AUTHORIZED DOCUMENTATION

# Role Mapping Administrator User Guide

# Novell® Identity Manager

**1.0**

May 29, 2009

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. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.



Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

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

*Online Documentation:* To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

## Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (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

This guide explains how to use the Novell® Identity Manager Role Mapping Administrator to map authorizations in connected systems to Identity Vault roles. It contains the following sections:



### Audience

This guide is intended for any users responsible for establishing and maintaining cross-domain policy relationships between Novell Identity Manager and connected systems. To use the Role Mapping Administrator, you must be defined as a Roles Administrator or Roles Manager in the Identity Manager Roles Based Provisioning Module.

### Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments 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 the Novell Identity Manager *Role Mapping Administrator User Guide*, visit the Novell Compliance Management Platform Extension for SAP Environments Documentation Web site (http://www.novell.com/documentation/ncmp_sap10).

### Additional Documentation

For documentation on Identity Manager, see the Novell Identity Manager Documentation Web site (http://www.novell.com/documentation/idm36).

For documentation on the Identity Manager Roles Based Provisioning Module, see the Novell Identity Manager Roles Based Provisioning Module Documentation Web site (http://www.novell.com/documentation/idmbpm361/index.html).

### Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

# Getting Started

# 1

The Novell® Identity Manager Role Mapping Administrator lets you map connected systems roles, composite roles, and profiles (collectively referred to as *authorizations*) to Identity Manager roles. When a user is assigned a role through the Identity Manager Roles Based Provisioning Module, he or she receives all authorizations mapped to that role.

The following sections provide information to help you start using the Role Mapping Administrator:



## 1.1 Logging In

To successfully log in to the Role Mapping Administrator, you must be defined as a Roles Administrator or a Roles Manager in the Roles Based Provisioning Module. If you are not, your login fails.

To log in:

1. In your Web browser, navigate to the Role Mapping Administrator by using the Web address (URL) or Web page link supplied to you.
2. (Conditional) If a Login page is displayed, specify the same username and password you use to log in to the Roles Based Provisioning Module.

   If a Login page does not appear, the Role Mapping Administrator has been configured to automatically log you in to the Role Mapping Administrator.

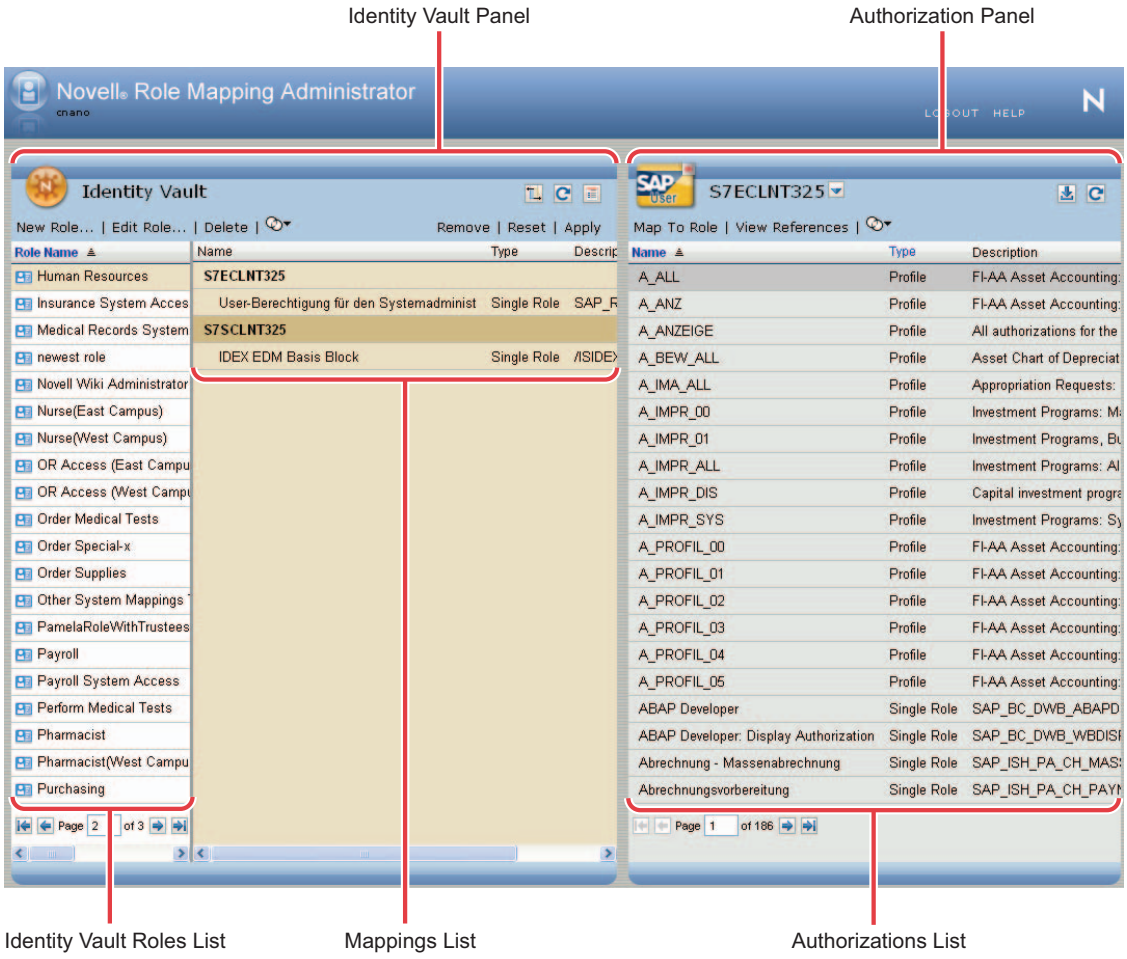
If the Role Mapping Administrator has not been configured, you are presented with an administration configuration page.

If you are presented with this page, contact your system administrator to configure the Role Mapping Administrator.

# 1.2 Getting to Know the Role Mapping Administrator Interface

The primary work area in the Role Mapping Administrator is called the Main Window. You use the Main Window to perform all of the tasks required to map authorizations to Identity Manager roles and to manage (create, edit, delete) Identity Manager roles.

***Figure 1-1*** *Role Mapping Administrator Interface*




### Identity Vault Panel

The Identity Vault panel contains two lists: *Identity Vault Roles* list and *Mappings* list. The *Identity Vault Roles* list displays the roles that you are authorized to manage. After you select a role, the *Mappings* list displays any authorizations that are mapped to it.

The Identity Vault panel also contains options to refresh roles from the Identity Vault, filter the roles that you see in the *Identity Vault Roles* list, and manage (create, edit, and delete) roles.

### Authorizations Panel

The Authorizations panel displays the authorizations that are available for mapping to Identity Manager roles. To map an authorization to a role, you select the role in the *Identity Vault Roles* list, select the authorization in the *Authorizations* list, then drag the authorization to the *Mappings* list.

Depending how your Identity Manager environment is configured, you might have more than one system. The *Authorizations* list displays only the authorizations from the connected system that is currently selected in the list box at the top of the panel. To view authorizations from another system, you must select that system from the list.

The Authorizations panel also contain options to refresh authorizations from the Role Mapping Administrator database, reload the Role Mapping Administrator database with authorizations from the available connected systems, and filter the authorizations that you see in the *Authorizations* list.

## 1.3 Terminology

The following terms are used throughout the Role Mapping Administrator interface and documentation:

**authorization:** A role, composite role, or profile.

**Identity Vault:** The LDAP directory used by the Role Mapping Administrator for user authentication, data retrieval, and data storage.

**role (or Identity Vault role):** An enterprise role that has been defined in the Role Based Provisioning Module for automating the provisioning of entitlements to users. For the Role Mapping Administrator, the authorizations being mapped to the role are added to the entitlements that are provisioned by the role.

**Role Mapping Administrator:** The Web application used to map authorizations to Identity Vault roles, and to create, edit, and delete Identity Vault roles.

**Role Mapping Administrator database:** The database used to store the authorizations that the Role Mapping Administrator retrieves from the available connected systems.

# Mapping Roles

# 2

The following sections provide instructions for mapping connected system authorizations to Identity Vault roles.



## 2.1 Loading Authorizations

The Role Mapping Administrator stores the authorizations for the connected systems in its local database. This database must be loaded before you can map authorizations to roles.

If your administrator for the Role Mapping Administrator has not preloaded the database, or if you need to update the database because the authorizations have changed in the connected system, you need to load the database.

You can control which connected systems authorizations are loaded, and you can control which types of authorizations (Groups, Roles, Profiles, or all of them) are loaded.

1. In the Authorizations panel, click the *Load Authorizations* icon  to display the Authorizations Loader dialog box.
2. In the *Systems* list, select the connected systems from which you want to load authorizations.
3. In the *Authorizations* list, select the types of authorizations (Groups, Roles, and Profiles) you want loaded. Repeat this for each connected system you selected.

   If you select Roles, both roles and composite roles are loaded.
4. Click *OK*.

   The Role Mapping Administrator begins retrieving the authorizations from the selected connected systems. The time required to retrieve and load the authorizations depends on the number of systems you selected and the number or authorizations contained in each system.

## 2.2 Mapping Authorizations to Roles

1. In the *Identity Vault Roles* list, select the role to which you want to map authorizations.

   You can filter and sort the *Identity Vault Roles* list to more easily locate the role. For information, see Section 4.1, “Filtering Lists,” on page 17 and Section 4.2, “Sorting Lists,” on page 18.
2. In the *Authorizations* list, select the authorization you want to map, then drag it to the *Mappings* list in the Identity Vault panel.

   or

   In the *Authorizations* list, select the authorization you want to map, then click *Map To Role* in the toolbar.

You can Ctrl+click and Shift+click to select multiple authorizations. You can also filter and sort the *Authorizations* list to more easily locate the authorizations. For information, see Section 4.1, “Filtering Lists,” on page 17 and Section 4.2, “Sorting Lists,” on page 18.

3. Click *Apply*, in the toolbar to save the mappings.
4. Click *OK* in the confirmation message.

   Any users assigned to the role that the connected system authorizations are mapped to are automatically granted rights to the mapped connected system authorizations.

If you have added a mapping, but you do not want to apply the mapping, click *Reset* in the toolbar to reset the mapping before clicking *Apply*. When you click *Apply*, the mappings are saves and applied to the connected system.

You can add or remove mappings in the same session. Add or remove the desired mappings, then click *Apply*.

## 2.3 Removing Mappings

1. In the Identity Vault Roles list, select the role whose authorization mapping you want to remove.

   You can filter and sort the Vault Roles list to more easily locate the role. For information, see Section 4.1, “Filtering Lists,” on page 17 and Section 4.2, “Sorting Lists,” on page 18.
2. In the *Mappings* list, select the authorization mapping you want to remove.

   You can Ctrl+click and Shift+click to select multiple mappings. You can also sort the Mappings list to more easily locate the mappings. For information, see Section 4.2, “Sorting Lists,” on page 18.
3. Click *Remove* in the toolbar to remove the mapping.
4. Click *Apply* to save the changes.
5. Click *OK* in the confirmation message.

   Any users assigned to the role the connected system authorizations are mapped to are automatically removed from the connected system authorizations.

You can add or remove mappings in the same session. Add or remove the desired mappings, then click *Apply*.

# Managing Roles

# 3

The Role Mapping Administrator lets you add roles to the Identity Vault, edit existing roles, and remove roles you no longer need.



## 3.1 Creating Roles

1. In the Identity Vault panel, click *New Role* to display the Add Role dialog box,
2. Fill in the following fields to define the role:

   **Name:** Specify a name to identify the role. You cannot include the following characters in the name: < > , ; \ " + # = / | & *

   **Description:** Specify a description of the role.

   **Level:** Select whether the role is a Business Role, IT Role, or Permission Role. Business Roles define operations that have business meaning within the organization. IT Roles support technology functions. Permission Roles define lower-level privileges.

   If the level you select has a [+] next to it, the level includes containers to organize the roles. You can click the [+] to display the containers.

   **Category:** Select the category in which to place the role.

   **Owners:** Select the users who are responsible for the role definition. To select an owner, specify whether you want to search using First Name or Last Name, specify the name (or the partial name) in the *Search* field, then click *Search*. After the matching names are displayed, select the desired user, then click [›] to move the user to the *Selected Owners* list.
3. Click *OK* to create the role in the Identity Vault.

## 3.2 Removing Roles

1. In the Identity Vault panel, select the role to remove from the Identity Vault.
2. Click *Delete*, then click *OK* to confirm the deletion.

## 3.3 Editing Role Information

1. In the Identity Vault panel, select the role you want to edit, then click *Edit Role* to display the Edit Role dialog box.
2. Modify the following fields as needed:

   **Name:** Specify a name to identify the role in the Roles Based Provisioning Module and Role Mapping Administrator. You cannot include the following characters in the name: < > , ; \ " + # = / | & *

   **Description:** Specify a description of the role to display in the Roles Based Provisioning Module.

**Level:** Lists whether the role is a Business Role, IT Role, or Permission Role. Business Roles define operations that have business meaning within the organization. IT Roles support technology functions. Permission Roles define lower-level privileges.

You can not edit this field.

**Category:** Select the category in which to place the role.

**Owners:** Select the users who are responsible for the role definition. To select an owner, specify whether you want to search using First Name or Last Name, specify the name (or the partial name) in the *Search* field, then click *Search*. After the matching names are displayed, select the desired user, then click › to move the user to the *Selected Owners* list.

3 Click *OK* to change the role in the Identity Vault.

# Managing Lists

# 4

The primary purpose of the Role Mapping Administrator is to let you map authorizations to Identity Vault roles. To effectively and efficiently carry out your mapping tasks, you need to know how to filter, sort, and refresh the *Identity Vault Roles* list and *Authorizations* list.



## 4.1 Filtering Lists

The Identity Vault and the connected systems might contain more roles than can be displayed in the *Identity Vault Roles* list and the *Authorizations* list. Rather than paging through the lists to find the roles and authorizations you want to map, you can filter the lists to show the desired items.



### 4.1.1 Filtering the Identity Vault Roles List

1. In the Identity Vault panel, click the *Define Filter* icon to display the Roles Filter dialog box.
2. Use the *Name*, *Category*, and *Level* fields to define the filter criteria.

   The filter can utilize criteria in one, two, or all three fields. You can also use * and ? as wildcards. The *Name* field is case sensitive. The following are examples of possible filters:

| Desired Result | Name Field | Category Field | Level Field |
|---|---|---|---|
| All roles that start with M | M* | Blank | Blank |
| All IT roles that start with M | M* | Blank | IT Role |
| All roles that start with M and are in the Systems Access category | M* | Systems Access | Blank |

3. Click *OK* to apply the filter.

### 4.1.2 Filtering the Authorizations List

1. In the Authorizations panel, click the *Define Filter* icon to display the Authorizations Filter dialog box.
2. Use the *Name*, *Description*, and *Type* fields to define the filter criteria.

The filter can utilize criteria in one, two, or all three fields. You can also use * and ? as wildcards. The following are examples of possible filters:

| Desired Result | ID Field | Description Field | Type Field |
|---|---|---|---|
| All authorizations that start with S | S* | Blank | Blank |
| All authorizations that start with S and whose type is Role | S* | Blank | Role |

3 Click *OK* to apply the filter.

# 4.2 Sorting Lists

You can sort the *Identity Vault Roles* list and the *Authorizations* list, by clicking on the *Name* column in each panel. This sorts the roles and authorization from A to Z or from Z to A.

# 4.3 Refreshing Lists

If roles or authorizations are added or removed while you are in the Role Mapping Administrator, you must manually refresh the *Identity Vault Roles* list and *Authorizations* list to see the changes.

- Section 4.3.1, "Refreshing the Identity Vault Roles List," on page 18
- Section 4.3.2, "Refreshing the Authorizations List," on page 18

## 4.3.1 Refreshing the Identity Vault Roles List

1 In the Identity Vault panel, click the *Refresh List* icon .

## 4.3.2 Refreshing the Authorizations List

Refreshing the Authorizations list causes the Role Mapping Administrator to reread its database and display the stored authorizations. It does not update the database authorizations from the connected systems. To update authorizations from the systems, you must reload the authorizations (see Section 2.1, "Loading Authorizations," on page 13).

Typically, you should only need to refresh the Authorizations List if you believe that another Role Mapping Administrator user might have reloaded authorizations from the connected systems while you have been working in the Role Mapping Administrator.

1 In the Authorizations panel, click the *Refresh List* icon .

## 4.4 Adjusting the Width of the Roles and Mapping Lists

By default, the *Mappings* list is wider than the *Identity Vault Roles* list. You can toggle the lists so that the *Identity Vault Roles* list becomes the wider list. This enables you to see more of the information displayed in the *Identity Vault Roles* list's columns.

1 In the Identity Vault panel, click the *Toggle Roles/Mappings List* icon  .

# Generating Reports

5

The Role Mapping Administrator allows you to export a `.csv` file of the Identity Vault roles and any associated authorizations that are mapped to the connected system roles. This allows you to import the file into any third-party reporting applications to create your own custom reports.

To generate a report:

1. In the Identity Vault panel, click *New Report*  .
2. Fill in the following fields to filter information in the report. If nothing is specified, the report contains information about all roles.

   **Name:** Specify the starts with criteria to filter on. No wildcards are supported. Leaving the field blank is the same as no filter being applied. For example, specifying an A returns all roles that begin with an A. The AND operator is used with the *Name* field and the *Categories* and *Level* fields.

   **Categories:** Select one or more values that a role must match before appearing in the report. The OR operator is used for the list of categories. For example, when you select *Doctor* and *Nurse* the report returns any roles in the categories of Doctor or Nurse.

   **Level:** Select one or more values that a role must match before appearing in the report. The OR operator is used for the list of levels.
3. Click *OK* to generate the report.

   The filename for the report is `idmrmap.csv`.

# Troubleshooting

6



## 6.1 Authentication Issues

### Problem

Failing to authenticate to the Role Mapping Administrator.

### Solutions

Check the following items to correct the authentication problem. If the authentication issues continue, contact your system administrator.

- The password is not correct.
- The username does not exist in the user store.
- There are multiple user accounts matching the specified username. Use the distinguished name (DN) instead of the common name (CN).
- There are network problems. The user’s credentials are verified against the user store through an LDAP connection.
- The LDAP server is not communicating.
- If the eDirectory™ connection is using SSL, the certificate might have expired. Check with your system administrator to confirm whether the eDirectory certificate is valid or has expired.
- The user account you are using does not have sufficient rights in the Roles Based Provisioning Module. Check with your administrator to verify that you have sufficient rights to use the Role Mapping Administrator.