

Role Mapping Administrator User Guide

Novell® Identity Manager

4.0.1

April 15, 2011

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 \(http://www.novell.com/info/exports/\)](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.

Copyright © 2007-2010 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 latest online documentation for this and other Novell products, see [the Novell Documentation Web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](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 Getting Started	9
1.1 Logging In	9
1.2 Getting to Know the Role Mapping Administrator Interface	10
1.3 Terminology	12
2 Mapping Roles	13
2.1 Loading Authorizations	13
2.2 Mapping Authorizations to Roles	14
2.3 Editing Mappings	14
2.4 Removing Mappings	15
3 Managing Roles	17
3.1 Creating Roles	17
3.2 Removing Roles	17
3.3 Editing Role Information	17
4 Managing Lists	19
4.1 Configuring Lists	19
4.1.1 Filtering the Identity Vault Roles List	19
4.1.2 Filtering the Authorizations List	19
4.1.3 Customizing the Mapping List	20
4.2 Sorting Lists	20
4.3 Refreshing Lists	20
4.3.1 Refreshing the Identity Vault Roles List	21
4.3.2 Refreshing the Authorizations List	21
4.4 Adjusting the Width of the Roles and Mapping Lists	21
5 Generating Reports	23
6 Troubleshooting	25
6.1 Troubleshooting the Role Mapping Administrator	25

About This Guide

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

- ♦ Chapter 1, “Getting Started,” on page 9
- ♦ Chapter 2, “Mapping Roles,” on page 13
- ♦ Chapter 3, “Managing Roles,” on page 17
- ♦ Chapter 4, “Managing Lists,” on page 19
- ♦ Chapter 5, “Generating Reports,” on page 23
- ♦ Chapter 6, “Troubleshooting,” on page 25

Audience

This guide is intended for any users responsible for establishing and maintaining cross-domain policy relationships between Novell Identity Manager and managed 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.

Documentation Updates

For the most recent version of the *Novell Identity Manager Role Mapping Administrator 4.0.1 User Guide*, visit the [Identity Manager 4.0.1 Documentation Web site \(http://www.novell.com/documentation/idm401/\)](http://www.novell.com/documentation/idm401/).

Additional Documentation

For documentation on the Novell Compliance Management Platform, see the [Novell Compliance Management Platform Documentation Web site \(http://www.novell.com/documentation/ncmp10/index.html\)](http://www.novell.com/documentation/ncmp10/index.html).

For documentation on the Identity Manager Roles Based Provisioning Module, see the [Identity Manager Roles Based Provisioning Module 4.0.1 Documentation Web site \(http://www.novell.com/documentation/idmrbpm401/index.html\)](http://www.novell.com/documentation/idmrbpm401/index.html).

For documentation on the SAP drivers, see the [Identity Manager 4.0.1 Drivers Documentation Web site \(http://www.novell.com/documentation/idm401drivers/index.html\)](http://www.novell.com/documentation/idm401drivers/index.html).

For documentation on Access Manager, see the [Access Manager 3.1 Documentation Web site \(http://www.novell.com/documentation/novellaccessmanager31/index.html\)](http://www.novell.com/documentation/novellaccessmanager31/index.html).

For documentation on Sentinel, see the [Sentinel 6.1 Documentation Web site \(http://www.novell.com/documentation/sentinel61/index.html\)](http://www.novell.com/documentation/sentinel61/index.html).

For documentation on the SAP Connector, SAP Collector, and the SAP Solution Pack, see the Sentinel 6.1 download Web site (<http://support.novell.com/products/sentinel/secure/sentinel61.html>).

Getting Started

1

The Novell Identity Manager Role Mapping Administrator lets you map managed 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:

- ♦ [Section 1.1, “Logging In,” on page 9](#)
- ♦ [Section 1.2, “Getting to Know the Role Mapping Administrator Interface,” on page 10](#)
- ♦ [Section 1.3, “Terminology,” on page 12](#)

1.1 Logging In

If you have both Role Administrator and the Resource Administrator roles, you can create, edit, and delete mappings. If you login with only one of these roles, either the login fails or you can just view the mappings. For more information about the roles required for different operations, see [Table 1-1](#).

Table 1-1 *Different Roles Required to Perform Different Operations*

	Resource Administrator	Resource Manager
Role Administrator	Create, edit, and delete mappings	View mappings
Role Manager	View mappings	View mappings

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.
For example, `http://hostname:port`, where `hostname` represents the hostname/IP address of the server where Role Mapping Administrator is installed and `8081` is the default port number.
- 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.

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

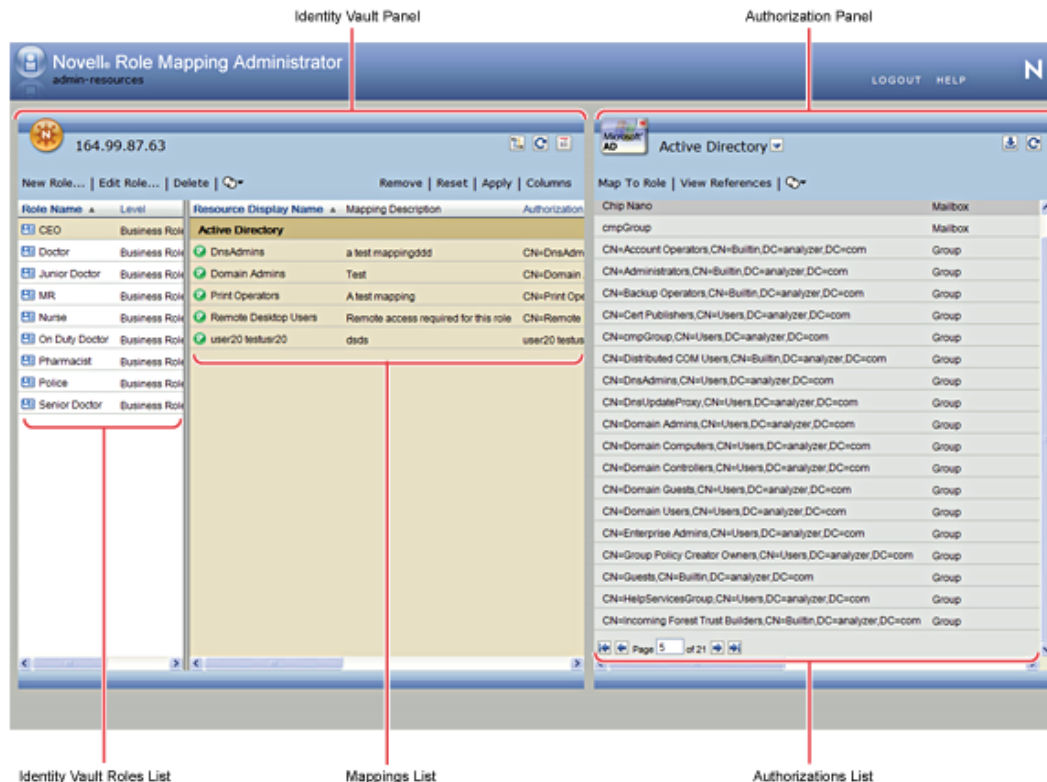


If you are presented with this page, contact your system administrator to configure the Role Mapping Administrator.

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: the *Identity Vault Roles* list and the *Mappings* list. The *Identity Vault Roles* list displays the roles that you are authorized to manage. The *Mappings* list displays any authorizations that are mapped to it, the name of the resource to which an authorization is mapped, and the mapping description. You can reload and edit the mapping. 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 on how your Identity Manager environment is configured, you might have more than one system. The *Authorizations* list displays only the authorizations from the managed 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 managed 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.

resource: An enterprise resource provides the ability for end users to request provisioning of entitlements/authorizations for themselves or for users that they have a relationship with. Resources provide the ability for administrators to gain better control over the management of user access to entitlements/authorizations, ensuring that the right people have the right access to the right resources.

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 managed systems.

Mapping Roles

2

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


- ♦ [Section 2.1, “Loading Authorizations,” on page 13](#)
- ♦ [Section 2.2, “Mapping Authorizations to Roles,” on page 14](#)
- ♦ [Section 2.3, “Editing Mappings,” on page 14](#)
- ♦ [Section 2.4, “Removing Mappings,” on page 15](#)

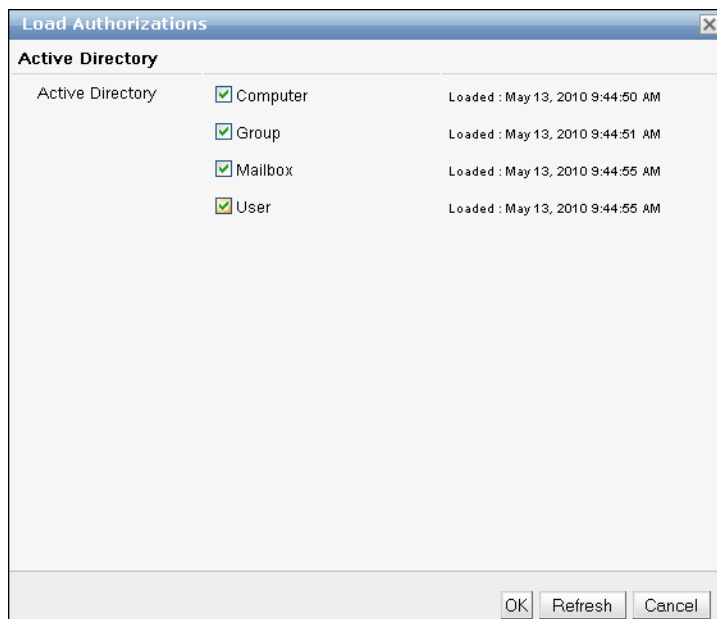
2.1 Loading Authorizations

The Role Mapping Administrator stores the authorizations for the managed 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 managed system, you need to load the database.

You can control which managed 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 Load Authorizations dialog box.



- 2 In the *Systems* list, select the managed systems from which you want to load authorizations.
- 3 In the *Authorizations* list, select the types of authorizations (for example, Groups, Roles, and Profiles) you want loaded. Repeat this for each managed 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 managed systems. The time required to retrieve and load the authorizations depends on the number of systems you selected and the number of 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, “Configuring Lists,” on page 19](#) and [Section 4.2, “Sorting Lists,” on page 20](#).

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 filter and sort the *Authorizations* list to more easily locate the authorizations. For information, see [Section 4.1, “Configuring Lists,” on page 19](#) and [Section 4.2, “Sorting Lists,” on page 20](#).

You can drag and drop multiple authorizations.

NOTE: Resources with multiple entitlement values are not displayed in the *Mappings* list.

3 Click *Apply* in the toolbar to save the mappings.

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 saved and applied to the managed system.

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

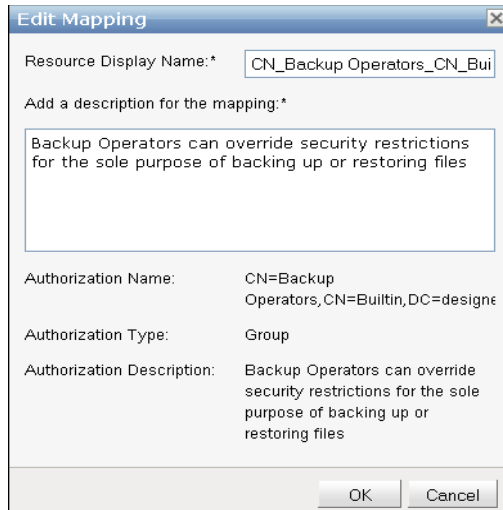
4 Click *OK* in the confirmation message.

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

2.3 Editing Mappings

You can change the display name of resources and edit the mapping description. When an authorization mapping is removed, resources mapped to this authorization are not removed.

1 In the *Mappings* list, select the resource whose description you want to change, then click *Edit Mapping* in the toolbar.



- 2 Specify a new description for the resource.
- 3 Click *Apply* to save the changes.
- 4 Click *OK* in the confirmation message.

2.4 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, “Configuring Lists,” on page 19](#) and [Section 4.2, “Sorting Lists,” on page 20](#).
- 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 20](#).
- 3 Click *Remove* in the toolbar to remove the mapping.
- 4 Click *Apply* to save the changes.
You can add or remove mappings in the same session. Add or remove the desired mappings, then click *Apply*.
- 5 Click *OK* in the confirmation message.
Any users assigned to the role the managed system authorizations are mapped to are automatically removed from the managed system authorizations.

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.

- ♦ [Section 3.1, “Creating Roles,” on page 17](#)
- ♦ [Section 3.2, “Removing Roles,” on page 17](#)
- ♦ [Section 3.3, “Editing Role Information,” on page 17](#)



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 cannot 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

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.


- ◆ [Section 4.1, “Configuring Lists,” on page 19](#)
- ◆ [Section 4.2, “Sorting Lists,” on page 20](#)
- ◆ [Section 4.3, “Refreshing Lists,” on page 20](#)
- ◆ [Section 4.4, “Adjusting the Width of the Roles and Mapping Lists,” on page 21](#)

4.1 Configuring Lists

The Identity Vault and the managed 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.

- ◆ [Section 4.1.1, “Filtering the Identity Vault Roles List,” on page 19](#)
- ◆ [Section 4.1.2, “Filtering the Authorizations List,” on page 19](#)
- ◆ [Section 4.1.3, “Customizing the Mapping List,” on page 20](#)

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:

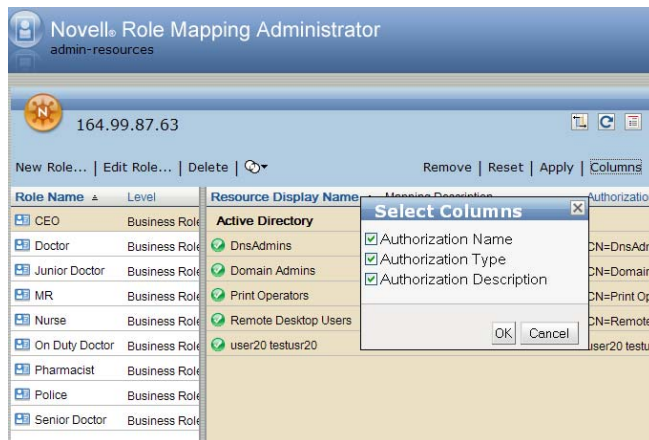
Desired Result	ID Field	Description Field	Type Field
All authorizations that start with S	S*	Blank	Blank
All authorizations that start with S and whose type is Role	S*	Blank	Role

3 Click *OK* to apply the filter.

4.1.3 Customizing the Mapping List

The Role Mapping Administrator displays all the columns, including *Resource Name*, *Mapping Description*, *Authorization Name*, *Authorization Type*, and *Authorization Description* by default. You can hide the *Authorization Name*, *Authorization type*, and *Authorization Description* columns.

1 Click *Columns* to open the Select Columns dialog box.



2 Select or deselect the columns that you want to display, then click *OK*. The Role Mapping Administrator stores the column setting for subsequent sessions.

4.2 Sorting Lists

You can sort the *Identity Vault Roles* list by clicking the *Name* or *Level* columns in the Roles panel. This sorts the roles and authorizations from A to Z or from Z to A.


You can sort the *Authorizations* list, by clicking on the *Authorization Name* or the *Authorization Type* columns in the Authorizations panel.

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 21](#)
- ◆ [Section 4.3.2, “Refreshing the Authorizations List,” on page 21](#)


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 managed 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 managed 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 managed 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.
Role 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`.

- ♦ [Section 6.1, “Troubleshooting the Role Mapping Administrator,”](#) on page 25

6.1 Troubleshooting the Role Mapping Administrator

A Tomcat port conflict error occurs when you are starting the Role Mapping Administrator

Explanation: If you have the Role Mapping Administrator and the Roles Based Provisioning Module installed on the same server, the Tomcat shutdown ports conflict.

Action: To solve the problem:

- 1 Stop Role Mapping Administrator.
- 2 Edit the `/installation_directory/idmrmmap/tomcat/conf/server.xml` file.
- 3 Find the line `<Server port="8006" shutdown="SHUTDOWN">`.
- 4 Change the port to another port that is not in use.
- 5 Save the changes, then restart the Role Mapping Administrator by using the following command from the `<rma_install_path>/rma/` location.

Linux: `./start.sh`

Windows: `start.bat`

The Role Mapping Administrator uses the following default ports:

- ♦ **8081:** Used for HTTP access.
- ♦ **8443:** Used for secure HTTP access.
- ♦ **8006:** Used by the Tomcat application server.

The Role Mapping Administrator is not accessible when Tomcat is already installed in a system using port 8443

Source: See the `catalina.out` file from the `<rma_install_path>/rma/tomcat/logs/` location to find the `java.net.BindException: Address already in use<null>:8080` error.

Action: To solve the problem:

- 1 Stop the Role Mapping Administrator.
- 2 Change the port. Refer to the Section 3.3.1 Changing Port Number for more information.
- 3 Restart the Role Mapping Administrator.

You cannot authenticate to the Role Mapping Administrator

Action: 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.

You cannot access the Role Mapping Administrator after a successful installation

Action: Use the following procedure to resolve the problem:

- 1 Start the Role Mapping Administrator after installing it.
- 2 Check the `<rma_install_path>/rma/tomcat/conf/logging.properties` file. Use a different port if the port is already in use.
- 3 Stop the Role Mapping Administrator.
- 4 Change the port to another port in the `<rma_install_path>/rma/tomcat/conf/server.xml` file.
- 5 Start Role Mapping Administrator.

Expected roles are not being displayed

Explanation: Not all of the roles from the Roles Based Provisioning Module are being displayed, or too many roles are being displayed.

Action: If a user belongs to the Role Module Administrator role in the Roles Based Provisioning Module, the Role Mapping Administrator uses the proxy admin credentials defined in the Role Mapping Administrator configuration. Verify that the proxy admin user has the correct rights to the Identity Vault that contains the User Application driver.

Expected roles from the SAP Portal are not being displayed

Explanation: When you load authorizations from the SAP Portal system, groups that start with SAP_, are not being displayed.

Action: If the SAP Portal is using an ABAP server as the Authentication DataSource, then by default the UME cannot assign ABAP roles (which appear as groups in the SAP Portal) directly to ABAP users. Most of these ABAP roles begin with SAP_. The SAP Portal driver is configured to filter these roles when the Role Mapping Administrator queries for the available groups.

The filter is an XML filter element that is appended to the entitlement configuration object. By default, the filter element contains an attribute type that has a value of exclude. The filter element holds individual filters. Each filter contains the following attributes:

- ◆ **read-attr:** The source for the match.
- ◆ **source-name:** The attribute on which the regular expression is evaluated against.
- ◆ **regex:** The regular expression that is used.

You can modify the regular expression value or remove the value to change how the Role Mapping Administrator filters the results. By default, the regular expression is ^SAP_, which is evaluated as start with SAP underscore.

Figure 6-1 XML Filter Element

```
append XML element("filters", "{$xml/entitlement-configuration/entitlements/entitlement[last()]}")
set XML attribute("type", "{$xml/entitlement-configuration/entitlements/entitlement[last()]/filters[last()}" exclude")
append XML element("filter", "{$xml/entitlement-configuration/entitlements/entitlement[last()]/filters[last()}" )
set XML attribute("source", "{$xml/entitlement-configuration/entitlements/entitlement[last()]/filters[last()}/filter[last()}", "read-attr")
set XML attribute("source-name", "{$xml/entitlement-configuration/entitlements/entitlement[last()]/filters[last()}/filter[last()}", "CN")
set XML attribute("regex", "{$xml/entitlement-configuration/entitlements/entitlement[last()]/filters[last()}/filter[last()}", "^SAP_")
```

To change the filter so you can see all groups:

- 1 Using Designer or iManager, edit the SAP Portal driver policy pub-its-InitEntitlementConfigurationResource on the Publisher channel.
- 2 In Policy Builder, select the Entitlements rule.
- 3 In the for each action, find the XML element of the filter.
- 4 Change the type attribute value from exclude to include.
- 5 Remove the regular expression value of ^SAP_.
- 6 Save the changes, then restart the driver to have the changes take effect.

Authorizations are not being displayed

Explanation: Even after the authorizations being loaded, they are not displayed in the *Authorizations* panel.

Possible Cause: One of the reasons for this issue could be because of shutting down the Tomcat server by pressing the CTRL+C key combination, which stops the Tomcat server but not the Role Mapping Administrator database server.

Action: To shut down the Role Mapping Administrator service, use the `stop.sh/stop.bat` command from the `<rma_install_path>/rma/` directory.

Drivers are not being displayed

Explanation: After configuring the new driver for role mapping, the driver is not displayed in the *Authorizations* panel.

Possible Cause: One of the reasons for this issue could be because of shutting down the Tomcat server by pressing the CTRL+C key combination, which stops the Tomcat server but not the Role Mapping Administrator database server.

Action: To shut down the Role Mapping Administrator service, use the `stop.sh/stop.bat` command from the `<rma_install_path>/rma/` directory.