

Implementation Guide

Novell® Identity Manager Entitlements Service Driver

4.0

October 15, 2010

www.novell.com



Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. For more information on exporting Novell software, see the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/). Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2008-2010 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see [Novell Documentation \(http://www.novell.com/documentation/\)](http://www.novell.com/documentation/).

Novell Trademarks

For a list of Novell trademarks, see [Trademarks \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide	7
1 Understanding the Entitlement Service Driver	9
1.1 How the Entitlements Service Driver Works.	9
1.2 Role-Based Entitlements Versus Other Entitlements.	11
1.3 Using Multiple Entitlements Service Drivers.	11
2 Implementation Checklist	13
3 Installing the Driver Files	15
4 Creating a New Driver	17
4.1 Creating the Driver in Designer	17
4.1.1 Importing the Current Driver Packages	17
4.1.2 Installing the Driver Packages	18
4.1.3 Configuring the Driver Settings	18
4.1.4 Deploying the Driver	19
4.1.5 Starting the Driver	19
4.2 Creating the Driver in iManager	20
4.3 Activating the Driver	20
5 Upgrading an Existing Driver	21
5.1 Supported Upgrade Paths	21
5.2 What's New in Version 4.0	21
5.3 Upgrade Procedure	21
6 Creating Entitlement Policies	23
7 Controlling How Entitlements Are Granted or Revoked	27
8 Managing the Driver	29
9 Troubleshooting Role-Based Entitlements	31
9.1 General Troubleshooting Issues	31
9.2 Conflict Resolution between Entitlement Policies	32
9.2.1 Conflict Overview	32
9.2.2 Changing the Conflict Resolution Method for an Individual Entitlement	33
9.2.3 Prioritizing Entitlement Policies	34
A Driver Properties	37
A.1 Driver Configuration	37
A.1.1 Driver Module	38

A.1.2	Driver Object Password (iManager Only)	38
A.1.3	Authentication	38
A.1.4	Startup Option	38
A.1.5	Driver Parameters	39
A.1.6	ECMAScript	39
A.1.7	Global Configurations	39
A.2	Global Configuration Values	39

About This Guide

This guide explains how to install and configure the Identity Manager Entitlements Service Driver.

- ♦ [Chapter 1, “Understanding the Entitlement Service Driver,” on page 9](#)
- ♦ [Chapter 2, “Implementation Checklist,” on page 13](#)
- ♦ [Chapter 3, “Installing the Driver Files,” on page 15](#)
- ♦ [Chapter 4, “Creating a New Driver,” on page 17](#)
- ♦ [Chapter 5, “Upgrading an Existing Driver,” on page 21](#)
- ♦ [Chapter 6, “Creating Entitlement Policies,” on page 23](#)
- ♦ [Chapter 7, “Controlling How Entitlements Are Granted or Revoked,” on page 27](#)
- ♦ [Chapter 8, “Managing the Driver,” on page 29](#)
- ♦ [Chapter 9, “Troubleshooting Role-Based Entitlements,” on page 31](#)
- ♦ [Appendix A, “Driver Properties,” on page 37](#)

Audience

This guide is for Novell eDirectory and Identity Manager administrators who are using the Entitlements Service driver to implement role-based entitlements.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Use the User Comment feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of this document, see the [Novell Identity Manager Drivers Documentation Web site \(http://www.novell.com/documentation/idm40drivers/index.html\)](http://www.novell.com/documentation/idm40drivers/index.html).

Additional Documentation

For information on Identity Manager and other Identity Manager drivers, see the [Identity Manager Documentation Web site \(http://www.novell.com/documentation/idm40/index.html\)](http://www.novell.com/documentation/idm40/index.html).

Understanding the Entitlement Service Driver

1

The following overview assumes that you understand entitlements (as explained in the “[Entitlements Overview](#)” in the *Identity Manager 4.0 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 *Identity Manager 4.0 Entitlements Guide*) and workflow-based provisioning component in the User Application (see “[User Application Workflow-Based Provisioning](#)” in the *Identity Manager 4.0 Entitlements Guide*).

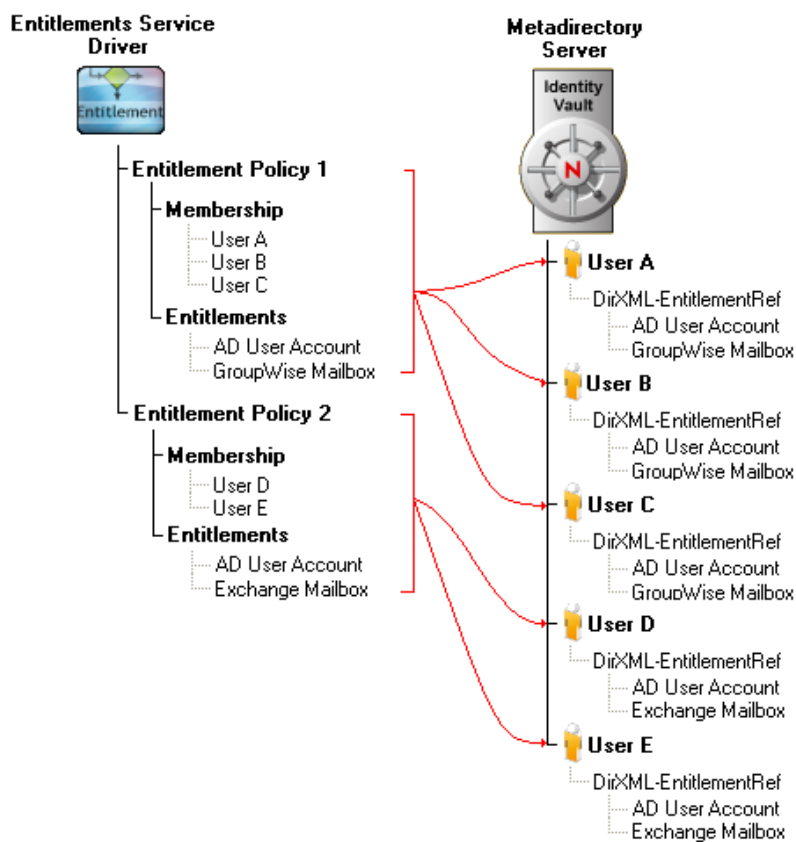
The following sections provide information to help you understand the Entitlements Service driver:

- ♦ [Section 1.1, “How the Entitlements Service Driver Works,” on page 9](#)
- ♦ [Section 1.2, “Role-Based Entitlements Versus Other Entitlements,” on page 11](#)
- ♦ [Section 1.3, “Using Multiple Entitlements Service Drivers,” on page 11](#)

1.1 How the Entitlements Service Driver Works

The Entitlements Service driver grants entitlements to and revokes entitlements from users, as shown in the following diagram.

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 [Identity Manager 4.0 Entitlements Guide](#).

1.2 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 iManager lets you manage the entitlement policies used by the Entitlements Service driver.

1.3 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 Metadirectory 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.

Implementation Checklist

2

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 Identity Manager 4.0 Entitlements Guide.</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 Metadirectory server when the Metadirectory 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 Identity Manager 4.0 Entitlements Guide.</p> <p>If you have an existing driver to upgrade, see Chapter 5, "Upgrading an Existing Driver," on page 21.</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 Chapter 6, "Creating Entitlement Policies," on page 23.</p>

Installing the Driver Files

3

By default, the Entitlements Service driver files are installed on the Metadirectory server at the same time as the Metadirectory 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," on page 17](#)) or upgrade an existing driver's configuration (see [Chapter 5, "Upgrading an Existing Driver," on page 21](#)).

Creating a New Driver

4

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 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 17](#)
- ♦ [Section 4.2, “Creating the Driver in iManager,” on page 20](#)
- ♦ [Section 4.3, “Activating the Driver,” on page 20](#)

4.1 Creating the Driver in Designer

You create the Entitlements 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.

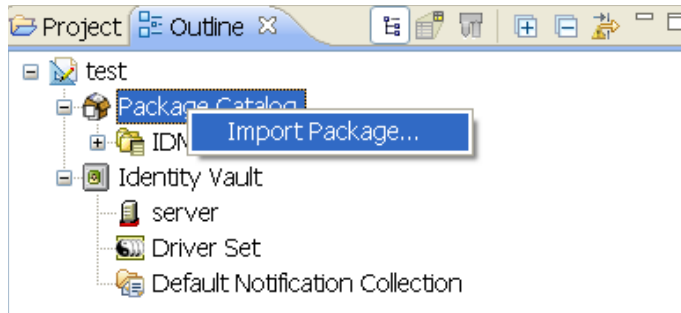
- ♦ [Section 4.1.1, “Importing the Current Driver Packages,” on page 17](#)
- ♦ [Section 4.1.2, “Installing the Driver Packages,” on page 18](#)
- ♦ [Section 4.1.3, “Configuring the Driver Settings,” on page 18](#)
- ♦ [Section 4.1.4, “Deploying the Driver,” on page 19](#)
- ♦ [Section 4.1.5, “Starting the Driver,” on page 19](#)

4.1.1 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 and can be updated after they are initially installed. You must have the most current version of the packages in the Package Catalog before you can create a new driver object.

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 [Section 4.1.2, “Installing the Driver Packages,”](#) on page 18.

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 *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 [Section 4.1.3, “Configuring the Driver Settings,”](#) on page 18.
or
If you do not need to change the configuration, continue with [Section 4.1.4, “Deploying the Driver,”](#) on page 19.

4.1.3 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 [Section 4.1.4, “Deploying the Driver,” on page 19](#).

4.1.4 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. Whatever rights that the driver needs to have on the server, the DriversUser object must have the same security 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.
 - 8d Click *OK*.
- 9 Click *OK*.

4.1.5 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 29](#).

4.2 Creating the Driver in iManager

Drivers are created with packages, and iManager does not support packages. In order to create or modify drivers, you must use Designer. See [Chapter 4, “Creating a New Driver,” on page 17](#).

4.3 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.

For information on activation, refer to the “[Activating Novell Identity Manager Products](#)” in the *Identity Manager 4.0 Framework Installation Guide*.

Upgrading an Existing Driver

5

The following sections provide information to help you upgrade an existing driver's configuration to version 4.0:

- ♦ [Section 5.1, “Supported Upgrade Paths,” on page 21](#)
- ♦ [Section 5.2, “What's New in Version 4.0,” on page 21](#)
- ♦ [Section 5.3, “Upgrade Procedure,” on page 21](#)

5.1 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 is not supported.

5.2 What's New in Version 4.0

Driver content is delivered in packages instead of through a driver configuration file.

5.3 Upgrade Procedure

The process for upgrading the eDirectory driver is the same as for other Identity Manager drivers. For detailed instructions, see “[Upgrading Drivers to Packages](#)” in the *Identity Manager 4.0 Framework Installation Guide*.



Creating Entitlement Policies

6

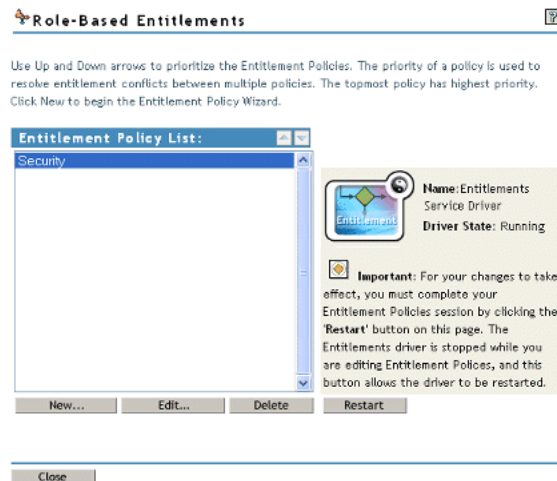
The Entitlements Service driver implements entitlements through the use of entitlement policies. An entitlement policy contains the following:

- ♦ **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 In iManager, click  to display the Identity Manager Administration page.
- 2 In the Feature list, click *Role-Based Entitlements*.
- 3 In the *Select driver set* field, click  to browse for and select the driver set where you want to create the entitlement policy, then click *OK* to display the Entitlement Policy List.

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 *New* to launch the Entitlement Policy Wizard.

Entitlement Policy Wizard

Step 1 of 6: Name and describe the Entitlement Policy

Entitlement Policy Name: * Required

(ex. Engineering Entitlement Policy)

Description:

<< Back Next >> Cancel Finish

- 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.

- 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 Metadirectory 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 *Add New Group* 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 *Add Driver* 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 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 subcontainers 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 *Add Property* 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.

Controlling How Entitlements Are Granted or Revoked

7

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.

Managing the Driver

8

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 [*Identity Manager 4.0 Common Driver Administration Guide*](#).

Troubleshooting Role-Based Entitlements

9

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

- ♦ [Section 9.1, “General Troubleshooting Issues,” on page 31](#)
- ♦ [Section 9.2, “Conflict Resolution between Entitlement Policies,” on page 32](#)

9.1 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.

9.2 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:

- ♦ [Section 9.2.1, “Conflict Overview,” on page 32](#)
- ♦ [Section 9.2.2, “Changing the Conflict Resolution Method for an Individual Entitlement,” on page 33](#)
- ♦ [Section 9.2.3, “Prioritizing Entitlement Policies,” on page 34](#)

9.2.1 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.

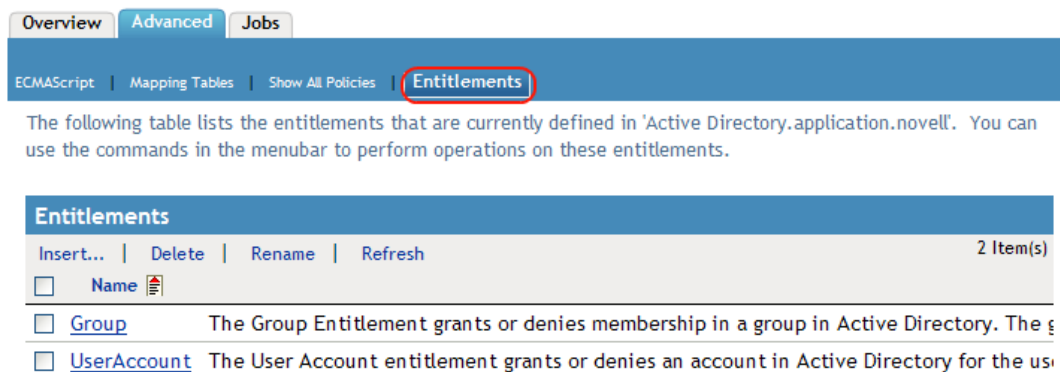
This functionality is useful if, for example, you configure your environment to use role-based entitlements to place users in a hierarchical structure on another system. You would want the user to be placed in either one place or another, not in two places at the same time.

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.

9.2.2 Changing the Conflict Resolution Method for an Individual Entitlement

- 1 In iManager, click *Identity Manager > Identity Manager Overview*, then select a driver set.
- 2 Click the driver status 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*.



The screenshot shows the iManager interface with the 'Entitlements' tab selected. The table lists the following entitlements:

Entitlements
<input type="checkbox"/> Group The Group Entitlement grants or denies membership in a group in Active Directory. The g
<input type="checkbox"/> UserAccount The User Account entitlement grants or denies an account in Active Directory for the us

- 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 32](#).

- 9 Click *OK* to save the changes.
- 10 Click the *Overview* tab to access the driver icon.
- 11 Click *Restart* to restart the driver.
- 12 Click *Identity Manager Overview* to browse to and restart the Entitlements Service driver.

9.2.3 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 32](#).

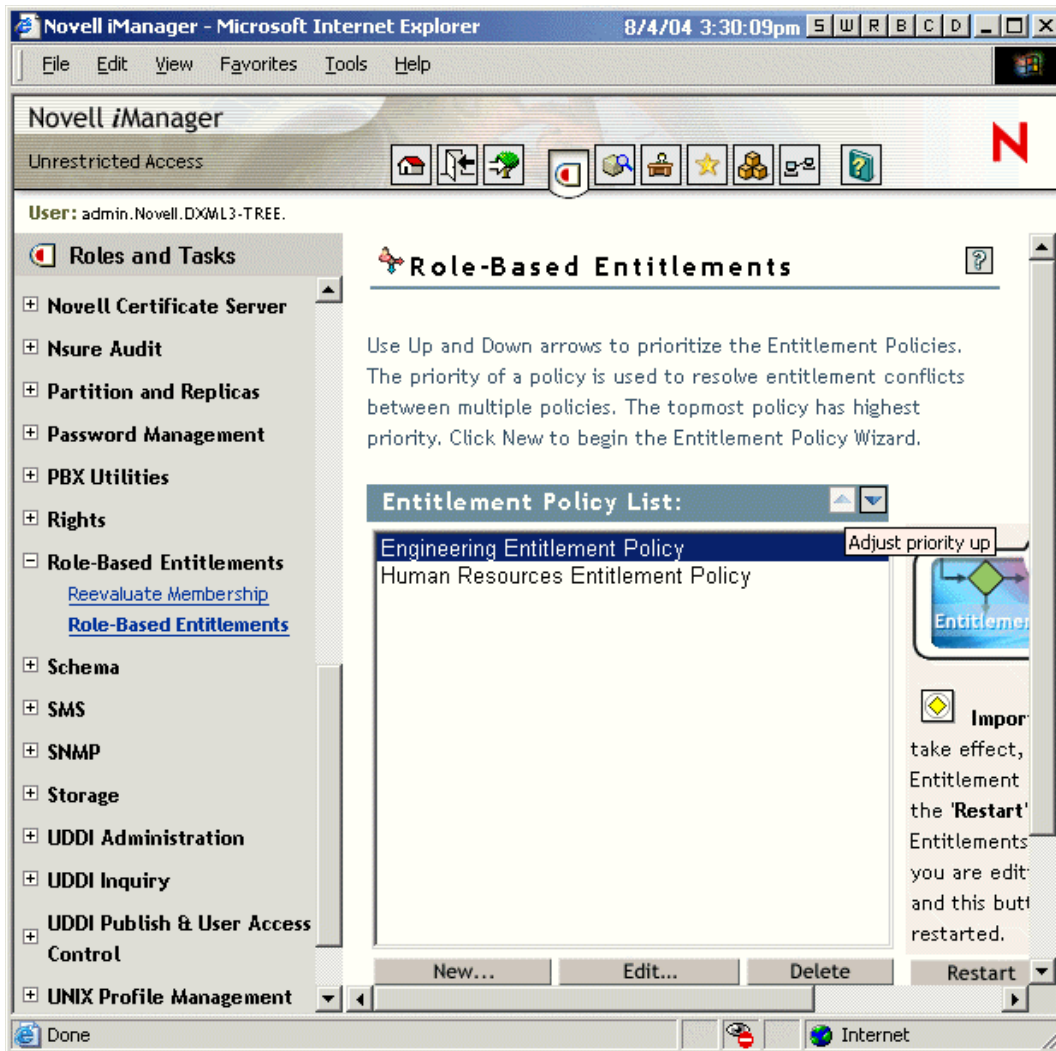
- 1 In iManager, click *Role-Based Entitlements > Role-Based Entitlements*.

- 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.

Driver Properties

A


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 *Identity Manager 4.0 Common Driver 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  icon.


- ♦ [Section A.1, “Driver Configuration,” on page 37](#)
- ♦ [Section A.2, “Global Configuration Values,” on page 39](#)

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 Entitlements Service 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 38](#)
- ♦ [Section A.1.2, “Driver Object Password \(iManager Only\),” on page 38](#)
- ♦ [Section A.1.3, “Authentication,” on page 38](#)
- ♦ [Section A.1.4, “Startup Option,” on page 38](#)
- ♦ [Section A.1.5, “Driver Parameters,” on page 39](#)
- ♦ [Section A.1.6, “ECMAScript,” on page 39](#)
- ♦ [Section A.1.7, “Global Configurations,” on page 39](#)

A.1.1 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.

A.1.2 Driver Object Password (iManager Only)

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

A.1.4 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 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.

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.

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 Entitlements 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. To do so:
 - 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 Entitlements Service 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*.

