HP Select Identity Software

Connector for Microsoft® Windows® Active Directory and Exchange

Software Version: 3.91

Installation and Configuration Guide

Document Release Date: September 2007
Software Release Date: September 2007

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

© Copyright 2006-2007 Hewlett-Packard Development Company, L.P.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/). Portions Copyright © 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 © 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 © 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

You can visit the HP software support web site at:

http://www.hp.com/go/hpsoftwaresupport

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into 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 sign in. Many also require an active support contract.

To find more information about support access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

1 Documentation Map

This chapter describes the organization of HP 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 Select Identity connector. For a list of available product documentation, refer to the Table 1.

Figure 1 Documentation Map

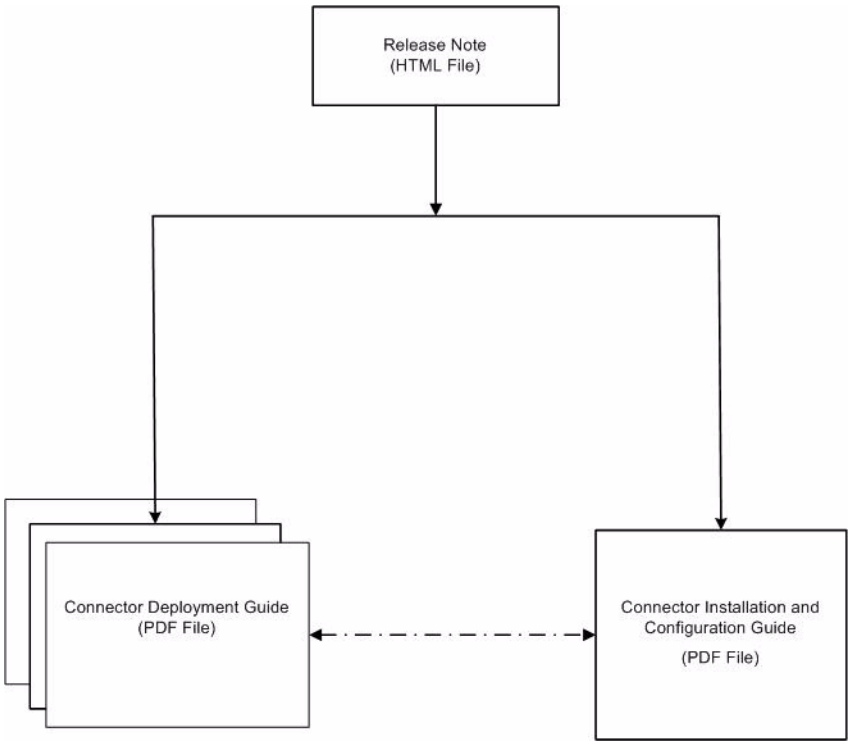


Table 1 Connector Documentation

Document Title and Filename	Contents	Location
Release Note `Active Directory and Exchange Connector v3.91 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 4.20) `connector_deploy_SI4.20.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/` root directory on the product's CD media.
Connector Deployment Guide (for Select Identity 4.10-4.13) `connector_deploy_SI4.13.pdf`		
Connector Deployment Guide (for Select Identity 4.0-4.01) `connector_deploy_SI4.pdf`		
Connector Deployment Guide (for Select Identity 3.3.1) `connector_deploy_SI3.3.1.pdf`		
Connector Installation and Configuration Guide `Active Directory and Exchange_guide.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 Select Identity connector for Active Directory and Exchange. An HP Select Identity connector for Active Directory and Exchange enables you to provision users and manage identities on Active Directory and Exchange server. At the end of this chapter, you will be able to know about:

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

About HP Select Identity

HP Select Identity provides a new approach to identity management. 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. 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 and Exchange Connector

The connector for Windows Active Directory and Exchange — hereafter referred to as Active Directory and Exchange connector — enables Select Identity to provision users on Microsoft Active Directory systems. As Microsoft Exchange relies on Active Directory for storing user data, you can also use this connector to provision user mailboxes in Exchange server.

The Active Directory and Exchange connector enables Select Identity to perform the following provisioning tasks on Active Directory and Exchange servers:

- 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
- Provision user mailboxes in Exchange server

When the connector adds a user to the Active Directory 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.

Active Directory and Exchange connector uses an agent for reverse synchronization. You must install the agent on Active Directory and Exchange resource system. Select Identity reconciles the changes made on resource by using the agent.

The Select Identity agent can also send changes made on the Windows system to Select Identity. This is called reverse synchronization. The updates made to Select Identity data depend on whether the Windows system is an authoritative or non-authoritative resource:

Operation	**Authoritative Resource**	**Non-authoritative Resource**
User is added on the resource.	The user is added to the respective Service.	User is not added. However, if the user exists, the entitlements are modified (not the user attributes).
User attributes are modified on the resource.	The user attributes are updated in Select Identity.	The user attributes are not updated in Select Identity.
User entitlements are modified on the resource.	The entitlements are modified in Select Identity.	The entitlements are modified in Select Identity.

Operation	Authoritative Resource	Non-authoritative Resource
User is deleted on the resource.	The user's Service membership is deleted in Select Identity.	The user is not deleted in Select Identity, though the entitlements for the resource are deleted.
Password is changed on the resource.	The user's password is reset in all Services for which the user is registered.	The user's password is reset in all Services for which the user is registered.
Move user to a different OU	The value of the UserSuffix attribute is updated in Select Identity to the new OU.	The value of the UserSuffix attribute is not updated in Select Identity.

Due to a known Active Directory limitation, events are not generated when some attributes are modified on Active Directory 2003. Events are generated when the following attributes are modified:

- Sam Account Name
- Display Name
- User Principal Name
- Home Directory
- Home Drive
- Script Path
- Profile Path
- User Workstations
- Password Last Set
- Account Expires
- Primary Group ID
- AllowedToDelegateTo
- User Account
- Control
- User Parameters
- Sid History
- Logon Hours
- Country description

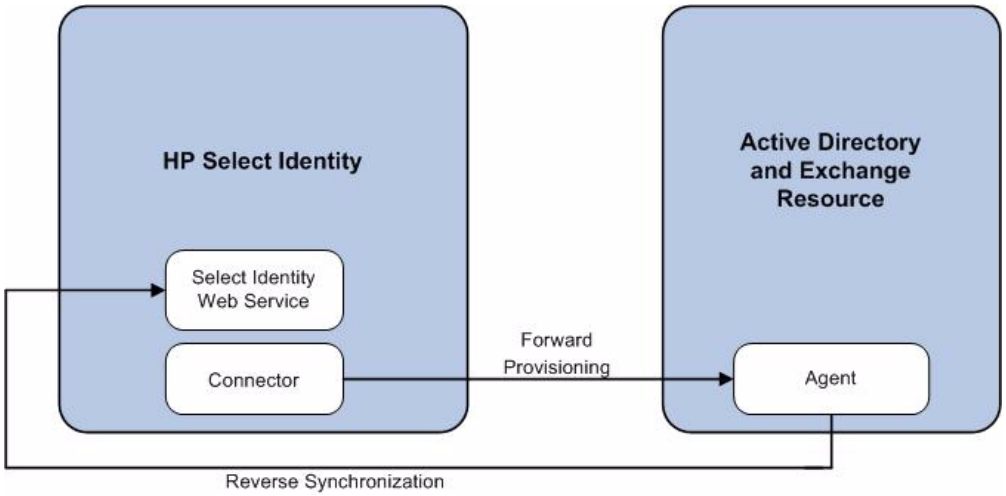
If an attribute other than one in this list is modified in Active Directory 2003, an event is not generated. This means that a reverse synchronization request cannot be sent to Select Identity.

This connector can be used with Select Identity 3.3.1-4.20.

High-Level Architecture

Figure 1 illustrates a high-level architecture of Active Directory and Exchange connector. You must install the connector on Select Identity server and the agent on resource system. The agent helps synchronizing the changes made on Active Directory and Exchange server with Select Identity.

Figure 1 High-Level Architecture of the Connector



To perform forward provisioning operation on Active Directory and Exchange server, the connector communicates with the agent. The agent executes the provisioning task on resource system.

The agent detects the changes on the host (Active Directory and Exchange) resource and sends SPML notifications to Select Identity to synchronize the changes. Thus, the Active Directory and Exchange connector enables data to flow in both the directions, as illustrated in Figure 1.

Organization of Tasks

Before you start installing the connector, you must ensure that system requirements and all the installation prerequisites are met. Refer to the Table 1 for an overview of installation tasks.

Table 1 Organization of Tasks

Task Number	Task Name	Reference
1	Install the connector on Select Identity server.	See Installing the Connector on page 15.
	— Meet the system requirement.	See System Requirements on page 16.
	— Extract contents of the Schema file.	See Extracting Contents of the Schema File on page 16.
	— Install the Resource Adapter Archive (RAR) file of the connector.	See Installing the Connector RAR on page 16.
2	Install the agent on the Active Directory and Exchange server.	See Installing the Agent on page 17.
3	Configure the connector with Select Identity.	See Configuring the Connector with Select Identity on page 29.

3 Installing the Connector

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

- Software requirements to install the Active Directory and Exchange connector.
- Procedure to install Active Directory and Exchange connector.

Active Directory and Exchange Connector Files

The Active Directory and Exchange connector is packaged in the following files, which are located in the `Active Directory & Exchange` folder on the Select Identity Connector CD:

Table 2 Active Directory and Exchange Connector Files

Serial Number	File Name	Description
1	• `ADConnector_420.rar` for WebSphere • `ADConnector_420WL9.rar` for WebLogic	It contains the binaries for the connector.
2	`ADSchema.jar`	It contains the mapping files, which control how Select Identity fields are mapped to Active Directory fields.
3	`AD_Agent_Installer.zip`	It contains the installation executable for the agent.

System Requirements

The Active Directory and Exchange connector is supported in the following environment:

Table 3 Platform Matrix for Active Directory and Exchange Connector

Select Identity Version	Application Server and Operating System	Database
3.3.1	WebLogic 8.1.4 on Windows 2003	Microsoft SQL Server 2000
	WebSphere 5.1.1 on HP-UX 11i	Oracle 9i
4.0-4.20	Active Directory and Exchange connector is supported on all the platform configurations of Select Identity 4.0-4.20.	

The agent is supported on the following platform:

Table 3A Platform Matrix for the Agent

Operating system	ADSI Version	Browser Version	Winsock Version
Microsoft Windows 2000 Server, Service Pack 4 or later, and Windows 2003 Server. The system must also be a primary or backup domain controller.	Version 5,0,00,0.	Internet Explorer 5.5 or later (supporting MSXML 2.0 or later).	Version 2.0 or later.

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

Installing the Connector RAR

To install the RAR file of the connector (such as `ADConnector_420.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 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/AD`**.

4 Installing the Agent

This chapter gives an overview of the agent for Active Directory and Exchange connector. 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 the Agent

The Active Directory and Exchange connector communicates to the resource Active Directory and Exchange with the help of the agent. For forward (Select Identity to Active Directory and Exchange) operations, the connector communicates with the agent and agent performs the provisioning on the resource. Agent sends back any changes made on Active Directory and Exchange to Select Identity web service in the form of SPML requests. The agent is packaged with the file `AD_Agent_Installer.zip`.

Installing the Agent on Active Directory and Exchange Server

After installing the connector on Select Identity server, you must install the agent on Active Directory and Exchange server.

Installation Prerequisites

Before you start installing the agent, make sure the following prerequisites are met.

- You must have the administrative privilege to log on to the Active Directory system during the agent installation.
- You must install the agent on a Primary Domain Controller (PDC) as the agent uses system event logs to monitor the changes.

  In a multi-domain or multi-master environment, you must install the agent on additional domain controllers if you want to reconcile the changes done on those systems with Select Identity. If the agent is installed only on the PDC, changes made on the other domain controllers are replicated to the PDC but security logs are not generated and changes are not captured by the agent.

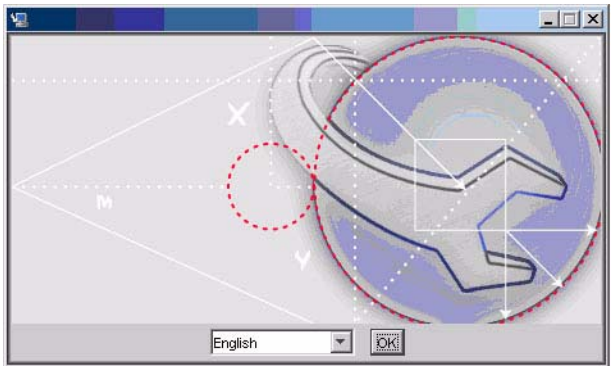
- If the Select Identity server and Active Directory and Exchange resource machines communicate across a firewall, they must allow bidirectional TCP flow on port 5000 (this can be configured on any other port, as well).

- The version of ADSI on resource machine must be 5,0,00,0. To verify the version of ADSI, perform the following steps:
  a. On the Active Directory and Exchange server, open the Registry Editor window.
  b. On the left pane, expand **HKEY_LOCAL_MACHINE → SOFTWARE → Microsoft → Active Setup → Installed Components**.
  c. Double-click **{E92B03AB-B707-11d2-9CBD-0000F87A369E}.**
  d. On the right pane, double-click **Version**. Edit String dialog box appears.
  e. The Value data field must display 5,0,00,0.

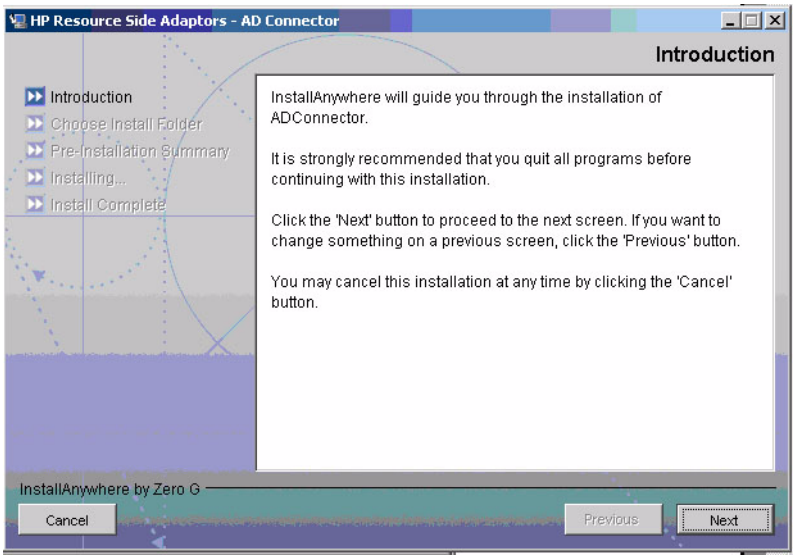
Agent Installation

Perform the following tasks to install the agent:

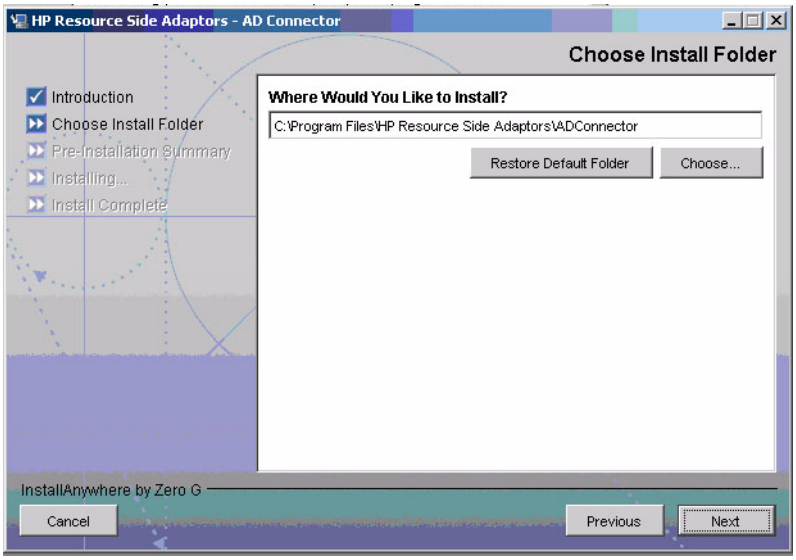
1. Extract the contents of `AD_Agent_Installer.zip` to a local folder (<*Extract_Dir*>) on Active Directory and Exchange server.
2. Double-click the agent installer program `SETUP.exe` from the location <*Extract_Dir*>`\Disk1\InstData\NoVM`. The installation wizard appears.



3. Click **OK** to start the installation. The Introduction screen appears.

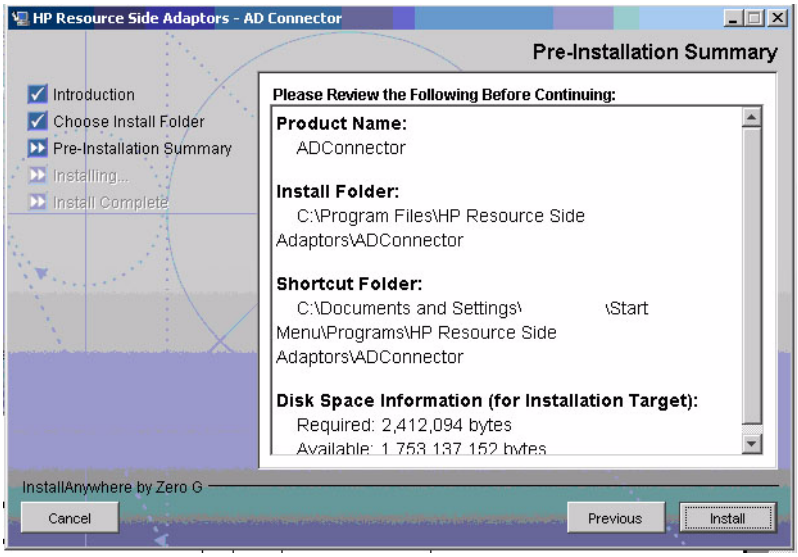


4 Click **Next**. The Choose Install Folder screen appears.

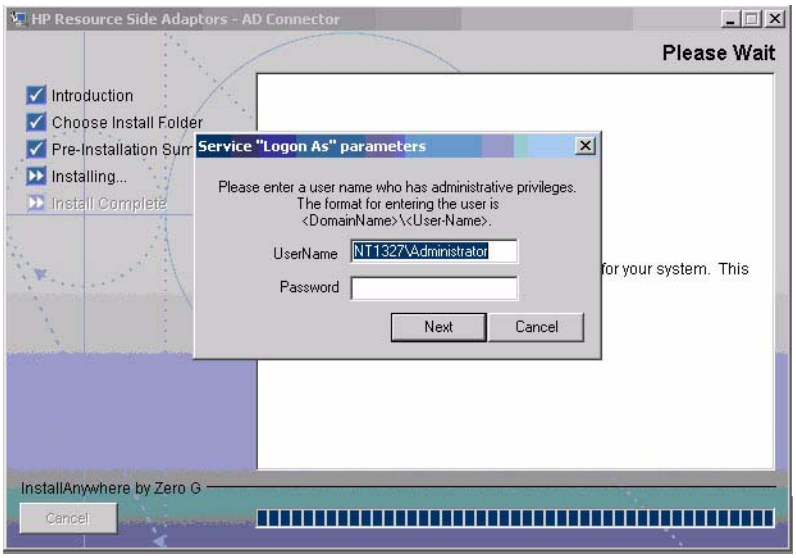


5 Click **Choose** to change the default installation folder if required.

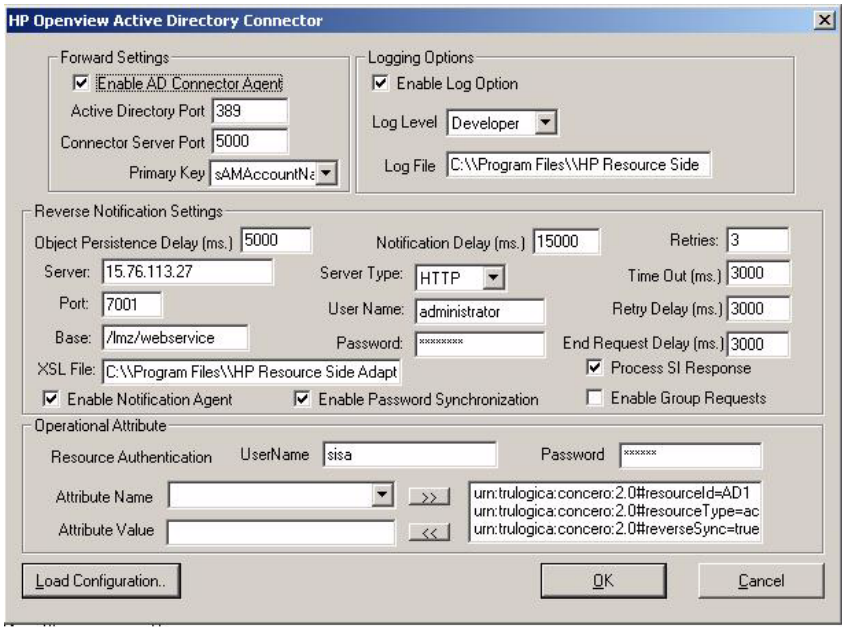
6 Click **Next**.The Pre-Installation Summary screen appears.



7 Click **Install**. Service “Logon as” parameters dialog box appears.



8 Provide the administrative logon information in the specified format, and then click **Next**. HP Active Directory Connector dialog box appears.



9 You must configure the following agent settings in this dialog box.

Forward settings —

a Check the Enable AD Connector Agent check box.

b Enter the Active Directory port number (the port on Active Directory and Exchange server used by Active Directory) in the Active Directory Port text box. The default value is 389.

c Enter the connector server port number (the port on Select Identity server used by the connector to communicate with the agent) in the Connector Server Port text box. The default port number is 5000.

d Keep the default option `sAMAccountName` in the Primary Key drop-down box.

➤ The `sAMAccountName` key works for all the functions in both forward and reverse provisioning. If you choose any one of the other two options — `distinguishedName` and `userPrincipalName` — the connector cannot reconcile `resetPassword` and `deleteuser` operations from Active Directory to Select Identity.

➤ When the number of groups in the Active Directory are more than 20000 , add the key `PSSync_MaxSupportedEntries` to the registry to the path `HKEY_LOCAL_MACHINE\SOFTWARE\HPOpenview\ADConnector`. The value for this key must be the total number of groups in the resource. If the number of groups are less than 20000, no change is needed.

Logging Options —

a Check the Enable Log Option check box.

b From the Log Level drop-down box, select the log level from the options Basic, Intermediate, Advanced, and Developer. Developer is the most verbose level.

c In the Log File text box, enter the location where the log file can be placed. The default location is <*Install_Dir*>`\Logs`.

Reverse Notification Settings —

a Check the Enable Notification Agent check box.

b Check the Enable Password Synchronization check box to synchronize the Windows server password with Select Identity. The information is sent back to Select Identity in the form of an SPML extendedRequest over SOAP/HTTP or HTTPS.

c In the Object Persistent Delay text box, enter the duration (in millisecond) for which an object in Active Directory should persist before the user details are retrieved by the agent. The optimal value is 1000 milliseconds.

d In the Notification Delay text box, enter the duration (in milliseconds) between two consecutive requests sent to Select Identity. The optimal value is 5000 milliseconds.

e In the Server text box, enter the IP address or fully-qualified name of Select Identity server.

f In the Port text box, enter the port number on which Select Identity listens for reverse synchronization requests.

g In the Base text box, enter the base URL for Select Identity Web Service.

h Select HTTP or HTTPS from the Server Type drop-down box. This defines the protocol for transfer of data back to Select Identity.

i In the User Name text box, enter the name of a user with administrative privileges on the Windows server. The installed agent runs under this user. Specify the Select Identity administrator or another administrative user on the system.

j In the Password text box, enter the password for the above mentioned administrative user.

k Set the Time Out, Retries, and Retry Delay settings as follows:

– The Time Out field specifies the number of milliseconds after which a request times out. The recommended value for this field is 5000 ms.

- The Retries field specifies the number of retries that the agent will attempt to send the SPML request (which is useful, for example, if Select Identity was unavailable during the original request; the agent retries the request according to these settings after Select Identity is available again).
- The Retry Delay setting is used to specify the delay between multiple retries.

l The End Request Delay is for the agent to write HTTP Buffer. This depends on the Network Latency. The default value is 3000 ms.

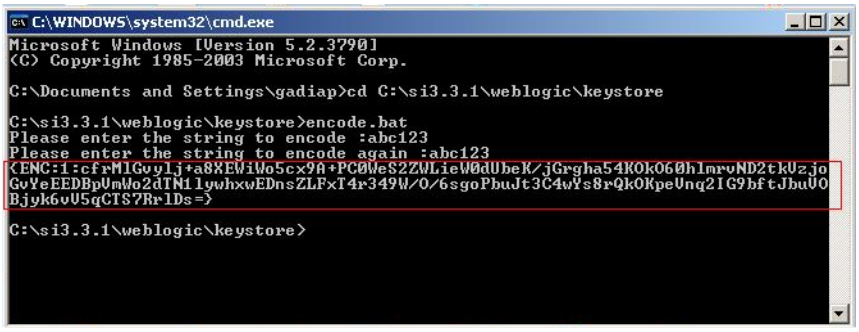
m Enable Group Requests field is to check whether to process the group provisioning or not.

Operational Attributes —

a In the UserName text box, enter the name of the administrator account in Select Identity.

b In the Password text box, enter the password of the administrative account in Select Identity.

Enter the password in the Password field. To encrypt the password, run encode.bat (on Windows) or encode.sh (on UNIX), which is provided in the WebLogic/keystore subdirectory in the Select Identity home directory. This utility prompts you for the password to encrypt and will generate the encrypted password. Be sure to copy the entire encrypted password in the field, as shown here:



c Edit the following operational attributes. This builds the operational attributes that are sent in SPML requests back to Select Identity for synchronization. Click the << button after each attribute and edit the value to specify the desired value, then click the >> button.

Attribute Name	Attribute Value	Description
urn:trulogica:concero:2.0#resourceId	resource_name	This is the name of the resource that you add in Select Identity for this Active Directory server. For example, if you specify AD_Exchange here, then specify AD_Exchange as the resource name in Select Identity.
urn:trulogica:concero:2.0#reverseSync	true	
urn:trulogica:concero:2.0#resourceType	activedirectory	This is the name of the XSL file (without the .xsl extension), which provides reverse mappings for the agent to send data back to Select Identity.

d Click the **Load Configuration** button to load all values in the console from a properties file (instead of entering the values in the console). For example, you could enter the values for the attributes in a `.properties` file in the following format:

```
PSNotify_EIS_Port=389
PSLog_Enabled=1
PSLog_Level=2
PSPassFilt_Enabled=1
PSSync_Server_Name=ps0111
PSSync_Server_Port=80
PSSync_Timeout=400
PSSync_Retries=8
PSSync_Retries_Delay=3000
PSSync_Server_Secure=0
Installing the Connector 25
PSSync_Server_Username=Administrator
PSSync_Server_Password=Trulogica
PSSync_Request_Delay=5000
PSConnector_Port=5000
PSSync_Server_BaseURL=/lmz/webservice
PSSync_Res_Username=sisa
PSSync_Res_Password=abc123
PSMap_Path=C:\\Program Files\\HP Openview\\HP Openview
ADConnector\\Map\\agent.properties
PSLog_Path=C:\\Program Files\\HP Openview\\HP Openview
ADConnector\\Logs
```

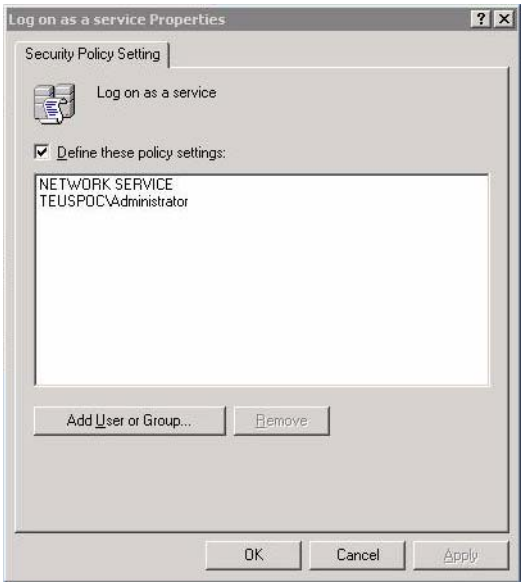
10 Click **OK**.

11 Click **Done**, and then restart the Active Directory and Exchange server.

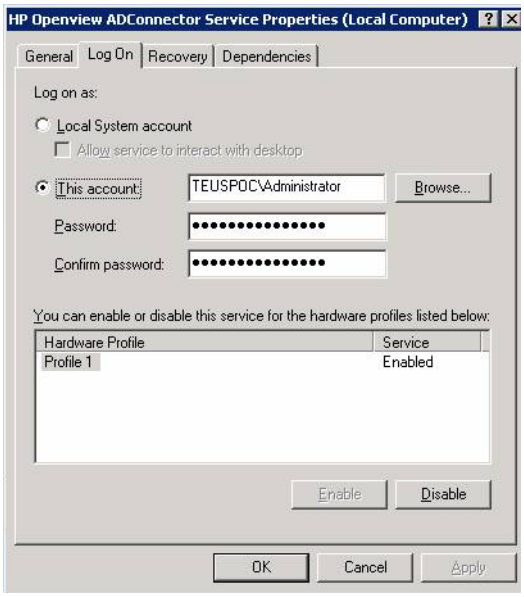
Configuring a User for the Agent's Service

By default, the agent logs on as the Local System account on the Active Directory server. However, if the server reboots, the agent's service is not automatically started; the Local System account does not have permission to restart the agent's service. To ensure that the agent is automatically restarted after reboot, you can create a user for the agent and configure that user to automatically restart the service. Perform the following steps:

1. From the Start menu, click **Programs** → **Administrative Tools** → **Active Directory Users and Computers**. Active Directory Users and Computers Console window opens.
2. Create or identify a user on the Active Directory server that can be assigned as the Log On As user for the agent. You must have administrative permissions on the system to create a user.
3. Update the local security policy to allow the new user to run as a service. Set this policy from the Default Domain Controller Security Settings window through **Start** → **Programs** → **Administrative Tools** → **Default Domain Controller Security** → **Security Settings** → **Local Policies** → **User Rights Assignment** → **Log on as a service**. The following snapshot illustrates that the TEUSPOC\Administrator user, which is the user created for the agent, is granted permission to log on as a service:



4 Configure the HP ADConnector Service and ADNotification Service, which are installed with the agent, to use the newly created user as its Log On As user. Perform this step from the Services windows, which is accessible from the Administrative Tools window. In the following snapshot, the TEUSPOC\Administrator user is assigned to the HP Openview ADConnector Service:

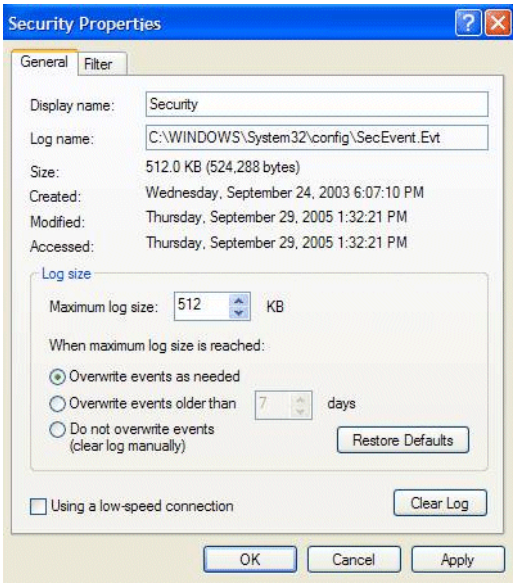


Configuring Active Directory to Support Reverse Synchronization

If you configure the agent to support reverse synchronization, perform the following configuration steps to enable Active Directory to support reverse synchronization:

- Verify the security log of the Windows Event Viewer. Perform the following steps to view the log:
  a From the Start menu, click **Settings** → **Control Panel**.
  b Double-click **Administrative Tools**. The Administrative Tools window appears.
  c In the Administrative Tools window, double-click **Event Viewer**. The Event Viewer window appears.

d In the Event Viewer window, right-click **Security** and open the Security Property dialog box.



e In the Security Property dialog box, select **Overwrite Events as needed**, if not already selected.

- If you installed the agent on a Windows 2000 Server (Primary Domain Controller or Backup Domain Controller), you must enable strong password enforcement. To do so, select **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Domain Controller Security Policy** → **Security Settings**. Expand the Account Policies folder and double-click **Passwords must meet complexity requirements**. Select the **Enable** option and click **OK**.
- Set the Audit Account Management and Audit Directory Service Access policies to Success in the Audit Policy. (This must be done for the Default Domain Controllers Group Policy.) To do so, launch the Control Panel, double-click **Administrative Tools**, then double-click **Domain Controller Security Policy**. Select **Local Policies** → **Audit Policy**. Right-click **Audit account management**, select **Security...**, and then select the Success check box.

  Repeat this step for Audit directory service access. After configuring the policies, enter the following command in a Command Prompt window:

  ```
  gpupdate /force
  ```

- Configure the Access Control Lists (ACL) to enable auditing by performing the following steps:

  These steps are needed for Active Directory 2003 only. You can skip these steps on Active Directory 2000.

  a Select **Start** → **Settings** → **Control Panel**, double-click **Administrative Tools**, and then double-click **Active Directory Users and Computers**.

  b Select **View** → **Advanced Features**.

  c Right-click the Active Directory object that you want to audit, then click **Properties**.

  d Click the **Security** tab, then click **Advanced**.

  e Click the **Auditing** tab, then click **Add**.

f Enter the name of the user or group whose access you want to audit in the Enter the object name to select field, and then click **OK** (You can enter Everyone).

g In the list of names, double-click the user or group whose access you want to audit.

h Select the Successful check box or the Failed check box for the actions that you want to audit. You can also select Success or Failure for the Write all properties option. Then, click **OK**.

i Click **OK**, and then click **OK**.

5 Configuring the Connector with Select Identity

This chapter describes the procedure to configure the Active Directory and Exchange connector with Select Identity and the connector specific parameters that you must provide while configuring the 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 and Exchange 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/AD`**.
- Select No for the Mapper Available section.

Refer to the *HP 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 Select Identity Connector Deployment Guide* for detailed instructions on adding a resource in Select Identity.

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

Table 4 Resource Configuration Parameters

Field Name	Sample Value	Description	Comment
Resource Name	AD_Exchange	Name given to the resource. If you enabled reverse synchronization, this must be the same as the value provided for the urn:trulog-ica:concero:2.0#resourceId attribute on the agent console.	
Connector Name	ADConnector	The newly deployed connector.	Known as Resource Type on Select Identity 3.3.1.
Authoritative Source*	No	Whether this resource is a system that is considered to be the authoritative source for user data in your environment. Specify **No** if the connector is not enabled for reverse synchronization. Specify **Yes** if you want to add users through reverse synchronization. If the resource is not authoritative, the resource can only modify user entitlements during reverse synchronization.	
Associate to Group	Selected	Whether the system uses the concept of groups. For the Active Directory and Exchange connector, select this option.	Applicable only on Select Identity 3.3.1.
Delete User	No	Specifies whether the user should be deleted from the resource when a DeleteServiceMembership operation is performed for the user in Select Identity.	
Reconciliation Workflow	ReconciliationDefaultProcess	Specifies the workflow to be used during reverse synchronization.	

Table 4 Resource Configuration Parameters (cont'd)

Field Name	Sample Value	Description	Comment
Resource Owner	sisa	Specifies the user who is the resource owner.	
Username	Administrator	Administrative account on the target Windows resource.	
Password	Password123	Password corresponding to the UserName account.	
Server Name	server	The NETBIOS name or IP address of the Windows system running Active Directory. If you specify a server name, specify the name without the domain. For Active Directory 2003, specify the NETBIOS name without the domain extension and do not specify an IP address.	
AD Port	389	Active Directory port on the Windows resource.	
Agent Port	5000	Forward connector server port, as configured on the resource agent.	

Map Attributes

After successfully adding a resource for the Active Directory and Exchange connector, you must map the resource attributes to Select Identity attributes. Refer to the *HP 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 5 Active Directory and Exchange Mapping Information

Select Identity Resource Attribute	Active Directory User Attribute	Label on Active Directory UI	Description
UserName	UserId	sAMAccountName	Primary key for the Active Directory user. *This attribute is mandatory and must be mapped.*
Password	Password	Password (on the Account tab)	User's password. *This attribute is mandatory and must be mapped.*
Common Name	cn	RDN portion of distinguished name or cn	*This attribute is mandatory and must be mapped else the value passed to the UserId will be set to this field.*
userPrincipal-Name	userPrincipal-Name	userPrincipal-Name	
DisplayName	displayName	Display Name	Name displayed in the address book.
countryName	C	Country/Region (on the Address tab)	Two-character abbreviation of the country or region, per the ISO 3166-1 format.
Comment	Info	Notes (on the Telephone tab)	Notes about the user.
ScriptPath	ScriptPath	Logon Script (on the Profile tab)	The path of the user's logon script, which can be a .CMD, .EXE, or .BAT file. The string can be null.

Table 5 Active Directory and Exchange Mapping Information

Select Identity Resource Attribute	Active Directory User Attribute	Label on Active Directory UI	Description
UserSuffix	UserSuffix		The organization unit or the container in the distinguished name. For example, if the distinguished name is CN=Userid, OU=subdept1, OU=dept1,DC=tru, DC=hp,DC=com, then the value of this field is OU=subdept1, OU=dept1.
HomeDirectory	HomeDirectory	Home Folder: Local path or Home Folder: To (on the Profile tab, field dependent on homeDrive)	A path to a home share or a local directory path, but not both.
(not mapped by default)	GivenName	First Name (on the General tab)	First (given) name.
(not mapped by default)	sn	Last Name (on the General tab)	Last name (surname).
(not mapped by default)	Initials	Initials (on the General tab)	Single-valued property containing the initials of the user's full name. This may be used as the middle initial in the Windows Address Book.
(not mapped by default)	Description	Description (on the General tab)	Description of the user.
(not mapped by default)	physical Delivery OfficeName	Office (on the General tab)	The office location in the user's place of business.
(not mapped by default)	Telephone Number	Telephone Number (on the General tab)	Primary telephone number.
(not mapped by default)	Other Telephone	Telephone: Other (on the General tab)	Alternate telephone number.
(not mapped by default)	Mail	E-Mail (on the General tab)	Email address.

Table 5 Active Directory and Exchange Mapping Information

Select Identity Resource Attribute	Active Directory User Attribute	Label on Active Directory UI	Description
(not mapped by default)	wwwHomePage	Web Page (on the General tab)	URL of the user's primary web page.
(not mapped by default)	url	Web Page: Other (on the General tab)	Alternate web page address.
(not mapped by default)	StreetAddress	Street (on the Address tab)	Street address.
(not mapped by default)	PostOfficeBox	P.O.Box (on the Address tab)	Post Office box.
(not mapped by default)	L	City (on the Address tab)	Single-valued property containing the locality, such as the town or city, in the user's address.
(not mapped by default)	St	State/Province (on the Address tab)	State or province.
(not mapped by default)	PostalCode	Zip/Postal Code (on the Address tab)	Postal (zip) code.
(not mapped by default)	HomePhone	Home (on the Telephone tab)	User's home phone number.
(not mapped by default)	OtherHome Phone	Home: Other (on the Telephone tab)	Alternate home phone number.
(not mapped by default)	Pager	Pager (on the Telephone tab)	User's pager number.
(not mapped by default)	OtherPager	Pager: Other (on the Telephone tab)	Alternate pager number.
(not mapped by default)	Mobile	Mobile (on the Telephone tab)	Primary mobile telephone number.
(not mapped by default)	OtherMobile	Mobile: Other (on the Telephone tab)	Alternate mobile number.
(not mapped by default)	facsimile Telephone Number	Fax (on the Telephone tab)	Telephone number of the user's business fax machine.

Table 5 Active Directory and Exchange Mapping Information

Select Identity Resource Attribute	Active Directory User Attribute	Label on Active Directory UI	Description
(not mapped by default)	other Facsimile Telephone Number	Fax: Other (on the Telephone tab)	Alternate fax number.
(not mapped by default)	IpPhone	IP phone (on the Telephone tab)	Telephony phone number.
(not mapped by default)	OtherIpPhone	IP phone: Other (on the Telephone tab)	Alternate telephony number.
(not mapped by default)	ProfilePath	Profile Path (on the Profile tab)	A path to the user's profile. This value can be a null string, a local absolute path, or a UNC path.
(not mapped by default)	HomeDrive	Home Folder: Connect (on the Profile tab)	If a valid drive letter is specified, the HomeDirectory attribute becomes a share path; otherwise, it is considered a local directory path.
(not mapped by default)	Department	Department (on the Organization tab)	User’s department.

Table 5 Active Directory and Exchange Mapping Information

Select Identity Resource Attribute	Active Directory User Attribute	Label on Active Directory UI	Description
(not mapped by default)	Title	Title (on the Organization tab)	User's formal job title or designation, such as “Senior manager.”
(not mapped by default)	Company	Company (on the Organization tab)	Company for which the user works.
(not mapped by default)	Manager	Manager: Name (on the Organization tab)	The fully qualified, distinguished name of the manager. The manager's user object contains a directReports property that contains references to all user objects that have their manager properties set to the manager's user object.

Map Attributes for Exchange

If you wish to configure the connector to provision user mailboxes in Exchange 2000, you *must* add the following Exchange 2000 attributes in the `aduser.properties` file:

```
<SI Attribute>|mailNickname
<SI Attribute>|msExchHomeServerName
```

where the Select Identity attributes are attributes configured on the Select Identity server.

The mailNickname attribute on the Exchange 2000 server is the name portion of the Email address. For example, if the email address is vlee@mydomain.com, the mailNickname attribute is assigned the vlee portion of the email address.

The msExchHomeServerName attribute is a concatenation of several server values. Here is the syntax:

/o=*exOrg*/ou=First Administrative Group/cn=Configuration/cn=Servers/cn=*mailStorage*

where

- *exOrg* is the Exchange organization name. An example is **`First Organization`**.
- *mailStorage* is the Exchange mailbox name. An example is **`MYSTORAGE`**.

In addition, you can map a Select Identity attribute to the HomeMDB attribute on the Exchange 2000 server. (On the Exchange 2000 interface, this attribute maps to the Mailbox store property on the General tab for Active Directory User.) The HomeMDB attribute represents the URL of the user’s mailbox. This property is read-only and is set when the mailbox is created.

After mapping the attributes, you can use the connector to create a service, or you can associate the connector with an existing service. Refer to the *Service Studio* chapter of the *HP Select Identity Administration Online Help* for information on Select Identity services.

If you enable reverse synchronization, configure the service as follows:

- When selecting the Business Relationship, choose the ReconciliationDefaultProcess workflow for the RECONCILIATION:Add Service and RECONCILIATION:Delete Service Membership request events. For RECONCILIATION:Add Service, use the user addition view.
- In the user addition view, specify mandatory attributes that are guaranteed to be passed by the reverse synchronization request when adding a user. If you specify a mandatory attribute that is not passed by the resource, the user can be created in Select Identity but reverse synchronization will not succeed.
- When specifying the context, obtain the value from the add request issued by the resource. For example, if the context is Country and the value is US, the `<addRequest>` element in the reverse synchronization request should have an attribute called country and a value of US. If the context attribute is not present in the add user request, the user can be created in Select Identity but will not be assigned to a Service.

6 Uninstalling the Connector

If you want to uninstall Active Directory and Exchange connector from Select Identity, perform the following steps:

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

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

Uninstalling the Agent

Perform the following steps to delete the agent on the Windows server:

1. From the Start menu, select **Programs** → **HP OpenView AD Connector** → **Uninstall Agent**. The uninstallation wizard appears.
2. Follow the instruction on the wizard to uninstall the agent.

A Frequently Asked Questions (FAQ)

This appendix provides questions to frequently asked questions about the Windows Active Directory connector and its agent.

General

FAQ 1: How does the connector interact with Active Directory to accomplish its purpose of provisioning users and entitlements?

The connector relies on an agent, which is installed on the Domain Controller, to provision users and entitlements in Active Directory. The agent also initiates reverse synchronization, to push changes made in Active Directory back to the Select Identity database. The agent uses the ADSI API to interact with Active Directory.

FAQ 2: How does the connector interact with other servers?

The connector interacts with the agent, and the agent must reside on the Domain Controller.

FAQ 3: Does the connector have internal administrative roles and security?

Yes, the agent uses 128-bit PC1 encryption for JCA to communicate with the agent.

FAQ 4: How are queries defined and by whom?

The Select Identity server controls the connector.

FAQ 5: How are OUs targeted for account creation and placement?

The target OU is a connection parameter that is defined when the connector is created (deployed) in Select Identity.

FAQ 6: What objects can be deleted by the connector?

The Active Directory connect can remove users, groups, and computers from Active Directory.

FAQ 7: When I attempt to provision in Active Directory, the connection fails. How can I debug this problem?

There are several actions you can perform to find the root of this problem:

- Stop the Active Directory services (HP ADConnector Service and HP Openview ADNotification Service) and restart the server and services.
- Make sure that you can connect to the Active Directory resource using another tool and specifying the same parameters that you supplied for the attempted resource creation or modification.
- Ensure that the `aduser.properties`, `adgroups.properties`, and `adcomputer.properties` files are in the application server's class path.

- Verify the port specified in the agent console and ensure the same port is specified on the resource creation/modification page.
- On the agent console, be sure to supply the same resource name (in the operation attributes) that you specified in the resource creation/modification page.
- If necessary, remove the connector from the application server then redeploy it. In Select Identity, simply modify the connector to update it.
- Check the browser version in Active Directory Resource machine.It should be Internet Explorer 5.5 or later (supporting MSXML 2.0 or later).

FAQ 8: Do we need to install agent on all the domain controllers under the domain forest?

Yes, it needs to be installed on all the domain controllers, whichever needs the reconciliation of user attributes and password to Select Identity.

Permissions, Privileges, and Rights

FAQ 9: If a service account is given full control of an OU and the account does not have Domain Admin or BUILTIN\Administrator privileges, permissions, or rights, can the connector perform its functions?

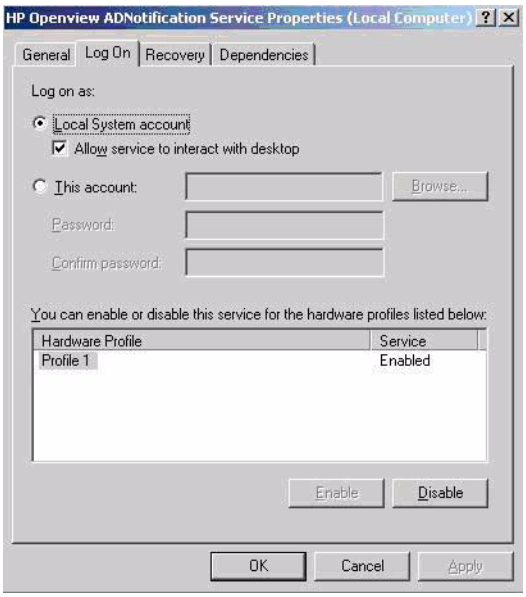
Yes, the connector can provision (forward provisioning) users and entitlements on the Active Directory or Exchange resource. The agent is responsible for sending changes made in Active Directory to the connector for reconciliation with the Select Identity database. The following are required for forward provisioning and reverse synchronization:

- Any user account that is a member of the Account Operators group
- Access to the HKEY_LOCAL_MACHINE\SOFTWARE\HPOpenview\ ADConnector registry key is enabled for non-administrative accounts Refer to **http:// support.microsoft.com/?kbid=245031** for information about changing registry access.

The Account Operators group has the following privileges:

- Domain Controller Security Policy → Local Policies → User Rights → Log on as Service right
- Domain Controller Security Policy → Local Policies → User Rights → Backup Files and Directory rights
- Domain Controller Security Policy → Local Policies → User Rights → Manage Auditing and Security Log rights
- Domain Controller Security Policy → Local Policies → User Rights → Access this computer from the network
- Read/Write/Execute Permission on the installation folder of the agent and its subfolders
- Configure the HP Openview ADConnector Service and HP Openview ADNotification Service in the following way:
  a. From the Start menu, click **Run**.
  b. Type **`services.msc`** and click **OK**. The Services window opens.
  c. In the right pane, locate the services mentioned above.

d Double-click on each service name. The properties dialog box appears.



e Click the Log On tab.

f Select the LocalSystem account radio button.

g Select the Allow service to interact with desktop check box.

h Enable the service to start automatically.

FAQ 10: If the connector cannot function with lesser privileges, permissions, and rights, what specific areas or functions of Active Directory require administrative status?

For forward provisioning, membership in the Account Operators group is mandatory. The rest of the restrictions arise due to configuration storage (registry access) and logging (directory access) requirements.

FAQ 11: What facets of Select Identity and the Windows Active Directory connector require full control of all Domain Controllers, all facets of Active Directory, and every Windows-based computer in the Enterprise?

See FAQ 9 on page 42.

FAQ 12: What account is used to run Select Identity services?

See FAQ 9 on page 42.

Agent

FAQ 13: How is the agent installed on the Domain Controller?

The agent is a Windows service that is installed by an EXE file. A console application is provided for configuring the agent.

FAQ 14: Is the agent configurable? If so, what tools are used and where are those tools located?

A console application is provided for configuring the agent. This console application is also installed by the installer.

FAQ 15: What services are used by the agent?

For forward provisioning, the agent uses the TLServer service. For reverse synchronization, the agent uses the TLADNotify service.

FAQ 16: What does the agent access on the Domain Controller?

The agent uses ADSI to access users and groups in Active Directory on the Domain Controller for provisioning. It uses the registry for configuration storage (password filters cannot access files). It also uses the file system for logging.

For reverse synchronization, the agent uses the Windows Security Event Log to detect changes. It uses the registry for configuration storage (password filters cannot access files), and it uses the file system for logging.

FAQ 17: Can the agent alone be used to view or change anything on the Domain Controller or within Active Directory? If so, what can be controlled?

No, the connector must be used to control the agent. However, stubs can be written to emulate the connector.

FAQ 18: When the agent is installed, what changes are made to the registry, the boot and root partitions, share security, and NTFS security on the Domain Controller?

During installation, the following changes are made to the Domain Controller's system:

- Two services are created with the account specified
- Registry entries are created for the configuration
- The folder structure is created at the selected location
- Security policies related to Auditing Security Event Log are configured to enable auditing of account management and directory access
- LSA Security policy is edited to enable password synchronization

FAQ 19: How is configuration information stored on the agent's host system?

The configuration data for the agent is stored in the registry.

FAQ 20: Does the agent have log files? If so, what is logged? Where are the logs stored and in what format?

The agent uses a custom logging utility to create its log files. The utility enables you to configure levels of logging, using the agent's console application. The amount of available disk space restricts the size of the log files.

FAQ 21: Who can access and delete logs created by the agent?

Any user with write permissions can access and delete the logs.

FAQ 22: What configuration files are created for the agent? Where are they stored and in what format? Who has access and can make changes?

The agent stores its configuration in the registry. See FAQ 9 on page 42 for specific information on this registry key.

FAQ 23: Are local service accounts required by the agent? What privileges, permissions and rights do the accounts require? Who needs to know the passwords for these accounts?

See FAQ 9 on page 42.

FAQ 24: What Domain-level service accounts are required?

See FAQ 9 on page 42.

FAQ 25: To what service or function does each account relate?

See FAQ 9 on page 42.

FAQ 26: Do any of these accounts impact other servers? If so, what servers, how do they connect, what permissions and rights are needed, and what impact do they have on the target servers?

The accounts and agent affect all systems in domain because provisioning occurs for Domain Users.