HP OpenView Select Identity

Connector for Microsoft Windows NT Domain Systems

Installation and Configuration Guide

Connector Version: 3.4
Select Identity Version: 3.3.1

August 2005

Legal Notices

Warranty

Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices

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

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

HP OpenView Select Identity is a trademark of Hewlett-Packard Development Company, L.P.

Microsoft, Windows, the Windows logo, and SQL Server are trademarks or registered trademarks of Microsoft Corporation.

Sun™ workstation, Solaris Operating Environment™ software, SPARCstation™ 20 system, Java technology, and Sun RPC are registered trademarks or trademarks of Sun Microsystems, Inc. JavaScript is a trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

This product includes the Sun Java Runtime. This product includes code licensed from RSA Security, Inc. Some portions licensed from IBM are available at http://oss.software.ibm.com/icu4j/.

IBM, DB2 Universal Database, DB2, WebSphere, and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group.

This product includes software provided by the World Wide Web Consortium. This software includes xml-apis. Copyright © 1994-2000 World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. http://www.w3.org/Consortium/Legal/

Intel and Pentium are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

AMD and the AMD logo are trademarks of Advanced Micro Devices, Inc.

BEA and WebLogic are registered trademarks of BEA Systems, Inc.

VeriSign is a registered trademark of VeriSign, Inc. Copyright © 2001 VeriSign, Inc. All rights reserved.

All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

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

Chapter 1 Installing the Connector 7
Operations Supported by the Connector 8
System Requirements. 10
Deploying on the Web Application Server. 10
Installing the Agent on the Windows Server 12

Chapter 2 Understanding the Mapping Files 17
User Attributes. 18
Reverse Synchronization 21

Chapter 3 Configuring the Connector 24

Chapter 4 Uninstalling the Connector 29
Uninstalling the Connector from WebLogic 29
Uninstalling the Agent. 30

1

Installing the Connector

The 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 is packaged in the following files, which are located in the `NTDomain` directory on the Select Identity Connector CD:

- `NTConnector.rar`— contains the binaries for the connector.
- `ntschema.jar`— contains the following mapping files, which control how Select Identity fields are mapped to NT Domain fields:
  - `ntuser.properties` — maps the Select Identity user attributes to the Windows user attributes.
  - `ntgroup.properties` — maps the Select Identity group attributes to Windows group attributes. Group provisioning is not currently supported, though this file must be extracted during installation.
  - `ntdomain.xsl` — maps attributes on the NT Domain server to attributes on the Select Identity server. This file is used by the agent during reverse synchronization.
- `NTDomainSetup.zip` — contains the installation executable for the agent.

Operations Supported by the Connector

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
- Assign and unassign entitlements to and from users

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.

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.	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.
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 NT Domain 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
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 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.

Deploying on the Web Application Server

To install the NT Domain 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 `NTConnector.rar` file from the Select Identity Connector CD to the connector subdirectory.

3. 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.)
4. Extract the contents of the `ntschema.jar` file (on the Select Identity Connector CD) to the schema subdirectory.
5. Ensure that the CLASSPATH environment variable in the WebLogic server startup script references the schema subdirectory.
6. Start the application server if it is not currently running.
7. Log on to the WebLogic Server Console.
8. Navigate to ***My_domain*** →**Deployments** →**Connector Modules**.
9. Click **Deploy a New Connector Module**.
10. Locate and select the `NTConnector.rar` file from the list. It is stored in the connector subdirectory.
11. Click **Target Module**.
12. Select the **My Server** (your server instance) check box.
13. Click **Continue**. Review your settings.
14. Keep all default settings and click **Deploy**. The Status of Last Action column should display Success.
15. Modify the mapping files, if necessary. See Understanding the Mapping Files on page 17 for details.
16. To configure reverse synchronization on the server, extract the `ntdomain.xsl` file from the `ntschema.jar` to the Select Identity home directory. This file maps user attributes on the NT Domain server to attributes in Select Identity.

    Because the attributes in the `ntdomain.xsl` file are based on those in the `ntuser.properties` and `ntgroup.properties` files, you must modify the `ntdomain.xsl` file to reflect changes made to these files (Step 15).

After installing the connector, see Configuring the Connector on page 24 for information about registering and installing the connector in Select Identity.

Installing the Agent on the Windows Server

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:

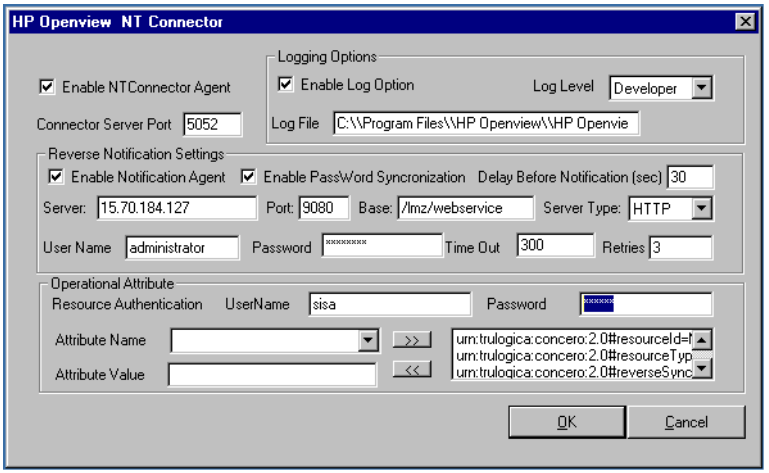
- Microsoft Windows NT Server or Workstation (Service Pack 6 or later) with Domain Controller, or Windows 2000 Server with Domain Controller
- Internet Explorer 5.5 or later (supporting MSXML 2.0 or later)
- Winsock 2.0 or later

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

Perform the following to install the agent:

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.

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



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.

7 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.

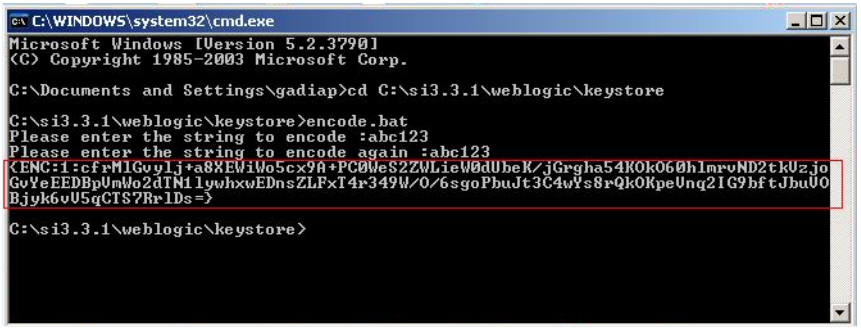
e In the Port field, enter the port on which Select Identity listens for reverse synchronization requests. For example, on WebLogic, the default is 7001.

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:



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.

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

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

10 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.

2

Understanding the Mapping Files

This connector is deployed with the following mapping files:

- `ntuser.properties`
- `ntgroup.properties`

These files contain the attributes required by the resource and are used to map user and group account additions and modifications from Select Identity to the system resource. When you deploy a resource through the Resources home page on the Select Identity client, you can review these files.

Note that the `ntgroup.properties` file is installed with the NT Domain connector and must be present on the system, but group provisioning is not supported at this time.

In addition, the NT Domain connector provides the `ntdomain.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 home page on the Select Identity client. You can then use these attributes to associate Select Identity user accounts with system resources by mapping the attributes in the connector mapping file described in this chapter. This process becomes necessary because, for example, a single attribute “username” can have a different definition on three different

resources, such as “login” for UNIX, “UID” for a database, and “userID” on a Windows server. However, you do not need to edit the `ntuser.properties` file unless you want to map additional attributes to your resource.

User Attributes

The `ntuser.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 Domain 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] [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 Domain. A space is used as a separator between the two Select Identity attributes.

The `ntuser.properties` file provides the mandatory mappings that must be configured for Select Identity to provision users on the NT Domain server. The primary key is UserId; this NT Domain attribute must be mapped to a Select Identity attribute in order for user information to be stored on the NT Domain server. It should be the first entry in `ntuser.properties`, and Password must be the second mapping in the file.

The following table provides a list of all NT Domain 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 Domain connector, as defined in the mapping file.
- **NT Domain User Attribute —** The name of the attribute on the Windows server.

- **Label on NT Domain 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.

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.*
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.

Select Identity Resource Attribute	NT Domain User Attribute	Label on NT Domain UI	Description
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.
PasswordExpires Flag	PasswordExpired	Password Expires	An option that expires the user's password.
(not mapped by default)	UserComment	User Comment	A comment by the user.
(not mapped by default)	ProfilePath (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.
(not mapped by default)	HomeDirectory Drive (not available for NT Workstation)	Home Directory: Connect	If a valid drive letter is specified, the HomeDirectory becomes a share path; otherwise, it is considered to be a local directory path.

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 `ntdomain.xsl` file.

The `ntuser.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 `ntuser.properties` must also be made in `ntdomain.xsl`. Each block in `ntdomain.xsl` corresponds with each attribute entry in `ntuser.properties`.

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

SI_RESOURCE_ATTRIBUTE|*WIN_ATTRIBUTE*

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

```
<xsl:when test="$ATTRNAME ='WIN_ATTRIBUTE' ">
  <xsl:call-template name="AttributeBuilder">
    <xsl:with-param name="DSMLELEMENT" select="$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 *WIN_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 `ntuser.properties`, as follows:

`Email`|**`mail`**

Then, the following block is added to ntdomain.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 Windowsserver and **Email** represents the attribute in Select Identity.

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

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

The ntdomain.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 is 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:

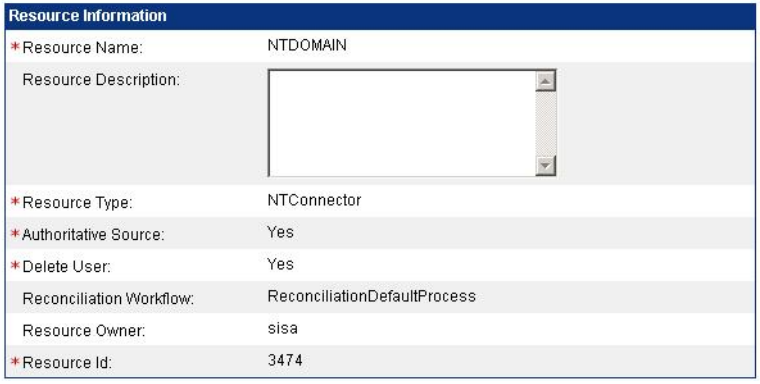
2 Deploy a resource that uses the newly created connector. On the Resources home page, click the **Deploy New Resource** button. When configuring the resource, refer to the following table for parameters specific to this connector:

Field Name	Sample Values	Description
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:trulog-ica:concero:2.0#resourceId attribute on the agent console.
Resource Type	NTDomain	The connector that was deployed in Step 1 on page 24.
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.
Domain	mydomain.com	The name of the NT domain.
Username	Administrator	Administrative account on the target resource.
Password	Password123	Password corresponding to the administrative account.

Field Name	Sample Values	Description
Server Name	server.company.com	The NETBIOS name or IP address of the NT Domain server.
AgentPort	5052	Forward connector server port, as configured on the resource agent.

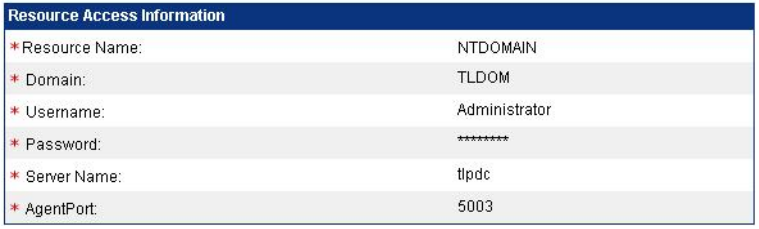
* Instead of creating an authoritative resource, you can create authoritative attributes (in the next step) for the attributes that will be synchronized. Entitlements are authoritative by default in a non-authoritative resource but other attributes are not.

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:



The Additional Info page will look similar to this:

The Access Info page will look similar to this:



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 feature in Select Identity. For example, if you added the PasswordExpired mapping to the mapping file as follows:

```
PasswordExpiresFlag | PasswordExpired
```

Create an attribute in Select Identity that will map to the connector and resource. Set the value of the attribute to **1**, which will force the password to expire.

Refer to the “Attributes” chapter in the *HP OpenView Select Identity Administrator Guide* for details. After you create the attributes for the

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

(Resource Name=NTDOMAIN)

Page 1 of 1 Total Records:10

Name	Min Length	Max Length	Attribute Mapped To	Authorative
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
NTDomain_ENTITLEMENTS	1	255	NTDomain_ENTITLEMENTS	Y
NTDomain_KEY	1	255	NTDomain_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 Connectors home page on the Select Identity client.

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 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.