NetIQ® Identity Manager

Null Service and Loopback Service Drivers Implementation Guide

December 2014

Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government’s rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

© 2014 NetIQ Corporation. All Rights Reserved.

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

Contents

About This Guide

This guide provides information about the Identity Manager Loopback Service and Null Service drivers. Service drivers are used only for Metadirectory engine functions, not for connecting with external systems. They are automatically installed when you install Identity Manager.

The guide is organized as follows:

Audience

This guide is intended for administrators, consultants, and network engineers who require a high-level introduction to Identity Manager business solutions, technologies, and tools.

Documentation Updates

For the most recent version of this document, see the Identity Manager Documentation Web site (http://www.netiq.com/documentation/idm402/index.html).

Additional Documentation

For documentation on other Identity Manager drivers, see the Identity Manager Drivers Web site (http://www.netiq.com/documentation/idm402drivers/index.html).

1 Understanding the Null Service and Loopback Service Drivers

NetIQ Identity Manager includes two utility drivers, Null Service and Loopback Service, whose purpose is to implement custom behavior through policies established on the drivers' Subscriber and Publisher channels. Like other service drivers such as Entitlement and Workflow, the Null Service and Loopback Service drivers do not connect to external applications or systems.

The Null Service driver performs any tasks that are implemented through policies on the Subscriber channel. The Publisher channel is not used; the driver does not connect the Subscriber channel to the Publisher channel, but rather acts as a sink for most operations, simulates doing something with operations, and then returns success. Typical uses for the Null Service driver include the following:

- Adding the classes and attributes that you want to monitor for change in the Subscriber Filter as *Synchronize* for the class and *Notify* for the attribute.
- Adding Subscriber Event Transformation policies that react to specific object or attribute changes, and performing actions such as:
    - Making modifications back into the Identity Vault (using actions that manipulate source attributes and objects).
    - Sending e-mail.
    - Generating custom Audit events.
    - Calling extension functions to communicate the change outside of Identity Manager.
- Adding a final Subscriber Event Transformation policy that vetoes all events.

The Null Service driver should be sufficient for the majority of the tasks you want to perform. However, if you need to process policies on both the Subscriber and Publisher channels, you can use the Loopback Service driver instead. The only difference between the two drivers is that the Loopback Service driver's Subscriber channel connects to the Publisher channel so that events can also be processed on the Publisher channel.

1.1 Key Terms

1.1.1 Identity Manager

NetIQ Identity Manager is a service that synchronizes data among servers in a set of connected systems by using a robust set of configurable policies. Identity Manager uses the Identity Vault to store shared information, and uses the Metadirectory engine for policy-based management of the information as it changes in the vault or connected system. Identity Manager runs on the server where the Identity Vault and the Metadirectory engine are located.

1.1.2 Identity Vault

The Identity Vault is a persistent database powered by eDirectory and used by Identity Manager to hold data for synchronization with a connected system. You can view the vault as a private data store for Identity Manager or more broadly as a metadirectory that holds enterprise-wide data. Data in the vault is available to any protocol supported by eDirectory, including the NetWare Core Protocol (NCP), which is the traditional protocol used by iManager, LDAP, and DSML.

Because the Identity Vault is powered by eDirectory, you can easily integrate Identity Manager into your corporate directory infrastructure by using your existing directory tree as the vault.

1.1.3 Metadirectory Engine

The Metadirectory engine is the core server that implements the event management and policies of Identity Manager. The engine runs on the Java Virtual Machine in eDirectory.

1.1.4 Drivers

A driver implements a data sharing policy for a connected system. You control the actions of the driver using iManager to define the filters and the policy.

1.1.5 Driver Shim

A driver shim is the component of a driver that converts the XML-based Identity Manager command and event language (XDS) to the protocols and API calls needed to interact with a connected system. The shim is called to execute commands on the connected system after the Output Transformation runs. Commands are usually generated on the Subscriber channel but can be generated by command write-back on the Publisher channel.

The shim also generates events from the connected system for the Input Transformation policy. A driver shim can be implemented either in Java class or as a native Windows DLL file. The shim for Loopback Service driver is `com.novell.nds.dirxml.driver.loopback.LoopbackDriverShim`.

1.1.6 Remote Loader

A Remote Loader enables a driver shim to execute outside of the Metadirectory engine (perhaps remotely on a different machine). The Remote Loader is typically used when a requirement of the driver shim is not met by the Identity Manager server.

The Remote Loader is a service that executes the driver shim and passes information between the shim and the Metadirectory engine. When you use a Remote Loader, you install the driver shim on the server where the Remote Loader is running, not on the server where the Metadirectory engine is running. You can choose to use SSL to encrypt the connection between the Metadirectory engine and the Remote Loader. For more information, see the *Identity Manager 4.5 Remote Loader Guide*.

1.2 Key Driver Features

1.2.1 Entitlements

Entitlements make it easier to integrate Identity Manager with the Identity Manager User Application and Role-Based Services in eDirectory. The Loopback Service driver supports custom and administrator-defined entitlements with the use of a new entitlement package. This package contains the content that allows you to keep the Resource Catalog up-to-date with the user permissions stored in the Identity Vault, dynamically create an entitlement and dynamic resource for each permission type, and load the permission data as entitlement values into Identity Manager Role-Based Provisioning Module. The new functionality is called Permission Collection and Reconciliation service. It addresses the challenge of synchronizing changes made to the users in the Identity Vault with the Identity Manager Role-Based Provisioning Module. The Permission Collection and Reconciliation service allows the driver to automatically provision or deprovision these resources to Identity Manager identities based on attribute values consumed during standard Publication channel processing.

The Permission Collection and Reconciliation service automatically creates a dynamic group resource and manages user assignments (assign and revoke) in the Role-Based Provisioning Module for the Identity Vault groups. For example, if Alex is a new employee and you want to add him to a Security group, you can modify the Security group membership attribute using iManager. The Resource Administrator can also grant him access to the Security group by assigning him to this group resource in the User Application. This group assignment is immediately reflected in the Identity Vault. In addition, it allows you to migrate existing group memberships as resource assignments into the Role-Based Provisioning Module.

The Permission Collection and Reconciliation service also allows you to manage permissions of identities in the Role-Based Provisioning Module with the use of a CSV file. The driver creates dynamic resources for each of the permission types specified during driver creation. You can use these permission types to control the assignment of values to the user attributes. For example, if Printer is a permission type configured during driver configuration in Designer, the Loopback Service driver creates a dynamic resource, *Printer_LoopbackServiceDriver* for this permission type in the User Application. The Identity Vault attribute, `Printer Control`, that holds values for printers available to users, maps to Printer_LoopbackServiceDriver in the User Application. To grant users access to a particular printer using iManager, you need set a value for the `Printer Control` attribute for specific users. With this service enabled, this change immediately reflects on the *Printer_LoopbackServiceDriver* resource in the User Application. As a Resource Administrator, if you assign or revoke users from *Printer_LoopbackServiceDriver* in the User Application, this change immediately reflects in the Identity Vault.

CSV File Format

The CSV file must contain the Identity Vault permission information in a correct format so that the driver reads it correctly from the file. A separate CSV file must be maintained for every custom entitlement. For example, a CSV file that holds *Printer* entitlement details for employees represents this information in the following format:

```
Printer1, First Floor Printer1, Printer Access for Employees
```

where *Printer1* is the entitlement value, *First Floor Printer1* is the display name in the User Application for the entitlement value *Printer1*, and *Printer Access for Employees* is the description for the entitlement value. This description is displayed in the User Application.

You must place the CSV file on the same server as the driver. This file contains the values for Identity Vault entitlements.

The following packages contain the content necessary for Permission Collection and Reconciliation service:

- NOVLLBACKB_2.0.0 (Base Package)
- NOVLLBACKENT_2.0.0 (Entitlements Package)

The Permission Collection and Reconciliation service provides GCVs that you can use to control the flow of Identity Vault changes to the User Application. For more information, see Section A.2.1, “Entitlements,” on page 36.

Prerequisites

Before continuing, ensure that you go through the prerequisites needed for enabling this service. For general prerequisites, see “Prerequisites” in the “Understanding Permission Collection and Reconciliation Service ” in the *NetIQ Identity Manager Driver Administration Guide*. In addition to the general prerequisites, ensure that the Loopback Service driver version is 4.0.0.1.

Also, you need to set up administrative user accounts and configure a password policy for them. For more information, see “Setting Up Administrative User Accounts” and “Setting Up Administrative Passwords” in the *NetIQ Identity Manager Driver Administration Guide*.

To use the Permission Collection and Reconciliation service included in the Loopback Service driver, you can either create a new driver with the latest packages or upgrade packages on an existing driver. For more information about creating a driver, see Section 4.1, “Creating the Driver in Designer,” on page 21 or Section 3.3, “Adding Packages to an Existing Driver,” on page 19.

1.2.2 Password Synchronization Support

The Loopback Service driver does not synchronize passwords.

1.2.3 Data Synchronization Support

The Loopback Service driver synchronizes User and Group objects.

1.3 Default Driver Configuration

The Loopback Service driver is shipped with packages. You can create the driver in Designer. If your requirements for the driver are different from the default policies, you need to modify the default policies to do what you want.

1.3.1 Data Flow

Data flow between the Loopback Service driver and the Identity Vault is controlled by the filters, mappings, and policies that are in place for the Loopback Service driver.

The driver filter determines which classes and attributes are synchronized between the driver and the Identity Vault, and in which direction synchronization takes place.

2 Installing the Driver Files

By default, the Null Service and Loopback Service driver files are installed on the Metadirectory server at the same time as the Metadirectory engine. The installation program extends the Identity Vault's schema and installs the driver shim. It does not create the driver in the Identity Vault (see Chapter 3, "Creating a New Null Service Driver Object," on page 15 or Chapter 4, "Creating a New Loopback Service Driver," on page 21) or upgrade an existing driver's configuration (see Chapter 5, "Upgrading an Existing Driver," on page 29).

If you performed a custom installation and did not install the Null Service or the Loopback Service driver on the Metadirectory server, you have two options:

- Install the files on the Metadirectory server, using the instructions in "Installing the Identity Manager Engine, Drivers, and Plug-ins" in the *NetIQ Identity Manager Setup Guide*.
- Install the Remote Loader (required to run the driver on a non-Metadirectory server) and the driver files on a non-Metadirectory server where you want to run the driver. See "Installing the Identity Manager Engine, Drivers, and Plug-ins" in the *NetIQ Identity Manager Setup Guide*.

3 Creating a New Null Service Driver Object

After the Null Service driver files are installed on the server where you want to run the driver (see Chapter 2, “Installing the Driver Files,” on page 13), you can create the driver in the Identity Vault. You do so by importing the driver packages and then modifying the driver configuration to suit your environment.

- Section 3.1, “Creating the Driver Object in Designer,” on page 15
- Section 3.2, “Activating the Driver,” on page 18
- Section 3.3, “Adding Packages to an Existing Driver,” on page 19

3.1 Creating the Driver Object in Designer

To create the Null Service driver object, install the driver packages and then modify 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.

- Section 3.1.1, “Importing the Current Driver Packages,” on page 15
- Section 3.1.2, “Installing the Driver Packages,” on page 16
- Section 3.1.3, “Configuring the Driver Settings,” on page 17
- Section 3.1.4, “Configuring the Driver Policies,” on page 17
- Section 3.1.5, “Deploying the Driver,” on page 17
- Section 3.1.6, “Starting the Driver,” on page 18

NOTE: You should not create driver objects using the new Identity Manager 4.0 and later configuration files through iManager. This method of creating driver objects is no longer supported. To create drivers, you now need to use the new package management features provided in Designer.

3.1.1 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. Before creating a driver object in Designer, it is recommended to have the latest packages in the Package

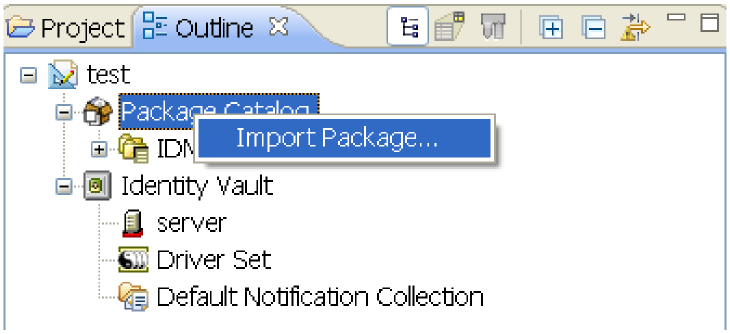
Catalog. Designer prompts you for importing the required packages when it creates the driver object. For more information on upgrading packages, see “Upgrading Installed Packages”in the *NetIQ Designer for Identity Manager Administration Guide*.

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

1. Open Designer.
2. In the toolbar, click *Help* > *Check for Package Updates*.
3. Click *OK* to update the packages

   or

   Click *OK* if the packages are up-to-date.
4. In the Outline view, right-click the Package Catalog.
5. Click *Import Package*.



6. Select any Null Service 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 Section 3.1.2, “Installing the Driver Packages,” on page 16.

3.1.2 Installing the Driver Packages

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

1. In Designer, open your project.
2. In the Modeler, right-click the driver set where you want to create the driver, then click *New* > *Driver*.
3. Select *Null Service Base*, then click *Next*.
4. On the Null Service page, specify a name for the driver, then click *Next*.
5. Review the summary of tasks that will be completed to create the driver, then click *Finish*.

6. After the driver packages are installed, if you want to change the configuration of the Role-Based Entitlement driver, continue to Section 3.1.3, “Configuring the Driver Settings,” on page 17.

   or

   If you do not want to change the configuration of the driver, continue to Section 3.1.5, “Deploying the Driver,” on page 17.

3.1.3 Configuring the Driver Settings

After you installed the driver packages, the Null Service driver will run. However, there are many configuration settings that you can use to customize and optimize the driver. The settings are divided into categories such as Driver Configuration, Engine Control Values, and Global Configuration Values (GCVs). The settings are described in Appendix A, “Driver Properties,” on page 33.

If you do not have the Driver Properties page displayed in Designer:

1. Open your project.
2. In the Modeler, right-click the driver icon or the driver line, then select *Properties*.
3. Make the changes you want, then continue to Section 3.1.4, “Configuring the Driver Policies,” on page 17.

3.1.4 Configuring the Driver Policies

The basic driver configuration does not include any policies. To have the driver perform any work, you need to create the appropriate policies. For information about creating policies, see the *NetIQ Identity Manager Policies in Designer* guide.

After you have created the appropriate policies, continue with Section 3.1.5, “Deploying the Driver,” on page 17.

3.1.5 Deploying the Driver

After a driver 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 5; 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 successful 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. Whatever rights that the driver needs to have on the server, the DriversUser object must have the same security rights.

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 8a for each object you want to exclude, then click *OK*.

8 Click *OK*.

3.1.6 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*.

For information about management tasks for the driver, see Chapter 6, "Managing the Driver," on page 31.

3.2 Activating the Driver

If you created the driver in a driver set where you have already activated the Metadirectory engine and service drivers, the driver inherits the activation. If you created the driver in a driver set that has not been activated, you must activate the driver within 90 days. Otherwise, the driver stops working.

If driver activation has expired, the following error message is displayed in the ndstrace window:

```
DirXML Log Event -------------------
Driver: \META-RHEL6\system\DriverSet\eDirDriver-BulkOperations
Channel: Subscriber
Status: Error
Message: Code(-9075) Shutting down because DirXML engine evaluation period
has expired. Activation is required for further use.
```

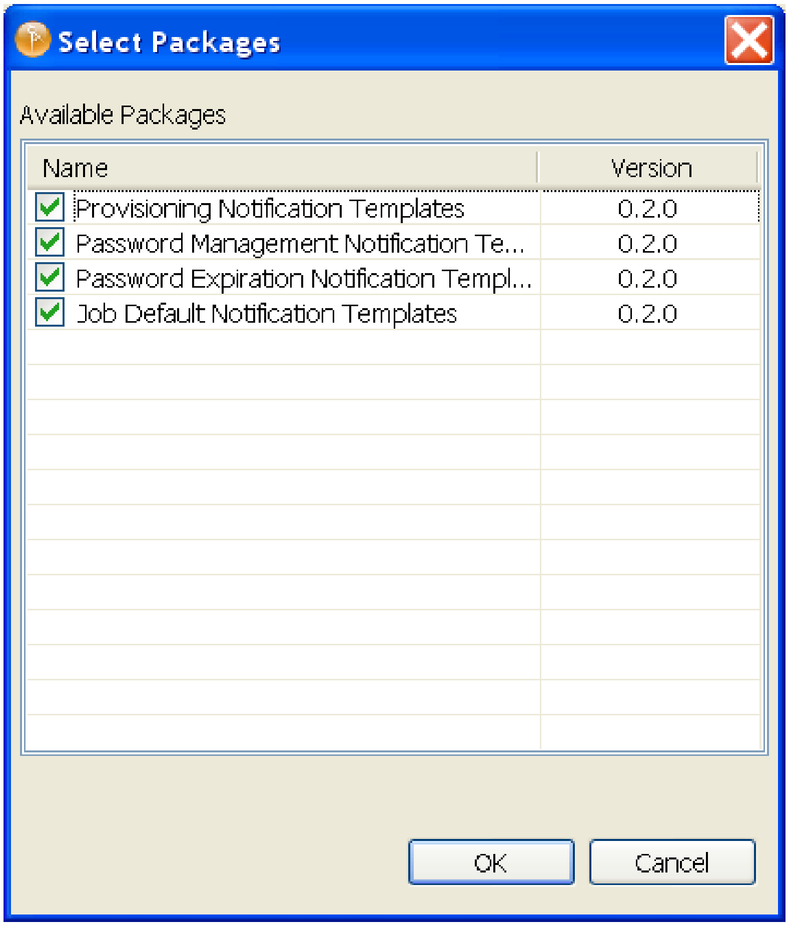
To use the driver, you must reactivate it.

For information on activation, refer to "Activating Identity Manager" in the *NetIQ Identity Manager Setup Guide*.

3.3 Adding Packages to an Existing Driver

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

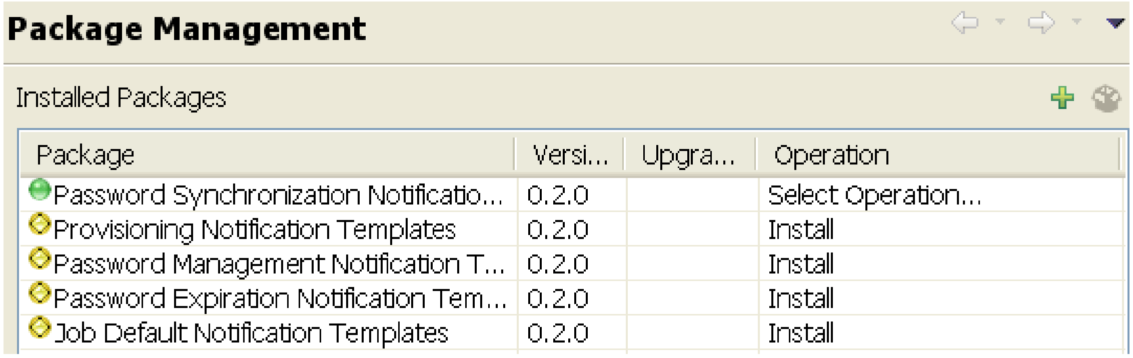
1. Right-click the driver, then click *Properties*.
2. Click *Packages*, then click the *Add Packages* icon ✚.
3. Select the packages to install. If the list is empty, there are no available packages to install.



Name	Version
☑ Provisioning Notification Templates	0.2.0
☑ Password Management Notification Te...	0.2.0
☑ Password Expiration Notification Templ...	0.2.0
☑ Job Default Notification Templates	0.2.0

4. (Optional) Deselect the *Show only applicable package versions* option, if you want to see all available packages for the driver, then click *OK*.

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



Package Management

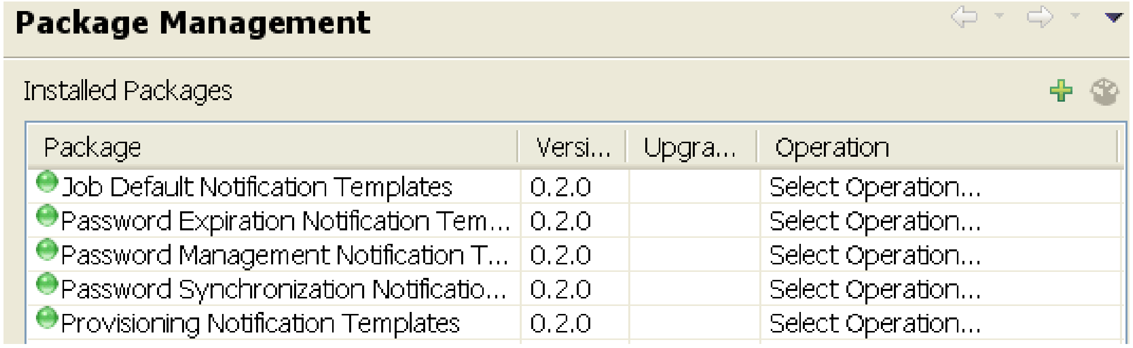
Installed Packages

Package	Versi...	Upgra...	Operation
● Password Synchronization Notificatio...	0.2.0		Select Operation...
◇ Provisioning Notification Templates	0.2.0		Install
◇ Password Management Notification T...	0.2.0		Install
◇ Password Expiration Notification Tem...	0.2.0		Install
◇ Job Default Notification Templates	0.2.0		Install

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

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

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



Package Management

Installed Packages

Package	Versi...	Upgra...	Operation
● Job Default Notification Templates	0.2.0		Select Operation...
● Password Expiration Notification Tem...	0.2.0		Select Operation...
● Password Management Notification T...	0.2.0		Select Operation...
● Password Synchronization Notificatio...	0.2.0		Select Operation...
● Provisioning Notification Templates	0.2.0		Select Operation...

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

4 Creating a New Loopback Service Driver

After the Loopback Service driver files are installed on the server where you want to run the driver (see Chapter 2, "Installing the Driver Files," on page 13), you can create the driver in the Identity Vault. You do so by importing the driver packages and then modifying the driver configuration to suit your environment.

- Section 4.1, "Creating the Driver in Designer," on page 21
- Section 4.2, "Activating the Driver," on page 26
- Section 4.3, "Adding Packages to an Existing Driver," on page 26
- Section 4.4, "Viewing Permission Collection and Reconciliation Service Configuration Objects," on page 27

4.1 Creating the Driver in Designer

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

- Section 4.1.1, "Importing the Current Driver Packages," on page 21
- Section 4.1.2, "Installing the Driver Packages," on page 22
- Section 4.1.3, "Configuring the Driver Settings," on page 24
- Section 4.1.4, "Configuring the Driver Policies," on page 25
- Section 4.1.5, "Deploying the Driver," on page 25
- Section 4.1.6, "Starting the Driver," on page 26

4.1.1 Importing the Current Driver Packages

You can update the driver packages at any time and store them in the Package Catalog. Packages are initially imported into the Package Catalog when you create a project, import a project, or convert a project. It is important to verify you have the latest packages imported into the Package Catalog before you install the driver.

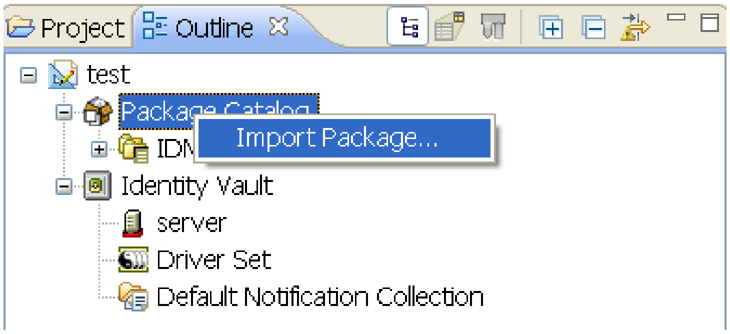
To verify you have the most recent version of the driver packages in the Package Catalog:

1. Open Designer.
2. In the toolbar, click *Help* > *Check for Package Updates*.
3. Click *OK* if there are no package updates

   or

   Click *OK* to import the package updates.
4. In the Outline view, right-click the Package Catalog.

5 Click *Import Package*.



6 Select any Loopback Service 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.

IMPORTANT: If you want the driver to support the Permission Collection and Reconciliation Service functionality, ensure you import the following packages to the driver:

- NOVLLBACKB_2.0.0 (Base Package)
- NOVLLBACKENT_2.0.0 (Entitlements Package)
- NOVLACOMSET_2.0.0 (Common Settings Advanced Edition Package)

For information about the Permission Collection and Reconciliation service, see "Understanding Permission Collection and Reconciliation Service " in the *NetIQ Identity Manager Driver Administration Guide*.

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 Section 3.1.2, "Installing the Driver Packages," on page 16.

4.1.2 Installing the Driver Packages

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

1 In Designer, open your project.

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

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

4 Select the optional features to install for the Loopback Service driver.

There is only one option. It is selected by default.

- **Loopback Entitlements:** This package contains policies that allow Identity Manager to consume CSV files containing Identity Vault permission information, dynamically create an entitlement and dynamic resource for each permission type, and load the permission data as entitlement values into Identity Manager Role-Based Provisioning Module. This package also contains GCVs to control the resource mapping. Select this package if you want the driver to support custom and administrator-defined entitlements. For more information about the Permission Collection and Reconciliation Service functionality, see "Understanding Permission Collection and Reconciliation Service " in the *NetIQ Identity Manager Entitlements Guide*.

NOTE: If you are enabling Permission Collection and Reconciliation service, ensure that you upgrade the Managed System Gateway driver version to 4.0.0.6.

5. Click *Next*.
6. (Conditional) If there are package dependencies for the packages you selected to install, you must install them to install the selected package. Click *OK* to install the package dependencies listed.
7. (Conditional) If not already configured, fill in the following fields on the Common Settings Advanced Edition page, then click *Next*:

   NOTE: This page is only displayed if you installed the Common Settings Advanced Edition package.

   - **User Application Provisioning Services URL:** Specify the User Application Identity

     Manager Provisioning URL.
   - **User Application Provisioning Services Administrator:** Specify the DN of the User Application Administrator user. This user should have the rights for creating and assigning resources. For more information, see "Setting Up Administrative User Accounts" in the *NetIQ Identity Manager Driver Administration Guide*.
8. On the Install Loopback page, specify a name for the driver, then click *Next*.
9. (Conditional) On the Entitlements Name to CSV File Mappings page, click the *Add Name to File Mapping* ✚ icon to populate the page with the entitlement configuration options.

   Identity Manager uses the CSV file to map Loopback entitlements into corresponding resources in the Identity Manager catalog.

   NOTE: This page is only displayed if you selected to install the Entitlements package.

   - **Entitlement Name:** Specify a descriptive name for the entitlement to map it to the CSV file that contains entitlement details.

     Entitlement Name is the name of the entitlement. For example, you can define an entitlement called *Printer*.

     This parameter is used to create a resource in the User Application.
   - **Entitlement Assignment Attribute:** Specify a descriptive name for the assignment attribute for an entitlement.

     Entitlement Assignment Attribute holds the entitlement values in the Identity Vault. For example, this parameter can hold an attribute called *Printer Control*.

     You must add this parameter to *Field Names* in the Driver Parameters page or modify it in driver settings after creating the driver.
   - **CSV File:** Specify the location of the CSV file. This file must be located on the same server as the driver. This file contains the values for Identity Vault entitlements.
   - **Multi-valued?:** Set the value of this parameter to *True* if you want to assign resources and entitlements multiple times with different values to the same user. Otherwise, set it to *False*.
10. Click *Next*.

11. Review the settings and click *Finish* to create the driver.
12. After the driver is created, if you want to change the configuration settings of the driver, continue to Section 4.1.3, "Configuring the Driver Settings," on page 24. If you do not want to change the configuration of the driver, continue to Section 4.1.5, "Deploying the Driver," on page 25.

4.1.3 Configuring the Driver Settings

After you have installed the driver packages, the Loopback Service driver will run. However, there are many configuration settings that you can use to customize and optimize the driver. The settings are divided into categories such as Driver Configuration, Engine Control Values, and Global Configuration Values (GCVs). The settings are described in Appendix A, "Driver Properties," on page 33.

To access the Driver Properties page in Designer:

1. Open your project.
2. In the Modeler, right-click the driver icon or the driver line, then select *Properties*.
3. (Conditional) Click *GCVs* > *Entitlements* and review the following settings:

   NOTE: These settings are only displayed if you installed the Entitlements package.

   - **Enable Permission Collection and Reconciliation:** Select the value of this parameter to *True* for allowing permission collection and entitlement assignment. By default it is set to *False*, which allows the driver to override any other conditions to reconcile custom entitlements.
   - **Enable Permission Reconciliation for Group Entitlement:** Ensure the value of this parameter is set to *Yes* to enable the driver to assign group entitlements. By default, the value is set to *Yes*.
   - **Enable Permission Reconciliation for all Custom Entitlements:** If the value of this parameter is set to *No*, it allows you to select specific custom entitlements for reconciling them. By default, it is set to *Yes*, which allows reconciling of all custom entitlements.
   - **Add Custom Entitlements for Reconciliation:** This parameter is presented if the value of *Enable Permission Reconciliation for all Custom Entitlements* is set to *No*.

     Click the *Add* + icon to add custom entitlements you want to selectively reconcile and specify *Assignment Attribute Name* for them.

   NOTE: Ensure that *Entitlement Assignment Attributes* values are added to the *Field Names* parameter in the driver configuration if they are not added initially during driver creation.
4. Click *Apply*.
5. Modify any other settings as necessary.
6. Deploy the driver to the Identity Vault. Proceed to Section 4.1.5, "Deploying the Driver," on page 25.

4.1.4 Configuring the Driver Policies

The basic driver configuration does not include any policies. To have the driver perform any work, you need to create the appropriate policies. For information about creating policies, see the *NetIQ Identity Manager Policies in Designer* guide.

After you have created the appropriate policies, continue to Section 4.1.5, “Deploying the Driver,” on page 25.

4.1.5 Deploying the Driver

After a driver 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 5; otherwise, specify the follow information:
    - **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. Click *OK*.
5. Read the deployment summary, then click *Deploy*.
6. Read the successful message, then click *OK*.
7. Click *Define Security Equivalence* to assign rights to the driver.

    The driver requires rights to objects within the Identity Vault and to the input and output directories on the server. 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. For more information about defining a Security Equivalent User in objects for drivers in the Identity Vault, see “Establishing a Security Equivalent User” in the *NetIQ Identity Manager Security Guide*.

    For receiving events from the Identity Vault, ensure that the driver’s Security Equals DN has the following rights in the Identity Vault:

    - **Entry:** Browse rights.
    - **Attributes:** Read rights.

    7a Click *Add*, then browse to and select the object with the correct rights.

    7b Click *OK* twice.
8. 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.

    8a Click *Add*, then browse to and select the user object you want to exclude.

    8b Click *OK*.

    8c Repeat Step 8a and Step 8b for each object you want to exclude, then click *OK*.
9. Click *OK*.

4.1.6 Starting the Driver

If you configured the driver with the Permission Collection and Reconciliation service, ensure the driver meets the following requirements before it is started for the first time:

- The Entitlement value CSV files are available in the locations specified during driver configuration. You can check the location you specified by examining the *PermissionNameToFile* mapping table under the driver in the Outline View of Designer.
- The driver administrator and the User Application Resource Administrator are added to a Password Policy.

To start the driver, in the Modeler, right-click the driver icon or the driver line, then select *Live > Start Driver*.

For information about management tasks with the driver, see Chapter 6, "Managing the Driver," on page 31.

4.2 Activating the Driver

If you created the driver in a driver set where you already activated the Metadirectory engine and service drivers, the driver inherits the activation. If you created the driver in a driver set that has not been activated, you must activate the driver within 90 days. Otherwise, the driver stops working.

For information on activation, refer to "Activating Identity Manager" in the *NetIQ Identity Manager Setup Guide*.

4.3 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 Loopback 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.
3. Click the *Add Packages* icon.
4. Select the packages to install.

   NOTE: The Loopback Entitlements package contains the content for Permission Collection and Reconciliation service. Select this package to enable this service.
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*.
6. This option is only displayed on drivers. By default, only the packages that can be installed on the selected driver are displayed.
7. Click *Apply* to install all of the packages listed with the Install operation.
8. (Conditional) Fill in the fields with appropriate information to install the package you selected for the driver, then click *Next*.
9. Read the summary of the installation, then click *Finish*.

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

11 Modify the driver configuration settings. See Section 4.1.3, “Configuring the Driver Settings,” on page 24.

12 Deploy the driver. See Section 4.1.5, “Deploying the Driver,” on page 25.

13 Start the driver. See Section 4.1.6, “Starting the Driver,” on page 26.

14 (Conditional) Review the newly created or modified configuration objects. See Section 4.4, “Viewing Permission Collection and Reconciliation Service Configuration Objects,” on page 27.

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

4.4 Viewing Permission Collection and Reconciliation Service Configuration Objects

NOTE: This section contains information about verifying the objects that are either newly created or modified as part of enabling the Permission Collection and Reconciliation service. If this service is not enabled for the driver, skip this section.

After the driver is deployed and configured with the new Permission Collection and Reconciliation service, verify that the driver correctly creates and updates the entitlements information in the Identity Vault.

Complete the following steps:

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

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

2a (Conditional) 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.

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

3 Click the Loopback Service driver icon.

4 Click the *Jobs* tab. The *PermissionOnboarding* job is displayed in the Jobs page. For more information, see “PermissionOnboarding Job” in the *NetIQ Identity Manager Driver Administration Guide*.

5 Click *Advanced* > *Mapping Tables*. The DNs of the Entitlement objects are displayed in the Mapping Table page based on the InitEntitlementResourceObjects policy and data from the configuration objects. For more information, see “Mapping Tables” in the *NetIQ Identity Manager Driver Administration Guide*.

6 Click *Global Config Values* to display the driver set GCV page.

This page contains two sets of GCVs that are consumed by the drivers in the driver set. Ensure that you configure them for the driver set containing the drivers for Permission Collection and Reconciliation service.

- **NOVLCOMSET:** This GCV object contains the following:
  - **User Container:** Specifies the Identity Vault container where the users are added, if they don’t already exist in the Identity Vault. This value is the default value for all drivers in the driver set.
  - **Group Container:** Specifies the Identity Vault container where the groups are added, if they don’t already exist in the Identity Vault. This value is the default value for all drivers in the driver set.

- **NOVLACOMSET:** This GCV object contains the following:
    - **User Application Provisioning Services URL:** Specifies the User Application Identity Manager Provisioning URL.
    - **User Application Provisioning Administrator:** Specifies the DN of the provisioning administrator. This user should have the rights for creating and assigning resources.

5 Upgrading an Existing Driver

The following sections provide information to help you upgrade an existing driver to version 4.0.1:

5.1 Supported Upgrade Paths

You can upgrade from any 3.*x* version of the Null Service driver or Loopback Service driver. Upgrading a pre-3.*x* version of the driver directly to version 4.0.2 is not supported.

5.2 What's New

Version 4.0.2 of the driver does not include any new features.

From 4.0 version of the driver, driver content is delivered in packages instead of through a driver configuration file.

5.3 Upgrade Procedure

The process for upgrading the Null or Loopback Service driver is the same as for other Identity Manager drivers. For detailed instructions, see "Upgrading the Identity Manager Drivers" in the *NetIQ Identity Manager Setup Guide*.

6 Managing the Driver

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

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

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

A Driver Properties

This section provides information about the Driver Configuration and Global Configuration Values properties for the Null Service driver and the Loopback Service driver. These are the only unique properties for drivers. All other driver properties (Named Password, Engine Control Values, Log Level, and so forth) are common to all drivers. Refer to "Driver Properties" in the *Client Login Extension 3.7.2 Administration Guide* for information about the common properties.

The properties information is presented from the viewpoint of iManager. If a field is different in Designer, it is marked with a Designer icon.

- Section A.1, "Driver Configuration," on page 33
- Section A.2, "Global Configuration Values," on page 36

A.1 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 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.

5 Click *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.*

The Driver Configuration options are divided into the following sections:

- Section A.1.1, "Driver Module," on page 34
- Section A.1.2, "Driver Object Password," on page 34
- Section A.1.3, "Authentication," on page 34
- Section A.1.4, "Startup Option," on page 35
- Section A.1.5, "Driver Parameters," on page 35

- Section A.1.6, “ECMAScript,” on page 35
- Section A.1.7, “Global Configurations,” on page 35

A.1.1 Driver Module

The Driver Module section lets you change the driver from running locally to running remotely or the reverse.

Option	Description

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 Null Service driver is:
	`com.novell.nds.dirxml.driver.nulldriver.NullDriverShim`
	The name of the Java class for the Loopback Service driver is:
	`com.novell.nds.dirxml.driver.loopback.LoopbackDriverShim`

Native	Used to specify the name of the `.dll` file that is instantiated for the application shim component of the driver. If this option is selected, the driver is running locally.
Connect to Remote Loader	This setting does not apply to the Null Service driver or the Loopback Service driver. You cannot use these drivers with the Remote Loader.

A.1.2 Driver Object Password

Option	Description
Driver Object Password	This setting does not apply to the Null Service driver or the Loopback Service driver.

A.1.3 Authentication

The Authentication section stores the information required to authenticate to the connected system and to the Remote Loader. The Null Service driver and Loopback Service driver function only against the Identity Vault and cannot use the Remote Loader. Therefore, the authentication settings do not apply.

The only setting that applies to the drivers is the cache setting.

Option	Description
Driver Cache Limit (kilobytes) or *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.

A.1.4 Startup Option

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

Option	Description
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 applies only if the driver is deployed and was previously disabled. If this is not selected, the driver re-synchronizes the next time it is started.

A.1.5 Driver Parameters

The Driver Parameters section lets you configure the driver-specific parameters.

Parameter	Description
Driver parameters for server	Displays or specifies the server name or IP address of the server whose driver parameters you want to modify.
Edit XML	Opens an editor so that you can edit the driver’s configuration file.
Driver Options	There are no general driver options.
Subscriber Options	There are no general Subscriber channel options.
Publisher Options	There are no Publisher channel options.
Publisher Heartbeat Interval	Configures the driver to send a periodic status message on the Publisher channel when there has been no Publisher traffic for the given number of minutes. The default is every minute.

A.1.6 ECMAScript

Enables you to add ECMAScript resource files. The resources extend the driver’s functionality when Identity Manager starts the driver.

A.1.7 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.

A.2 Global Configuration Values

There are no predefined global configuration values (GCVs) specific to the Loopback Service driver and Null Service driver. As with all drivers, you can add GCVs that you need.

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 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.
5. Click *Global Config Values*.

In Designer:

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

The global configuration values are organized as follows:

- Section A.2.1, "Entitlements," on page 36

A.2.1 Entitlements

Permission Collection and Reconciliation Service

If you installed the Entitlements package for using the Permission Collection and Reconciliation service, iManager and Designer display the following options. For information about the Permission Collection and Reconciliation service, see "Understanding Permission Collection and Reconciliation Service " in the *NetIQ Identity Manager Driver Administration Guide*.

- **Enable Permission Collection and Reconciliation:** Set the value of this parameter to *true* for resource onboarding and entitlement assignment. By default, the value is set to *false*, which allows the driver to override any other conditions to onboard custom entitlements.
- **Enable Permission Reconciliation for Group Entitlement:** Ensure the value of this parameter is set to *Yes* to enable the driver to assign group entitlements. By default, the value is set to *Yes*.
- **Enable Permission Reconciliation for all Custom Entitlements:** If the value of this parameter is set to *No*, it allows you to select specific custom entitlements for reconciling them. By default, it is set to *Yes*, which allows reconciling of all custom entitlements.
- **Add Custom Entitlements for Reconciliation:** This parameter is presented if the value of *Enable Permission Reconciliation for all Custom Entitlements* is set to *No*.

  Click the *Add* ✚ icon to add custom entitlements you want to selectively reconcile and specify *Assignment Attribute Name* for them.

Advanced Settings

Show Advanced Options: Select *show* to display the advanced configuration options for the driver.

Role Mapping

The Role Mapping Administrator allows you to map business roles with IT roles.

- **Enable role mapping:** Select *Yes* to make this driver visible to the Role Mapping Administrator.
- **Allow mapping of groups:** Select *Yes* if you want to allow mapping of groups in the Role Mapping Administrator.

Resource Mapping

The Roles Based Provisioning Module allows you to map resources to users. For more information, see the *NetIQ User Application: User Guide*.

- **Enables resource mapping:** Select *Yes* to make this driver visible to the Roles Based Provisioning Module.
- **Allow mapping of groups:** Select *Yes* if you want to allow mapping of groups in the Roles Based Provisioning Module.