NetIQ® Identity Manager
Driver for PeopleSoft Implementation Guide

May 2022

Legal Notices

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/.

Copyright (C) 2022 NetIQ Corporation. All rights reserved.

Contents

About this Book and the Library **7**
About NetIQ Corporation **9**

1 Understanding the PeopleSoft Driver **11**

Supported PeopleSoft Versions . . . 11
Support for People Tools Version 8.61 . . . 11
Prerequisites . . . 12
Driver Concepts . . . 12
Driver Components . . . 12
How the Driver Works . . . 13
Configuring Your PeopleSoft Environment . . . 15
Configuring Your Identity Manager System . . . 15
Support for Standard Driver Features . . . 16
Local Platforms . . . 16
Remote Platforms . . . 16
Entitlements . . . 17

2 Installing the Driver Files **19**

Installing the Driver Files . . . 19
Installing the PeopleSoft Components . . . 19
Copying the PeopleSoft Middleware Library File (psjoa.jar) to the Driver Directory . . . 20

3 Configuring Your PeopleSoft Environment **21**

Using the PeopleSoft Service Agent . . . 21
The Component Interface Infrastructure for Identity Manager . . . 22
The Sample Application . . . 22
Installing the PSA Sample Project . . . 23
Installing the PSA Files . . . 23
Importing the PSA Project into the PeopleSoft Database . . . 23
Building Project Record Definitions . . . 24
Applying Security to the PSA . . . 24
Understanding the Architecture of the PSA Sample Project . . . 25
Testing Sample PeopleSoft Applications . . . 27
Component Interfaces . . . 28
Accessing Transactions and Data through Component Interfaces . . . 28
Configuring the Transaction Record SQL Date/Time Format . . . 31
Configuring PeopleCode to Trigger Transactions . . . 32
Testing Component Interfaces . . . 34

4 Creating a New Driver Object **41**

Creating a PeopleSoft Account . . . 41
Creating the Driver Object in Designer . . . 41
Importing the Current Driver Packages . . . 41

Installing the Driver Packages . . . 42
Configuring the Driver . . . 45
Deploying, Starting and Activating the Driver . . . 46
Adding Packages to an Existing Driver . . . 46

5 Upgrading an Existing Driver 49

Supported Upgrade Paths . . . 49
Upgrade Procedure . . . 49

6 Customizing the Driver 51

Customizing the PSA by Triggering Transactions . . . 51
Changing the Data Schema Component Interface . . . 53
Building the PeopleSoft Java Component Interface API . . . 53
Compiling the Java CI API . . . 55
Building the CI API JAR File . . . 55
Modifying Driver Policies . . . 56
Modifying the Driver Mapping Policy . . . 57
Using the Schema Query to Refresh the PeopleSoft Schema Component Interface . . . 57
Publisher Channel Objects . . . 57
Understanding the Publisher Filter . . . 58
Publisher Filter Attributes . . . 58
Securing the Data . . . 59
Publisher Object Policies . . . 59
Subscriber Channel Objects . . . 64
Understanding the Subscriber Filter . . . 65
Securing the Data . . . 66
Modifying the Filter . . . 66
Subscriber Object Policies . . . 66
SSL Configuration for PeopleSoft Application . . . 69

7 Managing the Driver 71

8 Troubleshooting the Driver 73

The Driver Is Not Processing Available Transactions or Is Processing Them Out of Order . . . 73
Error Trying to Obtain Data Record . . . 73
Error: joltServiceException: Invalid Session . . . 74
The Driver Does Not Start . . . 74
Attributes Are Not Refreshed on the Data Schema Object . . . 74
Data Does Not Appear in the Identity Vault on the Publisher Channel . . . 74
Error: Check Application Server IP Address and Jolt Port Number . . . 75
Data Does Not Update in PeopleSoft on the Subscriber Channel . . . 75
No Transactions Are Coming Across the Publisher Channel . . . 75
Transactions Are Not Placed in the PeopleSoft Queue . . . 75
Transactions Are Left in the “Process” State and Not Processed . . . 75
Errors on the Publisher Channel When Processing a Transaction . . . 76
Component Interface Relationships Are Not Functioning . . . 76
SQL Error When Saving “Sample Person” Records . . . 76
Troubleshooting Driver Processes . . . 77

A Driver Properties **79**

Driver Configuration 79
Driver Module 79
Driver Object Password 80
Authentication 80
Startup Option 81
Driver Parameters 81
ECMAScript. 82
Global Configuration 83
Global Configuration Values. 83
Password Synchronization. 84
Managed System Information 84

B Trace Levels **87**

About this Book and the Library

The *Identity Manager Driver for PeopleSoft Implementation Guide* provides a solution for synchronizing data between NetIQ Identity Vault and PeopleSoft.

Intended Audience

This book provides information for individuals who need to install, configure, and maintain the PeopleSoft driver.

Other Information in the Library

For more information about the library for Identity Manager, see the following resources:

- Identity Manager documentation website (https://www.netiq.com/documentation/identity-manager-48/)
- Identity Manager drivers documentation website (https://www.netiq.com/documentation/identity-manager-48-drivers/)

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **Add Comment** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit community.netiq.com.

1 Understanding the PeopleSoft Driver

PeopleSoft applications are some of the most popular Enterprise Resource Planning (ERP) systems available. The Identity Manager Driver for PeopleSoft enables you to create and manage Identity Vault (NetIQ eDirectory) objects by using data you receive from a PeopleSoft application. It's a powerful solution to maintain, propagate, and transform your data.

This driver can integrate any PeopleSoft component with the Identity Vault. Using NetIQ Identity Manager technology, you can share and synchronize authoritative PeopleSoft data with other enterprise applications, databases, or directories. As new records are added, modified, disabled, or deactivated in PeopleSoft, tasks associated with these events can be processed automatically through Identity Manager.

Because Identity Manager is a bidirectional data management solution, you can also synchronize authoritative data from other systems to PeopleSoft components. This dynamic, business-specific solution allows you to manage and integrate information however you desire.

This section contains the following topics:

- "Supported PeopleSoft Versions" on page 11
- "Prerequisites" on page 12
- "Driver Concepts" on page 12
- "Support for Standard Driver Features" on page 16

Supported PeopleSoft Versions

You can use the PeopleSoft driver 5.2 with PeopleTools application v8.5x or above. The PeopleSoft driver 5.2.4.0 has been certified with People Tools v8.57, v8.58, 8.59, 8.60 and v8.61.

Support for People Tools Version 8.61

Following steps allows the driver to connect to PeopleSoft using JOLT LLE:

1. Add JVM Options in identity console as:

   Go to **Edit Driver Set Properties** > **Driver Set Configuration** tab > **Java Environment Parameters** > **JVM options**. Specify -DTM_ALLOW_NOTLS=Y in **JVM options**.

2. Restart the **edirectory**.

Perform the below steps to connect the driver with SSL / TLS:

1. Execute the steps as mentioned in "SSL Configuration for PeopleSoft Application" on page 67.

NOTE: The default length of RSA key is 2048. To specify the minimum length allowed for RSA key, set the Java property `TM_MIN_PUB_KEY_LENGTH` under JVM options in identity console. For example, `DTM_MIN_PUB_KEY_LENGTH=1024`.

2 Restart the **edirectory**.

Prerequisites

- ❒ The appropriate version of the PeopleTools `psjoa.jar` client to match the PeopleTools version of the target PeopleSoft Application Server.
- ❒ A `.jar` file containing the compiled Java Component Interface APIs for the desired integration component. For the default PSA components, the file containing the interfaces is named `dirxmlcomps.jar`. For more information on creating Component Interface APIs, refer to Chapter 6, "Customizing the Driver," on page 51.

Driver Concepts

The following sections explain the concepts you should understand before attempting to implement the PeopleSoft driver in your environment:

- "Driver Components" on page 12
- "How the Driver Works" on page 13
- "Configuring Your PeopleSoft Environment" on page 15
- "Configuring Your Identity Manager System" on page 15

Driver Components

The driver includes the following components:

- "Driver Shim" on page 12
- "Driver Packages" on page 13
- "PeopleSoft Service Agent" on page 13

Driver Shim

The driver shim (`psoftshim.jar`) enables communication between PeopleSoft and the Identity Vault. It bidirectionally reports object change events and applies object modification commands between these systems.

Driver Packages

The driver packages contain configuration information and policies that enable Identity manager to handle the synchronization and data object manipulation between PeopleSoft and the Identity Vault.

The packages act as a template that contains the most common synchronization tasks performed in a typical integration scenario. You should configure your policies based on your own business processes and integration points. For more information, refer to Chapter 4, “Creating a New Driver Object,” on page 41 and “Modifying Driver Policies” on page 56.

PeopleSoft Service Agent

The PeopleSoft Service Agent (PSA) is a collection of PeopleSoft application objects developed for use with the driver shim and default driver configuration. Because all of the objects (fields, records, pages, components, component interfaces) are specifically named with a DirXML identifier, the PSA can be deployed onto a PeopleSoft application server without affecting existing PeopleSoft applications and objects.

The various pieces of the PSA provide examples of how data can be integrated between Identity Vault and PeopleSoft, such as the following:

- Implementation of an intermediate staging table. The synchronization between the NetIQ sample Personnel Application and the staging table shows the best practices of PeopleSoft internal application integration using PeopleCode Component Interfaces.
- Integration can be accomplished directly to the sample Personnel Application by simply changing the driver's configuration.
- PeopleCode is provided to show how database events on the sample Personnel Application can be reported to the driver shim via the transaction record interface required by the driver shim.
- PeopleCode is provided to show how to implement a Delete method on a Component Interface.

Similar to the driver configuration, the PSA is not intended for use in a production environment. It acts as a template that contains most of the common synchronization tasks needed in typical integration scenarios. You should configure your policies based on your own business processes and integration points. For more information, refer to Chapter 3, “Configuring Your PeopleSoft Environment,” on page 21.

How the Driver Works

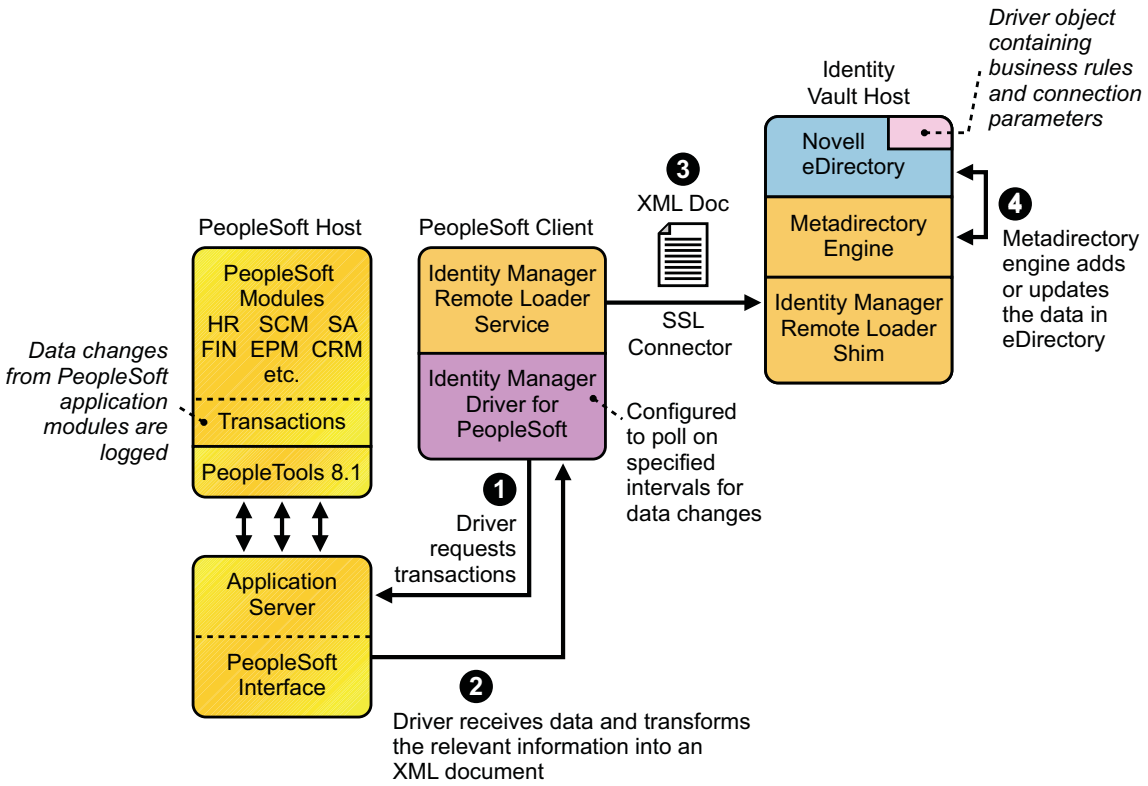
The following section describes the basic functions of the driver. It uses the Remote Loader configuration as an example; however, the driver does not require the use of the Remote Loader. For more information, refer to Chapter 2, “Installing the Driver Files,” on page 19.

- “The Publisher Channel” on page 13
- “The Subscriber Channel” on page 14

The Publisher Channel

The Publisher channel synchronizes data from PeopleSoft to the Identity Vault.

Figure 1-1 The Publisher Channel



As events occur within PeopleSoft, transactions are placed into a transaction table. These transactions are usually written to the table through PeopleCode (you can use other methods such as Batch SQL, COBOL, SQR, and so forth.) Component Interface (CI) objects enable the driver to access transactions within the PeopleSoft system, and to query for relevant data associated with an individual transaction type. These CI objects are included as part of the PeopleSoft Service Agent (PSA).

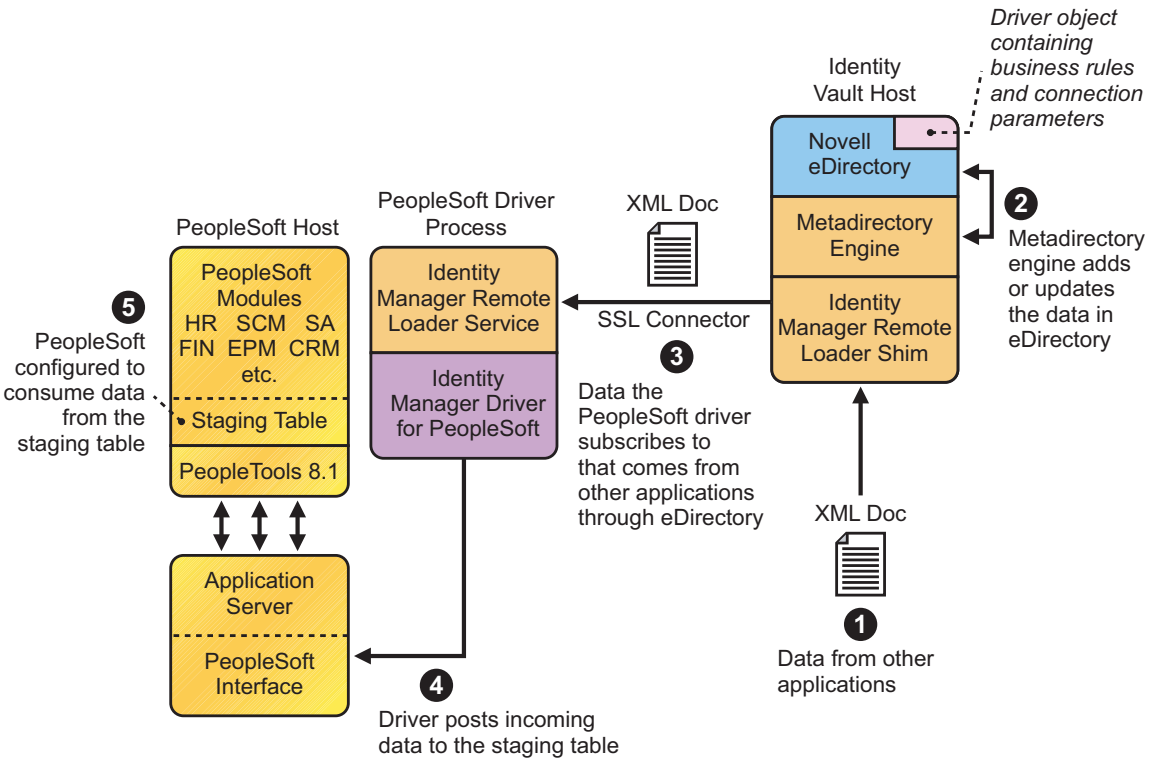
The driver accesses the PeopleSoft environment by connecting through the Component Interface at the Application Server level. The driver periodically requests transactions that are waiting to be processed by driver subtype (such as Employee, Student, or Customer.) It processes only those transactions that have an available status and a transaction date and time less than or equal to the current date and time.

The driver then constructs an XML document from the data it retrieves and passes it to the Identity Manager engine for processing. When Identity Manager engine finishes processing the transaction, the driver updates the transaction with the status and any applicable messages in the transaction table inside of PeopleSoft. When events occur within Identity Vault, the driver connects to the appropriate CI and updates the PeopleSoft staging table accordingly. You can also configure the Driver to poll the Application server for event changes.

The Subscriber Channel

The Subscriber channel synchronizes data from other applications via Identity Vault to PeopleSoft.

Figure 1-2 The Subscriber Channel



As events occur within Identity Vault, the driver receives an XML document from the Identity Manager engine and updates PeopleSoft. By configuring the filter on the Subscriber channel, you can specify what data you want updated in PeopleSoft. The driver uses the Schema Component Interface (CI) and updates a staging table inside the PeopleSoft environment.

If you want to move the data from the staging table into PeopleSoft, you can create and apply the necessary PeopleCode to handle this transaction. (All PeopleSoft objects that can interact with the transaction table, application data, as well as the CI, are delivered with the sample project.)

Configuring Your PeopleSoft Environment

You must configure your PeopleSoft application to do two things:

- Trap events that occur within PeopleSoft and place transactions into a transaction table.
- Expose the transactions and any other desired data to the driver.

For detailed instructions regarding how to configure these processes, refer to Chapter 3, “Configuring Your PeopleSoft Environment,” on page 21.

Configuring Your Identity Manager System

The driver interacts with PeopleSoft at the PeopleTools level by using Component Interface (CI) technology. By using existing CI definitions within the PeopleSoft modules, along with a collection of the driver's preconfigured CI objects, you can do the following:

- Create Identity Vault objects as new data is synchronized from PeopleSoft.

- Synchronize data bidirectionally between a PeopleSoft application and Identity Vault.
- Enable bidirectional object Create and Delete events.
- Transform Identity Vault events (such as Delete, Rename, or Move events) into different events in PeopleSoft.
- Maintain publication authority over data.
- Establish Group, Role, or other relationships in Identity Vault based on relationships defined within the PeopleSoft application.
- Provide notifications based on various events or required approval processes.
- Adhere to enterprise business processes and policies.
- Share data with other systems involved in your enterprise provisioning solution.

For more information on configuring your Identity Manager system, refer to Chapter 6, "Customizing the Driver," on page 51.

Support for Standard Driver Features

The following sections provide information about how the PeopleSoft driver supports these standard driver features:

- "Local Platforms" on page 16
- "Remote Platforms" on page 16
- "Entitlements" on page 17

Local Platforms

A local installation is an installation of the driver on the Identity Manager server. The PeopleSoft driver can be installed on the operating systems supported for the Identity Manager server.

For information about the operating systems supported for the Identity Manager server, see "Planning Your Installation " in the *NetIQ Identity Manager Setup Guide for Linux* or "Planning Your Installation " in the *NetIQ Identity Manager Setup Guide for Windows*.

NOTE: Support for the local and remote platforms depends on the supported platforms of the PeopleTools Client (PSJOA) software.

Remote Platforms

The PeopleSoft driver can use the Remote Loader service to run on a server other than Identity Manager server. The PeopleSoft driver can be installed on the operating systems supported for the Remote Loader.

For information about the supported operating systems, see "Planning Your Installation " in the *NetIQ Identity Manager Setup Guide for Linux* or "Planning Your Installation " in the *NetIQ Identity Manager Setup Guide for Windows*.

NOTE: The support for the local and remote platforms depends on the supported platforms of the PeopleTools Client (PSJOA) software.

Entitlements

The PeopleSoft driver does not have entitlement functionality defined within the default driver packages. The driver does support entitlements, if there are policies created for the driver to consume.

2 Installing the Driver Files

By default, the PeopleSoft driver files are installed on the Identity Manager server at the same time as the Identity Manager engine. The installation program extends the Identity Vault's schema and installs the driver shim and the driver configuration file. It does not create the driver in the Identity Vault (see Chapter 4, "Creating a New Driver Object," on page 41) or upgrade an existing driver's configuration (see Chapter 5, "Upgrading an Existing Driver," on page 49).

To ensure that you have the driver installed in the right location, and to finish the installation by manually copying required PeopleSoft files to the driver's directory, refer to the following sections:

- "Installing the Driver Files" on page 19
- "Installing the PeopleSoft Components" on page 19
- "Copying the PeopleSoft Middleware Library File (psjoa.jar) to the Driver Directory" on page 20

Installing the Driver Files

Install the driver files using one of the following options:

- Install the Identity Manager server (Identity Manager engine and drivers). This requires NetIQ eDirectory to be installed on the server. See the instructions for Linux in "Planning Your Installation " in the *NetIQ Identity Manager Setup Guide for Linux* and for Windows, see "Planning Your Installation " in the *NetIQ Identity Manager Setup Guide for Windows*.
- Install the Identity Manager server (Identity Manager engine and drivers) on a different server other than the PeopleSoft server.
- Install the Remote Loader (required to run the driver on a non-Identity Manager server) and the PeopleSoft driver files to the PeopleSoft server. This assumes that you already have a Identity Manager server installed on another server in your environment. For Linux, see "Planning Your Installation " in the *NetIQ Identity Manager Setup Guide for Linux* and for Windows, see "Planning Your Installation " in the *NetIQ Identity Manager Setup Guide for Windows*.
- Install the Remote Loader (required to run the driver on a non-Identity Manager server) and the PeopleSoft driver files on a different server other than the PeopleSoft server.

NOTE: Ensure that the `psjoa.jar` file is running on the same server where the driver is installed, irrespective of local or remote installation of the driver.

Installing the PeopleSoft Components

As part of the Identity Manager installation, select the **Utilities** option and install the PeopleSoft Components. This installs the PeopleSoft Server Agent files and the Component Tester program. If you have already installed the driver files but did not install the PeopleSoft Components, you can run the installation program again to install only the PeopleSoft Components.

Copying the PeopleSoft Middleware Library File (psjoa.jar) to the Driver Directory

The PeopleSoft middleware library is located in the `web/psjoa` directory of the PeopleTools software distribution.

You must copy the `psjoa.jar` file, and any additional Component Interface API class libraries that your solution requires, to the driver's `\lib` subdirectory. By default, this is `Novell\NDS\lib` for local driver installation or `Novell\RemoteLoader\lib` for a remote installation.

3 Configuring Your PeopleSoft Environment

The PeopleSoft Server Agent (PSA) is a set of PeopleTools objects and code that enables you to define the integration between PeopleSoft applications and the Identity Vault. The following sections explain how the PSA works and how to configure your PeopleSoft environment:

- "Using the PeopleSoft Service Agent" on page 21
- "Installing the PSA Sample Project" on page 23
- "Component Interfaces" on page 28

Using the PeopleSoft Service Agent

The PeopleSoft Server Agent (PSA) includes all of the components for a sample Personnel application, a staging table for moving data between the Sample application and the driver, a Transaction record interface for recording data events of interest to the driver, and utilities for managing the Transaction record interface. Using the sample data and code in the PSA, you can quickly model and implement an Identity Manager solution that is not intrusive to the existing functions and applications on your PeopleSoft system.

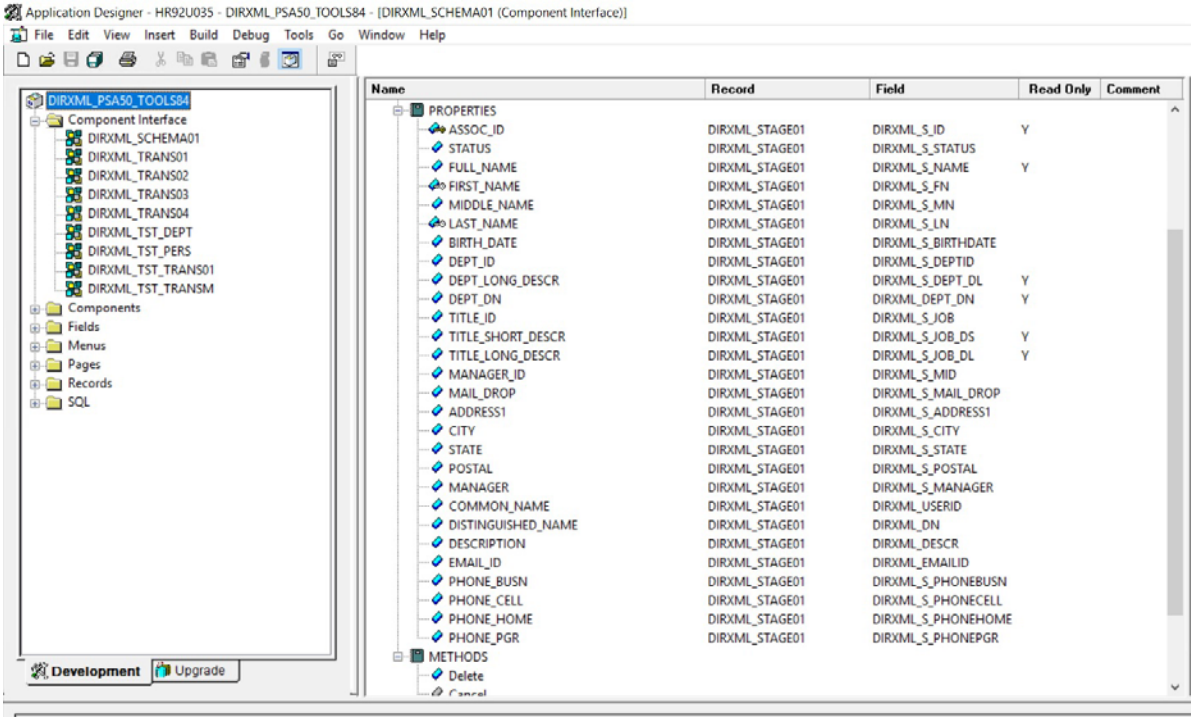
This version of the PSA works with any PeopleSoft database on the required release level of PeopleTools, see "Prerequisites" on page 12. Before you can install the PSA, you need access to a PeopleSoft user ID and password with Administrator or appropriate developer rights. You can create a unique user ID and password for implementing these objects.

The PSA contains SQLExec statements in the PeopleCode for the various Table and View records. There is no guarantee that all of these statements are compatible with the underlying database software. If you encounter problems, refer to Chapter 8, "Troubleshooting the Driver," on page 73 for specific issues and consult with your DBMS/PeopleSoft Database administrator for additional assistance.

- "The Component Interface Infrastructure for Identity Manager" on page 22
- "The Sample Application" on page 22

The Component Interface Infrastructure for Identity Manager

Figure 3-1 *The DirXML Component Interface*



You can use the Component Interface infrastructure and PeopleCode function calls to specify the type and content of Transaction records that are generated in relation to PeopleSoft Component events. You can also decide if the driver processes events and how they are processed. For example, a new row event generated by the sample application generates a slightly different event than a new row event generated by the driver's Subscriber channel.

For more information, refer to "Configuring PeopleCode to Trigger Transactions" on page 32.

The Sample Application

The PSA project has sample Personnel Applications that you can install to use with PeopleTools 8.5x for configuration and testing purposes.

Depending on your business requirements, you should configure internal processes to do things like trigger events into transaction tables or synchronize with other PeopleSoft tables, either by replicating the provided PeopleCode or by merging the components within your PeopleSoft environment. When you synchronize data internally between application tables, you should always try to use the tools that provide the highest degree of data integrity checking. For example, the Staging CI to Application CI synchronization in the PSA utilizes the PeopleCode CI interface to ensure proper syntax, translate table usage, and check related fields as it has been defined on the Application record. For more information, refer to "Understanding the Architecture of the PSA Sample Project" on page 25.

Installing the PSA Sample Project

Complete the following tasks to install the sample project for testing and configuration purposes:

- "Installing the PSA Files" on page 23
- "Importing the PSA Project into the PeopleSoft Database" on page 23
- "Building Project Record Definitions" on page 24
- "Applying Security to the PSA" on page 24
- "Understanding the Architecture of the PSA Sample Project" on page 25
- "Testing Sample PeopleSoft Applications" on page 27

Installing the PSA Files

If you did not install the PSA during the initial driver installation, locate the product CD or download, go to the PeopleSoft application server, and run `install.exe`. You should see the following PSA files on your target server:

- `DIRXML_PSA50_TOOLS84.exe` for PeopleTools 8.5x

NOTE: For installing PeopleSoft 8.5 version, use the `DIRXML_PSA50_TOOLS84.exe` file. There is no change in the installation procedure for PeopleSoft 8.5x from PeopleSoft 8.4x version.

These files are self-extracting zip files that contain the PSA project folder and files for the different versions of PeopleTools. Extract the appropriate file onto the file system of your PeopleSoft Application Designer host (`c:\psa`).

To ensure that the PSA can be imported into the PeopleSoft Application server, make sure that the PSA files have write access enabled. For example, in Windows, you should turn off read-only file properties.

Importing the PSA Project into the PeopleSoft Database

After the PSA files have been installed in an accessible file system location, they must be imported into the PeopleSoft Database via the PeopleSoft Application Designer tool.

- "PeopleSoft 8.5x" on page 23

PeopleSoft 8.5x

1. Connect to the PeopleSoft database as administrator in two tier mode.
2. In the Application Designer, select **Tools > Copy Project> From File**.
3. Click **Browse** and select the PSA project directory: `c:\psa\DIRXML_PSA50_TOOLS84`.
4. Click **Open**.
5. Select all object types, then click **Copy** to copy all project components into the PeopleSoft database.

Building Project Record Definitions

After you have imported the project into the PeopleSoft database, you should build project record definitions and project views.

1. Log in to the PeopleSoft Application Designer by using an administrator username that has administrative and development rights.
2. In the Application Designer, select **Build > Project**.
3. In Build Options, click **Create Tables and Execute SQL Now**. After the project tables are created, click **Close** to close the Build Progress window.
4. Click **Build** to create sample project tables.

   You must create project tables before creating the views. Views are created with information from table fields.
5. In the Application Designer, select **Build > Project**.
6. In Build Options, click **Create Views and Execute SQL Now**.
7. Click **Build** to create the sample project views. After views are created, click **Close** to close the Build Progress window.

Applying Security to the PSA

In order for the driver to access PeopleSoft transaction tables, you need to apply security to the PSA. You accomplish this by creating the DirXML Administrator role and then assigning it to the administrative user. You can assign the role to an existing account or create a new account specifically for PSA security.

- "PeopleSoft 8.5" on page 24

PeopleSoft 8.5

1. Log in to the PeopleSoft portal.
2. Click **PeopleTools > Security > Permissions & Roles > Roles**.
3. Click **Add a New Value**, then specify a role name (for example, **DirXML Administrator**).
4. Type a description for the role.
5. (Optional) Type a long description for the role.
6. Click the **Permissions List** tab.
7. Search for and select the DirXML permissions list, then click **Save**.
8. Assign **DirXML Administrator** role to your administrative user by clicking **PeopleTools > Security > User Profiles > User Profiles**.
9. Click **Search** to locate the User Profile that you want to add the DirXML Administrator role to, then click the **User ID**.
10. Click the **Roles** tab, then click one of the + buttons to add a new role.
11. Search and select the role, click **DirXML Administrator** to add it, then click **Save**.

Understanding the Architecture of the PSA Sample Project

The PSA Sample project is intended to provide recommended PeopleSoft integration scenarios through the use of very comprehensive instructions and examples. The various elements of the PSA are completely independent of any existing PeopleSoft application software, so there is no risk of data table corruption, extension, or modification.

The objects of the PSA include:

- Field definitions
- Record definitions
- Page definitions
- Component definitions
- Component Interface definitions
- Menu definitions
- SQL code

All of these objects are named with a prefix of DIRXML_ so that they cannot be confused with existing objects.

- "Sample Application" on page 25
- "Staging Table" on page 25
- "Transaction Table" on page 26
- "PSA Best Practices" on page 26

Sample Application

This application is intended to simulate the data and functions of an HR or other type of Person provisioning application. The base Record definitions for the application are:

- DIRXML_S_PERS: Provides basic HR field data
- DIRXML_S_DEPT: Sample Department codes table
- DIRXML_S_PHONES: Phone Numbers table

The data is accessed through the DIRXML_ADMINISTRATOR menu options. The menu provides access to a **DirXML Sample People** component and a **DirXML Sample Department** component. These applications simulate the standard methods for adding and updating Department and Person data into the PeopleSoft database. The driver default configuration does not directly access any of these tables or components. Additionally, the data provided by this application is not passed directly to the driver from these components. The actual transfer of data takes place through staging table components.

Staging Table

The staging table interface is designed to insulate the PeopleSoft Application data from direct manipulation by the driver. This allows an interface to be designed to:

- Combine access to the data from multiple data tables and applications through a single interface.

- Prevent the driver from viewing or modifying sensitive application data.
- Provide storage for external data that does not easily fit into standard PeopleSoft applications.

The Record definition that represents all of the data that can be published or subscribed by the driver is called DIRXML_STAGE01. This record aggregates most of the data fields from the three Application data records into a single access point. There are also additional fields not in the Application records that are used to contain references to the synchronized eDirectory objects.

For PeopleSoft users, the data in the staging table can be accessed via the DirXML Schema 01 component of the DIRXML_ADMINISTRATOR menu. The driver accesses the data via the DIRXML_SCHEMA01 Component Interface.

Transaction Table

Every time a modification is made to the Application Data Records, transaction records are placed in the DIRXML_TRANS01 table. The PSA places identifiers indicating the key of the data row being modified, the time of the event, the type of event, and various other pieces of transaction related data. Any change made to a data row via the DIRXML_ADMINISTRATOR application interfaces is recorded with an NPSDriver1P identifier that shows the data is being published by a PeopleSoft administrator. Changes made via the Component Interface API are recorded with an NPSDriver1S identifier that shows the data was subscribed into the application tables programmatically.

In addition to providing an audit trail of database modifications, the transaction table is utilized by the driver to facilitate Publisher channel activities. The driver polls the transaction table for records in the *Available* state, reads the related application data record, and processes the data through the Publisher channel. The transaction records are then updated with the processing status.

In addition to the transaction tables and interfaces, the PSA includes utilities to monitor, maintain, archive, and remove transaction records.

PSA Best Practices

Data moves between the various PeopleSoft components and tables through PeopleCode. Each of the application data records in the PSA contains PeopleCode that performs the basic functions of moving data between the Staging table and Application tables, ensuring the integrity of the data and data transfers, and generating Transaction table records at the appropriate time and with the appropriate data. PeopleCode is very powerful and is capable of performing a wide variety of tasks, some of which are potentially destructive to your data.

IMPORTANT: Only personnel who have completed PeopleTools and PeopleCode training should modify the elements of the PSA.

These guidelines might prove helpful when implementing changes to the PSA.

- Whenever possible, always provide a Component Interface (CI) to affected data tables. In the PSA, the DIRXML_S_PERS data rows are created and updated with PeopleCode via the DIRXML_TST_PERS CI. The CI guarantees the integrity of the data as defined by the designer of the application. It ensures that valid Translate values, proper data format, and required fields are present. Most importantly, the CI can restrict the data fields that can be accessed on a particular record or record set. This is a very important aspect of data security.

- The DIRXML_SCHEMA01 CI has been extended with a Delete method that enables removal of data schema records via the driver's Subscriber channel. Using this functionality is not required. The method can be removed from the CI or the driver can be configured to not use it.
- Make sure that the staging table record contains the same required fields that exist on the target Application records. This helps ensure successful record data synchronization.
- It is important to generate transactions whenever the application data table records are created or updated, even if the changes are made by the driver. Although data loopback can occur, the generation process ensures that Translate table values and related field values generated by the changes are properly synchronized.
- If you are using SQLExec() statements to update tables or create records, use great care to ensure that you are not violating the logic and rules of the applications overlying the tables. SQL is the easiest and most powerful, and therefore most destructive, method for updating data, but it is also the most potentially destructive.
- Do not generate Transaction records until after you have successfully updated the application tables.
- You can completely bypass the staging table interface in your synchronization scenario. The driver can be directed to interact with any CI. Make sure that the PeopleCode generating the transaction records is updated to specify the new Application data CI and is triggered appropriately. Also ensure that the same CI methods are implemented and enabled.
- The driver is delivered with a Java archive (JAR) file that contains the compiled Java interfaces for all of the CI defined in the PSA. If the driver is to be configured to use different application CIs, it is necessary to build and JAR those interfaces. For more information, refer to "Changing the Data Schema Component Interface" on page 53.
- Test everything thoroughly.

Testing Sample PeopleSoft Applications

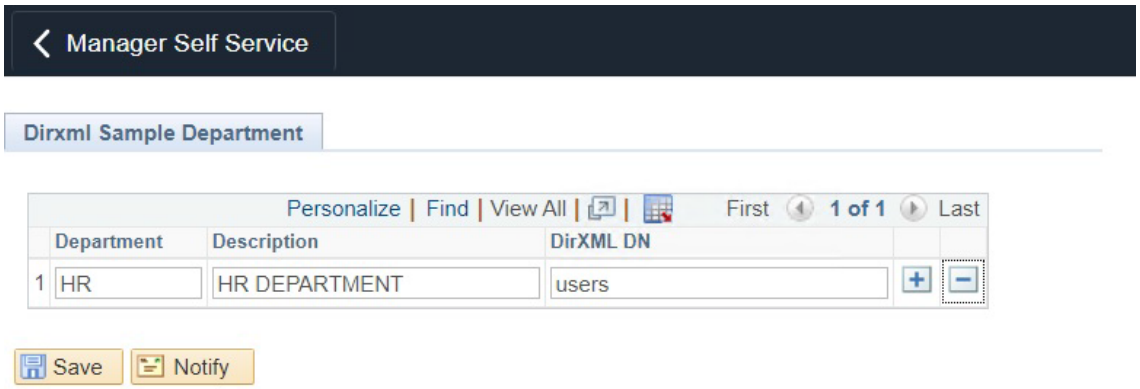
You can test to ensure that transactions are created and to validate that the application works. The following information explains how to create a Department and add a new person to test your sample application.

- **"PeopleSoft 8.5x" on page 27**

PeopleSoft 8.5x

1. Log in to the PeopleSoft portal.
2. Click **DirXML Administrator** from the left menu.

   If the **DirXML Administrator** menu doesn't appear, you should delete the Application Server cache and reboot the Application Server.
3. Click **DirXML Sample Department**.



4 Specify a sample department, then click **Save**.

5 Click **DirXML Sample People**.

6 Specify values for a sample user, then click **Save** and verify that the user's data appears in the Transaction01 table. You do this by searching in the DirXML Transaction01 application.

7 Verify that other delivered applications work by selecting them from the **DirXML Administrator** menu.

Component Interfaces

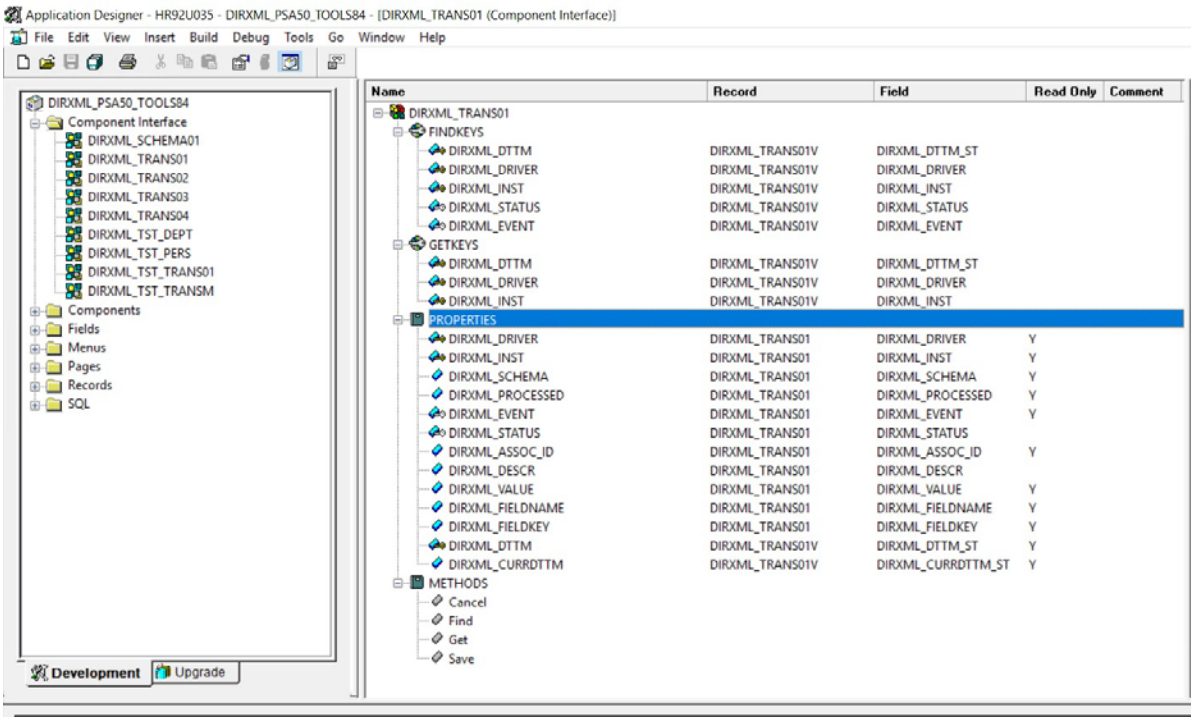
- "Accessing Transactions and Data through Component Interfaces" on page 28
- "Configuring the Transaction Record SQL Date/Time Format" on page 31
- "Configuring PeopleCode to Trigger Transactions" on page 32
- "Testing Component Interfaces" on page 34

Accessing Transactions and Data through Component Interfaces

The driver accesses transactions waiting to be processed from the transaction table via the Component Interface (CI) object that is defined within PeopleTools. Each CI maps to a particular component. Components are built in order to access transaction tables and "schema" application object data. Schema objects represent all the necessary fields and methods that need to be exposed for data synchronization to the driver. These objects also enable the driver to update PeopleSoft data.

Each driver uses only one Transaction CI to access transactions. Every transaction is assigned to one default Schema CI. In the driver's parameters, you must specify the Transaction CI object name as defined in PeopleSoft. This CI object maps to a predefined component that enables the driver to access transactions from one transaction table. The following represents the CI for a transaction table:

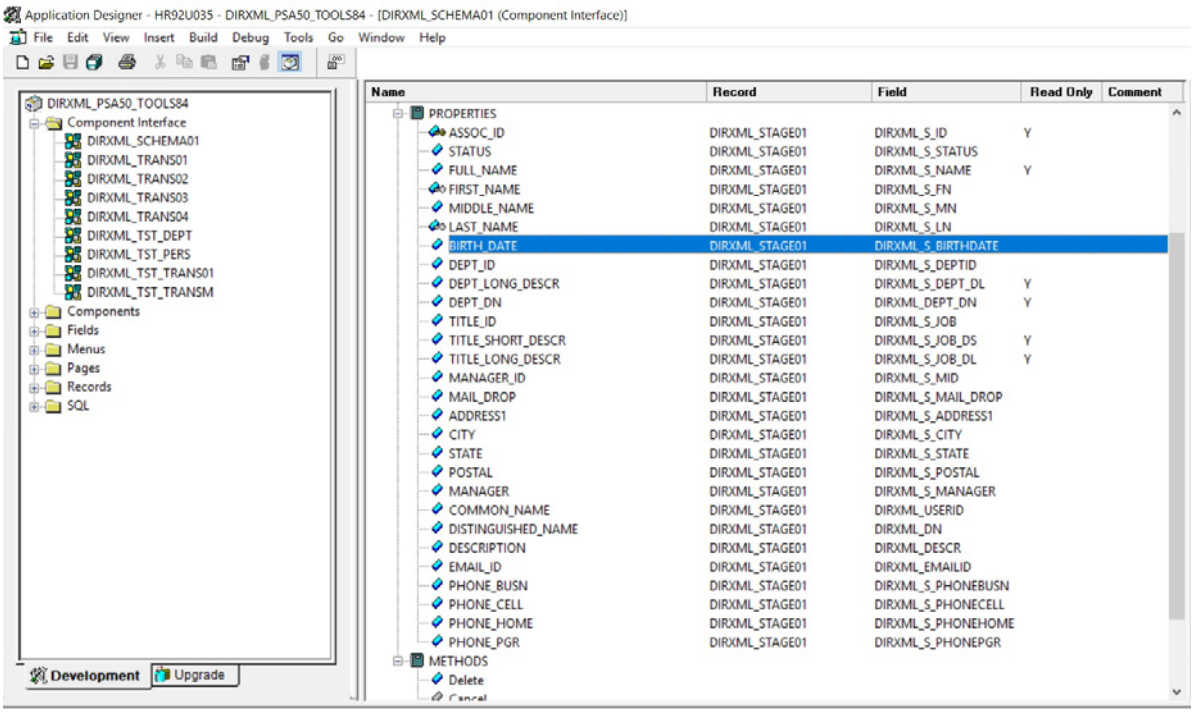
Figure 3-2 *Transaction Table Component Interface (CI)*



In addition to the Transaction CI name, the driver configuration contains a parameter that can specify a particular subset of the transactions that are available for processing. This allows a single Transaction CI to interface with multiple drivers, which might be synchronizing different sets of object data or different object types. This subset identifier is maintained in the DIRXML_DRIVER field of the Transaction CI.

The following figure represents the CI for a Schema Component:

Figure 3-3 *Schema Component*



The PeopleSoft developer can specify these values when configuring the PeopleCode function calls to trigger a transaction online, or when creating transactions via a batch process. The PSA provides PeopleCode function DirXML_Trans and is responsible for generating transaction events. The PSA contains several function calls which you may use to guide customization.

The PeopleCode DirXML_Trans schema calls should always be placed in the SavePostChange PeopleCode on the record definitions. This ensures that the data is committed prior to the transaction being generated.

Changes to Field Names in PeopleSoft 8.41

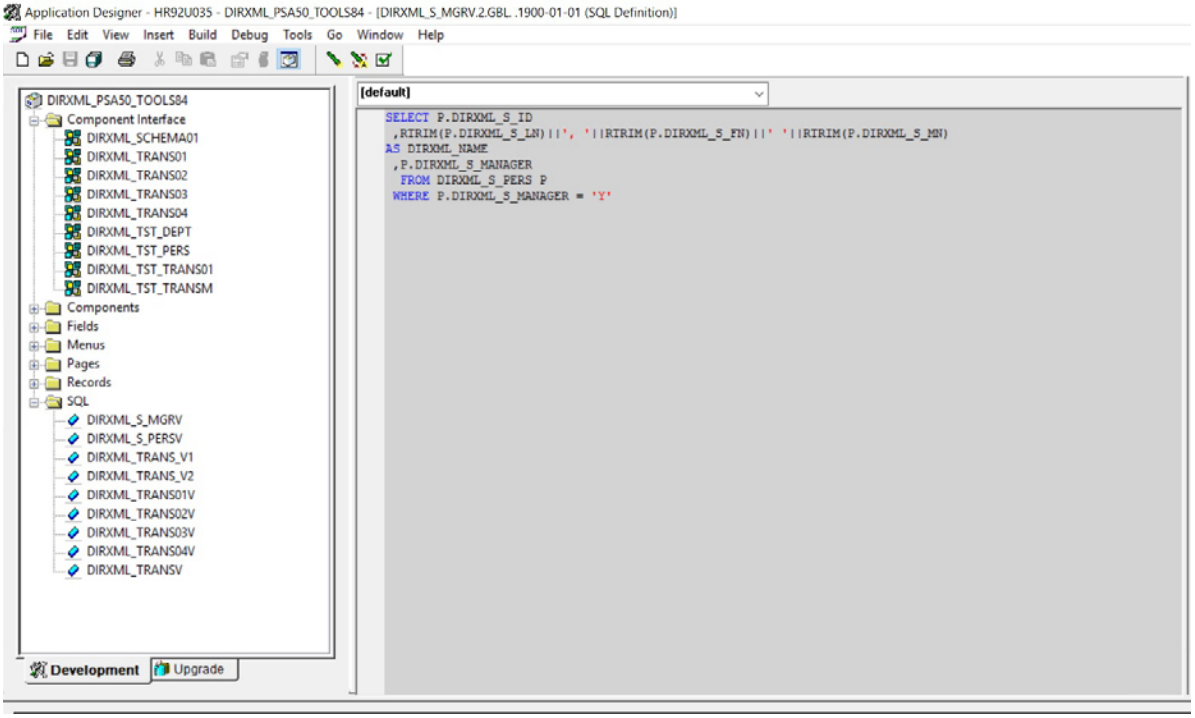
With new releases of PeopleTools, changes are made to the policies regarding field names. With PeopleTools 8.41, there were two significant changes:

- Spaces are no longer allowed in CI field names.
- There are now case sensitivity issues in the CI API. Field names and field name values no longer align because of case-sensitive sorting. For example, a field named CN is sorted prior to a field named City. The result of trying to access the value of City returns the value for CN. The default schema of the CIs used by the driver now uses naming conventions that eliminate this unusual sorting error. This issue is particularly important for any field name modifications or additions customized for a prior implementation of the driver.
- Use the standard ALL-CAPS format to avoid any field name issues.

Configuring the Transaction Record SQL Date/Time Format

The proper functioning of the driver depends on the Date/Time strings in the Transaction View record to determine processing availability and relative event order of Transaction data rows. The Date/Time fields in the Transaction data rows are converted to formatted strings in the Transaction Views by using the PeopleCode Meta-SQL%DateTimeOut() function. The following image shows the default SQL View code for the DIRXML_TRANS01V record:

Figure 3-4 *SQL View of Code for the DirXML_TRANS01V Record*



Unfortunately, the format of the strings presented by %DateTimeOut() might differ depending on the underlying DBMS software. To make sure a date and time string is generated in a consistently increasing lexicographic format, the following format is recommended:

- The date should be presented first in *YYYY-MM-DD* format.
- The time should be presented in 24-hour form with *HH:MM:SS* format (Additional information concatenated to this string, such as <milliseconds> is acceptable)
- These two strings should be placed together in “date-time” format.

The characters used to delimit the numerical values are not important as long as they are consistent. Examples of a well-formed, lexicographically ordered format are:

2004-08-26-14.44.33.000000 (ODBC Canonical style 121)

or

2004/08/26-14:44:33 (Generic)

The fields used by the driver are DIRXML_DTTM_ST and DIRXML_CURRDTTM_ST. These fields represent the date and time that the Transaction data row was created and the current processing date and time of the transaction.

If you are using a driver trace level of 2 or above, the driver traces the CurrDate and ActionDate of each Transaction row that it processes. If the format shown does not match the criteria specified, edit the SQL of the desired Transaction View record to perform the appropriate conversions on these fields. Make sure that you use the **Build > Create Views** option after making any modifications to the SQL definition of the View Record.

Because the configuration of the Date and Time format varies depending on the DBMS being utilized, changing this format should be done by the DBMS/PeopleSoft Database Administrator or other qualified personnel.

Configuring PeopleCode to Trigger Transactions

The PSA contains a number of PeopleTools objects that enable PeopleSoft to trap events into a transaction table. The driver then accesses the transaction tables through CI objects. The driver periodically requests transactions that need to be processed, based on their driver subtypes. It processes only those transactions that have a transaction date or time less than or equal to the current date or time value, along with an available status. Also, the driver processes transactions one at a time from the transaction table before getting a new transaction.

The driver then constructs an XML document from the data it retrieved and passes this to the Identity Manager engine for processing. It updates the transaction status and any applicable messages on the transaction table inside of PeopleSoft after processing is completed by the Identity Manager engine. When events occur within eDirectory, the driver connects to the appropriate CI and updates the PeopleSoft staging table as appropriate.

You trigger transactions using PeopleCode within the PeopleSoft application.This document assumes that you know how to write PeopleCode. If you need further assistance, refer to PeopleSoft documentation for more information.

The driver requires a Transaction CI and a Schema CI to process transactions. For more information on calling the PeopleSoft function that creates transaction records, please refer to "Customizing the PSA by Triggering Transactions" on page 51.

- "Transaction Component" on page 32
- "Schema Component" on page 33

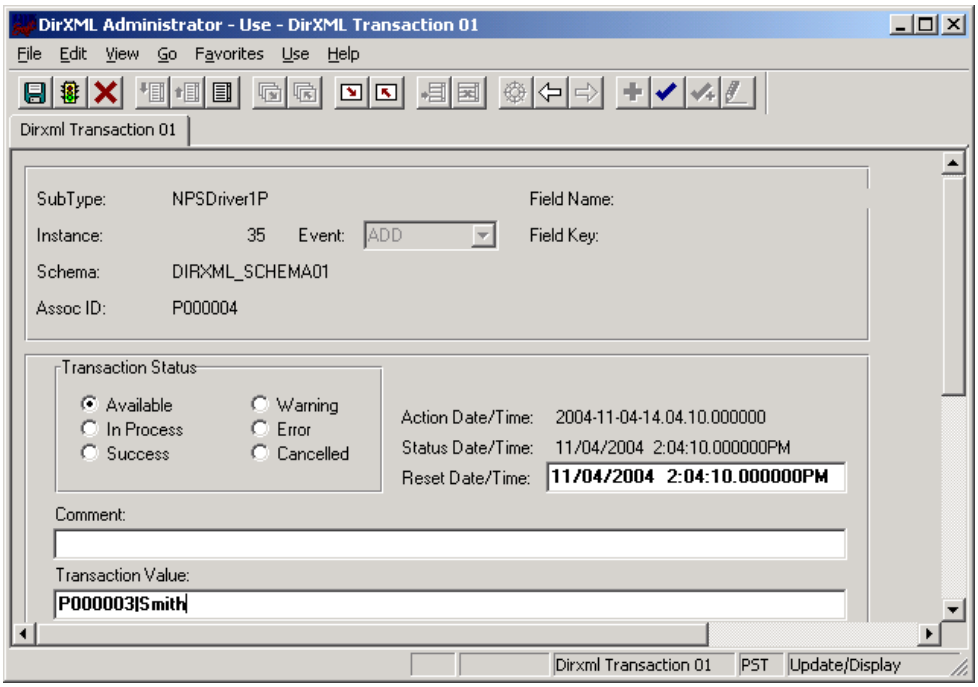
Transaction Component

The Transaction Component interface enables the driver to request transactions by driver subtype, date and time, and event type. The driver requests a single transaction for processing and obtains the object ID for the record being processed.

When the driver selects the first transaction to process, it sets the status of the transaction to In Process. The driver then retrieves the Event Name (DIRXML_EVENT), which it uses to create an Add, Modify, or Delete XML document. The driver uses the Schema ID (DIRXML_SCHEMA) and the Associate ID (DIRXML_ASSOC_ID) values to access the appropriate CI Schema and appropriate record information associated with the object.

After the transaction has been processed by the Identity Manager engine, the driver updates the status of the transaction (DIRXML_STATUS) and updates the **Comment** field (DIRXML_DESCR) if an error or warning message is applicable.

Figure 3-5 *DirXML Transaction01*



Schema Component

The Schema Component interface lets the driver retrieve data for a particular record and update the PeopleSoft staging table for that record. After the driver retrieves the Association ID (DIRXML_ASSOC_ID) and Schema name (DIRXML_SCHEMA), it accesses the appropriate Schema object.

The driver also uses Schema CI as a Class identifier for object type matching. When the driver accesses the Schema CI, it uses the value it received in the Association ID (DIRXML_ASSOC_ID) as the key value to retrieve the data from the PeopleSoft environment. It also uses this CI to update PeopleSoft records.

For example, assume you want to process transactions for an employee with the DIRXML_ASSOC_ID field (key) value = P000001. The driver accesses the Schema CI with a key value of P000001. It retrieves all of the configured component elements that have been defined for that employee. The driver then converts the data collection into XML documents to be consumed by the Identity Manager engine. If there is a write-back command processed, or when data is written on the Subscriber channel, the driver uses this CI to update the staging table with the appropriate information into PeopleSoft for this particular employee.

Testing Component Interfaces

The Component Tester program (`CITester.class`) is included as part of the driver package. The program validates the proper installation, configuration, and revision of the PeopleSoft PeopleTools client software on the computer hosting the Identity Manager Driver for PeopleSoft. The program also validates a selected Transaction CI and Schema CI. Successful operation of the CITester helps ensure the proper client functionality for the driver.

The CITester completes the following checks during four phases:

- Phase I: Ensures that a PeopleSoft client session can be created.
- Phase II: Ensures that connection and authentication parameters to the PeopleSoft Application Server are correct.
- Phase III: Verifies that the Transaction CI required fields and keys are present.
- Phase IV: Verifies that the Schema CI required fields and keys are present.

If you are not using the default Schema CI, it is necessary to build the APIs for the desired CI. See "Changing the Data Schema Component Interface" on page 53 for information on building custom CI API JAR files.

There might be variations of the error message data depending on the PeopleTools release. The CITester program runs all platforms supporting Java 1.3.1 or later and uses the Java PeopleSoft Component Interface (`psjoa.jar`) package from the PeopleTools distribution.

- "Important Considerations" on page 34
- "Running the Test" on page 35
- "Phase I: Creating a PeopleSoft Client Session" on page 35
- "Phase II: Authenticating to the PeopleSoft Client" on page 35
- "Phase III: Authenticating to the PeopleSoft Client" on page 36
- "Phase IV: Retrieving the Schema Component Interface" on page 38
- "Summary" on page 39

Important Considerations

When you run the test, you must do one of the following:

- Set the CLASSPATH environment variable to include the path of the `CITester.class`, `psjoa.jar` and `dirxmlcomps.jar` files. If a custom CI API JAR file is required, include it in CLASSPATH.
- Set the **-classpath** option on the Java command line to include the `CITester.class`, `psjoa.jar` and `dixmlcomps.jar` files and any required custom CI API JAR files.

In addition, the `java.exe` for JRE/JDK version 1.3.1 or later must be installed and accessible via the PATH environment variable or be explicitly called out from the Java command line.

Running the Test

From a command shell, execute the `CITester.class` test file. A sample `CITester.bat` file is provided as a reference that indicates the correct syntax and class files required to execute the test and the driver. To accept the test's default values, press Enter. In Phase II, you are required to enter a value for the Application Server name.

The test writes output to the screen and to `CITesterOutput.txt`. The output file is written to the location where `CITester.class` resides.

Phase I: Creating a PeopleSoft Client Session

If the test program establishes a session with the PeopleSoft client, you see the following message:

```
** PeopleSoft client session established successfully.
```

You might encounter the following errors during the test:

Error Message	Solution
`Exception in thread "main" java.lang.NoClassDefFoundError: psft/pt8/util/PSProperties.`	You must add a path to the 8.1*x* or 8.4*x* `psjoa.jar` file to the environment CLASSPATH variable or set the path to the `psjoa.jar` file in the Java command line. This error also occurs if an invalid version of the JVM (JRE/JDK) is being used. Refer to the Important Considerations at the beginning of this section for more information.

Phase II: Authenticating to the PeopleSoft Client

1. Specify the Application Server name or IP address. Forward slashes are required when you enter the Application Server name (for example, //255.255.255.255).
2. Specify the Application Server Jolt port number.
3. Specify the PeopleSoft UserID
4. Specify the PeopleSoft UserID password.

If the test program verifies the connection and authentication parameters, you see the following message indicating success:

```
** The Connection and Authentication Parameters are verified to be correct.
```

You might encounter the following errors during the test:

Error Message	Solution
`ERROR: Failed Connection to the PeopleSoft Application Server. Please make sure you entered your authentication information correctly.`	The target Application Server generates error and warning messages. This error indicates that you entered the wrong Application Server name or Application Server port number.
`PeopleSoft Error/Warning Messages Pending. Number of Messages: 1 Message 1: Connect Failed: No additional information available (90, 01)`	Ensure that the server name or address you entered contains a leading double slash (//) and that the address and name data is correct. Also, verify that you entered the Jolt port configured on the Application Server.

`ERROR: Failed Connection to the PeopleSoft Application Server. Please make sure you entered your authentication information correctly.`
 	
`PeopleSoft Error/Warning Messages Pending. Number of Messages: 1 Message 1: DOWNbea.jolt.ServiceException: Invalid Session`
	This message indicates an invalid Application Server name or port number. In some instances, if an invalid port number is specified, the CITester program hangs and requires a manual interrupt.

`PeopleSoft Error/Warning Messages Pending Number of Messages: 2`
 	
`Message 1: PeopleTools release (8.<num>) from web server '' is not the same as Application Server PeopleTools release (8.<num>) Access denied.`
	This message indicates that the PeopleTools version of the specified `psjoa.jar` does not match the version of the target PeopleSoft Application Server. PeopleTools requires a version match of the client and server.

`PeopleSoft Error/Warning Messages Pending. Number of Messages: 3`
 	
`Message 1: <UserID>@<Client computer> is an Invalid User ID, or you typed the wrong password. User ID and Password are required and case-sensitive. Make sure you're typing in the correct upper and lower case.`
 	
`Message 2: Failed to execute GetCertificate request`
 	
`Message 3: Invalid certificate for user <User ID>`
	The target Application Server generates the error and warning messages. Either the UserID or User ID password are incorrect or have been entered with the incorrect case.

Phase III: Authenticating to the PeopleSoft Client

The driver uses a Component Interface (CI) to access application modification transaction records from the Application Server. The field definitions of this interface must be identical to the DIRXML_TRANS01 CI delivered with the driver. This test phase validates the field definitions of the named Transaction CI.

Enter the Transaction CI name or press Enter to validate DIRXML_TRANS01.

If the test program retrieves and validates that all required fields and elements are present, you see the following message:

```
** Retrieval of Transaction Component Interface "DIRXML_TRANS01" succeeded.

- Property 'DIRXML_ASSOC_ID' is present.
- Property 'DIRXML_CURRDTTM' is present.
- Property 'DIRXML_DESCR' is present.
- Property 'DIRXML_DRIVER' is present and validated as key field.
- Property 'DIRXML_DTTM' is present.
- Property 'DIRXML_EVENT' is present.
- Property 'DIRXML_FIELDKEY' is present.
- Property 'DIRXML_FIELDNAME' is present.
- Property 'DIRXML_INST' is present and validated as key field.
- Property 'DIRXML_PROCESSED' is present.
- Property 'DIRXML_SCHEMA' is present.
- Property 'DIRXML_STATUS' is present.
- Property 'DIRXML_VALUE' is present.

** Transaction Component Interface element validation succeeded.
```

You might encounter the following errors during the test:

Error Message	Solution
`PeopleSoft Error/Warning Messages Pending. Number of Messages: 4Message 1: Cannot find Component Interface {<Transaction CI Name>} (91,2) Message 2: Initialization Failed (90,7) Message 3: Not Authorized (90,6) Message 4: Failed to execute PSSession request ERROR: Retrieval of Component Interface <Transaction CI Name> failed.`	The target Application Server generates error and warning messages. This error indicates that the Transaction CI name specified does not exist or cannot be found by the Application Server. Ensure that you specified the correct name.
`-Property '<property field name>' is not required.`	This is an advisory message. It indicates that an additional field or fields that are not required by the driver have been defined in the specified Component Interface.
`ERROR: Transaction Component Interface element validation failed. Required Fields are not all present.`	The specified Transaction Component Interface does not contain all of the fields required by the driver. Verify that you entered the proper Transaction Component Interface name and validate that all fields contained in the default DIRXML_TRANS01 Component Interface are present.
`ERROR: Property '<Key field name>' is not defined as key field.`	A field in the Transaction Component Interface is present, but is not properly configured as a key field. The Transaction Component Interface DIRXML_DRIVER and DIRXML_INST fields must be specified as key fields.

Phase IV: Retrieving the Schema Component Interface

The Schema CI defines the application data that is to be synchronized via the driver. The specified Schema CI must contain a primary key field that is specified via the Data Record ID field name.

To test the Schema CI, type the Schema CI name or press Enter to retrieve DIRXML_SCHEMA01. Enter the Data Record ID field name. If the test program retrieves and validates that all required fields and elements are present, you see the following message:

```
** Retrieval of Schema Component Interface "DIRXML_SCHEMA01" succeeded.

- Property 'ASSOC_ID' is present and validated as key field.
- Property 'STATUS' is present.
- Property 'FULL_NAME' is present.
- Property 'FIRST_NAME' is present.
- Property 'MIDDLE_NAME' is present and validated as key field.
- Property 'LAST_NAME' is present.
- Property 'BIRTH_DATE' is present.
- Property 'DEPT_ID' is present.
- Property 'DEPT_LONG_DESCR' is present.
- Property 'DEPT_DN' is present.
- Property 'TITLE_ID' is present.
- Property 'TITLE_SHORT_DESCR' is present.
- Property 'TITLE_LONG_DESCR' is present.
- Property 'MANAGER_ID' is present.
- Property 'MAIL_DROP' is present.
- Property 'ADDRESS1' is present.
- Property 'CITY' is present.
- Property 'STATE' is present.
- Property 'POSTAL' is present.
- Property 'MANAGER' is present.
- Property 'COMMON_NAME' is present.
- Property 'DISTINGUISHED_NAME' is present.
- Property 'DESCRIPTION' is present.
- Property 'EMAIL_ID' is present.
- Property 'PHONE_BUSN' is present.
- Property 'PHONE_CELL' is present.
- Property 'PHONE_HOME' is present.
- Property 'PHONE_PGR' is present.

** Schema Component Interface element validation succeeded.

** All expected platform support is verified correct.
```

You might encounter the following errors during the test:

Error Message	Solution
PeopleSoft Error/Warning Messages Pending. Number of Messages: 4 Message 1: Cannot find Component Interface {<Schema CI Name>} (91,2) Message 2: Initialization Failed (90,7) Message 3: Not Authorized (90,6) Message 4: Failed to execute PSSession request ERROR: Retrieval of Component Interface <Schema CI Name> failed.	The target Application Server generates error and Warning messages. This error indicates that the specified Schema CI name does not exist or cannot be found by the Application Server. Ensure that you specified the correct name.
ERROR: Specified Schema Component Interface Data Record ID Field '<Data Record ID Field Name>' not found.	The field name specified as the key field of the Schema Component Interface is not in the Component Interface definition. Verify that you entered the proper field name.
ERROR: Property '<Data Record ID Field Name>' is not defined as key field.	The field name specified as the key field of the Schema Component Interface is present but is not properly defined as the key field. Validate the Component Interface definition or verify that the proper field name was specified.

Summary

At the completion of the test, the program provides a summary containing the results of the test. The validated parameters are shown below in the summary.

```
Component Interface Test Summary
--------------------------------
Full Component Interface Functionality has been verified.
The following parameters may be used for PeopleSoft 5.0 Driver
Configuration

Authentication ID            : PSADMIN
Authentication context     : //255.255.255.255:9000
Application Password      : PSADMIN
Schema CI Name             : DIRXML_SCHEMA01
Data Record ID Field       : ASSOC_ID
Transaction CI Name       : DIRXML_TRANS01
```

4 Creating a New Driver Object

After the PeopleSoft driver files are installed on the server where you want to run the driver (see Chapter 2, "Installing the Driver Files," on page 19) and you have configured your PeopleSoft environment (see Chapter 3, "Configuring Your PeopleSoft Environment," on page 21), you can create the driver in the Identity Vault. You do so by installing the driver packages and then modifying the driver configuration to suit your environment. The following sections provide instructions:

- "Creating a PeopleSoft Account" on page 41
- "Creating the Driver Object in Designer" on page 41
- "Deploying, Starting and Activating the Driver" on page 46
- "Adding Packages to an Existing Driver" on page 46

Creating a PeopleSoft Account

The driver requires an administrative account for the PeopleSoft system. The driver uses this account to authenticate to PeopleSoft and make changes. You can use an existing administrative account; however, we recommend that you create an administrative account exclusively for the driver.

Creating the Driver Object in Designer

You create the PeopleSoft driver by installing the driver packages and then modifying the configuration to suit your environment. After you create and configure the driver, you need to deploy it to the Identity Vault and start it.

NOTE: To create drivers, you now need to use the new package management features provided in Designer.

- "Importing the Current Driver Packages" on page 41
- "Installing the Driver Packages" on page 42
- "Configuring the Driver" on page 45

Importing the Current Driver Packages

The driver packages contain the items required to create a driver object, such as policies, entitlements, filters, and Schema Mapping policies. These packages are only available in Designer. You can upgrade any package that is installed if there is a newer version of the package available.It is

recommended to have the latest packages in the Package Catalog before creating a new driver object. For more information on upgrading packages, see "Upgrading Installed Packages" in the *NetIQ Designer for Identity Manager Administration Guide*.

To verify you have the most recent version of the driver packages in the Package Catalog:

1 Open Designer.

2 In the toolbar, click **Help** > **Check for Package Updates**.

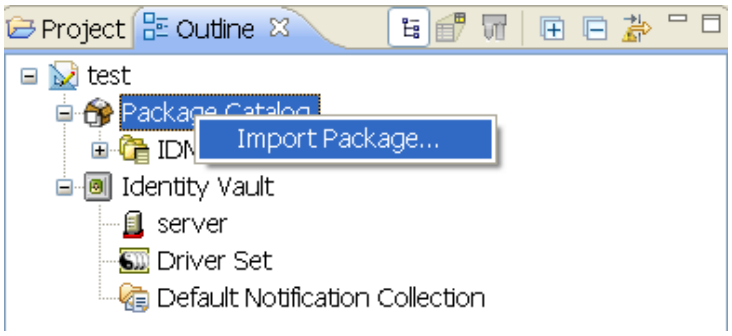
3 Click **OK** to update the packages

   or

   Click **OK** if the packages are up-to-date.

4 In the Outline view, right-click the Package Catalog.

5 Click **Import Package**.



   You can download the new packages from the *Download site* (https://download.microfocus.com/Download?buildid=xGC_suQ7uiM~).

6 Select any PeopleSoft driver packages

   or

   Click **Select All** to import all of the packages displayed.

   By default, only the base packages are displayed. Deselect **Show Base Packages Only** to display all packages.

7 Click **OK** to import the selected packages, then click **OK** in the successfully imported packages message.

8 After the current packages are imported, continue with "Installing the Driver Packages" on page 42.

Installing the Driver Packages

After you have imported the current driver packages into the Package Catalog, you can install the driver packages to create a new driver.

1 In Designer, open your project.

2 In the Modeler, right-click the driver set where you want to create the driver, then click **New** > **Driver**.

3 Select **PeopleSoft Base**, then click **Next**.

4 Select the optional features to install for the PeopleSoft driver, then click **Next**. All options are selected by default.

PeopleSoft Password Synchronization: This package contains the policies that enable the PeopleSoft driver to synchronize passwords. If you want to synchronize passwords, verify that this option is selected. For more information, see the NetIQ Identity Manager Password Management Guide.

Managed System Information: This package contains the policies that enable Identity Reporting. For more information, see the Administrator Guide to NetIQ Identity Reporting.

5 (Conditional) If there are package dependencies for the packages you selected to install, you must install them to install the selected package. Click **OK** to install the package dependency listed.

6 (Conditional) If more than one type of package dependency must be installed, you are presented with these packages separately. Continue to click **OK** to install any additional package dependencies.

7 (Conditional) On the Install Common Settings page, fill in the following fields, then click **Next**:

The Common Settings page is displayed only if the Common Settings package is installed as a dependency.

User Container: Select the Identity Vault container where the PeopleSoft accounts will be added if they don't already exist in the vault. This value becomes the default for all drivers in the driver set.

If you want a unique location for this driver, set the value for all drivers on this page. After the driver is created, change the value on the driver's Global Configuration Values page.

Group Container: Select the Identity Vault container where the PeopleSoft accounts will be added if they don't already exist in the vault. This value becomes the default for all drivers in the driver set.

If you want a unique location for this driver, set the value for all drivers on this page. After the driver is created, change the value on the driver's Global Configuration Values page.

8 On the Driver Information page, specify a name for the driver, then click **Next**.

9 On the Application Authentication page, fill in the following fields, then click **Next**:

Authentication ID: Specify the authentication ID for the driver.

Connection Information: Specify the connection information for the driver to connect to the PeopleSoft system.

Password: Specify the password for the authentication ID.

10 Fill in the following fields for Remote Loader information:

Connect To Remote Loader: Select **Yes** or **No** to determine if the driver will use the Remote Loader. For more information, see Configuring the Remote Loader and Drivers in the *NetIQ Identity Manager Setup Guide for Linux* or Configuring the Remote Loader and Drivers in the *NetIQ Identity Manager Setup Guide for Windows*.

If you select **No**, then click **Next**. If you select **Yes**, use the following information to complete the configuration of the Remote Loader, then click **Next**:

Host Name: Specify the IP address or DNS name of the server where the Remote Loader is installed and running.

Port: Specify the port number for this driver. Each driver connects to the Remote Loader on a separate port. The default value is 8090.

KMO: Specify the key name of the Key Material Object containing the keys and certificates used for SSL. It is only used when there is an SSL connection between the Remote Loader and the Identity Manager engine.

Other Parameters: Specify other parameters required for the driver in the connection string.These parameters must be in the key-value pair. For example, paraName1=paraValue1.

Remote Loader Password: Specify a password to control access to the Remote Loader. It must be the same password that is specified as the Remote Loader password on the Remote Loader.

Driver Password: Specify a password for the driver to authenticate to the Identity Manager server. It must be the same password that is specified as the Driver Object password on the Remote Loader.

11 (Conditional) On the Install PeopleSoft Managed System Information page, fill in the following fields to define your PeopleSoft system, then click **Next**:

The Install PeopleSoft Managed System Information page is displayed only if you selected to install the Managed System packages.

Name: Specify a descriptive name for this PeopleSoft system. The name is displayed in reports.

Description: Specify a brief description for this PeopleSoft system. The description is displayed in reports.

Location: Specify the physical location of this PeopleSoft system. The location is displayed in reports.

Vendor: Specify the vendor of PeopleSoft system. This information is displayed in reports.

Version: Specify the version of this PeopleSoft system. The version is displayed in the reports.

12 (Conditional) On the Install PeopleSoft Managed System Information page, fill in the following fields to define the classification of the PeopleSoft system, then click **Next**:

The Install PeopleSoft Managed System Information page is displayed only if you selected to install the Data Collection and Account Tracking packages.

Classification: Select the classification of the PeopleSoft system. This information is displayed in the reports. Your options are:

- Mission-Critical
- Vital
- Not-Critical
- Other

  If you select **Other**, you must specify a custom classification for the PeopleSoft system.

Environment: Select the type of environment the PeopleSoft system provides. The options are:

- Development
- Test
- Staging
- Production
- Other

  If you select **Other**, you must specify a custom classification for the PeopleSoft system.

13 (Conditional) On the Install PeopleSoft Managed System Information page, fill in the following fields to define the ownership of the PeopleSoft system, then click **Next**:

The Install PeopleSoft Managed System Information page is displayed only if you selected to install the Data Collection and Account Tracking packages.

Business Owner: Select a user object in the Identity Vault that is the business owner of the PeopleSoft system. This can only be a user object, not a role, group, or container.

Application Owner: Select a user object in the Identity Vault that is the application owner of the PeopleSoft system. This can only be a user object, not a role, group, or container.

14 (Conditional) On the Install PeopleSoft Password Synchronization page, fill in the following fields, then click **Next**:

The Install PeopleSoft Password Synchronization page is displayed only if you selected to install the Password Synchronization packages.

Identity Manager accepts passwords from application: Select **True** to allow passwords to flow from the connected system to the Identity Vault.

Publish passwords to NDS password: Select **True** to use the password from the connected system to set the non-reversible NDS password in the Identity Vault.

Publish passwords to Distribution Password: Select **True** to use the password from the connected system to set the NMAS Distribution Password used for Identity Manager password synchronization.

Require password policy validation before publishing passwords: Select **True** to apply the NMAS password policies during publish password operations. The password is not written to the Identity Vault if it does not comply.

Notify the user of password synchronization failure via e-mail: Select **True** to notify the user by e-mail of any password synchronization failures.

15 Review the summary of tasks that will be completed to create the driver, then click **Finish**.

16 After you have installed the driver, you must change the configuration for your environment. Proceed to "Configuring the Driver" on page 45.

Configuring the Driver

After importing the packages, you need to configure the driver before it can run. You should complete the following tasks to configure the driver:

- **Ensure that the driver can authenticate to PeopleSoft:** Make sure that you have established a PeopleSoft administrative account for the driver (see "Creating a PeopleSoft Account" on page 41) and that the correct authentication information, including the User ID and password, is defined for the driver parameters (see "Authentication ID:" on page 80).
- **Configure the driver parameters:** There are many settings that can help you customize and optimize the driver. The settings are divided into categories such as Driver Configuration, Engine Control Values, and Global Configuration Values (GCVs). Although it is important for you to understand all of the settings, your first priority should be to configure the driver parameters located on the Driver Configuration page. For information about the driver parameters, see "Driver Parameters" on page 81.
- **Configure the driver policies and filter:** Modify the driver policies and filter to implement your business policies. For instructions, see "Modifying Driver Policies" on page 56.
- **Configure password synchronization:** The basic driver configuration supports password synchronization through Universal Password. If you don't want this setup, see Configuring Password Flow in the NetIQ Identity Manager Password Management Guide.

After completing the configuration tasks, continue with the next section, Deploying, Starting and Activating the Driver.

Deploying, Starting and Activating the Driver

After installing and configuring the driver you must deploy, start and activate it. To perform the respective operations see:

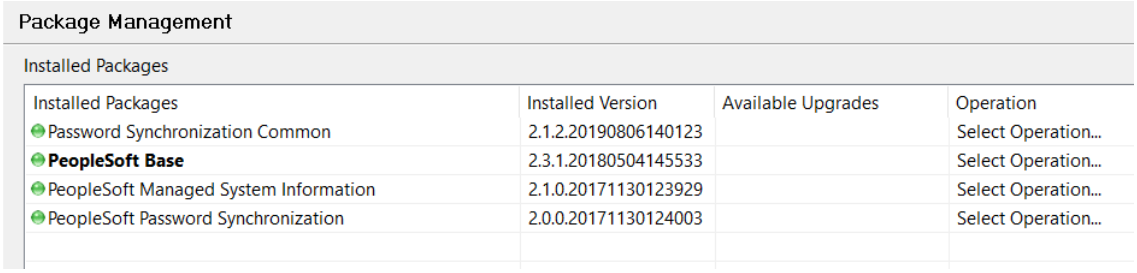
- Deploying the Driver in "*NetIQ Identity Manager Driver Administration Guide*"
- Starting the Driver in "*NetIQ Identity Manager Driver Administration Guide*"
- Activating Drivers in "*NetIQ Identity Manager Driver Administration Guide*"

Adding Packages to an Existing Driver

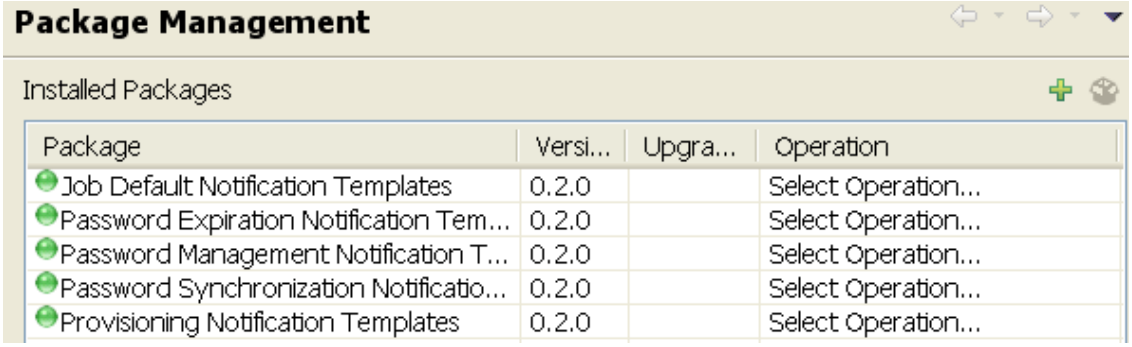
You can add new functionality to an existing driver by adding new packages to an existing driver.

1. Right-click the driver, then click **Properties**.
2. Click **Packages**, then click the **Add Packages** icon .
3. Select the packages to install. If the list is empty, there are no available packages to install.
4. (Optional) Deselect the **Show only applicable package versions** option, if you want to see all available packages for the driver, then click **OK**.

   This option is only displayed on drivers. By default, only the packages that can be installed on the selected driver are displayed.
5. Click **Apply** to install all of the packages listed with the Install operation.



6. (Conditional) Fill in the fields with appropriate information to install the package you selected for the driver, then click **Next**.
7. Read the summary of the installation, then click **Finish**.
8. Click **OK** to close the Package Management page after you have reviewed the installed packages.



9 Repeat Step 1 through Step 8 for each driver where you want to add the new packages.

5 Upgrading an Existing Driver

The following sections provide information to help you upgrade an existing driver:

- "Supported Upgrade Paths" on page 49
- "Upgrade Procedure" on page 49

Supported Upgrade Paths

You can upgrade from any 3.*x* version of the PeopleSoft driver. Upgrading a pre-3.*x* version of the driver directly to version 4.x or later is not supported.

Upgrade Procedure

The process for upgrading the PeopleSoft driver is the same as for other Identity Manager drivers. For detailed instructions, see *NetIQ Identity Manager Setup Guide for Linux* or *NetIQ Identity Manager Setup Guide for Windows*.

6 Customizing the Driver

This section covers how you can customize the driver by triggering transactions through the PSA via PeopleCode.

- "Customizing the PSA by Triggering Transactions" on page 51
- "Changing the Data Schema Component Interface" on page 53
- "Modifying Driver Policies" on page 56
- "SSL Configuration for PeopleSoft Application" on page 69

Customizing the PSA by Triggering Transactions

Transaction record creation is triggered by PeopleCode associated with modifications and additions to data on the Schema Data record (DIRXML_S_PERS) and row Delete events on the Staging record (DIRXML_SCHEMA01). If desired, the PeopleSoft administrator or consultant can use these examples to trigger transactions based on other events within the PeopleSoft application.

NOTE: The D Event Type operation has been redefined for the 5.0*x* PeopleSoft Service Agent (PSA). The D Event Type is now generated for application object Delete events instead of object Disable events. All Modification events now generate M (Modify) transaction events.

The default Transaction creation function is defined on the DIRXML_DRIVER field of the DIRXML_DERIVED Record definition:

A PeopleCode function call would be as follows:

```
DirXML_Trans( Transaction Table Name,
    Transaction Channel Type,
          Schema CI Name,
          Event Type,
          Schema Record Key Value,
          Transaction Date and Time,
          Transaction Miscellaneous Info,
          Collection Row Delete Field Name,
          Collection Row Delete Field Key Value,
          Transaction Status);
```

An example of sample Modification event transaction from the PSA looks like this:

```
DirXML_Trans("DIRXML_TRANS01",
      &channel,
        "DIRXML_SCHEMA01",
        "A",
        DIRXML_S_PERS.DIRXML_S_ID,
        %DateTime,
        &tValue,
        "",
        "",
        "A");
```

Table 6-1 *Function Call Parameter Definitions*

Parameter	Description	Default Value
Transaction Table	The name of the table where transactions are written. This table is built within PeopleTools and the field elements should be consistent with the delivered DIRXML_TRANS01 table.	DIRXML_TRANS01
Transaction Channel Type	The name used to identify the driver that processes the transactions and the channel that created the transactions.	The NPSDriver1S transaction was caused by a Subscriber channel event and is processed by driver NPSDriver1. The NPSDriver1P transaction was caused by a Publisher channel event and is processed by driver NPSDriver1.
Schema CI Name	The name of the Schema CI object that the transaction type is connected to. The driver uses the name of this object to query for the data connected to the transaction type.	DIRXML_SCHEMA01
Event Type	The type of XML event that is written to the transaction table. This can be 1 of 4 values as listed.	A=ADD M=MODIFY D=DELETE R=ROW DELETE
Schema Record Key Value	The identifier that is used to associate a particular record within PeopleSoft to an eDirectory object. It could be the EMPLID value for employees, STUDENTID value for students, DEPTID for departments, ACCTID for account codes, and so forth. Key elements must be identified for the Transaction Schema.	ASSOC_ID
Transaction Date Time	The date/time element used to determine when the transaction is processed.	%Datetime

Parameter	Description	Default Value
Transaction Miscellaneous Info	The parameter contains 1...n values that the developer wants to pass to the driver during processing. This value might not be available via the Schema object when a transaction is processed by the driver.	ASSOC_ID | "|" | LAST_NAME
Collection Row Delete Field Name	The field name of the scroll level attribute in the application record.	DIRXML_S_PHONES
Collection Row Delete Field Key	The key field value of the deleted data row (CELL, PGR, BUSN).	
Transaction Status	The initial processing status of the transaction. Generally this value is set to A for Available. For Subscriber delete events, it is not desirable for the driver to process the transaction event. Therefore, delete event transactions generated by the default PSA are assigned a status of S for Success.	

Changing the Data Schema Component Interface

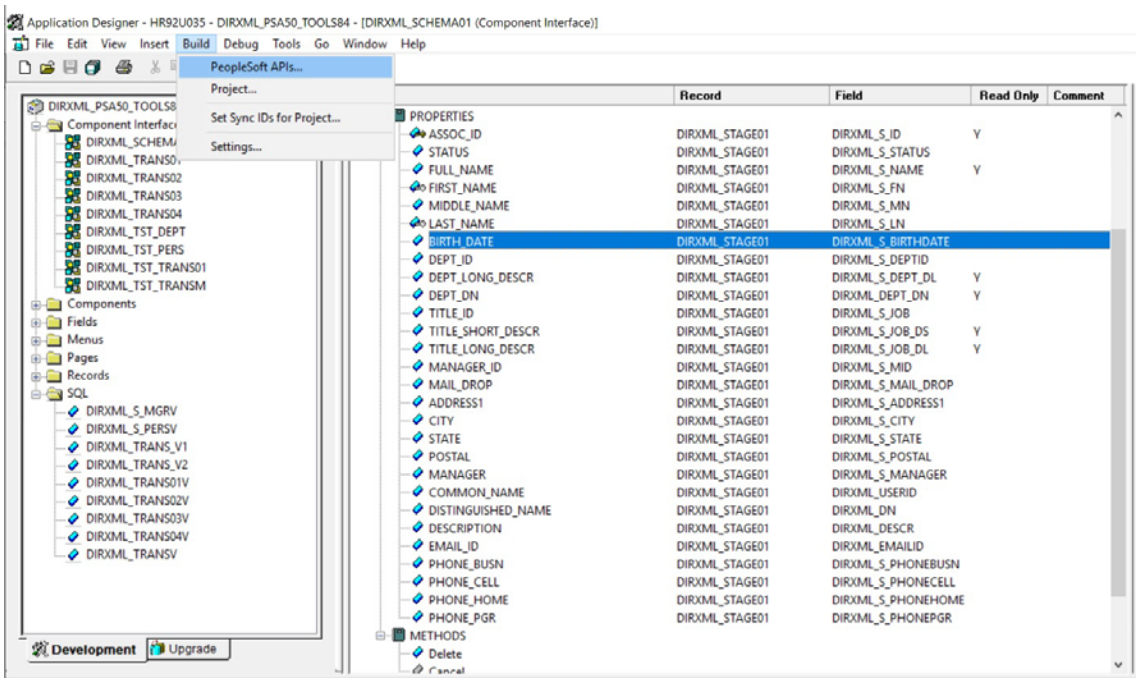
The driver is preconfigured to use the Component Interfaces (CIs) defined in the PSA. The APIs for these CIs have been compiled and combined into the `dirxmlcomps.jar` file. At run time, the driver imports the interfaces required to interact with the appropriate CI.

If the driver is configured to use different data schema CIs, the Java APIs for these CIs also need to be built, compiled, and archived into a `.jar` file. The directions for building the CI APIs is documented in the **PeopleBooks > PeopleSoft Component Interfaces > Programming Component Interfaces in Java > Building APIs in Java** section of the PeopleTools documentation. (It is not necessary to rebuild all of the Java CI APIs, just those that are associated with your new schema CI.) The compiled and archived `.jar` file should be placed in the DirXML `/lib` subdirectory with the `psoftshim.jar` file.

- "Building the PeopleSoft Java Component Interface API" on page 53
- "Compiling the Java CI API" on page 55
- "Building the CI API JAR File" on page 55

Building the PeopleSoft Java Component Interface API

1. In the PeopleTools Application Designer, select the Schema CI you want to build.
2. Click **Build > PeopleSoft APIs**. In this example, the **DirXML_SCHEMA01 CI** is used.



3 In the Build PeopleSoft API Bindings dialog box, select the **build** option for the Java classes.

4 Select a target directory for the Java CI APIs (For our example, `C:\newci`).

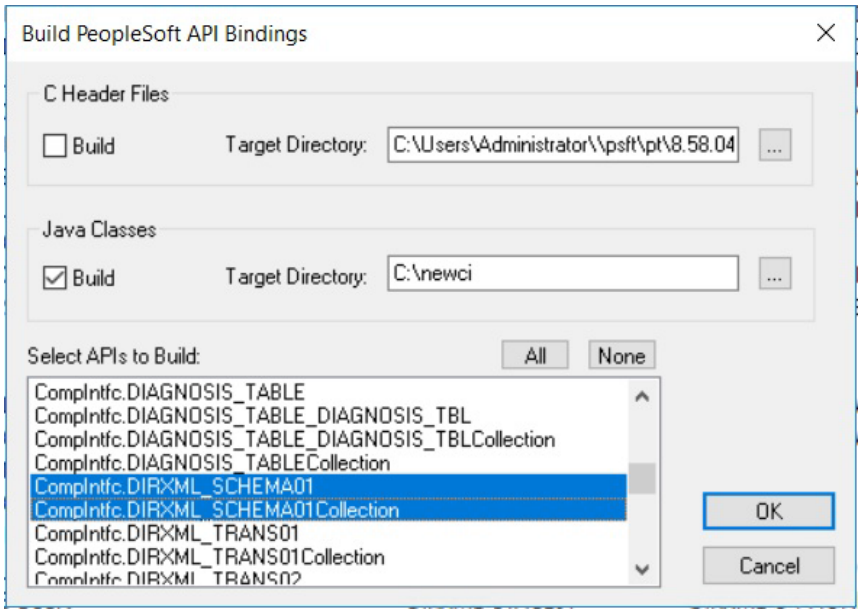
5 For the **Select APIs to Build** prompt, click **None** to deselect all CIs.

6 Using the scroll area, select the CIs for which you wish to generate an API. Make sure you select all CIs that begin with the name of the desired interface. This example uses CompIntfc.DIRXML_SCHEMA01 and CompIntfc.DIRXML_SCHEMA01Collection.

IMPORTANT: In addition to your schema CIs, you must always select the CompIntfc.CompIntfcPropertyInfo and CompIntfc.CompIntfcPropertyInfoCollection APIs. They are required in order to compile the schema APIs.

---

7 Click **OK** to generate the CI APIs. You might be prompted to create the target directory you specified.



The Application Designer status window should show a `Generating API Wrappers` message with the selected CIs, and then a `Done` message.

Compiling the Java CI API

After the APIs are generated, they must be compiled. The files are in `C:\newci\PeopleSoft\Generated\CompIntfc`. For our example, there should be eight Java files in this directory, including the four selected CI API files and four associated Java Interface files. Change directories to the file location and compile the Java files, using an appropriate JVM with a classpath argument specifying the PeopleTools `psjoa.jar` file.

An example command line is:

```
javac -classpath c:\psoft\pt84\class\psjoa.jar *.java
```

After a successful compile, there is a `.class` file for each `.java` file in the directory.

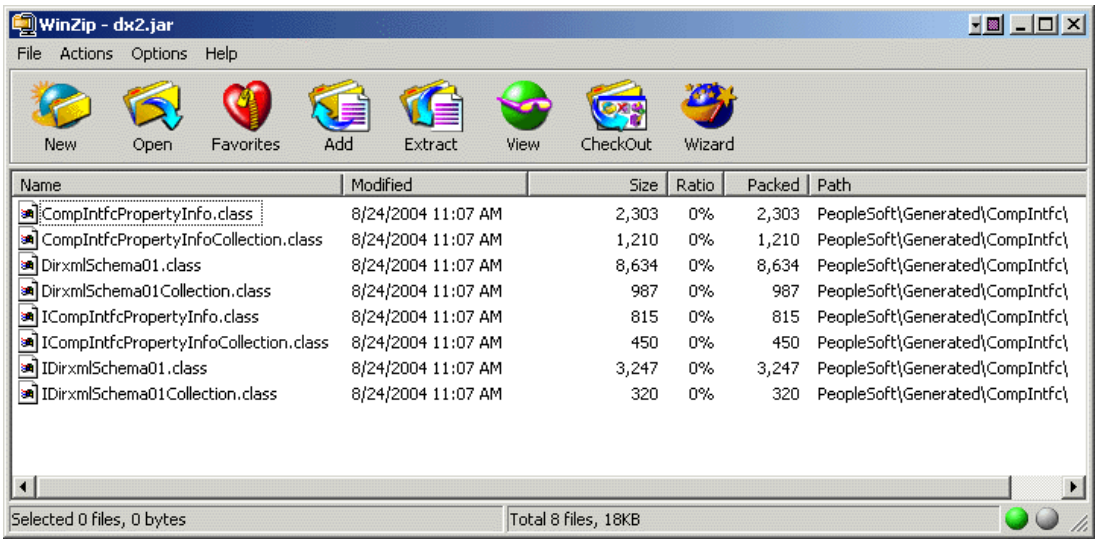
Building the CI API JAR File

The final step of the build process is the generation of a `.jar` file containing the compiled `.class` files. It is important that the full class path be generated with the JAR file, so the process must begin at the root of the CI API directory, `C:\newci`. From this directory, use the following command line:

```
jar cvf0M newci.jar PeopleSoft/Generated/CompIntfc/*.class
```

This command builds a JAR file called `newci.jar` that is comprised of the previously compiled `.class` files and contains the full class paths. The contents of the file can be verified by using WinZIP or another appropriate tool.

Figure 6-1 Building a New .jar File



If the driver is currently running, it must be stopped. If you are using the Remote Loader, the driver must be shut down. If you are using a local driver, it is also necessary to shut down eDirectory.

Copy the new JAR file to the same lib location with the driver components `psoftshim.jar`, `dirxmlcomps.jar`, and `psjoa.jar`. Restart eDirectory (if required) and the driver and Remote Loader.

Modifying Driver Policies

The following sections contains information to help you understand how the driver's policies are implemented, as well as information about how you can modify these objects:

- "Modifying the Driver Mapping Policy" on page 57
- "Using the Schema Query to Refresh the PeopleSoft Schema Component Interface" on page 57
- "Publisher Channel Objects" on page 57
- "Understanding the Publisher Filter" on page 58
- "Publisher Filter Attributes" on page 58
- "Securing the Data" on page 59
- "Publisher Object Policies" on page 59
- "Subscriber Channel Objects" on page 64
- "Understanding the Subscriber Filter" on page 65
- "Securing the Data" on page 66
- "Modifying the Filter" on page 66
- "Subscriber Object Policies" on page 66

Modifying the Driver Mapping Policy

The Mapping policy is a NetIQ eDirectory object that defines the relationship between data fields defined in the PeopleSoft application and eDirectory attributes. The Mapping policy is located in the driver object container and is used by both the Publisher and Subscriber channels of the driver.

A preconfigured default Mapping policy is delivered with the driver product. The mappings defined in the Mapping policy are designed in coordination with the preconfigured PeopleSoft application Component Interface (CI) that is also delivered with the driver product.

The default Data Schema CI is called DIRXML_SCHEMA01 and represents a set of employee data. The data fields in this CI are mapped to similar attributes of the eDirectory User object.

The following is a short sample of the delivered Mapping policy in `.xml` format. The nds-name represents the name of the class or attribute in eDirectory and the app-name represents the class or field name of the PeopleSoft CI.

```
<?xml version="1.0" encoding="UTF-8"?> <attr-name-map>
     <class-name>
          <nds-name>User</nds-name>
          <app-name>DIRXML_SCHEMA01</app-name>
     </class-name>      <attr-name classname="User">
          <nds-name>Given Name</nds-name>
          <app-name>FIRST_NAME</app-name>
     </attr-name>      ... </attr-name-map >
```

When you modify or create a Mapping policy, verify that the PeopleSoft field names appear identically (spelling and capitalization) in the Mapping policy and PeopleSoft CI definition. If you use the Identity Manager Mapping policy editor, correct mapping behavior is ensured. It is also important to note that if new attributes are included or removed from the Mapping policy, the new attribute set should be reflected in the respective Publisher and Subscriber filters. If mapped attributes are not included in the filters, they cannot be synchronized.

Using the Schema Query to Refresh the PeopleSoft Schema Component Interface

By default, the schema that the driver reads from PeopleSoft consists of the data fields defined on the DIRXML_SCHEMA01 CI. If the data elements are modified, the CI is renamed, or additional Data Schema CIs are added to the driver configuration, it is necessary to refresh the PeopleSoft application schema definition and re-map affected attributes.

Publisher Channel Objects

The Publisher object contains a filter and a set of policies. Policies are necessary for converting data from the PeopleSoft CI into XDS format. The driver then submits the data to the Identity Manager engine. The engine applies the Publisher filter to the data and applies the business logic defined by the Publisher policies prior to submitting the data to Identity Vault.

Understanding the Publisher Filter

The Publisher filter is a logical component of the driver filter object. The filter specifies the object classes and accompanying attributes that are passed from the PeopleSoft CI to eDirectory. The filter is defined by using eDirectory attribute naming, so it is applied after schema mapping takes place.

For example, if the User class is specified in the Publisher filter with only the Surname and Given Name attributes, the Identity Manager engine allows changes to only these attributes to be passed to the Publisher policies from the PeopleSoft Driver. If a Telephone Number attribute is modified, the Publisher filter removes this data from the event document because the Telephone Number attribute is not in the filter. Other attribute values can be created by the Publisher policies according to the integration scenario.

You can configure the Publisher filter to include attributes required by your environment and allowable by eDirectory access controls. Configure it to include the following:

- Object classes that you want to synchronize.
- Attributes on those objects that you want to synchronize.
- Attributes that are required by your Publisher policies. These attributes are not synchronized, but are required to perform some defined business logic that is to be applied to the synchronized data. These are known as “notify” attributes.

The Publisher filter specifies a set of data to be considered as authoritative from the PeopleSoft database. Based on business logic, there might be multiple authoritative sources of specific data (such as another driver or eDirectory itself). The configuration of the filters in your environment determines data ownership and authority.

Publisher Filter Attributes

By default, PeopleSoft applications are considered to be highly authoritative. Therefore, most of the field names in the default DIRXML_SCHEMA01 Component Interface are passed through the Publisher filter. As noted earlier, the names of attributes in the filter are eDirectory attribute names that have been mapped via the Mapping policies.

The Publisher channel attributes listed below are included in the default filter:

Table 6-2 Publisher Channel Attributes

departmentNumber	OU
employeeStatus	pager
Full Name	Physical Delivery Office Name
Given Name	Postal Code
homePhone	S
Initials	SA
isManager	Surname
jobCode	Telephone Number
mailstop	Title
managerWorkforceID	workforceID
mobile	

Most of the attributes in the Driver Filter are configured for bidirectional synchronization. This is done for sample purposes to allow the driver to perform add, modify, and delete operations on both the Subscriber and Publisher channels. In most installations, the driver policies and filter are configured to function in either a predominant Subscriber or Publisher mode.

Securing the Data

PeopleSoft applications, like many other applications, contain sensitive data that must be highly secured by organizations. There are two ways to ensure that secure data is not published from the PeopleSoft application:

- Remove it from the synchronized data CI definition.
- Remove it from the Publisher filter.

The first method guarantees that the data does not leave the PeopleSoft application. The second method guarantees that the data is not synchronized to Identity Vault via the driver.

Publisher Object Policies

Policies contain rules or templates that perform specific operations that can manipulate data, query either Identity Vault or PeopleSoft for additional data required for processing, create new attributes based on values of other attributes, or even discard entire data events. The following sections explain each policy and describe the operations of each policy or template. Because XML, DirXML Script, and XSLT allow for great flexibility, all policies can be modified to meet the individual needs of your organization. The Mapping policy has been previously described and is addressed in this section under "Modifying the Driver Mapping Policy" on page 57.

The Publisher channel object, by default, contains or uses the following policies:

- "Input Transformation Policy" on page 60
- "Matching Policy" on page 60

- "Create Policy" on page 60
- "Placement Policy" on page 61
- "Command Transformation Policy" on page 61

Input Transformation Policy

The Input Transformation policy is implemented as a default policy for the PeopleSoft Driver. Although the Input Transformation policy is not exclusively used by the Publisher channel, it performs a publishing role because it is used to transform the data format of any XDS document received from the PeopleSoft Driver shim, regardless of which channel generated the submission of the document. That is, the Subscriber channel can issue object queries to the driver shim. All data returned in the response is processed through the Input Transformation policy. An example of data transformation contained in this policy is the transformation of character attributes in PeopleSoft to Boolean attributes in eDirectory.

Manager Flag Data Transformation Template

This template, contained in the Input Transformation policy, converts the Y or N data values in the PeopleSoft Manager attribute into True or False Boolean values to reflect the data format of the Identity Vault's Manager attribute.

Matching Policy

The Matching policy is used by the Identity Manager engine to apply criteria to determine if a matching data object already exists in Identity Vault. The Matching policy is applied to all Add documents received from the PeopleSoft Driver shim. If a match is found by this policy, the Add event is automatically converted to a Modify event by the Identity Manager engine. If a matched object in eDirectory is not currently associated with the PeopleSoft application, an association is created.

The Matching policy should provide criteria that are guaranteed to produce a 0 or 1 match. More than one policy can exist, and the Identity Manager engine applies them in the order that they are defined. Any policy producing 0 or more matches is skipped and the next policy is applied. Processing finishes when one match is found or after the last policy has been processed.

The default Publisher Matching policy is a DirXML Script policy that attempts to match eDirectory User objects containing the same value in the workforceID attribute (mapped from the DIRXML_SCHEMA01 attribute). A secondary policy attempts to match using the Surname and Given Name attribute.

Create Policy

The Create policy is used to specify the criteria for creating a new object after the Matching policy has failed to find a match. This policy performs various tests and transformations based on the requirements for object creation in eDirectory and the business logic being applied.

The default PeopleSoft Create policy is an XML policy that asserts that the <add> document is for a User object and that it must contain a Surname and Given Name attribute. The Surname attribute is mandatory in eDirectory, and the business logic used for object naming requires the existence of the

Given Name attribute. If this criteria is met, a secondary XSLT style sheet policy is called to create the eDirectory Name attribute. A final policy is provided to append a default password to new User objects.

Placement Policy

The Placement policy defines where an object is placed in the eDirectory tree when the object is created. This placement can be determined based on the presence (or absence) of attributes, particular values of attributes, etc. Placement can also be determined by the Create policy and passed to the Placement policy.

In a typical PeopleSoft HR environment, an employee is hired within PeopleSoft, a notification is sent to the IS department, and an IS administrator determines the location of the new User object in the eDirectory tree. Before defining location policies in the Placement policy, analyze your organization's current business process.

The default PeopleSoft Placement policy is a DirXML Script policy that handles placement of User objects based on the employeeStatus attribute. It uses the following order of processing: If the employeeStatus value is A, the employee is placed in the Organizational Unit specified by the Active Users Container GCV value. If the employeeStatus is I, the employee’s User object is placed in the Organizational Unit as specified by the Inactive Users Container GCV value. If the employeeStatus attribute is not present, the employee’s User object is placed in the Organizational Unit as specified by the Inactive Users Container GCV value.

Command Transformation Policy

The Command Transformation policy is the final transformation policy to be processed prior to submission of a Publisher document to Identity Vault. To demonstrate this functionality, the default PeopleSoft Driver configuration implements an unusual example of business logic that demonstrates the flexibility and power of Identity Manager.

The business logic scenario is a requirement to maintain the object CN attribute and full distinguished name DN of each User in the PeopleSoft application. The CN attribute is generated on new objects when they are created in eDirectory. The DN is not a true attribute, but a concatenation of the directory path and CN of a User. The DN changes based on the employeeStatus attribute of an object, so it is set on User Add events and Delete events that are transformed into Move events.

Because this data is known during the processing of the Command Transformation policy, the CN and DN data is placed into an `<operation-data>` element appended to the document, causing the object to be added or moved. After Identity Manager applies the data to Identity Vault, a status document is returned. The Output Transformation policy (documented in the Subscriber channel) monitors status documents that are returned and transforms successfully processed documents with attached `<operation-data>` elements into modification documents that are applied to the PeopleSoft application. This is known as *write-back functionality*.

As the final transformation policy, the Command Transformation policy provides an excellent location to define operations that must be applied without the risk of further event transformation, thus allowing complicated policy processing to be programmed in one location. The bulk of the business logic transformations in the Publisher channel are implemented in this policy.

The following templates exist in the default Command Transformation policy. In addition to the listed templates, all Identity Manager policies contain identity-transform templates that allow the copying of XML attributes and elements that are passed through unmodified. The default configuration only handles documents related to User objects.

- "match <add> element" on page 62
- "match <modify> element" on page 63
- "get-empl-status" on page 63
- "get-empl-isManager" on page 63
- "get-empl-CN" on page 63
- "get-empl-managerWorkforceID" on page 63
- "get-empl-ID" on page 63
- "set-manager-on-user" on page 63
- "set-manager-on-direct-reports" on page 64
- "clear-manager-on-direct-reports" on page 64
- "set-directReports-on-manager" on page 64
- "clear-directReports-on-manager" on page 64
- "set-directReports-on-user" on page 64

match <add> element

This template does the following:

- Tries to find the User's manager. If the manager is found and the manager's employeeStatus attribute is set to A, the template sets the manager and managerWorkforceID attribute on the User.
- Sets the Login Disabled attribute based on employeeStatus. If the status is A, Login Disabled is set to False. If the status is I, then Login Disabled is set to True.
- Adds or removes the Group Membership value based on the employeeStatus attribute value. All active employees with the isManager attribute set to False are placed into an Employee Group. All active employees with the isManager attribute set to True are placed into a Manager Group. The Group Membership attribute and associated links on the group objects are cleared if the employeeStatus is set to I.
- Determines placement of an object based on the employeeStatus attribute value. Active User objects are placed in an Active Organizational Unit. Inactive User objects are placed in an InActive Organizational Unit.
- Adds the manager attribute to any other active User objects in the directory whose managerWorkforceID attribute specifies this new User.
- Adds the directReports attribute value to any active User object in the directory that is specified by this User's managerWorkforceID attribute.
- Generates a write-back `<operation-data>` element to facilitate the addition of the CN and DN attributes in PeopleSoft.

match <modify> element

This template does the following:

- Tries to find the User's manager. If the manager is found and the manager's employeeStatus attribute is set to A, the template sets the manager and managerWorkforceID attribute on the User.
- Sets the Login Disabled attribute based on employeeStatus. If the status is A, Login Disabled is set to False. If the status is I, then Login Disabled is set to True.
- Adds or removes the Group Membership value based on the employeeStatus attribute value. All active employees with the isManager attribute set to False are placed into an Employee Group. All active employees with the isManager attribute set to True are placed into a Manager Group. The Group Membership attribute and associated links on the group objects are cleared if the employeeStatus is set to I.
- Adds the manager attribute to any other active User objects in the directory whose managerWorkforceID attribute specifies this new User.
- Adds the directReports attribute value to any active User object in the directory that is specified by this User's managerWorkforceID attribute.
- If the employeeStatus is changing from I to A, generates a Move event with a write-back event-id to facilitate the modification of the DN attribute in PeopleSoft. This event moves the User object from the InActive Organizational Unit to the Active Organizational Unit.

get-empl-status

This template requests the value of the employeeStatus attribute from a specified User object in eDirectory.

get-empl-isManager

This template requests the value of the isManager attribute from a specified User object in eDirectory.

get-empl-CN

This template requests the value of the CN attribute from a specified User object in eDirectory.

get-empl-managerWorkforceID

This template requests the value of the managerWorkforceID attribute from a specified User object in eDirectory.

get-empl-ID

This template requests the value of the Identity Manager WorkforceID attribute from a specified User object in eDirectory.

set-manager-on-user

This template queries Identity Vault to determine if the passed-in managerWorkforceID parameter references an active User object in eDirectory. The name of the manager-User object is set in the User's manager attribute if the manager is active.

set-manager-on-direct-reports

This template receives a manager-User object ID parameter. A query is sent to Identity Vault for a list of all active Users who have the specified manager-User object ID in the managerWorkforceID attribute. The manager attribute of all Users in the list is set with the name of the manager-User.

clear-manager-on-direct-reports

This template receives a manager-User object ID parameter. A query is sent to Identity Vault for a list of all active Users who have the specified manager-User object ID in the managerWorkforceID attribute. The manager attribute of all Users in the list is removed.

set-directReports-on-manager

This template receives a manager-User object ID parameter. A query is sent to Identity Vault to find an active User who has the specified manager-User object ID in the workforceID attribute. The directReports attribute of the manager-User object is modified to include the DN of the User object specified in the source document.

clear-directReports-on-manager

This template receives a manager-User object ID parameter. A query is sent to Identity Vault to find an active User who has the specified manager-User object ID in the workforceID attribute. The directReports attribute of the manager-User object is modified to remove the DN of the User object specified in the source document.

set-directReports-on-user

This template receives a User object ID parameter. A query is sent to Identity Vault to find a list of active Users who have the specified User object ID in the managerWorkforceID attribute. The directReports attribute of the User object is modified to include the DN of all User objects in the list.

Subscriber Channel Objects

The Subscriber object contains a filter and a set of policies. These policies are necessary for converting data from Identity Vault to the PeopleSoft Driver.

The Identity Vault sends filtered data modification events to PeopleSoft through the Identity Manager engine. The engine applies the business logic defined by the Subscriber policies prior to submitting the data to the PeopleSoft Driver, which converts the data from the Identity Manager XDS format into PeopleSoft Component Interface format. The PeopleSoft Driver then submits the data to the PeopleSoft application and updates the staging table.

Understanding the Subscriber Filter

The Subscriber filter is a logical component of the Driver Filter object. The filter specifies the object classes and accompanying attributes that are passed from eDirectory to the PeopleSoft Component Interface. The filter is defined by using eDirectory attribute naming, so it is applied before schema mapping takes place.

For example, if the User class is specified in the Subscriber filter with only the mobile and pager attributes, the filter allows changes to only these attributes to be passed to the Identity Manager engine. If a Telephone Number attribute is modified, the Subscriber filter removes this data because the Telephone Number attribute is not in the filter. Other attribute values can be created by the Subscriber policies according to the integration scenario.

You can configure the Subscriber filter to include attributes required by your environment and allowable by eDirectory access controls. Configure it to include the following:

- Object classes you want to synchronize.
- Attributes on those objects you want to synchronize.
- Attributes that are required by your Subscriber policies. These attributes cannot be synchronized, but are required to perform some defined business logic that is to be applied to the synchronized data. These are known as “notify” attributes.

The Subscriber filter specifies a set of data to be considered as authoritative from Identity Vault or any other authoritative application that might have written the data to Identity Vault. Based on business logic, there might be multiple authoritative sources of specific data (such as another driver or eDirectory itself). The configuration of the filters in your environment determines data ownership and authority.

Subscriber Filter Attributes

Most of the attributes in the Subscriber filter are configured for bidirectional synchronization. This is done for sample purposes to allow the driver to perform add, modify, and delete operations on both the Subscriber and Publisher channels. In most installations the driver policies and filter are configured to function in either a predominant Subscriber or Publisher mode.

The attributes listed below are included in the default Subscriber filter.

Table 6-3 The Subscriber Channel Attributes

CN	managerWorkforceID
departmentNumber	mobile
Description	pager
employeeStatus	Physical Delivery Office Name
Given Name	Postal Code
homePhone	S
Initials	SA
Internet EMail Address	Surname
jobCode	Telephone Number
mailstop	workforceID

As mentioned previously, the Subscriber synchronization attributes in the Driver filter are present for demonstration purposes. It is very important to note that Subscriber filter and policies should be set to match the requirements of the PeopleSoft CI being utilized. If you want the ability to add objects on the Subscriber channel, make sure all required attributes in the CI are allowed to pass through the filter. Also make note of which fields in the CI are related display fields or translate values that cannot be synchronized, such as, Title, OU, and Full Name. By implementing and enforcing the CI application restrictions in your filter and policies, you encounter fewer synchronization errors and achieve higher throughput.

Securing the Data

If there is sensitive data that should not be shared with the PeopleSoft application, it should be removed from the Subscriber filter.

Modifying the Filter

A properly configured Subscriber filter promotes a secure environment and secures data sharing from Identity Vault to PeopleSoft. Make sure that attributes that are required for Subscriber policies processing (such as workforceID) are present in the filter even if they won't be synchronized to the PeopleSoft application.

Subscriber Object Policies

Policies contain templates that perform specific operations that can manipulate data, query either Identity Vault or PeopleSoft for additional data required for processing, create new attributes based on values of other attributes, or even discard entire data events. The following section explains each policy and provides a description of the operations each policy performs. Because XML, DirXML Script, and XSLT allow for great flexibility, all policies can be modified to meet the individual needs of

your organization. The Schema Mapping policy has been previously described and is not addressed in this section. For information on the Schema Mapping policy, refer to "Modifying the Driver Mapping Policy" on page 57.

The Subscriber object, by default, contains or uses the following policies:

- "Event Transformation Policy" on page 67
- "Matching Policy" on page 67
- "Create Policy" on page 68
- "Output Transformation Policy" on page 68

Event Transformation Policy

The Event Transformation Policy is used to remove or change received event types into different events. The following templates exist in the default Event Transformation Policy:

- "Match <rename> Element" on page 67
- "Match <move> Element" on page 67
- "Match <delete> Element" on page 67

Match <rename> Element

PeopleSoft does not allow the rename or modification of primary key values. This policy transforms a User Rename event into a Modify event that resets the CN and DISTINGUISHED_NAME fields in the CI.

Match <move> Element

PeopleSoft does not support object containment or hierarchy. This policy transforms User Move events into Modify events that reset the DISTINGUISHED_NAME field in the CI.

Match <delete> Element

This template is commented out by default to allow delete events to be passed to the driver. This policy remains for reference for non-delete scenarios. Previous versions of the driver did not support Delete events, so this template transforms them into Modify events that remove only Subscriber channel fields in the CI (CN, DISTINGUISHED_NAME, Internet Email Address, and Description).

Matching Policy

The Matching policy is used by the Identity Manager engine to apply criteria to determine if a matching data object already exists in the PeopleSoft application. The Matching policy is applied to all documents received from Identity Vault that contain User objects that are not currently associated with PeopleSoft objects. If a match is found by this policy, the Add event is converted into an object merge operation. This merge queries PeopleSoft for all attributes in the Publisher filter and

applies them to Identity Vault, and queries Identity Vault for all attributes in the Subscriber filter and applies them to the PeopleSoft application. The process is finalized when an association value is written on the eDirectory User object.

The Matching policy should provide criteria that are guaranteed to produce a 0 or 1 match. More than one policy can exist, and the Identity Manager engine applies them in the order that they are defined. Any policy producing 0 or more than one match is skipped and the next policy is applied. Processing finishes when one match is found or after the last policy has been processed.

The default Subscriber Matching policy is an XML policy that attempts to find a PeopleSoft DIRXML_SCHEMA01 object that contains an ASSOC_ID attribute that matches the eDirectory User object's workforceID attribute. If that policy fails, the driver uses another policy to locate a PeopleSoft DIRXML_SCHEMA01 secondary object with a matching Given Name and Surname. The policy is defined in eDirectory class and attribute names because schema mapping has not yet been applied.

Create Policy

The Create policy specifies the criteria for creating a new object after the Matching policy has failed to find a match. This policy performs various tests and transformations based on the requirements for object creation in the DIRXML_SCHEMA01 CI in PeopleSoft and the business logic being applied.

The default Subscriber Create policy is a DirXML Script policy that asserts that the Add document is for a User object and that it must contain a value for Given Name, Surname, employeeStatus, departmentNumber, and jobCode. These fields are required because the default PSA has defined these fields as required in the DIRXML_SCHEMA01 CI. (Additional required fields, such as BirthDate and Manager, have defined default values in the CI and are thus not required here.) By making sure all required fields are present before submitting the Add event to the driver, synchronization performance and integrity is enhanced.

This default policy does not assert particular values that are required for employeeStatus, departmentNumber, and jobCode in the PSA, but such assertions can be added to the Subscriber policies if desired.

Output Transformation Policy

The Output Transformation policy is implemented as both a DirXML Script and an XSLT policy by default for the PeopleSoft Driver. Although the Output Transformation policy is not exclusively used by the Subscriber channel, it performs a subscribing role because it is used to transform the data format of any XDS document received from Identity Vault, regardless of which channel generated the submission of the document. An example of data transformation contained in this policy is the transformation of single-value eDirectory attributes into structured, multivalue scroll elements in PeopleSoft.

The following templates exist in the default Output Transformation policy. In addition to the listed templates, all Identity Manager policies contain identity-transform templates that allow the copying of XML attributes and elements that are passed through unmodified. Multiple instances of each listed template exist for each type of document or data element that can be received by the policy.

- "Write-back" on page 69
- "From-merge Write-back" on page 69

- "Manager Flag Data Transformation" on page 69
- "Add DN Value to Subscribe Adds" on page 69

Write-back

As documented in the Publisher channel Command Transformation policy, this template monitors all status document responses from Identity Vault. If a status document with a Success value is received and it contains `<operation-data>` with peoplesoft-cn and peoplesoft-dn values, the template holds the status document and issues a Modify document with the CN and DN values to the PeopleSoft application. When the write-back command completes, the original status document is returned to the Publisher channel.

From-merge Write-back

This policy behaves similarly to the "Write-back" on page 69 policy, but it is applied to modify documents that are generated when the Identity Manager engine merges data on matched or resynchronized objects.

Manager Flag Data Transformation

This template converts the Boolean True and False values of the Identity Vault isManager attribute into character Y and N values of the **PeopleSoft Manager** field.

Add DN Value to Subscribe Adds

When objects are added to PeopleSoft, this policy adds the DN of the IDV object to the event attributes.

SSL Configuration for PeopleSoft Application

1. Create a Certificate and import to KeyStore file in PeopleSoft System.
2. Add **"SSL_KEY_STORE_PATH"** in the Identity Manager (IDM) or Development system to set the **"SSL_KEY_STORE_PATH"** as an environment variable for respective Operating Systems (OS) as follows.
   - Linux OS

     SSL_KEY_STORE_PATH=<path>\keystore

     For Ex: **SSL_KEY_STORE_PATH= /root/drivers/psoft/keystore**
   - Windows OS

     SSL_KEY_STORE_PATH=<path>\keystore

     For Ex: **SSL_KEY_STORE_PATH= E:\PeopleSoft\PeopleSoft_8_59\Certificates\keystore**
3. Copy the created TrustStore/KeyStore file to the Identity Manager Machine.
4. Follow the steps to add Java Virtual Machine (JVM) Options in Identity Console.
   - **4a** Click the **IDM Administration** tile.
   - **4b** On the Driver Dashboard, click the upper right corner of the driver set to display the Action menu.

4c Select **Driver Set Properties**.

4d Expand the **Java Environment Parameters** section to move to **JVM Options**.

Enter TrustStore/Keystore file path and password -

- File Path **-Djavax.net.ssl.TrustStore=PeopleSoft created TrustStore/Keystore**

  Ex: **-Djavax.net.ssl.TrustStore=/home/certificates/keystore -**
- Password: **-Djavax.net.ssl.TrustStorePassword**

  Ex: **-Djavax.net.ssl.TrustStorePassword=password**

5 Restart eDirectory.

NOTE: If the Certificate expires, generate a new KeyStore executing the above steps.

---

7 Managing the Driver

As you work with the PeopleSoft driver, there are a variety of management tasks you might need to perform, including the following:

- Starting and stopping the driver
- Viewing driver version information
- Using Named Passwords to securely store passwords associated with the driver
- Monitoring the driver's health status
- Backing up the driver
- Inspecting the driver's cache files
- Viewing the driver's statistics
- Using the DirXML Command Line utility to perform management tasks through scripts
- Securing the driver and its information

Because these tasks, as well as several others, are common to all Identity Manager drivers, they are included in one reference, the *NetIQ Identity Manager Driver Administration Guide*.

8 Troubleshooting the Driver

This section contains potential problems and error codes you might encounter while configuring or using the driver.

- "The Driver Is Not Processing Available Transactions or Is Processing Them Out of Order" on page 73
- "Error Trying to Obtain Data Record" on page 73
- "Error: joltServiceException: Invalid Session" on page 74
- "The Driver Does Not Start" on page 74
- "Attributes Are Not Refreshed on the Data Schema Object" on page 74
- "Data Does Not Appear in the Identity Vault on the Publisher Channel" on page 74
- "Error: Check Application Server IP Address and Jolt Port Number" on page 75
- "Data Does Not Update in PeopleSoft on the Subscriber Channel" on page 75
- "No Transactions Are Coming Across the Publisher Channel" on page 75
- "Transactions Are Not Placed in the PeopleSoft Queue" on page 75
- "Transactions Are Left in the "Process" State and Not Processed" on page 75
- "Errors on the Publisher Channel When Processing a Transaction" on page 76
- "Component Interface Relationships Are Not Functioning" on page 76
- "SQL Error When Saving "Sample Person" Records" on page 76
- "Troubleshooting Driver Processes" on page 77

The Driver Is Not Processing Available Transactions or Is Processing Them Out of Order

- Set the driver trace level to 5 and verify that the DIRXML_DTTM and DIRXML_CURRDTTM values of the Transaction records being processed are in proper lexicographic format.
- If the records are not in the correct format, refer to Chapter 3, "Configuring Your PeopleSoft Environment," on page 21.
- If the records are in the correct format, verify that Transaction date and time field values are correct and correspond to the system date and time.

Error Trying to Obtain Data Record

The following are typical reasons for this error:

- The Data record identified in a Transaction record was deleted from the PeopleSoft server before the Transaction was processed.

- The Data record identified in a query or Subscriber channel operation has been deleted from the PeopleSoft server.
- Through a database error or bad configuration, multiple Data records with the same primary key value exist in the PeopleSoft database.

  Verify the reason for the problem by using either an SQL tool, the PSA DirXML Schema 01 sample application, or the PeopleSoft Application Designer's Test Component Interface tool (see Chapter 3, "Configuring Your PeopleSoft Environment," on page 21.) Correct any errors that might exist.

Error: joltServiceException: Invalid Session

This error is generated whenever the driver cannot access the target PeopleSoft Application Server. Typical reasons for the error are:

- The Application Server address and port number are incorrect or incorrectly specified (the format must be: //*address:port number*).
- The Application Server is down.

If this error occurs on the Publisher channel, the driver retries transaction processing in 60 seconds or the configured poll interval, whichever is greater. If the error occurs on the Subscriber channel, the Identity Manager engine schedules event retries.

The Driver Does Not Start

- Verify that `psoftshim.jar`, `dirxmlcomps.jar`, `psjoa.jar`, and the required CI API jar files are present in the DirXML `lib` subdirectory.
- Verify that the connection parameters are set correctly.
- Ensure that the configured CI names are valid.

Attributes Are Not Refreshed on the Data Schema Object

Verify that the Component Interfaces are working correctly by using PeopleSoft Application Designer tool. Refer to Chapter 3, "Configuring Your PeopleSoft Environment," on page 21.

Data Does Not Appear in the Identity Vault on the Publisher Channel

- Verify that the Mapping policy and filters are configured correctly.
- Verify that the APIs are working correctly and data is being produced by them.

Error: Check Application Server IP Address and Jolt Port Number

Run the CITester utility to verify that proper connection and authentication parameters are set. Refer to Chapter 3, "Configuring Your PeopleSoft Environment," on page 21.

Data Does Not Update in PeopleSoft on the Subscriber Channel

- Verify that the Mapping policy and filters are configured correctly.
- Verify that the APIs are working correctly.
- If you are using <add> event functionality, verify that the Create method is available on the target schema CI.
- If you are using <delete> event functionality, verify that the Delete method is available on the target schema CI.

No Transactions Are Coming Across the Publisher Channel

- Verify that there are active transactions in the queue ready for processing.
- Ensure that driver parameters are pointing to the correct PeopleSoft database. For example, transactions do not process if they are in the PROD database, and the driver is still pointing to the test database (which is configured to run with the driver, but holds no transactions).

Transactions Are Not Placed in the PeopleSoft Queue

Verify that PeopleCode is working properly.

Transactions Are Left in the "Process" State and Not Processed

- Verify that all of the CI objects can be processed and that the status can be updated to a Success (S), Warning (W), or Error (E) state.

  If e-mail is configured in PeopleSoft and the SMTP gateway is down, an error can occur, causing the update of the transaction to fail. You should verify that all online processing of the application works correctly. PeopleCode attached to the update might sometimes fail, causing the transaction to fail. If system connectivity is lost, the database or application server goes down during processing and causes the driver to abandon the transaction. The transaction is left in the selected state with a status of I.

  NOTE: If notification processing is required, we recommend using the Identity Manager Notification Service instead of using SMTP processing as configured in PeopleSoft. For more information, see the NetIQ Identity Manager E-Mail Notification Guide.

Errors on the Publisher Channel When Processing a Transaction

The following list gives a sampling of errors and what they represent:

- Operation vetoed by the Create policy

  Required data might be missing in the Create policy or other criteria in the Create policy have an error.
- generateKeyPair: -216 DSERR_PASSWORD_TOO_SHORT

  The attribute used for the initial password does not comply with the policy; however, the user object is still created.
- Unable to read current state of 8101

  No association exists for this identity.
- nameToID: -601 ERR_NO_SUCH_ENTRY

  Possible Placement policy error with an invalid container object designated.
- No DN generated by Placement policy

  Possible missing or invalid data, so a valid DN cannot be created.

Component Interface Relationships Are Not Functioning

If data does not appear in the attributes, data isn't getting posted into PeopleSoft, or data is missing, you should begin looking at the Component Interface relationships.

First, verify that the API is getting the data from the PeopleSoft buffer.

After all of the CIs have been tested completely with validation of all processes that the driver is configured to do, there should be no issues regarding the driver accessing PeopleSoft through the CIs. Other problem areas include:

- Connectivity IP address and port for the application server
- ID and password
- Correct naming of all activities in the parameters for the driver.

For troubleshooting these problems, try three basic tests:

1. Manually test all of the processes online using the PeopleSoft applications as configured.
2. Test all of the processes that are using the Component Interfaces.
3. Test the driver connection to the API through the Component Interfaces.

SQL Error When Saving "Sample Person" Records

Error text example:

```
SQL error.Function: SQLExec
Error Position:  0
 Return:  8601 - [Microsoft][ODBC SQL Server Driver][SQL Server]FOR
 UPDATE cannot be specified on a READ ONLY cursor.
```

The DirXML_DERIVED.DIRXML_DRIVER.FieldFormula PeopleCode contains an SQLExec command that performs an exclusive lock on selected rows returned from a query for the current sequential transaction number in the DIRXML_TRANSNXT table. The command line is:

```
SQLExec("Select DIRXML_INST from DIRXML_TRANSXT Where DIRXML_DRIVER =:1
FOR UPDATE", &Driver, &InstanceID);
```

The “FOR UPDATE” locking clause is not valid for all flavors of SQL (such as SQL Server.) The clause can be safely removed to allow the PSA to function. However, if there is a possibility of simultaneous administrative access to the Transaction row creation functionality, the code should be modified by a qualified DBMS/PeopleSoft Database administrator to appropriately serialize the “Select” and “Insert or Update” of the DIRXML_TRANSNXT table.

Troubleshooting Driver Processes

Viewing driver processes is necessary to analyze unexpected behavior. To view the driver processing events, use DSTrace. You should only use it during testing and troubleshooting the driver. Running DSTrace while the drivers are in production increases the utilization on the Identity Manager server and can cause events to process very slowly. For more information, see “Viewing Identity Manager Processes” in the *NetIQ Identity Manager Driver Administration Guide*.

A Driver Properties

This section provides information about the Driver Configuration and Global Configuration Values properties for the PeopleSoft driver. These are the only unique properties for drivers. All other driver properties (Named Password, Engine Control Values, Log Level, and so forth) are common to all drivers. Refer to "Driver Properties" in the *NetIQ Identity Manager Driver Administration Guide* for information about the common properties.

The information is presented from Identity Console's perspective. If a field is different in Designer, it is marked with a Designer icon.

- "Driver Configuration" on page 79
- "Global Configuration Values" on page 83

Driver Configuration

In Identity Console:

1. Click the **IDM Administration** tile.
2. On the Driver Dashboard, locate the driver, then click the driver icon to display the driver's properties page.

In Designer:

1. Open a project in the Modeler.
2. Right-click the driver icon or line, then select click **Properties > Driver Configuration.**

The following sections describe driver configuration in details:

- "Driver Module" on page 79
- "Driver Object Password" on page 80
- "Authentication" on page 80
- "Startup Option" on page 81
- "Driver Parameters" on page 81
- "ECMAScript" on page 82
- "Global Configuration" on page 83

Driver Module

The driver module changes the driver from running locally to running remotely or the reverse.

Java: Used to specify the name of the Java class that is instantiated for the shim component of the driver. This class can be located in the `classes` directory as a class file, or in the `lib` directory as a `.jar` file. If this option is selected, the driver is running locally.

The java class name is:

`com.novell.nds.dirxml.driver.psoftshim.PSOFTDriverShim`

Native: This option is not used with the PeopleSoft driver.

Connect to Remote Loader: Used when the driver is connecting remotely to the connected system. Designer includes two suboptions:

- **Remote Loader Client Configuration for Documentation**: Includes information on the Remote Loader client configuration when Designer generates documentation for the driver.
- **Driver Object Password**: Specifies a password for the Driver object. If you are using the Remote Loader, you must enter a password on this page. Otherwise, the remote driver does not run. The Remote Loader uses this password to authenticate itself to the remote driver shim.

Driver Object Password

Driver Object Password: Use this option to set a password for the driver object. If you are using the Remote Loader, you must enter a password on this page or the remote driver does not run. This password is used by the Remote Loader to authenticate itself to the remote driver shim.

Authentication

The Authentication section stores the information required to authenticate to the connected system.

Authentication ID: Specify a user application ID. This ID is used to pass Identity Vault subscription information to the application.

Example: `PSAdmin`

Connection Information: Specify the IP address or name of the PeopleSoft server the driver should communicate with.

The connection string uses the following format:

`<hostname or IP address>:<Port Number>`

Example: `//PSServer:9000`

To enable failover and load balancing, you can supply multiple server connection strings separated by a comma.

Application Password: Specify the password for the user object listed in the **Authentication ID** field.

Remote Loader Authentication Parameters: Used only if the driver is connecting to the application through the Remote Loader. The parameter to enter is `hostname=xxx.xxx.xxx.xxx port=xxxx kmo=certificatename`, where the hostname is the IP address of the application server running the Remote Loader server and the port is the port the Remote Loader is listening on. The default port for the Remote Loader is 8090.

The `kmo` entry is optional. It is only used when there is an SSL connection between the Remote Loader and the Identity Manager engine.

Example: `hostname=10.0.0.1 port=8090 kmo=IDMCertificate`

Remote Loader Password: Used only if the driver is connecting to the application through the Remote Loader. The password is used to control access to the Remote Loader instance. It must be the same password specified during the configuration of the Remote Loader on the connected system.

Cache limit (KB): Specify the maximum event cache file size (in KB). If it is set to zero, the file size is unlimited.

Click **Unlimited** to set the file size to unlimited in Designer.

Startup Option

The Startup Option section allows you to set the driver state when the Identity Manager server is started.

Auto start: The driver starts every time the Identity Manager server is started.

Manual: The driver does not start when the Identity Manager server is started. The driver must be started through Designer or Identity Console.

Disabled: The driver has a cache file that stores all of the events. When the driver is set to Disabled, this file is deleted and no new events are stored in the file until the driver state is changed to Manual or Auto Start.

Do not automatically synchronize the driver: This option only applies if the driver is deployed and was previously disabled. If this is not selected, the driver re-synchronizes the next time it is started.

Driver Parameters

The Driver Parameters section lets you configure the driver-specific parameters. When you change driver parameters, you tune driver behavior to align with your network environment.

The parameters are presented by category:

- "Driver Options" on page 81
- "Subscriber Options" on page 82
- "Publisher Options" on page 82

Driver Options

Schema CI Name: Allows you to list the Data Schema Component interfaces that the driver synchronizes. Use the **Plus** icon to add an item, the **Minus** icon to delete an item, and the **Pen** icon to edit an item. The default is **DIRXML_SCHEMA01**.

Data Record ID Field: Specify the name of the data record definition that uniquely identifies a PeopleSoft object. The default is **Assoc_ID**.

Use Case-Sensitive Search: Controls whether the driver uses case-sensitive matching criteria while evaluating search attribute matches. The default is **No Case-Sensitive Matching**.

Domain Connection Password: Controls enabling and disabling of domain connection password functionality. When this option is set to **Enable** on the PeopleSoft server, an unencrypted domain connection password is provided. By default, this option is set to **Disable**.

Subscriber Options

Allow Subscriber channel add events: Subscriber Add events are implemented by invoking the Component Interface Create method (if present). If you want the driver to allow Subscriber channel Add events, select **Allow Subscriber add**. The default is **Disallow Subscriber add**.

- **Data Record ID Field Default Value:** Specify a default value for the Schema CI key field. This parameter is used only for Subscriber channel Add events. The default is **New**.

Allow Subscriber channel delete events: Subscriber Delete events are implemented by invoking the Component Interface Delete method (if present). If you want the driver to allow Subscriber channel Delete events, select **Allow Subscriber delete**. The default is **Disallow Subscriber delete**.

Publisher Options

Transaction CI Name: Specify the name of the PeopleSoft CI object that defines the set of fields required for the driver Transaction interface. The set of fields in the specified transaction CI must contain the same fields and keys that are identified in the default transaction CI in order for the driver to work. The default is **DIRXML_TRANS01.**

Driver Subset Identifier: Specify the value of the DIRXML_DRIVER field in the transaction CI that identifies a subset of published transactions. This value is used for polling the transaction CI to retrieve relevant transactions from the PeopleSoft application.

Publisher Polling Option: The PeopleSoft driver supports two options for Publisher Transaction record polling. To choose an interval of seconds between polls, select **Utilize Interval Polling**. To use a crontab format, select **Utilize crontab Format Polling**.

If you select **Utilize Interval Polling**, fill in the **Queue Poll Interval** by specifying the number of seconds between checks for available transactions to process. The default is **5**.

If you select **Utilize crontab Format Polling**, fill in the **Enter Queue Poll crontab Format String** by specifying the polling interval in crontab format. The default value of * * * * * generates a poll every minute.

- **Queue Poll Interval (seconds):** Specify the number of seconds between checks for available transactions to process.

Publisher heartbeat interval: Specify how many minutes of inactivity can elapse before this channel sends a heartbeat document. In practice, more than the number of minutes specified can elapse. That is, this parameter defines a lower bound.

ECMAScript

Displays an ordered list of ECMAScript resource files. The files contain extension functions for the driver that Identity Manager loads when the driver starts. You can add additional files, remove existing files, or change the order the files are executed.

Global Configuration

Displays an ordered list of Global Configuration objects. The objects contain extension GCV definitions for the driver that Identity Manager loads when the driver is started. You can add or remove the Global Configuration objects, and you can change the order in which the objects are executed.

Global Configuration Values

Global configuration values (GCVs) are values that can be used by the driver to control functionality. GCVs are defined on the driver or on the driver set. Driver set GCVs can be used by all drivers in the driver set. Driver GCVs can be used only by the driver on which they are defined.

The PeopleSoft driver includes several predefined GCVs. You can also add your own if you discover you need additional ones as you implement policies in the driver.

To access the driver's GCVs in Identity Console:

1. Click the **IDM Administration** tile.
2. On the Driver Dashboard, locate the driver icon, then click the upper right corner of the driver icon to display the driver's properties page.
   - **2a** Select the **Configuration** tab.
   - **2b** Expand the **Global Config Values** section.

To add a GCV to the driver set:

1. On the Driver Dashboard, click the upper right corner of the driver set to display the Action menu.
2. Select **Driver Set Properties**.
3. On the **Driver Set Configuration** tab, expand the **Global Config Values** section.
4. Save the values.

To access the driver's GCVs in Designer:

1. Open a project in the Modeler.
2. Right-click the driver icon or line, then select **Properties > Global Configuration Values.**

   or

   To add a GCV to the driver set, right-click the driver set icon , then click **Properties > GCVs**.

The global configuration values are organized as follows:

- "Password Synchronization" on page 84
- "Managed System Information" on page 84

Password Synchronization

These GCVs enable password synchronization between the Identity Vault and the PeopleSoft system.

In Designer, you must click the icon next to a GCV to edit it. This displays the Password Synchronization Options dialog box for a better view of the relationship between the different GCVs.

In Identity Console, to edit the Password management option, follow the steps given below:

1. Click the **IDM Administration** tile.
2. On the Driver Dashboard, locate the driver, then click the driver icon to display the driver's properties page.
3. Select the **Configuration** tab.
4. Expand the **Global Config Values** section.
5. Select the **Password Synchronization** tab.

For more information about how to use the Password Management GCVs, see Configuring Password Flow in the NetIQ Identity Manager Password Management Guide.

Connected System Name: Specifies the name of the PeopleSoft system or the driver name. This value is used by the e-mail notification template to identify the source of the notification message.

Application accepts passwords from Identity Manager: If **True**, allows passwords to flow from the Identity Manager data store to the connected system.

Identity Manager accepts passwords from application: If **True**, allows passwords to flow from the connected system to Identity Manager.

Publish passwords to NDS password: If **True**, uses the password from the connected system to set the non-reversible NDS password in eDirectory.

Publish passwords to Distribution Password: If **True**, uses the password from the connected system to set the NMAS Distribution Password used for Identity Manager password synchronization.

Require password policy validation before publishing passwords: If **True**, applies NMAS password policies during publish password operations. The password is not written to the data store if it does not comply.

Reset user's external system password to the Identity Manager password on failure: If **True**, on a publish Distribution Password failure, attempts to reset the password in the connected system by using the Distribution Password from the Identity Manager data store.

Notify the user of password synchronization failure via e-mail: If **True**, notifies the user by e-mail of any password synchronization failures.

Managed System Information

These settings help Identity Reporting to generate reports.

ID: Specifies an ID that uniquely identifies the managed system.

Name: Specifies a descriptive name for this PeopleSoft system. This name is displayed in the reports.

Description: Specifies a brief description of this PeopleSoft system. This description is displayed in the reports.

Type: Specifies the type for the PeopleSoft system.

Classification: Specifies the classification of the PeopleSoft system. This information is displayed in the reports.

Vendor: Specifies Oracle as the vendor of the PeopleSoft system. This information is displayed in the reports.

Version: Specifies the version of this PeopleSoft system. This version information is displayed in the reports.

Business Owner: Specifies the business owner in the Identity Vault for this PeopleSoft system. Ensure that a user object is selected. You must not select a role, group, or container.

Application Owner: Specifies the application owner in the Identity Vault for this PeopleSoft system. Ensure that a user object is selected. You must not select a role, group, or container.

Location: Specifies the physical location of this PeopleSoft system. This location is displayed in the reports.

- Mission-Critical
- Vital
- Not-Critical
- Other

  If you select **Other**, you must specify a custom classification for the PeopleSoft system.

Environment: Specifies the type of environment the PeopleSoft system provides. The options are:

- Development
- Test
- Staging
- Production
- Other

  If you select **Other**, you must specify a custom classification for the PeopleSoft system.

Authentication IP Address: Specifies the IP address used to authenticate to the PeopleSoft system.

Authentication Port: Specifies the port used to authenticate to the PeopleSoft system.

Authentication ID: Specifies the user ID used to authenticate to the PeopleSoft system.

B Trace Levels

The driver supports the following trace levels:

Table B-1 *Supported Trace Levels*

Level	Description
0	No debugging
1-2	Identity Manager messages. Higher trace levels provide more detail.
3	Previous level plus transaction status, driver schema, and connection status
4	Previous level plus Remote Loader, driver, driver shim, and driver connection messages
5	Previous level plus driver status log, driver parameters, driver security,, , driver communication details, data record processing details, request and response XML

For information about setting driver trace levels, see "Viewing Identity Manager Processes" in the *NetIQ Identity Manager Driver Administration Guide*.