NetIQ® Identity Manager

Driver for Oracle E-Business Suite (User Management, HR, and TCA) Implementation Guide

February 2020

NetIQ

Legal Notices

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

Contents

About this Book and the Library

The *Identity Manager Driver for Oracle E-Business Suite (User Management, HR, and TCA) Implementation Guide* introduces Identity Manager Administrators to the process of integrating identity information stored in Identity Manager with the User Management, HR, and TCA modules of the Oracle Business Suite.

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.

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-47/)
- Identity Manager drivers documentation website (https://www.netiq.com/documentation/identity-manager-47-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. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions 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

Qmunity, 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, Qmunity 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 http://community.netiq.com.

1 Introduction

The Identity Manager Drivers for Oracle E-Business Suite synchronize users between the Identity Vault and the Oracle E-Business Suite. Oracle E-Business Suite (EBS) is a comprehensive suite of integrated, global business applications that includes modules for finance, human resources, supply chain management, customer relationship management, and business intelligence. There are mainly three types of user records in the Oracle EBS system. They are:

- **EBS User Record:** Represents a record in the FND_USER table in the Oracle EBS system. To log in to the Oracle EBS system, a user must have a record in the FND_USER table.

- **HRMS/PERSON Record:** Represents a Human Resources Management System (HRMS) record in the Oracle EBS system. Some applications in the Oracle EBS system; for example, iExpense require a user to have a HRMS (Person) record. The Person record can be of different types like Employee, Part-time worker, Contractor, and so on. Person records are stored in the PER_ALL_PEOPLE_F table in the Oracle EBS system.

- **Customer/Vender Record:** Represents a TCA record in the HZ_PARTIES table in the Oracle EBS system. Some applications in the Oracle EBS system such as iStore, iProcurement require users to have a Trading Community Architecture (TCA) record that are representatives or employees of customers and vendors.

There are three different Identity Manager drivers for synchronizing Oracle EBS users with the Identity Vault. They are:

- Driver for User Management
- Driver for HR
- Driver for TCA

Each driver has a definite purpose and allows administrators to propagate user data among Oracle systems and other business applications and databases without the need for custom integration solutions. Administrators can decide what data to share and how to present data within their enterprises. The drivers offer the following features:

- Automated, rule-based user creation, modification, and deletion of user data with the Oracle EBS system
- Bidirectional attribute synchronization
- Basic password set and synchronization
- Support for standard Identity Manager features such as entitlements, identity tracking, and reporting

Table 1-1 distinguishes features of each driver:

Table 1-1   Driver Features

Driver for User Management	Driver for User Management with HR Foundation	Driver for User Management with TCA Foundation
Synchronizes attributes between the Oracle EBS system and the Identity Vault.	Synchronizes attributes between the Oracle EBS system and the Identity Vault.	Synchronizes attributes between the Oracle EBS system and the Identity Vault.
Creates FND_USER records in the Oracle EBS system for the Identity Manager users and grants them roles and responsibilities.	Creates basic HRMS users in the PER_ALL_PEOPLE_F table.	Creates FND_USER records in the Oracle EBS system for the Identity Manager users and grants them roles and responsibilities. Creates basic TCA records in the HZ_PARTIES table and links them to the FND_USER table records. For example, the PERSON_PARTY_ID column in the FND_USER table is linked with the PARTY_ID column of the HZ_PARTIES table.

To use all the three drivers together, you must use entitlements.

Driver Concepts

Data flows between the Oracle EBS system and the Identity Vault by using the Publisher and Subscriber channels.

The Publisher channel does the following:

- ◆ Reads events from the Oracle EBS system on the server that the driver shim is connecting to.
- ◆ Submits that information to the Identity Vault.

The Subscriber channel does the following:

- ◆ Watches for additions and modifications to the Identity Vault objects.
- ◆ Makes changes to the Oracle EBS system to reflect those changes.

Through the use of filters and policies, the driver can be configured to control and manage what changes are detected and sent to the Oracle EBS system.

The driver uses SOAP (Simple Object Access Protocol) to exchange data between Identity Manager and a Web service. SOAP is an XML-based protocol for exchanging messages. It defines the message exchange but not the message content. The driver supports SOAP 1.1. SOAP follows the HTTP request/response message model, which provides SOAP request parameters in an HTTP request and SOAP response parameters in an HTTP response.

How the Drivers Work

The driver is a bidirectional synchronization product between the Oracle EBS system and the Identity Vault. This framework uses XML and XSLT to provide data and event transformation capabilities that convert Identity Vault data and events into Oracle data and vice-versa.

The Identity Vault acts as a hub, with other applications and directories publishing their changes to it. The Identity Vault then sends changes to the applications and directories that have subscribed for them. This results in two main flows of data: the Publisher channel and the Subscriber channel.

- "Publisher Channel" on page 11
- "Subscriber Channel" on page 12
- "Associations" on page 12

Publisher Channel

The Oracle Workflow Business Event System (BES) is an application service that uses Oracle Advanced Queuing (AQ) technology to communicate business events among different Oracle systems. The BES consists of the Event Manager and Workflow that process event activities. The BES can propagate Add, Delete, and Modify event data to the Identity Vault. Only events specifically selected by the system administrator are transported from the Oracle EBS system to the PL/SQL APIs. The PL/SQL APIs (installed in the Oracle EBS system as part of the driver installation) handle the parsing of the events and read the appropriate data fields specified by the driver configuration, and provide secure transport of the data over an HTTP/HTTPS port to the Publisher channel. Figure 1-1 shows the Publisher channel data flow from the Oracle EBS system to the Identity Vault.

Only the event attributes that have been specified in the driver Publisher filter are published to the Identity Vault. The Publisher channel then submits XML-formatted documents to the Identity Manager engine to publish them into the Identity Vault.

Figure 1-1   Publisher Channel Data Transfer
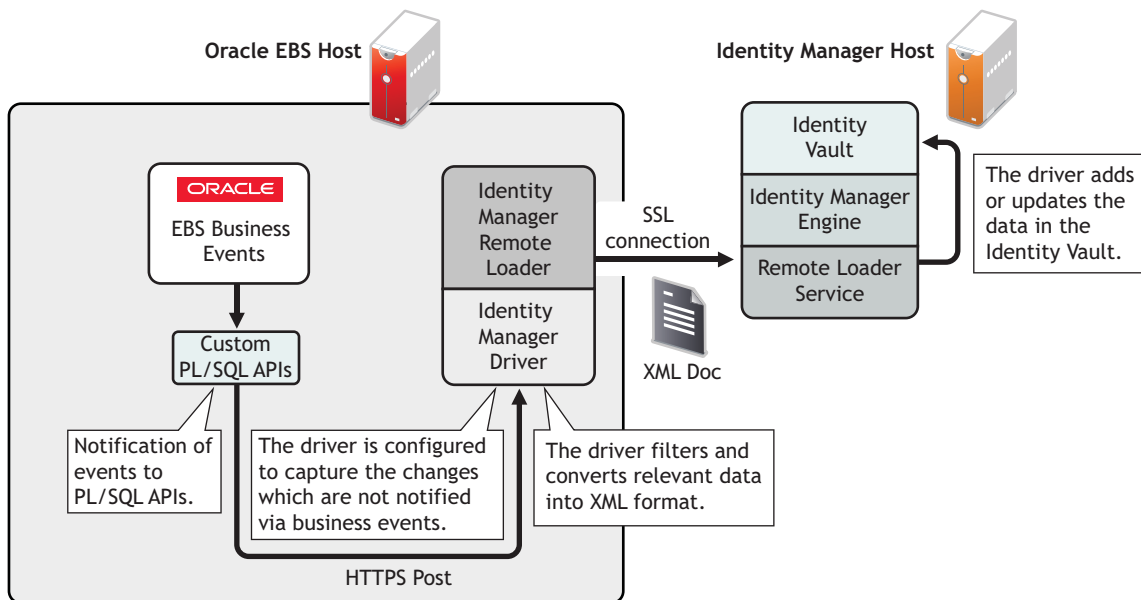
The business events are cached and stored into a database table (idmusrmgt.idm_events table) in the Oracle EBS system. To guarantee the delivery of events to the Identity Manager, the events remain in the idmusrmgt.idm_events table until they are successfully send to the Identity Vault. The Publisher channel uses a SOAP endpoint to poll the idmusrmgt.idm_events table for certain future events such as future add or delete events or modification of roles and responsibilities to the existing users, which are meant to be executed at a later time. A future date of when these events need to be executed is specified along with the events. Future events are immediately synchronized with the Identity Vault. The login attribute is disabled for the future events until when they are required to be operational.

Subscriber Channel

The Subscriber channel receives XML-formatted Identity Vault events from the Identity Manager engine. The driver uses the Web Service security (WSS) token for authentication and updates the idmusrmgt.idm_events table with the Identity Vault changes.

Figure 1-2 Subscriber Channel Data Transfer
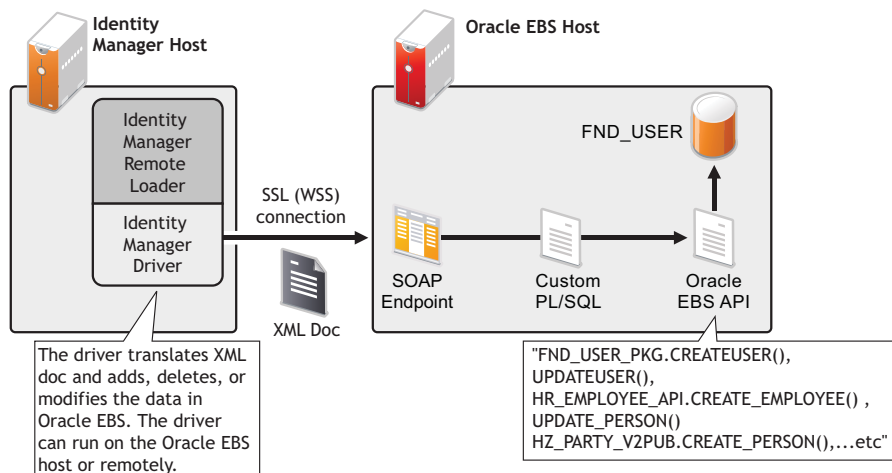
For data to flow from the Identity Vault to the Oracle system, the driver uses the SOAP functions. By using Identity Manager and other Identity Manager drivers, the data can be shared with other business applications and directories. These other applications can add additional data, which in turn can be transferred back to the idmusrmgt.idm_events table using the SOAP service on the Subscriber channel.

Associations

Associations are created between the Oracle EBS system and the Identity Vault objects during the synchronization process. For the Oracle EBS user object, a unique 7-digit number must be created. However, the Identity Vault and other applications do not need to share this same unique ID. Identity Manager allows various naming policies in an organization to be applied to objects by using the DirXML-Association attribute.

The DirXML-Association attribute is multivalued. Therefore, if Identity Manager is being used to synchronize an object among multiple applications, all of the object's unique IDs (or associations) can be stored in this attribute on the Identity Vault object.

The unique ID association links objects from the Oracle EBS database to the corresponding objects in the Identity Vault. When an Add or Matching event occurs, the association is made. This association allows the driver to perform subsequent tasks on the appropriate object.

The DirXML-Associations field is stored on the Identity Vault object on the Identity Manager property page. The User ID of a user in the Oracle EBS system is used to create association for the User Management and TCA drivers. The Person ID of an employee is used to create association for the HR driver.

Supported Oracle Versions

The driver supports the Oracle E-Business Suite 12.1.1 and above (Oracle E-Business Suite 12.2.6 is the latest supported version).

Key Driver Features

The following sections provide information about the standard driver features supported by the Oracle EBS drivers:

Password Synchronization

The Subscriber channel sets the password. Passwords are not synchronized on the Publisher channel. This means that passwords are synchronized from the Identity Vault to the Oracle EBS system, but not from the Oracle EBS system to the Identity Vault. This feature is not needed for the HR driver.

Entitlements

The Oracle EBS drivers driver implements entitlements. You can use entitlements to grant or revoke rights to an account in the driver. You should enable entitlements for the drivers only if you plan to use the User Application or Role-Based Entitlements with the drivers. For more information about entitlements, see the *NetIQ Identity Manager Entitlements Guide*.

NOTE: The HR driver only supports the employee entitlement.

Object Synchronization

The Oracle EBS drivers synchronize users on the Subscriber and Publisher channels.

Driver Packages

The Identity Manager content is delivered in packages. The packages create a driver with a set of policies suitable for synchronizing data with the Identity Vault. The following packages provide basic functionality for configuring the Oracle EBS drivers:

Common Packages

- NOVLEBSATRK
- NOVLEBSAENT

- NOVLEBSENT
- NOVLEBSMSI
- NOVLPWDSYNC
- NOVLEBSPWD

Packages for the User Management Driver

- NOVLORAUBASE
- NOVLORAUDCFG

Packages for the HR Driver

- NOVLORAHBASE
- NOVLORAHDCFG
- NOVLORAHENT
- NOVLORAHATRK

Packages for the TCA Driver

- NOVLORATBASE
- NOVLORATDCFG

Supported Operations

The Oracle EBS drivers support Add, Modify, Delete, Rename, Move, Future Add or Delete, Migrate, and Password Synchronization operations on the user objects on the Subscriber channels. All of them except Password Synchronization are supported on the Publisher channel.

Checklist for Enabling User Synchronization

Use the following checklist to verify that you complete the following tasks in order to have a complete solution with the driver.

- Ensure that you have installed the software mentioned in "Prerequisites" on page 15.
- Install the driver object. For more information, see Chapter 2, "Installing the Driver Files," on page 15.
- Create and configure the driver object. For more information, see Chapter 3, "Creating a New Driver Object," on page 19.
- Create a secure connection between Identity Manager and the Oracle EBS system. For more information, see Chapter 5, "Securing Communication," on page 33.

2 Installing the Driver Files

You can install Oracle EBS drivers on multiple systems and platforms. To verify the system requirement list, see the *NetIQ Identity Manager Setup Guide for Linux* or *NetIQ Identity Manager Setup Guide for Windows*.

By default, the Oracle EBS driver files 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 shims and the driver packages. It does not create the driver in the Identity Vault (see Chapter 3, "Creating a New Driver Object," on page 19) or upgrade an existing driver's configuration (see Chapter 4, "Upgrading an Existing Driver," on page 29).

To install the drivers, you first need to install the driver files and driver packages, and then modify the driver configuration to suit your environment. This section tells you how to install the driver files. For information on installing and configuring the packages, see Chapter 3, "Creating a New Driver Object," on page 19.

- "Prerequisites" on page 15
- "Installing the Oracle EBS Driver Jar Files" on page 15
- "Installing the PL/SQL APIs" on page 16
- "Updating the PL/SQL APIs" on page 17
- "Creating a SOAP Endpoint" on page 17
- "Subscribing to the Business Events" on page 18

Prerequisites

- Identity Manager 4.7 or later
- Oracle E-Business Suite 12.1.1 and above

  NOTE: The latest supported version of Oracle E-Business Suite is 12.2.6.

Installing the Oracle EBS Driver Jar Files

You can install the Oracle EBS driver(s) shim in the following ways:

- On a local machine: Install the Oracle EBS driver files on the Identity Manager server and use a SOAP endpoint to connect to the Oracle EBS system. For information on installing the Identity Manager server, see "Planning Overview" in the *NetIQ Identity Manager Setup Guide for Linux* or "Planning Overview" in the *NetIQ Identity Manager Setup Guide for Windows*.
- On a remote machine: Install the Remote Loader (required to run the driver on a non-Identity Manager server) and the Oracle EBS driver files on a non-Identity Manager server where you want to run the driver. For information on installing the Remote Loader, see "Installing Identity Manager " in the *NetIQ Identity Manager Setup Guide for Linux* or "Installing the Engine, Drivers, and iManager Plug-ins" in the *NetIQ Identity Manager Setup Guide for Windows*.

To communicate with the Oracle EBS, the Oracle EBS driver requires that you copy the appropriate Oracle EBS driver jar files to the driver location.

1. Locate the appropriate Oracle EBS driver jar files.

   The Oracle EBS driver jar files are generally present on the system. Check for the following files in the `/opt/novell/eDirectory/lib/dirxml/classes` directory:

   - `EBSHRShim.jar`
   - `EBSShim.jar`
   - `EBSTCAShim.jar`
   - `EBSUserShim.jar`

2. Place the files in the appropriate location.

   The following tables show the default paths where the driver files are placed on an Identity Manager server or on a Remote Loader server.

Table 2-1 *Locations for JAR Files: Identity Manager Server*

Platform	Directory Path
Linux	`/opt/novell/eDirectory/lib/dirxml/classes`
Windows	`C:\novell\NDS\lib`

Table 2-2 *Locations for JAR Files: Remote Loader*

Platform	Directory Path
Linux	`/opt/novell/eDirectory/lib/dirxml/classes`
Windows	`C:\novell\RemoteLoader\lib`

Installing the PL/SQL APIs

The PL/SQL scripts handle the parsing of events in the Oracle EBS database. The PL/SQL scripts configure database objects such as tables and procedures for data synchronization with the driver. If you don't configure the database objects, the data communication might not work properly.

Installing the PL/SQL scripts includes performing the following tasks:

- Installing the `install_EBS.sql` PL/SQL scripts in the Oracle EBS system.
- Creating packages for the Publisher and Subscriber channels.

Locate the `install_EBS.sql` PL/SQL scripts from `/mnt/products/IDM/scripts/OracleEBS` installation directory and install them in the Oracle EBS system.

1 Log in to the Oracle SQL developer tool or Oracle database as a system user (Oracle EBS user name).

2 Run the `install_EBS.sql` command.

   Copy the contents from the `install_EBS.sql` file and paste them in the Oracle SQL developer editor, then run the copied script to create the database tables.

3 Log out of the Oracle SQL developer tool or the Oracle database.

To create packages for the Publisher channel, do the following:

1 Log in to the Oracle SQL developer tool or Oracle database as an apps user.

2 In the left panel of the Oracle SQL developer tool, navigate to **Packages** and create a new package and name it **IDM_DRIVER**.

3 Add the `publisher.pls` script to the `IDM_DRIVER` package and save the package.

4 Right-click the `IDM_DRIVER` package, select **create body** and paste the contents of the `publisher.pkb` file from the Identity Manager installation directory.

5 Save the package.

Repeat this procedure for creating the `IDM_DRIVER_S` package for the Subscriber channel and add `subsciber.pls` and `subsciber.pkb` files from the Identity Manager installation directory to the package and save it.

Updating the PL/SQL APIs

To update the already installed PL/SQL APIs, perform the following steps:

1 Log in to the Oracle SQL developer tool or Oracle database as an `apps` user.

2 Run the `install_EBS.sql` command.

Copy the contents from the `install_EBS.sql` file and paste them in the Oracle SQL developer editor, then run the copied script to create the database tables.

3 In the left panel of the Oracle SQL developer tool, navigate to **Packages** and search for the `IDM_DRIVER` package.

4 Replace the header of the `IDM_DRIVER` package with `Publisher.pls` and body with `Publisher.pkb` and save the package.

5 Navigate to **Packages** and search for the `IDM_DRIVER_S` package.

6 Replace the header of the `IDM_DRIVER_S` package with `Subscriber.pls` and body with `Subscriber.pkb` and save the package.

Creating a SOAP Endpoint

The driver uses a SOAP endpoint to synchronize the Identity Manager events in the Subscriber channel and poll the Oracle database for fetching events.

1 Create a new SOAP endpoint. Run the following shell script on the Oracle EBS server:

```
export FND_TOP=/u01/app/VIS/apps/apps_st/appl/fnd/12.0.0
export APPL_TOP=/u01/app/VIS/apps/apps_st/appl
. $APPL_TOP/APPS_instancename_hostname-ora.env
#. /configure_EBS.sh
```

NOTE: Currently, this script is available only for UNIX platforms.

You must specify appropriate values for FND_TOP and APPL_TOP variables in the commands.

2 Using a Web browser, log into the Oracle EBS system as `sysadmin` user.

3 On the Dashboard, click the Integrated SOA Gateway link.

4 Click **Integration Repository** under the **Integrated SOA Gateway** tab, then change the view to **By option to Product Family**.

The Novell IDM Suite displays.

5 Expand the view and click **Novell IDM Suite > Driver > Subscriber > IDM Subscriber.**

6 Click **Generate WSDL**, then click **Deploy**.

7 Select the **Subscribe Identity Manager Events** method under **Procedures and Functions**, then click **Create Grant**.

8 Select the user as `sysadmin` and click **Apply**.

On executing this command, if you get the error message, `"Can't locate Class/MethodMaker.pm in @INC (@INC contains:..."`, you need to install the Perl modules. For installation instructions, see the Oracle E-Business Suite Integrated SOA Gateway Implementation Guide (http://docs.oracle.com/cd/E18727_01/doc.121/e12169/T511175T543269.htm).

If the deployment fails, go to the `/u01/app/VIS/inst/apps/VIS_sles11sp164-ora/soa/PLSQL/4723/SUBSCRIBE_EVENTS.wsdl` file and remove the line, `IRepOverloadSeq="1"` under the operation tag, then save the file and use the GUI method to redeploy the SOAP service.

Subscribing to the Business Events

For the driver to subscribe to the business events from the Oracle EBS system, the driver must log in to the Oracle EBS system through an EBS account.

1 Using a Web browser, log into the Oracle EBS system as `sysadmin` user.

2 On the Dashboard, click the Workflow Administrator Web Applications link.

3 Click **Business Events** under the Administrator Workflow tab.

4 Type `oracle.apps.fnd.user.insert` in the **Search** text field, then click **Go**.

5 Click the **Subscription** link of the search result.

6 Click **Create Subscription** and specify the following information, then click **Next**.

  ◆ **system:** Click **Search**, then browse to the correct system name you want to include.

  ◆ **action type:** Specify action type as custom.

7 Specify the following information and click **Apply**:

  ◆ **PL/SQL Rule Function:** Enter the IDM_DRIVER.PUBLISH_EVENT_TO_IDM function.

  ◆ **Owner Name:** Specify the name of the owner as PER.

  ◆ **Owner Tag:** Specify the tag of the owner as PER.

8 Repeat Step 1 to Step 7 for `oracle.apps.fnd.user.update` business events.

When a business event occurs in the Oracle EBS system, the PL/SQL API handles the capturing of the event data and performs an HTTP post to the driver.

9 Provision users in the Oracle EBS system.

  9a Install a custom PL/SQL.

    The PL/SQL API processes events that are sent from Identity Manager via the SOAP endpoint.

  9b Create a SOAP endpoint using IREP of the Oracle EBS system.

    This PL/SQL executes the appropriate SQL API based on the request it receives from the Identity Manager.

3 Creating a New Driver Object

After the Oracle EBS driver files are installed on the server where you want to run the drivers (see Chapter 2, "Installing the Driver Files," on page 15), you can create each driver object 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 the Driver Object in Designer" on page 19
- "Activating the Driver" on page 26
- "Adding Packages to an Existing Driver" on page 26

Creating the Driver Object in Designer

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

- "Importing the Current Driver Packages" on page 19
- "Installing the Driver Packages" on page 20
- "Configuring the Driver Object" on page 24
- "Deploying the Driver Object" on page 25
- "Starting the Driver" on page 25

Importing the Current Driver Packages

The driver packages contain the items required to create a driver, 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 that 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**.
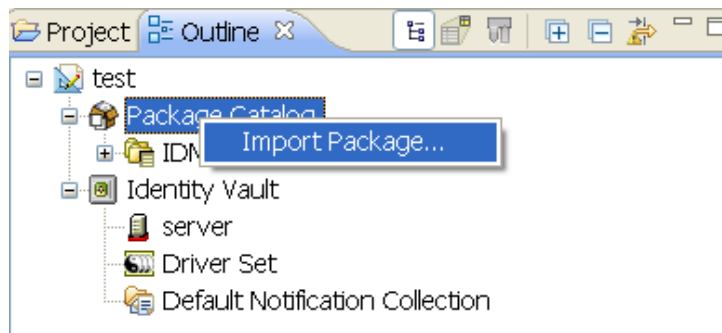
6 Select any Oracle EBS driver packages

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 20.

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**.

You need to do this for each driver you want to create.

3 Depending on the driver you want to create, select one of the following and then click **Next**:

- ◆ Oracle EBS User Management Base
- ◆ Oracle EBS HR Base
- ◆ Oracle EBS TCA Base

IMPORTANT: Run the following steps for each driver you want to create.

4 Select the optional features to install for the driver, then click **Next**.

All options are selected by default depending on the driver you choose to install. The options are:

Default Configuration: These packages contain the default configuration information for the Oracle EBS driver. Always leave this option selected.

Password Synchronization: These packages contain the policies required to enable password synchronization. Leave this option selected if you want to synchronize passwords between the Identity Vault and the Oracle EBS system.

Entitlements: These packages contain the policies and entitlements required to enable the driver for account creation and management with entitlements. For more information, see the *NetIQ Identity Manager Entitlements Guide*.

Data Collection: These packages contain the policies that enable the driver to collect data for reports. If you are using Identity Reporting, verify that this option is selected. For more information, see the *Administrator Guide to NetIQ Identity Reporting*.

Account Tracking: These packages contain the policies that enables account tracking information for reports. If you are using Identity Reporting, verify that this option is selected. 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 these dependencies to install the selected packages. Click **OK** to install the Password Synchronization Notification package dependency.

6 (Conditional) Click **OK** to install the Common Settings package, if you have not installed any other packages into the selected driver set.

7 Click **OK** to install the Advanced Java Class package if you have not installed any other packages into the selected driver set.

8 (Conditional) Fill in the following fields on the Common Settings page, 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 users are added if they don't already existing in the Identity Vault. This value becomes the default value 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.

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

10 Select **Web Service Type**. You can choose one of the following web services:

- **SOAP**: Choose to use the SOAP APIs
- **REST**: Choose to use the REST APIs
  - **Authentication Type**: Select the authentication type. By default **Basic** is selected.
  - **Http Connection Timeout**: Specify the time in minutes for the driver to wait for a REST response.

NOTE: REST web service type is available from Oracle EBS Driver 4.1.2 onwards.

Once done, click **Next**.

11 Fill in the following fields to configure the driver, then click **Next**:

Web Service Endpoint URL of the Oracle EBS: Specify the URL of the Web service.

EBS Username: Specify a name for the EBS user. This user should have appropriate privileges to access the SOAP/REST endpoint.

EBS Password: Specify a password for the EBS user.

12 On the Install Oracle EBS Base page, fill in the following fields for the Subscriber options, then click **Next**:

Subscriber Channel Enabled: By default, the Subscriber channel is enabled. This means that the events are synchronized from Identity Manager to the Oracle EBS system. Fill the following fields for the Subscriber options:

- **Use SSL:** Specify **Yes** to use SSL to secure communication between the driver and the Oracle EBS server. For more information, see Chapter 5, "Securing Communication," on page 33.

  To use SSL, fill in the following parameters:

Truststore File: Specify the name and path of the keystore file containing the trusted certificates used when the remote server is configured to provide server authentication. For example, `c:\security\truststore`. Leave this field empty when server authentication is not used.

Set Mutual Authentication Parameters: Specify Yes to use mutual authentication between the driver and the Oracle EBS server and specify the following information:

- **Keystore File:** Specify the path and the name of the keystore file that contains the trusted certificates for the remote server to provide mutual authentication. For example, `C:\security\keystore`. Leave this field blank when mutual authentication is not used.

- **Keystore Password:** Specify the password for the keystore file. Leave this field blank when mutual authentication is not used.

Use Proxy: Specify Yes if you want to use a proxy connection between the driver and the Oracle EBS server.

To use a proxy connection, fill in the following parameters:

- **Proxy Host and Port:** Specify the host address and the host port when a proxy host and port are used. For example: 192.10.1.3:18180.

  Or, if a proxy host and port are not used, leave this field empty.

- **Proxy Username:** Specify a name for the proxy connection.

- **Proxy Password:** Specify a password for the proxy connection.

- **HTTP Errors to Retry:** The HTTP error codes that return a retry status. The list of integers is separated by spaces. The error codes are: 307 404 408 503 504.

13 On the Install Oracle EBS Base page, fill in the following fields for the Publisher options, then click Next:

Publisher Channel Enabled: By default, the Publisher channel is enabled. The events are synchronized from the Oracle EBS system to the Identity Manager. Fill the following fields for the Publisher options:

- **Listening IP Address and Port:** Specify the IP address of the server where this driver is installed and the port that this driver listens on. You can specify 127.0.0.1 if there is only one network card installed in the server. Choose an unused port number on your server. For example: 127.0.0.1:18180. The driver listens on this address for incoming requests, processes the requests, and returns a result.

- **Authentication ID:** Specify the authentication ID to validate incoming requests if Basic Authorization (on the HTTP header) is used.

- **Authentication Password:** Specify the password for the authentication ID.

  NOTE: The Authentication Password prompts when the Publisher channel is disabled.

Use SSL: By default, the SSL connection is used for secure communication between the driver and the Oracle EBS server. Change this option to No if you don't want to use SSL.

 When SSL is used, you need to fill the following parameters:

- **Select Certificate Store Mode:** Select KMO if you are using eDirectory KMO for secure connection. Select Keystore to use the Java Keystore.

- **KMO Name:** If you select KMO, when this server is configured to accept HTTPS connections, this is the KMO name in eDirectory. The KMO name is the name before the - in the RDN. Leave this field blank when a keystore file is issued or when HTTPS connections are not used.

- **Keystore File:** If you select **Keystore**, when this server is configured to accept HTTPS connections, this is the path and the name of the keystore file. For example; `C:\security\keystore`. Leave this field blank when a KMO name is used or when HTTPS connections are not used.

- **Keystore Password:** When this server is configured to accept HTTPS connections, this is the keystore file password. Leave this field blank when a KMO name is used or when HTTPS connections are not used.

- **Server Key Alias:** When this server is configured to accept HTTPS connections, this is the key alias. Leave this field blank when a KMO name is used or when HTTPS connections are not used.

- **Server Key Password:** When this server is configured to accept HTTPS connections, this is the key alias password (not the keystore password). Leave this field blank when a KMO name is used or when HTTPS connections are not used.

Require Mutual Authentication: When using SSL, it is common to do only server authentication. However, if you want to force both client and server to present certificates during the handshake process, select **Required**.

Polling Interval in Seconds: Specify the number of seconds that the Publisher channel waits after running the polling script and sending Oracle EBS events to the Identity Manager engine. The default value is 60 seconds.

Heartbeat Interval in Minutes: Specifies how often, in minutes, the driver shim contacts the Identity Manager engine when there has not been any traffic during the interval time. Specify 0 to disable the heartbeat. The default value is 1 minute.

14 Fill in the following fields for the Remote Loader information, then click **Next**:

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**, skip to Step 17. If you select **Yes**, use the following information to complete the configuration of the Remote Loader:

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 (for example, `kmo=remotecert`) of the Key Material Object (KMO) containing the keys and certificate to be used for SSL.

If you used spaces in the certificate name, you need to enclose the KMO object nickname in single quotation marks.

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.

15 (Conditional) On the Install Oracle EBS Account Tracking page, fill in the following fields for Account Tracking, then click **Next**:

Realm: Specify the name of the realm, security domain, or namespace in which the account name is unique. You must set the **Realm** to the Oracle EBS Domain Name.

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

General Information

- **Name**: Specify a descriptive name for the managed system.
- **Description**: Specify a brief description of the managed system.
- **Location**: Specify the physical location of the managed system.
- **Vendor:** Specify Oracle as the vendor of the managed system.
- **Version**: Specify the version of the managed system.

System Ownership

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

  This page is only displayed if you selected to install the Data Collection packages and the Account Tracking packages.

System Classification

- **Classification**: Select the classification of the Oracle EBS system. This information is displayed in the reports. The options are as follows:
    - Mission-Critical
    - Vital
    - Not-Critical
    - Other

      If you select Other, you must specify a custom classification for the Oracle EBS system
- Environment: Select the type of environment the Oracle EBS system provides. The options are as follows:
    - Development
    - Test
    - Staging
    - Production
    - Other

      If you select **Other**, you must specify a custom environment for the Oracle EBS system.

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

18 Continue with .

Configuring the Driver Object

After importing the driver configuration file, you need to configure the driver object before it can run. Complete the following tasks to configure the driver:

- **Set Up a Secure HTTPS Connection:** You can configure the connection between the driver and Oracle EBS to use a secure HTTPS connection rather than an HTTP connection. For instructions, see Chapter 5, "Securing Communication," on page 33.
- **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 47.

◆ **Customize the driver policies and filter:** Modify the driver policies and filter to implement your business policies.

Continue with "Deploying the Driver Object" on page 25.

Deploying the Driver Object

After the driver object is created in Designer, it must be deployed into the Identity Vault.

1 In Designer, open your project.

2 In the Modeler, right-click the driver icon or the driver line, then select **Live > Deploy**.

3 If you are authenticated to the Identity Vault, skip to Step 4, otherwise, specify the following information, then click **OK**:

Host: Specify the IP address or DNS name of the server hosting the Identity Vault.

Username: Specify the DN of the user object used to authenticate to the Identity Vault.

Password: Specify the user's password.

4 Read the deployment summary, then click **Deploy**.

5 Read the message, then click **OK**.

6 Click **Define Security Equivalence** to assign rights to the driver.

The driver requires rights to objects within the Identity Vault. The Admin user object is most often used to supply these rights. However, you might want to create a DriversUser (for example) and assign security equivalence to that user.

6a Click **Add**, then browse to and select the object with the correct rights.

6b Click **OK** twice.

7 Click **Exclude Administrative Roles** to exclude users that should not be synchronized.

You should exclude any administrative User objects (for example, Admin and DriversUser) from synchronization.

7a Click **Add**, then browse to and select the user object you want to exclude, then click **OK**.

7b Repeat Step 7a for each object you want to exclude, then click **OK**.

8 Click **OK**.

Starting the Driver

When a driver is created, it is stopped by default. To make the driver work, you must start the driver and cause events to occur. Identity Manager is an event-driven system, so after the driver is started, it won't do anything until an event occurs.

To start the driver:

1 In Designer, open your project.

2 In the Modeler, right-click the driver icon or the driver line, then select **Live > Start Driver**.

3 Continue with "Activating the Driver" on page 26.

Activating the Driver

The Identity Manager Drivers for Oracle EBS drivers are part of the Identity Manager Integration Module for Oracle Enterprise. This integration module includes the following drivers:

- Identity Manager driver for Peoplesoft
- Identity Manager drivers for Oracle E-Business Suite
  - Identity Manager driver for User Management
  - Identity Manager driver for HR
  - Identity Manager driver for TCA

This integration module requires a separate activation. After purchasing the integration module, you will receive activation details in your NetIQ Customer Center.

If you create a new Oracle EBS driver in a driver set that already includes an activated driver from this integration module, the new driver inherits the activation from the driver set.

If you create the driver in a driver set that has not been previously activated with this integration module, the driver will run in the evaluation mode for 90 days. You must activate the driver with this integration module during the evaluation period; otherwise, the driver will be disabled.

If driver activation has expired, the trace displays an error message indicating that you need to reactivate the driver to use it. For information on activation, refer to Activating Identity Manager in the *NetIQ Identity Manager Overview and Planning Guide*.

Adding Packages to an Existing Driver

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

1 Right-click the driver, then click **Properties**.

2 Click **Packages**, then upgrade the already installed Oracle EBS User Management Base package.

   2a Select the package from the list of packages, then click the **Select Operation** cell.

   2b Click **Upgrade** from the drop-down list, then click **Apply**.

   2c Click **OK** to close the Package Management page.

     You can upgrade the Password Synchronization package in a similar way.

3 Click the **Add Packages** icon ✚.

4 Select the packages to install.

5 (Optional) If you want to see all available packages for the driver, clear 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.

6 Click **Apply** to install all of the packages listed with the Install operation.

7 (Conditional) Fill in the fields with appropriate information to install the package you selected for the driver, then click **Next**.

8 Read the summary of the installation, then click **Finish**.

9 Click **OK** to close the Package Management page after you have reviewed the installed packages.

10 Modify the driver configuration settings. See "Configuring the Driver Object" on page 24.

11 Deploy the driver. See "Deploying the Driver Object" on page 25.

12 Start the driver. See "Starting the Driver" on page 25.

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

4 Upgrading an Existing Driver

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

Supported Upgrade Paths

You can upgrade the drivers to the following versions:

- HR driver to 4.1.2 version
- User Management driver to 4.1.2 version
- TCA driver to 4.1.2 version

The latest versions of the drivers provide support for configuring Suite B communication between the Remote Loader and the Identity Manager engine. For more information, see "Authentication" on page 46. For more information about Suite B, see Suite B Cryptography.

What's New in Version 4.0.2

This version of the driver does not provide any new features.

Upgrading the Driver

The driver upgrade process involves upgrading the installed driver packages and updating the driver files.

This section provides general instructions for updating a driver. For information about updating the driver to a specific version, search for that driver patch in the NetIQ Patch Finder Download Page and follow the instructions from the Readme file accompanying the driver patch release.

- "Upgrading the Installed Packages" on page 29
- "Applying the Driver Patch" on page 30

Before starting the upgrade process, ensure that you have taken a back-up of the current driver configuration.

Upgrading the Installed Packages

1 Download the latest available packages.

To configure Designer to automatically read the package updates when a new version of a package is available, click **Windows > Preferences > NetIQ > Package Manager > Online Updates** in Designer. However, if you need to add a custom package to the Package Catalog, you can import the package `.jar` file. For detailed information, see the Upgrading Installed Packages in *NetIQ Designer for Identity Manager Administration Guide*.

2 Upgrade the installed packages.

    2a Open the project containing the driver.

    2b Right-click the driver for which you want to upgrade an installed package, then click **Driver > Properties**.

    2c Click **Packages**.

        If there is a newer version of a package, there is check mark displayed in the Upgrades column.

    2d Click **Select Operation** for the package that indicates there is an upgrade available.

    2e From the drop-down list, click **Upgrade**.

    2f Select the version that you want to upgrade to, then click **OK**.

        NOTE: Designer lists all versions available for upgrade.

    2g Click **Apply**.

    2h (Conditional) Fill in the fields with appropriate information to upgrade the package, then click **Next**.

        Depending on which package you selected to upgrade, you must fill in the required information to upgrade the package.

    2i Read the summary of the packages that will be installed, then click **Finish**.

    2j Review the upgraded package, then click **OK** to close the Package Management page.

        For detailed information, see the Upgrading Installed Packages in *NetIQ Designer for Identity Manager Administration Guide*.

Applying the Driver Patch

The driver patch updates the driver files. You can install the patch as a `root` or `non-root` user.

Prerequisites

Before installing the patch, complete the following steps:

1 Take a back-up of the current driver configuration.

2 (Conditional) If the driver is running with the Identity Manager engine, stop the Identity Vault and the driver instance.

3 (Conditional) If the driver is running with a Remote Loader instance, stop the Remote Loader instance and the driver instance.

4 In a browser, navigate to the NetIQ Patch Finder Download Page.

5 Under **Patches**, click **Search Patches**.

6 Specify **Identity Manager Oracle E-Business Suite driver** in the search box.

7 Download and unzip the contents of the patch file to a temporary location on your server.

For example, `IDM45_OracleEBS_4003.zip`.

Applying the Patch as a Root User

In a root installation, the driver patch installs the driver files RPMs in the default locations on Linux. On Windows, you need to manually copy the files to the default locations.

1 Update the driver files:

- ◆ **Linux:** Log in to your server as `root` and run the following commands in a command prompt:

  `rpm -Uvh <Driver Patch File Temporary Location>/linux/novell-DXMLebsCommon.rpm`

  `rpm -Uvh <Driver Patch File Temporary Location>/linux/novell-DXMLebsHR.rpm`

  `rpm -Uvh <Driver Patch File Temporary Location>/linux/novell-DXMLebsTCA.rpm`

  `rpm -Uvh <Driver Patch File Temporary Location>/linux/novell-DXMLebsUM.rpm`

  For example, `rpm -Uvh <IDM45_OracleEBS_4003.zip>/linux/`novell-DXMLebsHR.rpm

- ◆ **Windows:** Navigate to the `<Extracted Driver Patch File Temporary Location>\windows` folder and copy the following files to `<IdentityManager installation>\NDS\lib` or `<IdentityManager installation>\RemoteLoader\<architecture>\lib` folder.

  - ◆ `EBSHRShim.jar`
  - ◆ `EBSUserShim.jar`
  - ◆ `EBSTCAShim.jar`

- ◆ **Solaris:** To install the driver patch on Solaris, contact NetIQ Support.

2 (Conditional) If the driver is running locally, start the Identity Vault and the driver instance.

For example, open a command prompt on Linux and run `ndsmanage startall`

3 (Conditional) If the driver is running with Remote Loader, start the Remote Loader and driver instances.

Applying the Patch as a Non-Root User

1 Verify that `<non-root eDirectory location>/rpm` directory exists and contains the file, `_db.000`.

The `_db.000` file is created during a non-root installation of the Identity Manager engine. Absence of this file might indicate that Identity Manager is not properly installed. Reinstall Identity Manager to correctly place the file in the directory.

2 To set the `root` directory to non-`root` eDirectory location, enter the following command in the command prompt:

`ROOTDIR=<non-root eDirectory location>`

This will set the environmental variables to the directory where eDirectory is installed as a non-`root` user.

3 Download the patch and untar or unzip the downloaded file.

4 To install the driver files, enter the following command:

`rpm --dbpath $ROOTDIR/rpm -Uvh --relocate=/usr=$ROOTDIR/opt/novell/eDirectory --relocate=/etc=$ROOTDIR/etc --relocate=/opt/novell/eDirectory=$ROOTDIR/opt/novell/eDirectory --relocate=/opt/novell/dirxml=$ROOTDIR/opt/novell/dirxml --relocate=/var=$ROOTDIR/var --badreloc --nodeps --replacefiles <rpm-location>`

For example, to install the HR driver RPM, use this command:

```
rpm --dbpath $ROOTDIR/rpm -Uvh --relocate=/usr=$ROOTDIR/opt/novell/eDirectory
--relocate=/etc=$ROOTDIR/etc --relocate=/opt/novell/eDirectory=$ROOTDIR/opt/
novell/eDirectory --relocate=/opt/novell/dirxml=$ROOTDIR/opt/novell/dirxml --
relocate=/var=$ROOTDIR/var --badreloc --nodeps --replacefiles /home/user/
novell-DXMLebsHR.rpm
```

5 Securing Communication

If the remote Web service you are accessing allows HTTPS connections, you can configure the driver to take advantage of this increased security.

IMPORTANT: Only certificates from a Java keystore are accepted. Make sure that the keystore for the certificates is a Java keystore.

The following sections provide instructions for creating a secure connection between Identity Manager and the Oracle EBS system:

- "Configuring the Publisher Channel Using the KMO File" on page 33
- "Configuring the Publisher Channel Using the Keystore File" on page 34
- "Configuring the Subscriber Channel" on page 36

Configuring the Publisher Channel Using the KMO File

The Publisher channel sends information from the Web service to the Identity Vault. To establish a secure connection for the Publisher channel, you need a keystore or a KMO containing a certificate issued by the certificate authority that signed the server's certificate.

Oracle Wallet Manager is an application used to manage and edit security credentials in Oracle wallets. A wallet is a password-protected container that stores authentication and signing credentials, including private keys, certificates, and trusted certificates, all of which are used by SSL for strong authentication. For more information, see Managing Wallets and Certificates.

1 Create a server certificate in iManager.:

   1a In the **Roles and Tasks** view, click **Novell Certificate Server > Create Server Certificate**.

   1b Browse to and select the server object where the Oracle EBS driver is installed.

   1c Specify a certificate nickname.

   1d Select **Standard** as the creation method, then click **Next**.

   1e Click **Finish**, then click **Close**.

2 Export a self-signed certificate from the certificate authority in eDirectory:

   2a In the **Roles and Tasks** view, click **Directory Administration > Modify Object**.

   2b Select your tree's certificate authority object, then click **OK**.

   It is usually found in the Security container and is named something like *TREENAME CA.Security*.

   2c Click **Certificate > Self Signed Certificate**., then click **Export**.

   2d When asked if you want to export the private key with the certificate, click **No**, then click **Next**.

   2e Based on the client to be accessing the Web service, select either **File in binary DER format** or **File in Base64 format** for the certificate, then click **Next**.

   If the client uses a Java-based keystore or trust store, then you can choose either format.

2f Click **Save the exported certificate to a file**.

2g Click **Save**, then browse to a known location on your computer.

2h Click **Save**, then click **Close**.

2i Save the certificate in the Wallet Manager.

3 Start the Oracle Wallet Manager and create the certificate in the Oracle EBS system:

- ◆ **UNIX:** At the command line, enter `owm`.

- ◆ **Windows:** Select **Start > Programs > Oracle-HOME_NAME > Network Administration > Wallet Manager**.

4 Import the certificate to the list of trusted certificates in the Oracle Wallet Manager:

4a Click **Operations > Import Trusted Certificate**, the Import Trusted Certificate dialog appears. Select the certificate created in Step 2 and click **OK**.

A message informs you that the trusted certificate was successfully imported into the wallet. The trusted certificate appears at the bottom of the Trusted Certificates tree in the Oracle Wallet Manager main panel.

4b Save the wallet.

4c Copy the Wallet Manager folder to a new location (for example, `/opt/wallet`).

4d Execute the following SQL statements in the Oracle EBS system to configure the wallet:

```
insert into idmusrmgt.idm_config values('WALLET_PATH','file:/etc/ORACLE/
WALLETS/pub')

insert into idmusrmgt.idm_config values('WALLET_PASSWORD','test123');
```

4e Add the required permissions for the folder in Step 4c, then click **OK**.

5 Configure the Publisher channel to use the server certificate created in Step 1:

5a In iManager, in the **Roles and Tasks** view, click **Identity Manager > Identity Manager Overview**.

5b Locate the driver set containing the Oracle EBS driver, then click the driver's icon to display the Identity Manager Driver Overview page.

5c In the Identity Manager Driver Overview page, click the driver's icon again, then scroll to **Publisher Settings**.

5d In the **KMO name** setting, specify the certificate nickname used in Step 1.

6 Click **Apply**, then click **OK**.

Configuring the Publisher Channel Using the Keystore File

1 Create a keystore and its alias:

```
keytool -genkey -alias publisher10 -dname "cn=172.18.4.15:6060" -keypass novell
-keystore publisherstore10.keystore -keyalg RSA
```

where **publisher10** is the alias and **publisherstore10.keystore** is the name of the keystore. CN is the IP address of the Publisher listener (port). RSA algorithm is required for creating certificates in the Oracle wallets.

2 Self-sign the certificate:

```
keytool -selfcert -alias publisher10 -dname "cn=172.18.4.15:6060" -keypass
novell -keystore publisherstore10.keystore
```

3 Export the certificate to a file called `publisher10.cert`:

```
keytool -export -alias publisher10 -file publisher10.cert -keystore
publisherstore10.keystore -storepass novell
```

4 Import the certificate in the Wallet Manager.

5 Start Oracle Wallet Manager.

   ◆ **UNIX:** At the command line, enter `owm`.

   ◆ **Windows:** Select **Start > Programs > Oracle-HOME_NAME > Network Administration > Wallet Manager**.

6 Add the certificate (`publisher10.cert`) to the list of trusted certificates in the Oracle Wallet Manager:

   6a Click **Operations > Import Trusted Certificate**, the Import Trusted Certificate dialog appears. Select the certificate created in Step 3 and click OK.

   A message informs you that the trusted certificate was successfully imported into the wallet. The trusted certificate appears at the bottom of the Trusted Certificates tree in the Oracle Wallet Manager main panel.

   6b Save the wallet.

   6c The trusted certificate appears at the bottom of the Trusted Certificates tree in the Oracle Wallet Manager main panel.

   6d Copy the Wallet Manager folder to a new location (for example, `/opt/wallet`).

   6e Execute the following SQL statements in the Oracle EBS system to configure the wallet:

   ```
   insert into idmusrmgt.idm_config values('WALLET_PATH','fi le:/etc/ORACLE/
   WALLETS/pub')

   insert into idmusrmgt.idm_config values('WALLET_PASSWORD','test123');
   ```

   6f Add the required permissions for the folder in Step 6d.

NOTE: The certificate generated using Java 7 is not compatible with the Oracle Wallet Manager. To generate a new certificate, use Java 6 in the `/opt/novell/eDirectory/lib64/nds-modules/embox/jre/bin/java` directory.

7 Configure the Publisher channel to use the server certificate created in Step 1:

   7a In iManager, in the **Roles and Tasks** view, click **Identity Manager > Identity Manager Overview**.

   7b Locate the driver set containing the Oracle EBS driver, then click the driver's icon to display the Identity Manager Driver Overview page.

   7c In the Identity Manager Driver Overview page, click the driver's icon again, then scroll to **Publisher Settings**.

   7d In the **Keystore File** setting, specify the certificate nickname you used in Step 1.

8 Click **Apply**, then click **OK**.

NOTE: For setting up mutual authentication on a Publisher channel (by using either the KMO or the keystore file), set the `Require mutual authentication` flag status to `Required`.

Configuring the Subscriber Channel

The Subscriber channel sends information from the Identity Vault to the Web service. To establish a secure connection for the Subscriber channel, you need a trust store containing a certificate issued by the certificate authority that signed the server's certificate.

Oracle Wallet Manager is an application used to manage and edit security credentials in Oracle wallets. A wallet is a password-protected container that stores authentication and signing credentials, including private keys, certificates, and trusted certificates, all of which are used by SSL for strong authentication. For more information, see Managing Wallets and Certificates.

1 If you are not using the default wallet.

   1a Change the **SSLWallet** property in the `ssl.conf` file to point the path of the wallet. For example, if SSL wallet file is present in the `/etc/ORACLE/WALLETS/pub` location, enter this path in the `ssl.conf` file (for example, `/u01/app/VIS/inst/apps/VIS_hostname/ora/10.1.3/conf/ssl.conf`).

   1b Add the path of the wallet in the `sqlnet.ora` file:

```
WALLET_LOCATION=
 (SOURCE=
      (METHOD=file)
      (METHOD_DATA=
          (DIRECTORY=/etc/ORACLE/WALLETS/pub)))
```

The `sqlnet.ora` file is present in the `<ORACLE_HOME>/network/admin/<VIS_hostname>` location.

2 Specify the HTTPS port as **Listen** in the `ssl.conf` file. For example, **Listen 4443**.

3 Start the Oracle Wallet Manager and create the certificate in the Oracle EBS system:

- **UNIX:** At the command line, enter `owm`.
- **Windows:** Select **Start > Programs > Oracle-HOME_NAME > Network Administration > Wallet Manager**.

   3a Add a certificate request to an Oracle wallet. Click **Operations > Add Certificate Request**.

The **Common Name** must match with the **hostname** (don't include port). This is same as the **Server Name** entry in the `httpd.conf` file (for example, `sles11sp164-ora.novell.com`)

   3b Export the certificate request created in 3a. Click **Operations > Export Certificate Request**, then save the exported file with a `.csr` extension (for example, `subreq.csr`).

   3c (Conditional) Create a new Certificate Authority.

```
openssl req -new -x509 -keyout cakey.pem -out cacert.crt -days 365
```

Omit this step if you are using an existing Certificate Authority.

   3d Create the user certificate.

```
openssl x509 -req -in subreq.csr -CA cacert.crt -CAkey cakey.pem -
CAcreateserial -days 365 > server.crt
```

   3e Add the `cacert.crt` certificate to the wallet. Click **Operations > Import Trusted Certificate**.

   3f Add the `server.crt` certificate to the wallet. Click **Operations > Import User Certificate**.

   3g Save the wallet, then restart the Oracle EBS system.

If you are not using default wallet location, copy the wallet files to the custom location.

4 Download the certificate created in Step 3 from the Oracle EBS system.

- Export the certificate using the Oracle Wallet Manager.

Or

- ◆ Type the URL in a Web browser and download the certificate.

  For example, type `https://sles11sp164-ora.novell.com:4443`.

5 Copy the certificate to the Identity Vault machine.

6 Add the certificate to the trust store using the keytool.

```
keytool -import -file subscriber.cer -trustcacerts -noprompt -keystore
dirxml.keystore -storepass novell
```

where `subscriber.cer` is the certificate downloaded in Step 4.

7 Configure the Subscriber channel to use the keystore name (`dirxml.keystore`) created in Step 6:

7a In iManager, in the **Roles and Tasks** view, click **Identity Manager > Identity Manager Overview**.

7b Locate the driver set containing the Oracle EBS driver, then click the driver's icon to display the Identity Manager Driver Overview page.

7c On the Identity Manager Driver Overview page, click the driver's icon again, then scroll to **Subscriber Settings**.

7d In the **Truststore File** setting, specify the path to the keystore created in Step 6.

8 Click **Apply**, then click **OK**.

NOTE: For setting up mutual authentication on the Subscriber channel, follow the instructions from Configuring the Publisher Channel Using the Keystore File and add the certificate to the keystore file in the Subscriber channel mutual authentication settings.

---

6 Managing the Driver

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

- Starting, stopping, and restarting 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
- Synchronizing objects
- Migrating and resynchronizing data

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*.

7 Troubleshooting the Driver

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

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*.

Troubleshooting Driver Issues

The following known issues exist for this version of the driver:

NDSTrace shows http connection protocol on the Publisher channel

The trace shows http when https has been setup on the Publisher channel.

OutOfMemory Error

1If the driver shuts down with a java.lang.OutOfMemory error, do the following:

1 Try setting or increasing the DHOST_JVM_INITIAL_HEAP and DHOST_JVM_MAX_HEAP environment variables.

2 Restart the driver.

3 Monitor the driver to make sure that the variables provide enough memory.

For more information, see "Configuring Java Environment Parameters" in the *NetIQ Identity Manager Driver Administration Guide*.

Increasing the memory heap size

The `oafm` module handles Webservices in the Oracle EBS system. To increase the memory heap size,

1 Go to the `opmn.xml` file in the `/u01/app/VIS/inst/apps/VIS_sles11sp164-ora/ora/10.1.3/opmn/conf` directory and search for `oafm <process-type> id`.

2 Edit the start-parameters and stop-parameters. Increase the Xmx to 2048, Xms to 1024, and MaxPermSize to 512.

8 Schema Mapping

The policies and filters included in the driver packages provide bidirectional creation, deletion, and modification of user information in the Identity Vault and the Oracle EBS system. The driver is configured to synchronize information from the Identity Vault to the Oracle EBS system (Subscriber channel) and from the Oracle EBS system to the Identity Vault (Publisher channel). You can modify the policies and the filter to work with your specific business environment.

The Schema Mapping policy is referenced by the driver object and applies to both the Subscriber and the Publisher channel. The purpose of the Schema Mapping policy is to map schema names (particularly attribute names and class names) between the Identity Vault and the Oracle User database table (idmusrmgt.idm_events). Any modification or removal of existing entries in the Schema Mapping policy could destroy the default configuration and policies processing behavior. Adding new attribute mappings is discretionary.

Table 8-1, Table 8-2, and Table 8-3 contain default mappings between the Oracle EBS user attributes for User Management, HR, and TCA modules and the Identity Vault attributes.

Table 8-1 *Oracle User Management Attributes and the Identity Vault Attributes*

Identity Vault Attribute	Oracle User Management Attribute
User	i**netOrgPerson**
CN	USER_NAME
Description	DESCRIPTION
Facsimile Telephone Number	FAX
Internet EMail Address	EMAIL_ADDRESS
Surname	Mapped as default password if the password is not specified for the user.
Login Expiration Time	END_DATE
loginActivationTime	START_DATE
Password Expiration Interval	PASSWORD_LIFESPAN_DAYS
	IMPORTANT: If the **Password Expiration** field is set to **Accesses** in the Oracle EBS system, the password expiration interval is turned off. The Identity Vault does not have a corresponding attribute for **Accesses**; therefore, the driver fails to synchronize the password expiration changes with the Identity Vault. However, the changes are successfully synchronized if the password expiration interval is set to **number of days**.
Login Disabled	LOGIN_DISABLED
DirXML-ebsPersonId	EMPLOYEE_ID

Table 8-2   *Oracle HR Attributes and the Identity Vault Attributes*

Identity Vault Attribute	Oracle HR Attribute
User	i**netOrgPerson**
Internet EMail Address	P_EMAIL_ADDRESS
Surname	P_LAST_NAME
Given Name	P_FIRST_NAME
mailstop	P_MAILSTOP
L	P_INTERNAL_LOCATION
Initials	P_MIDDLE_NAMES
DirXML-ebsGender	P_SEX

Table 8-3   *Oracle TCA Attributes and the Identity Vault Attributes*

Identity Vault Attribute	Oracle TCA Attribute
User	i**netOrgPerson**
CN	USER_NAME
Description	DESCRIPTION
Facsimile Telephone Number	FAX
Login Expiration Time	END_DATE
loginActivationTime	START_DATE
Password Expiration Interval	PASSWORD_LIFESPAN_DAYS
Internet EMail Address	TCA_EMAIL_ADDRESS
Login Disabled	LOGIN_DISABLED
Surname	TCA_PERSON_LAST_NAME
Given Name	TCA_PERSON_FIRST_NAME
EMail Address	EMAIL_ADDRESS
Initials	TCA_PERSON_MIDDLE_NAME

A Driver Properties

This section provides information about the Driver Configuration and Global Configuration Values properties for the Oracle EBS driver. These are the only unique properties for this driver. 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 the viewpoint of iManager. If a field is different in Designer, it is marked with a Designer icon.

- "Driver Configuration" on page 45
- "Global Configuration Values" on page 50

Driver Configuration

In Designer:

1 Open a project in the Modeler.

2 Right-click the driver icon 🔧 or line, then select click **Properties > Driver Configuration.**

In iManager:

1 In iManager, click 👤 to display the Identity Manager Administration page.

2 Open the driver set that contains the driver whose properties you want to edit:

  2a In the **Administration** list, click **Identity Manager Overview**.

  2b If the driver set is not listed on the **Driver Sets** tab, use the **Search In** field to search for and display the driver set.

  2c Click the driver set to open the Driver Set Overview page.

3 Locate the Oracle EBS driver icon, then click the upper right corner of the driver icon to display the Actions menu.

4 Click **Edit Properties** to display the driver's properties page.

  By default, the properties page opens with the **Driver Configuration** tab displayed.

The Driver Configuration options are divided into the following sections:

- "Driver Module" on page 46
- "Driver Object Password" on page 46
- "Authentication" on page 46
- "Startup Option" on page 47
- "Driver Parameters" on page 47
- "Global Configurations" on page 50

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 name of the Java class for the User Management driver is:
  `com.novell.nds.dirxml.driver.ebs.user.EBSUserDriver`
- The name of the Java class is for the HR driver is:
  `com.novell.nds.dirxml.driver.ebs.hr.EBSHRDriver`
- The name of the Java class for the TCA driver is:
  `com.novell.nds.dirxml.driver.ebs.tca.EBSTCADriver`

Native: This option is not used with the Oracle drivers.

Connect to Remote Loader: Used when the driver is connecting remotely to the Oracle EBS 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 Oracle User 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 Oracle EBS system.

Authentication ID: Specify an Oracle account that the driver can use to authenticate to the Oracle system.

For example:

For all drivers (User Management, HR, or TCA), assign `System Administrator` responsibility to the user.

Authentication Context: Specify the IP address or name of the Oracle EBS server the driver should communicate with. For example, `http://myoracleserver.com:8000/webservices/SOAProvider/plsql/idm_driver_s/`.

NOTE: To test the connection with Oracle EBS server, use the following command:

```
curl -v -u "$USERNAME:$PASSWORD" -H "$CONTENTTYPE" -H "$SOAPACTION" -d "$POSTDATA" "$SOAPURL"
```

Remote Loader Connection Parameters: Used only if the driver is connecting to the application through the Remote Loader.

In iManager, enter `hostname=xxx.xxx.xxx.xxx port=xxxx secureprotocol=TLS version enforceSuiteB=`*true/false* `kmo=certificatename`.

- `hostname` specifies the IP address of the Remote Loader server.
- `port` specifies the TCP/IP port on which the Remote Loader listens for connections from the remote interface shim. The default port for the Remote Loader is 8090.
- `secureprotocol` specifies the version of the TLS protocol that the Remote Loader uses to connect to the Identity Manager engine. Identity Manager supports TLSv1, TLS v1_1, and TLSv1_2 versions only.
- `enforceSuiteB` specifies whether the Remote Loader uses Suite B for communicating with the Identity Manager engine. To use Suite B, specify `enforceSuiteB=true`. The communication supports only TLS version 1.2 version. Communication is not established if the connection has non-Suite B authentication algorithms.
- The `kmo` entry is optional. Use it only when an SSL connection exists between the Remote Loader and the Identity Manager engine.

  For example: `hostname=10.0.0.1 port=8090 kmo=IDMCertificate`

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

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 Oracle EBS system.

Driver 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 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 iManager.

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:

Subscriber Options

Subscriber Channel Enabled: By default, the Subscriber channel is enabled. This means that the events are synchronized from the Identity Manager to the Oracle EBS system. Fill the following fields for the Subscriber options:

Use SSL: By default, the SSL connection is enabled to secure communication between the driver and the Oracle EBS server. Specify **No** to not use SSL. For more information, see Chapter 5, "Securing Communication," on page 33.

If you use SSL, fill in the following parameters:

Truststore File: Specifies the name and path of the keystore file containing the trusted certificates used when the remote server is configured to provide server authentication. For example, `c:\security\truststore`. Leave this field empty when server authentication is not used.

Set Mutual Authentication Parameters: Specify **Yes** to set mutual authentication information. Specify **No** to not use mutual authentication.

- **Keystore File:** Specify the path and the name of the keystore file that contains the trusted certificates for the remote server to provide mutual authentication. For example, `C:\security\keystore`. Leave this field blank when mutual authentication is not used.

- **Keystore Password:** Specify the password for the keystore file. Leave this field blank when mutual authentication is not used.

Use Proxy: Specify **Yes** if you want to use the proxy connection. Specify **No** to not use proxy.

- **Proxy Host and Port:** Specify the host address and the host port when a proxy host and port are used. For example: xxx.xx.x.x:xxxxx.

  Or, if a proxy host and port are not used, leave this field empty.

- **Proxy Username:** Specify a name for the proxy connection.

- **Proxy Password:** Specify a password for the proxy connection.

HTTP Errors to Retry: The HTTP error codes that return a retry status. The list of integers is separated by spaces. The error codes are: 307 404 408 503 504.

Publisher Options

Publisher Channel Enabled: By default, the Publisher channel is enabled. The events are synchronized from the Oracle EBS system to Identity Manager. Fill the following fields for the Publisher options:

Listening IP Address and Port: Specifies the IP address of the server where the Oracle EBS driver is installed and the port number that this driver listens on.

Choose an unused port number on your server. For example: 192.168.10.1:18180. The driver listens on this address for incoming requests, processes the requests, and returns a result. Leave this field blank when the Publisher channel is not active.

Authentication ID: Specify the Authentication ID that the driver will use to validate the Publisher events from the Oracle EBS system. It is communicated to the Oracle EBS system when the driver is started. The driver uses it to determine which events it should ignore. For example, it ignores events from the unauthorized connected systems.

Authentication Password: Specify the authentication password that the driver will use to validate the Publisher events from the Oracle EBS system. It is communicated to the Oracle EBS system when the driver is started.

If you need to clear the password, select **Remove existing password**, then click **Apply**.

Server Key Alias: When this server is configured to accept HTTPS connections, this is the key alias. Leave this field blank when a KMO name is used or when HTTPS connections are not used.

Server Key Password: When this server is configured to accept HTTPS connections, this is the key alias password (not the keystore password). Leave this field blank when a KMO name is used or when HTTPS connections are not used.

Use SSL: By default, the SSL connection is used for secure communication between the Oracle drivers and the Oracle EBS server. Specify **No** to not use SSL. For more information, see Chapter 5, "Securing Communication," on page 33.

When SSL is used, fill the following parameters:

Select Certificate Store Mode: There are two options: **KMO** and **Keystore**. Select **KMO** if you are using eDirectory KMO for secure connection. Select **Keystore** to use the Java Keystore.

KMO Name: If you select KMO for the secure connection, specify the KMO name to be used in eDirectory.

When the server is configured to accept HTTPS connections, this name becomes the KMO name in the Identity Vault. The KMO name is the name before the "-" (dash) in the RDN.

Leave this field empty when a keystore file is used or when HTTPS connections are not used.

Keystore File: If Keystore option is used for the secure connection, this field specifies the keystore name and path to the keystore file. This file is used when the server is configured to accept HTTPS connections.

Leave this field empty when a KMO name is used or when HTTPS connections are not used.

Keystore Password: Specifies the keystore file password used with the **Keystore File** field when this server is configured to accept HTTPS connections.

Leave this field empty when a KMO name is used or when HTTPS connections are not used.

Server Key Alias: Specifies a Server key alias when this server is configured to accept HTTPS connections.

Leave this field empty when a KMO name is used or when HTTPS connections are not used.

Server Key Password: When this server is configured to accept HTTPS connections, this is the key alias password (not the keystore password). Leave this field empty when a KMO name is used or when HTTPS connections are not used.

Require Mutual Authentication: When using SSL, it is common to do only server authentication. However, if you want to force both client and server to present certificates during the handshake process, mutual authentication is required.

Polling Interval in Seconds: Specifies how often the Publisher channel polls for unprocessed events. Leave this field blank to turn off the polling. The default value is 60 seconds.

Heartbeat Interval in Minutes: Configures the driver shim to send a periodic status message on the Publisher channel when there has been no Publisher traffic for the given number of minutes. Leave this field empty to turn off the heartbeat. The default value is 1 minute.

Global Configurations

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 Oracle User Management 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 iManager:

1 Click 🌐 to display the Identity Manager Administration page.

2 Open the driver set that contains the driver whose properties you want to edit.

   2a In the **Administration** list, click **Identity Manager Overview**.

   2b If the driver set is not listed on the **Driver Sets** tab, use the **Search In** field to search for and display the driver set.

   2c Click the driver set to open the Driver Set Overview page.

3 Locate the driver icon, click the upper right corner of the driver icon to display the **Actions** menu, then click **Edit Properties**.

   or

   To add a GCV to the driver set, click **Driver Set**, then click **Edit Driver Set properties**.

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 GCVs are divided into the following categories:

- "Password Synchronization" on page 51
- "(Conditional) Default Configuration" on page 51
- "Entitlements" on page 51
- "Account Tracking" on page 54
- "Managed System Information" on page 54

IMPORTANT: The HR driver synchronizes employee information; therefore, Account Tracking and Password Synchronization GCVs do not apply to this driver.

Password Synchronization

These GCVs enable password synchronization between the Identity Vault and the Oracle EBS 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 iManager, to edit the Password management options go to **Driver Properties > Global Configuration Values**, and then edit it in your Password synchronization policy tab.

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

Oracle EBS User's Default password: Specify the default password for the Oracle EBS users. The minimum length of the password should be more than 5 characters. If the user password is empty or contains less than 5 characters, the default password is set.

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

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

Publish passwords to NDS password: Use the password from the Oracle EBS system to set the non-reversible NDS password in the Identity Vault.

Publish passwords to Distribution Password: Use the password from the Oracle EBS 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, attempt to reset the password in the Oracle EBS system by using the Distribution Password from the Identity Manager data store.

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

(Conditional) Default Configuration

Set Oracle EBS HR As Authoritative Data Source: Select True if you don't want to synchronize add and delete operations on the Subscriber channel. All other operations including modify are synchronized. By default, False is selected.

Entitlements

There are multiple sections in the **Entitlements** tab. Depending on which packages you installed, different options are enabled or displayed.

- "Entitlements Options for User Management and TCA Drivers" on page 52
- "Data Collection Options for User Management and TCA Drivers" on page 52
- "Role Mapping Options for User Management and TCA Drivers" on page 52
- "Resource Mapping Options for User Management and TCA Drivers" on page 53

Entitlements Options for User Management and TCA Drivers

(User Management and TCA drivers) Use User Account Entitlement: Select **True** to enable the driver to manage user accounts based on the driver's defined entitlements. Select **False** to disable management of user accounts based on the entitlements.

- **Enable Login Disabled Attribute Sync:** Select **Yes** if the changes made to the LoginDisabled attribute in the Identity Vault should be synchronized even if the User Account entitlement (Account) is enabled.
- **Account Action on Entitlement Revoke?:** Select the action to take when a user account entitlement is revoked. The options are **Disable User or Do Nothing**. By default, **Disable User** is selected.

Use Role Entitlement: Enables the Role entitlement that is included with the driver. Select **True** to enable this entitlement.

Use Responsibility Entitlement: Enables the Responsibility entitlement that is included with the driver. Select **True** to enable this entitlement.

Advanced Settings: Select **Show** to display the entitlement options that allow or deny additional functionality like data collection and others. These settings should rarely be changed.

Data Collection Options for User Management and TCA Drivers

Data collection enables the Identity Report Module to gather information to generate reports. For more information, see the *Administrator Guide to NetIQ Identity Reporting*.

Enable data collection: Select **Yes** to enable data collection for the driver through the Data Collection Service by the Managed System Gateway driver. If you are not going to run reports on data collected by this driver, select **No**.

Allow data collection from user accounts: If **Yes**, it allows data collection by the Data Collection Service for the user accounts.

Allow data collection from roles: If **Yes**, it allows data collection by the Data Collection Service for roles.

Allow data collection from resources: If **Yes**, it allows data collection by the Data Collection Service for responsibilities.

Role Mapping Options for User Management and TCA Drivers

The Identity Manager Catalog Administrator allows you to map business roles with IT roles. For more information, see the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Enable role mapping: If **Yes**, the driver is visible to Catalog Administrator.

Allow mapping of user accounts: If **Yes**, it allows mapping of user accounts in Catalog Administrator. An account is required before a role or responsibility can be granted to it through Catalog Administrator.

Allow mapping of roles: If **Yes**, it allows mapping of groups in Catalog Administrator.

Allow mapping of responsibilities: If **Yes**, it allows mapping of responsibilities in Catalog Administrator.

Resource Mapping Options for User Management and TCA Drivers

Identity Applications allow you to map resources to users. For more information, see the *NetIQ Identity Manager - User's Guide to the Identity Applications*.

Enables resource mapping: If **Yes**, the driver is visible to Identity Applications.

Allow mapping of user accounts: If **Yes**, it allows mapping of user accounts in Identity Applications. An account is required before a role or responsibility can be granted to it.

Allow mapping of roles: If **Yes**, it allows mapping of roles in Identity Applications.

Allow mapping of responsibilities: If **Yes**, it allows mapping of responsibilities in Identity Applications.

Entitlements Options for the HR Driver

Use Employee Entitlements: Select **True** to enable the HR driver to manage employees based on the driver's defined entitlements. Select **False** to disable employees based on the entitlements.

- **Action on Employee while Entitlement Revoke?:** Select the action to take when an entitlement is revoked for an employee. The options are **Delete User or Do Nothing**. By default, **Delete User** is selected.

Format for Employee entitlement: Specifies the parameter format that the entitlement agent uses when granting this entitlement. The options are **Identity Manager 4** or **Legacy**.

Data Collection Options for the HR Driver

Data collection enables Identity Reporting to gather information to generate reports. For more information, see the *Administrator Guide to NetIQ Identity Reporting*.

Enable data collection: Select **Yes** to enable data collection for the driver through Data Collection Service by the Managed System Gateway driver. If you are not going to run reports on data collected by this driver, select **No**.

Allow data collection from employees: If **Yes**, it allows data collection by Data Collection Service for employees.

Role Mapping Options for the HR Driver

Identity Applications allow you to map business roles with IT roles. For more information, see the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Enable role mapping: If **Yes**, the driver is visible to Identity Applications.

Allow mapping of employees: If **Yes**, it allows mapping of employees in Identity Applications.

Resource Mapping Options for the HR Driver

Identity Applications allow you to map resources to employees. For more information, see the *NetIQ Identity Manager - User's Guide to the Identity Applications*.

Enables resource mapping: If **Yes**, the driver is visible to Identity Applications.

Allow mapping of employees: If **Yes**, it allows mapping of employees in Identity Applications.

Entitlement Extensions

User account extensions: The content of this field is added below the entitlement elements in the EntitlementConfiguration resource object.

Role extensions: The content of this field is added below the entitlement elements in the EntitlementConfiguration resource object.

Resource extensions: The content of this field is added below the entitlement elements in the EntitlementConfiguration resource object.

Account Tracking

Account tracking is part of Identity Reporting. For more information, see the *Administrator Guide to NetIQ Identity Reporting*.

Enable account tracking: Set this to **True** to enable account tracking policies. Set it to **False** if you do not want to execute account tracking policies.

Realm: Specify the name of the realm, security domain, or namespace in which the account name is unique. You must set the **Realm** to the Oracle EBS Domain Name.

Object Class: Adds the object class to track. Class names must be in the application namespace.

Identifiers: Adds the account identifier attributes. Attribute names must be in the application namespace.

Status attribute: Is the name of the attribute in the application namespace to represent the account status.

Status active value: Is the value of the status attribute that represents an active state.

Status inactive value: Is the value of the status attribute that represents an inactive state.

Subscription default status: Specifies the default status that the policies assume when an object is subscribed to the application and the status attribute is not set in the Identity Vault.

Publication default status: Specifies the default status that the policies assume when an object is published to the Identity Vault and the status attribute is not set in the application.

Managed System Information

These settings help Identity Reporting function to generate reports. There are different sections in the **Managed System Information** tab.

- "General Information" on page 55
- "System Ownership" on page 55

General Information

Name: Specify a descriptive name for the managed system.

Description: Specify a brief description of the managed system.

Location: Specify the physical location of the managed system.

Vendor: Specify Oracle as the vendor of the managed system.

Version: Specify the version of the managed system.

System Ownership

Business Owner: Browse to and select the business owner in the Identity Vault for the Oracle EBS system. You must select a user object, not a role, group, or container.

Application Owner: Browse to and select the application owner in the Identity Vault for the Oracle EBS system. You must select a user object, not a role, group, or container.

System Classification

Classification: Select the classification of the Oracle EBS system. This information is displayed in the reports. The options are:

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

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

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

- Development
- Test
- Staging
- Production
- Other

  If you select **Other**, you must specify a custom classification for the Oracle EBS system

Connection and Miscellaneous Information

Connection and miscellaneous information: This set of options is always set to **hide**, so that you don't make changes to these options. These options are system options that are necessary for reporting to work.

B ^{Trace Levels}

Trace Levels

The driver supports the following trace levels:

Table B-1 *Supported Trace Levels*

Level	Description
0	No debugging
1-3	Identity Manager messages. Higher trace levels provide more detail.
4	Previous level plus Remote Loader, driver, driver shim, and driver connection messages, driver parameters, driver security, driver schema, request and response XML.

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

Oracle EBS Trace and Logging

You can enable trace and logging in the Oracle User Management, HR, or TCA modules. For example, to enable trace in the User Management module,

1. Log in to the Oracle EBS system with an administrator role.
2. Go to **System Administrator > Security:User > Define window**.
3. Click **Help > Diagnostics > Trace,** then select one of the following options:
   - No Trace

      Regular Trace

      Trace with Binds

      Trace with Waits

      Trace with Binds and Waits
   - PL/SQL Profiling

To disable the trace, click **No Trace**.

To enable logging in the User Management module,

1. Log in to the Oracle EBS system with an administrator role.
2. Go to **System Administrator > Security:User > Define window**.
3. Click **Help > Diagnostics > Logging > Preferences.**

A screen like this appears:

C Customizing the Drivers

This section provides information about customizing the Identity Manager User Management, HRMS, and TCA drivers. To synchronize the extended attribute between the drivers and Identity Manager, you need to modify the Publisher and Subscriber channels appropriately.

Before proceeding with the driver customization, ensure that you have a good working knowledge of the PL/SQL scripts and Oracle database concepts. For more information, refer to the Oracle documentation set.

Customizing the Publisher Channel

The Publisher channel of the Oracle EBS drivers is enabled by default. To change the default driver configuration, use Designer.

The following sections provide information about customizing the Publisher channel to synchronize additional attributes from the different Oracle modules with which the drivers synchronize attributes.

Using the Oracle E-Business Events

The Publisher channel of the driver is enabled by default unless you change this setting during driver configuration in Designer. The driver starts when the Oracle EBS system starts and internally starts the HTTP jetty server and listens on the specified port for the Publisher events from the Oracle EBS system. The PL/SQL script securely transports the events to the `http://<driver IP address>:<Port>` URL, then the driver submits the XML documents to the Identity Manager engine to publish the XML documents in the Identity Vault.

The following are sample XML documents for User Add and Modify operations supported in the Publisher channel. You can customize them to suit your environment.

Example C-1   Publisher XML Request for a User Add Event

```
<EBS_EVENT>
        <EVENT_NAME>oracle.apps.fnd.user.insert</EVENT_NAME>
        <EVENT_KEY>$user id</EVENT_KEY>
        <OBJECT type="user">
                <USER_NAME></USER_NAME>
                <EMAIL_ADDRESS></EMAIL_ADDRESS>
                <DESCRIPTION></DESCRIPTION>
                        .
                        .
                        .
                        .
                <LOGIN_DISABLED>false</LOGIN_DISABLED>
        </OBJECT>
</EBS_EVENT>
```

Example C-2 Publisher XML Request for a User Modify Event

```
<EBS_EVENT>
    <EVENT_NAME>oracle.apps.fnd.user.update</EVENT_NAME>
    <EVENT_KEY>$user id</EVENT_KEY>
    <OBJECT type="user">
        <USER_NAME></USER_NAME>
        <EMAIL_ADDRESS></EMAIL_ADDRESS>
        <DESCRIPTION></DESCRIPTION>
            .
            .
            .
            .
        <LOGIN_DISABLED>false</LOGIN_DISABLED>
    </OBJECT>
    <OLD_OBJECT type="user">
        <USER_NAME></USER_NAME>
        <EMAIL_ADDRESS></EMAIL_ADDRESS>
        <DESCRIPTION></DESCRIPTION>
            .
            .
            .
            .
            .
            .
            .
         <LOGIN_DISABLED>false</LOGIN_DISABLED>
    </OLD_OBJECT>
</EBS_EVENT>
```

The Oracle E-Business events post the user attribute changes from the Oracle EBS system to the driver. Subscribe to these events to add or modify the users in the Identity Vault. You can write specific PL/SQL methods and then subscribe to the business events for receiving user information modifications. Otherwise, modify the PL/SQL scripts shipped with the driver.

By default, the driver can synchronize all attributes from the `FND_USER, ER_ALL_PEOPLE_F` and `HZ_PARTIES` tables. You need not modify the PL/SQL scripts to add new attributes. However, you need to modify the `IDM_DRIVER.PUBLISH_EVENT_TO_ IDM PL/SQL` script to synchronize attributes from the different tables in the Oracle EBS system.

NetIQ recommends that you add the new attributes as XML tags under the `<OBJECT>` tag and also add them to the driver Schema Mapping policy in the Identity Manager.

Polling the Oracle EBS System Tables

Another way of synchronizing the columns of other tables from the Oracle EBS system is to create a new PL/SQL procedure in the IDMDRIVER package, then modify the XML document and add it to the newly created PL/SQL procedure.

To synchronize an attribute from the PER_ADDRESSES table with Identity Manager, perform the following actions:

1 Construct the driver understandable XML document by creating a new `FIND_PER_ADDRESSES_ADD_EVENTS` procedure.

   This procedure should be similar to the `FIND_EMPLOYEE_ADD_EVENTS` procedure.

2 Post the XML document to the driver.

3 Call the new PL/SQL method as part of the driver polling cycle by adding the `FIND_PER_ADDRESSES_ADD_EVENTS` procedure in the `IDMDRIVER.SYNCH_EVENTS_WITH_IDM` procedure.

4 Modify the schema mapping policy for the driver to add the new attributes in Identity Manager.

5 Restart the driver.

Sample XML code for the Publisher Channel

1 Create a temporary table `IDMUSRMGT.IDM_PER_ADDRESSES` in the Oracle EBS system.

2 Identify the differences in the value between the temporary table and the Oracle EBS table using the below SQL query:

```
sql>CREATE TABLE IDMUSRMGT.IDM_ PER_ADDRESSES
  AS (SELECT *
        FROM PER_ADDRESSES
        WHERE ADDRESS_ID< 0);
```

3 Create a new procedure to read the user address.

```
PROCEDURE FIND_PER_ADDRESSES_ADD_EVENTS

IS
  HR_EVENT_DOC CLOB := NULL;
  clob_locator CLOB;
  v_person_id NUMBER(15) :=100;
  CURSOR PER_ADDRESSES_CUR
  IS
    SELECT *
    FROM (
      (SELECT unique PERSON_ID
      FROM PER_ADDRESSES
      WHERE CREATED_BY!=-1
      AND CREATION_DATE BETWEEN (SELECT START_DATE FROM
IDMUSRMGT.IDM_SYNC_START_DATE) AND SYSDATE
    MINUS
    SELECT PERSON_ID FROM IDMUSRMGT.IDM_PER_ADDRESSES
      ));
    PER_ALL_PEOPLE_REC PER_ADDRESSES_CUR%rowtype;
  BEGIN
    OPEN PER_ADDRESSES_CUR;
    LOOP
      FETCH PER_ADDRESSES_CUR INTO PER_ALL_PEOPLE_REC;
      EXIT
    WHEN PER_ADDRESSES_CUR%NOTFOUND;
      v_person_id    := PER_ALL_PEOPLE_REC.PERSON_ID;
      HR_EVENT_DOC :='<EBS_EVENT><EVENT_NAME>oracle.apps.fnd.user.insert</
EVENT_NAME><OBJECT type="user"><LOGIN_DISABLED>false</LOGIN_DISABLED></
OBJECT></EBS_EVENT>';
      SELECT dbms_xmlquery.getxml('SELECT * FROM PER_ADDRESSES where
PERSON_ID='
        ||v_person_id,10)
      INTO clob_locator
      FROM DUAL;
      DBMS_LOB.COPY(HR_EVENT_DOC, to_clob('<EMPLOYEE></EMPLOYEE>'), 21
```

```
     ,INSTR(HR_EVENT_DOC,'</EBS_EVENT>', -1), 1);
      DBMS_LOB.COPY(HR_EVENT_DOC,CLOB_LOCATOR,INSTR(CLOB_LOCATOR,'</ROW>',
   -1)- INSTR(CLOB_LOCATOR,'<ROW num="1">')-14 ,INSTR(HR_EVENT_DOC,'</EMPLOYEE>',
   -1), INSTR(CLOB_LOCATOR,'<ROW num="1">')+14);
          DELETE FROM IDMUSRMGT.IDM_PER_ADDRESSES WHERE PERSON_ID=v_person_id;
          INSERT INTO IDMUSRMGT.IDM_PER_ADDRESSES
          SELECT * FROM PER_ADDRESSES WHERE PERSON_ID=v_person_id;
          HR_EVENT_DOC:=HR_EVENT_DOC||'</EMPLOYEE></EBS_EVENT>';
          PERSISTS_EVENT(
   'oracle.apps.fnd.user.insert','EMPLOYEE_ADD',NULL,HR_EVENT_DOC,NULL,'NEW',SYSD
   ATE);
          commit;
          END LOOP;
      END;
```

4 Add the newly created procedure to the existing method.

```
PROCEDURE SYNCH_EVENTS_WITH_IDM(
    request IN VARCHAR2 )
IS
BEGIN
  FIND_EMPLOYEE_ADD_EVENTS();
      :
      :
      :
      :
      :
      :
  FIND_PER_ADDRESSES_ADD_EVENTS();
  PUBLISH_EVENTS();
END;
```

Verifying the Changes

1 Create a user/employee in the Oracle EBS system with the recently added attributes.

2 Modify the attributes.

3 Verify if the attributes are synchronised with the Identity Manager.

Customizing the Subscriber Channel

The following sections provide information about customizing the Subscriber channel to synchronize additional attributes from the different Oracle modules with which the drivers synchronize attributes.

Modifying the IDM_DRIVER_S PL/SQL Script

The Oracle EBS system provides many built-in APIs for making certain changes to the user or employee data. You can use the IDM_DRIVER_S PL/SQL package to make these changes on the Subscriber channel. This package uses some of the Oracle EBS built-in APIs.

Table C-1 lists the APIs used for each module.

Table C-1 *Oracle Module and EBS System APIs*

Oracle Modules	Oracle EBS System APIs
User Management	◆ fnd_user_pkg.createuser ◆ fnd_user_pkg.updateuser
HR Implementation	◆ r_employee_api.create_employee ◆ hr_person_api.update_person ◆ hr_person_api.delete_person
TCA	◆ hz_party_v2pub.create_person ◆ hz_party_v2pub.update_person ◆ hz_contact_point_v2pub.create_email_contact_point

To understand which attributes are supported by these APIs, use the SQL Developer tool and connect to the database where Oracle EBS system is installed. The API information is stored under the **Packages** panel on the left side of the screen. To view the APIs, expand the **Packages** panel.

NOTE: Currently, the query operations are supported on the FND_USER, PER_ALL_PEOPLE_F, and HZ_PARTIES tables.

Table C-2 lists the Identity Manager Schema attributes.

Table C-2 *Schema Attributes*

Condition	Action
Condition 1: The attribute is supported by one of the Oracle EBS system APIs and belongs to one of the FND_USER, PER_ALL_PEOPLE_F, or HZ_PARTIES tables.	There is no change required in the PL/SQL script. You can directly add the attribute to the driver schema and filter for extending it.
Condition 2: The attribute is supported by one of the Oracle EBS system APIs but does not belong to any of the FND_USER, PER_ALL_PEOPLE_F, or HZ_PARTIES tables.	Modify the query in the IDM_DRIVER_S package to specify the appropriate table name in the IF condition that starts with IF EVENT_NAME = TO_CHAR('oracle.apps.fnd.user.search') THEN statement.
Condition 3: The attribute is not supported by any of the Oracle EBS system APIs but belongs to one of the FND_USER, PER_ALL_PEOPLE_F, or HZ_PARTIES tables.	Determine which Oracle EBS system API is required to find the attribute, then add that API to the IDM_DRIVER_S PL/SQL package. You can use the EMPLOYEE_OPERATION and EXECUTE_EMPLOYEE_API functions as examples in the IDM_DRIVER_S package.
Condition 4: The attribute is neither supported by the Oracle EBS system APIs nor belongs to the FND_USER, PER_ALL_PEOPLE_F, or HZ_PARTIES tables.	Make changes as instructed for condition 2 and 3. A new Oracle EBS system API is needed to find the attribute and then modify the query to include it in the new table.

IMPORTANT: Restart the driver after making the required changes.

Verifying the Changes

1 Create a user in the Identity Vault with the recently added attributes and verify that the newly added attributes are synchronized to the EBS.

2 Perform a query operation for the recently added attributes and verify the response.

Example C-3   *XML Code for the Subscriber Changes*

```
<EBS_EVENT>
                <EVENT_NAME>oracle.apps.fnd.user.insert</EVENT_NAME>
                <DRIVER_TYPE>UM</DRIVER_TYPE>
                <OBJECT TYPE="USER">
                    <x_user_name>IDM_TEST_SUB_996111</x_user_name>
                    <x_description>IDM_TEST_SUB_998</x_description>
                    <x_email_address>IDM_TEST_SUB_998@test.com</x_email_address>
                    <x_fax>19999989</x_fax>
                </OBJECT>
            </EBS_EVENT>
```

Recommendations

NetIQ recommends that you apply the appropriate changes after the driver is successfully configured. After completing the changes, ensure that basic functionality of the drivers is working.