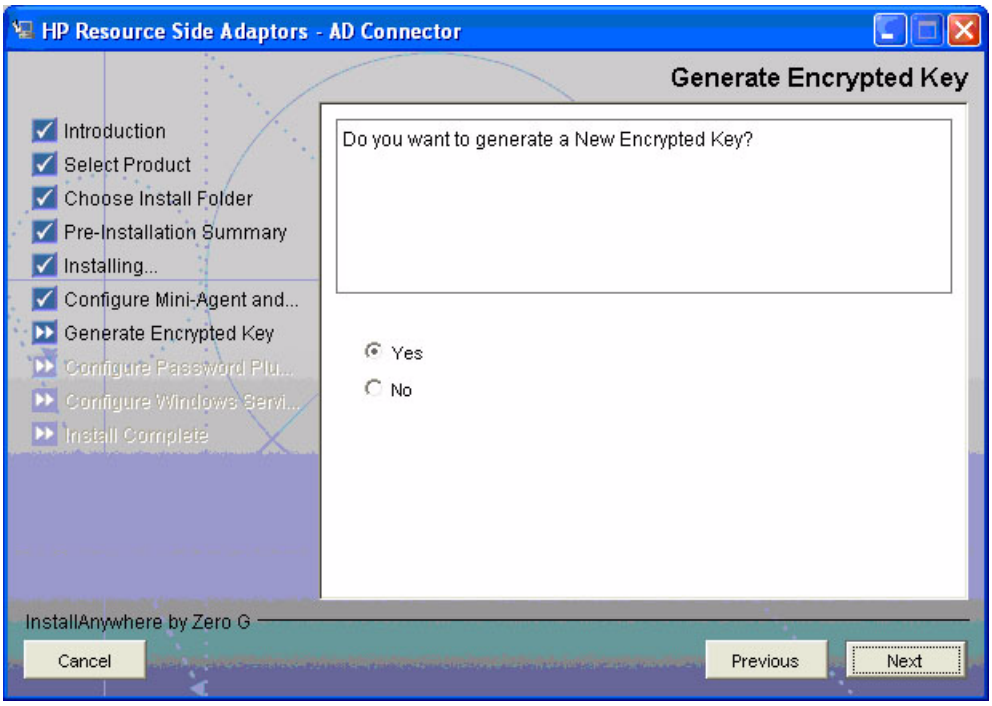
In the text fields, you must enter the following parameters.

- `PSLog_Path`: The folder name (not filename) under which log file is created. Mention an existing location of Active Directory server in this field, or create a new folder in Active Directory server and enter the path of the newly created folder.
- `PSSync_Base_Suffix`: This is the base suffix on Active Directory where user entries are located. (For example, DC = openview2k3, DC= hp, DC = com)
- `PSSync_Server_Name`: Name of the Active directory server (For example, 2k3ps2227.openview2k3.hp.com)
- `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.
- `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. For example, `description` attribute in Active Directory.

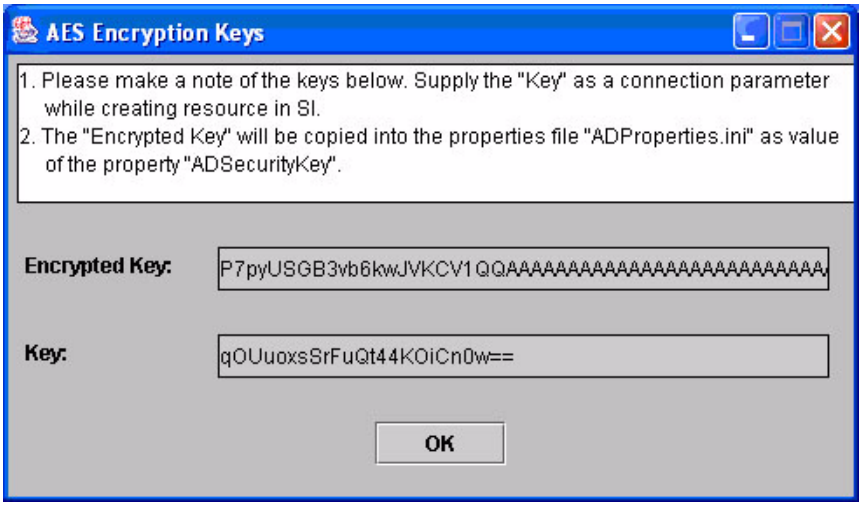
This is a sensitive attribute containing user's encrypted password. It is highly recommended to choose an attribute that is not used by any application and is not easily visible or available. Extending the Active Directory schema for this additional attribute is a good way to make this attribute obscure.

– `PSSync_Modifier_Name`: The newly created user on Active Directory with administration privilege (created in step 2 on page 21), 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.

6 Click **Next**. Generate Encrypted Key screen appears.



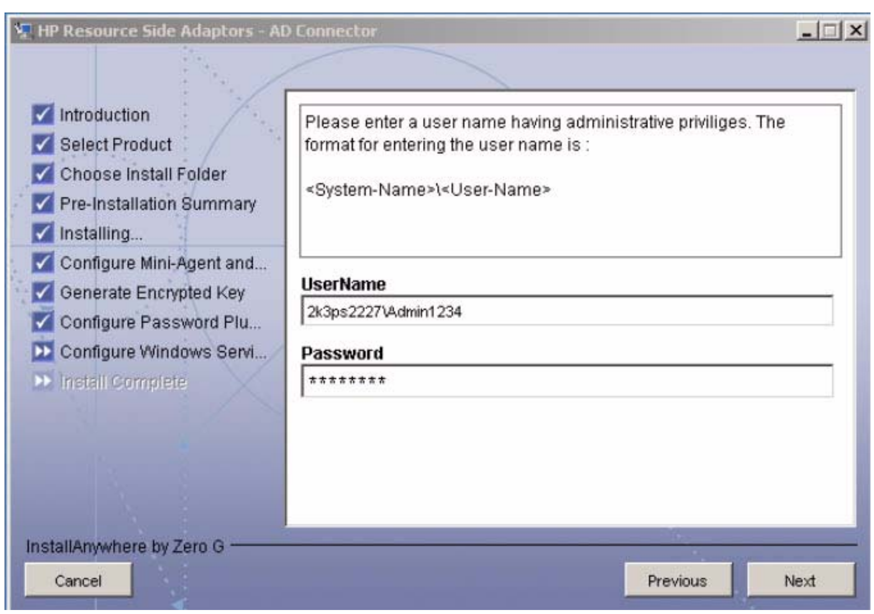
7 Check the Yes radio button and click **Next**. AES Encryption Keys popup appears.



➤ Note down the value in Key field. You must supply this value against Ecryption Key field while entering resource access information parameters in Select Identity.

8 Configure Password Plug-in screen appears.

9 Enter the `PSSYnc_Password_Suffix` as suffix on the directory where user entry is located. (For example, DC=openview2k3,DC=hp,DC=com), and then click **Next**.



10 Enter a username with administrative privilege and corresponding password, and then click **Next**.

11 Restart the machine after installation.

5 Configuring the Connector with Select Identity

This chapter describes the procedure to configure the Active Directory Bidirectional LDAP connector with Select Identity. At the end of this chapter, you will know the procedure to configure the Active Directory Bidirectional 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 Bidirectional 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/ActiveDirConnector`**.
- Select **`Yes`** for the Mapper Available section.

Refer to the *HP OpenView Select Identity Connector Deployment Guide* for detailed information on adding a new connector in Select Identity.

Add a New Resource

Add a new resource in Select Identity that uses the newly added connector. Refer to the *HP OpenView Select Identity Connector Deployment Guide* for detailed instruction on adding a resource in Select Identity.

Refer to the following table while entering the parameters in the Basic Information and the Access Information pages:

Table 5 Resource Configuration Parameters

Field Name	Sample Values	Description	Comment
Resource Name	ELDAPAD	Name given to the resource.	
Connector Name	ELDAPAD	The newly deployed connector.	Known as Resource Type on Select Identity 3.3.1.
Associate to Group	Selected	Whether the system uses the concept of groups. For this connector, select this option.	Applicable only for Select Identity 3.3.1.
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 5 Resource Configuration Parameters

Field Name	Sample Values	Description	Comment
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 mini agent and password plug-in installer program.	

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.

Map Attributes

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

Select Identity Resource Attribute	Connector Attribute	Attribute on Active Directory Bidirectional LDAP	Description
Street	streetAddress	streetAddress	
PhHome	homePhone	homePhone	
Email	Mail	mail	
PhMobile	mobile	mobile	
UserName	sAMAccountName	sAMAccountName	*This attribute is mandatory for user creation.*

Table 6 Active Directory Bidirectional LDAP Mapping Information

Select Identity Resource Attribute	Connector Attribute	Attribute on Active Directory Bidirectional LDAP	Description
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.*
Title	title	title	
DisplayName	displayName	displayName	
LastName	sn	Sn	*This attribute is mandatory for user creation.*
ObjectGUID	objectGUID	objectGUID	While associating Active Directory Bidirectional LDAP 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 Bidirectional LDAP 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 6A Exchange Mapping Information

Select Identity Resource Attribute	Connector Attribute	Attribute on Active Directory Bidirectional LDAP	Description
Email	Mail	mail	
MailBoxStore	homeMDB	homeMDB	
mailNickName	mailNickname	mailNickname	
AlternateRecipient	altRecipient	altRecipient	
HomeDirectory	homeDirectory	homeDirectory	
AddressBook	showInAddressBook	showInAddressBook	

Configure Workflow External Call on Select Identity

To achieve reverse synchronization, you must configure the workflow external call for user enable/ disable operation for Active Directory Bidirectional LDAP connector. When a user is enabled or disabled on resource (Active Directory), a specific Active Directory attribute value (`PSSync_ATTRIBUTE`) changes. The connector detects the change in the attribute value and registers the event as a user modification.

Refer to the *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 7 below.

Table 7 User Enable/Disable Parameters for Active Directory Bidirectional LDAP Connector

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

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

Configure Polling for Reverse Provisioning on Select Identity 3.3.1

If you install the Active Directory Bidirectional LDAP connector on Select Identity 3.3.1, you must perform some additional configuration steps on Select Identity to enable polling operation. For Active Directory Bidirectional LDAP connector, reverse synchronization of Active Directory is achieved by polling.

Each time the polling is invoked, the following sequences take place in the background:

1. Polling batch task is invoked.
2. The polling batch gets the resource name from the `TruAccess.properties` property file and get the ChangeLogs made from the last polling via the connector.
3. The polling batch task converts all the ChangeLogs into an SPML files, and the SPML file will be 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.
4. In the provisioning stage of request execution, Select Identity will be updated with the changes in the resource (normal non-authorized resource reconciliation).

Perform the following additional configuration steps on Select Identity:

1. Modify the Truaccess.properties File
2. Modify the Select Identity Database

Modify the Truaccess.properties File

You must add the following properties in the `TruAccess.properties` file to enable polling from Select Identity:

- A new entry "si.reconciliation.resync.polling" is used to point out the resource name for RESYNC or for reconciliation. The resource must be non-authoritative, otherwise no action will be taken for resync. For a regular reconciliation, the resource may be authoritative.

  si.reconciliation.resync.polling= <Resource Name on SI>

- To enable the RESYNC for reconciliation, following entries are also necessary.

  # The recon provisioning back feature is enabled for the specified resource.
  si.reconciliation.resync.<Resource Name on SI>=true

  # Workflow used for recon provisioning back feature of specified resource.
  truaccess.fixedtemplate.recon.resync.<Resource Name on SI>=SI\ Recon\ User\ Enable\ Disable\ Workflow

  # Default Workflow used for recon provisioning back feature.
  truaccess.fixedtemplate.recon.resync= SI\ Recon\ User\ Enable\ Disable\ Workflow

  # Another property is required to specify the keyfield name in the operational attributes of the spml request.
  si.reconciliation.polling.keyfield.<Resource Name on SI>= cn

  # Modify the following already existing entries as mentioned below.
  # Initially their values will be ReconciliationDefaultProcess, change it to
  # SI Recon User Enable Disable Workflow

truaccess.fixedtemplate.recon_enable=SI\ Recon\ User\ Enable\ Disable\ Workflow
truaccess.fixedtemplate.recon_disable=SI\ Recon\ User\ Enable\ Disable\ Workflow

A sample of modified `TruAccess.properties` file is shown below:

```
truaccess.fixedtemplate.recon_enable=SI\ Recon\ User\ Enable\ Disable\
Workflow truaccess.fixedtemplate.recon_disable=SI\ Recon\ User\ Enable\
Disable\ Workflow

si.reconciliation.resync.polling=AD

si.reconciliation.resync.AD=true

truaccess.fixedtemplate.recon.resync.AD=SI\ Recon\ User\ Enable\ Disable\
Workflow

truaccess.fixedtemplate.recon.resync=SI\ Recon\ User\ Enable\ Disable\
Workflow

si.reconciliation.polling.keyfield.AD=cn
```

Modify the Select Identity Database

You must add a row for a periodic polling task to the Batch table manually.

The xml text of the batch is:

```
<?xml version="1.0" encoding="UTF-8"?><Batch at="00:00:00" enabled="true"
handlerClass="
com.trulogica.truaccess.reconciliation.util.ReconPollingTaskHandler"
name="ReconPollingTask"
taskid="0"><RecurringSchedule><BySecond><RepeatInterval value="300"></
RepeatInterval></BySecond></RecurringSchedule></Batch>
```

You must run the following SQL command on the Select Identity database to add the batch task:

```
INSERT INTO BATCH (ID, ENABLED, STATE, REPEATCOUNT, NEXTSCHEDULED,
LASTSCHEDULED, JOBID, XMLTEXT, OWNER, STATECHANGETIME)
VALUES (-105, 1, 2, 1, '1/1/1975', null, null, '<?xml version="1.0"
encoding="UTF-8"?><Batch at="00:00:00" enabled="true"
handlerClass="com.trulogica.truaccess.reconciliation.util.ReconPollingTa
skHandler" name="ReconPollingTask"
taskid="0"><RecurringSchedule><BySecond><RepeatInterval value="300"></
RepeatInterval></BySecond></RecurringSchedule></Batch>', 0, null);
```

You have to add a new table(PollingJob), RESOURCECHANGELOG, to Select Identity database to store the lastChangeNumber as the parameter for calling the method `getChangeLog`.

To give the initial value of `lastChangeNumber` of the RESYNC resource, this PollingJob should be added before the first execution of polling batch with correct value of lastChangeNumber to prevent retrieve all users from the resource.

The SQL command that has to be run on SI database to create & initialize this table is:

```
CREATE TABLE RESOURCECHANGELOG
(
ResourceId int PRIMARY KEY NOT NULL,
lastChangeNumber int,
maxChangeLogCount int);

INSERT INTO RESOURCECHANGELOG  VALUES(<resourceId>, <lastChangeNumber>,
<maxChangeLogCount>);

Commit;
```

Where **<resourceId>** is the primary key (ID column) of the Active Directory resource from the APPLICATION table (There will be an entry for each Select Identity resource in APPLICATION table.)

<lastChangeNumber> is generated based on current date and time to a number. All changelogs generated on the resource after this time should be considered for Reconciliation. If **<lastChangeNumber>** is set to zero, then it indicates all changelogs are to be considered. After each polling execution, the lastChangeNumber will be updated.

<maxChangeLogCount> indicates the maximum number of changelogs that will be retrieved in one polling action from one resource.

Once these changes are done in database, Select Identity will start polling for the change logs every 5 mins. If you want to change the next poll time, you can modify the NEXTSCHEDULED column of the row with ID=-105 under BATCH table. Then next poll will be done when you have specified in this column.

After configuring the connector with Select Identity, you can use the connector to create a service, or you can associate the connector with an existing service. Refer to the *Service Studio* chapter of the *HP OpenView Select Identity Administrator Guide* for information on Select Identity services.

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.

Configuring 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.

6 Uninstalling the Connector

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

- Remove all resource dependencies.
- Delete the connector from the Select Identity.
- Delete the connector from application server.
- Uninstall the Mini-Agent and Password Plug-In from Active Directory resource by using automatic uninstaller program.

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

A 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`