HP OpenView Select Identity

Connector for Microsoft® Windows® NT Domain Systems

Software Version: 3.5

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

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

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

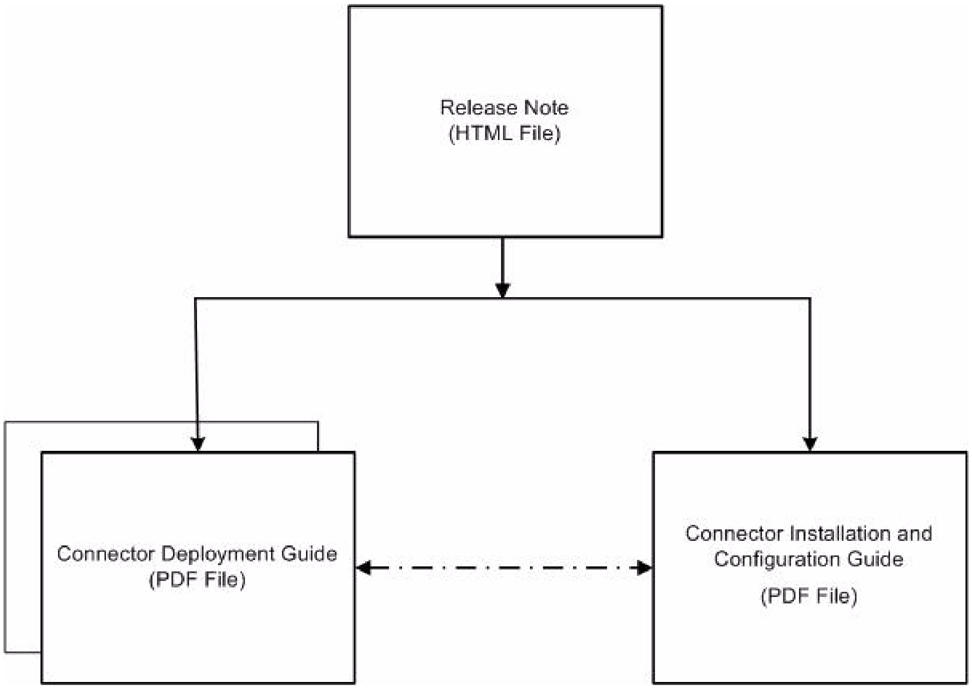


Table 1 Connector Documentation

Document Title and Filename	Contents	Location
Release Note `NT Domain Connector v3.5 Release Note.htm`	This file contains necessary information on new features of the connector, enhancements, known problems or limitations, and support information.	`/Docs/` subdirectory under the connector directory.
Connector Deployment Guide (for Select Identity 4.0/4.01.000) `connector_deploy_SI4.pdf`	Connector deployment guides provide detailed information on: • Deploying a connector on an application server. • Configuring a connector with Select Identity. Refer to these guides when you need generic information on connector installation.	`/Docs/` subdirectory under the connector directory.
Connector Deployment Guide (for Select Identity 3.3.1) `connector_deploy_SI3.3.1.pdf`		
Connector Installation and Configuration Guide `NT Domain_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 Microsoft Windows NT Domain . An HP OpenView Select Identity connector enables you to provision users and manage identities on Microsoft Windows NT Domain systems. At the end of this chapter, you will be able to know about:

- The benefits of HP OpenView Select Identity.
- The role of a connector.
- The connector for Microsoft Windows NT Domain .

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 NT Domain Connector

The connector for Microsoft Windows NT Domain systems — hereafter referred to as NT Domain connector — enables HP OpenView Select Identity to provision users on Windows NT systems with the Domain Controller. (If your Windows systems are based on Active Directory, you must use the Windows Active Directory connector.) This connector is a two-way connector and can send user changes made on the NT Domain server to the Select Identity.

The NT Domain connector enables Select Identity to perform the following provisioning tasks on NT-based systems:

- 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

The agent of the connector detects the changes on the host (Microsoft Windows NT Domain) resource and sends SPML notifications to Select Identity to synchronize the changes. The updates made to Select Identity data depend on whether the Windows system is an authoritative or non-authoritative resource. The table below compares the reconciliation mechanism of an authoritative resource and a non-authoritative resource.

Operation	Authoritative Resource	Non-Authoritative Resource
User addition 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 modification on the resource.	Attributes are updated in Select Identity.	Attributes are not updated in Select Identity.
User entitlements modification on the resource.	Entitlements are modified in Select Identity.	Entitlements are modified in Select Identity.
User deletion 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 change 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.

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

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

Overview of Installation Tasks

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

Table 2 Organization of Tasks

Task Number	Task Name	Reference
1	Install the connector on the Select Identity server.	See Installing the Connector on page 13.
	— Meet the system requirements.	See System Requirements on page 13.
	— Extract contents of the Schema file (file that contains the mapping files for the connector) to location on the Select Identity server.	See Extracting Contents of the Schema File on page 14.
	— Install the Resource Adapter Archive (RAR) of the connector on an application server.	See Installing the Connector RAR on page 14.
2	Installing the agent for NT Domain connector.	See Installing the Agent on page 15.
3	Configure the connector with the Select Identity server.	See Configuring the Connector with Select Identity on page 19.

3 Installing the Connector

This chapter elaborates the procedure to install NT Domain on Select Identity server and agent on Microsoft Windows NT Domain systems. At the end of this chapter, you will know about

- Software requirements to install the NT Domain connector.
- Prerequisite conditions to install NT Domain connector.
- Procedure to install NT Domain connector.

NT Domain Connector Files

The NT Domain connector is packaged in the following files in the `NTLocal` directory on the Select Identity Connector CD:

Table 3 NT Domain Connector Files

Serial Number	File Name	Description
1	`NTConnector.rar`	The Resource Adapter Archive (RAR) file contains the connector binaries.
2	`NTschema.jar`	The Schema file contains the mapping files that contain attribute information of Microsoft Windows NT Domain .
3	`NTDomainSetup.zip`	The zip file contains the executable to install the agent.

System Requirements

The NT Domain connector is supported in the following environment:

Table 4 Platform Matrix for NT Domain connector

Select Identity Version	Application Server	Database
3.0.2	WebLogic 8.1.2 on Windows 2003	Microsoft SQL Server 2000
	WebLogic 8.1.2 on Solaris 9	Oracle 9i
	WebLogic 8.1.2 on HP-UX 11i	Oracle 9i
3.3	WebLogic 8.1.4 on Windows 2003	Microsoft SQL Server 2000
	WebLogic 8.1.4 on Solaris 9	Oracle 9i
	WebLogic 8.1.4 on Red Hat Enterprise Linux 3.0	Microsoft SQL Server 2000
3.3.1	WebLogic 8.1.4 on Windows 2003	Microsoft SQL Server 2000
	WebSphere 5.1.1 on HP-UX 11i	Oracle 9i
4.0/4.01.000	The NT Domain connector is supported on all the platform configurations of Select Identity 4.0 and 4.01.000.	

This connector is supported on Windows NT 4.0 Domain servers. Internet Explorer (IE) version 6.x is also required on the resource, and the domain of the application server and NT Domain server must be registered in DNS before you can install this connector..

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

Installing the Connector RAR

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

4 Installing the Agent

After you install the NT Domain connector on the Select Identity server, you can install the agent on the Windows NT-based system. The agent is a suite of services and support DLLs deployed on the resource.

The following environment is required:

- Microsoft Windows NT Server or Workstation (Service Pack 6 or later) with Domain Controller, or Windows 2000 Server with Domain Controller
- Internet Explorer 5.5 or later (supporting MSXML 2.0 or later)
- Winsock 2.0 or later

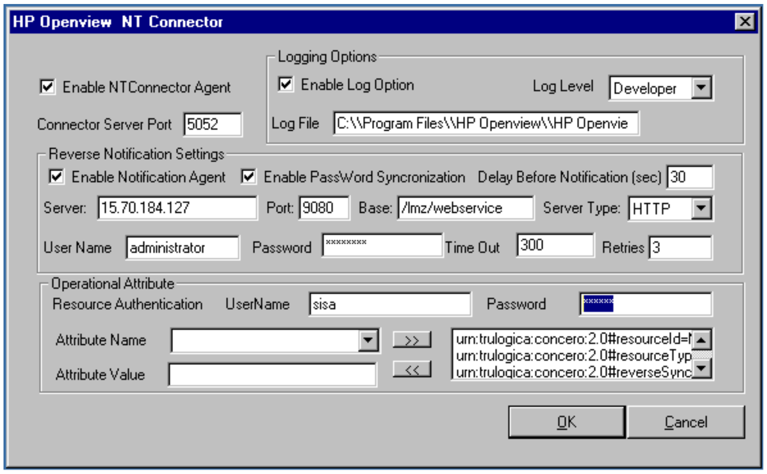
You also need the administrative user name and password to log on to the system during the installation.

Installation Procedure

Perform the following to install the agent on the Microsoft Windows NT Domain server:

1. Copy the `NTSetup.zip` file from the Select Identity Connector CD to a directory on the NT Domain server.
2. Extract the `NTSetup.zip` file.
3. Double-click `SETUP.exe` to start the installation program.
4. Click **Next** to proceed through the installation.
5. If needed, provide administrative logon information when prompted.

Configure the NT Connector agent options. The configuration is defined on the HP Openview NT Connector dialog..



HP Openview NT Connector

☑ Enable NTConnector Agent

Connector Server Port: 5052

Logging Options

☑ Enable Log Option

Log Level: Developer

Log File: C:\\Program Files\\HP Openview\\HP Openvie

Reverse Notification Settings

☑ Enable Notification Agent ☑ Enable PassWord Syncronization

Delay Before Notification (sec): 30

Server: 15.70.184.127 Port: 9080 Base: /lmz/webservice Server Type: HTTP

User Name: administrator Password: ******** Time Out: 300 Retries: 3

Operational Attribute

Resource Authentication UserName: sisa Password: ******

Attribute Name:

Attribute Value:

urn:trulogica:concero:2.0#resourceId=I
urn:trulogica:concero:2.0#resourceTyp
urn:trulogica:concero:2.0#reverseSync

a Select the **Enable NT Connector Agent** check box. This starts the connector, enabling it to receive provisioning requests from Select Identity.

b Enter a port number for the agent in the Connector Server Port field. The connector uses this port to communicate with the agent. The default is 5052.

c Select the **Enable Log Option** check box.

6 Configure the following settings for reverse synchronization. Perform these steps if you want to synchronize changes made to users on the NT Domain server with Select Identify.

a Select the **Enable Notification Agent** option.

b If you want to synchronize the NT Domain server password with Select Identity, select **Enable Password Synchronization**. This is used by the agent to synchronize user account password changes 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 Delay Before Notification field, enter the number of seconds between requests sent to Select Identity.

d In the Server field, enter the IP address or fully-qualified name of the server running Select Identity.

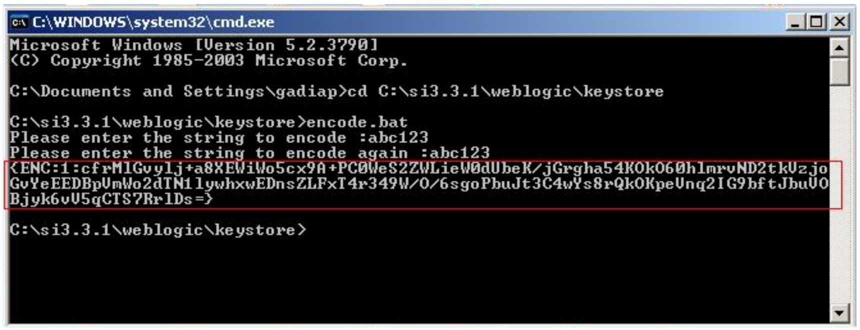
e In the Port field, enter the port on which Select Identity listens for reverse synchronization requests. For example, on WebLogic, the default is 7001.

f Enter the base URL for the Select Identity Web Service in the Base field. The default value is /lmz/webservice/.

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

h Enter the name of a user that has administrative privileges on the NT Domain server in the User Name field.

i 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:



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\gadiap>cd C:\si3.3.1\weblogic\keystore

C:\si3.3.1\weblogic\keystore>encode.bat
Please enter the string to encode :abc123
Please enter the string to encode again :abc123
<ENC:1:cfrMlGvylj+a8XEWiWo5cx9A+PC0WeS2ZWLieW0dUbeK/jGrgha54KOkO60hlmrvND2tkVzjo
GvYeEEDBpVmWo2dTN1lywhxwEDnsZLFxT4r349W/O/6sgoPbuJt3C4wYs8rQkOKpeVnq2IG9bftJbuVO
Bjyk6vV5qCTS7RrlDs=>

C:\si3.3.1\weblogic\keystore>
```

j Keep the **TimeOut** and **Retries** settings.

k In the UserName field (in the Operational Attribute section), enter the name of the administrator account in Select Identity. The default is sisa.

l Enter the password of the administrative account in Select Identity in the Password field.

m Add 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 addition.

— Attribute Name: **`urn:trulogica:concero:2.0#resourceId`**

Attribute Value: ***`resource_name`***

This is the name of the resource that you add in Select Identity for this NT server. For example, if you specify **`NT_Domain`** here, then specify **`NT_Domain`** as the resource name in Select Identity.

— Attribute Name: **`urn:trulogica:concero:2.0#reverseSync`**

Attribute Value: **`true`**

— Attribute Name: **`urn:trulogica:concero:2.0#resourceType`**

Attribute Value: **`ntdomain`**

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.

7 After defining all of your settings, click **OK**.

8 After the installation is complete, click **Finish**.

9 Restart the server.

The installation process performed the following:

- Created the target directory with the binaries and support files in the appropriate folders. Placed `TLPassfilt.dll` and `TLUtils.dll` in the Windows System directory, $WinSysPath$ (`c:\winnt\system32`). The following is the folder structure created:

  — `<TARGETDIR>` — The parent folder

  — `<TARGETDIR>\Bin` — Program binaries

  — `<TARGETDIR>\Logs` — Connector log folder

  — `<TARGETDIR>\Map` — Mapping of operational attributes

- `<TARGETDIR>\Servers` — Server binaries

- Created and configured corresponding services.
- Created a Program group and shortcuts for the connector configuration console and the uninstall script.
- Set up the registry for program parameters.

5 Configuring the Connector with Select Identity

This chapter describes the procedure to configure the NT Domain connector with Select Identity. At the end of this chapter, you will know the procedure to configure the NT Domain 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 NT Domain 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/NT`**.
- Select No for the Mapper Available section.

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

Add a New Resource

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

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

Table 5 Resource Configuration Parameters

Field Name	Sample Values	Description	Comment
Resource Name	nt_server	Name given to the resource. If you enabled reverse synchronization, this must be the same as the value provided for the urn:trulogica:concero:2.0#resourceId attribute on the agent console.	
Connector Name	NTDomain	The newly deployed connector.	On Select Identity 3.3.1, this field is called Resource Type.
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 this connector, select this option.	Applicable only to Select Identity 3.3.1.
Domain	mydomain.com	The name of the NT domain.	
Username	Administrator	Administrative account on the target resource.	

Table 5 Resource Configuration Parameters

Field Name	Sample Values	Description	Comment
Password	Password123	Password corresponding to the administrative account.	
Resource Name	nt_server	Name given to the resource. If you enabled reverse synchronization, this must be the same as the value provided for the urn:trulogica:concero:2.0#resourceId attribute on the agent console.	
Server Name	server.company.com	The NETBIOS name or IP address of the NT Domain server.	

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

Map Attributes

After successfully adding a resource for the NT Domain 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 Windows NT Local Mapping Information

Select Identity Resource Attribute	NT Domain User Attribute	Label on NT Domain UI	Description
User Name	UserId	User Logon Name	Primary key for NT Domain and NT Local User. *This attribute is mandatory and must be mapped.*
Password	Password	Password	The user's password. *This attribute is mandatory and must be mapped.*
[First Name] [Last Name]	FullName	Full Name	The user's full name. *This attribute is mandatory and must be mapped.*

Table 6 Windows NT Local Mapping Information

Select Identity Resource Attribute	NT Domain User Attribute	Label on NT Domain UI	Description
Description	Comment	Description	Description of the user.
CountryId	Country	Country	A DWORD value that indicates the country or region code.
ScriptPath	ScriptPath	Logon Script Name	The path to the user's logon script file, which can be a .CMD, .EXE, or .BAT file.
HomeDirectory	HomeDirectory	Home Directory: Local path or Home Directory: To (depending on HomeDirectory-Drive)	A home share or a local directory path, but not both.
PasswordExpiresFla g	PasswordExpired	Password Expires	An option that expires the user’s password.
(not mapped by default)	UserComment	User Comment	A comment by the user.

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

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 will 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 synchroniation 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 will be created in Select Identity but will not be assigned to a Service.

6 Uninstalling the Connector

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

1 Remove all the resource dependency.

2 Delete the connector from Select Identity homepage.

3 Uninstall the connector from application server. For more information on this, refer to Connector Integration Guide.

4 Uninstall the agent

See *HP OpenView 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 NT Domain system:

1 From the Start menu, select **Programs** → **HP OpenView NT Domain Connector** → **Uninstall Agent**.

2 Complete the installation as prompted by the wizard.