www.novell.com/documentation

Administrator Accounts and Rights Reference

ZENworks® 11 Support Pack 3

February 2014

Novell®

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.

Copyright © 2007-2014 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.
1800 South Novell Place
Provo, UT 84606
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

7 Rights Descriptions 39

About This Guide

This *ZENworks 11 SP3 Administrator Accounts and Rights Reference* explains how to create accounts for ZENworks administrators and control the rights associated with those accounts. An administrator's rights determine which management operations the administrator can perform in the ZENworks Management Zone. The guide includes the following sections:

Audience

This guide is intended for ZENworks administrators.

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.

Additional Documentation

ZENworks 11 SP3 is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the ZENworks 11 SP3 documentation web site (http://www.novell.com/documentation/zenworks113).

1 Overview

The following sections provide information to help you successfully manage ZENworks administrator accounts and rights for your Management Zone:

- Section 1.1, "Administrators," on page 9
- Section 1.2, "Administrator Groups," on page 10
- Section 1.3, "Roles," on page 10
- Section 1.4, "Rights," on page 10
- Section 1.5, "Rights Assignments and Conflict Resolution," on page 11

1.1 Administrators

During installation, a default ZENworks administrator account (named *Administrator*) is created. This account, which is a Super Administrator account, provides full administrative rights to the Management Zone and cannot be deleted.

Typically, you should create ZENworks administrator accounts for each person who will perform administrative tasks in your Management Zone. This allows you to give each administrator only the rights required to carry out his or her ZENworks management responsibilities. It also allows you to audit the changes each administrator makes in the zone.

There are two types of ZENworks administrator accounts:

- **ZENworks Super Administrator:** A Super Administrator account provides full administrative rights to the ZENworks Management Zone. The default Administrator account is a Super Administrator account. In addition to the default Administrator account, you should ensure that you have at least one other Super Administrator account. This provides redundancy in case the password for the Administrator account is forgotten or lost.
- **ZENworks Administrator:** A standard ZENworks administrator account can provide full administrative rights (like a Super Administrator account), but typically is used to limit an administrator's rights to only those administrative tasks he or she needs to perform.

  For example, you might create an administrator account that limits the administrator to discovering and registering devices in the Management Zone; an account that only allows the administrator to assign bundles to devices; or, an account that only allows the administrator to perform asset management tasks such as contract, license, and document management.

For information about creating administrator accounts, see Chapter 3, "Managing Administrator Accounts," on page 15.

1.2 Administrator Groups

An *administrator group* is a collection of administrators. The administrators receive all rights assigned to the group. There are two types of administrator groups:

- **ZENworks administrator group:** A ZENworks administrator group exists only in the ZENworks system. You create the group and maintain its membership in ZENworks Control Center.
- **User Source administrator group:** A user source administrator group exists in one of your LDAP user sources. You import the group into your ZENworks system, but the group's membership is maintained in the LDAP user source.

You can assign rights to ZENworks administrator groups and to user source administrator groups.

For information about creating administrator groups, see Chapter 4, "Managing Administrator Groups," on page 19.

1.3 Roles

A *role*, or *administrator role*, is a collection of rights that enable a specific administrative task or tasks to be performed. For example, you might have a Help Desk role that provides rights to remotely manage devices; a Software Management role that provides rights to create and distribute application bundles to managed devices; or a Desktop Security role that provides rights to create and apply security policies to managed devices.

You can assign administrator roles to administrators and to administrator groups.

For information about creating roles, see Chapter 5, "Managing Administrator Roles," on page 23.

1.4 Rights

A ZENworks administrator's *rights* control which administrative tasks he or she can perform in the Management Zone. There are 23 categories of rights:

Administrator
Bundle
Contract Management
Credential
Deployment
Device
Discovery
Document
Inventoried Device
LDAP Import
License Management
Location
Policy
Remote Management
Sharing
Subscriptions
System Update
User
User Source
ZENworks User Group
Zone
Inventory Report
Asset Management Report

Each rights category contains multiple rights that provide granular control of administrative tasks related to the category. For example, the Bundle Rights category includes the following rights:

View Leaf
Modify Groups
Create/Delete Groups
Modify Group Membership
Modify Folders
Create/Delete Folders
Author
Publish
Modify Settings
Assign Bundles
View Audit Logs
View Audit Events

Each right has two settings: *Allow* and *Deny*. Depending on the setting that is selected, the administrator is either allowed to perform the administrative task controlled by the right or not allowed to perform the task.

When you assign rights, you assign the entire rights category and specify the *context* in which the rights applies. For example, when you assign the Bundle Rights, you would configure each individual bundle right setting (Assign Bundles, Author, Publish, and so forth) to either *Allow* or *Deny*, and then specify the context to which the rights apply. In the case of Bundle Rights, the rights could be applied to the *Bundles* root folder or to any subfolders within the root folder. Some rights, such as Administrator Rights and Discovery Rights, apply only to the Management Zone, so their contexts are automatically set to *zone*.

For detailed descriptions of all rights, see Chapter 7, "Rights Descriptions," on page 39.

1.5 Rights Assignments and Conflict Resolution

There are multiple ways that an administrator can be assigned a right:

- A right is assigned directly to the administrator's account
- A right is assigned to an administrator group in which the administrator is a member
- A right is included in an administrator role that is assigned to the administrator or to an administrator group in which the administrator is a member

In some cases, rights assignments might conflict. When assignments conflict, the most restrictive setting is enforced. For example, an administrator might be assigned the same bundle right through his or her administrator account and through a role. If the settings are different in the two assignments (for example, one setting is *Allow* and the other is *Deny*), the *Deny* setting is used because it is more restrictive than *Allow*.

For information about assigning rights to administrators, groups, and roles, see Chapter 6, "Assigning Rights," on page 31.

2 Best Practices

The following sections provide a best practice approach to managing ZENworks administrator accounts and rights.

Practice 1: Create an account for each administrator

Each user who will perform administrative tasks for ZENworks should have his or her own ZENworks administrator account. This allows you to individually control the rights that each administrator has within the system. It also allows you to know which administrator has made changes to the system (see the *ZENworks 11 SP3 Audit Management Reference*).

For information about creating ZENworks administrator accounts, see Chapter 3, "Managing Administrator Accounts," on page 15.

Practice 2: Use administrator groups to reduce rights assignments

Use administrator groups to reduce the number of rights assignments you need to manage. You can create ZENworks administrator groups that exist only in the ZENworks system. You can also import user groups from your user sources to use as administrator groups, in which case the administrator group membership is managed through the user source.

For information about using administrator groups, see Chapter 4, "Managing Administrator Groups," on page 19.

Practice 3: Use administrator roles to provide assignment flexibility

An administrator role is a collection of rights that enable a specific ZENworks administrative task or tasks to be performed. For example, a Help Desk role might include the rights to remotely manage users' workstations.

Roles provide the following advantages when assigning rights:

- Roles can be assigned to administrators and to administrator groups.
- When you create roles, you do not assign a context to them. The context is set when you assign the role to an administrator or administrator group. This means that you can use the same role for administrators who require the role in different contexts.
- When you assign rights directly to an administrator or administrator group, you must set the right's privileges to either *Allow* or *Deny*. However, when adding rights to a role, you can configure any of the right's privileges as *Unset*. An unset privilege is not applied unless it is set elsewhere, such as on the administrator account, on a group in which the administrator is a member, or on another role.

For information about using administrator groups, see Chapter 5, "Managing Administrator Roles," on page 23.

3 Managing Administrator Accounts

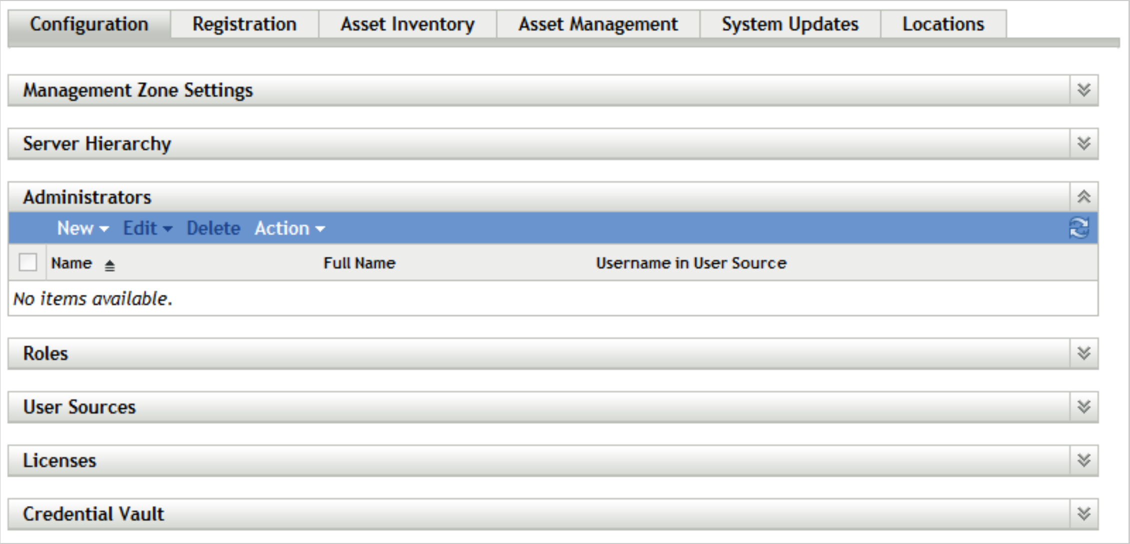
Typically, you should create ZENworks administrator accounts for each person who will perform administrative tasks. This allows you to give each administrator only the rights required to carry out his or her ZENworks management responsibilities. It also allows you to audit the changes each administrator makes in the zone.

The following sections help you create and manage administrator accounts:

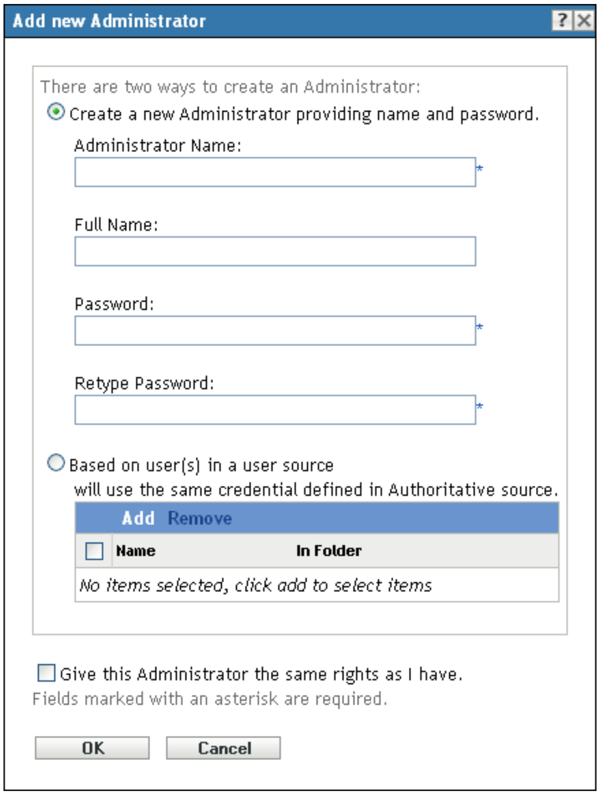
3.1 Creating Administrators

To create an administrator account:

1 In ZENworks Control Center, click the *Configuration* tab.



2 In the Administrators panel, click *New* > *Administrator* to display the Add New Administrator dialog box.



Add new Administrator

There are two ways to create an Administrator:

● Create a new Administrator providing name and password.

Administrator Name: *

Full Name:

Password: *

Retype Password: *

○ Based on user(s) in a user source

will use the same credential defined in Authoritative source.

Add Remove

□	Name	In Folder
No items selected, click add to select items		

□ Give this Administrator the same rights as I have.

Fields marked with an asterisk are required.

OK Cancel

3 Fill in the fields:

Create a New Administrator by Providing Name, Password: Select this option if you want to create a new administrator account by manually specifying the name and password.

When specifying a name, do not use characters such as / \ * ? : " ' < > | ` % ~. These characters are invalid and are not allowed in administrator names. For more information on conventions to follow, see "Naming Objects in ZENworks Control Center"in the *ZENworks 11 SP3 ZENworks Control Center Reference*.

Administrator login names with Unicode characters are case sensitive. Ensure that you use the correct case for each character in the login name when it contains Unicode characters.

The new administrator can change the password the first time he or she logs in by clicking the icon located next to the *Logout* link in the upper-right corner of ZENworks Control Center.

Based on User(s) in a User Source: Select this option if you want to create a new administrator account based on information from your user source. To do so, click *Add*, then browse for and select the user you want.

Give this Administrator the Same Rights as I Have: By default, new administrator accounts are granted View rights in the Management Zone, which means that they can log in and see most information but cannot modify any of it.

Select this option if you want to assign the new administrator the same rights that you have as the currently-logged in administrator. Otherwise, you will need to assign rights to the administrator after the administrator account is created.

4 When you have finished filling in the fields, click *OK* to add the new administrator.

5 Assign rights to the new administrator using any of the following methods:

- Assign rights directly to the administrator account. For instructions, see Chapter 6, “Assigning Rights,” on page 31.
- Add the administrator to an administrator group. The administrator receives all rights assigned to the group. For information about creating groups and adding administrators to them, see Chapter 4, “Managing Administrator Groups,” on page 19.
- Assign an administrator role to the administrator account. The administrator receives all rights assigned to the role. For information about creating and assigning roles, see Chapter 5, “Managing Administrator Roles,” on page 23.

You can also use the `admin-create` command in zman to create an administrator account. For more information, see “Administrator Commands” in the *ZENworks 11 SP3 Command Line Utilities Reference*.

3.2 Deleting Administrators

1. In ZENworks Control Center, click the *Configuration* tab.
2. In the Administrators panel, select the check box next to the administrator’s name, then click *Delete*.
3. Click *OK* to confirm the deletion.

You can also use the `admin-delete` command in zman to delete an administrator account. For more information, see “Administrator Commands” in the *ZENworks 11 SP3 Command Line Utilities Reference*.

3.3 Renaming Administrators

You cannot rename an administrator who is created based on an existing user in the user source.

1. In ZENworks Control Center, click the *Configuration* tab.
2. In the Administrators panel, select the check box next to the administrator’s name, then click *Edit* > *Rename*.
3. Specify the new name, then click *OK*.

You can also use the `admin-rename` command in zman to rename an administrator account. For more information, see “Administrator Commands” in the *ZENworks 11 SP3 Command Line Utilities Reference*.

3.4 Changing Administrator Passwords

Refer to the following sections for information about changing administrator passwords:

- Section 3.4.1, “Changing Your Own Administrator Password,” on page 18
- Section 3.4.2, “Changing Another Administrator’s Password,” on page 18

3.4.1 Changing Your Own Administrator Password

All administrators have rights to change their own password after logging in to ZENworks Control Center. This is the only method that can be used to change the default Administrator password.

1 In ZENworks Control Center, click the 🔧 icon located next to the *Logout* option in the top-right corner to display the Change Administrator Password dialog box.

2 Fill in the fields, then click *OK*.

3.4.2 Changing Another Administrator’s Password

To change another administrator’s password, you must be a Super Administrator or have the *Administrator Rights* > *Create/Delete* right. This method cannot be used to change the default Administrator password. To change the default Administrator password, you must log in as the default Administrator; see Section 3.4.1, “Changing Your Own Administrator Password,” on page 18.

1 In ZENworks Control Center, click the *Configuration* tab.

2 In the Administrators panel, select the check box next to the administrator, then click *Edit* > *Set Password* to display the Change Administrator Password Dialog box.

3 Fill in the fields, then click *OK*.

Ensure that the password is at least six characters long.

4 Managing Administrator Groups

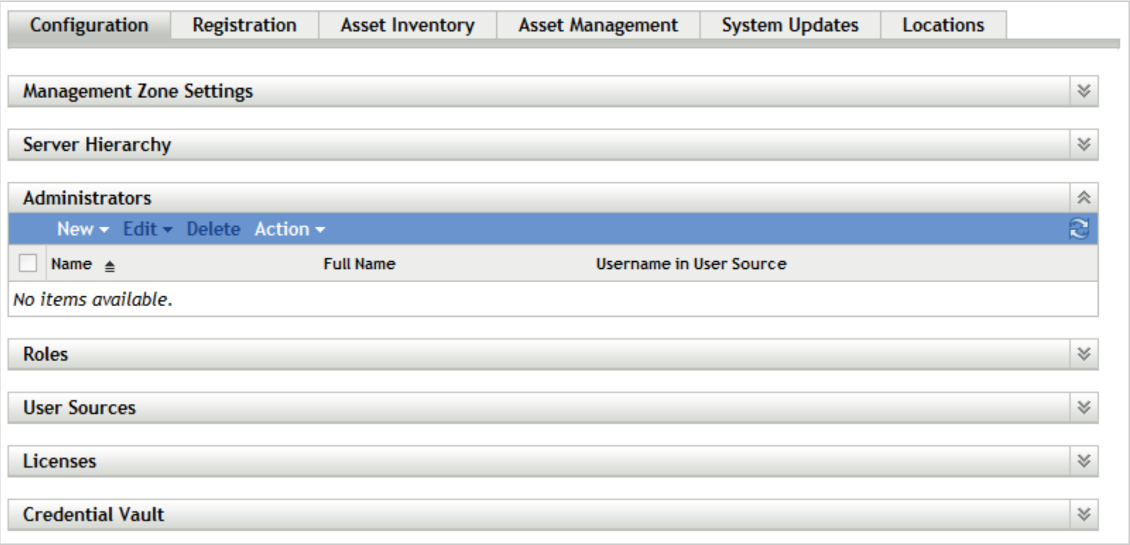
You can create administrator groups and assign rights to the groups. All administrators who are members of a group receive the rights assigned to the group.

The following sections help you create and manage administrator groups:

- Section 4.1, "Creating Administrator Groups," on page 19
- Section 4.2, "Creating Administrator Accounts for Members of User Source Administrator Groups," on page 21
- Section 4.3, "Modifying the Membership of ZENworks Administrator Groups," on page 21
- Section 4.4, "Deleting Administrator Groups," on page 22
- Section 4.5, "Renaming Administrator Groups," on page 22

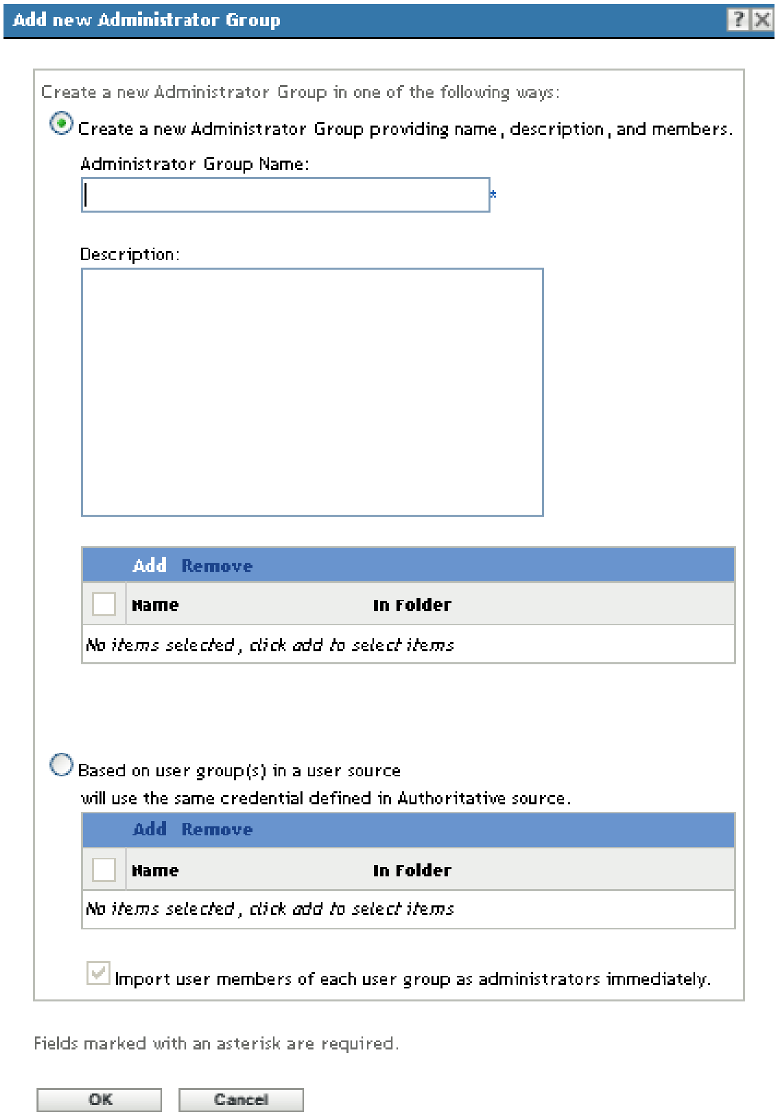
4.1 Creating Administrator Groups

1 In ZENworks Control Center, click the *Configuration* tab.



No items available.

2 In the Administrators panel, click *New* > *Administrator Group* to display the Add New Administrator Group dialog box.



Create a new Administrator Group in one of the following ways:

● Create a new Administrator Group providing name, description, and members.

Administrator Group Name: *

Description:

No items selected, click add to select items

○ Based on user group(s) in a user source

will use the same credential defined in Authoritative source.

No items selected, click add to select items

☑ Import user members of each user group as administrators immediately.

Fields marked with an asterisk are required.

3 Fill in the fields.

The Add New Administrator Group dialog box lets you create a new administrator group account by providing a group name and adding members to the group, or you can create a new administrator group based on an existing user group in the user source. Each administrator group name must be unique.

Create a New Administrator Group by Providing a Name and Adding Members: Select this option if you want to create a new administrator group account by manually specifying the name and adding the members. To add members, click *Add*, then browse for and select the administrators you want.

You can add any number of administrators to the group. You cannot add other administrator groups to the group.

Based on User Groups in a User Source: Select this option if you want to create a new administrator group account based on user group information from your user source. To do so, click *Add*, then browse for and select the user group you want.

Import user members of each user group as administrators immediately: Select this option to enable the user members of the selected user groups to be immediately added as administrators who can only view the ZENworks Control Center pages.

4. When you have finished filling in the fields, click *OK* to add the new administrator group to the Administrators panel.
5. Assign rights to the new administrator group using any of the following methods:
   - Assign rights directly to the administrator group. For instructions, see Chapter 6, "Assigning Rights," on page 31.
   - Assign an administrator role to the administrator group. The group receives all rights assigned to the role. For information about creating and assigning roles, see Chapter 5, "Managing Administrator Roles," on page 23.

4.2 Creating Administrator Accounts for Members of User Source Administrator Groups

This section applies only to user source (LDAP) administrator groups.

By default, ZENworks queries its user sources every 24 hours to refresh the membership of the administrator groups that are based on user source groups. If a group's membership has changed in the user source, the appropriate ZENworks administrator accounts are added or deleted during the refresh.

Rather than wait for administrator accounts to be created during the scheduled refresh, you can initiate the refresh to automatically create administrator accounts for any members of the group that do not already have administrator accounts. To do so:

1. In ZENworks Control Center, click the *Configuration* tab.
2. In the Administrators panel, select the check box next to the administrator group.
3. Click *Action* > *Create Administrators*.
4. Review the message, then click *OK*

4.3 Modifying the Membership of ZENworks Administrator Groups

This section applies only to ZENworks administrator groups. It does not apply to user source administrator groups; you cannot change a user source group's membership within ZENworks.

1. In ZENworks Control Center, click the *Configuration* tab.
2. In the Administrators panel, click the administrator group whose membership you want to change.
3. On the group's *Summary* tab, use the Members panel to add and remove members.

4.4 Deleting Administrator Groups

1. In ZENworks Control Center, click the *Configuration* tab.
2. In the Administrators panel, select the check box next to the administrator group's name, then click *Delete*.
3. Click *OK* to confirm the deletion.

4.5 Renaming Administrator Groups

You cannot rename an administrator group that is created based on an existing user group in the user source.

1. In ZENworks Control Center, click the *Configuration* tab.
2. In the Administrators panel, select the check box next to the administrator group's name, then click *Edit* > *Rename*.
3. Specify the new name, then click *OK*.

5 Managing Administrator Roles

An administrator role is a group of rights that allows an administrator to perform specialized ZENworks administrative tasks. For example, you might have a Help Desk role that provides the rights needed to remotely manage devices; a Software Management role that provides the rights needed to create and distribute software applications; or a Desktop Security role that provides rights to create and apply security policies to managed devices.

You can assign administrator roles to administrators and administrator groups.

Perform the following tasks to manage administrator roles:

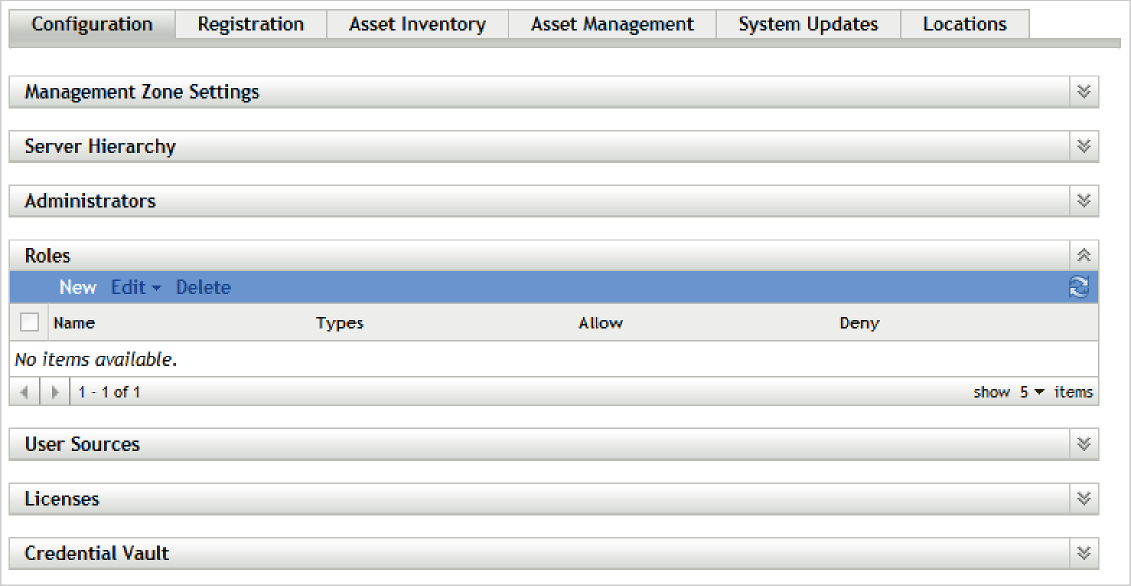
- Section 5.1, “Creating Roles,” on page 23
- Section 5.2, “Assigning Roles,” on page 24
- Section 5.3, “Modifying Roles,” on page 28
- Section 5.4, “Renaming Roles,” on page 30
- Section 5.5, “Deleting Roles,” on page 30

5.1 Creating Roles

You must be logged in either as a Super Administrator or as an Administrator with grant rights to create roles.

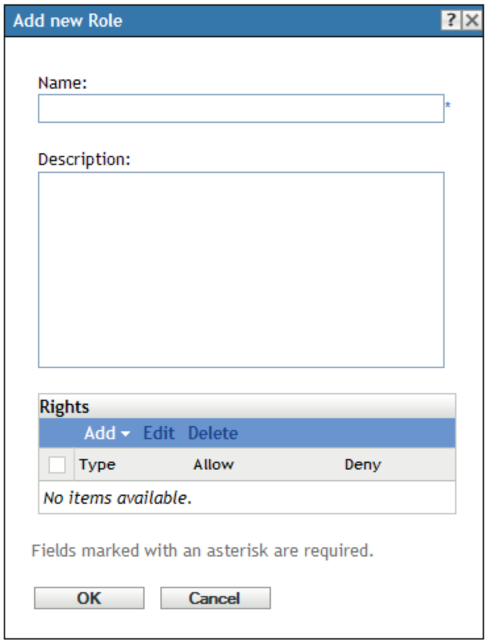
A role can include one or more rights categories. You can create as many roles as you need. To create a role:

1 In ZENworks Control Center, click *Configuration*.



No items available.

2 In the Roles panel, click *New* to open the Add New Role dialog box:



3 Fill in the following fields:

Name: When specifying a name, do not use characters such as / \ * ? : " ' < > | ` % ~. These characters are invalid and are not allowed in administrator role names. For more information on conventions to follow, see "Naming Objects in ZENworks Control Center"in the *ZENworks 11 SP3 ZENworks Control Center Reference*.

Description: Provide optional information to identify the role.

Rights: Click *Add*, select a rights category you want to include in the role, configure each of the right's privileges, then click *OK* to add the rights to the Rights list. You can allow the privilege, deny the privilege, or leave the privilege unset. If you select the *Unset* option, the privilege is not applied (denied or allowed) unless it is set elsewhere in ZENworks (for example, on an administrator account, an administrator group, or another role). For more information about rights, see Chapter 7, "Rights Descriptions," on page 39.

4 When you are finished adding rights to the role, click *OK* to save the role.

5 To assign the role to administrators or administrator groups, see Section 5.2, "Assigning Roles," on page 24.

5.2 Assigning Roles

You can assign multiple roles to a single administrator or group at one time, or you can assign multiple administrators and groups to a single role at one time, as explained in the following sections:

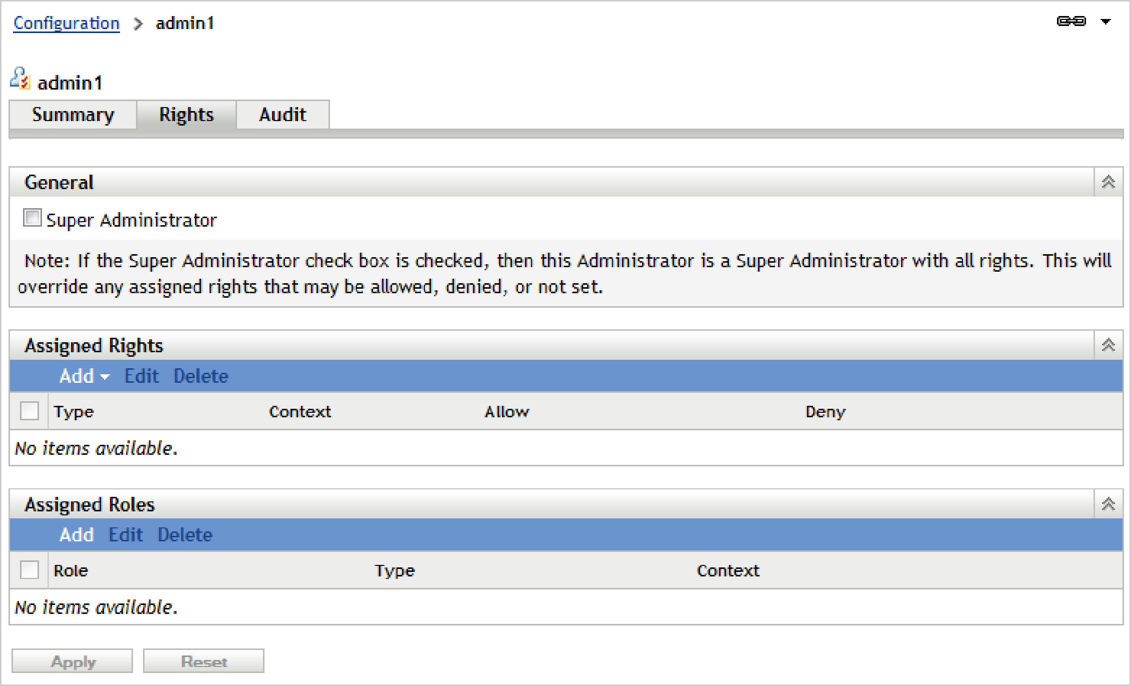
- Section 5.2.1, "Assigning Roles to an Administrator or Administrator Group," on page 25
- Section 5.2.2, "Assigning Administrators and Administrator Groups to a Role," on page 26

5.2.1 Assigning Roles to an Administrator or Administrator Group

1 In ZENworks Control Center, click *Configuration*.

2 In the Administrators panel, click the name of the administrator or group to which you want to add roles.

3 Click the *Rights* tab:



Configuration > admin1

admin1

Summary | Rights | Audit

General

□ Super Administrator

Note: If the Super Administrator check box is checked, then this Administrator is a Super Administrator with all rights. This will override any assigned rights that may be allowed, denied, or not set.

Assigned Rights

Add ▾ Edit Delete

□	Type	Context	Allow	Deny

No items available.

Assigned Roles

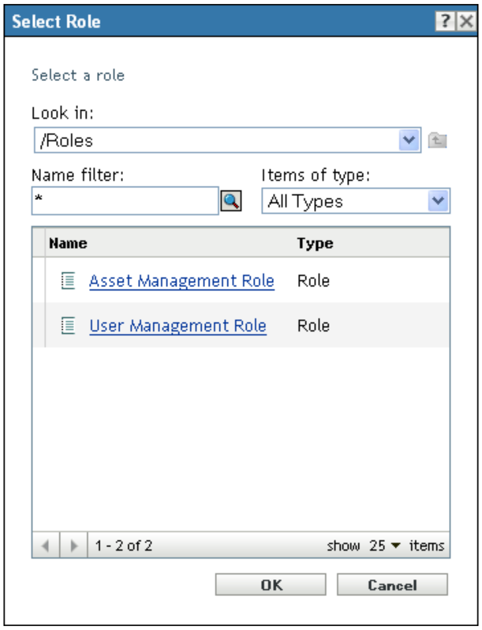
Add Edit Delete

□	Role	Type	Context

No items available.

Apply Reset

4 In the Assigned Roles panel, click *Add* to display the Select Role dialog box.



Select Role

Select a role

Look in: /Roles

Name filter: *

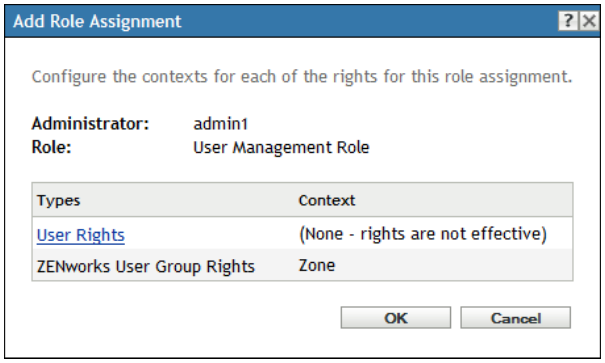
Items of type: All Types

Name	Type
Asset Management Role	Role
User Management Role	Role

1 - 2 of 2 show 25 ▾ items

OK Cancel

5 Browse for and select the role to apply, then click *OK* to display the Add Role Assignment dialog box:



Configure the contexts for each of the rights for this role assignment.

Administrator: admin1
Role: User Management Role

Types	Context
User Rights	(None - rights are not effective)
ZENworks User Group Rights	Zone

The Add Role Assignment dialog box is displayed so that you can define the contexts for the rights included in the role. The contexts determine where the rights are applied. Some rights apply to the entire Management Zone, in which case *Zone* is displayed in the Context field and you cannot change it. Otherwise, you need to add each context to which you want the rights to apply.

If you do not specify a context, the right is not applied to any context.

6 To set contexts for the role's rights:

6a In the *Types* column, click a right to display the Select Context dialog box.

Rights that have a *Zone* context cannot be changed; they apply to the entire Management Zone.

6b In the Select Context dialog box, click *Add* and browse for the desired context.

While browsing, you can select multiple contexts in the Browse dialog box.

6c When you are finished selecting the contexts for a the right, click *OK* to close the Select Contexts dialog box.

6d Repeat Step 6a through Step 6c for each right whose context needs to be set.

6e When you are finished, click *OK* to close the Add Role Assignment dialog box.

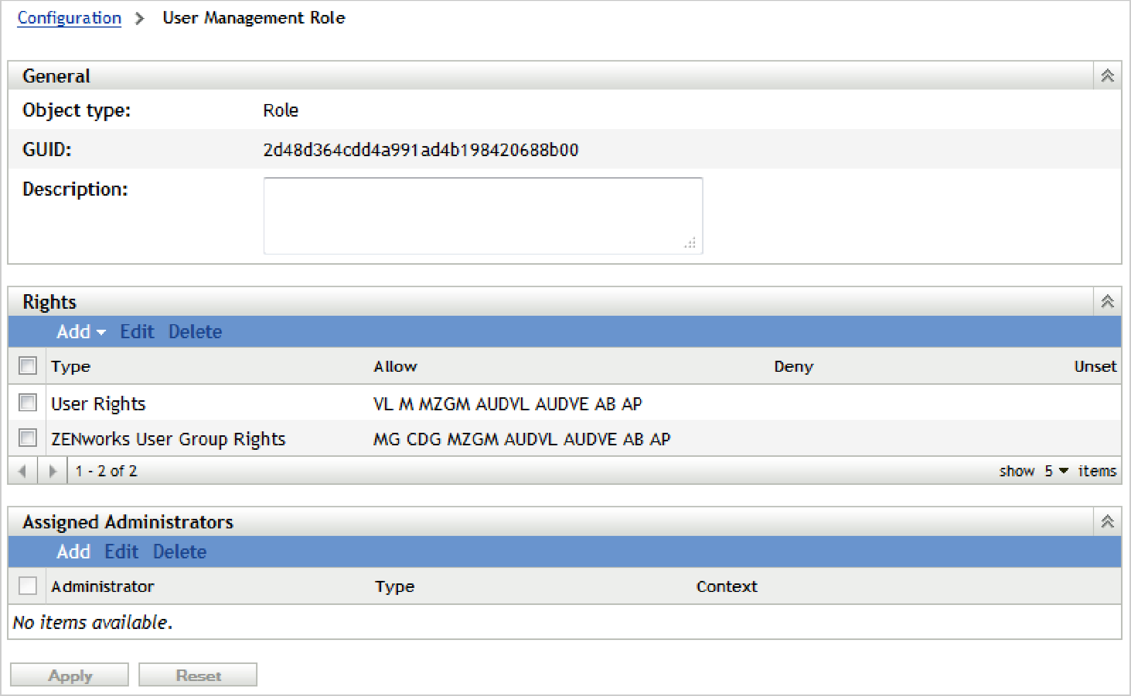
7 To add another role, repeat Step 4 and Step 6.

8 When you are finished assigning roles to the administrator or group, click *Apply* to save the changes.

5.2.2 Assigning Administrators and Administrator Groups to a Role

1 In ZENworks Control Center, click *Configuration*.

2 In the Roles panel, click the name of the role that you want to assign to administrators or administrator groups.



Configuration > User Management Role

General

Object type: Role

GUID: 2d48d364cdd4a991ad4b198420688b00

Description:

Rights

□	Type	Allow	Deny	Unset
□	User Rights	VL M MZGM AUDVL AUDVE AB AP		
□	ZENworks User Group Rights	MG CDG MZGM AUDVL AUDVE AB AP		

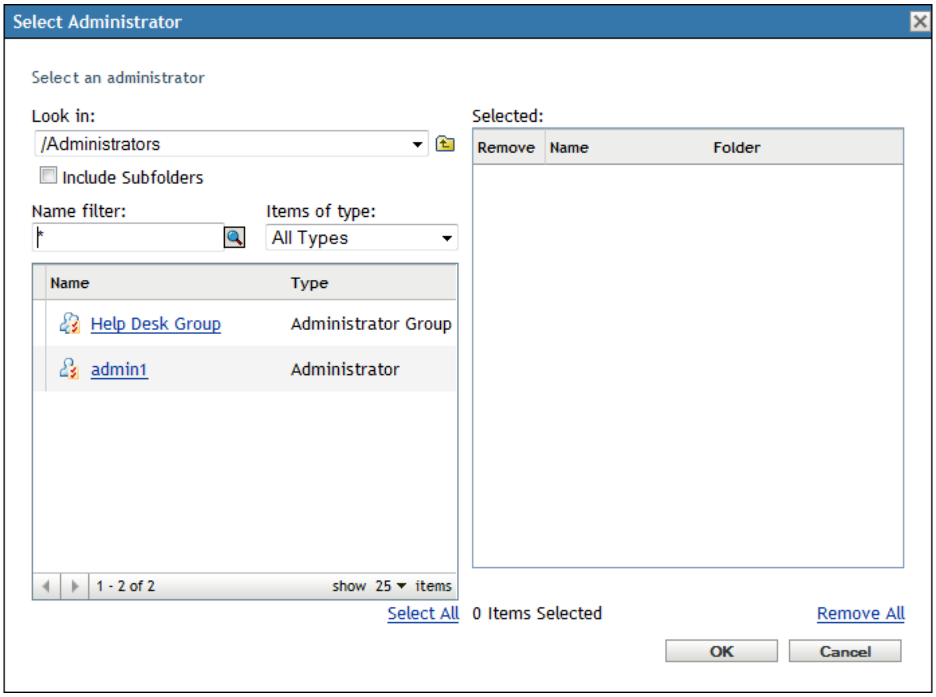
1 - 2 of 2 show 5 items

Assigned Administrators

□	Administrator	Type	Context

No items available.

3 In the Assigned Administrators panel, click *Add* to display the Select Administrator dialog box:



Select Administrator

Select an administrator

Look in: /Administrators

□ Include Subfolders

Name filter: *

Items of type: All Types

Name	Type
Help Desk Group	Administrator Group
admin1	Administrator

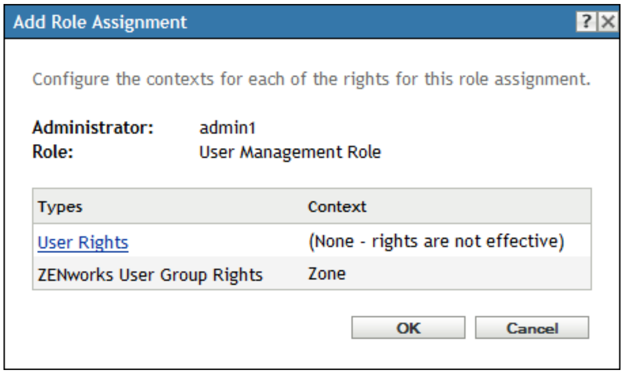
1 - 2 of 2 show 25 items

Selected:

Remove	Name	Folder

0 Items Selected

4 Browse for and select the administrators and administrator groups to which you want to assign the role, then click *OK* to display the Add Role Assignment dialog box:



Add Role Assignment

Configure the contexts for each of the rights for this role assignment.

Administrator: admin1
Role: User Management Role

Types	Context
User Rights	(None - rights are not effective)
ZENworks User Group Rights	Zone

The Add Role Assignment dialog box is displayed so that you can define the contexts for the rights included in the role. The contexts determine where the rights are applied. Some rights apply to the entire Management Zone, in which case *Zone* is displayed in the Context field and you cannot change it. Otherwise, you need to add each context to which you want the rights to apply.

If you do not specify a context, the right is not applied to any context.

5 To set contexts for the role's rights:

5a In the *Types* column, click a right to display the Select Context dialog box.

Rights that have a *Zone* context cannot be changed; they apply to the entire Management Zone.

5b In the Select Context dialog box, click *Add* and browse for the desired context.

While browsing, you can select multiple contexts in the Browse dialog box.

5c When you are finished selecting the contexts for a the right, click *OK* to close the Select Contexts dialog box.

5d Repeat Step 6a through Step 6c for each right whose context needs to be set.

5e When you are finished, click *OK* to close the Add Role Assignment dialog box.

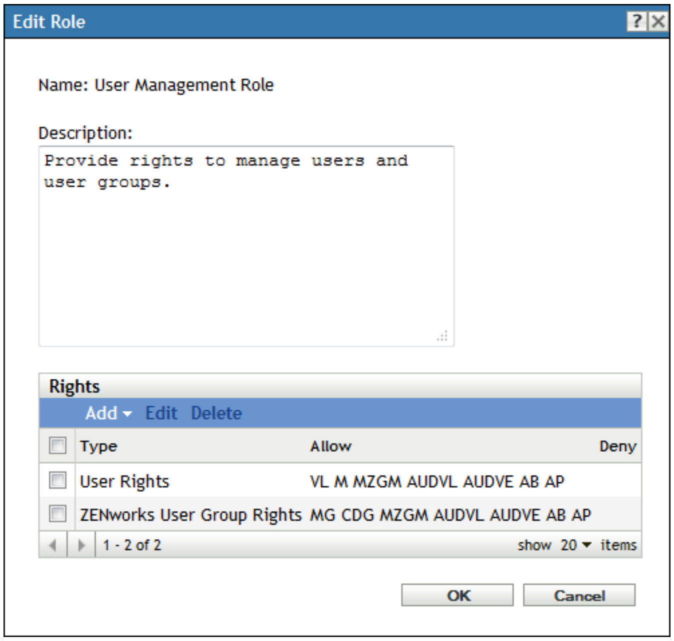
6 Click *Apply* to save the changes to the role.

5.3 Modifying Roles

You can change a role's description, rights, and administrator assignments at any time. After you save the changes, any rights changes are immediately effective for assigned administrators and groups.

1 In ZENworks Control Center, click *Configuration*.

2 In the Roles panel, select the check box for the role you want to modify, then click *Edit* > *Edit* to open the Edit Role dialog box:



Name: User Management Role

Description:

```
Provide rights to manage users and
user groups.
```

Rights

□	Type	Allow	Deny
□	User Rights	VL M MZGM AUDVL AUDVE AB AP	
□	ZENworks User Group Rights	MG CDG MZGM AUDVL AUDVE AB AP	

3 To change the description, make the changes directly in the *Description* field.

4 To change existing rights:

4a In the Rights panel, select the check box for the right whose settings you want to change, then click *Edit* to open the Rights dialog box.

4b For each privilege, select whether the role allows it, denies it, or leaves it unset.

The most restrictive right set in ZENworks prevails. If you select the *Deny* option, the right is denied for any administrator or group assigned that role, even if the administrator is allowed the right elsewhere in ZENworks.

If you select the *Unset* option, the administrator is not granted the right for the role unless it is granted elsewhere in ZENworks (for example, on an administrator account, an administrator group, or another role).

4c Click *OK* to save the change.

4d Repeat Step 4a through Step 4c for each right you want to change.

5 To add new rights:

5a In the Rights panel, click *Add*, then select one of the rights categories from the list.

5b In the Rights dialog box, select whether each privilege should be allowed, denied, or left unset.

The most restrictive right set in ZENworks prevails. If you select the *Deny* option, the right is denied for any administrator assigned to that role, even if the administrator is granted that right elsewhere in ZENworks.

If you select the *Unset* option, the administrator is not granted the right for the role unless it is granted elsewhere in ZENworks.

5c Click *OK* to continue.

5d Repeat Step 5a through Step 5c for each right you want to add.

6 To delete rights:

   6a In the Rights panel, select the check box for the right to be deleted, then click *Delete*.

   6b Click *OK* to confirm the deletion.

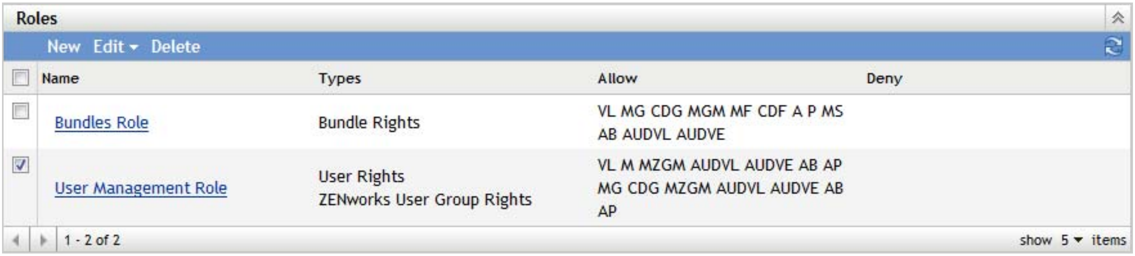
7 When you are finished modifying the rights, click OK to exit the dialog box and save your changes to the role.

5.4 Renaming Roles

Role names can be changed at any time. The changed role name is automatically replicated wherever it is displayed in ZENworks Control Center.

1 In ZENworks Control Center, click *Configuration*.

2 In the Roles panel, select the check box for the role to be renamed.



□	Name	Types	Allow	Deny
□	Bundles Role	Bundle Rights	VL MG CDG MGM MF CDF A P MS AB AUDVL AUDVE	
☑	User Management Role	User Rights ZENworks User Group Rights	VL M MZGM AUDVL AUDVE AB AP MG CDG MZGM AUDVL AUDVE AB AP	

3 Click *Edit* > *Rename* to open the Rename Role dialog box.

4 Specify the new role name, then click *OK*.

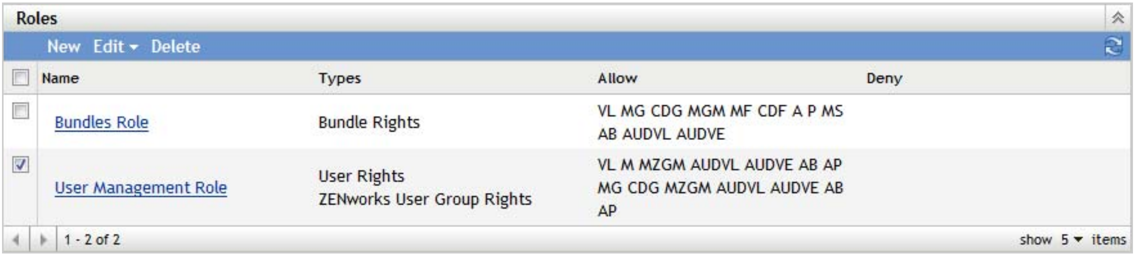
5.5 Deleting Roles

When you delete a role, its rights configurations are no longer applicable to any administrator that was assigned to the role.

Deleted roles cannot be recovered. You must re-create them.

1 In ZENworks Control Center, click *Configuration* in the left pane.

2 In the Roles panel, select the check box for the role to be deleted.



□	Name	Types	Allow	Deny
□	Bundles Role	Bundle Rights	VL MG CDG MGM MF CDF A P MS AB AUDVL AUDVE	
☑	User Management Role	User Rights ZENworks User Group Rights	VL M MZGM AUDVL AUDVE AB AP MG CDG MZGM AUDVL AUDVE AB AP	

3 Click *Delete*, then click *OK* to confirm the deletion.

6 Assigning Rights

The following sections help you manage rights assignments for administrators, administrator groups, and administrator roles:

- Section 6.1, "Assigning Rights," on page 31
- Section 6.2, "Modifying Assigned Rights," on page 36
- Section 6.3, "Removing Assigned Rights," on page 38

6.1 Assigning Rights

The following sections help you assign rights to administrators, groups, and roles:

- Section 6.1.1, "Assigning Super Administrator Rights," on page 31
- Section 6.1.2, "Assigning Rights to Administrators and Administrator Groups," on page 32
- Section 6.1.3, "Assigning Rights to Administrator Roles," on page 33
- Section 6.1.4, "Assigning Inventory Report Rights to Administrators and Administrator Groups," on page 34
- Section 6.1.5, "Assigning Asset Management Report Rights to Administrators and Administrator Groups," on page 35

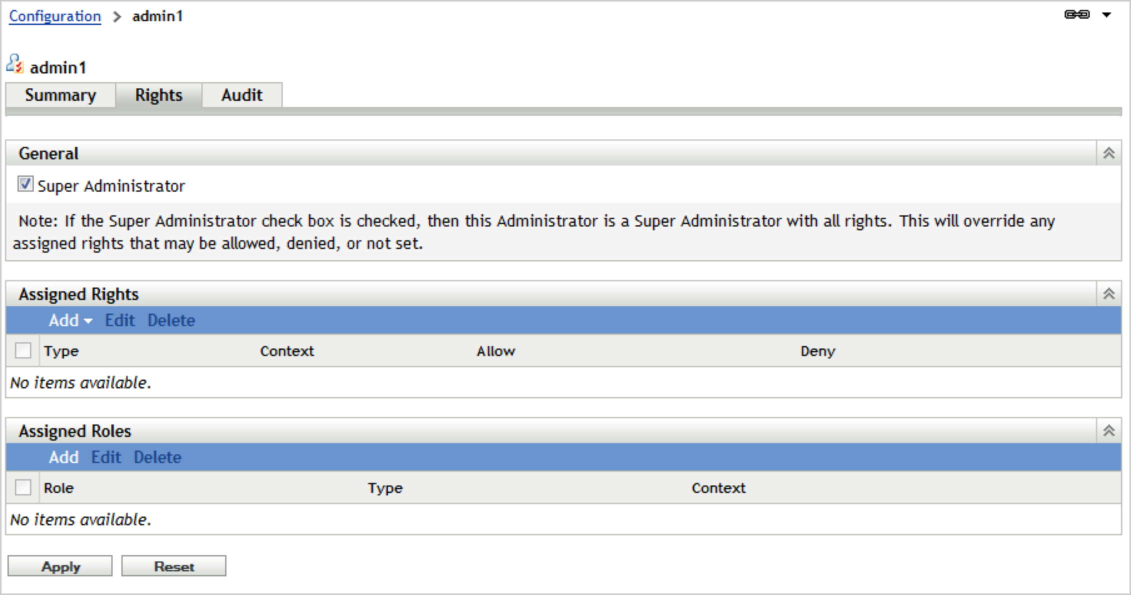
6.1.1 Assigning Super Administrator Rights

A Super Administrator has rights to perform all administrative tasks. For more information about all of the rights that a Super Administrator has, see Section 7, "Rights Descriptions," on page 39. When you grant an administrator Super Administrator rights, all other assigned rights are overridden.

Super Administrator rights can be assigned only to administrator accounts. They cannot be assigned to administrator groups or roles.

1. In ZENworks Control Center, click the *Configuration* tab.
2. In the Administrators panel, click the name of the administrator to whom you want to assign Super Administrator rights.
3. Click the *Rights* tab.

4 In the General panel, select the *Super Administrator* check box.



General

☑ Super Administrator

Note: If the Super Administrator check box is checked, then this Administrator is a Super Administrator with all rights. This will override any assigned rights that may be allowed, denied, or not set.

Assigned Rights

□ Type	Context	Allow	Deny
No items available.			

Assigned Roles

□ Role	Type	Context
No items available.		

5 Click *Apply*.

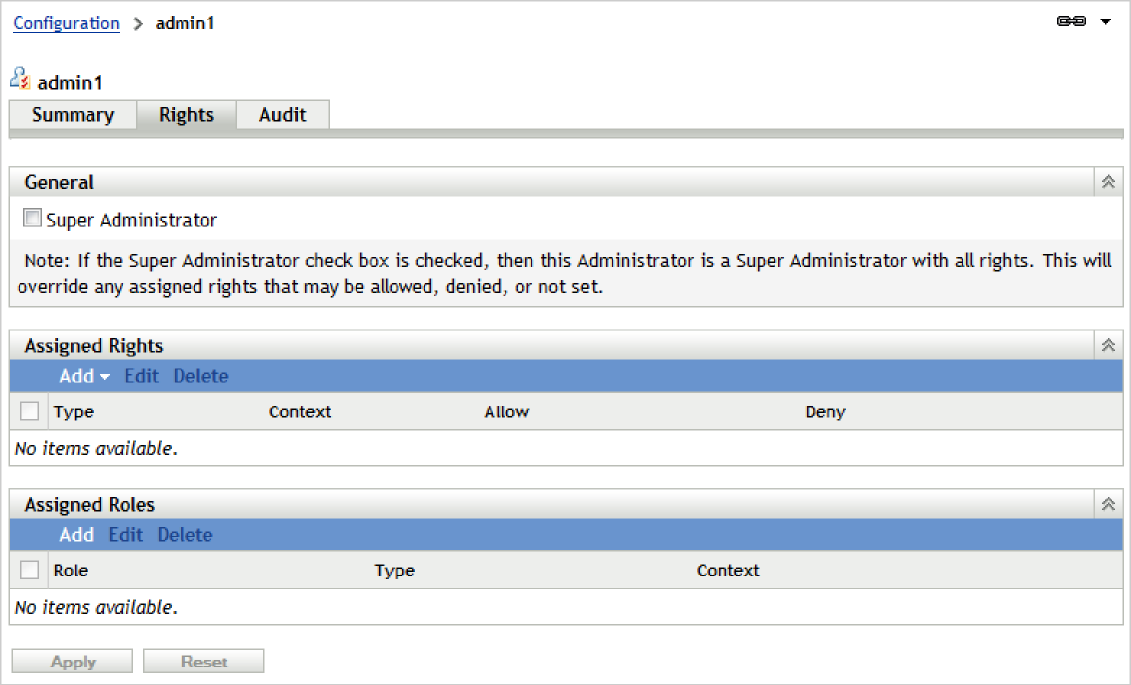
6.1.2 Assigning Rights to Administrators and Administrator Groups

This section explains how to assign all rights other than Inventory Report Rights and Asset Management Report Rights to administrators and administrator groups. For information about assigning Inventory Report rights, see Section 6.1.4, “Assigning Inventory Report Rights to Administrators and Administrator Groups,” on page 34. For information about assigning Asset Management Report rights, see Section 6.1.5, “Assigning Asset Management Report Rights to Administrators and Administrator Groups,” on page 35.

1 In ZENworks Control Center, click the *Configuration* tab.

2 In the Administrators panel, click the name of the administrator or administrator group to which you want to assign rights.

3. Click the *Rights* tab.



General

□ Super Administrator

Note: If the Super Administrator check box is checked, then this Administrator is a Super Administrator with all rights. This will override any assigned rights that may be allowed, denied, or not set.

Assigned Rights

□	Type	Context	Allow	Deny
No items available.				

Assigned Roles

□	Role	Type	Context
No items available.			

4. In the Assigned Rights panel, click *Add*, then select the rights you want to assign.

   For example, if you want to assign rights for device tasks, select *Device Rights*.

5. Configure the following settings:

   Contexts: The contexts determine where the rights are applied. Some rights apply to the entire Management Zone, in which case *Zone* is displayed in the Contexts box and you cannot change it. Otherwise, you need to add each context to which you want the rights to apply.

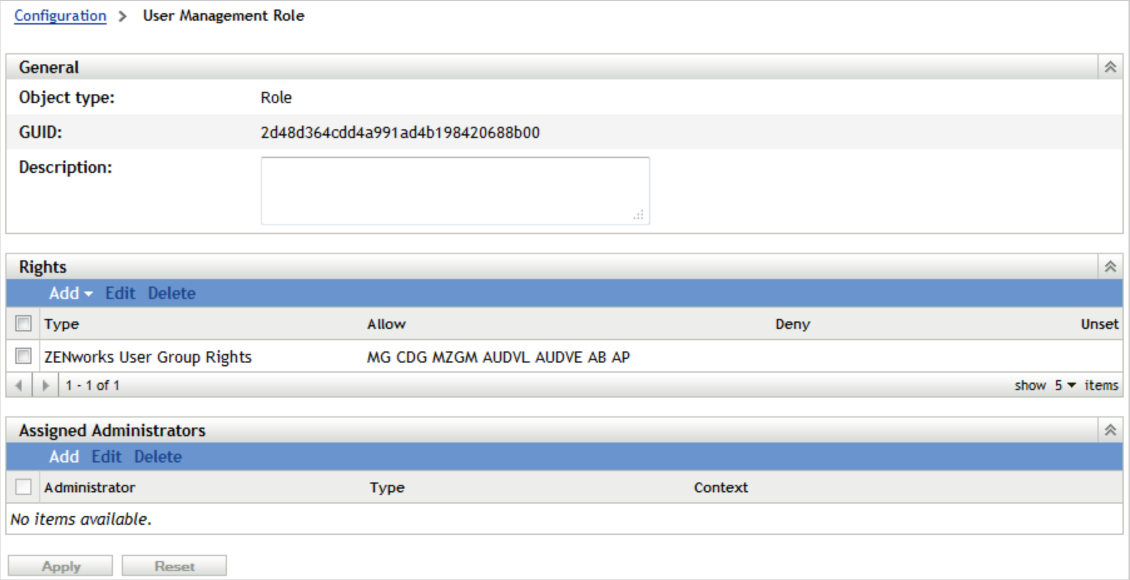
   Privileges: Each privilege, or task, has a rights setting associated with it. Click *Allow* to enable the privilege or click *Deny* to disable the privilege. For more information about right's privileges, see Chapter 7, "Rights Descriptions," on page 39.

6. Click *OK* to add the rights to the Assigned Rights panel.
7. Click *Apply* to save the changes to the administrator or administrator group.

You can also use the `admin-rights-set` command in zman to assign rights for an administrator account. For more information, see "Administrator Commands" in the *ZENworks 11 SP3 Command Line Utilities Reference*.

6.1.3 Assigning Rights to Administrator Roles

1. In ZENworks Control Center, click the *Configuration* tab.
2. In the Roles panel, click the name of the role to which you want to assign rights.



General

Object type:	Role
GUID:	2d48d364cdd4a991ad4b198420688b00
Description:	

Rights

□	Type	Allow	Deny	Unset
□	ZENworks User Group Rights	MG CDG MZGM AUDVL AUDVE AB AP		

1 - 1 of 1 show 5 ▾ items

Assigned Administrators

□	Administrator	Type	Context

No items available.

3 In the Rights panel, click *Add*, then select the rights you want to assign.

For example, if you want to assign rights for device tasks, select *Device Rights*.

4 For each privilege, click *Allow* to enable the privilege, *Deny* to disable the privilege, or *Unset* to not configure the privilege.

If you select *Unset*, the privilege is not applied (denied or allowed) unless it is set elsewhere in ZENworks (for example, on an administrator account, an administrator group, or another role). For more information about the right's privileges, see Section 7, "Rights Descriptions," on page 39.

NOTE: You do not configure the contexts to which the rights apply until you assign the role to an administrator or administrator group. This allows you to use the same role for administrators requiring the role in different contexts. For information about assigning roles, see Section 5.2, "Assigning Roles," on page 24.

5 Click *OK*.

6 Click *Apply* to save the changes to the administrator role.

You can also use the `role-rights-set` command in zman to assign rights to an administrator role. For more information, see "Role Commands" in the *ZENworks 11 SP3 Command Line Utilities Reference*.

6.1.4 Assigning Inventory Report Rights to Administrators and Administrator Groups

This section explains how to assign Inventory Report rights to administrators and administrator groups. Inventory Report rights control an administrator's rights to edit and run the standard and custom inventory reports. These are the reports located on the Reports tab in ZENworks Control Center.

For information about assigning Asset Management Report rights, see Section 6.1.5, "Assigning Asset Management Report Rights to Administrators and Administrator Groups," on page 35. For information about assigning all other rights, see Section 6.1.2, "Assigning Rights to Administrators and Administrator Groups," on page 32.

By default, each administrator receives rights to view and run all of the inventory reports. You can increase the rights to enable the administrator to also create and delete reports. Or, you can remove the rights to prevent the administrator from even seeing the reports.

1. In ZENworks Control Center, click the *Configuration* tab.
2. In the Administrators panel, click the name of the administrator or administrator group whose Inventory Reports rights assignments you want to modify.
3. Click the *Rights* tab.
4. In the Administrator Tasks panel, click *Inventory Report Rights*.

   The Inventory Report Rights panel lists the folders that contain the custom and standard inventory reports. The report rights are set at the folder level.
5. Select the check box next to the folder containing the reports for which you want to modify the administrator's rights.
6. Click *Edit*, then select the rights you want to assign:
   - **Remove All Rights:** Removes all rights to the folder and its reports.
   - **Assign View/Execute Rights:** Allows the administrator to view and execute the folder's report, but not to edit, move, or delete the reports.
   - **Assign Full Rights:** Gives the administrator rights to create, edit, move, and delete reports. For standard reports, this setting is the same as View/Execute, because you cannot alter a standard report.

   The changes to the rights are saved immediately.

For more information, see Section 7.25, "Inventory Report Rights," on page 73.

6.1.5 Assigning Asset Management Report Rights to Administrators and Administrator Groups

This section explains how to assign Asset Management Report rights to administrators and administrator groups. Asset Management Report rights control an administrator's rights to edit and run the standard and custom Asset Management reports. These are the reports located on the Asset Management Reports tab in ZENworks Control Center.

For information about assigning Inventory Report rights, see Section 6.1.4, "Assigning Inventory Report Rights to Administrators and Administrator Groups," on page 34. For information about assigning all other rights, see Section 6.1.2, "Assigning Rights to Administrators and Administrator Groups," on page 32.

By default, each administrator receives rights to view and run all of the Asset Management reports. You can increase the rights to enable the administrator to also create and delete reports. Or, you can remove the rights to prevent the administrator from even seeing the reports.

1. In ZENworks Control Center, click the *Configuration* tab.
2. In the Administrators panel, click the name of the administrator or administrator group whose Inventory Reports rights assignments you want to modify.
3. Click the *Rights* tab.
4. In the Administrator Tasks panel, click *Asset Management Report Rights*.

   The Asset Management Report Rights panel lists the folders that contain the custom and standard inventory reports, as well as the source for the folders. The report rights are set at the folder level.

5. Select the check box next to the folder containing the reports for which you want to modify the administrator's rights.
6. Click *Edit*, then select the rights you want to assign:
   - **Remove All Rights:** Removes all rights to the folder and its reports.
   - **Assign View/Execute Rights:** Allows the administrator to view and execute the folder's report, but not to edit, move, or delete the reports.
   - **Assign Full Rights:** Gives the administrator rights to create, edit, move, and delete reports. For standard reports, this setting is the same as View/Execute, because you cannot alter a standard report.

   The changes to the rights are saved immediately.

For more information, see Section 7.26, "Asset Management Report Rights," on page 73.

6.2 Modifying Assigned Rights

The following sections describe how to modify the rights assigned to administrators, groups, and roles:

- Section 6.2.1, "Modifying Assigned Rights for Administrators and Administrator Groups," on page 36
- Section 6.2.2, "Modifying Assigned Rights for Administrator Roles," on page 37
- Section 6.2.3, "Modifying Inventory Report Rights for Administrators and Administrator Groups," on page 37
- Section 6.2.4, "Modifying Asset Management Report Rights for Administrators and Administrator Groups," on page 37

6.2.1 Modifying Assigned Rights for Administrators and Administrator Groups

You can change the settings (*Allow* or *Deny*) for assigned rights, but you cannot change the contexts for the rights. If you want to change the contexts, you must delete the rights (see Section 6.3, "Removing Assigned Rights," on page 38) and add them again (see Section 6.1, "Assigning Rights," on page 31).

1. In ZENworks Control Center, click the *Configuration* tab.
2. In the Administrators panel, click the name of the administrator or administrator group whose assigned rights you want to change.
3. In the Assigned Rights panel, select the check box next to the assigned right you want to modify.
4. Click *Edit*, then modify the settings.

   For more information about the settings, see Section 7, "Rights Descriptions," on page 39.
5. Click *OK*.
6. When you are finished modifying rights, click *Apply* to apply the changes.

6.2.2 Modifying Assigned Rights for Administrator Roles

1. In ZENworks Control Center, click the *Configuration* tab.
2. In the Roles panel, click the name of the administrator role whose assigned rights you want to change.
3. In the Rights panel, select the check box next to the assigned right you want to modify.
4. Click *Edit*, then modify the settings.

   For more information about the settings, see Section 7, "Rights Descriptions," on page 39.
5. Click *OK*.
6. When you are finished modifying rights, click *Apply* to apply the changes.

6.2.3 Modifying Inventory Report Rights for Administrators and Administrator Groups

1. In ZENworks Control Center, click the *Configuration* tab.
2. In the Administrators panel, click the name of the administrator or administrator group whose Inventory Report rights you want to modify.
3. Click the *Rights* tab.
4. In the Administrator Tasks panel, click *Inventory Report Rights*.
5. Select the check box next to the folder containing the reports for which you want to modify the administrator's rights.
6. Click *Edit*, then select the rights you want to assign:
   - **Remove All Rights:** Removes all rights to the folder and its reports.
   - **Assign View/Execute Rights:** Allows the administrator to view and execute the folder's report, but not to edit, move, or delete the reports.
   - **Assign Full Rights:** Gives the administrator rights to create, edit, move, and delete reports. For standard reports, this setting is the same as View/Execute, because you cannot alter a standard report.

   The changes to the rights are saved immediately.

For more information, see Section 7.25, "Inventory Report Rights," on page 73.

6.2.4 Modifying Asset Management Report Rights for Administrators and Administrator Groups

1. In ZENworks Control Center, click the *Configuration* tab.
2. In the Administrators panel, click the name of the administrator or administrator group whose Asset Management rights you want to modify.
3. Click the *Rights* tab.
4. In the Administrator Tasks panel, click *Asset Management Report Rights*.
5. Select the check box next to the folder containing the reports for which you want to modify the administrator's rights.
6. Click *Edit*, then select the rights you want to assign:
   - **Remove All Rights:** Removes all rights to the folder and its reports.

- **Assign View/Execute Rights:** Allows the administrator to view and execute the folder's report, but not to edit, move, or delete the reports.
- **Assign Full Rights:** Gives the administrator rights to create, edit, move, and delete reports. For standard reports, this setting is the same as View/Execute, because you cannot alter a standard report.

The changes to the rights are saved immediately.

For more information, see Section 7.26, "Asset Management Report Rights," on page 73.

6.3 Removing Assigned Rights

1. In ZENworks Control Center, click the *Configuration* tab.
2. In the Administrators panel, click the administrator's name.
3. Select the check box next to the assigned right.
4. Click *Delete*.

You can also use the `admin-rights-delete` command in zman to delete assigned rights for an administrator account. For more information, see "Administrator Commands" in the *ZENworks 11 SP3 Command Line Utilities Reference*.

7 Rights Descriptions

The following sections contain information about the various rights that you can assign to administrators, administrator groups, and administrator roles:

7.1 Administrator Rights

The Administrator Rights dialog box lets you allow the selected administrator to grant rights to other administrators and to create or delete administrator accounts for your Management Zone.

The following rights are available:

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Grant Rights	◆ Assign rights to an administrator or administrator group ◆ Remove rights from an administrator or administrator group ◆ Assign roles to an administrator or administrator group ◆ Remove roles from an administrator or administrator group	To grant any object rights to other administrators, an administrator must have the Grant Rights and the rights for that object. For example, to grant bundle rights to other administrators, an administrator must have both the Grant Rights and the Bundle Rights.
Create/Delete	◆ Create an administrator ◆ Rename an administrator ◆ Set/reset an administrator's password ◆ Delete an administrator	
Create/Delete Groups	◆ Create an administrator group ◆ Delete an administrator group	
Modify Groups	◆ Add administrators to a group ◆ Remove administrators from a group	
View Audit Log	◆ View an administrator's Audit tab and the events logged to that tab ◆ View an administrator group's Audit tab and the events logged to that tab	This right does not allow the administrator to view event details. To view event details, the administrator must have the View Audit Event right.
View Audit Events	◆ View an administrator's Audit tab, the events logged to that tab, and the details for the events ◆ View an administrator group's Audit tab, the events logged to that tab, and the details for the events	Setting the View Audit Events right to Allow forces the View Audit Log right to Allow.

7.2 Bundle Rights

The Bundle Rights dialog box lets you control the bundle operations that the selected administrator can perform.

- "Contexts" on page 41
- "Privileges" on page 41

7.2.1 Contexts

Specify the Bundle folders (contexts) that you want the administrator's Bundle rights to apply to. To select a folder, click *Add* to display the Contexts dialog box, browse for and select the folder (or multiple folders), then click *OK*. The rights also apply to the folder's subfolders.

7.2.2 Privileges

The *Privileges* section lets you grant the selected administrator rights to create or modify bundles, groups, and folders listed in the Contexts section.

The following rights are available:

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
View Leaf	◆ View the contents in the specified context (folder and subfolders)	Setting the View Leaf right to Deny forces all other Bundle rights to Deny. The View Leaf right must be set to Allow to perform any other bundle operations.
Modify Groups	◆ Rename a bundle group ◆ Change a bundle group's description	
Create/Delete Groups	◆ Create a bundle group ◆ Delete a bundle group ◆ Move a bundle group	Setting the Create/Delete Groups right to Allow forces the Modify Groups right to Allow. This means that an administrator who creates a group also receives rights to modify it.
Modify Group Membership	◆ Add bundles to a group ◆ Remove bundles from a group ◆ Reorder bundles within a group	
Modify Folders	◆ Rename a bundle folder ◆ Change a bundle folder's description	
Create/Delete Folders	◆ Create a bundle folder ◆ Delete a bundle folder ◆ Move a bundle folder	Setting the Create/Delete Folders right to Allow forces the Modify Folders right to Allow. This means that an administrator who creates a folder also receives rights to modify it.

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Author	◆ Create a bundle (Sandbox version) ◆ For Sandbox bundles: ◆ Edit settings on a bundle's Summary tab ◆ Edit settings on a bundle's Requirements tab ◆ Edit settings on a bundle's Actions tab ◆ Rename a bundle ◆ Move a bundle from one folder to another ◆ Copy system requirements from one bundle to another ◆ Delete a bundle ◆ Enable/disable a bundle ◆ Publish (copy) a bundle to a new bundle (Sandbox version)	
Publish	◆ Publish a bundle as a new version or a new bundle ◆ Edit settings on a bundle's Summary tab ◆ Edit settings on a bundle's Requirements tab ◆ Edit settings on a bundle's Actions tab ◆ Rename a bundle ◆ Move a bundle from one folder to another ◆ Copy system requirements from one bundle to another ◆ Delete a bundle ◆ Enable/disable a bundle ◆ Publish (copy) a bundle to a new bundle (Sandbox version)	Setting the Publish right to Allow forces the Author right to Allow. This means that an administrator who can publish bundles can also author bundles.
Modify Settings	◆ Edit settings on a bundle's Settings tab with the following exception: ◆ Cannot create or add system variables (System Variables setting) on bundles	This right applies to bundles and bundle folders. It does not apply to bundle groups because bundle groups do not have a Settings tab.

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Assign Bundles	◆ Assign bundles to devices, device groups, and device folders ◆ Assign bundle groups to devices, device groups, and device folders ◆ Assign bundles to users, user groups, and user folders ◆ Assign bundle groups to users, user groups, and user folders ◆ Remove bundle assignments from the objects listed above ◆ Remove bundle group assignments from the objects listed above	To assign bundles to devices, groups, and folders, an administrator needs this right and the Device Rights – Assign Bundles right. In other words, the administrator needs Assign Bundle rights for the bundle and the device to which the bundle is being assigned. To assign bundles to users, groups, and folders, an administrator needs this right and the User Rights – Assign Bundles right. In other words, the administrator needs Assign Bundle rights for the bundle and the user to which the bundle is being assigned.
View Audit Log	◆ View a bundle's Audit tab and the events logged to that tab ◆ View a bundle group's Audit tab and the events logged to that tab ◆ View a bundle folder's Audit tab and the events logged to that tab	This right does not allow the administrator to view event details. To view event details, the administrator must have the View Audit Event right.
View Audit Events	◆ View a bundle's Audit tab, the events logged to that tab, and the details for the events ◆ View a bundle group's Audit tab, the events logged to that tab, and the details for the events ◆ View a bundle folder's Audit tab, the events logged to that tab, and the details for the events	Setting the View Audit Events right to Allow forces the View Audit Log right to Allow.

7.3 Contract Management Rights

The Contract Management Rights dialog box lets you control the operations that the selected administrator can perform to manage contracts.

- Section 7.3.1, "Contexts," on page 43
- Section 7.3.2, "Privileges," on page 44

7.3.1 Contexts

Specify the Contract Management folders (contexts) that you want the administrator's Contract Management rights to apply to. To select a folder, click *Add* to display the Contexts dialog box, browse for and select the folder (or multiple folders), then click *OK*. The rights also apply to the folder's subfolders.

7.3.2 Privileges

The *Privileges* section lets you grant the selected administrator rights to contracts and folders listed in the Contexts section.

The following rights are available:

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
View Leaf	◆ View the contents in the specified context (folder and subfolders)	Setting the View Leaf right to Deny forces all other Contract Management rights to Deny. The View Leaf right must be set to Allow to perform any other contract management operations.
Modify	◆ Change contract details, with the following exceptions: ◆ Date Notification changes also require Create/Delete rights ◆ Change default Date Notification settings ◆ Add relationships (Workstation/Server Devices, Network Devices, Licence Entitlements, Users, Sites, Cost Centers, and Departments) to contracts ◆ Remove relationships from contracts	To add or remove a license entitlement relationship, an administrator must have this right and the License Management Rights – Modify right. In other words, an administrator needs Modify rights to both the contract and the license entitlement.
Create/Delete	◆ Create a new contract ◆ Copy a contract to create a new contract ◆ Move a contract to a different folder ◆ Delete a contract ◆ Create a Date Notification ◆ Change a Date Notification ◆ Move a Date Notification to a different folder ◆ Delete a Date Notification	
Modify Folders	◆ Change a folder’s description	
Create/Delete Folders	◆ Create a folder ◆ Delete a folder ◆ Move a folder to another folder	To move a folder, an adminstrator must have this right and the Create/ Delete right.

Access to Contract Management reports is controlled through Asset Management Report Rights. For details, see Section 7.26, “Asset Management Report Rights,” on page 73.

7.4 Credential Rights

The Credential Rights dialog box lets you control the operations that the selected administrator can perform to manage credentials.

- Section 7.4.1, "Contexts," on page 45
- Section 7.4.2, "Privileges," on page 45

7.4.1 Contexts

Specify the Credential folders (contexts) that you want the administrator's Credential rights to apply to. To select a folder, click *Add* to display the Contexts dialog box, browse for and select the folder (or multiple folders), then click *OK*. The rights also apply to the folder's subfolders.

7.4.2 Privileges

The Privileges section lets you grant the selected administrator rights to create or modify credentials, groups, and folders listed in the Contexts section.

The following rights are available:

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
View Leaf	◆ View the contents in the specified context (folder and subfolders)	Setting the View Leaf right to Deny forces all other Credential rights to Deny. The View Leaf right must be set to Allow to perform any other credential operations.
Modify	◆ Rename a credential ◆ Change a credential's login name ◆ Change a credential's password ◆ Change a credential's description	
Create/Delete	◆ Create a credential ◆ Move a credential to a different folder ◆ Delete a credential	
Modify Folders	◆ Rename a credential folder ◆ Change a folder's description	To rename a folder, an administrator must have this right and the Modify right.
Create/Delete Folders	◆ Create a credential folder ◆ Delete a credential folder ◆ Move a credential folder to another folder	To move a folder, an administrator must have this right and the Create/ Delete right.

For more information about the tasks you can perform on credentials, see "Using the Credential Vault" in the *ZENworks 11 SP3 ZENworks Control Center Reference*.

7.5 Deployment Rights

Deployment lets you discover network devices and deploy the ZENworks Adaptive Agent to them so that they become managed devices in your Management Zone. For more information, see "ZENworks Adaptive Agent Deployment" in the *ZENworks 11 SP3 Discovery, Deployment, and Retirement Reference*.

The Deployment Rights dialog box lets you control the selected administrator's ability to perform deployment operations.

The following right is available:

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Deployment	◆ Create a deployment task ◆ Launch a deployment task ◆ Abort a deployment task ◆ Rename a deployment task ◆ Modify all deployment task settings ◆ Delete a deployment task ◆ Edit a deployment package ◆ Import devices from a CSV file into the Deployable Devices list ◆ Delete devices from the Deployable Devices list	

7.6 Device Rights

The Device Rights dialog box lets you control the operations that the selected administrator can perform on devices.

- Section 7.6.1, "Contexts," on page 46
- Section 7.6.2, "Privileges," on page 47

7.6.1 Contexts

Specify the Device folders (contexts) that you want the administrator's Device rights to apply to. To select a folder, click *Add* to display the Contexts dialog box, browse for and select the folder (or multiple folders), then click *OK*. The rights also apply to the folder's subfolders.

7.6.2 Privileges

The *Privileges* section lets you grant the selected administrator rights to work with devices, including device groups and folders listed in the Contexts section.

The following rights are available:

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
View Leaf	◆ View the contents in the specified context (folder and subfolders)	Setting the View Leaf right to Deny forces all other Device rights to Deny. The View Leaf right must be set to Allow to perform any other device operations.
Modify	◆ Retire a device ◆ Rename a device ◆ Acknowledge device messages ◆ Change a device to a test device ◆ Change a test device to a non-test device ◆ Copy device settings (from the Settings tab) to other devices ◆ View and edit a device's detailed inventory (Detailed Software Hardware Inventory link on the Inventory tab)	To copy device settings, the administrator also needs the Modify Settings right.
Create/Delete	◆ Create managed devices by importing device information from a CSV file ◆ Create managed devices by manually adding device information ◆ Delete a device ◆ Move a device	
Modify Groups	◆ Rename a device group ◆ Change a device group's description	To change a device group's description, an administrator needs this right and the Modify right.
Create/Delete Groups	◆ Create a device group ◆ Delete a device group ◆ Move a device group	Setting the Create/Delete Groups right to Allow forces the Modify Groups right to Allow. This means that an administrator who creates a group also receives rights to modify it.
Modify Group Membership	◆ Add devices to a device group ◆ Remove devices from a device group ◆ Change criteria for a dynamic device group	
Modify Folders	◆ Rename a device folder ◆ Change a device folder's description	

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Create/Delete Folders	◆ Create a device folder ◆ Delete a device folder ◆ Move a device folder	Setting the Create/Delete Folders right to Allow forces the Modify Folders right to Allow. This means that an administrator who creates a folder also receives rights to modify it.
Modify Settings	◆ Edit settings on a device's Settings tab	This right applies to devices and device folders. It does not apply to device groups because device groups do not have a Settings tab.
View Audit Log	◆ View a devices' Audit tab and the events logged to that tab ◆ View a device group's Audit tab and the events logged to that tab ◆ View a device folder's Audit tab and the events logged to that tab	This right does not allow the administrator to view event details. To view event details, the administrator must have the View Audit Event right.
View Audit Events	◆ View a device's Audit tab, the events logged to that tab, and the details for the events ◆ View a device group's Audit tab, the events logged to that tab, and the details for the events ◆ View a device folder's Audit tab, the events logged to that tab, and the details for the events	Setting the View Audit Events right to Allow forces the View Audit Log right to Allow.
Configure Audit Settings	◆ Configure which events to audit for a bundle (bundle object > Settings tab > Audit Management > Events Configuration) ◆ Configure which events to audit for a bundle group (bundle group object > Settings tab > Audit Management > Events Configuration) ◆ Configure which events to audit for a bundle folder (bundle folder object > Settings tab > Audit Management > Events Configuration)	
Assign Bundles	◆ Assign bundles to devices, device groups, and device folders ◆ Assign bundle groups to devices, device groups, and device folders ◆ Remove bundle assignments from the objects listed above ◆ Remove bundle group assignments from the objects listed above	To assign bundles to devices, groups, and folders, an administrator needs this right and the Bundle Rights – Assign Bundles right. In other words, the administrator needs Assign Bundle rights for the bundle and the device to which the bundle is being assigned.

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Assign Policies	◆ Assign policies to devices, device groups, and device folders ◆ Assign policy groups to devices, device groups, and device folders ◆ Remove policy assignments from the objects listed above ◆ Remove policy group assignments from the objects listed above	To assign policies to devices, groups, and folders, an administrator needs the following rights: ◆ Assign Policies (this right) ◆ Policy Rights - Assign Policies ◆ Policy Rights - Manage Configuration Policies or Policy Rights - Manage Security Policies In other words, an administrator needs Assign Policy rights for the policy and the device to which the policy is being assigned, and he needs the Manage Configuration Policies or Manage Security Policies right depending on whether the policy is a Configuration or Security policy.
Assign Locations	◆ Assign locations and network environments to devices and device folders ◆ Assign startup locations and network environments to devices and device folders	This right does not apply to device groups because device groups do not have a Locations tab.
View Detailed Inventory	◆ View a devices detailed inventory (Detailed Software/Hardware Inventory link on Inventory tab)	This right controls view-only access. If you want an administrator to be able to edit the detailed inventory, the administrator needs the Modify right.
Manage ERI	◆ Download a device's ERI file ◆ View an ERI file's password ◆ Delete an ERI file	

7.7 Discovery Rights

The Discovery Rights dialog box lets you control the selected administrator's ability to perform discovery operations.

The following rights are available:

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Discovery	◆ Create a discovery task ◆ Launch a discovery task ◆ Abort a discovery task ◆ Rename a discovery task ◆ Modify all discovery task settings ◆ Delete a discovery task ◆ Discover advertised devices (devices that have the ZENworks preagent installed, such as OEM devices or unregistered devices)	
Edit Discovered Devices	◆ Edit the following properties for discovered devices: ◆ Discovered Type ◆ Network Type ◆ Operating System Vendor ◆ Operating System Category ◆ Operating System Platform ◆ Support/Service Pack	

7.8 Document Rights

The Document Rights dialog box lets you control the operations that the selected administrator can perform to manage documents.

- Section 7.8.1, "Contexts," on page 50
- Section 7.8.2, "Privileges," on page 51

7.8.1 Contexts

Specify the Document folders (contexts) that you want the administrator's Document rights to apply to. To select a folder, click *Add* to display the Contexts dialog box, browse for and select the folder (or multiple folders), then click *OK*. The rights also apply to the folder's subfolders.

7.8.2 Privileges

The *Privileges* section lets you grant the selected administrator rights to create or modify documents and their folders listed in the Contexts section.

The following rights are available:

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
View Leaf	◆ View the contents in the specified context (folder and subfolders)	Setting the View Leaf right to Deny forces all other Document rights to Deny. The View Leaf right must be set to Allow to perform any other document operations.
Modify	◆ Change a document's details: ◆ Document ID ◆ Path ◆ Source Location ◆ As-Of-Date ◆ Description ◆ Download and open a document ◆ Add and remove relationships with contracts ◆ Add and remove relationships with license entitlements ◆ Add and remove relations with purchase summary records	To add and remove relationships with contracts, an administrator must also have the Contract Management Rights – Modify right. In other words, an administrator needs Modify rights to both the document and the contract. To add and remove relationships with license entitlements and purchase summary records, an administrator must also have the License Management Rights – Modify right. In other words, an administrator needs Modify rights to both the document and the license entitlement or purchase summary record.
Create/Delete	◆ Upload a new document so that it is available from the ZENworks Server ◆ Link (hyperlink) to a new document ◆ Move a document to a different folder ◆ Delete a document	
Modify Folders	◆ Change a folder's description	
Create/Delete Folders	◆ Create a folder ◆ Delete a folder ◆ Move a folder to another folder	To move a folder, an administrator must have this right and the Create/Delete right.

7.9 Inventoried Device Rights

The Inventoried Device Rights dialog box lets you control the operations that an administrator can perform on inventoried devices.

- Section 7.9.1, "Contexts," on page 52
- Section 7.9.2, "Privileges," on page 52

7.9.1 Contexts

Specify the Inventoried Device folders (contexts) that you want the administrator's Inventoried Device rights to apply to. To select a folder, click *Add* to display the Contexts dialog box, browse for and select the folder (or multiple folders), then click *OK*. The rights also apply to the folder's subfolders.

7.9.2 Privileges

The *Privileges* section lets you grant the selected administrator rights to work with inventoried devices, including device folders listed in the Contexts section.

The following rights are available:

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
View Leaf	◆ View the contents in the specified context (folder and subfolders)	Setting the View Leaf right to Deny forces all other Inventoried Device rights to Deny. The View Leaf right must be set to Allow to perform any other inventoried device operations.
Modify	◆ Retire an inventoried device ◆ Rename an inventoried device ◆ Edit a device's detailed inventory (Detailed Software Hardware Inventory link on the Inventory tab)	
Create/Delete	◆ Create an inventoried device ◆ Delete an inventoried device ◆ Move an inventoried device	To create an inventoried device, an administrator also requires the Device Rights – Create/Delete right so that he has access to the Create Portable Client and Import Inventory tasks.
Modify Groups	◆ None	This right has no operational effect when assigned to an administrator.
Create/Delete Groups	◆ None	This right has no operational effect when assigned to an administrator.
Modify Group Membership	◆ None	This right has no operational effect when assigned to an administrator.
Modify Folders	◆ Rename a device folder ◆ Change a device folder's description	
Create/Delete Folders	◆ Create a device folder ◆ Delete a device folder ◆ Move a device folder	Setting the Create/Delete Folders right to Allow forces the Modify Folders right to Allow. This means that an administrator who creates a folder also receives rights to modify it.
View Detailed Inventory	◆ View a device's detailed inventory (Detailed Software/Hardware Inventory link on Inventory tab)	This right controls view-only access. If you want an administrator to be able to edit the detailed inventory, the administrator needs the Modify right.

7.10 LDAP Import Rights

The LDAP Import Rights dialog box lets you control the selected administrator's ability to import LDAP information.

The following right is available:

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
LDAP Import	◆ Create a an LDAP import task; the task imports data from an LDAP source and uses it to populate device inventory information in ZENworks Control Center ◆ Rename an LDAP import task ◆ Delete an LDAP import task ◆ Launch an LDAP import task ◆ Abort an LDAP import task ◆ View results of an LDAP import task ◆ Modify tasks settings	The LDAP Import feature is located in Configuration > Asset Inventory tab > LDAP Import Tasks.

7.11 License Management Rights

The License Management Rights dialog box lets you control the operations that the selected administrator can perform to manage licenses.

- Section 7.11.1, "Contexts," on page 53
- Section 7.11.2, "Privileges," on page 53

7.11.1 Contexts

Specify the License Management folders (contexts) that you want the administrator's License Management rights to apply to. To select a folder, click *Add* to display the Contexts dialog box, browse for and select the folder (or multiple folders), then click *OK*. The rights also apply to the folder's subfolders.

7.11.2 Privileges

The Privileges section lets you grant the administrator rights to work with the software license components associated with the contexts (folders) you selected in the Contexts section.

The following rights are available:

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
View Leaf	◆ View the contents in the specified context (folder and subfolders)	Setting the View Leaf right to Deny forces all other License Management rights to Deny. The View Leaf right must be set to Allow to perform any other license management operations.

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Modify	◆ For purchase records: ◆ Change purchase record details ◆ Create, edit, and delete purchase details for existing purchase records ◆ For catalog products: ◆ Change catalog product details ◆ Add a catalog product to a licensed product ◆ Include or exclude a catalog product from being able to be added to a licensed product ◆ For licensed products: ◆ Change licensed product details ◆ Allocate licensed products to devices ◆ Remove licensed product allocations from devices ◆ Refresh compliance status ◆ Use auto-reconcile to add discovered products and catalog products to existing licensed products ◆ For discovered products: ◆ Include or exclude a discovered product from being able to be added to a licensed product ◆ Add a discovered product to a licensed product or to a software collection ◆ Assign a Standards category to a discovered product ◆ Refresh compliance status ◆ Change the usage period ◆ For software collections: ◆ Change a software collection’s details ◆ Add discovered products to a software collection ◆ Remove discovered products from a software collection	

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Create/Delete	◆ For purchase records: ◆ Create a new purchase record ◆ Import purchase records from a file ◆ Move a purchase record from one folder to another ◆ Move a purchase record from one folder to another ◆ For catalog products: ◆ Create a new catalog product ◆ Move a catalog product from one folder to another ◆ Delete a catalog product ◆ For licensed products: ◆ Create a new licensed product ◆ Auto-reconcile to create new licensed products from discovered products ◆ Merge two or more licensed products into one ◆ Move a licensed product from one folder to another ◆ Delete a licensed product ◆ For software collections: ◆ Create a new software collection ◆ Move a software collection from one folder to another ◆ Delete a software collection	
Modify Folders	◆ Change a folder’s description	
Create/Delete Folders	◆ Create a folder ◆ Delete a folder ◆ Move a folder to another folder	To move a folder, an adminstrator must have this right and the Create/Delete right.

Access to License Management reports is controlled through Asset Management Report Rights. For details, see Section 7.26, “Asset Management Report Rights,” on page 73.

7.12 Location Rights

The Location Rights dialog box lets you control the operations that the selected administrator can perform on locations and network environments.

The following rights are available:

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Modify	◆ For locations: ◆ Rename a location ◆ Reorder locations (move up/down) ◆ Add network environments to a location ◆ Remove network environments from a location ◆ Reorder network environments for a location (move up/down) ◆ Change a location's description ◆ Configure a location's closest servers (Servers page) ◆ Modify the location's settings (Settings page) ◆ Change the "Duration to Honor" setting for the startup location ◆ For network environments: ◆ Rename a network environment ◆ Change a network environment's description ◆ Modify a network environment's match criteria (network services) ◆ Configure a network environment's closest servers (Servers page) ◆ Modify a network environment's settings (Settings page)	
Create/Delete	◆ Create a location ◆ Delete a location ◆ Create a network environment ◆ Delete a network environment	

7.13 Patch Management Rights - Device

Patch Management rights are configurable at two levels: zone and device. The zone-level Patch Management rights (see Section 7.14, "Patch Management Rights - Zone," on page 57) control the operations that are available on the Patch Management page and on device objects, while the device-level Patch Management rights control only the operations available on device objects.

7.13.1 Contexts

Specify the Device folders (contexts) that you want the administrator's Patch Management rights to apply to. To select a folder, click *Add* to display the Contexts dialog box, browse for and select the folder (or multiple folders), then click *OK*. The rights also apply to the folder's subfolders.

7.13.2 Privileges

The Privileges section lets you grant the administrator rights to perform Patch Management operations associated with the contexts (folders) you selected in the Contexts section.

The following rights are available:

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Patch Deploy	◆ Deploy a patch to a device ◆ Deploy a patch to a device group	An administrator must have this right and Bundle Rights for the patch bundle being deployed.
Assign a Baseline	◆ Assign a patch to a device group's mandatory baseline of patches	
Remove from Baseline	◆ Remove a patch from a device group's mandatory baseline of patches	
View Patch Details	◆ View information for a patch that is listed in a device's Patches list	
Recalculate Baseline	◆ Initiate an immediate check of all devices in a device group to evaluate baseline patch compliance and apply the required baseline patches if necessary	
Export Patch	◆ Export patch information to a CSV file for one or more patches selected from a device's Patches list	

7.14 Patch Management Rights - Zone

Patch Management rights are configurable at two levels: zone and device. The zone-level Patch Management rights control the operations that are available on the Patch Management page and on device objects, while the device-level Patch Management rights (see Section 7.13, "Patch Management Rights - Device," on page 56) control only the operations available on device objects.

The following zone-level Patch Management rights are available:

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Patch Deploy	◆ Deploy a patch to a device ◆ Deploy a patch to a device group ◆ Deploy a patch to a device folder	An administrator must have this right and Bundle Rights for the patch bundle being deployed.
Patch Enable	◆ Enable a patch to be deployed	
Patch Disable	◆ Disable a patch so it can't be deployed	
Patch Update Cache	◆ Update a patch in the ZENworks Server cache by downloading the patch from the subscription service	
Assign a Baseline	◆ Assign a patch to a device group's mandatory baseline of patches	

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Remove from Baseline	◆ Remove a patch from a device group's mandatory baseline of patches	
View Patch Details	◆ View information for a patch that is listed in a device's Patches list	
Export Patch	◆ Export patch information to a CSV file for one or more patches selected from a device's Patches list	
Scan Now	◆ Initiate a patch detection scan (DAU task) on devices	
Remove Patch	◆ Remove a patch from a device	
Recalculate Baseline	◆ Initiate an immediate check of all devices in a device group to evaluate baseline patch compliance and apply the required baseline patches if necessary	
Configure	◆ Configure the Patch Management zone settings (Configuration > Management Zone Settings > Patch Management)	
Update Dashboard	◆ Update the Patch Management dashboard report (Patch Management > Dashboard > Update Dashboard Report)	
New Bundles	◆ Create a new patch bundle ◆ Delete a patch bundle	
Patch Policy	◆ Create a patch policy ◆ Rename a patch policy ◆ Copy a patch policy to create a new patch policy ◆ Delete a patch policy ◆ Assign a patch policy to devices, device groups, and device folders ◆ Enable and disable a patch policy ◆ Publish a patch policy	

7.15 Policy Rights

The Policy Rights dialog box lets you control the operations that the selected administrator can perform on policies.

- Section 7.15.1, "Contexts," on page 59
- Section 7.15.2, "Privileges," on page 59

7.15.1 Contexts

Specify the Policy folders (contexts) that you want the administrator's Policy rights to apply to. To select a folder, click *Add* to display the Contexts dialog box, browse for and select the folder (or multiple folders), then click *OK*. The rights also apply to the folder's subfolders.

7.15.2 Privileges

The Privileges section lets you grant the selected administrator rights to work with policies, including policy groups and folders listed in the Contexts section.

The following rights are available:

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
View Leaf	◆ View the contents in the specified context (folder and subfolders)	Setting the View Leaf right to Deny forces all other Policy rights to Deny. The View Leaf right must be set to Allow to perform any other policy operations.
Modify Groups	◆ Rename a policy group ◆ Change a policy group's description	
Create/Delete Groups	◆ Create a policy group ◆ Delete a policy group ◆ Move a policy group	Setting the Create/Delete Groups right to Allow forces the Modify Groups right to Allow. This means that an administrator who creates a group also receives rights to modify it.
Modify Group Membership	◆ Add policies to a group ◆ Remove policies from a group ◆ Reorder policies within a group	In addition to this right, an administrator must also have the Manage Configuration Policies right or the Management Security policies right. For example, to add a Configuration policy to a group, an administrator must have the following two rights: ◆ Modify Group Membership (this right) ◆ Manage Configuration Policies
Modify Folders	◆ Rename a policy folder ◆ Change a policy folder's description	
Create/Delete Folders	◆ Create a policy folder ◆ Delete a policy folder ◆ Move a policy folder	Setting the Create/Delete Folders right to Allow forces the Modify Folders right to Allow. This means that an administrator who creates a folder also receives rights to modify it.

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Author	◆ Create a policy (Sandbox version) ◆ For Sandbox policies: ◆ Edit settings on a policy's Summary tab ◆ Edit settings on a policy's Requirements tab ◆ Edit settings on a policy's Details tab ◆ Rename a policy ◆ Move a policy ◆ Copy system requirements from one policy to another ◆ Delete a policy ◆ Enable and disable a policy ◆ Publish (copy) a policy as a new policy (Sandbox version)	In addition to this right, an administrator must also have the Manage Configuration Policies right or the Management Security policies. For example, to create a Configuration policy, an administrator must have the following two rights: ◆ Author (this right) ◆ Manage Configuration Policies
Publish	◆ Publish a policy as a new version ◆ Edit settings on a policy's Summary tab ◆ Edit settings on a policy's Requirements tab ◆ Edit settings on a policy's Details tab ◆ Rename a policy ◆ Move a policy ◆ Copy system requirements from one policy to another ◆ Delete a policy ◆ Enable and disable a policy ◆ Publish (copy) a policy as a new policy (Sandbox version)	Setting the Publish right to Allow forces the Author right to Allow. This means that an administrator who has rights to publish policies also has rights to author policies. In addition to this right, an administrator must also have the Manage Configuration Policies right or the Management Security policies. For example, to publish a Security policy, an administrator must have the following two rights: ◆ Publish (this right) ◆ Manage Security Policies
Assign Policies	◆ Assign policies to devices, device groups, and device folders ◆ Assign policy groups to devices, device groups, and device folders ◆ Assign policies to users, user groups, and user folders ◆ Assign policy groups to users, user groups, and user folders ◆ Remove policy assignments from the objects listed above ◆ Remove policy group assignments from the objects listed above	In addition to this right, an administrator must also have the Manage Configuration Policies right or the Management Security policies right and the Device Rights - Assign Policies right or User Rights - Assign Policies right. For example, to assign a Security policy to a device, an administrator must have the following two rights: ◆ Assign Policies (this right) ◆ Manage Security Policies ◆ Device Rights - Assign Policies (for the target device)

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Manage Configuration Policies	◆ Access to Windows and Linux Configuration policies	This right enables the Author, Publish, Modify Group Membership, and Assign Policies rights to apply to Windows and Linux Configuration policies. Configuration policies are provided by ZENworks Configuration Management and include the Windows Configuration policies (Browser Bookmarks policy, Dynamic Local User policy, Local File Rights policy, Printer policy, Remote Management policy, Roaming Profile policy, SNMP policy, Windows Group policy, and ZENworks Explorer Configuration policy) and the Linux Configuration policies (External Services policy and Puppet policy).
Manage Security Policies	◆ Access to Windows Security policies (including the Full Disk Encryption policy)	This right enables the Author, Publish, Modify Group Membership, and Assign Policies rights to apply to Windows Security policies.
View Audit Log	◆ View a policy's Audit tab and the events logged to that tab ◆ View a policy group's Audit tab and the events logged to that tab ◆ View a policy folder's Audit tab and the events logged to that tab	This right does not allow the administrator to view event details. To view event details, the administrator must have the View Audit Event right.
View Audit Events	◆ View a policy's Audit tab, the events logged to that tab, and the details for the events ◆ View a policy group's Audit tab, the events logged to that tab, and the details for the events ◆ View a policy folder's Audit tab, the events logged to that tab, and the details for the events	Setting the View Audit Events right to Allow forces the View Audit Log right to Allow.

7.16 Quick Task Rights

Quick Tasks are tasks that appear in ZENworks Control Center task lists (for example, Server Tasks, Workstation Tasks, Bundles Tasks, and so forth). When you click a task, either a wizard launches to step you through the task or a dialog box appears in which you enter information to complete the task.

The Quick Tasks Rights dialog box lets you control the selected administrator's ability to perform specific quick tasks.

- Section 7.16.1, "Contexts," on page 62
- Section 7.16.2, "Privileges," on page 62

7.16.1 Contexts

Specify the Device folders (contexts) that you want the administrator's Quick Task rights to apply to. To select a folder, click *Add* to display the Contexts dialog box, browse for and select the folder (or multiple folders), then click *OK*. The rights also apply to the folder's subfolders.

7.16.2 Privileges

The *Privileges* section lets you control the selected administrator's rights to perform quick tasks associated with the contexts (folders) you selected in the Contexts section.

The following rights are available:

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Shutdown/Reboot/ Wake Up Device	◆ Reboot Shutdown Devices quick task ◆ Intel AMT Power Management quick task ◆ Wake Up quick task	
Execute Processes	◆ Launch Application quick task ◆ Run Script quick task ◆ Launch Java Application quick task	
Refresh ZENworks Adaptive Agent	◆ Refresh Device quick task ◆ Refresh Policies quick task	
Install/Launch Bundles	◆ Install Bundle quick task ◆ Launch Bundle quick task ◆ Verify Bundle quick task ◆ Uninstall Bundle quick task ◆ Distribute Bundle Now quick task	
Inventory	◆ Inventory Scan quick task ◆ Inventory Wizard quick task	
Apply Image	◆ Apply Assigned Imaging Bundle (Action menu) ◆ Apply Rule-Based Imaging Bundle (Action menu)	
Take Image	◆ Take an image (Action menu)	

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Manage Endpoint Security Settings and Task	◆ Clear ZESM User Defined Password quick task ◆ Clear ZESM Local Client Self Defense Settings quick task ◆ Clear ZESM Local Firewall Registration Settings quick task ◆ FDE – Decommission Full Disk Encryption quick task ◆ FDE – Enable Additive User Capturing quick task ◆ FDE – Force Device to Send ERI File to Server quick task ◆ FDE – Update PBA User quick task	

7.17 Remote Management Rights

The Remote Management Rights dialog box lets you control the operations that the selected administrator can perform on remote devices.

- Section 7.17.1, "Contexts," on page 63
- Section 7.17.2, "Privileges," on page 63

7.17.1 Contexts

Specify the Device folders or User folders (contexts) that you want the administrator's Remote Management rights to apply to. To select a folder, click *Add* to display the Contexts dialog box, browse for and select the folder (or multiple folders), then click *OK*. The rights also apply to the folder's subfolders.

7.17.2 Privileges

The Privileges section lets you grant the administrator rights to perform remote operations for devices and users located within the contexts (folders) you selected in the Contexts section.

The following rights are available:

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Remote Control	◆ Control a remote device	Setting the Remote Control right to Allow forces the Remote View and Transfer Files rights to Allow. This means that an administrator who can remotely control a device can also remotely view the device and transfer files to and from the device.
Remote View	◆ View a remote device's desktop	

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Transfer Files	◆ Transfer files to/from a remote device ◆ Create folders on a remote device ◆ Create folders on a remote device ◆ Delete files and folders on a remote device	
Remote Execute	◆ Run executable files with system privileges on a remote device.	Granting Remote Execute rights allows an administrator to execute processes in the system space.
Remote Diagnostics	◆ Run the following diagnostic tools on a remote device: ◆ System Information (msinfo32.exe) ◆ Computer Management (compmgmt.msc) ◆ Services (services.msc) ◆ Registry Editor (regedit.exe) ◆ Run other administrator-configured diagnostic tools on a remote device	To configure other diagnostic tools to run on a remote device, an administrator must have the Zone Rights – Modify Rights setting.
Unblock Remote Management Service	◆ Reset (unblock) the remote management connection to a device	

7.18 Sharing Rights

7.19 Subscription Rights

The Subscription Rights dialog box lets you control the selected administrator's rights to create and delete subscriptions.

The following rights are available:

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Modify	◆ Rename a subscription ◆ Enable a subscription ◆ Disable a subscription ◆ Edit all subscription details on the Summary page with the following exceptions: ◆ Cannot initiate (Run Now) a subscription replication ◆ Cannot change the subscription replication schedule ◆ Add and remove subscription catalogs ◆ Modify existing subscription catalogs	
Create/Delete	◆ Create a new subscription ◆ Delete a subscription ◆ Copy a subscription to create a new subscription ◆ Move a subscription to a different folder	Setting the Create/Delete right to Allow forces the Modify right to Allow. In other words, an administrator who creates a subscription automatically receives rights to modify it.
Modify Folders	◆ Rename a subscription folder ◆ Change a subscription folder's description	
Create/Delete Folders	◆ Create a subscription folder ◆ Delete a subscription folder ◆ Move a subscription folder	Setting the Create/Delete Folders right to Allow forces the Modify Folders right to Allow. In other words, an administrator who creates a folder automatically receives rights to modify it.
Run Now	◆ Initiate (Run Now) replication for a subscription ◆ Change the subscription replication schedule	The Run Now right allows an administrator to run a subscription. When the subscription runs, it can create bundles, bundle groups and bundle folders. The administrator does not require any separate bundle rights.
Modify Settings	◆ Edit settings on the subscription's Settings tab	
View Audit Log	◆ View a subscription's Audit tab and the events logged to that tab ◆ View a subscription folder's Audit tab and the events logged to that tab	This right does not allow the administrator to view event details. To view event details, the administrator must have the View Audit Event right.
View Audit Events	◆ View a subscription's Audit tab, the events logged to that tab, and the details for the events ◆ View a subscription folder's Audit tab, the events logged to that tab, and the details for the events	Setting the View Audit Events right to Allow forces the View Audit Log right to Allow.

7.20 System Update Rights

The System Updates Rights dialog box lets you allow or deny the administrator the rights to authorize any downloaded update and also the right to deploy the authorized update to devices. The deploy options are available only if the updates are authorized.

7.20.1 Privileges

The Privileges section lets you grant the selected administrator rights to authorize and deploy updates to devices.

The following rights are available:

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Authorize Update	◆ Authorize system updates to be deployed	
Deploy	◆ Deploy a system update to devices ◆ Schedule deployments ◆ Cancel deployments ◆ Create, modify, reorder, and delete stages (also requires View Leaf rights to all devices in zone)	In addition to this right, an administrator must also have View Leaf rights for the target devices.

7.21 User Rights

The User Rights dialog box lets you control the operations that the selected administrator can perform on users.

- Section 7.21.1, “Contexts,” on page 66
- Section 7.21.2, “Privileges,” on page 67

7.21.1 Contexts

Specify the User folders (contexts) that you want the administrator’s User rights to apply to. To select a folder, click *Add* to display the Contexts dialog box, browse for and select the folder (or multiple folders), then click *OK*. The rights also apply to the folder’s subfolders.

7.21.2 Privileges

The Privileges section lets you grant the selected administrator rights to work with users and folders listed in the Contexts section.

The following rights are available:

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
View Leaf	◆ View the contents in the specified context (folder and subfolders)	Setting the View Leaf right to Deny forces all other User rights to Deny. The View Leaf right must be set to Allow to perform any other user operations.
Modify	◆ Rename a user container ◆ Change a user to a test user ◆ Change a test user to a non-test user	
Modify ZENworks Group Membership	◆ Add users to a ZENworks user group ◆ Remove users from a ZENworks user group	In addition to this right, an administrator must also have the ZENworks User Group Rights - Modify ZENworks Group Membership right for the ZENworks user group whose membership is being modified. For example, to add a user to ZENUSERGROUP1, an administrator must have these two rights: ◆ Modify ZENworks Group Membership (this right) ◆ ZENworks User Group Rights - Modify ZENworks Group Membership right for ZENUSERGROUP1
View Audit Log	◆ View a user's Audit tab and the events logged to that tab ◆ View a user group's Audit tab and the events logged to that tab ◆ View a user folder's Audit tab and the events logged to that tab	In addition to this right, an administrator must have the User Source Rights - View Audit Log right for the user sources containing the target contexts. This right does not allow the administrator to view event details. To view event details, the administrator must have the View Audit Event right.

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
View Audit Events	◆ View a user's Audit tab, the events logged to that tab, and the details for the events ◆ View a user group's Audit tab, the events logged to that tab, and the details for the events ◆ View a user folder's Audit tab, the events logged to that tab, and the details for the events	In addition to this right, an administrator must have the User Source Rights - View Audit Event right for the user sources containing the target contexts. Setting the View Audit Events right to Allow forces the View Audit Log right to Allow.
Assign Bundles	◆ Assign bundles to users, user groups, and user folders ◆ Assign bundle groups to users, user groups, and user folders ◆ Remove bundle assignments from users, user groups, and user folders ◆ Remove bundle group assignments from users, user groups, and user folders	To assign bundles to users, groups, and folders, an administrator needs this right and the Bundle Rights – Assign Bundles right. In other words, the administrator needs Assign Bundles rights for the bundle and the user to which the bundle is being assigned.
Assign Policies	◆ Assign policies to users, user groups, and user folders ◆ Assign policy groups to users, user groups, and user folders ◆ Remove policy assignments from users, user groups, and user folders ◆ Remove policy group assignments from users, user groups, and user folders	To assign policies to users, groups, and folders, an administrator needs this right and the Policy Rights – Assign Policies right and the Policy Rights - Manage Configuration Policies or Policy Rights - Manage Security Policies right. For example, to assign a Security policy to a user, an administrator must have the following three rights: ◆ Assign Policies (this right) ◆ Policy Rights - Assign Policies ◆ Policy Rights - Manage Security Policies

7.22 User Source Rights

The User Source Rights dialog box lets you grant Audit-related rights to the selected user sources.

- Section 7.22.1, "Contexts," on page 68
- Section 7.22.2, "Privileges," on page 69

7.22.1 Contexts

Specify the User Source folders (contexts) that you want the administrator's User Source rights to apply to. To select a folder, click *Add* to display the Contexts dialog box, browse for and select the folder (or multiple folders), then click *OK*. The rights also apply to the folder's subfolders.

7.22.2 Privileges

The Privileges section lets you grant the selected administrator rights to work with users and folders listed in the Contexts section.

The following rights are available:

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
View Audit Log	◆ View a user source's Audit tab and the events logged to that tab	This right does not allow the administrator to view event details. To view event details, the administrator must have the View Audit Event right.
View Audit Events	◆ View a user source's tab, the events logged to that tab, and the details for the events	Setting the View Audit Events right to Allow forces the View Audit Log right to Allow.

7.23 ZENworks User Group Rights

The ZENworks User Group Rights dialog box lets you control the selected administrator's rights to create, delete, or modify ZENworks user groups.

The following rights are available:

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Modify Groups	◆ Rename a ZENworks user group ◆ Change a ZENworks user group's description	
Create/Delete Groups	◆ Create a ZENworks user group ◆ Delete a ZENworks user group	Setting the Create/Delete Groups right to Allow forces the Modify Groups right to Allow. In other words, an administrator who creates a group automatically receives rights to modify it.
Modify ZENworks Group Membership	◆ Add users to a ZENworks user group ◆ Remove users from a ZENworks user group	In addition to this right, an administrator must also have the User Rights - Modify ZENworks Group Membership right for the users being added to or removed from the group. For example, to add USER1 to ZENUSERGROUP1, an administrator must have these two rights: ◆ Modify ZENworks Group Membership (this right) for ZENUSERGROUP1 ◆ User Rights - Modify ZENworks Group Membership right for USER1

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
View Audit Log	◆ View a ZENworks user group’s Audit tab and the events logged to that tab	This right does not allow the administrator to view event details. To view event details, the administrator must have the View Audit Event right.
View Audit Events	◆ View a ZENworks user group’s Audit tab, the events logged to that tab, and the details for the events	Setting the View Audit Events right to Allow forces the View Audit Log right to Allow.
Assign Bundles	◆ Assign bundles to a ZENworks user group ◆ Assign bundle groups to a ZENworks user group ◆ Remove bundle assignments from a ZENworks user group ◆ Remove bundle group assignments from a ZENworks user group	To assign bundles to a ZENworks user group, an administrator needs this right and the Bundle Rights – Assign Bundles right. In other words, the administrator needs Assign Bundles rights for the bundle and the ZENworks user group to which the bundle is being assigned.
Assign Policies	◆ Assign policies to a ZENworks user group ◆ Assign policy groups to a ZENworks user group ◆ Remove policy assignments from a ZENworks user group ◆ Remove policy group assignments from a ZENworks user group	To assign policies to a ZENworks user group, an administrator needs this right and the Policy Rights – Assign Policies right and the Policy Rights - Manage Configuration Policies or Policy Rights - Manage Security Policies right. For example, to assign a Security policy to a ZENworks user group, an administrator must have the following three rights: ◆ Assign Policies (this right) ◆ Policy Rights - Assign Policies ◆ Policy Rights - Manage Security Policies

7.24 Zone Rights

The Zone Rights dialog box lets you control the administrator's rights to configure settings in your ZENworks Management Zone.

The following rights are available:

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Modify User Sources	◆ Change the following settings for a user source: ◆ Username and Password ◆ Authentication Mechanisms ◆ Use SSL ◆ Root Context ◆ Description ◆ Add a user container from a source ◆ Remove a user container from a source ◆ Rename a user container ◆ Replace a user container's context with another context from the user source ◆ Add a connection to a user source ◆ Edit a connection's details (name, address, port) ◆ Remove a connection to a user source	A user source is an LDAP directory that contains users that you want to reference in your ZENworks Management Zone. User containers are the LDAP contexts in which users are located.
Create/Delete User Sources	◆ Create a user source ◆ Delete a user source	Setting the Create/Delete User Sources right to Allow forces the Modify User Sources right to Allow. In other words, an administrator who creates a user source automatically receives rights to modify it.
Modify Settings	◆ Configure Management Zone settings (Configuration > Management Zone Settings)	
Modify Zone Infrastructure	◆ Specify what content is hosted on a device (ZENworks Primary Server or Satellite) ◆ Move a device in the server hierarchy ◆ Designate a workstation as a Satellite ◆ Configure a Satellite ◆ Remove a workstation as a Satellite	

RIGHT	OPERATIONS CONTROLLED BY THE RIGHT	NOTES
Configure Registration	◆ Create a registration key ◆ Edit a registration key ◆ Delete a registration key ◆ Rename a registration key ◆ Create folders for registration keys ◆ Move a registration key from one folder to another ◆ Copy a registration key to create a new registration key ◆ Create a registration rule ◆ Edit a registration rule ◆ Delete a registration rule	
Create/Delete Local Products	◆ Create local software product definitions from device inventory ◆ Add local software product definitions into the ZENworks Knowledgebase ◆ Delete local software product definitions ◆ Delete local software product definitions	
Manage FDE PBA Override	◆ Generate response sequences for overriding the ZENworks PBA used with ZENworks Full Disk Encryption	
View Audit Dashboard	◆ View the Zone Audit Dashboard and the events logged to the dashboard	This right does not allow the administrator to view event details. To view event details, the administrator must have the View Audit Event right.
View Audit Events	◆ View the Zone Audit Dashboard, the events logged to the dashboard, and the details for the events	Setting the View Audit Events right to Allow forces the View Audit Log right to Allow.
Configure Audit Settings	◆ Configure the Audit settings (Events Configuration, Local Audit Logging, and Audit Purge Schedule) for the zone	The Audit settings are under the Configuration tab > Zone Management Settings > Audit Management.
Delete News Alerts	◆ Delete ZENworks news alerts	
Update News Alerts	◆ Generate response sequences for overriding the ZENworks PBA used with ZENworks Full Disk Encryption	

7.25 Inventory Report Rights

The Inventory Report Rights panel allows you to control an administrator's rights to edit and run the standard and custom inventory reports.

Each report folder has rights associated with it, governing all the reports within that folder. For example, if you have full rights to a report folder, you can edit a report; but with view/execute rights, you can only see the report and run it. With inventory report rights, you can limit who has access to certain reports and who can edit them. The report folder type, custom or standard, and the report name are listed along with the rights associated with the folder. The choices are *Remove All Rights*, *Assign View/Execute Rights*, and *Assign Full Rights*.

7.25.1 Available Tasks

You can perform the following tasks:

Task	Steps	Additional Details
Remove all rights	1. Select the report folder. 2. Click *Edit* > *Remove All Rights*.	This removes all rights to the folder, so the specified administrator cannot see it.
Assign view/execute rights	1. Select the report folder. 2. Click *Edit* > *Assign View/ Execute Rights.*	This allows the specified administrator to view and execute a report in the specified folder, but not to edit, move, or delete a report in that folder.
Assign full rights	1. Select the report folder. 2. Click *Edit* > *Assign Full Rights*.	This gives the specified administrator full rights to create, edit, move, and delete reports. For standard reports, this setting is the same as *View/Execute*, because you cannot alter a standard report.

For more information on Inventory Report Rights, see "Inventory Report Rights" in the Asset Inventory Reference.

7.26 Asset Management Report Rights

The Asset Management Report Rights panel allows you to control an administrator's rights to edit and run the standard and custom Asset Management reports.

Each report folder has rights associated with it, governing all the reports within that folder. For example, if you have full rights, you can edit a report; but with view/execute rights, you can only see the report and run it. With asset management report rights, you can limit who has access to certain reports and who can edit them. The report folder type, custom or standard, and the report name are listed along with the rights associated with the folder. The choices are *Remove All Rights*, *Assign View/ Execute Rights*, and *Assign Full Rights*.

7.26.1 Available Tasks

You can perform the following tasks:

Task	Steps	Additional Details
Remove all rights	1. Select the report folder. 2. Click *Edit* > *Remove All Rights*.	This removes all rights to the folder, so the specified administrator cannot see it.
Assign view/execute rights	1. Select the report folder. 2. Click *Edit* > *Assign View/ Execute Rights.*	This allows the specified administrator to view and execute a report in the specified folder, but not to edit, move, or delete a report in that folder.
Assign full rights	1. Select the report folder. 2. Click *Edit* > *Assign Full Rights*.	This gives the specified administrator full rights to create, edit, move, and delete reports. For standard reports, this setting is the same as *View/Execute*, because you cannot alter a standard report.

For information on Configuring Asset Management Report Rights, see"Configuring Report Rights"in the Asset Management Reference.