# NetIQ Identity Manager Catalog Administrator

## NetIQ Identity Manager

**January 2016**

NetIQ.

## Legal Notice

# Contents

# About this Book and the Library

The *Catalog Administrator User Guide* provides conceptual information about the Catalog Administration feature of the NetIQ Identity Manager product. This book defines terminology and includes implementation scenarios.

## Intended Audience

This book provides information for individuals responsible for understanding administration concepts for roles and resource management across the enterprise, and implementing a secure, distributed administration model.

## Other Information in the Library

The library provides the following information resources:

**Identity Manager Framework Installation Guide**

Provides detailed planning and installation information for Identity Manager components.

**Identity Manager Overview Guide**

Provides conceptual information about Identity Manager. This book also provides an overview of the various components and many administration tasks.

**Identity Manager Catalog Administration Release Notes**

Provides overview information and known issues for this release of Identity Manager Catalog Administrator.

**Identity Manager Catalog Administration Online Help**

Provides information about Identity Manager Catalog Administrator in an online Help format.

# About NetIQ Corporation

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

## Our Viewpoint

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

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

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

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

## Our Philosophy

**Selling intelligent solutions, not just software**

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

**Driving your success is our passion**

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

## Our Solutions

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

# Contacting Sales Support

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

| | |
|---|---|
| **Worldwide:** | www.netiq.com/about_netiq/officelocations.asp |
| **United States and Canada:** | 1-888-323-6768 |
| **Email:** | info@netiq.com |
| **Web Site:** | www.netiq.com |

# Contacting Technical Support

For specific product issues, contact our Technical Support team.

| | |
|---|---|
| **Worldwide:** | www.netiq.com/support/contactinfo.asp |
| **North and South America:** | 1-713-418-5555 |
| **Europe, Middle East, and Africa:** | +353 (0) 91-782 677 |
| **Email:** | support@netiq.com |
| **Web Site:** | www.netiq.com/support |

# Contacting Documentation Support

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

# Contacting the Online User Community

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

# 1 Overview

NetIQ Identity Manager Catalog Administrator is a Web-based tool that allows business and security analysts manage roles and resources in Identity Manager. Though catalog is not a unique database or a set of files, it encompasses all information about roles, resources, and relationship between them. Catalog Administrator allows you to view and manage permission assignments across various connected systems in organizations managed by Identity Manager. You can also design roles and map them with resources across connected systems.

You can use Catalog Administrator to:

- Associate resources to roles within your organization
- Create new roles and assign other roles to them
- Create separation of duties (SoD) constraints to manage potential conflicts between roles
- Find out which role or resource is associated with which container
- Create new resources, either from an entitlement or without an entitlement
- Modify existing roles and resources

Identity Manager Catalog Administrator leverages the Identity Manager resource model and provides you an up-to-date and easy-to-manage view of an organization’s roles and resources. Catalog Administrator gets role and resource information from the User Application driver.

## 1.1 Understanding Roles

A role defines a set of permissions related to one or more target systems or applications. The Identity Manager roles system includes several different built-in roles that provide different levels of access rights to the role-based provisioning system. For example, someone assigned to administer the Roles Module has unlimited scope within the Roles system, but someone assigned to just manage roles is limited to specifically designated users, groups, and roles.

## 1.2 Understanding Resources

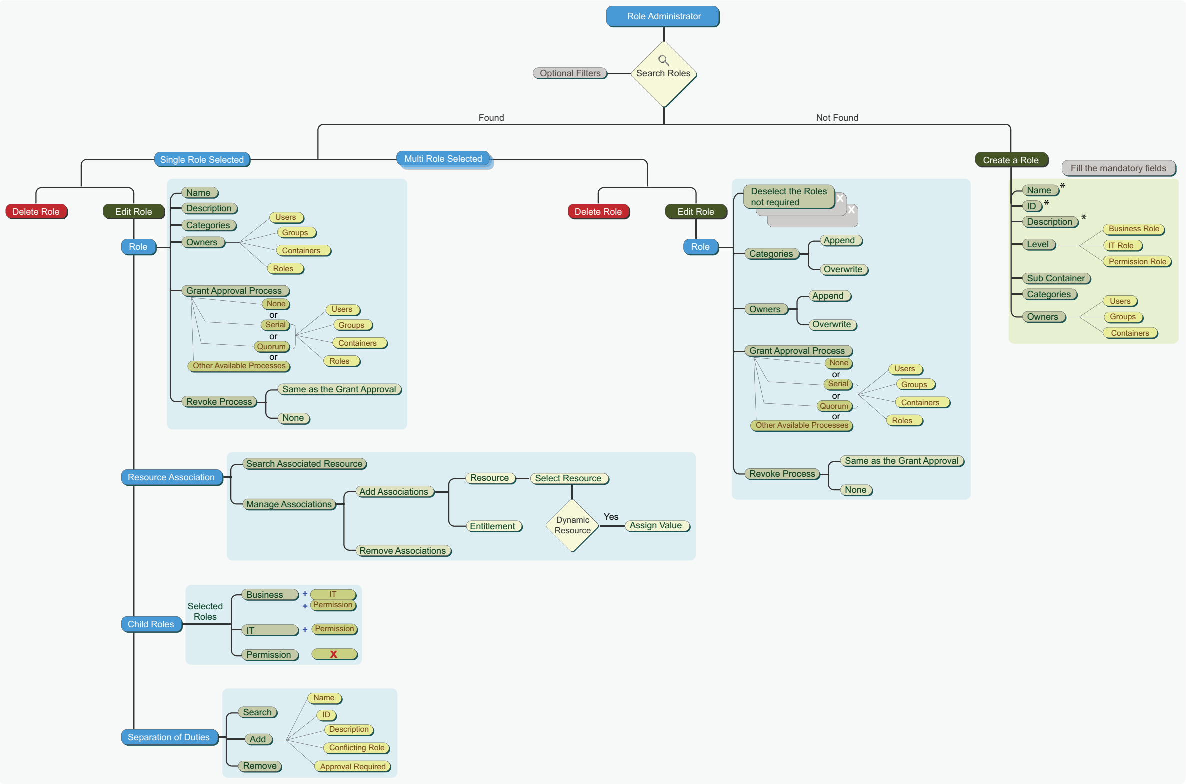
The Identity Manager drivers maintain the permission model by collecting account IDs and permissions assignments from external systems. Identity Manager calls these permissions entitlements. Identity Manager uses entitlements to provide users with access to resources in connected systems. For more information about entitlements, see Identity Manager Entitlements Guide..

Entitlement model can become technical and difficult for business users to manage. The Identity Manager Resource model simplifies the entitlement model by providing you a convenient way to do resource-based provisioning. A resource is any digital entity such as a user account, computer, or database that a business user needs to be able to access. A resource definition can have no more than one entitlement bound to it. A resource definition can be bound to the same entitlement more than once, with different entitlement parameters for each resource.

The resource model makes it easy for business managers to make decisions about who should get access to what. The resource model also allows IT personnel to quickly see what users have access to what, what resources are available, and which rights and resources are assigned to what roles. For more information, see “Introducing Roles and Resources” in the *User Application: User Guide*.

Figure 1-1 illustrates the role administration scenario. For more information about roles, see Chapter 3, “Role Administration,” on page 17.

***Figure 1-1*** *Role Administration*



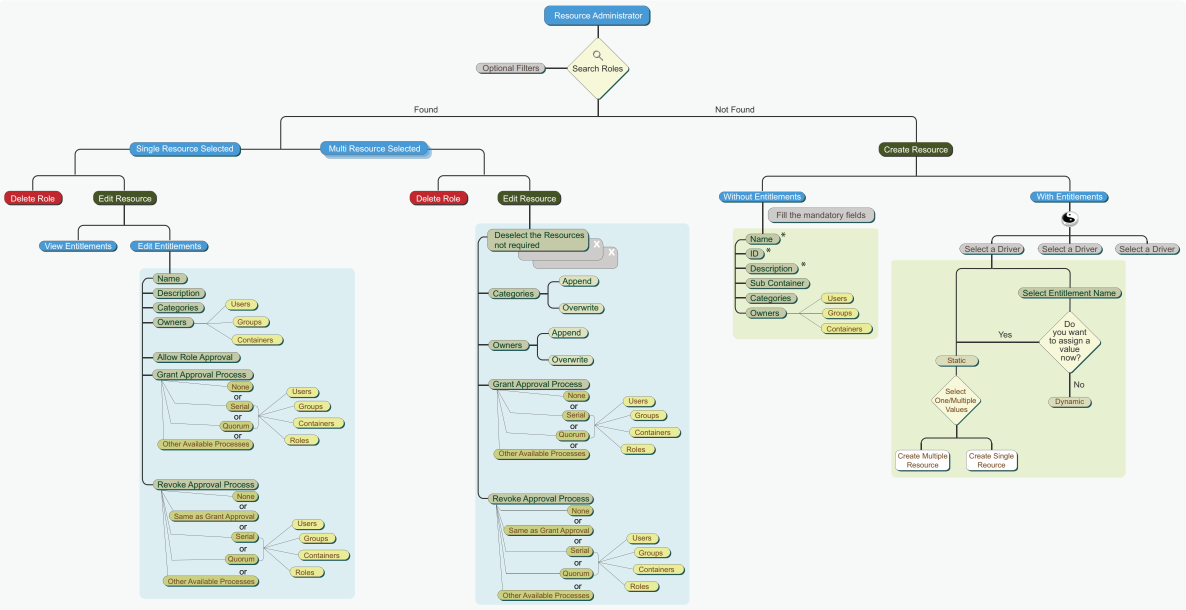
You can leverage Catalog Administrator to create and manage roles by defining several aspects of roles such as role levels, categories, and owners. You can also define child roles and separation of duties constraints for roles. When the Role Administrator sets up a role, the Resource Administrator can associate a resource to this role.

As a Role Administrator, you can perform the following tasks in Catalog Administrator:

- Create, remove, and modify roles
- Modify role relationships for roles
- Create, remove, and modify separation of duty constraints
- Browse the list of roles

Figure 1-2 illustrates the resource administration scenario. For more information about resources, see Chapter 4, “Resource Administration,” on page 21.

***Figure 1-2*** *Resource Administration*



As a Resource Administrator, you have the ability to create, modify, delete, browse resources or associate resources to an individual role or a role that is part of other role, group, or a container in an organization. You can associate only resources to a role.

## 1.3 What is Different in Catalog Administrator?

Catalog Administrator and Role Mapping Administrator are different in many ways. Catalog Administrator provides improved functionality over Role Mapping Administrator. Feature distinction between them is illustrated in a graphical representation. Figure 1-3 lists how role management is handled in Catalog Administrator and Role Mapping Administrator.

***Figure 1-3** Differences in Role Functionality*

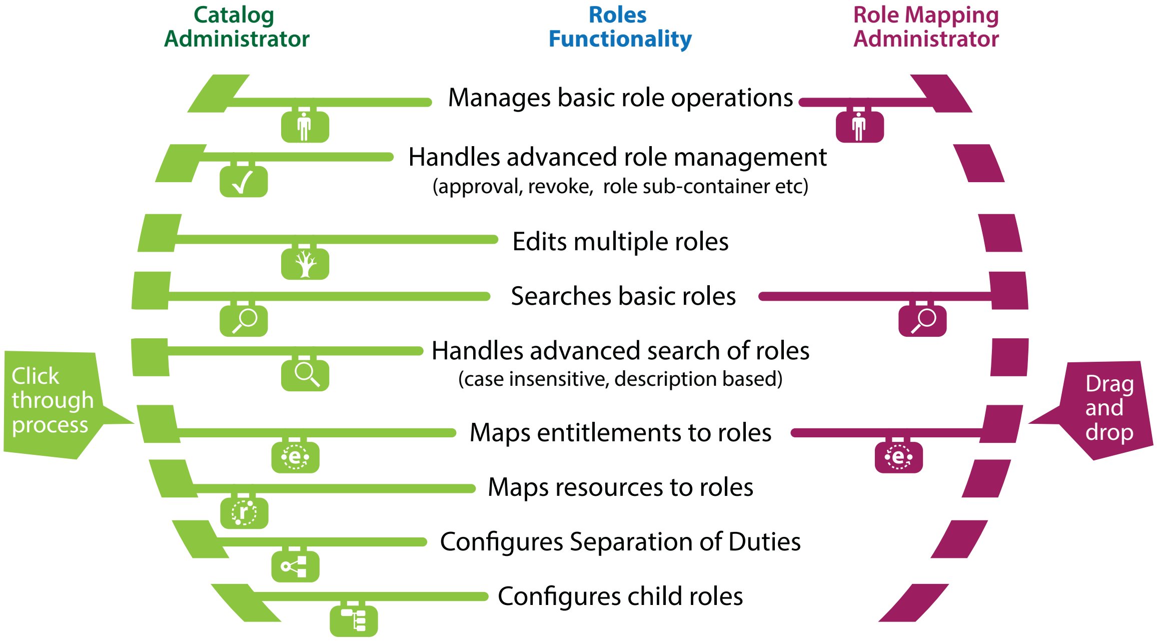

Catalog Administrator
Roles Functionality
Role Mapping Administrator
Manages basic role operations
Handles advanced role management
(approval, revoke, role sub-container etc)
Edits multiple roles
Searches basic roles
Handles advanced search of roles
(case insensitive, description based)
Maps entitlements to roles
Maps resources to roles
Configures Separation of Duties
Configures child roles
Click through process
Drag and drop

Figure 1-4 lists how resource management is handled in Catalog Administrator and Role Mapping Administrator.

***Figure 1-4** Differences in Resource Functionality*

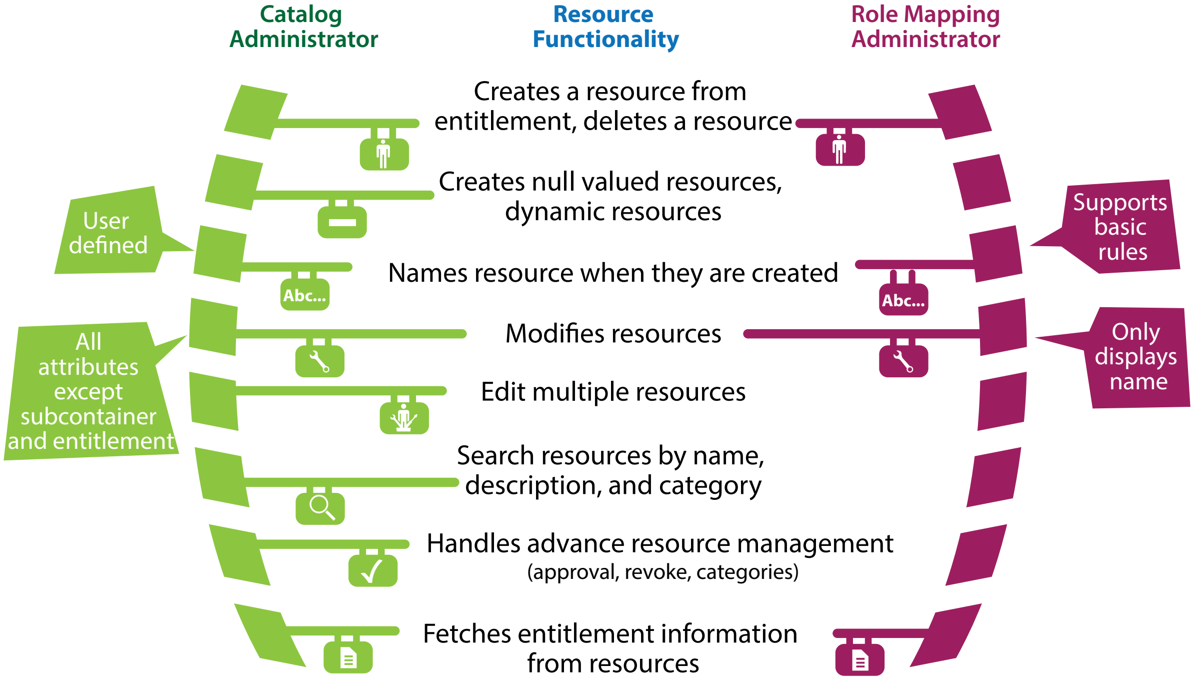
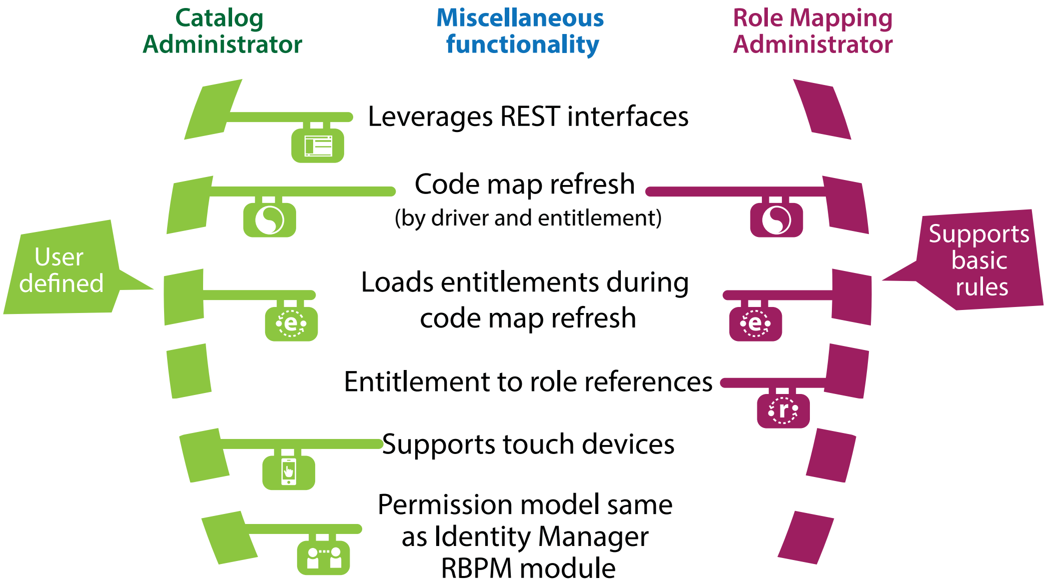

Catalog Administrator
Resource Functionality
Role Mapping Administrator
Creates a resource from entitlement, deletes a resource
Creates null valued resources, dynamic resources
Names resource when they are created
Abc...
Modifies resources
Edit multiple resources
Search resources by name, description, and category
Handles advance resource management
(approval, revoke, categories)
Fetches entitlement information from resources
User defined
All attributes except subcontainer and entitlement
Supports basic rules
Only displays name

Figure 1-5 lists comparison of other functionality in Catalog Administrator and Role Mapping Administrator.

***Figure 1-5** Differences in Other General Functionality*


Catalog Administrator
Miscellaneous functionality
Role Mapping Administrator
Leverages REST interfaces
Code map refresh
(by driver and entitlement)
User defined
Supports basic rules
Loads entitlements during code map refresh
Entitlement to role references
Supports touch devices
Permission model same as Identity Manager RBPM module

# 2 Installing

Identity Manager 4.5 includes a new Web-based tool called Catalog Administrator. Catalog Administrator simplifies the usage of entitlements from Identity Manager connected systems in the organization by associating them to Resources. You can manage Roles and Resources, associate Resources to Roles, and manage Separation of Duties conflicts between Roles. Catalog Administrator gets the Role and Resource information from the User Application driver.

## 2.1 Product Requirements

For a list of the product requirements and other prerequisites, see “Prerequisites and Considerations for Installing the Identity Applications” in the *NetIQ Identity Manager Setup Guide*.

## 2.2 Installing Catalog Administrator

The identity applications installation includes Catalog Administrator.

NetIQ recommends that you review the prerequisites and computer requirements for identity applications before you begin the installation process. For more information about configuring the User Application environment, see the User Application Administration Guide. For more information see “Installing the Identity Applications ” in the *NetIQ Identity Manager Setup Guide*.

## 2.3 Uninstalling Catalog Administrator

Uninstall Catalog Administrator only if you also want to uninstall all components of Identity Manager Home. Because Catalog Administrator is used along with the Identity Manager Home, you do not normally uninstall the component by itself. However, to stop using Catalog Administrator, remove the `rra.war` file. If you remove `IDMProv.war`, Identity Manager Home stops working.

# 3 Role Administration

A role defines a set of permissions related to one or more target systems or applications. For example, a user administrator role might be authorized to reset a user's password, while a system administrator role might have the ability to assign a user to a specific server.

You must define roles in Catalog Administrator. This tool allows you to create roles, establish roles hierarchy, define role relationships, and perform administrative actions on the roles. When creating a role, you must not include the following characters in the **Name** and **Description** fields for the role: < > , ; \ " +  # = / | & *

Except **Role Level** and **Subcontainers**, you can modify all other parameters of a role. Once you have defined a role, you cannot change the level of the role. To change the level of the role, you must delete the role and create it again. With Catalog Administrator, you can select multiple roles for modify and delete operations.

You can access the Role Administrator page from the Identity Manager Home and Provisioning Dashboard page. The Role Administrator page displays a list of currently defined roles in your organization. It also allows you to define new roles and manage existing ones. When you select a role from the list of roles, the page displays information about that role.

To change information associated with a role, you can either select it from the list of roles or search for it using **Filter**. The Roles page displays the details associated with the role.

The following sections contain information about operations that you can perform in the Role Administration page.

- Section 3.1, “Searching for Roles,” on page 17
- Section 3.2, “Role Ownership,” on page 18
- Section 3.3, “Role Approval and Revocation,” on page 18
- Section 3.4, “Role Hierarchy,” on page 18
- Section 3.5, “Resource Associations,” on page 19
- Section 3.6, “Separation of Duties Constraints,” on page 19
- Section 3.7, “Editing Multiple Roles at Once,” on page 20

## 3.1 Searching for Roles

Click **Filter** icon in the Role Administration page. The **Filter** dialog displays **Role Categories** and **Role Level** fields that you can use to filter the roles.

When you are doing a simple search for a role, you can type in part of a role name or a description to display a list of roles that meet the criteria. When you enter some characters strings, called “stop words”, the search does not display the associated item. Also, the browser’s built-in search mechanism cannot search through the generated list of items. The filter is a more robust search feature that you should use to find all items that meet your search criteria.

## 3.2 Role Ownership

When you define a role, you have the option to designate one or more owners for that role. A role owner is the person who is designated as the owner of the role definition. The role owner can be a user, a group, or a container. The role owner does not automatically have the authorization to administer changes to a role definition. In some cases, the owner must ask a Role Administrator to perform any administration actions on the role.

## 3.3 Role Approval and Revocation

After you create a role, you can modify it to define the approval process for that role. An approver can be a user, a group, a container, or a specific role.

To change the approval process for a role, select it from the list of roles or search for it using **Filter**. The page displays information for the role. You can define the approval process for a role using one of the following options:

- **Serial Approval:** Specify multiple approvers, and define the order by selecting an approver and moving that approver earlier or later in the order by clicking the arrows at the right of the approval list.
- **Quorum Approval:** Specify the approvers, then use the slide bar to specify the percent of those approvers that are required to grant access.
- **Other Available Processes:** Specify the other approval process that you want to use. This approval process must be available for use in Catalog Administrator.

**NOTE:** You must set up this approval process in Identity Manager Designer. For more information, see User Application: Design Guide..

If you choose **None**, no approvers are required for the role.

You can choose to have a revoke process or not. The revocation process can match the approval process. Also, you can define a different revocation process. Select the **Revoke Process** check box if you want the revocation process to match the approval process. If you define a different process, you are presented with same options that you have for defining the approval process.

## 3.4 Role Hierarchy

Role levels define role hierarchy. The roles hierarchy supports three levels. Roles defined at the highest level (called Business Roles) define operations that have business meaning within the organization. Mid-level roles (called IT Roles) supports technology functions. Roles defined at the lowest level of the hierarchy (called Permission Roles) define lower-level privileges.

A higher-level role automatically includes privileges from the lower-level roles that it contains. For example, a Business Role automatically includes privileges from the IT Roles that it contains. Similarly, an IT Role automatically includes privileges from the Permission Roles that it contains.

Role relationships are not permitted between peer roles within the hierarchy. In addition, lower-level roles cannot contain higher-level roles.

You can modify the label used for each role level in the User Application by defining localized strings for the level’s **Name** and **Description** in the role configuration editor.

To associate a role with another role, select it from the list of roles or search for it using **Filter**. The page displays information about the role. A child role must have a lower role level than the parent role, and the parent role is automatically assigned the privileges assigned to the lower-level roles.

## 3.5 Resource Associations

A role is only useful when it is defined to have access to a resource, and a resource is only useful as an entity that a user has access to. Therefore, you must associate roles and resources to make them useful. A user assigned to a role has access to all resources that are associated with that role.

To associate a resource with a role,

1. Go to the Roles Administration page.
2. Select the role you want to map from the list of roles.
3. Click **Resource Associations**, then click **Manage Associations**.
4. Select **Resources** or **Entitlements** to associate to a role.

   You are presents with two options: **Resources** and **Entitlements**. You can bind entitlements with a role. If a role has an entitlement bound to it, it allows you to see the entitlement mapping.

   or

   Search for a resource by drivers installed in your Identity Manager environment. You can type in part of a driver name to display a list of resources that meet the criteria.
5. (Conditional) If you select **Resources**, you can either search for a resource or select it from the list of available resources.
6. (Conditional) If you select **Entitlements**, select the driver for granting entitlements to this role from the list of available drivers. Based on the type of the role, the list of entitlements is displayed in the page. Select an entitlement to grant for this role. Also, you can search for values associated with an entitlement. To do this, you can either enter text in the **Entitlements Values** search field for the entitlement you are searching for.
7. Click **Add Association.**
8. Enter a mapping description for the resource or entitlement you selected.
9. Click **Apply** and **Close** to return to the Roles Administration page.

## 3.6 Separation of Duties Constraints

Separation of duties is an important aspect of an organization’s security controls because it helps prevent fraud and user error related to user access. In a separation of duties constraint, the conflicting roles must be at the same level in the roles hierarchy.

An SoD constraint represents a rule that makes two roles mutually exclusive, unless there is an exception allowed for that constraint. You can define whether exceptions to the constraint are always allowed or are only allowed through an approval flow. When a role assignment results in a potential separation of duties conflict, the initiator has the option to override the separation of duties constraint, and provide a justification for making an exception to the constraint.

You can add or delete separation of duties constraints.

To add separation of duties constraints, do the following:

1. Go to the Role Administration page.
2. Click **Manage Constraints**.

**3** In the Add Separation of Duties page, fill in the mandatory fields.

**4** Click **Apply** and **Close** to return to the Roles Administration page.

## 3.7 Editing Multiple Roles at Once

Catalog Administrator provides you the ability to perform actions on multiple roles as a group instead of requiring you to repeat those actions on each role individually. Select the roles you want to manage from the list of roles. You can change **Categories, Owners, and Approval Details** for the roles you selected. Also, you can append or overwrite values for **Categories** and **Owners** for the selected role.

# 4 Resource Administration

A resource is any digital entity such as a user account, computer, or database that a business user needs to be able to access. Each resource is mapped to an entitlement. For more information, see Section 1.2, “Understanding Resources,” on page 9.

Catalog Administrator allows you to create entitlement-based dynamic resources and non-valued resources (without entitlements). It also allows you to create static resources. You can modify **Categories, Owners**, and **Approval Process** for a resource. With Catalog Administrator, you can select multiple resources for modify and delete operations.

You can access the Resource Administrator page from the Identity Manager Home and Provisioning Dashboard page. The Resource Administrator page displays a list of currently defined resources in your organization.

To change information associated with a resource, you can either select it from the list of resources or search for it using **Filter**. The Resources page displays information about that resource.

The following sections contain information about operations that you can perform in the Resource Administration page.

- Section 4.1, “Searching for Resources,” on page 21
- Section 4.2, “Creating Resources,” on page 21
- Section 4.3, “Modifying Resources,” on page 22
- Section 4.4, “Resource Approval and Revocation,” on page 22
- Section 4.5, “Editing Multiple Resources at Once,” on page 23

## 4.1 Searching for Resources

Click **Filter** icon in the Resource Administration page. The **Filter** dialog displays **Resource Categories** field that you can use to filter the resources.

When you are doing a simple search for a resource, you can type in part of a resource name or a description to display a list of resources that meet the criteria. When you enter some characters strings, called “stop words”, the search does not display the associated item. Also, the browser’s built-in search mechanism cannot search through the generated list of items. The filter is a more robust search feature that you should use to find all items that meet your search criteria.

## 4.2 Creating Resources

You can create a non-valued resource (without entitlements) and entitlement based static or dynamic resource. If you choose to create a resource with entitlements, you have the following choices:

- Select the driver from the list of available drivers installed in your Identity Manager environment. When you click the tree view of the driver you selected, the entitlements associated with the driver are displayed. Select an entitlement and specify a value for it. If you select **Entitlement Association**, Catalog Administrator creates a dynamic resource. You must enter a description for the entitlement for the resource to be created. Ensure that you do not include the following characters in the **Name** and **Description** fields for the resource: `< > , ; \ " +  # = / | & *`

After creating a dynamic resource, you can specify the entitlement value when the resource is requested using Identity Manager Home and Provisioning Dashboard or when you are associating the resource with a role using Catalog Administrator.

**NOTE:** Select **Allow this resource and entitlement to be assigned multiple times with different values** only if this resource will be requested by business users multiple times with different values.

This option is displayed for User Account entitlement though it should not be because User Account entitlement is a single-valued entitlement.

- Select the driver from the list of available drivers installed in your Identity Manager environment and select an entitlement value from the list. The new static resource is associated with this entitlement value. If you select multiple entitlement values for creating a resource, Catalog Administrator automatically creates only one resource for each entitlement value.

To create a resource without entitlements, you must specify the mandatory fields to create it. The newly added resources are added to the organizational resources and available for business managers.

## 4.3 Modifying Resources

You can modify several parameters of a resource. You can select a resource whose parameters you want to change from the list of available resources or search for it in the filter dialog. The tool allows you to modify all parameters that are displayed in the page.

You can modify more than one resources at one time. For more information, see Section 4.5, “Editing Multiple Resources at Once,” on page 23.

## 4.4 Resource Approval and Revocation

After you create a resource, you can modify the resource information and define the approval process for it. You can choose the role approval process to override the resource approval process.

To change the approval process for a resource, select it from the list of resources or search for it using **Filter**. The page displays information for the resource. A resource approver can be a user, a group, a container, or a specific role. You can define the approval process for a resource using one of the following options:

- **Serial Approval:** Specify multiple approvers, and define the order by selecting an approver and moving that approver earlier or later in the order by clicking the arrows at the right of the approval list.
- **Quorum Approval:** Specify the approvers, then use the slide bar to specify the percent of those approvers that are required to grant access.
- **Other Available Processes:** Specify the other approval process that you want to use. This approval process must be available for use in Catalog Administrator.

**NOTE:** You must set up this approval process in Identity Manager Designer. For more information, see User Application: Design Guide.

If you choose **None**, no approvers are required for assigning the resource.

You can revoke the resource assignment by choosing one of the available options. The resource revocation process can match the resource approval process, or you can define a different process. Select the **Same as Grant Approval** option if you want the revocation process to match the approval process. If you define a different process, you are presented with same options that you have for defining the approval process.

## 4.5 Editing Multiple Resources at Once

Catalog Administrator provides you the ability to perform actions on multiple resources as a group instead of requiring you to repeat those actions on each resource individually. You need to select the resources you want to manage. You have the option to change **Owners, Categories, Grant Approval Process**, and **Revoke Process** for the resources you selected. Also, you can append or overwrite values for **Categories** and **Owners** for the selected resource.

# 5 Managing Teams

A team identifies a group of users and determines who can manage provisioning requests and approval tasks associated with this team. The team definition consists of a list of team requesters, team recipients, and team options, as described below:

- A team requester is a user who can administer requests and tasks for the team. Team requesters can be users or groups.
- The team recipients are those users who are allowed to participate on the team. Team recipients can be users, or groups within the directory. Alternatively, they can be derived through directory relationships. For example, the list of members could be derived by the manager-employee relationship within the organization. In this case, the team recipients would be all users that report to the team manager.

  **NOTE:** The Provisioning Application Administrator can configure the directory abstraction layer to support cascading relationships so that multiple levels within an organization can be included within a team. The number of levels to include is configurable by the administrator.

- The team options determine the provisioning request scope, which specifies whether the team requesters can act on an individual provisioning request, one or more categories of requests, or all requests.

The Provisioning Application Administrator can perform all team management functions.

The teams you define are stored locally in the Designer project's `Provisioning\AppConfig\TeamDefs` directory.

Although a team can sometimes refer to a group in the Identity Vault, a team is not the same thing as a group. When you define a group in the Identity Vault, you identify a set of users that have something in common. However, the group does not automatically have the capabilities of a team within the User Application. To take advantage of the team capabilities within the User Application, you must define a team that points to the group.

## 5.1 Managing Teams

Identity Manager includes a new Team Configuration page that allows you to create and manage teams and define permissions for the teams. The Team Configuration page is accessible to the roles listed in Table 5-1.

***Table 5-1** Role Access to the Team Configuration Page*

| User | Capabilities |
|---|---|
| Security Administrator | Can perform all operations on the Team Configuration page. |
| Domain Administrator | Can define a team for the domain (Role, Resource, and PRD) over which the administrator has authority. |
| Team Requester | Can view a team definition for which the user is configured to be the requester. The team requester can only read the team definition. This user cannot modify the team configuration. |

## 5.2 Accessing the Team Configuration Page

You can access the Team Configuration page in the following ways:

- Click the Manage Teams link from the Identity Manager Home page
- Launch the Team Configuration page from a Web browser on your workstation

To launch the Team Configuration page in your Web browser:

1. Open a Web browser and navigate to one of the following URLs, depending on whether SSL is configured in your environment:
   - `http://IDMServer:application_server_port_number/rra_context/teams`
   - `https://IDMServer:application_server_port_number/rra_context/teams`

   Where `IDMServer` is the fully-qualified name or IP address of your Identity Manager Roles

   Based Provisioning Module server and `rra_context` is the context you provided while deploying the Catalog Administrator `war` on your application server. If you do not know the address you need to use, contact your Identity Manager administrator.
2. Provide your Identity Manager user name and password.

   **NOTE:** You cannot access the Team Configuration page using an account that includes any of the following characters in the name: \ /, * ? $ # +
3. Select **Login**.

   The Team Configuration page displays.

## 5.3 Viewing Team Configurations

To view existing team configurations, access the Team configuration page as instructed in Section 5.2, “Accessing the Team Configuration Page,” on page 26. The Team Configuration page displays a list of currently defined teams in your organization.

**NOTE:** Identity Manager allows you to take specific actions in the Team Configuration page depending on your role. For more information, see Table 5-1.

The page allows you to create new teams and manage the existing teams. When you select a team from the list of existing teams, the page displays information about that team. Also, the page allows you to perform the following settings:

- Section 5.3.1, “Sorting the Team List,” on page 26
- Section 5.3.2, “Searching the Team List,” on page 27

### 5.3.1 Sorting the Team List

The default sort column is the Name column. To sort the team list, click the pyramid-shaped sort indicator. When you sort in the ascending order, the sort indicator is shown in its normal, upright position. When you sort in the descending order, the sort indicator is upside down.

### 5.3.2 Searching the Team List

Type in part of a team name or a description to display a list of teams that meet the criteria in the Search dialog at the top of the Team Configuration display.

To refresh the page, click **Refresh**. This cleans the cache containing the team list and fetches the latest team list from the Identity Vault and rebuilds the cache.

## 5.4 Creating a New Team

To create a new team:

**1** Click the **Create Team** button at the top of the Team page.

The New Team dialog displays.

**2** Provide a name and description for the team.

To specify a localized name and description for the team, click the arrow near the **Name** and **Description** field labels in the form.

**NOTE:** The Team page allows you to create multiple teams with the same name. However, Identity Manager recommends that you define teams with unique names.

**3** In the **Requesters** field, select the users and groups that will be the requesters for the team.

**4** To include the selected requesters as recipients of the permissions that will be requested, select the **Include the selected requesters in the recipients list** check-box.

**5** In the **Recipients** field, choose the objects for which you are making a request.

The following objects are supported in the team configuration:

- **All Users**
- **Relationship**
- **Members**

For more information about these objects, see Working with Relationships in the NetIQ User Application: Design Guide.

**6** Click **Apply** to preserve your team configuration settings.

After the team is saved, the **Permissions** section is added to the page, and the Team Permissions Configuration interface is displayed.

The Team Permissions Configuration interface includes buttons for adding new permissions, deleting permissions and refreshing the display. The **Permission**s section of the page does not include an Edit button because the details associated with each permission are shown in the **Permissions** list. If a particular team permission is not properly defined, you can simply delete the permission and add a new one in its place.

**7** To define the permissions for the team, click **Add Permission**.

This interface shows controls that apply to the domain selected for the team. These controls allow you to specify which objects are within the scope of the team and which permissions team recipients have with respect to these objects.

**8** Follow these steps to define permissions for a team that uses the Provisioning domain:

**8a** To include all provisioning request definitions, click the **All Provisioning Request Definitions** radio button.

**8b** To select provisioning request definitions individually, choose the **Select Provisioning Request Definitions** radio button and search for the provisioning request definitions.

**8c** After defining the scope for the team, choose the permissions you want to allow for each object by selecting the object and picking the desired permissions in the **Permissions** control.

The provisioning permissions are same for team configurations as for User Application administrator assignments.

| Permission | Description |
|---|---|
| Initiate PRD | Allows the user to initiate the selected provisioning requests.<br>**NOTE:** The Initiate PRD permission has no effect on the behavior of the Novell-installed PRDs for resources, roles, and attestation within the User Application, since these PRDs cannot be initiated directly from the User Application. However, this permission does control whether these PRDs can be initiated from a SOAP call. |
| Retract PRD | Allows the user to retract the selected provisioning requests when they are in progress. |
| View Running PRD | Allows the user to view the selected provisioning requests when they are in progress. |

For more information on the provisioning permissions, see Administrator Assignments in the NetIQ Identity Manager User Application: Administration Guide.

**8d** Click **Add** to save the permissions for the selected objects or containers.

To delete a permission, select the permission and click **Remove Permission**.

To refresh the list of permissions for the team, click **Refresh**.

**9** Follow these steps to define permissions for a team that uses the Role domain:

**9a** To include all roles in all levels in the roles hierarchy, choose **All Role Levels** in the **Role Sub Containers** radio button.

To include all roles at a particular level in the role hierarchy, expand **All Role Level**s and choose one of the following levels:

- **IT Role**
- **Business Role**
- **Permission Role**

  To include all roles in a particular sub container under the selected role level, expand the selected role level and select the sub container.

**9b** To select roles individually, choose **Select Roles** radio button and search for the roles.

**9c** After defining the role scope for the team, choose the permissions you want to allow for each object by selecting the object and picking the desired permissions from the **Permissions** control.

The following role permissions are supported in team configurations:

- **View Role**
- **Assign Role**
- **Revoke Role**

- **Assign Role to Group and Container**
- **Revoke Role from Group and Container**

These role permissions have the same behavior as for User Application administrator assignments.

| Permission | Description |
|---|---|
| View Role | Allows the user to view the selected roles.<br>This setting applies only at the container level. |
| Assign Role To User | Allows the user to assign users to the selected roles.<br>**IMPORTANT:** Only the Security Administrator can assign system roles on the Work Dashboard tab and the Roles and Resources tab. |
| Revoke Role From User | Allows the user to revoke user assignments for the selected roles. |
| Assign Role To Group And Container | Allows user to assign groups and containers to the selected roles. |
| Revoke Role From Group And Container | Allows the user to revoke group and container assignments for the selected roles. |

For more information, see Administrator Assignments in the NetIQ Identity Manager User Application: Administration Guide.

**9d** Click **Add** to save the permissions for the selected objects or containers.

To delete a permission, select the permission and click **Remove Permission**.

To refresh the list of permissions for the team, click **Refresh**.

**10** Follow these steps to define permissions for a team that uses the Resource domain.

**10a** To include all resources, click the **All Resources** radio button.

**10b** To select resources individually, choose the **Select Resources** radio button and search for the resources.

**10c** After defining the resource scope for the team, choose the permissions you want to allow for each object by selecting the object and picking the desired permissions from the **Permissions** control.

The following resource permissions are supported in team configurations:

- **View Resource**
- **Assign Resource**
- **Revoke Resource**

These resource permissions have the same behavior as for User Application administrator assignments.

| Permission | Description |
|---|---|
| View Resource | Allows the user to view the selected resources. |
| Assign Resource | Allows the user to assign users to the selected resources. |
| Revoke Resource | Allows the user to revoke user assignments for the selected resources. |

For more information on resource permissions, see Administrator Assignments in the NetIQ Identity Manager User Application: Administration Guide.

**10d** Click **Add** to save the permissions for the team.

To delete a permission, select the permission and click **Remove Permission**.

To refresh the list of permissions for the team, click **Refresh**.

## 5.5 Editing an Existing Team

To edit an existing team:

1. Select a previously defined team.

   **IMPORTANT:** The team definition is read-only for a team requester. Therefore, the team requester cannot modify the team configuration.

2. Make your changes to the team settings and click **Update**.

## 5.6 Refreshing the Team List

To refresh the page containing the list of existing teams, click **Refresh**. This cleans the cache containing the team list and fetches the latest team list from the Identity Vault and rebuilds the cache.

## 5.7 Deleting Teams

To delete an existing team, select the team and click **Delete**.

To delete multiple teams at the same time, select the teams from the list of available teams and click **Remove Teams**.

## 5.8 Defining the Navigation Access Permissions

As a Security Administrator, you need to set the access permissions for the **Manage Teams** item within the Identity Manager Home Page.

1. Log in to Identity Manager Home Page as a security administrator.
2. Click the **Navigation and Access** link.
3. Select **Home Page** in the **Navigation Area** under **Navigation Access Permissions**.
4. Select **Manage Teams** under **Navigation Item**.
5. Select the users in **Manage Teams Trustee** for whom you want to allow the access.
6. Click **Save**.

For more information, see Navigation Access Permissions in the NetIQ Identity Manager User Application: Administration Guide.

**NOTE:** Except the Security Administrator, the **Manage Teams** item is not visible to other users within the Identity Manager Home Page.