



# NetIQ® Identity Manager Entitlements Service Driver Implementation Guide

October 2019

## **Legal Notice**

For information about NetIQ legal notices, disclaimers, warranties, export and other use restrictions, U.S. Government restricted rights, patent policy, and FIPS compliance, see <https://www.netiq.com/company/legal/>.

**Copyright (C) 2019 NetIQ Corporation. All rights reserved.**

---

# Contents

<b>About this Book and the Library</b>	<b>5</b>
<b>About NetIQ Corporation</b>	<b>7</b>
<b>1 Understanding the Entitlement Service Driver</b>	<b>9</b>
How the Entitlements Service Driver Works . . . . .	9
Role-Based Entitlements Versus Other Entitlements . . . . .	11
Using Multiple Entitlements Service Drivers . . . . .	11
<b>2 Implementation Checklist</b>	<b>13</b>
<b>3 Installing the Driver Files</b>	<b>15</b>
<b>4 Creating a New Driver Object</b>	<b>17</b>
Creating the Driver Object in Designer . . . . .	17
Importing the Current Driver Packages . . . . .	17
Installing the Driver Packages . . . . .	18
Configuring the Driver Settings . . . . .	19
Deploying the Driver Object . . . . .	19
Starting the Driver . . . . .	20
Activating the Driver . . . . .	20
Adding Packages to an Existing Driver . . . . .	20
<b>5 Upgrading an Existing Driver</b>	<b>23</b>
Supported Upgrade Paths . . . . .	23
What's New in Version 4.0.0 . . . . .	23
Upgrading the Driver . . . . .	23
<b>6 Creating Entitlement Policies</b>	<b>25</b>
<b>7 Controlling How Entitlements Are Granted or Revoked</b>	<b>29</b>
<b>8 Managing the Driver</b>	<b>31</b>
<b>9 Troubleshooting Role-Based Entitlements</b>	<b>33</b>
General Troubleshooting Issues . . . . .	33
Conflict Resolution between Entitlement Policies . . . . .	34
Conflict Overview . . . . .	34
Changing the Conflict Resolution Method for an Individual Entitlement . . . . .	35
Prioritizing Entitlement Policies . . . . .	36

<b>A Driver Properties</b>	<b>37</b>
Driver Configuration .....	37
Driver Module .....	37
Driver Object Password (Identity Console Only) .....	38
Authentication .....	38
Startup Option .....	38
Driver Parameters .....	38
ECMAScript .....	39
Global Configurations .....	39
Global Configuration Values .....	39

# About this Book and the Library

The *Identity Manager Entitlements Service Driver Implementation Guide* explains how to install and configure the Identity Manager Entitlements Service Driver.

## Intended Audience

This book provides information for NetIQ eDirectory and Identity Manager administrators who are using the Entitlements Service driver to implement role-based entitlements.

## Other Information in the Library

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

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



# About NetIQ Corporation

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

## Our Viewpoint

### **Adapting to change and managing complexity and risk are nothing new**

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

### **Enabling critical business services, better and faster**

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

## Our Philosophy

### **Selling intelligent solutions, not just software**

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

### **Driving your success is our passion**

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

## Our Solutions

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

## Contacting Sales Support

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

<b>Worldwide:</b>	<a href="http://www.netiq.com/about_netiq/officelocations.asp">www.netiq.com/about_netiq/officelocations.asp</a>
<b>United States and Canada:</b>	1-888-323-6768
<b>Email:</b>	<a href="mailto:info@netiq.com">info@netiq.com</a>
<b>Web Site:</b>	<a href="http://www.netiq.com">www.netiq.com</a>

## Contacting Technical Support

For specific product issues, contact our Technical Support team.

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

## Contacting Documentation Support

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

## Contacting the Online User Community

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



# 1 Understanding the Entitlement Service Driver

The following overview assumes that you understand entitlements (as explained in the “[How Entitlements Work](#)” in the *NetIQ Identity Manager Entitlements Guide*) and have created the entitlements you want to manage through the Entitlements Service driver.

The Entitlements Service driver is one of three *entitlement agents* that you can use to grant entitlements, or permission slips, to users. The other two entitlement agents are the role-based provisioning component (see “[Role-Based Entitlements:](#)” in the *NetIQ Identity Manager Entitlements Guide*) and workflow-based provisioning component in the User Application (see “[User Application Workflow-Based Provisioning:](#)” in the *NetIQ Identity Manager Entitlements Guide*).

---

**IMPORTANT:** NetIQ recommends you to use User Application as the Roles-Based Entitlement granting authority instead of using the Entitlements Service driver. The Entitlement Service driver is not intended to be a roles service and is supported only as an entitlement granting authority.

---

Entitlements Service Driver supports legacy entitlement. It does not support the Identity Manager 4.0 entitlement format.

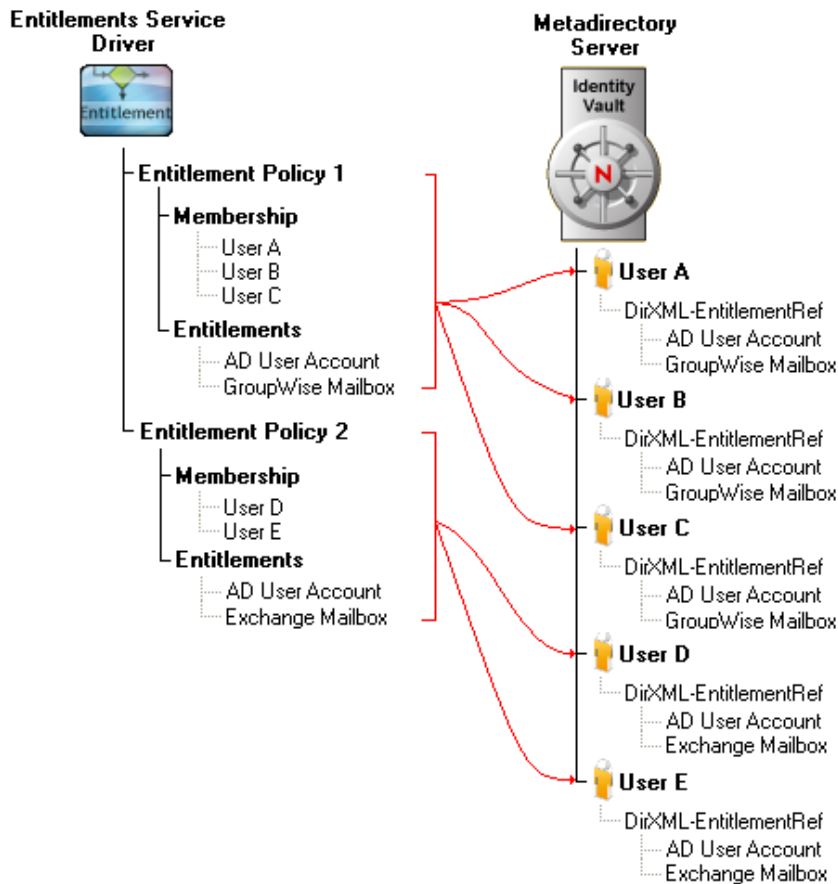
The following sections provide information to help you understand the Entitlements Service driver:

- ♦ “[How the Entitlements Service Driver Works](#)” on page 9
- ♦ “[Role-Based Entitlements Versus Other Entitlements](#)” on page 11
- ♦ “[Using Multiple Entitlements Service Drivers](#)” on page 11

## How the Entitlements Service Driver Works

The Entitlements Service driver grants entitlements to and revokes entitlements from users, as shown in [Figure 1-1](#).

Figure 1-1 Entitlements Service Driver Process



The driver implements entitlements through the use of entitlement policies. An entitlement policy contains the following:

- ♦ **Membership:** The list of users assigned to a policy. A user can be dynamically assigned to a policy when he or she meets the criteria for the policy, or the user can be statically (manually) assigned to the policy. In [Figure 1-1](#), User A, User B, and User C are all members of Entitlement Policy 1. User D and User E are members of Entitlement Policy 2.
- ♦ **Entitlements:** The list of entitlements associated with the policy. Users assigned to the policy receive all of the entitlements associated with the policy. If the user is removed from the policy, he or she loses all entitlements associated with the policy. In [Figure 1-1](#), the Entitlements Service driver has granted the AD User Account entitlement and GroupWise Mailbox entitlement to User A, User B, and User C. Likewise, the driver has granted the AD User Account entitlement and Exchange Mailbox entitlement to User D and User E.

The Entitlements Service driver uses the following basic process to grant entitlements to and revoke entitlements from users:

1. The driver evaluates the users within its defined scope to see if they meet the criteria established for membership in a policy. This occurs whenever:
  - ♦ Any criteria attribute used for determining membership in an entitlement policy is modified.
  - ♦ A user is moved.

- ◆ A user is renamed.
  - ◆ You manually initiate a reevaluation of a policy's membership.
2. The driver updates the DirXML-EntitlementRef attribute of any user whose entitlements have changed. This includes granting entitlements if the user was added to an entitlement policy or revoking entitlements if the user was removed from a policy.
  3. After the DirXML-EntitlementRef attribute for a user is updated, the Entitlements Service driver's job is finished. For the entitlement to be implemented, the entitlement must be defined on the appropriate driver and the driver's policies must include the actions required to enforce the entitlement. For information about creating entitlements and the policies to support them, see the [NetIQ Identity Manager Entitlements Guide](#).

## Role-Based Entitlements Versus Other Entitlements

Entitlements managed through the Entitlements Service driver are called “role-based entitlements”, or RBEs, because they are granted to users who are members of, or have a role in, an entitlement policy. Only the Entitlements Service driver uses role-based entitlements and entitlement policies. The two other entitlement agents (roles based provisioning and workflow-based provisioning through the User Application) use their own methods for assigning entitlements to users.

The role-based entitlement functionality in Identity Console lets you manage the entitlement policies used by the Entitlements Service driver.

## Using Multiple Entitlements Service Drivers

If your Identity Manager system includes multiple driver sets and you want to use role-based entitlements with each driver set, you must create an Entitlements Service driver in each driver set. In addition, the Entitlements Service driver can manage only those User objects that are in a master or read/write replica on the Identity Manager server where the Entitlements Service driver is located.

If necessary, you can run multiple Entitlements Service drivers in the same driver set. However, you must make sure that the scope of users managed by each of the drivers does not overlap. For example, entitlements for User A should not be managed by two different Entitlement Service drivers.

To grant entitlements to users through one or more Entitlements Service drivers in your Identity Manager system, ensure that all the replicas of the user objects and the Root of the tree reside on the same server.



# 2 Implementation Checklist

Use the following checklist to ensure that you complete all of the tasks required to set up and use the Entitlements Service driver.

---

Task	Details
<input type="checkbox"/> Create the entitlements you want to manage through the Entitlements Service driver	<p>The entitlements, and the policies required to implement them, must be created for the appropriate drivers. For example, if you want an Active Directory User Account entitlement, the entitlement must be created on the Active Directory driver and the driver's policies must include the actions required to grant and revoke the user account.</p> <p>For instructions, see the <a href="#">NetIQ Identity Manager Entitlements Guide</a>.</p>
<input type="checkbox"/> Create a new Entitlements Service driver or Upgrade an existing Entitlements Service driver to the new version	<p>By default, the Entitlements Service driver files (driver shim and configuration file) are copied to the Identity Manager server when the Identity Manager engine is installed. You need to use the configuration file to create a driver in each driver set where you want to use role-based entitlements. For instructions, see the <a href="#">NetIQ Identity Manager Entitlements Guide</a>.</p> <p>If you have an existing driver to upgrade, see <a href="#">Chapter 5, "Upgrading an Existing Driver,"</a> on page 23.</p>
<input type="checkbox"/> Create entitlement policies	<p>The Entitlements Service driver uses entitlement policies to grant entitlements to and revoke entitlements from users.</p> <p>For instructions, see <a href="#">Chapter 6, "Creating Entitlement Policies,"</a> on page 25.</p>

---



# 3 Installing the Driver Files

By default, the Entitlements Service driver files are installed on the Identity Manager server at the same time as the Identity Manager engine. No other installation configurations are supported; you cannot use the Remote Loader to run the Entitlements Service driver.

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 4, "Creating a New Driver Object,"](#) on page 17) or upgrade an existing driver's configuration (see [Chapter 5, "Upgrading an Existing Driver,"](#) on page 23).





# 1 Creating a New Driver Object

After the Entitlement Service driver files are installed on the server where you want to run the driver (see [Chapter 3, “Installing the Driver Files,” on page 15](#)), you can create the driver object in the Identity Vault. You do so by importing the driver packages and then modifying the driver configuration to suit your environment.

- ♦ [“Creating the Driver Object in Designer” on page 17](#)
- ♦ [“Activating the Driver” on page 20](#)
- ♦ [“Adding Packages to an Existing Driver” on page 20](#)

## Creating the Driver Object in Designer

To create the Entitlements Service driver, 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.

- ♦ [“Importing the Current Driver Packages” on page 17](#)
- ♦ [“Installing the Driver Packages” on page 18](#)
- ♦ [“Configuring the Driver Settings” on page 19](#)
- ♦ [“Deploying the Driver Object” on page 19](#)
- ♦ [“Starting the Driver” on page 20](#)

---

**NOTE:** To create drivers, you need to use the new package management features provided in Designer. This method of creating driver objects is not supported in Identity Console.

---

## Importing the Current Driver Packages

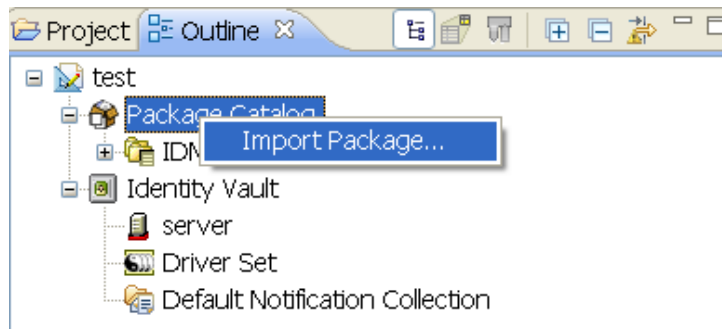
The driver packages contain the items required to create a driver, such as policies, entitlements, filters, and Schema Mapping policies. These packages are only available in Designer. You can upgrade any package that is installed if there is a newer version of the package available. Before creating a driver object in Designer, it is recommended to have all the required packages already imported in the Package Catalog of Designer. 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 Role-Based Entitlement 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 18](#).

## 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 **Role-Based Entitlements (RBE) Base**, then click **Next**.
- 4 On the Role-Based Entitlements 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 [“Configuring the Driver Settings” on page 19](#).  
or  
If you do not need to change the configuration, continue with [“Deploying the Driver Object” on page 19](#).

## Configuring the Driver Settings


After you import the driver configuration file, the Role-Based Entitlements 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 37.

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 click **OK**.
- 4 Continue with [“Deploying the Driver Object”](#) on page 19.

## 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 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.

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

**7b** Click **OK** twice.

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*.

- 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.
  - 8d Click **OK**.
- 9 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**.

For information about management tasks for the driver, see [Chapter 8, "Managing the Driver,"](#) on [page 31](#).


## Activating the Driver

The Identity Manager driver for Entitlements Service does not need a separate activation. If you create the driver in a driver set where you have already activated the Identity Manager server and service drivers, the driver inherits the activation from the driver set.

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

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

This option is only displayed on drivers. By default, only the packages that can be installed on the selected driver are displayed.

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

**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.



# 5 Upgrading an Existing Driver

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

- ♦ “Supported Upgrade Paths” on page 23
- ♦ “What’s New in Version 4.0.0” on page 23
- ♦ “Upgrading the Driver” on page 23

## Supported Upgrade Paths

You can upgrade from any 3.x version of the Entitlements Service driver. Upgrading a pre-3.x version of the driver directly to version 4.0.0 is not supported.

## What’s New in Version 4.0.0

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

## Upgrading the Driver

There is no separate procedure for upgrading an Entitlements Service driver shim. The driver shim is upgraded with a new version of Identity Manager engine.

To upgrade the installed packages for the driver, perform the following actions in Designer:

- 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 more information about creating custom packages, see [Developing Packages](#) in the *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 the *NetIQ Designer for Identity Manager Administration Guide*.



# 6 Creating Entitlement Policies

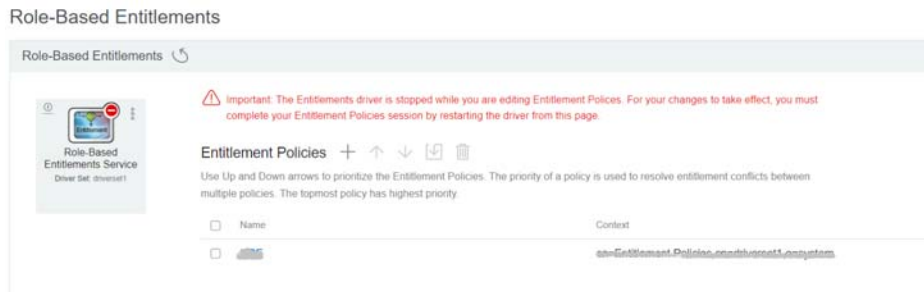
The Entitlements Service driver implements entitlements through the use of entitlement policies. An entitlement policy contains the following:

- ♦ **Membership:** The list of users assigned to the policy. A user can be dynamically assigned to the policy when he or she meets the criteria for the policy, or the user can be statically (manually) assigned to the policy.
- ♦ **Entitlements:** The list of entitlements associated with the policy. Users assigned to the policy receive all of the entitlements associated with the policy. If the user is removed from the policy, he or she loses all entitlements associated with the policy.

To create an entitlement policy:

- 1 Log in to Identity Console.
- 2 In the **IDM Administration**, click **Role-Based Entitlements**.
- 3 In the **Select driver set** field, select the driver set where you want to create the entitlement policy.

This list displays all entitlement policies that have been created for the driver set. If you are using role-based entitlements for the first time, no policies are listed.



- 4 Click **+** to launch the Entitlement Policy Wizard.
- 5 On the Step 1 of 6: Name and describe the Entitlement Policy page, fill in the fields:
  - Entitlement Policy Name:** Provide a name that indicates the purpose of the entitlement. The name must be unique within the driver set and cannot include more than 64 characters.
  - Description:** Provide any additional information you want to identify the policy.Click **Create**.
- 6 On the Step 2 of 6: Define Dynamic Membership page, fill in the fields:

Dynamic membership lets you define which users should be members of the entitlement policy by specifying criteria and specifying where in the tree to search for users that meet the criteria. If a user meets the criteria you specify, the policy's entitlements are automatically applied to the user. If the user's information changes and no longer meets the criteria, the entitlements are revoked without any manual intervention.

**Search Identity:** Specify an object that has the rights that you want to be used when querying for Dynamic Membership. This field defaults to the object you logged in as, but you can change it to an object with the appropriate rights.

For example, if you log in as the administrator, there might be parts of the tree that you have rights to, but you don't want them included in the query for the dynamic list of members.

You could use this field to specify the Driver Set object, making sure that the Driver Set has the appropriate rights. Or, you could create a User object specifically for use with entitlement policies, and assign it the rights you want the query to use.

**Begin Search at (Base DN):** Specify the base container where you want the user search to begin.

**Scope of Search:** Specify whether you want to search the base container and all of its subcontainers (**This container and its subcontainers**) or only the base container (**This container only**).

For the entitlement policy to evaluate users in the containers you specify, the users must be in a read/write or master replica on the Identity Manager server that is running the Entitlements Service driver.

**Criteria:** Specify the criteria that determine which users are members of the policy. The criteria are organized into criteria groups. Each group can contain one or more criteria. You click the **+** icon to add criterion to a group. You can also click **+** near **Criteria Group 1** to create additional groups.

By default, the criteria include all User class objects (and objects of classes derived from the User class) within the search scope.

If you create a new object class derived from User, an existing entitlement policy does not recognize that class until you make a modification to the entitlement policy. This prevents users of a new class from being granted entitlements unintentionally. When any modification is made to the entitlement policy, the list of user-derived classes for that policy is updated.

- 7 After you have added the criteria you want, click **Test Filter** to view the list of users who meet the criteria.


- 8 On the Step 3 of 6: Define Static Members page, fill in the fields:

Static membership lets you include users who don't meet the dynamic membership criteria or exclude users who meet the criteria but should not be members of the policy.

**Include Members:** Type the DN of a user you want to include, or click **+** to browse for and select the user, then press Enter to add the user to the inclusion list. To remove a user from the inclusion list, select the user and press Delete. To edit a user name, double-click the user.


**Exclude Members:** Type the DN of a user you want to exclude, or click **+** to browse for and select the user, then press Enter to add the user to the exclusion list. To remove a user from the exclusion list, select the user and press Delete. To edit a user name, double-click the user.

9 On the Step 4 of 6: Select Entitlements on the Connected Systems to Grant to Users page, add the entitlements you want associated with the policy:

9a Click  to display a list of drivers with entitlements.

9b Select the driver with the entitlement you want to add, then click **Add** to display a list of the driver's entitlements.


9c Select the entitlement you want to add, then click **Add**.

9d (Optional) If the entitlement requires you to set a value, click  to add the value.

or

If the entitlement requires a query to display the appropriate values (for example, a query for the groups in the connected system), run the query and select the appropriate value.

You can choose an external query, which runs a new query of the connected system, or you can choose a cached query, which simply displays the results of the last query that ran.

9e To add another entitlement from the same driver, click the  icon located on the same line as the driver name.

9f To add an entitlement from another driver, repeat [Step 9a](#) through [Step 9d](#).

10 On the Step 5 of 6: Assign Rights to Objects page, add the Identity Vault objects for which you want the entitlement policy to be a trustee.


Each member of the policy becomes a trustee of the objects you add. There are several reasons why you might want to make the policy a trustee of an object:


- ◆ One of the policy's entitlements requires the policy's members to have rights to an object.
- ◆ You want to use the policy to assign users as trustees of an object even though rights to the object are not required for an entitlement. In this case, you are using the entitlement policy to grant and revoke trustee rights for members of the policy.

Use the following options to manage the trustee assignments:

**Add Object:** Use this option to browse for and select the objects that you want to make the policy a trustee of.


**Rights to Selected Objects:** Click an object in the Object Name list to view the policy's rights to the object. You can add or remove rights by selecting or deselecting the desired rights. The Inherit check box determines whether the rights flow down in the tree. For example, if you are assigning rights to a container object, and you want the entitlement policy to have the same rights to the objects and sub-containers that are below that container, select the **Inherit** check box.

**Add Property:** In addition to doing a global assignment of rights to all properties ([All Attributes Rights]), you can assign rights to specific properties. This lets you limit rights to some properties and expand rights to others. To add a property, click  near **Properties** to browse for and select the desired property. After the property is added to the Rights to Selected Objects list, make the assigned rights modifications that you want.

**Remove Object or Property:** Click the  button to remove an object from the Object Name list or a property from the Rights to Selected Object list.

11 When you have finished making changes to trustee assignments, click **Next**.

12 On the Step 6 of 6: Entitlement Policy Summary page, review the policy information, then click **Finish** to create the policy and add it to the Entitlement Policy List.

**13** Click  > **Restart** to start the Entitlements Service driver.

After the driver starts, it evaluates the new policy (and all other policies in the list) and grants the appropriate entitlements to the policy members.

# 7 Controlling How Entitlements Are Granted or Revoked

You can control the consequences of granting or revoking an entitlement. Each driver provides a list of supported choices that control the meaning of “grant” or “revoke.”

For example, when you add a GroupWise account, you can specify that grant actually means to grant the user an account in a disabled state, so that the administrator must intervene before the user can access the account. Or, you could choose to enable the account, which is the default.

By default, the driver configurations use the option that is most likely to preserve data. For example, the default meaning of “remove” for a GroupWise account is set to “disable,” to avoid unintentionally losing accounts if a mistake is made when the administrator is making changes to policies. As another example, the Identity Manager driver configurations don’t revoke entitlements that have values from a user account in another system. If a user is granted membership in an e-mail distribution list, then later the user no longer meets the criteria for the entitlement policy, he or she is simply dropped from the policy membership. Accounts are disabled, but group membership and attribute values are not removed. An Identity Manager expert can customize the driver configurations if you want a different result.

The interpretation of revoking an entitlement is especially important because role-based entitlements give you the ability to make sweeping changes in an organization’s entitlements in a production environment, without testing the results in a lab.

You can change the settings for how to grant or revoke entitlements by editing the Global Configuration Variables on a preconfigured driver. If you are creating your own custom configuration, you can add GCVs to interpret how to grant and revoke entitlements.



# 8 Managing the Driver

As you work with the Entitlements 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](#).





# 9 Troubleshooting Role-Based Entitlements

The following sections provide information to help you troubleshoot problems with the Entitlements Service driver:

- ♦ “General Troubleshooting Issues” on page 33
- ♦ “Conflict Resolution between Entitlement Policies” on page 34

## General Troubleshooting Issues

When troubleshooting, keep in mind these issues:

- ♦ When you make any changes to policies by clicking **New**, **Edit**, or **Remove** on the page where the policies are listed, the Entitlements Service Driver is stopped. The driver is not restarted unless you click **Restart** on that page.

This feature prevents the driver from granting or revoking entitlements in your production environment while your changes to policies are incomplete.

If you don't use the **Restart** button on the page, you see the following in the trace:

```
DirXML Log Event -----
    Driver:   \ACME-LAB-LDAP\acme\Drivers\IDM\RBE-Entitlements Service
    Status:   Fatal
    Message:  Code(-9005) The driver returned a "fatal" status
indicating that the driver should be shut down. Detail from d
river: <description>Entitlement Policy editor is currently locked by
'acme\admins\admin@127.0.0.1'.</description>
<document xml:space="preserve"><nds dtdversion="3.5"
ndsversion="8.x">
  <source>
    <product version="3.6.1.4427">DirXML</product>
    <contact>Novell, Inc.</contact>
  </source>
  <input>
    <init-params src-dn="\ACME-LAB-
LDAP\acme\Drivers\IDM\RBE-Entitlements Service"/>
  </input>
</nds></document>
<application>DirXML </application>
<module>RBE-Entitlements Service </module>
<object-dn></object-dn>
<component>DirXML Engine</component>
```

- ♦ Similarly, the Entitlements Service Driver won't start if more than one person appears to be editing Entitlement Policies at the same time.
- ♦ Because one Entitlements Service Driver is used per driver set, an entitlement policy can manage only users that are in a read/write or master replica on the server that is associated with that driver set.

# Conflict Resolution between Entitlement Policies

When you are creating entitlement policies, it's possible that the policies that affect a particular user might conflict in assigning entitlements to that user. The following sections provide information to help you if conflicts are not being resolved the way you expect:

- ♦ [“Conflict Overview” on page 34](#)
- ♦ [“Changing the Conflict Resolution Method for an Individual Entitlement” on page 35](#)
- ♦ [“Prioritizing Entitlement Policies” on page 36](#)

## Conflict Overview

The following list describes how conflicts are resolved. For some entitlements, you can change the conflict resolution.

- ♦ **Entitlements that don't have values are additive.** In most cases an account entitlement doesn't have values. If a user is granted an account on a connected system by any entitlement policy, the user receives an account on that system. It does not matter whether another entitlement policy is in conflict; the result is additive.

This method of conflict resolution for granting accounts cannot be changed.

For example, if the Manager entitlement policy grants Jean Chandler an Exchange account, but Jean Chandler is excluded from the Mail Room Employees entitlement policy that also grants Exchange accounts, Jean still gets an Exchange account.

- ♦ **Entitlements that have values are additive by default, but you can choose to resolve by priority.** Entitlements, such as group membership, have a list of group names for the values, or have an attribute with a value. By default, these kinds of entitlements are also additive.

You can change the conflict resolution for these kinds of entitlements, if desired.

- ♦ **conflict-resolution=“union”:** A value of “union” means that the entitlements are additive. A user is granted all the entitlements that he or she is assigned by membership in any policy. The differing entitlement values are simply added together and the user gets them all.

For example, if Jameel is a member of the Trade Show Contractors policy that grants membership in a GroupWise e-mail distribution list named Trade Show Mailing List, and he is excluded from membership in the Trade Show Managers policy that also assigns the e-mail distribution list named Trade Show Mailing List, he still receives membership in the e-mail distribution list.

As another example, if Consuela is granted membership in the Active Directory group named Mailroom Staff by the Mailroom policy, and also granted membership in the Active Directory group named Emergency Response by the Emergency Volunteers policy, she is granted membership in both groups in Active Directory.

With this setting, the order of an entitlement policy in the list of policies is not important for the entitlement.

- ♦ **conflict-resolution=“priority”:** A value of “priority” means that if the values in two different policies conflict, or if one policy includes the user and another excludes the user, the entitlements granted to the user are only those in the entitlement policy that is listed higher in the list of Entitlement policies.

The previous examples would have a different result with this setting.

In the example above for Jameel, if the GroupWise e-mail distribution list entitlement had a value of “priority,” and the Trade Show Managers policy was higher in the list than the Trade Show Contractors policy, Jameel would not be granted membership in the Trade Show Mailing List.


In the example above for Consuela, if the Active Directory NOS group membership entitlement had a value of “priority,” and the Mailroom policy was higher in the list than the Emergency Volunteers policy, Consuela would be granted membership only in the Mailroom Staff group. She would not be granted membership in the Emergency Response group because the conflict resolution is by priority, not additive.

This functionality is useful if, for example, you configure your environment to use role-based entitlements to place users in a hierarchical structure on another system. You would want the user to be placed in either one place or another, not in two places at the same time.

Keep in mind that the setting is independent for each entitlement offered by each driver.

As a general rule, if you use the “priority” setting, you should place administrator or manager policies higher in the list than policies for end users or individual contributors. You should put groups with narrower membership higher than groups with broader membership.

## Changing the Conflict Resolution Method for an Individual Entitlement

- 1 Log in to Identity Console and select **IDM Administration** under Identity Manager. Select a driver set.
- 2 Click  button, then select **Stop driver**.
- 3 Click the driver icon for the driver that offers the entitlement you want to change.
- 4 On the Driver Overview page, click the **Advanced** tab, then click **Entitlements**.
- 5 Click the entitlement name to edit the entitlement in the XML viewer.
- 6 Select the check box for **Enable XML editing**.
- 7 In the XML, find the definition of the entitlement you want to change.

Here’s an example of the line you should look for:

```
<entitlement conflict-resolution="union" description="Grants membership to GroupWise Distribution lists" display-name="GroupWise Distribution Lists" name="gwDistLists">
```

- 8 Change the `conflict-resolution` value. The two possible values are the following:

```
conflict-resolution="union"
```

```
conflict-resolution="priority"
```

For information about these values, see [“Conflict Resolution between Entitlement Policies” on page 34](#).

- 9 Click **OK** to save the changes and restart the driver.
- 10 Click **IDM Administration** to browse to and restart the Entitlements Service driver.

## Prioritizing Entitlement Policies

By default, the order of the list of Entitlement Policies does not matter. This is because the driver configurations shipped with Identity Manager have `conflict-resolution="union"` as the method of conflict resolution for each entitlement.

If you change any of the entitlements to `conflict-resolution="priority,"` then the order of the list of Entitlement Policies matters, but only for those entitlements you changed. For information about these values, see [“Conflict Resolution between Entitlement Policies” on page 34](#).

- 1 In Identity Console, click **Role-Based Entitlements > Role-Based Entitlements**.

- 2 Search for and select a driver set.

A page appears with a list of the Entitlement policies.

- 3 Change the priority of the Entitlement policies by selecting a policy and using the arrow buttons to move it up and down in the list.

Moving an entitlement policy higher in the list gives it a higher priority.

- 4 Click **Close** to restart the driver.

Changes in priority don't take effect until the driver is restarted.

# A Driver Properties

This section provides information about the Driver Configuration and Global Configuration Values properties for the Entitlements 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 *NetIQ Identity Manager Driver Administration Guide* for information about the common properties.

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


- ♦ “[Driver Configuration](#)” on page 37
- ♦ “[Global Configuration Values](#)” on page 39

## Driver Configuration

In Identity Console:

- 1 Click the **IDM Administration** tile.
- 2 Select the driver set that contains the driver whose properties you want to edit.
- 3 Click the driver icon to display the driver’s properties page.

In Designer:

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

The Driver Configuration options are divided into the following sections:

- ♦ “[Driver Module](#)” on page 37
- ♦ “[Driver Object Password \(Identity Console Only\)](#)” on page 38
- ♦ “[Authentication](#)” on page 38
- ♦ “[Startup Option](#)” on page 38
- ♦ “[Driver Parameters](#)” on page 38
- ♦ “[ECMAScript](#)” on page 39
- ♦ “[Global Configurations](#)” on page 39

## Driver Module

The Driver Module section lets you change 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 is:

```
com.novell.nds.dirxml.driver.entitlement.EntitlementServiceDriver
```

**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 Entitlements Service driver. You cannot use the driver with the Remote Loader.

## Driver Object Password (Identity Console Only)

**Driver Object Password:** This setting does not apply to the Entitlements Service driver.

## Authentication

The Authentication section stores the information required to authenticate to the connected system and to the Remote Loader. The Entitlements Service driver functions 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 Entitlements Service driver is the cache setting.

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

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

## Startup Option

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

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

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

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

**Do not automatically synchronize the driver:** This option 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.

## Driver Parameters

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

**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.

**Subscriber Options > Result Threshold:** Specifies the maximum number of results that the driver logs for each object to which an entitlement is granted or revoked. For example, if a user is granted four entitlements, the default threshold of 10 results per entitlement causes a maximum of 40 results to be logged on the User object.

## ECMAScript

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

## 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

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

In Identity Console:

- 1 Click the **IDM Administration** tile.
- 2 Select the driver set that contains the driver whose properties you want to edit.
- 3 Locate the driver icon, then click the driver icon to display the driver's properties page.
- 4 Click **Global Config Values** drop down to display the GCV page.

In Designer:

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

