HP OpenView Select Identity

Connector for Windows NT Local Systems

Installation and Configuration Guide

Connector Version: 3.4
Select Identity Version: 3.3.1

August 2005

Legal Notices

Warranty

- 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.

Support

Please visit the HP OpenView web site at:

http://www.managementsoftware.hp.com/

This web site provides contact information and details about the products, services, and support that HP OpenView offers.

You can also go directly to the support web site at:

http://support.openview.hp.com/

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 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://support.openview.hp.com/access_level.jsp

To register for an HP Passport ID, go to:

https://passport2.hp.com/hpp/newuser.do

contents

Installing the Connector

The Windows NT Local connector enables HP OpenView Select Identity to provision in the local domain on Windows NT, XP, and 2000 systems. This connector is a two-way connector and can send data back to Select Identity based on changes made in the local domain.

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

- `NTLConnector.rar` — Contains the binaries.

- `NTLschema.jar` — Contains the following attribute mapping files, which control how Select Identity fields are mapped to Windows NT Local fields:

  - `NTLUser.properties` — Maps user attributes from the Select Identity User Model to Windows user attributes.

  - `NTLGroup.properties` — Maps group attributes from the Select Identity Group Model to Windows group attributes.

  - `ntlocal.xsl` — Maps attributes on the Windows server to attributes on the Select Identity server. This file is used by the agent during reverse synchronization.

- `NTLSetup.zip` — Contains the installation executable for the NT Local agent.

Operations Supported by the Connector

The Windows NT Local connector enables Select Identity to perform the following provisioning tasks on Windows NT, XP, and 2000 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
- Assign and unassign entitlements to and from users

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	If the Resource is Authoritative	If the Resource is Non-authoritative
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.	Attributes are updated in Select Identity.	Attributes are not updated in Select Identity.
User entitlements are modified on the resource.	Entitlements are modified in Select Identity.	Entitlements are modified in Select Identity.

Operation	If the Resource is Authoritative	If the Resource is Non-authoritative
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.

Additional configuration steps are required to enable reverse synchronization.

System Requirements

The Windows NT Local connector is supported in the following environment:

Select Identity Version	Application Server	Database
3.0.2	WebLogic 8.1.2 on Windows 2003	SQL Server 2000
	WebLogic 8.1.2 on Solaris 9	Oracle 9i
	WebLogic 8.1.2 on HP-UX 11i	Oracle 9i
	WebSphere 5.1.1 on Solaris 9	DB2 8.2 (or DB2 8.1 Service Pack 7)
3.3	WebLogic 8.1.4 on Windows 2003	SQL Server 2000
	WebLogic 8.1.4 on Solaris 9	Oracle 9i
	WebLogic 8.1.4 on Red Hat Enterprise Linux 3.0	SQL Server 2000
3.3.1	WebLogic 8.1.4 on Windows 2003	SQL Server 2000
	WebSphere 5.1.1 on HP-UX 11i	Oracle 9i

This connector is supported with Windows NT 4.0, Windows 2000, Windows 2003, and Windows XP.

The agent is supported in the following environment:

Operating system	• Microsoft Windows NT Server/Workstation, Service Pack 6 or later
	• Windows XP Professional, Service Pack 1
	• Windows 2000 Professional, Service Pack 4
	• Windows 2000 Server
Browser	Internet Explorer 5.5 or later (supporting MSXML 2.0 or later)
Winsock	Version 2.0 or later

You will also need the administrative user name and password for the machine during the installation.

Deploying on the Web Application Server

To install the Windows NT Local connector on the Select Identity server, complete these steps:

1   Create a subdirectory in the Select Identity home directory where the connector's RAR file will reside. For example, you could create the `C:\Select_Identity\connectors` folder on Windows. (A connector subdirectory may already exist.)

2   Copy the `NTLConnector.rar` file from the Select Identity Connector CD to the connector subdirectory.

3   If deploying the connector on WebLogic, complete the following steps. If deploying on WebSphere, skip to .

   a   Create a schema subdirectory in the Select Identity home directory where the connector's mapping file(s) will reside. For example, you could create the `C:\Select_Identity\schema` folder. (This subdirectory may already exist.)

b Extract the contents of the NTLschema.jar file (on the Select Identity Connector CD) to the schema subdirectory.

c Ensure that the CLASSPATH environment variable in the WebLogic server startup script references the schema subdirectory.

d Start the application server if it is not currently running.

e Log on to the WebLogic Server Console.

f Navigate to *My_domain* →**Deployments** →**Connector Modules**.

g Click **Deploy a New Connector Module**.

h Locate and select the NTLConnector.rar file from the list. It is stored in the connector subdirectory.

i Click **Target Module**.

j Select the **My Server** (your server instance) check box.

k Click **Continue**. Review your settings.

l Keep all default settings and click **Deploy**. The Status of Last Action column should display Success.

4 If deploying the connector on WebSphere, complete the following steps:

a Stop the application server.

b Extract the contents of the NTLschema.jar file (on the Select Identity Connector CD) to the WebSphere\AppServer\lib\ext directory.

c Start the application server.

d Log on to the WebSphere Application Server Console.

e Navigate to **Resources** →**Resource Adapters**.

f Click **Install RAR**.

g In the Server path field, enter the path to the NTLConnector.rar file. It is stored in the subdirectory created in Step 1.

h Click **Next**.

i In the Name field, enter a name for the connector.

j Click **OK**.

k Click the **Save** link (at the top of the page).

l   On the Save to Master Configuraton dialog, click the **Save** button.

m   Click **Resources** →**Resource Adapters**.

n   Click the new connector.

o   Click **J2C Connection Factories** in the Additional Properties table.

p   Click **New**.

q   In the Name field, enter the name of the factory for the connector. For the SQL connector, enter **eis/NTL**.

r   Click **OK**.

s   Click the **Save** link.

t   On the Save to Master Configuraton dialog, click the **Save** button.

u   Restart WebSphere.

5   Modify the mapping files, if necessary. See Understanding the Mapping Files on page 17 for details.

6   To configure reverse synchronization on the server, extract the ntlocal.xsl file from the NTLschema.jar to the Select Identity home directory. This file maps user attributes on the Windows server to attributes in Select Identity.

Because the attributes in the ntlocal.xsl file are based on those in the NTLUser.properties and NTLGroup.properties files, you must modify the ntlocal.xsl file to reflect changes made to these files (Step 5).

After installing the connector, see Configuring the Connector on page 23 for information about registering and configuring the connector in Select Identity.

Installing the Agent on the Windows Server

After you install the Windows NT Local connector on the Select Identity server, you can install the agent on the Windows server. The agent is a suite of Services and support DLLs deployed on the resource. Perform the following to install the agent:

1   Copy the `NTLSetup.zip` file from the Select Identity Connector CD to a directory on the NT Local server.

2   Extract the 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.

    Configuration is defined on the NTL Connector page.

6   Configure the Enable NTL Connector Agent options, as follows:

    a   Select the **Enable NTL Connector Agent** check box. This enables the agent to receive and send data to the connector.

    b   Select the **Enable Log Options** check box, which enables the agent to log events.

    c   Enter the port for the agent in the Connector Server Port field. The default is 5000. The agent uses this port to listen for provisioning requests from Select Identity.

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

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

    b   If you want to synchronize the Windows 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 Windows 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:

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

k   In the UserName field (in the Operational Attribute section), enter the administrator account name 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_LocalMachine** here, then specify **NT_LocalMachine** 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: **ntlocal**

This is the name of the XSL file (without the .xsl extension), which provides reverse mappings for the agent to send data to Select Identity.

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

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

10 Restart the server.

The install process performed the following:

- Creates the target directory with the binaries and support files in the appropriate folders. Places `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>\Lib`
    Connector library folder

  — `<TARGETDIR>\Logs`
    Connector log folder

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

  — `<TARGETDIR>\Servers`
    Server binaries

- Creates and configures corresponding services.

- Creates a Program group and shortcuts for the connector configuration console and the uninstall script.

- Sets up the registry for program parameters.

2

Understanding the Mapping Files

The NT Local connector is deployed with the following mapping files:

- `NTLUser.properties`
- `NTLGroup.properties`

These files reside in the `NTLSchema.jar` file and map user account additions and modifications from Select Identity to the system resource. When you deploy a resource using the Resources page of the Select Identity client, you can review these files.

In addition, the NT Local connector provides the `ntlocal.xsl` file, which maps attributes in Windows to those in Select Identity (reverse mapping). Configure this file if you wish to support reserve synchronization.

You can create attributes that are specific to Select Identity using the Attributes page in the Select Identity client. These attributes can be used to associate Select Identity user accounts with system resources by editing the connector mapping file described in this chapter. This process becomes necessary because, for example, a single attribute "username" can have a different name on different resources, such as "user" for UNIX, "UID" for a database, and "UserID" on a Windows server.

The mapping files do not need to be edited unless you want to map additional attributes to your resource. If attributes and values are not defined in the mapping files, they cannot be saved to the resource through Select Identity.

User Attributes

The `NTLUser.properties` file is a text file that maps each Select Identity attribute to an attribute on the resource; the attributes are delimited by |. Consider this excerpt:

```
User Name|UserId
```

The Select Identity user attribute is named User Name and it is mapped to the UserId attribute on the NT Local resource.

Attributes can be concatenated. The attribute names and the separators must not contain the | delimiter. For concatenation, the format is as follows:

```
[<SI Attribute>]<separator>[<SI Attribute>]|<Resource Attribute>
```

as in this example:

```
[First Name], [Middle Name] [Last Name]| FullName
```

where First Name and Last Name are attributes in Select Identity. They are concatenated to form the value of the FullName attribute in NT. A space is used as a separator between the two Select Identity attributes.

It is necessary to use the NT User Attribute Name column for mapping in the user properties file.

The following table provides a list of all NT attributes that you can map if you wish to provision users with this information. Here is a description of the columns provided in the table:

- **Select Identity Resource Attribute**— The attribute used by the NT Local connector, as defined in the mapping file.

- **NT Attribute —** The name of the attribute on the Windows server.

- **Label on NT UI** — The name of the property on the Windows UI that corresponds to the attribute on the Windows server.

- **Description** — A description of the attribute and any noteworthy information needed when assigning values to the attribute.

The primary key for Windows NT Local is UserId. This attribute must be mapped to an attribute in Select Identity in order for user information to be stored on the Windows server. It should be the first entry in `NTLUser.properties` and Password needs to be the second entry.

Select Identity Attribute	NT Attribute	Label on NT 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	User's password; *this attribute is mandatory and must be mapped.*
First Name + Last Name	FullName	Full Name	Full name; *this attribute is mandatory and must be mapped.*
Description	Comment	Description	Description.
UserComment	User Comment	User Comment	A user comment.
ProfilePath	`Profile Path` (not available for NT Workstation)	User Profile Path	A path to the user's profile. This value can be a null string, a local absolute path, or a UNC path.
ScriptPath	ScriptPath	Logon Script Name	The path for the user's logon script file. The script file can be a .CMD file, an .EXE file, or a .BAT file.
HomeDirectory Drive	`Home Directory Drive`	Home Directory: Connect	The local directory path. Not available for NT Workstation.

Group Attributes

The `NTLGroup.properties` file is a text file that maps each Select Identity group attribute to an attribute on the resource; the attributes are delimited by |. Consider this excerpt:

```
GroupId|GroupId
```

The Select Identity user attribute is named GroupId and it is mapped to the GroupId attribute on the NT Local resource. The attributes are named the same in this example but need not be.

Attributes can be concatenated. The attribute names and the separators must not contain the | delimiter. For concatenation, the format is as follows:

```
[<SI Attribute>]<separator>[<SI Attribute>]|<Resource Attribute>
```

Use the NT Group Attribute column for mapping in the group properties file.

The primary key for Windows NT Group is GroupId and needs to be mapped to an attribute of in the Select Identity Group Model. This attribute must be the first entry in `NTLGroup.properties` file.

Select Identity Attribute	NT Attribute Name	Label on NT UI	Description
GroupId	GroupId	Group Name	Primary Key for the NT Local Group
Description	Comment	Description	Description

Reverse Synchronization

The agent can send changes made to user attributes on the Windows server to the Select Identity server. The agent sends an SPML request to the Select Identity server that contains the attribute changes. The names of the attributes in the SPML request are defined by Windows. To transform the attribute names to Select Identity attribute names, the request is parsed by Select Identity using the `ntlocal.xsl` file.

The `NTLUser.properties` file contains generic Windows attributes that are typically used when a user is created. As described above, you can configure this file to include or exclude attributes. Any addition or deletion of attributes in `NTLUser.properties` must also be made in `ntlocal.xsl`. Each block in `ntlocal.xsl` corresponds with each attribute entry in `NTLUser.properties`.

If the following mapping is added to `NTLUser.properties`:

SI_RESOURCE_ATTRIBUTE|*NT_ATTRIBUTE*

You must add the following block to `ntlocal.xsl`:

```
<xsl:when test="$ATTRNAME =' NT_ATTRIBUTE' ">
  <xsl:call-template name="AttributeBuilder">
    <xsl:with-param name="DSMLELEMENT" select="$DSMLELEMENT"/>
    <xsl:with-param name="ATTRNAME" select="'
     SI_RESOURCE_ATTRIBUTE' "/>
    <xsl:with-param name="ATTRVALUE" select="$ATTRVALUE"/>
    <xsl:with-param name="MODIFYFLAG" select="$MODIFYFLAG"/>
  </xsl:call-template>
</xsl:when>
```

where *NT_ATTRIBUTE* represents the attribute passed from the Windows server and *SI_RESOURCE_ATTRIBUTE* represents the attribute defined by Select Identity and displayed in the resource attributes list.

▶ Note that the XSL file is case sensitive; attributes must be specified exactly as they exist in Select Identity and on the resource. For example, if the mail attribute is defined in Windows, you must specify **mail**, not **Mail** or **MAIL**, and so on.

The following is an example. The mail attribute is added to `NTLUser.properties`, as follows:

Email|mail

Then, the following block is added to `ntlocal.xsl`:

```
<xsl:when test="$ATTRNAME = 'mail'">
  <xsl:call-template name="AttributeBuilder">
    <xsl:with-param name="DSMLELEMENT" select="$DSMLELEMENT"/>
    <xsl:with-param name="ATTRNAME" select="'Email'"/>
    <xsl:with-param name="ATTRVALUE" select="$ATTRVALUE"/>
    <xsl:with-param name="MODIFYFLAG" select="$MODIFYFLAG"/>
  </xsl:call-template>
</xsl:when>
```

where **mail** represents the attribute passed from the Windows server and **Email** represents the attribute in Select Identity.

For composite attributes defined in the NTLUser.properties file, such as [First Name] [Last Name], you must provide two attribute name-value pairs in the ntlocal.xsl file. For example, for the following entry in NTLUser.properties:

```
[First Name] [Last Name]|displayname
```

The ntlocal.xsl file must contain the following:

```
<xsl:when test="$ATTRNAME = 'displayname'">
  <xsl:choose>
    <xsl:when test="contains($ATTRVALUE, ' ')">
      <!-- First Name is before space char -->
      <xsl:call-template name="AttributeBuilder">
        <xsl:with-param name="DSMLELEMENT" select="$DSMLELEMENT"/>
        <xsl:with-param name="ATTRNAME" select="'First Name'"/>
        <xsl:with-param name="ATTRVALUE"
         select="substring-before($ATTRVALUE, ' ')"/>
        <xsl:with-param name="MODIFYFLAG" select="$MODIFYFLAG"/>
      </xsl:call-template>
      <!-- Last Name is after space char -->
      <xsl:call-template name="AttributeBuilder">
        <xsl:with-param name="DSMLELEMENT" select="$DSMLELEMENT"/>
        <xsl:with-param name="ATTRNAME" select="'Last Name'"/>
        <xsl:with-param name="ATTRVALUE"
         select="substring-after($ATTRVALUE, ' ')"/>
        <xsl:with-param name="MODIFYFLAG" select="$MODIFYFLAG"/>
      </xsl:call-template>
    </xsl:when>
    <xsl:otherwise>
      <!-- If no space, take the whole string as First Name -->
      <xsl:call-template name="AttributeBuilder">
        <xsl:with-param name="DSMLELEMENT" select="$DSMLELEMENT"/>
        <xsl:with-param name="ATTRNAME" select="'First Name'"/>
        <xsl:with-param name="ATTRVALUE" select="$ATTRVALUE"/>
        <xsl:with-param name="MODIFYFLAG" select="$MODIFYFLAG"/>
      </xsl:call-template>
    </xsl:otherwise>
  </xsl:choose>
</xsl:when>
```
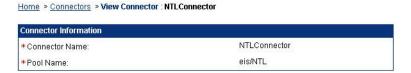
3

Configuring the Connector

After you deploy the connector on the application server, you must configure Select Identity to use the connector by deploying it in the Select Identity client. The following provides an overview of the procedures you must complete in order to deploy your connector. It also provides connector-specific information you must provide when configuring Select Identity to use the connector.

1 Register the connector with Select Identity by clicking the **Deploy New Connector** button on the Connectors home page. Complete this procedure as described in the "Connectors" chapter of the *HP OpenView Select Identity Administrator Guide*.

   After you deploy the connector, the connector properties will look similar to this:

   Home > Connectors > **View Connector** : **NTLConnector**

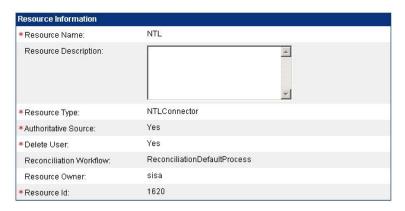 | Connector Information | |
   | --- | --- |
   | *Connector Name: | NTLConnector |
   | *Pool Name: | eis/NTL |

2 Deploy a resource that uses the newly created connector. On the Resources home page, click the **Deploy New Resource** button. When

configuring the resource, refer to the following for parameters specific to this connector:

Field Name	Sample Values	Description
Resource Name	local_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.
Resource Type	NT	The connector that was deployed in Step 1 on page 23.
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.
UserName	Administrator	Administrative account on the target resource.
Password	Password123	Password corresponding to the administrative account.
Server	server.company.com	Target resource NETBIOS name or IP address.
ServerPort	5001	Forward connector server port, as configured on the resource agent.

* Instead of creating an authoritative resource, you can create authoritative attributes (in the next step) for the attributes that will be synchronized.

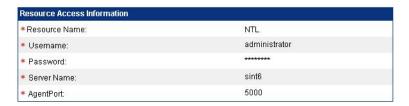Entitlements are authoritative by default in a non-authoritative resource but other attributes are not.

Complete the steps in this procedure as described in the "Resources" chapter of the *HP OpenView Select Identity Administrator Guide*. After you deploy the resource for the connector, the Basic Info page of the resource properties will look similar to this:

Resource Information	
* Resource Name:	NTL
Resource Description:	
* Resource Type:	NTLConnector
* Authoritative Source:	Yes
* Delete User:	Yes
Reconciliation Workflow:	ReconciliationDefaultProcess
Resource Owner:	sisa
* Resource Id:	1620

The Additional Info page will look similar to this:

Resource Information	
Resource Name:	NTL
☑ Manage User	
Associate to Group:	☑

The Access Info page will look similar to this:

Resource Access Information	
* Resource Name:	NTL
* Username:	administrator
* Password:	********
* Server Name:	sint6
* AgentPort:	5000

3 Create attributes that link Select Identity to the connector. For each mapping in the connector's mapping file, create an attribute using the Attributes capability on the Select Identity client.

Refer to the "Attributes" chapter in the *HP OpenView Select Identity Administrator Guide* for more information. After you create the attributes

for the connector, the View Attributes page for the resource will look similar to this:

(Resource Name=NTL)				
◁◁ ◁ Page 1 of 1 ▷ ▷▷				Total Records:10
Name	**Min Length**	**Max Length**	**Attribute Mapped To**	**Authoritative**
CountryId	0	255	Country	N
Description	0	255	Description	N
First Name	0	255	FirstName	N
HomeDirectory	0	255	HomeDirectory	N
Last Name	0	255	LastName	N
NTL_ENTITLEMENTS	1	255	NTL_ENTITLEMENTS	Y
NTL_KEY	1	255	NTL_KEY	Y
Password	0	255	Password	N
ScriptPath	0	255	ScriptPath	N
User Name	0	255	UserName	N

4   Create a Service that will use the newly created resource. To do so, click the **Deploy New Service** button on the Services home page. Complete this procedure as described in "Services" of the *HP OpenView Select Identity Administrator Guide*. You will reference your new resource created in Step 2 while creating this service.

If you are enabling 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.

4

Uninstalling the Connector

If you need to uninstall a connector from Select Identity, make sure that the following are performed:

*   All resource dependencies are removed.
*   The connector is deleted using the Select Identity client Connectors pages.

Uninstalling the Connector from WebLogic

Perform the following to delete a connector:

1   Log on to the WebLogic Server Console.
2   Navigate to *My_Domain* →**Deployments** →**Connector Modules**.
3   Click the delete icon next to the connector that you want to uninstall.
4   Click **Yes** to confirm the deletion.
5   Click **Continue**.

Uninstalling the Connector from WebSphere

Complete the following steps to uninstall the connector on WebSphere:

1   Log on to the WebSphere Application Server Console.

2   Navigate to **Resources** →**Resource Adapters**.

3   Select the connector to uninstall.

4   Click **Delete**.

5   Click the **Save** link (at the top of the page).

6   On the Save to Master Configuraton dialog, click the **Save** button.

Uninstalling the Agent

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

1   From the Start menu, select **Programs** →**HP OpenView NTLocalConnector** → **Uninstall Agent**.

2   Complete the installation as prompted by the wizard.