

Novell iManager

2.7

October 12, 2007

ADMINISTRATION GUIDE

www.novell.com



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

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

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

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

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

Contents

About This Guide	9
1 Overview	11
1.1 What's New in Version 2.7	11
1.2 Additional Resources	12
2 Accessing iManager	13
2.1 Using a Supported Web Browser	13
2.2 Accessing iManager	13
2.2.1 Accessing Server-based iManager	13
2.2.2 Accessing iManager Workstation	14
2.3 Access Modes	14
2.4 Authenticating	15
2.4.1 Tree Name Field	15
2.4.2 Logging In to a Server without a Replica	15
2.4.3 Unsuccessful Authentication	15
2.4.4 Expired Password Information	16
2.4.5 Contextless Login Using Alternate Object Classes and/or Alternate Attributes	16
2.5 iManager Session Time-Outs	17
3 Navigating the iManager Interface	19
3.1 iManager Interface	19
3.1.1 Header Frame	20
3.1.2 Navigation Frame	20
3.1.3 Content Frame	21
3.2 Special Characters	22
4 Browsing Objects	25
4.1 Using the Object View	26
4.1.1 Tree	26
4.1.2 Browse	28
4.1.3 Search	29
4.2 Using the Object Selector	31
4.2.1 Browse	32
4.2.2 Search	32
5 Roles and Tasks	35
5.1 Navigating Roles and Tasks	35
5.1.1 Selecting and Filtering Objects	35
5.2 Directory Administration	38
5.2.1 Copying an Object	38
5.2.2 Creating an Object	39
5.2.3 Deleting an Object	39
5.2.4 Modifying an Object	39
5.2.5 Moving an Object	39

5.2.6	Renaming an Object	40
5.3	Groups	40
5.3.1	Creating a Group	40
5.3.2	Deleting a Group	41
5.3.3	Modifying a Group	41
5.3.4	Modifying Members of Group	41
5.3.5	Move Group	41
5.3.6	Rename Group	41
5.3.7	Viewing My Groups	42
5.4	Help Desk	42
5.4.1	Clearing a Lockout	42
5.4.2	Creating a User	42
5.4.3	Setting a Password	42
5.5	Partitions and Replicas	42
5.5.1	Creating a Partition	43
5.5.2	Merging a Partition	43
5.5.3	Moving a Partition	43
5.5.4	Viewing Replica Information	44
5.5.5	Viewing Partition Information	44
5.5.6	Using the Filtered Replica Wizard	44
5.6	Rights	45
5.6.1	Modifying the Inherited Rights Filter	45
5.6.2	Modifying Trustee Rights	46
5.6.3	Rights to Other Objects	46
5.6.4	Viewing Effective Rights	46
5.7	Schema	47
5.7.1	Adding an Attribute	47
5.7.2	Viewing Attribute Information	47
5.7.3	Viewing Class Information	48
5.7.4	Creating an Attribute	48
5.7.5	Creating a Class	48
5.7.6	Deleting an Attribute	48
5.7.7	Deleting a Class	49
5.7.8	Extending a Schema	49
5.7.9	Extending an Object	49
5.8	Users	49
5.8.1	Creating a User	50
5.8.2	Deleting a User	50
5.8.3	Disabling an Account	50
5.8.4	Enabling an Account	51
5.8.5	Modifying a User	51
5.8.6	Moving a User	51
5.8.7	Renaming a User	51

6 Configuring and Customizing iManager 53

6.1	Role-Based Services	53
6.1.1	RBS Objects in eDirectory	54
6.1.2	Installing RBS	56
6.1.3	Removing RBS	56
6.2	RBS Configuration	57
6.2.1	The Role Tab	58
6.2.2	The Task Tab	60
6.2.3	The Property Book Tab	61
6.2.4	The Module Tab	62
6.2.5	The Category Tab	63
6.2.6	Plug-In Studio	64

6.2.7	Editing Member Associations	66
6.2.8	Editing Owner Collections	66
6.3	RBS Reporting	66
6.3.1	Creating Reports	67
6.3.2	Using Reports	67
6.4	iManager Server	69
6.4.1	Configure iManager	69
6.4.2	Security	70
6.4.3	Look and Feel	71
6.4.4	Logging Events	71
6.4.5	Authentication	71
6.4.6	RBS	72
6.4.7	Plug-In Download	73
6.4.8	Misc	73
6.5	Object Creation List	74
6.5.1	Adding an Object Class to the Creation List	74
6.5.2	Deleting an Object Class from the Creation List	74
6.6	Plug-In Module Installation	74
6.6.1	Available Novell Plug-in Modules	75
6.6.2	Installed Novell Plug-in Modules	75
6.7	Downloading and Installing Plug-in Modules	75
6.7.1	If RBS is Configured	76
6.7.2	Uninstalling a Plug-in Module	76
6.7.3	Customizing the Plug-In Download Location	76
6.8	E-Mail Notification	78
6.8.1	Mail Server Configuration	78
6.8.2	Task Event Notification	78
6.9	Views	79
6.9.1	Showing and Hiding iManager Views	79
7	Preferences	81
7.1	Manage Favorites	81
7.2	Object Selector	81
7.3	Object View	82
7.4	Set Initial View	82
7.5	Language	82
8	Troubleshooting	83
8.1	Authentication Issues	83
8.1.1	HTTP 404 Errors	84
8.1.2	HTTP 500 Errors	84
8.1.3	601 Error Messages	85
8.1.4	622 Error Messages	85
8.1.5	632 Error Messages	85
8.1.6	634 Error Messages	85
8.1.7	669 Error Messages	85
8.2	Deleting and Re-creating User Accounts with the Same Name (Windows XP/2000)	86
8.3	DNS 630 Error Message Appears When Creating a Property Book with Invalid Characters in Name	86
8.4	eDirectory Maintenance Task Errors	86
8.5	Enabling Debug Messages for Install and Configure	86
8.6	History Does Not Automatically Sync Across Multiple Simultaneous User Logins	87
8.7	iManager Doesn't Work after Installing Groupwise 7.0 WebAccess (Windows Server 2000/	

2003)	87
8.8 Missing Attribute, Object, or Value Errors	87
8.9 Missing Roles or Tasks in the Configure View	87
8.9.1 Possible Missing Roles or Tasks	87
8.9.2 Possible Reasons Why You Are Not an Authorized User	88
8.10 Performing a System Restore from Image Software	88
8.11 Running eDirectory and iManager on the Same Machine (Windows only)	88
8.12 "Service Unavailable" Message Appears During Multiple Plug-In Installs	89
8.13 Tomcat	89
8.13.1 Starting and Stopping Tomcat	90
8.13.2 Tomcat Ports	90
8.14 "Unable to Determine Universal Password Status" Error	90
8.15 (Windows) iManager workstation does not display information	91
9 Configuring for iManager Auditing	93
9.1 Installing the IMAN_EN.LSC File in iManager	93
9.2 Enabling Auditing in iManager	94
10 Best Practices and Common Questions	95
10.1 Backup and Restore Options	95
10.2 Coexistence with previous versions of iManager 2.x and Role-Based Services	95
10.3 Collections	96
10.4 Failed Installs	96
10.4.1 Windows	96
10.4.2 Linux	97
10.5 High Availability: Running iManager in a Clustered Environment	97
10.6 Patching iManager	98
10.7 Performance Tuning	98
10.7.1 Using Dynamic Groups with RBS	98
10.7.2 Role Assignments	98
10.8 iManager AppArmor Profile	99
A iManager Security Issues	101
A.1 Secure LDAP Certificates	101
A.2 Self-Signed Certificates	102
A.3 iManager Authorized Users	102
A.4 Preventing Username Discovery	103
A.5 Tomcat Settings	103
A.6 Encrypted Attributes	104
A.7 Secure Connections	104
B Novell Plug-in Modules	105

About This Guide

This guide describes how to administer Novell® iManager 2.7, and contains the following sections:

- ♦ Chapter 1, “Overview,” on page 11
- ♦ Chapter 2, “Accessing iManager,” on page 13
- ♦ Chapter 3, “Navigating the iManager Interface,” on page 19
- ♦ Chapter 4, “Browsing Objects,” on page 25
- ♦ Chapter 9, “Configuring for iManager Auditing,” on page 93
- ♦ Chapter 6, “Configuring and Customizing iManager,” on page 53
- ♦ Chapter 7, “Preferences,” on page 81
- ♦ Chapter 8, “Troubleshooting,” on page 83
- ♦ Chapter 10, “Best Practices and Common Questions,” on page 95

Audience

This guide is intended for network 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, or go to [Novell Documentation Feedback \(http://www.novell.com/documentation/feedback.html\)](http://www.novell.com/documentation/feedback.html) and enter your comments there.

Documentation Updates

For the most current version of the *iManager 2.7 Administration Guide*, see the English version of the documentation at the [iManager 2.7 documentation site \(http://www.novell.com/documentation/imanager27/index.html\)](http://www.novell.com/documentation/imanager27/index.html).

Additional Documentation

- ♦ *iManager 2.7 Installation Guide* (<http://www.novell.com/documentation/imanager27>)
- ♦ Tomcat servlet container (<http://jakarta.apache.org/tomcat>)
- ♦ Java® Web site (<http://java.sun.com>)
- ♦ eDirectory™ home (<http://www.novell.com/products/edirectory>)
- ♦ eDirectory documentation (<http://www.novell.com/documentation/edir88/index.html>)
- ♦ eDirectory Cool Solutions community (<http://www.novell.com/cool solutions/nds>)
- ♦ Novell Technical Services (<http://support.novell.com>)

Documentation Conventions

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

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

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

Overview

1

Novell® iManager is a Web-based administration console that provides secure, customized access to network administration utilities and content from virtually anywhere you have access to the Internet and a Web browser.

iManager provides the following:

- ♦ Single point of administration for Novell eDirectory™ objects, schema, partitions, and replicas
- ♦ Single point of administration for many other network resources
- ♦ Management of many other Novell products using iManager plug-ins
- ♦ Role-Based Services (RBS) for delegated administration

Because iManager is a Web-based tool, it enjoys several advantages over client-based administrative tools:

- ♦ Upgrade once, on the server, for all administrative users
- ♦ Changes to iManager look, feel, and functionality are immediately available to all administrative users
- ♦ Do not need to open additional administrative ports for remote access. iManager leverages standard HTTP ports (80/443)
- ♦ Not necessary to download and maintain an administrative client
- ♦ Not necessary to keep client software synchronized with changes to server software

1.1 What's New in Version 2.7

Novell iManager 2.7 contains the following new features:

Web Server Support: iManager 2.7 now requires and installs only Tomcat 5 in support of its Web services. Apache is no longer installed or configured by iManager. However, iManager can co-exist with Apache or IIS if those are properly configured. For more information, consult your Apache or IIS documentation.

Tree View: The iManager tree view approximates functionality available in ConsoleOne's Console View. The left-side navigation frame displays the tree structure of the current directory tree, and lets you navigate that tree structure, expanding and collapsing container objects as necessary. The right-side content frame displays contents and menu items for the object selected in the navigation frame.

File System Browse: iManager 2.7 lets you browse through an eDirectory Volume object to the underlying NCP-enabled volume. Within the volume structure, you can select File and/or Directory objects. The actual tasks you can perform on file system objects is provided by the NSS iManager plug-in, which is available separately.

File system browsing does not support accessing the file system through NCP Server objects or NSS junction point objects.

File system browsing is available from the Object Selector, Object Browse, and Tree view, but is not available in Advanced Browsing mode. Also, file system browsing is not accessible from the Search or Advanced Search panes.

Enhanced Volume Restriction and File System Rights Control For Template Object: iManager 2.7 now provides access to additional Template object property pages that let you specify Volume space restrictions and specific file system rights assignments for new objects created through the template.

Available Novell Plug-in Modules: iManager 2.7 lists all the available iManager plug-ins contained in the packages directory/download site by default. Previous versions of iManager listed only the updates to the installed plug-ins modules.

Subordinate Count: In iManager 2.7 both the Object View and Tree View offer the ability to list a subordinate object count next to each container object in the view.

1.2 Additional Resources

For more information on topics relevant to Novell iManager, refer to the following Web sites:

- ♦ Tomcat servlet container (<http://jakarta.apache.org/tomcat>)
- ♦ How to setup Tomcat to use a proxy (<http://jakarta.apache.org/tomcat/tomcat-4.1-doc/proxy-howto.html>)
- ♦ Java* Web site (<http://java.sun.com>)
- ♦ Microsoft* Windows* Web Services (<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/iis/default.asp>)
- ♦ Novell eDirectory product home page (<http://www.novell.com/products/edirectory>)
- ♦ Novell eDirectory product documentation (<http://www.novell.com/documentation/eDirectory.html>)
- ♦ Novell eDirectory Cool Solutions community (<http://www.novell.com/cool solutions/nds>)

Accessing iManager

2

You access Novell® iManager via a Web browser. This section includes the following topics:

- ♦ [Using a Supported Web Browser \(page 13\)](#)
- ♦ [Accessing iManager \(page 13\)](#)
- ♦ [Access Modes \(page 14\)](#)
- ♦ [Authenticating \(page 15\)](#)
- ♦ [iManager Session Time-Outs \(page 17\)](#)

2.1 Using a Supported Web Browser

For iManager access and complete use of all its features, use one of the following Web browsers. Although you might be able to access iManager via a Web browser not listed, we do not guarantee or support full functionality with any browser other than the following:

- ♦ Microsoft IE 6 SP1 on Windows 2000
- ♦ Microsoft IE 6 SP2 on Windows XP
- ♦ Microsoft IE 7
- ♦ Firefox* 1.5.x, or 2.x

In order for some iManager wizards and help to work, you must enable pop-up windows in your Web browser. If you use an application that blocks pop-up windows, then disable the blocking feature while working in iManager or allow pop-ups from the iManager host.

If you have configured your Web browser to not display Web site images, the iManager interface may become garbled and unusable. In Firefox v1.5.x, for example, users can disable image loading from *Tools > Options > Content*.

2.2 Accessing iManager

Accessing iManager varies based on the iManager version (server-based or workstation) and the platform on which iManager is running.

For information on installing iManager, see “[Installing a New Version of iManager](#)” in the *iManager 2.7 Installation Guide*.

2.2.1 Accessing Server-based iManager

To access server-based iManager:

- 1 Enter one of the following in the Address (URL) field of a supported Web browser.

Because iManager 2.7 uses only Tomcat 5 for its Web server requirements, on platforms other than Novell Open Enterprise Server 2 (OES 2) you must specify the Tomcat port as part of the iManager URL. The default URL to start iManager 2.7 is as follows:

Secure URL: `https://<server ip address>:8443/nps/iManager.html`

iManager 2.7 on the OES 2 platform, both Linux and NetWare, use the following default iManager URL:

Secure URL: `https://<server ip address>/nps/iManager.html`

Although slightly different iManager URLs might work on some platforms, Novell recommends using these URLs for consistency.

- 2 Log in using your username, password and treename.

2.2.2 Accessing iManager Workstation

To access iManager Workstation:

- 1 Execute the appropriate iManager Workstation startup script.

Linux: Navigate to the `imanager/bin` directory and execute `./iManager.sh`.

NOTE: If you plan to run iManager Workstation as a non-root user in the future, do not run iManager as root the first time.

Windows: Execute `imanager\bin\iManager.bat`.

- 2 Log in using your username, password and treename.

2.3 Access Modes

When you start iManager, you are granted an *access mode* based on the rights you've been assigned. iManager has three access modes. The mode you are in is displayed on the iManager homepage.

Unrestricted Access: This is the default mode before RBS is configured. It displays all of the roles and tasks installed. Although all roles and tasks are visible, the authenticated user still needs the necessary rights to use the tasks.

There is a setting that you can add to the `config.xml` file which forces Unrestricted Access, even if Role-Based Services is installed. To force Unrestricted Access for all users, add this setting to `TOMCAT_HOME\webapps\nps\WEB-INF\config.xml`, then restart Tomcat:

```
<setting>
<name><![CDATA[RBS.forceUnrestricted]]></name>
<value><![CDATA[true]]></value>
</setting>
```

For information about restarting Tomcat, see [“Starting and Stopping Tomcat” on page 90](#).

NOTE: When using iManager in Unrestricted mode, you typically see the following message on the iManager Home Page: Notice: Some of the roles and tasks are not available. Clicking *View Details* might display a Not supported by current authenticators message for several of the tasks, even though the tasks work correctly. This message is misleading, and iManager removes these messages after you configure RBS.

Assigned Access: Displays only the roles and tasks assigned to the authenticated user. This mode takes full advantage of the Role-Based Services technology.

Collection Owner: Displays all of the roles and tasks installed in the collection. It allows you to use all of the roles and tasks in the collection, even if specific roles have not been assigned. Role-Based Services must be installed in order to use this mode. Adding a group or user as a collection owner does not assign any RBS rights. To assign rights you must make explicit RBS role assignments or make trustee assignments.

NOTE: The collection owner sees all roles and tasks, regardless of role membership.

2.4 Authenticating

Be aware of the following issues related to iManager authentication:

- ♦ [Section 2.4.1, “Tree Name Field,” on page 15](#)
- ♦ [Section 2.4.2, “Logging In to a Server without a Replica,” on page 15](#)
- ♦ [Section 2.4.3, “Unsuccessful Authentication,” on page 15](#)
- ♦ [Section 2.4.4, “Expired Password Information,” on page 16](#)
- ♦ [Section 2.4.5, “Contextless Login Using Alternate Object Classes and/or Alternate Attributes,” on page 16](#)

NOTE: If your network has more than three servers, or one or more servers that do not host eDirectory™ replicas, you must have SLP properly configured for iManager to log in. For more information, see the [Novell Open Enterprise Server SLP documentation \(http://www.novell.com/documentation/oes/networking-protocols.html#slp\)](http://www.novell.com/documentation/oes/networking-protocols.html#slp).

2.4.1 Tree Name Field

If eDirectory is installed and running on another port besides the default port 524, you can use the IP address or DNS name of the eDirectory server to log in if you also specify the port (for example, 127.0.0.1: 1080). If you use the tree name to log in, you do not have to specify a port.

Possible values for the Tree Name field are the tree name, the server IP address, and the server DNS name. For best results, use the IP address.

2.4.2 Logging In to a Server without a Replica

If necessary, iManager can log in to the eDirectory tree using a server that does not host an eDirectory replica. To do this, iManager maintains a connection cache with the information it needs to successfully log in. To populate the connection cache, the first time you login to an eDirectory tree with iManager you must log in to a server that hosts a replica.

Restarting Tomcat or the iManager server clears the connection cache, so the first time iManager logs in following one of these events, you must log in to a server that hosts a replica.

2.4.3 Unsuccessful Authentication

Login failures occur for a variety of reasons. Authentication error messages are addressed in [“Authentication Issues” on page 83](#).

For information about limiting the error messages that iManager displays upon a failed authentication attempt, see [“Preventing Username Discovery” on page 103](#).

2.4.4 Expired Password Information

If a password expires, the user sees a message to this effect. However, users might not be aware that grace logins can be quickly consumed, depending on certain operations such as modifying a dynamic group, simple find, and setting a simple password.

These operations consume additional grace logins each time a user performs a task. We highly recommend that you encourage users to change their passwords the first time they are prompted.

2.4.5 Contextless Login Using Alternate Object Classes and/or Alternate Attributes

To enable contextless authentication using an alternate object type, do the following:

- 1 Open iManager and browse to *Configure > iManager Server > Configure iManager > Authentication*.

If you do not see this task, you are not an authorized user. See [“Authorized Users” on page 70](#).

- 2 Set *Public Username* and *Password* to a user that has rights to read the desired attributes.
- 3 Modify `TOMCAT_HOME\webapps\nps\WEB-INF\config.xml` to include a `<Setting>` property that lists the attributes you want to add to the contextless search, and then restart Tomcat.

For information about restarting Tomcat, see [“Starting and Stopping Tomcat” on page 90](#).

For example, the following XML adds the Alias and User objects to the contextless search:

```
<setting>
<name><![CDATA[Authenticate.Form.ContextlessLoginClass.NDAP.treename]]>
</name>
  <value><![CDATA[User]]></value>
  <value><![CDATA[Alias]]></value>
</setting>
```

Similarly, the following XML allows users to log in with the CN or uniqueID attribute:

```
<setting>
<name><![CDATA[Authenticate.Form.ContextlessLoginSearchAttributes.NDAP
.treename]]></name>
  <value><![CDATA[CN]]></value>
  <value><![CDATA[uniqueID]]></value>
</setting>
```

IMPORTANT:

- ♦ In the sample code above, replace *treename* with the name of the appropriate directory tree in lower case.
 - ♦ If you save any iManager Server settings from the Configure iManager task after editing the config.xml file, verify that the treename is still in lowercase or customized contextless login will fail.
-

2.5 iManager Session Time-Outs

iManager session time-outs are controlled by a time-out setting in `TOMCAT_HOME\webapps\nps\WEB-INF\web.xml`. Remove the comment tags to specify a time-out, in minutes, other than the default value of 30, as shown by the following example:

```
<session-config>  
<session-timeout>10</session-timeout>  
</session-config>
```


Navigating the iManager Interface

3

This section describes how to navigate through the Novell® iManager 2.7 interface.

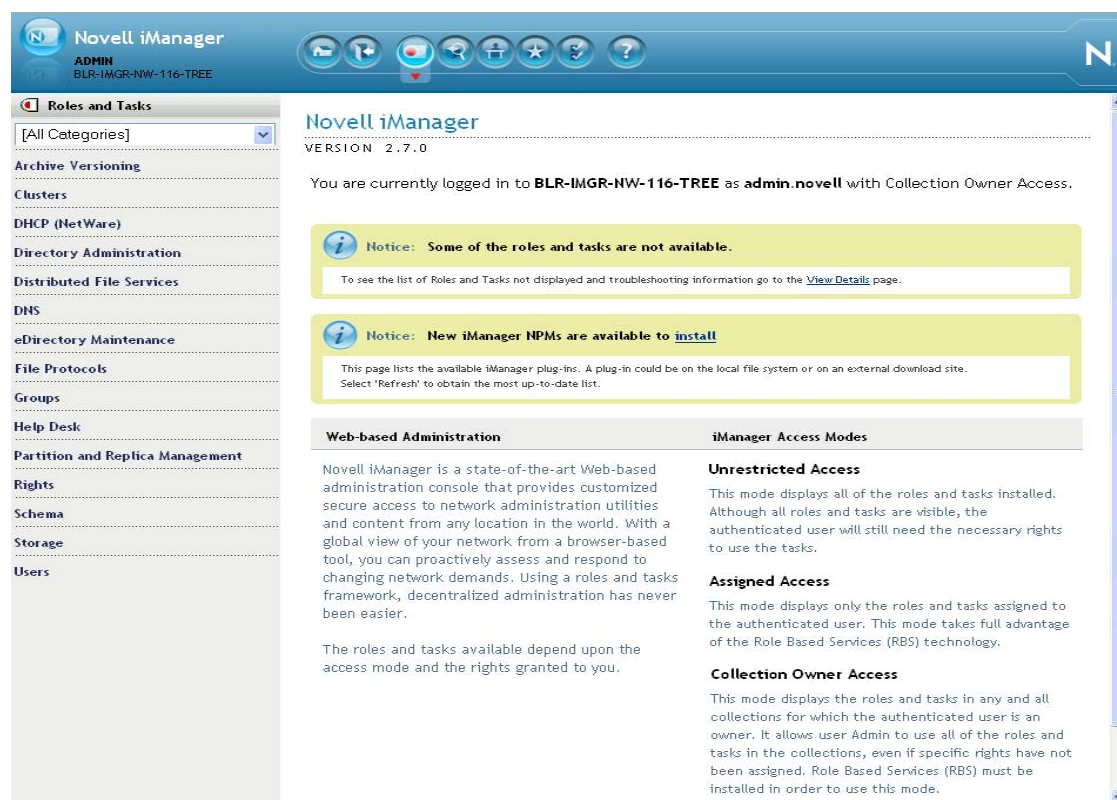
- ♦ [Section 3.1, “iManager Interface,” on page 19](#)
- ♦ [Section 3.2, “Special Characters,” on page 22](#)

3.1 iManager Interface

The iManager interface comprises three main regions, or frames.

- ♦ [Header Frame](#)
- ♦ [Navigation Frame](#)
- ♦ [Content Frame](#)

Figure 3-1 iManager interface with default Roles and Tasks view



NOTE: Use only the buttons within the interface when you are navigating in iManager. Do not use the Web browser's navigation buttons (*Back*, *Next*, etc.)

To change the default view in Preferences, see [“Set Initial View” on page 82](#).









3.1.1 Header Frame

The Header frame is a largely static frame that occupies the top of the iManager interface. It provides icons with which you can access iManager's various views. A *view* is a combination of Navigation and Content frames that deliver specific management functionality. For example, the default Roles and Tasks view lets you select a given task in the Navigation frame, and then perform the selected task in the Content frame.

Figure 3-2 iManager Header frame



The iManager Header frame includes the following icons:

-  Home: Returns the Content frame to its default view (as in Figure 3-1).
-  Exit: Logs you out of eDirectory.
-  Roles and Tasks: This view displays all the tasks you are authorized to perform in the Navigation frame. This is iManager's default view. For more information, see [Chapter 5, "Roles and Tasks," on page 35](#).
-  View Objects: This view contains browsing and searching functionality to find objects, including a Tree View feature similar to that used in ConsoleOne™. For more information, see [Chapter 4, "Browsing Objects," on page 25](#).
-  Configure: This view contains Role-Based Services, iManager Server, Object Creation List, Plug-in Installation, E-mail Notification, and Views, all of which you can configure as you want.
-  Favorites: This view displays your most frequent tasks, selected from the Preferences > Favorites page.
-  Preferences: This view sets your preferences according to your most frequent tasks, how the Object Selector displays, how your Object View displays, what view appears after logging in to iManager, and what language iManager displays in.
-  Help: Displays applicable context-sensitive help information, as determined by the current Content frame.

Additionally, the Header frame identifies the currently authenticated user and the treename to iManager in the upper left.

For information on how to change iManager's default view, see [Chapter 6, "Configuring and Customizing iManager," on page 53](#).

3.1.2 Navigation Frame

The Navigation frame resides along the left side of the iManager UI. It displays task and functionality options related to the currently selected view. For example, the default Roles and Tasks view lists all the tasks your are authorized to perform. Tasks are organized into categories. The list of categories and tasks varies based on the installed plug-ins and the rights granted to you as an authenticated iManager user.

Figure 3-3 Contents of the Navigation frame when in the Roles and Tasks view



The ordering of tasks within each category is determined by the author of the applicable iManager plug-in. Base plug-in tasks (those that are included with iManager) typically display before tasks from other plug-ins.


3.1.3 Content Frame

The Content frame provides the specific task or object interface, based on the current selection in the Navigation frame.


Figure 3-4 The default contents of the iManager Content view

Novell iManager
VERSION 2.7.0

You are currently logged in to NW65-54-TREE as admin.lab with Collection Owner Access.

 Notice: **Some of the roles and tasks are not available.**

To see the list of Roles and Tasks not displayed and troubleshooting information go to the [View Details](#) page.

 Notice: **New iManager NPMs are available to [install](#)**

This page lists the available iManager plug-ins. A plug-in could be on the local file system or on an external download site. Select 'Refresh' to obtain the most up-to-date list.

Web-based Administration	iManager Access Modes
Novell iManager is a web-based management tool. The functionality of the roles and tasks displayed in the left navigation frame depend upon the rights granted to your user object.	<p>Unrestricted Access</p> <p>This mode displays all of the roles and tasks installed. Although all roles and tasks are visible, the authenticated user will still need the necessary rights to use the tasks.</p> <p>Assigned Access</p> <p>This mode displays only the roles and tasks assigned to the authenticated user. This mode takes full advantage of the Role Based Services (RBS) technology.</p> <p>Collection Owner Access</p> <p>This mode displays the roles and tasks in any and all collections for which the authenticated user is an owner. It allows user Admin to use all of the roles and tasks in the collections, even if specific rights have not been assigned. Role Based Services (RBS) must be installed in order to use this mode.</p>

When a task is not selected, the Content frame displays the iManager homepage with general information related to your iManager access rights.

3.2 Special Characters

In iManager, some characters have special significance and must be escaped with the backslash (\) character:

NDAP (eDirectory):

- ♦ Period (.)
- ♦ Equal sign (=)
- ♦ Plus sign (+)
- ♦ Backslash (\)

LDAP:

- ♦ DN's and = + \ @; < >

- ♦ Leading #
- ♦ Leading or trailing spaces

For LDAP, any character can be specified with \xx. See RFC 2253 (<http://www.faqs.org/rfcs/rfc2253.html>) for more information.

Browsing Objects

4

iManager lets you manipulate and manage directory objects. There are two paradigms for doing this. First, you can browse for and select the objects with which you want to work, and then specify the task you want to perform on those objects (object-then-task.) Second, you can select the task you want to perform, and then specify the objects to which you want to apply the task (task-then-object.) Either way of doing things is valid, and iManager lets you use the method with which you are most comfortable.

iManager provides the Object View for those from the object-then-task school, and the Object Selector for those from the task-then-object school. The Object Selector is used extensively in the Roles and Tasks view. For more information, see [Chapter 5, “Roles and Tasks,” on page 35](#).

This chapter includes the following sections:

- ♦ [Section 4.1, “Using the Object View,” on page 26](#)
- ♦ [Section 4.2, “Using the Object Selector,” on page 31](#)

NOTE: iManager 2.7 now supports browsing and selecting objects in an NCP-enabled file system. Access file system objects through Server and Volume objects in the directory tree.

The ability to browse and select file system objects is available from both the Object View and the Object Selector. However, the actual tasks available for file system objects is provided by the NSS iManager plug-in, which is available separately.

Regardless of the tool you are using, remember the following guidelines when specifying object names:

- ♦ If the following characters are part of a dotted eDirectory[®] name, escape them with a backslash (\). You don't need escape characters in most values, but you do need them when the name is a distinguished name or relative distinguished name.
 - ♦ Period (.)
 - ♦ Equal sign (=)
 - ♦ Plus sign (+)
 - ♦ Backslash (\)
- ♦ If the following characters are part of a name you want to specify in a search, escape them with a backslash (\):
 - ♦ Asterisk (*)
 - ♦ Backslash (\)

For example:

- ♦ To search for all objects containing a period, use = *.* as the search filter
- ♦ To search for all objects containing a plus, use = *+* as the search filter
- ♦ To search for all objects containing a backslash, use = ** as the search filter

4.1 Using the Object View

The Object view is designed to let you browse for and locate objects in the directory. Once you have selected the objects with which you want to work, you can then specify the tasks to perform on those objects. Open the Object view by selecting the View Objects icon in the Header frame.

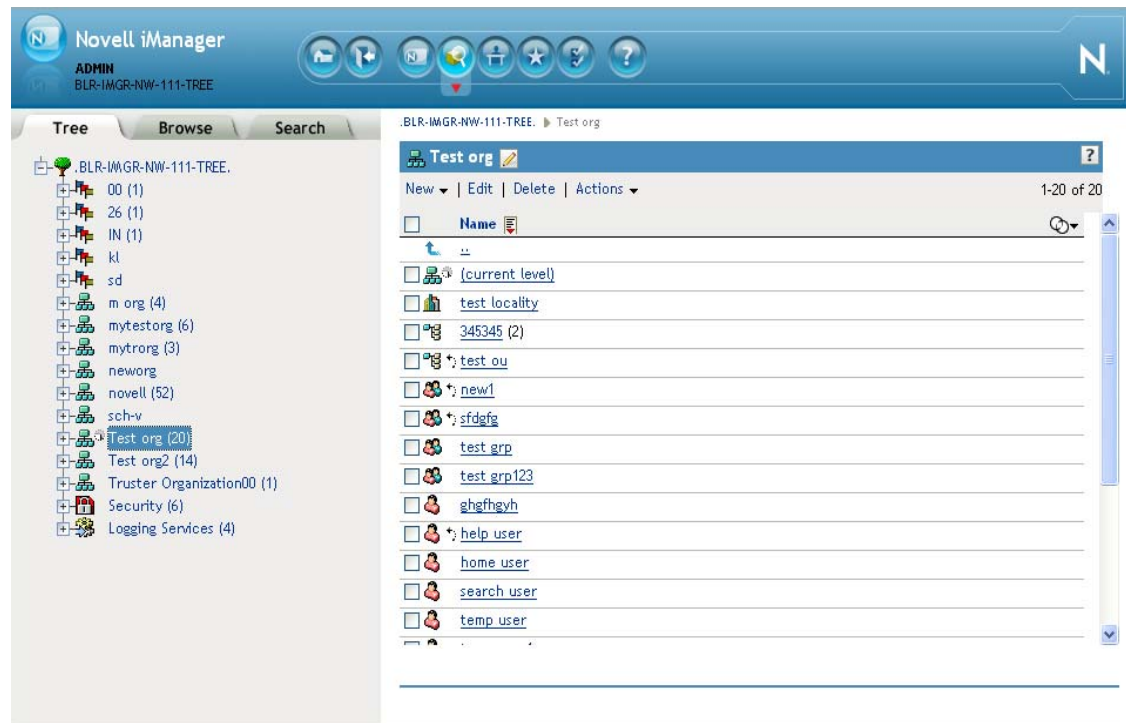
The Object View includes the following tabs in the Navigation frame, each of which give you a different way to browse for and locate directory objects:

- ♦ **Tree**
- ♦ **Browse**
- ♦ **Search**

4.1.1 Tree

The Tree tab lets you browse a directory tree with a look and feel similar to ConsoleOne™. Tree view uses both the Navigation frame and the Content frame to provide its functionality.

Figure 4-1 The Tree Tab in iManager's Object View



Tree View Navigation Frame

In the Tree view, the Navigation frame displays the directory structure in the familiar ConsoleOne format. The Navigation frame displays Container, including Volume (file system), objects. Click on the plus and minus icons to expand and collapse the container objects and browse the directory tree.

By default, Tree View displays up to 100 subordinate objects per container, but you can change this setting in the **Object View Preferences**.

Tree View Content Frame

Selecting one of the container objects in the Navigation frame causes the Content frame to display all the objects in that container. The Content frame is where you actually manipulate directory objects. The Content frame includes a header from which you can select from among several available actions:

Bread Crumbs: At the very top of the Content frame, Tree view provides a bread crumb feature that lets you navigate along the containers in the current context.

Title Bar: The Content frame's title bar displays the name of the currently selected container object. Click the Pencil icon to edit the properties of this container.



Object List Header: The object list header provides access to the following:

- ♦ **Menu Bar:** The Content frame's menu bar provides access to the object-related actions you can perform. Options include the following:
 - ♦ **New:** Opens a dropdown menu of “create” tasks.
 - ♦ **Edit:** Opens the property book for the selected objects so you can modify their attributes. Selecting multiple objects of the same type lets you set attributes for all the objects to the same value.

NOTE: You can also open a leaf object's property book by selecting it in the object list. Selecting a container object in the object list opens the selected container and displays all that container's subordinate. To edit the attributes of a container object, you must select its checkbox, then click *Edit*.



- ♦ **Delete:** Deletes the selected objects. To select an object to edit, select its checkbox in the object list.
- ♦ **Actions:** Opens a dropdown menu of supported tasks for the selected objects. To perform a task, select it from the dropdown menu and provide the required information.

NOTE: If you have configured RBS, the Actions menu displays only those tasks in your assigned roles.

- ♦ **Object Count:** To the right of the menu bar, Tree view lists the number of objects in the current page and the total number of objects in the selected container.
- ♦ **Select All:** The checkbox in the header functions as a “select all” checkbox for the current page of objects.
- ♦ **Sort:** Directly above the Object list is a “Name” column heading and a sort icon . Click either of these to toggle the object sort between ascending and descending alphabetical order.
- ♦ **Define Filter:** At the far right of the header, under the object count, is the object filter icon . Select this icon to create a filter that limits the objects displayed in the object list. You can filter on object type and object name, as needed.

Select *Show All Containers* to display container objects in the Object List regardless of the defined filter.

Select **Advanced Filter** to open the Advanced Filter dialog that lets you create a filter using almost any object attribute. For more information, see **“Advanced Selection” on page 36**.

NOTE: When a filter is active, the filter icon changes to a colored icon , and the filter setting is listed next to the icon. If you configure an advanced filter, iManager displays a checkmark icon  next to the filter icon.

Object List: The Content frame's object list displays all objects in the container currently selected in the Navigation frame. By default, the object list displays 100 objects on a page, but you can change this setting in the [Object View Preferences](#).

To perform an action on an object, select its checkbox, then select the action from the Object List header. Select the (current level) object to perform an action on the container in which you are currently browsing.

Select the double-period object to navigate up one level to the parent container.

IMPORTANT: Tree view does not support selecting objects across multiple pages in the object list. If you need to do this, use Object View's Browse tab to perform the multiple object action. For more information, see ["Browse" on page 28](#).

4.1.2 Browse

The Browse tab leverages a user interface and functionality similar to the Object Selector to provide a directory browsing tool. For information on navigating the Browse user interface, see ["Using the Object Selector" on page 31](#).

Figure 4-2 The Browse tab in iManager's Object View



The Browse tab uses only the Navigation frame to provide its functionality. It includes the following primary components:

Object Filter: Located at the top of the Navigation frame, the object filter lets you limit the objects displayed in the object list. Once defined, click *Apply* to use the filter.

IMPORTANT: The object filtering in the Browse tab only applies to directory objects. It does not filter file system objects, even though they might be visible in the Browse tab.

The object filter uses the following fields:



- ♦ Context: Displays only those objects in the specified context. This is identical to opening the container from the object list.
- ♦ Name: Displays only those objects that conform to the specified name filter. Use the asterisk (*) wildcard to specify a partial name. For example: ldap*, *cert, *server*.
- ♦ Type: Displays only those objects of the type specified.

NOTE: If you select a specific object type, a plus icon [+] appears that lets you open the Advanced Selection tool, from which you can specify additional, attribute-level filter settings. For more information, see [“Advanced Selection” on page 36](#).

- ♦ Load/Save: These two links let you load a previously defined filter definition and save the current filter so it can be re-used, respectively.

Multiple Select / Single Select: Located above the right side of the object list, this link lets you toggle between selecting a single object or multiple objects against which you want to perform a task. The default option is Single Select. For more information, see [“Selecting and Filtering Objects” on page 35](#).

Object List: Displays a list of directory objects, as defined by the criteria in the Object Filter. By default, the object list displays 100 objects on a page, but you can change this value in the [Object View Preferences](#). Use the Previous and Next buttons to navigate between object pages. You can navigate amongst the objects in the object list by doing the following:

- ♦  Select the down arrow icon next to a container object to open that container and view its objects in the object list.
- ♦  Select the up arrow icon at the top of the object list to view the contents of the current container’s parent. This moves you up one level in the directory tree.
- ♦ Select an object, either container or leaf, to open a window with the available tasks for that type of object. Selecting a task opens that tasks UI in the Content frame.

4.1.3 Search

The Search tab is similar to the Browse tab, but instead of displaying a tree structure in the Navigation frame, it displays only those objects resulting from the specified search.

Figure 4-3 The Search tab in iManager's Object view



The Search tab uses only the Navigation frame to provide its functionality. It includes the following primary components:

Object Search: Located at the top of the Navigation frame, the object search lets you define the search criteria. Once defined, click *Search* to perform the specified search operation.

IMPORTANT: The object filtering in the Search tab only applies to directory objects. It does not filter file system objects, even though they might be visible in the Search tab.

You can define your search using the following fields:

- ♦ Context: Specifies the starting container for the search operation. If you want the search to include subordinate containers, select *Search sub-containers*.
- ♦ Name: Defines the object name filter for this search. Use the asterisk wildcard to specify a partial name. For example: ldap*, *cert, *server*.
- ♦ Type: Defines the object type filter for this search. iManager only displays objects of the specified type.

NOTE: If you select a specific object type, a plus icon [+] appears that lets you open the Advanced Selection tool, from which you can specify additional, attribute-level filter settings. For more information, see [“Advanced Selection” on page 36](#).

- ♦ Load/Save: These links let you load a previously defined search definition and save the current search so it can be re-used, respectively.

Multiple Select / Single Select: Located above the right side of the results list, this link lets you toggle between selecting a single object or multiple objects against which you want to perform a task. The default option is Single Select. For more information, see “[Selecting and Filtering Objects](#)” on page 35.

Results List: Displays the results of the search operation. By default, the object list displays 100 objects on a page, but you can change this value in the [Object View Preferences](#). Use the Previous and Next buttons to navigate between results pages. Select an object, either container or leaf, to open a window with the available tasks for that type of object. Selecting a task opens that tasks UI in the Content frame.

NOTE: The Search tab does not let you navigate objects, such as opening container objects, in the results list. If you want to be able to do this, use the Tree tab or the Browse tab.

4.2 Using the Object Selector

The Object Selector lets you select the objects with which you want to work in the current task. iManager provides this tool in any situation where you are selecting a task or action before specifying the objects to which the task or action is applied.


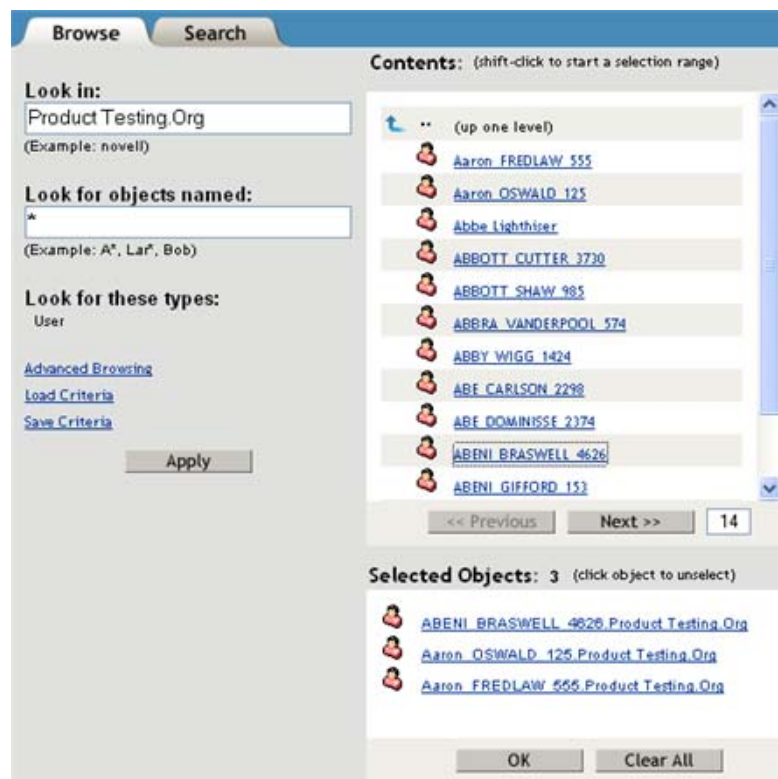
Access the Object Selector by selecting the magnifying glass icon  anywhere it appears in the Content frame. The Object Selector opens in its own window on top of iManager.

Figure 4-4 iManager's Object Selector



Object Selector includes two tabs for locating target objects for the tasks you want to perform:

- ◆ [Section 4.2.1, “Browse,” on page 32](#)

- ♦ [Section 4.2.2, “Search,” on page 32](#)



4.2.1 Browse

The Browse tab (default) lets you navigate the directory tree to search for the desired objects. It includes the following primary components:

Object Filter: Located on the left side of the Object Selector, the object filter lets you limit the objects displayed in the Contents list. Once defined, click Apply to use the filter. The object filter uses the following fields:

- ♦ Look in: Displays only those objects in the specified context. This is identical to opening the container from the Contents list.
- ♦ Look for objects named: Displays only those objects that conform to the specified name filter. Use the asterisk (*) wildcard to specify a partial name. For example: ldap*, *cert, *server*.
- ♦ Advanced Browsing: This link opens the Advanced Selection tool, from which you can specify additional, attribute-level filter settings. For more information, see [“Advanced Selection” on page 36](#).
- ♦ Load Criteria/Save Criteria: These two links let you load a previously defined filter definition and save the current filter so it can be re-used, respectively.

Contents List: Displays a list of directory objects, as defined by the criteria in the object filter. By default, the object list displays 100 objects on a page, but you can change this number, if desired. Use the Previous and Next buttons to navigate between object pages. You can navigate amongst the objects in the Contents list by doing the following:

- ♦  Select the down arrow icon next to a container object to open that container and view its objects in the Contents list.
- ♦  Select the up arrow icon at the top of the object list to view the contents of the current container’s parent. This moves you up one level in the directory tree.
- ♦ Selecting an object causes iManager to identify that object as one on which you want to perform the current task.

Selected Objects: This component only appears when you are selecting multiple objects for the current task. The Selected Objects field lists the objects currently selected for the task. Click OK when the list is complete. Click Clear All if you want to empty the selected objects list and start over.

For more information about selecting single or multiple objects for a task, see [“Selecting and Filtering Objects” on page 35](#).

4.2.2 Search

The Search tab lets you specify a search operation to perform on the directory tree and display the results. It includes the following primary components:

Object Search: Located on the left side of the Object Selector, the object search lets you define the search criteria. Once defined, click Search to perform the specified search operation. You can define your search using the following fields:

- ♦ Start search in: Specifies the starting container for the search operation. If you want the search to include subordinate containers, select Search sub-containers.

- ♦ **Search for objects named:** Defines the object name filter for this search. Use the asterisk wildcard to specify a partial name. For example: ldap*, *cert, *server*.
- ♦ **Advanced Browsing:** This link opens the Advanced Selection tool, from which you can specify additional, attribute-level search settings. For more information, see [“Advanced Selection” on page 36](#).
- ♦ **Load Criteria/Save Criteria:** These two links let you load a previously defined search definition and save the current filter so it can be re-used, respectively.

Multiple Select / Single Select: Located above the right side of the results list, this link lets you toggle between selecting a single object or multiple objects against which you want to perform a task. The default option is Single Select. For more information, see [“Selecting and Filtering Objects” on page 35](#).

Results List: Displays the results of the search operation. By default, the results list displays 100 objects on a page, but you can change this number, if desired. Use the Previous and Next buttons to navigate between results pages.

NOTE: The Search tab does not let you navigate objects, such as opening container objects, in the results list. If you want to be able to do this, use Object Selector’s Browse tab.

Selected Objects: This component only appears when you are selecting multiple objects for the current task. The Selected Objects field lists the objects currently selected for the task. Click OK when the list is complete. Click Clear All if you want to empty the selected objects list and start over.

For more information about selecting single or multiple objects for a task, see [“Selecting and Filtering Objects” on page 35](#).

Roles and Tasks

5

Selecting the Roles and Tasks view in the Header frame displays all of iManager's available roles and tasks in the Navigation frame. iManager groups related roles and tasks into categories. However, you can create custom category groups and assign roles and tasks to them. For more information, see [“The Category Tab” on page 63](#).

This section includes the following topics:

- ♦ [Section 5.1, “Navigating Roles and Tasks,” on page 35](#)
- ♦ [Section 5.2, “Directory Administration,” on page 38](#)
- ♦ [Section 5.3, “Groups,” on page 40](#)
- ♦ [Section 5.4, “Help Desk,” on page 42](#)
- ♦ [Section 5.5, “Partitions and Replicas,” on page 42](#)
- ♦ [Section 5.6, “Rights,” on page 45](#)
- ♦ [Section 5.7, “Schema,” on page 47](#)
- ♦ [Section 5.8, “Users,” on page 49](#)

The first section in this chapter introduces Roles and Tasks navigation. The remaining sections provide a detailed description of the tasks available in iManager's core set of roles and tasks. For information about the roles and tasks provided by a product-specific plug-in, consult that product's documentation.

In addition to the Roles and Tasks view, you can configure iManager's Favorites view to display your most frequently used tasks. For more information, see [“Manage Favorites” on page 81](#).

5.1 Navigating Roles and Tasks

Navigating iManager's tasks is a straight-forward process that includes the following general steps:

- 1** (Navigation frame) Open the category that contains the desired task.
- 2** (Navigation frame) Select the desired task from the category's list of tasks.
- 3** (Content frame) Provide the necessary information to complete the task. When applicable, this includes specifying those objects to which the task is applied.

For information about selecting objects to which the task will apply, see [“Selecting and Filtering Objects” on page 35](#).

- 4** (Content frame) Click OK to perform the task.

5.1.1 Selecting and Filtering Objects

For those tasks that can be applied to more than one object at a time (for example, Modify User), iManager provides options, selectable in the Content frame, for locating the desired objects.

Figure 5-1 Object selection options in a task



Select a Single Object

This is the default object selection method. Select a Single Object lets you specify a single object to which the task is applied. When using the Object Selector to locate the object, selecting an object automatically closes the Object Selector and inserts the selected object in the task's object name field. For more information about the Object Selector, see [“Using the Object Selector” on page 31](#).

Select Multiple Objects

Select Multiple Objects modifies the tasks object name field to accept a list of objects instead of only one object. The Object Selector also runs in “multiple object” mode so that you can select more than one object at a time. For more information about the Object Selector, see [“Using the Object Selector” on page 31](#).

Simple Selection

Simple Selection opens a basic search tool in the Content frame. With this tool, you can search for objects in the directory tree based on a specified property value.

Figure 5-2 Basic object filter in a task



Simple Selection includes the following limitations:

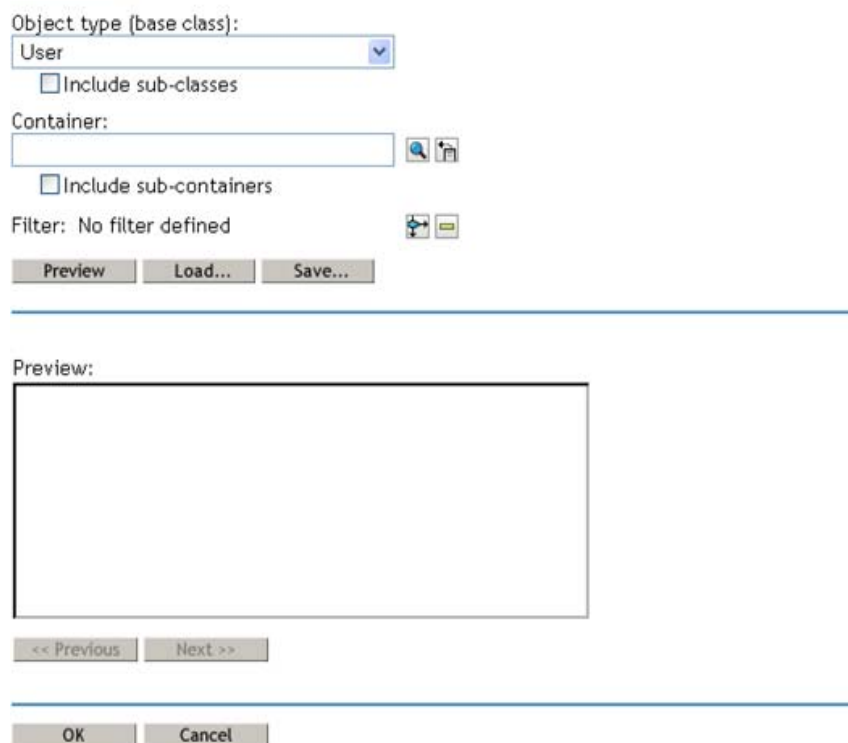
- ♦ Searches the entire directory tree
- ♦ Does not support wildcards in the search criteria
- ♦ Supports only “starts with” and “equals” filters for property values

Advanced Selection

Advanced Selection provides a more configurable environment for searching the directory for the desired objects.

Figure 5-3 *iManager's Advanced Selection Interface*

This advanced selection tab is for working with large sets of objects (greater than 500). Instead of selecting or searching for individual objects, you specify a filter and the subsequent modifications are applied to all objects that match the filter.



Object type (base class):
User
☐ Include sub-classes

Container:

☐ Include sub-containers

Filter: No filter defined

Preview:

Advanced Selection gives you more granular control over the object filter used during the search operation. You can configure advanced selection options using the following fields:

Object Type: Specifies the object base class for which you are searching. For example, User.

Container: Specifies the container at which you want to start the search. To search subordinate containers, select *Include sub-containers*.

Filter: Specifies a filter to apply to the search. Select the Filter icon to open a separate window from which you can define the filter. Click *OK* when the filter is done.

Figure 5-4 *iManager's Advanced Filter dialog*



Object type(s): User

Aux class(es):

☐ Logic Group 1

☐ [attribute] [operator]

The Filter interface includes the following fields:

Aux Classes: Specifies an Auxiliary Class to include in the search.

Attribute: Specifies an attribute (property) that you want to utilize as part of the filter.

Operator: Specifies the logical operator to apply to the filter. Options include

Value: Specifies the attribute value you are using as a filter. You can use the asterisk (*) as a wildcard to indicate part of a value. For example, smi*, *th, and *mit*.

Additionally, you can chain multiple attribute filters together into a filter group by using the + icon to add a second attribute to the list. When using multiple attribute filters, link them together with a logical AND or logical OR.

5.2 Directory Administration

Directory administration involves the management of objects in your directory tree. You can create, edit, and organize objects.

- ♦ [Section 5.2.1, “Copying an Object,” on page 38](#)
- ♦ [Section 5.2.2, “Creating an Object,” on page 39](#)
- ♦ [Section 5.2.3, “Deleting an Object,” on page 39](#)
- ♦ [Section 5.2.4, “Modifying an Object,” on page 39](#)
- ♦ [Section 5.2.5, “Moving an Object,” on page 39](#)
- ♦ [Section 5.2.6, “Renaming an Object,” on page 40](#)

For more information about eDirectory™ objects, see the *eDirectory Administration guide* (<http://www.novell.com/documentation/edir88/index.html?page=/documentation/edir88/edir88/data/fbabihe.html#fbabihe>).

5.2.1 Copying an Object

You can either create a new object with the same attribute values as an existing object, or copy attribute values from one object to another.

- 1 In Roles and Tasks, click *Directory Administration > Copy Object*.
- 2 In the *Object to Copy From* field, type the name and context of the object or use the Object Selector to find it.
- 3 Select one of the following options:
 - ♦ *Create New Object and Copy Attribute Values*
 - ♦ *Copy Attribute Values to an Existing Object*
- 4 Select *Copy ACL Rights* if you want to copy access control list (ACL) rights to this object.
This step might take additional processing time, depending on your system and networking environment.

NOTE: The copy object operation does not copy the following object attributes:

- ♦ ACL (unless you select *Copy ACL Rights*)
- ♦ CN
- ♦ DirXML-Associations
- ♦ Equivalent To Me
- ♦ Group Membership

- ♦ Member
 - ♦ Security Equals
 - ♦ Any naming attribute
 - ♦ Any Read Only attribute
 - ♦ Any RBS attribute
-

5.2.2 Creating an Object

- 1 In Roles and Tasks, click *Directory Administration > Create Object*.
- 2 Select the object class from the list that appears, then click *OK*.
- 3 Specify the requested information that appears according to the object class you selected, then click *OK*.

If you are using a Mozilla browser, click the + symbol to add information instead of typing directly in the field.

- 4 When the confirmation message appears, click *OK*, *Repeat Task*, or *Modify*.

5.2.3 Deleting an Object

- 1 In Roles and Tasks, click *Directory Administration > Delete Object*.
- 2 Type the name and context of the object, or use the Object Selector to find it, and click *OK*.
A confirmation message appears indicating the object was successfully deleted.

5.2.4 Modifying an Object

- 1 In Roles and Tasks, click *Directory Administration > Modify Object*.
- 2 Type the name and context of the object or use the Object Selector to find it, then click *OK*.
The Modify Object page displays pages with the selected object's attributes.
- 3 Modify the object as desired, then click *OK*.
If you are using a Mozilla browser, click the + symbol to add information instead of typing directly in the field.

5.2.5 Moving an Object

- 1 In Roles and Tasks, select *Directory Administration > Move Object*.
Type the name and context of the object or use the Object Selector to find it, then click *OK*.
- 2 In the *Move To* field, select the container to which you want to move the object.
- 3 Select *Create an Alias in Place of Moved Object* to create an alias in an old location for each object being moved.
- 4 Click *OK*.
A confirmation message appears indicating the move object operation was successful.

5.2.6 Renaming an Object

- 1 In Roles and Tasks, select *Directory Administration > Rename Object*.
- 2 Type the name and context of the object or use the search feature to find it.
Type only the name of the new object; do not include a context.
- 3 Select to save the old name, if you want to save it.
This saves the old name as an additional unofficial value of the Name property. Saving the old name lets users search for the object based on that name. After renaming the object, you can view the old name in the *Other Name* field on the object's *General Identification* tab.
- 4 Select *Create an Alias in Place of Renamed Object*, if you want to create an alias for the object being named.
This allows any operations that are dependent on the old object name to continue uninterrupted until you can update those operations to use the new object name.
- 5 Click *OK*.
A confirmation message appears indicating that the object renaming operation was successful.

5.3 Groups

Any user who creates a group automatically becomes the owner of the group. Available group operations include the following:

- ♦ [Section 5.3.1, “Creating a Group,” on page 40](#)
- ♦ [Section 5.3.2, “Deleting a Group,” on page 41](#)
- ♦ [Section 5.3.3, “Modifying a Group,” on page 41](#)
- ♦ [Section 5.3.4, “Modifying Members of Group,” on page 41](#)
- ♦ [Section 5.3.5, “Move Group,” on page 41](#)
- ♦ [Section 5.3.6, “Rename Group,” on page 41](#)
- ♦ [Section 5.3.7, “Viewing My Groups,” on page 42](#)

For more information about using and configuring Group objects, see the *eDirectory Administration guide* (<http://www.novell.com/documentation/edir88/index.html?page=/documentation/edir88/edir88/data/fbabihe.html#fbacjdfg>).

5.3.1 Creating a Group

- 1 In Roles and Tasks, select *Groups > Create Group*.
- 2 In the Create Group page, provide the required information, then click *OK*.
Select *Dynamic Group* to make the new group a dynamic group, of the class *dynamicGroup*. Otherwise, the group is created as a static group, of the class *Group*.
Select *Set Owner* to make the creator of a group object the group owner. The group's Owner attribute is set to the DN of iManager's logged-in user. Deselect *Set Owner* to leave the Owner attribute undefined.

NOTE: You can convert a static group to a dynamic group after the fact by using the **Modifying a Group** option. This extends the selected Group object to belong to the `dynamicGroupAux` class.

5.3.2 Deleting a Group

- 1 In Roles and Tasks, select *Groups > Delete Group*.
- 2 In the Delete Group page, specify the name of the group object to delete, or use the Object Selector to locate it, then click *OK*.

The Delete Group page lets you Select a single object, Select multiple objects, or use Advanced Selection option to specify the object to delete.

5.3.3 Modifying a Group

- 1 In Roles and Tasks, select *Groups > Modify Group*.
- 2 In the Modify Group page, specify the name of a Group object, or use the Object Selector to locate it, then click *OK*.
- 3 Make the desired changes to the Group object's attributes, then click *OK*.

NOTE: If you modify a static group to be a dynamic group, and you are using RBS, you must enable `dynamicGroupAux` class support. To do this, open *Configure > iManager Server > Configure iManager > RBS > Dynamic Group Search Type*. Select *DynamicGroupObjects&AuxClasses* from the drop-down menu, then click *Save*.

5.3.4 Modifying Members of Group

This task lets you make simultaneous identical modifications to the attributes of all member objects of a specified group.

- 1 In Roles and Tasks, select *Groups > Modify Members of Group*.
- 2 In the Modify Members of Group page, specify the name of a Group object, or use the Object Selector to locate it, then click *OK*.
- 3 Make the desired changes to the member object's attributes, then click *OK*.

5.3.5 Move Group

This link redirects you to the Move an Object task. For more information, see **"Moving an Object" on page 39**.

5.3.6 Rename Group

This option is identical to the Rename an Object task. For more information, see **"Renaming an Object" on page 40**.

5.3.7 Viewing My Groups

This page displays the groups that you own. From it, you can create a new group, and edit or delete an existing group.

5.4 Help Desk

Help Desk provides access to a limited number of user-related tasks. The user who owns this role can do the following:

- ♦ [Section 5.4.1, “Clearing a Lockout,” on page 42](#)
- ♦ [Section 5.4.2, “Creating a User,” on page 42](#)
- ♦ [Section 5.4.3, “Setting a Password,” on page 42](#)

For more information about User objects, see the *eDirectory Administration guide* (<http://www.novell.com/documentation/edir88/index.html?page=/documentation/edir88/edir88/data/afxkmdi.html>).

5.4.1 Clearing a Lockout

A user can be locked out for entering the wrong password too many times or trying to log in with an expired password.

- 1 In Roles and Tasks, select *Help Desk > Clear Lockout*.
- 2 In the Clear Lockout page, specify the name of a User object, or use the Object Selector to locate it, then click *OK*.

5.4.2 Creating a User

To create a new user object:

- 1 In Roles and Tasks, select *Help Desk > Create User*.
Fill out the necessary user information, as described in [“Creating a User” on page 50](#).

5.4.3 Setting a Password

- 1 In Roles and Tasks, select *Help Desk > Set Password*.
- 2 In the Set Password page, specify the name of a User object, or use the Object Selector to locate it.
- 3 Specify the new password for the selected User object (twice), then click *OK*.
Select *Set simple password* to define a simple password, which is required for native file access for Windows* and Macintosh* users. It is not necessary when Universal Password is enabled.

5.5 Partitions and Replicas

Partition and replica operations let you manage eDirectory’s physical design and distribution across your directory servers, and includes the following tasks:

- ♦ [Section 5.5.1, “Creating a Partition,” on page 43](#)

- ♦ [Section 5.5.2, “Merging a Partition,” on page 43](#)
- ♦ [Section 5.5.3, “Moving a Partition,” on page 43](#)
- ♦ [Section 5.5.4, “Viewing Replica Information,” on page 44](#)
- ♦ [Section 5.5.5, “Viewing Partition Information,” on page 44](#)
- ♦ [Section 5.5.6, “Using the Filtered Replica Wizard,” on page 44](#)

For information about partitions and replicas, see the *eDirectory Administration guide* (<http://www.novell.com/documentation/edir88/index.html?page=/documentation/edir88/edir88/data/a2iiiiik.html#a2iiiiik>).

5.5.1 Creating a Partition

Partitions create logical divisions of the eDirectory tree. For example, if you choose an Organizational Unit and create it as a new partition, you split the Organizational Unit and all of its subordinate objects from its parent partition. The Organizational Unit you choose becomes the root of a new partition. The replicas of the new partition exist on the same servers as the replicas of the parent, and objects in the new partition belong to the new partition’s root object.

- 1 In Roles and Tasks, select *Partitions and Replicas > Create Partition*.
- 2 In the Create Partition page, specify the container to use as the root of the new partition, or use the Object Selector to locate it, then click *OK*.

A confirmation message appears indicating that the partition create operation was successful.

5.5.2 Merging a Partition

Merging a partition effectively recombines it with its parent partition. Creating and merging partitions is how you determine how the directory is logically divided.

- 1 In Roles and Tasks, select *Partitions and Replicas > Merge Partition*.
- 2 In the Merge Partition page, specify the partition to merge with its parent, or use the Object Selector to locate it, then click *OK*.

To specify a partition, specify the Container object that acts as the partition root.

A confirmation message appears indicating that the partition create operation was successful.

5.5.3 Moving a Partition

Moving a partition lets you move a subtree in your directory tree. This is also known as a prune and graft operation. You can only move partitions that have no subordinate partitions. If subordinate partitions exist, you must first merge those partitions before performing the move operation.

When you move a partition, eDirectory changes all references to the partition Root object. Although the object’s common name remains unchanged, the complete name of the container (and of all its subordinates) changes.

NOTE: When you move a partition, you must follow eDirectory containment rules. For example, you cannot move an Organizational Unit directly under the root of the directory tree, because the

root's containment rules permit only Locality, Country, or Organization objects, but not Organizational Unit objects.

- 1 In Roles and Tasks, select *Partitions and Replicas > Merge Partition*.
- 2 In the Move partition page, specify the required information, then click *OK*.
 - ♦ The *Object name* field specifies the partition to move, or use the Object Selector to locate it.
 - ♦ The *Move to* field specifies the Container object into which you want to move the specified partition.
 - ♦ The Create an alias in place of moved object creates a pointer to the partition's new location. This allows any operations that are dependent on the old location to continue uninterrupted until you can update those operations to reflect the new location. Users can continue to log in to the network and find objects in the original directory location.

WARNING: Make sure your directory tree is synchronizing correctly before you move a partition. If you have any errors in synchronization in either the partition you want to move or the destination partition, do not perform a move partition operation. First, fix the synchronization errors. After moving the partition, if you don't want the partition to remain a partition, merge it with its parent partition.

5.5.4 Viewing Replica Information

Viewing a replica tells you about its current state. An eDirectory replica can be in various states depending on the partition or replication operations it is undergoing.

- 1 In Roles and Tasks, click *Partitions and Replicas > Replica View*.
- 2 In the Replica View page, specify the partition or server whose replica table you want to view, then click *OK*.

A table appears listing the replica Partition, Type, Filter, and State. For information about replica states, see the *eDirectory Administration guide* (<http://www.novell.com/documentation/edir88/index.html?page=/documentation/edir88/edir88/data/fbgeaaeg.html#a2iikn>).

5.5.5 Viewing Partition Information

- 1 In Roles and Tasks, select *Partitions and Replicas > View Partition Information*.
- 2 In the Partition Information page, specify the partition for which you want to view information, then click *OK*.

To specify a partition, specify the Container object that acts as the partition root.

5.5.6 Using the Filtered Replica Wizard

Filtered replicas maintain a filtered subset of information from an eDirectory partition (objects or object classes along with a filtered set of attributes and values for those objects). The Filtered Replica Wizard steps you through the configuration of the filtered replicas on the selected server.

- 1 In Roles and Tasks, select *Partitions and Replicas > Filtered Replica Wizard*.

- 2 Specify the name and context of the server on which you want to configure a filtered replica, or use the Object Selector to find it, then click *Next*.
- 3 Click Define the Filter Set to specify the classes and attributes for a filter set on the selected server, then click *Next*.
The replication filter contains the set of eDirectory classes and attributes you want to host on this server's set of filtered replicas.
- 4 Click *Finish*.

For more information about filtered replicas, see the *eDirectory Administration guide* (<http://www.novell.com/documentation/edir88/index.html?page=/documentation/edir88/edir88/data/a5lhibw.html>).

5.6 Rights

Rights refers to eDirectory trustee rights and trustees. When you create a tree, the default rights assignments give your network generalized access and security. iManager lets you perform the following rights-related tasks:

- ♦ Section 5.6.1, “Modifying the Inherited Rights Filter,” on page 45
- ♦ Section 5.6.2, “Modifying Trustee Rights,” on page 46
- ♦ Section 5.6.3, “Rights to Other Objects,” on page 46
- ♦ Section 5.6.4, “Viewing Effective Rights,” on page 46

For more information about eDirectory rights, see the *eDirectory Administration guide* (<http://www.novell.com/documentation/edir88/index.html?page=/documentation/edir88/edir88/data/fbachifb.html>).

5.6.1 Modifying the Inherited Rights Filter

Both eDirectory and the NetWare file system provide an Inherited Rights Filter (IRF) mechanism to block rights inheritance on individual subordinate items. One exception is that the Supervisor right can't be blocked in the NetWare file system.

For more information about Inherited Rights Filters, see the *eDirectory Administration guide* (<http://www.novell.com/documentation/edir88/index.html?page=/documentation/edir88/edir88/data/fbachifb.html#a2iidd>).

- 1 In Roles and Tasks, select *Rights > Modify Inherited Rights Filter*.
- 2 Specify the full name of the object whose inherited rights filter you want to modify, or use the Object Selector to find it, then click *OK*.
This displays a list of the inherited rights filters that have already been set on the object.
- 3 On the property page, edit the list of inherited rights filters as needed, then click *OK*.
To edit the list of filters, you must have the Supervisor or Access Control right to the ACL property of the object. You can set filters that block inherited rights to the object as a whole, to all the properties of the object, and to individual properties.

5.6.2 Modifying Trustee Rights

A trustee is one object that has been granted explicit rights to another object in your directory tree. To modify the trustee list for a given object:

- 1 In Roles and Tasks, select *Rights > Modify Trustees*.
- 2 Specify, or use the Object Selector to find, the name of the object whose trustee list you want to view, then click *OK*.

This opens a list of the object's currently assigned trustees.

- 3 Modify the trustee list as needed, then click *OK*.
 - ♦ Add a trustee by clicking *Add Trustee*.
 - ♦ Remove a trustee by selecting its check box and clicking *Remove Selected*.
 - ♦ Modify a trustee's rights assignment by selecting the *Assigned Rights* link for that trustee.

5.6.3 Rights to Other Objects

This task allows you to view and modify the list of objects to which an object is a trustee.

- 1 In Roles and Tasks, select *Rights > Rights To Other Objects*.
- 2 In the Rights To Other Objects page, provide the required information, then click *OK*.
 - ♦ Specify the name of the object in *Trustee name*.
 - ♦ Specify the context in which you want to search for objects that have this trustee in *Context to search from*.

Select *Search entire subtree* to search all containers under the specified context.

- 3 Modify the object list as needed, then click *OK*.
 - ♦ Add explicit rights to another object by clicking *Add Object*.
 - ♦ Remove explicit rights to an object by selecting its check box and clicking *Remove Selected*.
 - ♦ Modify the explicit rights granted to an object by selecting the *Assigned Rights* link for that object.

5.6.4 Viewing Effective Rights

Effective rights is the combination of explicit and inherited rights that an object has at any point in the directory tree. To view an object's effective rights to another object:

- 1 In Roles and Tasks, select *Rights > View Effective Rights*.
- 2 Specify, or use the Object Selector to find, the name of the trustee whose rights you want to view, then click *OK*.
- 3 In the Object name field, specify the name of the object for which you want to calculate the trustee's effective rights.

eDirectory calculates the effective rights and displays them in the *Effective Rights* field.
- 4 Click *Done* when finished.

5.7 Schema

The directory schema defines the types of objects that can be created in your tree (such as Users, Printers, and Groups) and what information is required or optional at the time the object is created. iManager provides the following schema-related tasks:

- ♦ [Section 5.7.1, “Adding an Attribute,” on page 47](#)
- ♦ [Section 5.7.2, “Viewing Attribute Information,” on page 47](#)
- ♦ [Section 5.7.3, “Viewing Class Information,” on page 48](#)
- ♦ [Section 5.7.4, “Creating an Attribute,” on page 48](#)
- ♦ [Section 5.7.5, “Creating a Class,” on page 48](#)
- ♦ [Section 5.7.6, “Deleting an Attribute,” on page 48](#)
- ♦ [Section 5.7.7, “Deleting a Class,” on page 49](#)
- ♦ [Section 5.7.8, “Extending a Schema,” on page 49](#)
- ♦ [Section 5.7.9, “Extending an Object,” on page 49](#)

For more information about eDirectory schema, see the *eDirectory Administration guide* (<http://www.novell.com/documentation/edir88/index.html?page=/documentation/edir88/edir88/data/a4a9bz0.html>).

5.7.1 Adding an Attribute

You can add optional attributes to existing classes if your organization’s information needs change or if you are preparing to merge trees. To add an attribute to an existing class:

NOTE: Mandatory attributes can be defined only while creating a class. (A mandatory attribute is one that must be completed when an object is being created.)

- 1 In Roles and Tasks, select *Schema > Add Attribute*.
- 2 Select the class you want to add an attribute to, then click *OK*.
- 3 Select the attributes you want to add, then click *OK*.

Select the desired attributes from the *Available Optional Attributes* list, then click the *Right-arrow* to add these attributes to the *Add These Optional Attributes* list. Use the *Left-arrow* to remove attributes from *Add These Optional Attributes*.

Objects you create of this class now have the properties you added. To set values for the added properties, use the generic *Other property* page of the object.

5.7.2 Viewing Attribute Information

You can view an attribute’s structural details such as Syntax, flags and Classes that use the attribute. To see an attribute’s information:

- 1 In Roles and Tasks, select *Schema > Attribute Information*.
- 2 Select the attribute for which you want to see information, then click *View*.
The Content frame displays information related to the selected attribute.
- 3 When finished, click *Close*.

5.7.3 Viewing Class Information

The Class Information page displays information about the selected class and lets you add attributes. During class creation, if the class is specified to inherit attributes from another class, the inherited attributes are classified as they are in the parent class. For instance, if Object Class is a mandatory attribute for the parent class, then it displays on this screen as a mandatory attribute for the selected class.

To see a Class's information:

- 1 In Roles and Tasks, select *Schema > Class Information*.
- 2 Select the class for which you want to see information, then click *View*.

The Content frame displays information related to the selected class. To add an attribute to the class, select *Add a new attribute*. To view the class's parent class, select *View superclass*.

- 3 When finished, click *Close*.

5.7.4 Creating an Attribute

You can define your own custom types of attributes and add them as optional attributes to existing object classes. However, you cannot add mandatory attributes to existing classes. To create an attribute:

- 1 In Roles and Tasks, click *Schema > Create Attribute*.
- 2 Follow the steps in the Create Attribute Wizard to complete the attribute creation procedure.

5.7.5 Creating a Class

An auxiliary class is a set of properties (attributes) added to particular object rather than to an entire class of objects. For example, an e-mail application could extend the schema of your eDirectory tree to include an E-Mail Properties auxiliary class and then extend individual objects with those properties as needed.

Using Schema Manager, you can define your own auxiliary classes. You can then extend individual objects with the properties defined in your auxiliary classes. To create an auxiliary class:

- 1 In Roles and Tasks, click *Schema > Create Class*.
- 2 Follow the steps in the Create Class Wizard to define the new class.

5.7.6 Deleting an Attribute

You can delete unused attributes that aren't part of the base schema of your eDirectory tree. This might be useful after merging two directory trees, or if an attribute has become obsolete over time. To delete an attribute:

- 1 In Roles and Tasks, click *Schema > Delete Attribute*.
- 2 Select the attribute you want to delete, then click *Delete*.

Only attributes that you can delete are displayed.

5.7.7 Deleting a Class

You can delete unused classes that aren't part of the base schema of your eDirectory tree. iManager prevents you from deleting classes that are currently being used in locally replicated partitions. To delete a class:

- 1 In Roles and Tasks, click *Schema > Delete Class*.
- 2 Select the class you want to delete, then click *Delete*.
Only classes that are allowed to be deleted are shown.

5.7.8 Extending a Schema

You can extend the schema of a tree by creating a new class or attribute. To extend the schema of your eDirectory tree, you need Administrator/Supervisor right to the entire tree. To extend the schema:

- 1 In Roles and Tasks, click *Schema > Extend Schema*.
- 2 Follow the ICE Wizard through the import, export, migration of data, or schema update and compare operations.

5.7.9 Extending an Object

- 1 In Roles and Tasks, click *Schema > Object Extensions*.
- 2 Specify the name and context of the object you want to extend, then click *OK*.
- 3 Depending on whether the auxiliary class that you want to use is already listed under Current Auxiliary Class Extensions, click one of the following:
 - ♦ *Yes*: Quit this procedure. See [Modifying an Object's Auxiliary Properties](http://www.novell.com/documentation/edir88/index.html?page=/documentation/edir88/edir88/data/fbbdchgh.html#a3olrac) (<http://www.novell.com/documentation/edir88/index.html?page=/documentation/edir88/edir88/data/fbbdchgh.html#a3olrac>) in the *eDirectory Administration Guide* instead.
 - ♦ *No*: Click *Add*, select the auxiliary class, then click *OK*.
- 4 Click *Close*.

5.8 Users

Managing users and their network access is a central purpose of the directory. iManager provides the following user-related tasks:

- ♦ [Section 5.8.1, "Creating a User," on page 50](#)
- ♦ [Section 5.8.2, "Deleting a User," on page 50](#)
- ♦ [Section 5.8.3, "Disabling an Account," on page 50](#)
- ♦ [Section 5.8.4, "Enabling an Account," on page 51](#)
- ♦ [Section 5.8.5, "Modifying a User," on page 51](#)
- ♦ [Section 5.8.6, "Moving a User," on page 51](#)
- ♦ [Section 5.8.7, "Renaming a User," on page 51](#)

For more information about user objects in the directory, see the *eDirectory Administration guide* (<http://www.novell.com/documentation/edir88/index.html?page=/documentation/edir88/edir88/data/afxkmdi.html>).

5.8.1 Creating a User

To create a new user object:

- 1 In Roles and Tasks, select *User > Create User*.
- 2 In the Create User page provide, at a minimum, the required user-related information, then click *OK*.
 - ♦ Username
 - ♦ Last Name
 - ♦ Context
 - ♦ Password (twice)

IMPORTANT: If you fail to enter a password, you are prompted to either allow the user to log in without a password (not recommended) or require a password for login.

Select *Set simple password* to define a simple password, which is required for native file access for Windows* and Macintosh* users. It is not necessary when Universal Password is enabled.

Select *Copy from template or user object* to create a user based on an existing Template or User object. When copying from a user object, iManager allows only a copy of the New Object NDS rights instead of a copy of NDS rights, to prevent users from receiving the same rights as the administrator.

Select *Create home directory* to specify a location for the user's home directory, which is created when the user object is created. If you specify a path that doesn't exist, a message appears stating that the user's home directory has not been created.

5.8.2 Deleting a User

To delete a user object:

- 1 In Roles and Tasks, select *Users > Delete User*.
- 2 Type the name and context of the object or use the search feature to find it, then click *OK*.
- 3 Click *Delete*.

A confirmation appears indicating the user object has been deleted.

5.8.3 Disabling an Account

To disable a user account, thereby preventing the user from authenticating to the directory:

NOTE: This only prevents a user from authenticating subsequent to disabling the account. If they are logged in when the account is disabled, their access continues unchanged until they log out.

- 1 In Roles and Tasks, select *Users > Disable Account*.
- 2 Specify, or use the Object Selector to find, the name and context of the object, then click *OK*.

- 3 Click *Disable*.

5.8.4 Enabling an Account

To enable a previously disabled user account:

- 1 In Roles and Tasks, select *Users > Enable Account*.
- 2 Specify, or use the Object Selector to find, the name and context of the object, then click *OK*.
- 3 Click *Enable*.

5.8.5 Modifying a User

To modify an existing user object's properties:

- 1 In Roles and Tasks, select *Users > Modify User*.
- 2 Specify, or use the Object Selector to find, the name and context of the object, then click *OK*.
The Content frame displays the user object's property book.
- 3 Make your changes, then click *Apply* or *OK* to save the changes.

5.8.6 Moving a User

To move a user object:

- 1 In Roles and Tasks, select *Users > Move User*.
- 2 Provide the required information, as described in [“Moving an Object” on page 39](#).

5.8.7 Renaming a User

To rename a user object:

- 1 In Roles and Tasks, select *Users > Rename User*.
- 2 Provide the required information, as described in [“Renaming an Object” on page 40](#).

Configuring and Customizing iManager

6

This section describes the various features of Novell® iManager configuration. You configure iManager from the Configure view. This section discusses the following topics:

- ♦ [Section 6.1, “Role-Based Services,” on page 53](#)
- ♦ [Section 6.2, “RBS Configuration,” on page 57](#)
- ♦ [Section 6.3, “RBS Reporting,” on page 66](#)
- ♦ [Section 6.4, “iManager Server,” on page 69](#)
- ♦ [Section 6.5, “Object Creation List,” on page 74](#)
- ♦ [Section 6.6, “Plug-In Module Installation,” on page 74](#)
- ♦ [Section 6.7, “Downloading and Installing Plug-in Modules,” on page 75](#)
- ♦ [Section 6.8, “E-Mail Notification,” on page 78](#)
- ♦ [Section 6.9, “Views,” on page 79](#)

IMPORTANT: Using Role-Based Services is optional, although we recommend setting it up for the optimal use of the iManager software. RBS must be configured in the eDirectory™ tree in order to use the Plug-In Studio.

Do not use Novell ConsoleOne® to modify or delete any RBS objects. RBS objects should be managed using only iManager.

If desired, you can prevent non-admin and non-collection-owner users from accessing iManager's Configure view. For more information see the following topics:

- ♦ iManager Views: [“Views” on page 79](#).
- ♦ User Preferences: [Chapter 7, “Preferences,” on page 81](#).
- ♦ Authorized Users: [“Authorized Users” on page 70](#).

6.1 Role-Based Services

iManager gives you the ability to assign specific responsibilities to users and to present them with the tools (and their accompanying rights) necessary to perform those sets of responsibilities. This functionality is called Role-Based Services (RBS).

Role-Based Services is a set of extensions to the eDirectory schema. RBS defines several object classes and attributes that provide a mechanism for administrators to grant a user access to management tasks based on the user's role in the organization. This gives users access to only those tasks that the users need to perform. RBS grants only the rights necessary to perform assigned tasks.

NOTE: Novell iManager Role-Based Services (RBS) grants rights based upon the Access Control List (ACL) capability of Novell eDirectory. The ACLs allow a trustee to be granted rights to a specific object or its subordinate objects. ACLs are not granted based upon specific object types. Each Novell iManager task defines its applicable object types and necessary ACLs. However, these

ACLs allow the user to perform those operations with other object types through eDirectory APIs or other tools such as Novell ConsoleOne or NWAdmin.

Use RBS to create specific roles within your organization; the roles contain tasks that an assigned user can perform within iManager, such as creating a new user or changing a password. Tasks are preassigned to roles but can be replaced, reassigned, or removed altogether.

Furthermore, users are associated with roles in a specified scope, which is a container in the tree in which the user has the requisite permissions to perform a task. A role requires this threefold association of role, members, and scope to be complete.

An RBS Role object creates an association between users and tasks. An administrator grants a user access to a task by making the user a member of the role to which the task is assigned.


A user can be assigned to a role in the following ways:







- ♦ Directly as a user
- ♦ Through group and dynamic group assignments
If a user is a member of a group or a dynamic group that is assigned to a role, then the user has access to the role.
- ♦ Through organizational role assignments
If a user is an occupant of a organizational role that is assigned a role, then the user has access to the role.
- ♦ Through container assignment
A User object has access to all of the roles that its parent container is assigned. This could also include other containers up to the root of the tree.

A user can be associated with a role multiple times, each with a different scope.

6.1.1 RBS Objects in eDirectory

The following table lists the RBS objects. iManager extends the eDirectory schema to include these objects when you install RBS. For more information, see [“Installing RBS” on page 56](#).

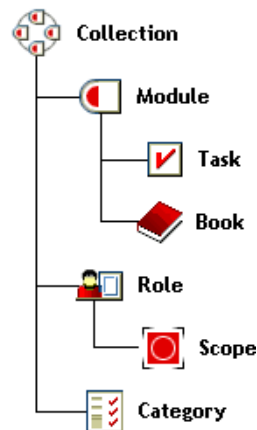
Object	Description
 rbsCollection	<p>A container object that holds all RBS Role and Module objects.</p> <p>rbsCollection objects are the uppermost containers for all RBS objects. A tree can have any number of rbsCollection objects. These objects have owners, which are users who have management rights over the collection.</p> <p>rbsCollection objects can be created in any of the following containers:</p> <ul style="list-style-type: none">♦ Country♦ Domain♦ Locality♦ Organization♦ Organizational Unit

Object	Description
 rbsRole	<p>Defining a role includes creating an rbsRole object and specifying the tasks that the role can perform.</p> <p>rbsRoles are container objects that can be created only in an rbsCollection container.</p> <p>Role members can be Users, Groups, Organizations, Organization Roles, or Organizational Units, and role members are associated to a role in a specific scope of the tree. The rbsTask and rbsBook objects are assigned to rbsRole objects.</p>
 rbsTask	<p>A leaf object that holds a specific function, such as resetting login passwords.</p> <p>rbsTask objects are located only in rbsModule containers.</p>
 rbsBook (aka Property Book)	<p>A book is a leaf object that displays a group of pages that allow a user to view or modify the properties of an object or set of objects of the same type. Each page of the book has a tab that you click, to view a different page.</p> <p>A book object resides only in rbsModule containers and can be assigned to one or more roles and to one or more object class types.</p>
 rbsScope	<p>A leaf object used for ACL assignments (instead of making assignments for each User object). rbsScope objects represent the context in the tree where a role is performed and are associated with rbsRole objects. They inherit from the Group class. User objects are assigned to an rbsScope object. These objects have a reference to the scope of the tree that they are associated with.</p> <p>The objects are dynamically created when needed, then automatically deleted when no longer needed. They are located only in rbsRole containers.</p> <hr/> <p>WARNING: Never change the configuration of an rbsScope object. Doing so has serious consequences and could possibly break the system.</p> <hr/>
 rbs Module	<p>Represents a container object that holds rbsTask and rbsBook objects. rbsModule objects have a module name attribute that represents the name of the product that defines the tasks or books (for example, eDirectory Maintenance Utilities, NMAS™ Management, or Novell Certificate Server™ Access).</p> <p>rbsModule objects can be created only in rbsCollection containers.</p>
 rbs Category	<p>A category groups roles and tasks together which are specific to a particular function. iManager has 14 default categories: Authentication & Passwords, Collaboration, Directory, File Management, Identity Manager, Infrastructure, Install & Upgrade, Network, Novell Audit, Printing, Security, Servers, Software Licenses & Network, Usage, and Users & Groups.</p> <p>The All Categories selection displays all available roles and tasks.</p> <p>You can also create new categories and assign roles and tasks to them.</p>

RBS objects reside in the eDirectory tree as depicted in the following figure:

Figure 6-1 *Role-Based Services in eDirectory*

**Role-Based Services
in eDirectory**



6.1.2 Installing RBS

RBS is installed using the iManager Configuration Wizard.

- 1 In the Configure view, select *Role Based Services > RBS Configuration*.
- 2 Select *Configure iManager*.
- 3 Follow the on-screen instructions.

6.1.3 Removing RBS

If Role-Based Services is no longer needed in the tree, the RBS Collection object can be safely deleted through iManager. Deleting the RBS collection automatically cleans up all user role associations and scopes in the tree. Do not delete the RBS collection using other utilities, such as ConsoleOne.

To remove Role-based Services:

- 1 In the Configure view, select *Role Based Services > RBS Configuration*.
- 2 Select the collection to be deleted.
- 3 Click *Delete*.

After the RBS collection is deleted, all users logging in to iManager enter in Assigned Access mode even though there is no RBS collection object in the tree.

To switch back to Unrestricted mode (the default mode):

- 1 In the Configure view, select *iManager Server > Configure iManager*.
- 2 Select the *RBS* tab.
- 3 Select the appropriate tree name in the *RBS Tree List* field, then click the minus button.
- 4 Click *Save*.

NOTE: When using iManager in Unrestricted mode, you typically see the following message on the iManager Home Page: `Notice: Some of the roles and tasks are not available. Clicking View Details might display a Not supported by current authenticators message for several of the tasks, even though the tasks work correctly. This message is misleading, and iManager removes these messages after you configure RBS.`

6.2 RBS Configuration

The RBS Configuration task provides complete control over RBS objects. It is a central place for managing and configuring RBS objects. You can list and modify RBS objects by type. The task also gives you useful information about the RBS system, such as the number of modules in a collection, how many are installed, how many are not installed, and how many are outdated. Some tasks let you operate on multiple objects simultaneously. For example, you can associate or disassociate multiple members from a role at the same time.

From the Configure view, select *Role-Based Services > RBS Configuration* to open the RBS Configuration page in the Content frame.

The page includes two tabs:

iManager 2.x Collection: Displays current RBS collections.

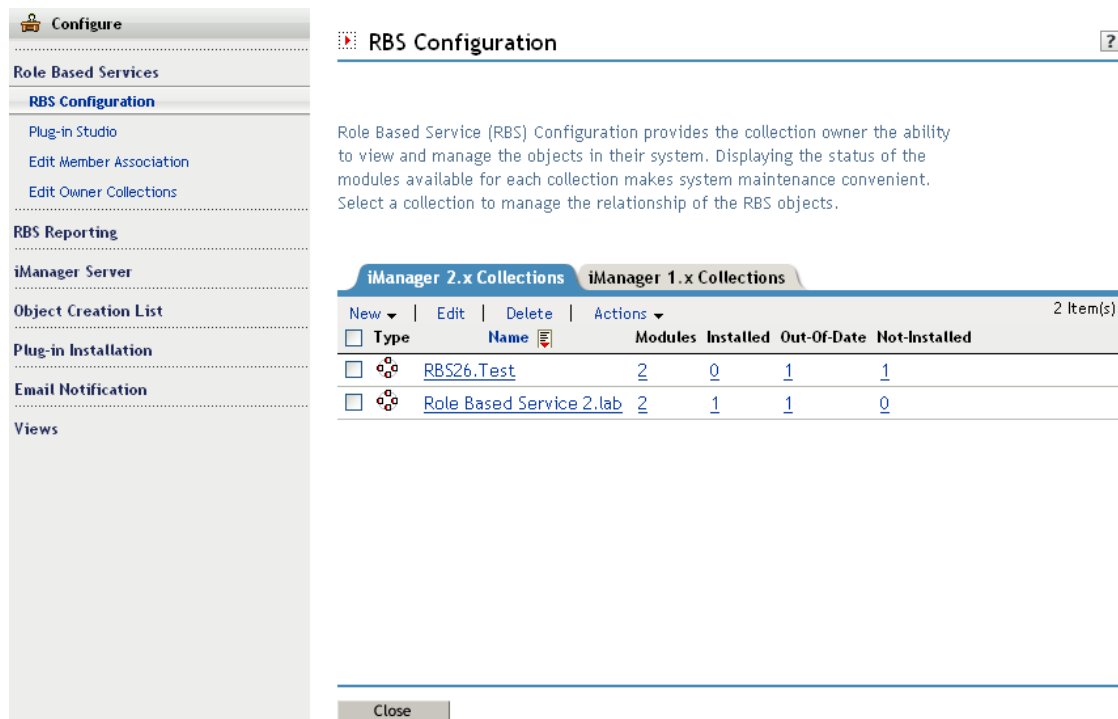
iManager 1.x Collections: Displays older RBS collections that you can either delete or migrate to iManager 2.x. If you select Migrate, a wizard steps you through the migration process.

iManager displays only those collections you own, and includes the following information about each collection:

- ♦ **Module:** Indicates the number of modules on the Web server that you are logged in to.
- ♦ **Installed:** Indicates the number of modules that are currently installed.
- ♦ **Outdated:** Indicates the number of outdated modules currently installed.
- ♦ **Not-Installed:** Indicates the number of modules that are available but not installed.

To work with a particular collection, select it from the list. This opens a collection-specific view, as shown in [Figure 6-2](#).

Figure 6-2 Working with RBS collections in iManager



The remainder of this section describes the various tabs in the RBS Collection page as well as the other RBS-related tasks in the Role Based Services category.

- ◆ [Section 6.2.1, “The Role Tab,” on page 58](#)
- ◆ [Section 6.2.2, “The Task Tab,” on page 60](#)
- ◆ [Section 6.2.3, “The Property Book Tab,” on page 61](#)
- ◆ [Section 6.2.4, “The Module Tab,” on page 62](#)
- ◆ [Section 6.2.5, “The Category Tab,” on page 63](#)
- ◆ [Section 6.2.6, “Plug-In Studio,” on page 64](#)
- ◆ [Section 6.2.7, “Editing Member Associations,” on page 66](#)
- ◆ [Section 6.2.8, “Editing Owner Collections,” on page 66](#)

6.2.1 The Role Tab

The RBS Collection Role tab lets you manage the RBS roles in the collection. From this tab you can do the following:

- ◆ [“Create a New Role” on page 59](#)
- ◆ [“Edit a Role” on page 59](#)
- ◆ [“Delete a Role” on page 59](#)
- ◆ [“Set a Member Association” on page 59](#)
- ◆ [“Assign a Category” on page 60](#)
- ◆ [“Add a Description to a Role” on page 60](#)

NOTE: To select a role, select the checkbox to the left of the role name.

Create a New Role

To create a new role in the collection:

- 1 In the *Role* tab, select *New > iManager Role*.
- 2 Complete the steps in the iManager Role Wizard.

The wizard steps you through naming the role; assigning tasks and categories to the role; and assigning role members and scopes to the role.

Edit a Role

To edit an existing role in the collection:

- 1 In the *Role* tab, select the role, then click *Edit*.
The role's task list appears.
- 2 Add or remove a task from this page as needed, then click *OK*.

Delete a Role

To delete a role in the collection:

- 1 In the *Role* tab select the role, then click *Delete*.

A message appears: This operation will delete all of the selected roles. Do you want to continue?

- 2 Click *OK* to complete the deletion of the role.

Set a Member Association

To add a member to an existing role:

- 1 In the *Role* tab select the role, then select *Actions > Member Associations*.
- 2 Provide the required member information, then click *Add*.
 - ♦ *Name*: Specify, or use the Object Selector to find, the desired object to be a role member.
 - ♦ *Scope*: Specify, or use the Object Selector to find, the container that defines the scope within which this member can perform the role.
- 3 In the members list, specify how you want rights related to this role assigned to the member, then click *OK*.
 - ♦ *Assign Rights*: Instructs eDirectory to automatically grant the member rights necessary to perform the assigned role. When not selected, the member is assigned the role but might not have rights to perform all tasks associated with the role. The member's rights assignments are handled separately.
 - ♦ *Inheritable*: Select *subtree* to indicate that the member's scope includes all sub-containers in the specified context. Select *base object* to indicate that the member can perform the role only in the specified container.

Assign a Category

To add a category assignment to an existing role:

- 1 In the *Role* tab, select the role, then select *Actions > Category Assignment*.
The Category Assignment page appears.
- 2 Select a category, then click the right-arrow to assign it to the role.
- 3 Click *OK*.

Add a Description to a Role

To add a description to an existing role:

- 1 In the *Role* tab, select the role and click *Actions > Description*.
- 2 Specify the description in the text box, then click *OK*.

6.2.2 The Task Tab

A task is a plug-in that performs a distinct management function, such as creating a user or setting a password. iManager lists the tasks by group in the navigation area on the left side of the window.

The RBS Collection Task tab lets you do the following operations:

- ♦ “Creating a New Task” on page 60
- ♦ “Deleting a Task” on page 60
- ♦ “Editing the Role Assignment of a Task” on page 61
- ♦ “Adding a Description to a Task” on page 61

Creating a New Task

To create a new task:

- 1 In the *Task* tab, select *New > iManager Task*.
- 2 Complete the steps in the Create iManager Task Wizard.

The wizard steps you through providing the necessary detail about the new task you are creating.

For information on creating tasks in the Plug-in Studio, see “Creating a New Task from Plug-In Studio” on page 64.

Deleting a Task

To delete an existing task:

- 1 In the *Task* tab, select the task, then select *Delete*.

A message appears: This operation will delete all of the selected tasks. Do you want to continue?

- 2 Click *OK*.

Editing the Role Assignment of a Task

To edit the list of roles to which a task is assigned:

- 1 In the *Task* tab, select the task, then select *Actions > Role Assignment*.
- 2 On the Edit Role Assignment page, add or remove roles from the *Assigned Roles* field, then click *OK*.

Adding a Description to a Task

To add a description to an existing task:

- 1 In the *Task* tab, select the task, then select *Actions > Description*.
- 2 Specify the description in the text box, then click *OK*.

6.2.3 The Property Book Tab

A property book displays the attributes of a specific object type that you can modify. These properties are of an object or set of objects of the same type.

Property books can be assigned to roles and appear in the list of tasks for a role. For example, a property book that modifies the attributes of User objects might have a page that lets you to specify a user's login script. Another page could let you change a user's e-mail address and telephone number.

Property book pages are similar to tasks. However, they are for displaying and modifying attributes in a single view. For a more complex, wizard-like UI, you should create a task.

The RBS Collection Property Book tab lets you perform the following operations:

- ♦ “Creating a New Property Book” on page 61
- ♦ “Deleting a Property Book.” on page 62
- ♦ “Editing the Role Assignment in a Property Book” on page 62
- ♦ “Modifying the Page List for a Property Book” on page 62
- ♦ “Modifying the Object Type Assignment of a Property Book” on page 62
- ♦ “Modifying the Description of a Property Book” on page 62

Creating a New Property Book

To create a new property book:

- 1 In the *Property Book* tab, select *New*.
- 2 Complete the steps in the Create Property Book Wizard.

The wizard steps you through providing the necessary detail for the property book you are creating.

IMPORTANT: In iManager, some characters have special significance and must be escaped with the backslash (\) character. For more information, see [Section 3.2, “Special Characters,” on page 22](#).

Deleting a Property Book.

To delete a property book:

- 1 In the *Property Book* tab, select the property book, then select *Delete*.

A message appears: This operation will delete all of the selected property books. Do you want to continue?

- 2 Click *OK*.

Editing the Role Assignment in a Property Book

To modify the list of roles to which a property book is assigned:

- 1 In the *Property Book* tab, select the property book, then select *Actions > Role Assignment*.
- 2 On the Edit Role Assignment page, add or remove roles from the *Assigned Roles* field, then click *OK*.

Modifying the Page List for a Property Book

To modify the attribute pages associated with a property book:

- 1 In the *Property Book* tab, select the property book, then select *Actions > Page List*.
- 2 On the Edit Page List page, add or remove roles from the *Assigned Pages* field, then click *OK*.

Modifying the Object Type Assignment of a Property Book

To modify the list of object types associated with a property book:

- 1 In the *Property Book* tab, select the property book, then select *Actions > Object Type*.
- 2 On the Edit Object Type page, add or remove roles from the *Assigned Object Types* field, then click *OK*.

Modifying the Description of a Property Book

To add a description to an existing task:

- 1 In the *Property Book* tab, select the property book, then select *Actions > Description*.
- 2 Specify the description in the text box, then click *OK*.

6.2.4 The Module Tab

The Module page lists the RBS modules currently installed on a selected collection. Each module contains RBS property books and tasks. From this page, you can add (if you want to create a custom property book) and delete modules, and also type a description for a selected plug-in module.

The RBS Collection Module tab lets you perform the following operations:

- ♦ “Adding a New Plug-in Module” on page 63
- ♦ “Deleting an RBS Module” on page 63
- ♦ “Adding a description” on page 63

Adding a New Plug-in Module

To add a new plug-in module:

- 1 In the *Module* tab, select *New*.
- 2 Specify the RBS module name and a destination context, then click *OK*.
iManager displays a message indicating the module has been added.

Deleting an RBS Module

To delete an existing plug-in module:

- 1 In the *Module* tab, select a module to delete, then select *Delete*.
- 2 Click OK to confirm the module deletion..

Adding a description

To add a description to an existing plug-in module:

- 1 In the *Module* tab, select a module, then select *Actions > Description*.
- 2 Specify the module description, then click *OK*.

6.2.5 The Category Tab

Categories group related roles and tasks together. The RBS Collection Category tab lets you perform the following operations:

- ♦ “Adding a New Category” on page 63
- ♦ “Deleting a Category” on page 63
- ♦ “Adding a Description” on page 64

Adding a New Category

To add a description to an existing plug-in module:

- 1 In the *Category* tab, select *New*.
This launches the Create Category Wizard.
- 2 Specify category name and description (optional), then click *Next*.
- 3 Select the roles to be associated with the new category, then click *Next*.
- 4 Review the new category summary, then click *Finish*.

Deleting a Category

To delete an existing category:

- 1 In the *Category* tab, select a module to delete, then select *Delete*.
- 2 Click OK to confirm the category deletion..

Adding a Description

To add or modify the description of an existing category:

- 1 In the *Category* tab, select a category, then select *Actions > Description*.
- 2 Specify the category description, then click *OK*.

6.2.6 Plug-In Studio

Plug-In Studio offers a quick and easy way to streamline the tasks that you do several times a day. Use Plug-in Studio to dynamically create tasks for your most frequently used operations. You can also edit and delete tasks here.

For example, to modify a user, instead of selecting *Modify Object*, you can create a dynamic UI to edit only the attributes you have selected, such as first name or title. Data is stored in the `TOMCAT_HOME/webapps/nps/portal/modules/custom` directory.

From the Plug-in Studio task, you can perform the following operations:

- ♦ “Creating a New Task from Plug-In Studio” on page 64
- ♦ “Editing a Task” on page 65
- ♦ “Deleting a task” on page 65
- ♦ “Copying Custom Tasks” on page 65
- ♦ “Exporting Custom Tasks” on page 65
- ♦ “Importing Custom Tasks” on page 65

Creating a New Task from Plug-In Studio

To create a new task with Plug-In Studio:

- 1 In the Configure view, select *Role-Based Services > Plug-in Studio*.
- 2 Select *New*.

The Task Builder appears to help you build custom tasks and property pages.

- 3 Specify the object type and platform information, then click *Next*.

Available classes: Specify the object class associated with the new task.

Target device: Specify the platform on which the task is used. Typically, the default selection (Default) works fine.

Plug-in type: Specify the type of task you are creating.

Add Auxiliary Classes: Select this option to add aux class support to the task.

- 4 In the Plug-in Fields screen, provide the necessary information, then click *Install*.

When you click *Install*, iManager dynamically builds the task’s `.xml` file, `.jsp` file, and the Java files that execute the task, then it installs those files into the system.

Attributes: Select an attribute to associate with the task from the list of available attributes.

Double-click the attribute to move it to the *Plug-in Fields* field, using the default control.

Controls: Displays the available controls for the attribute selected in the *Attributes* field.

Double-click a control to move the current attribute to the *Plug-in Fields* field, using the selected control.

Plug-in Fields: Displays each attribute/control currently associated with the task. From this field, you can remove attributes from the task, change the control associated with an attribute, and modify the control properties for the attribute.

Plug-in Properties: Lets you specify a *Plug-in ID*, assign the task to an *RBS collection*, and assign the task to a *Role*. The role you assign determines where this task appears in the Roles and Tasks Navigation frame.

Editing a Task

To edit an existing plug-in with Plug-in Studio:

- 1 In the Configure view, select *Role-Based Services > Plug-in Studio*.
- 2 Select the task, then select *Edit*.
- 3 Modify the settings described in “Creating a New Task” on page 60, then click *Install*.
iManager displays a confirmation message indicating the plug-in was successfully created and installed.

Deleting a task

To delete an existing plug-in with Plug-in Studio:

- 1 In the Configure view, select *Role-Based Services > Plug-in Studio*.
- 2 Select the plug-in from the list of installed custom plug-ins, then click *Delete*.
A message appears: Are you sure you want to delete this plug-in?
- 3 Click *OK* to delete the plug-in.
iManager displays a confirmation message indicating the plug-in was successfully deleted.

Copying Custom Tasks

To copy an existing plug-in with Plug-in Studio:

- 1 In the Configure view, select *Role-Based Services > Plug-in Studio*.
- 2 Select the plug-in from the list of installed custom plug-ins, then click *Actions > Copy*.
- 3 Specify a name for the copied plug-in, then click *OK*.

Exporting Custom Tasks

Use this task to export your custom tasks, making them deployable to other iManager servers.

- 1 In the Configure view, select *Role-Based Services > Plug-in Studio*.
- 2 Select the custom plug-in to export, then click *Actions > Export*.

Importing Custom Tasks

Use this task to deployan exported custom tasks onto multiple iManager servers.

- 1 In the Configure view, select *Role-Based Services > Plug-in Studio*.

- 2 Select *Actions > Import*.
- 3 Specify, or use the Object Selector to find, the RBS collection into which you want to import the custom plug-ins.
- 4 Specify, or browse to, the NPM file that you previously exported.
- 5 Click *Import*.

6.2.7 Editing Member Associations

There are two ways to associate members with roles:

- ♦ Select a member, then assign it to a role within a scope as described in “[Set a Member Association](#)” on page 59.
- ♦ Select a role, then assign members and a scope to it as described below.

To assign an existing role to a selected member

- 1 In the Configure view, select *Role Based Services > Edit Member Association*.
- 2 Specify, or use the Object Selector to find, a member, then click *OK*.
A list appears displaying the roles to which this member is assigned.
- 3 Specify a role and role scope to add to this member, then click *OK*.

This data is saved to eDirectory. After login, the newly assigned role appears in the left column of the member who owns it.

6.2.8 Editing Owner Collections

Use this task to change the owner assigned to a collection.

- 1 In the Configure view, select *Role Based Services > Edit Owner Collections*.
- 2 Specify, or use the Object Selector to find, a collection owner, then click *OK*.
- 3 Add or remove collections this person can own, then click *OK*.

6.3 RBS Reporting

The RBS Reporting feature lets you generate reports about RBS objects in the directory and their configuration. Reports are in chart format and can be exported to other formats and printed. RBS Reporting generates the following reports:

Role Assignments	Unassigned Tasks
Role Tasks Assignments	Unassigned Categories
User Roles Assignments	Custom Roles
User Task Assignments	Custom Tasks
Role Rights Assignments	Custom Categories
Unassigned Roles	Collections

6.3.1 Creating Reports

To create an RBS Report:

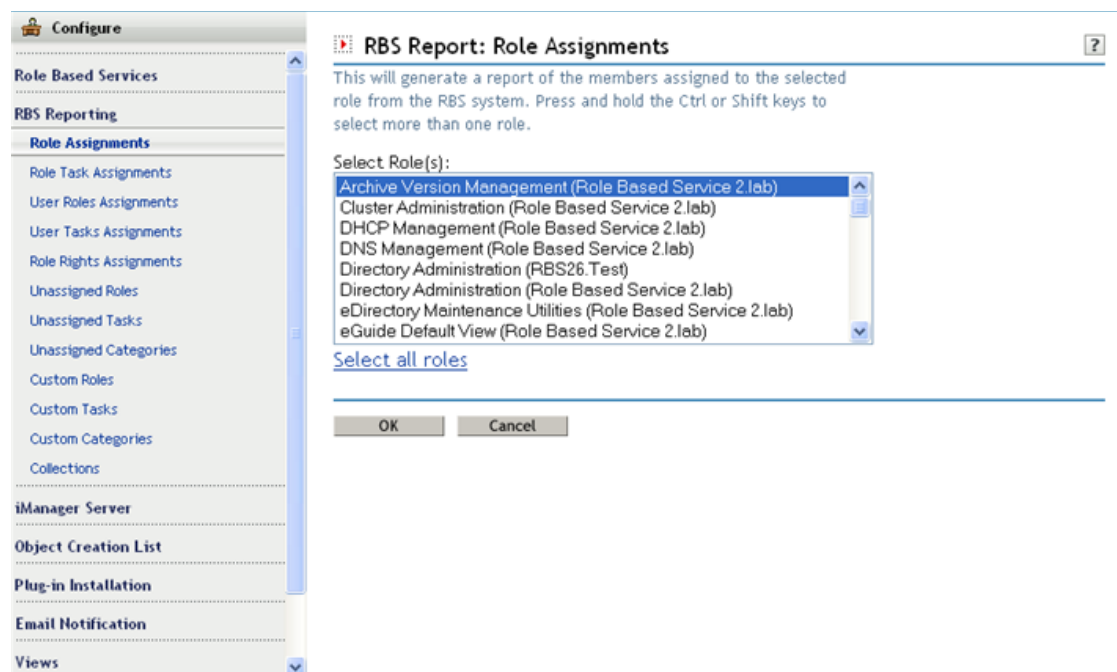
- 1 In the Configure view, select *RBS Reporting*.

Each type of report is implemented as a task.

- 2 Select the desired report, provide the necessary information, then click *OK*.

Each report requires that you provide some initial information, such as the roles for which you want to generate a list of assigned members.

Figure 6-3 iManager Configure View Showing the Role Assignments Task



6.3.2 Using Reports

The RBS Reporting tasks generate reports that you can sort, print, and export. The following figure shows an example of an iManager report.

Figure 6-4 Members Assigned to a Role



Sorting Reports

By default, the items listed in a report are sorted alphabetically in ascending order on the first column. To indicate the column in which items are sorted, iManager displays a small icon next to the column name, and the icon indicates the sort order. To change the column in which items are sorted, click the name of the column you want. To change the sort order, click the name of the column in which items are currently sorted.

Printing Reports

You can easily print RBS reports by clicking the *Print* button. This opens your browser's print dialog box, where you can select a printer and other printing options. This feature prints only the browser frame that contains the report and it prints the report as displayed in the frame, so you should make sure the items are sorted in the order you want before you click *Print*.

Exporting Reports

You can export report data to XML, CSV, and plain text files to use in other applications such as spreadsheets and databases. The export files contain only data and enough metadata to describe the report columns. Other information, such as the report title and date, is not exported. Items in a report are exported in the currently displayed sort order.

- 1 Click the *Export* button.
- 2 In the RBS Report Export window, select the format for the exported data, then click *Export*.
- 3 When your browser prompts you to open or save the file generated by iManager, select the option you prefer and proceed as required by your browser.

The following are examples of XML, CSV, and plain text files exported from the same RBS report:

XML:

```
<?xml version="1.0"?>
<rbs-report>
  <rbs-record>
    <role-name>eDirectory Administration</role-name>
    <role-object>eDirectory Administration.Role Based Service
2.novell</role-object>
    <member-type>User</member-type>
    <member-object>admin.novell</member-object>
    <scope>.MY_TREE.</scope>
    <rights-assigned>true</rights-assigned>
    <rights-inherit>true</rights-inherit>
  </rbs-record>
  <rbs-record>
    <role-name>eDirectory Administration</role-name>
    <role-object>eDirectory Administration.Role Based Service
2.novell</role-object>
    <member-type>User</member-type>
    <member-object>jdoe.novell</member-object>
    <scope>novell</scope>
    <rights-assigned>true</rights-assigned>
    <rights-inherit>true</rights-inherit>
  </rbs-record>
</rbs-report>
```

CSV:

```
"Role Name","Role
Object","Type","Member","Scope","Assigned","Inherit",
"eDirectory Administration","eDirectory Administration.Role Based
Service 2.novell","User","admin.novell",".MY_TREE.","true","true",
"eDirectory Administration","eDirectory Administration.Role Based
Service 2.novell","User","jdoe.novell","novell","true","true",
```

Plain text:

```
Role Name: eDirectory Administration
Role Object: eDirectory Administration.Role Based Service 2.novell
Type: User
Member: admin.novell
Scope: .MY_TREE.
Assigned: true
Inherit: true
```

```
-----
Role Name: eDirectory Administration
Role Object: eDirectory Administration.Role Based Service 2.novell
Type: User
Member: jdoe.novell
Scope: novell
Assigned: true
Inherit: true
-----
```

6.4 iManager Server

If you do not see this task, you are not an authorized user. See [“Authorized Users” on page 70](#). This topic includes the following information:

- ♦ [Section 6.4.1, “Configure iManager,” on page 69](#)
- ♦ [Section 6.4.2, “Security,” on page 70](#)
- ♦ [Section 6.4.3, “Look and Feel,” on page 71](#)
- ♦ [Section 6.4.4, “Logging Events,” on page 71](#)
- ♦ [Section 6.4.5, “Authentication,” on page 71](#)
- ♦ [Section 6.4.6, “RBS,” on page 72](#)
- ♦ [Section 6.4.7, “Plug-In Download,” on page 73](#)
- ♦ [Section 6.4.8, “Misc,” on page 73](#)

6.4.1 Configure iManager

There are three settings in the `config.xml` file that control the security and the certificates used when iManager creates an LDAP SSL connection:

Security.Keystore.AutoUpdate: If the value of AutoUpdate is True, when a user successfully logs in to iManager, the certificate from that eDirectory server might automatically be imported into the iManager-specific keystore. Select the setting [Auto Import Tree Certificate for Secure LDAP](#) (*Configure iManager > Security*).

Security.Keystore.UpdateAllowAll: When UpdateAllowAll is True, then any successful user login imports/updates a certificate into the iManager certificate keystore. If the setting is false, only an **authorized user** login imports/updates certificates.

Security.Keystore.Priority: The priority setting contains two words that define the search order for certificates during a connection: *system*, and *imanager.system* uses the default JVM* keystore to locate certificates when created the SSL context. If that fails, it then goes to the iManager keystore.

You can change the search order of *system* and *iManager* by removing either word from the entry.

To further tighten security, do not allow AutoUpdate and use only the system keystore. If you do this, you must manually import the certificates that you want to reside in the default system keystore by using the tools that come with Java. If you disable UpdateAllowAll, then certificate imports occur only from a successful iManager authorized user login.

6.4.2 Security

These settings affect your entire Web server configuration and are saved in the `config.xml` file. You can either save as you go or click *Save* once after you have made all your changes.

Warn When Using a Nonsecure Connection

Select this option if you want users without a secure connection between the Web browser and the Web server to receive the following warning: You are using a non-secure connection.

Enable Novell Audit

Make sure you have met the Novell Audit **Prerequisites**. Select the Enable Novell Audit option and select specific iManager logging events, then click *Save*.

Auto Import Tree Certificate for Secure LDAP

Secure LDAP connections require a certificate. If you select this feature, the system automatically imports a public tree certificate for secure LDAP.

Authorized Users

Authorized users are those that iManager permits to perform its various administrative tasks. Authorized user data is saved in `TOMCAT_HOME\webapps\nps\WEB-INF\configiman.properties`. The iManager installation process creates this file only if authorized user information is provided, but doing so is not required. Failure to do so results in iManager allowing any user to install iManager plug-ins and modify iManager server settings (not recommended long-term.)

After installing iManager, you can add an authorized user by specifying, or using the Objector Selector to find, the user object in the *Authorized Users* field. Doing this modifies the `configiman.properties` file.

To designate all users as authorized users, type `AllUsers`.

For security-related information about the `configiman.properties` file, see **“iManager Authorized Users” on page 102**.

6.4.3 Look and Feel

The *Look and Feel* tab lets you customize the appearance of the iManager interface. This information is stored in `TOMCAT_HOME\webapps\nps\WEB-INF\config.xml`.

Title Bar Name

Specify your organization name in this text box. It then appears in the title bar of the Web browser in place of the default text (Novell iManager).

Images

The Title bar contains three images: the header background image, the header filler image, and the header branding image. Your own images must conform to the dimensions given in the interface.

Store these files in `nps/portal/modules/fw/images`. Specify the path of each image in its respective text field.

Navigation Menu Colors

You can customize the color of the menu header and the background of the navigation menu on the left.

You can type either color names or hexadecimal numbers. Entries do not need to be case sensitive. Click *Reset* to return to default colors and images, or click *Save* to save the settings. to the `config.xml` file.

6.4.4 Logging Events

The *Logging Events* tab lets you configure iManager's logging environment. There are two logging settings:

Logging Level: Select the types of messages you want to log, from four options: *No Logging*, *Errors only*, *Errors and Warnings*, and *Errors, Warnings and Debug Information*.

Select your logging output options.

Logging Output: Select the destination for logged messages, from three options: *Send Log Output to Standard Error Device*, *Send Log Output to Standard output Device*, and *Send Log Output to Debug.html File*.

The log file path and log file size both appear on this page. Select *View* to display the current log file in HTML format. Select *Clear* to clear the current log file and reset the log file size to 0 (zero) bytes.

6.4.5 Authentication

The *Authentication* tab configures iManager's login page. It contains the following options:

Remember login credentials: When selected, users must only enter a password to log in.

Use Secure LDAP for auto-connection: When selected, iManager performs LDAP communications using SSL. Some plug-ins, such as Dynamic Groups and NMAS™, do not work if this option is not selected. This setting does not take effect until you log out of iManager.

Hide specific reason for login failure: When selected, iManager replaces authentication-related eDirectory messages with a generic error message that reads: `Login Failure. Invalid Username or Password`. For more information, see “[Preventing Username Discovery](#)” on [page 103](#).

Allow ‘Tree’ selection on Login page: When selected, iManager’s login page displays the *Tree* field. If you do not select this option, you must have a default tree name specified or you cannot log in.

Contextless Login: Contextless login allows users to log in with only a username and password, without knowing their entire User object context (for example, `.admin.support.sales.novell`.)

If there are multiple users with the same username in the tree, contextless login tries to log in using the first user account it finds with the supplied password. In this case, a user should provide a full context when logging in or limit the search containers that contextless login searches.

Select *Search from Root* to perform the user search from the root of the directory tree. Select *Search Containers* to specify one or more containers where User objects can be found.

By default, iManager connects with public access, requiring no specific credentials. You can specify a user with specific credentials to do the search for the contextless lookup. The iManager public user is used if you don’t specify a user.

IMPORTANT: If you specify a public user, consider carefully the implications of password expiration settings. If the password is set to expire for the public user, you do not have the opportunity to change the password during login after it expires.

6.4.6 RBS

Role-Based Services (RBS) assigns the rights within eDirectory to perform tasks. When you assign a role to a user, by default RBS assigns the rights necessary to perform the tasks included with that role.

The *RBS* tab lets you configure the following settings:

Enable Dynamic Groups: When selected, RBS allows dynamic groups to be members of a role. For more information about dynamic groups, see the [eDirectory Administration guide \(http://www.novell.com/documentation/edir88/index.html?page=/documentation/edir88/edir88/data/fbabihtml#fbacjdfg\)](http://www.novell.com/documentation/edir88/index.html?page=/documentation/edir88/edir88/data/fbabihtml#fbacjdfg).

Show Roles in Owned Collections: When selected, collection owners see all roles and tasks whether they are members of them or not. Deselect this option to force collection owners to see only their assigned roles.

Role Discovery Domain: Indicates where in the tree iManager is to search for roles that are assigned to a member.

- ♦ Parent, iManager searches for Dynamic Groups up to the parent container.
- ♦ Partition, iManager searches for Dynamic Groups up to the first eDirectory partition.
- ♦ Root, iManager searches for Dynamic Groups in the entire tree.

Dynamic Group Discovery Domain: Indicates where in the tree iManager is to search for Dynamic Group membership. Role membership is then checked in the Dynamic Groups found.

- ♦ Parent, iManager searches for roles in the user's parent container.
- ♦ Partition, iManager searches for roles up to the first eDirectory partition.
- ♦ Root, iManager searches for roles in the entire tree.

Dynamic Group Search Type: Selects which type of Dynamic Groups should be searched for role membership.

- ♦ Dynamic Groups only, searches for objects that are of the Dynamic Group class type.
- ♦ Dynamic Group Objects and Aux classes, searches for objects that are either of the dynamicGroup class type or have been extended with the dynamicGroupAux class. This includes group objects that were later converted to Dynamic Groups.

RBS Tree List: Auto-populated with the eDirectory tree's name when a collection owner or a role member authenticates. If RBS is removed from an eDirectory tree, remove that tree's entry in this list in order to return to Unassigned Access mode.

6.4.7 Plug-In Download

The *Plug-in Download* tab lets you configure the following settings:

Query Novell download site for new Novell Plug-in Modules (NPM): Indicates that the iManager Server should query the [Novell Download site](http://download.novell.com/index.jsp?product_id=&search=Search&build_type=SDBuildBean&families=&date_range=&keywords=iManager&x=23&y=4) (http://download.novell.com/index.jsp?product_id=&search=Search&build_type=SDBuildBean&families=&date_range=&keywords=iManager&x=23&y=4) for new plug-in modules (NPMs).

Two radio buttons let you configure the query for every available NPM, or query only for updates to already-installed NPMs.

IMPORTANT: iManager 2.7 plug-ins are not compatible with previous versions of iManager. Additionally, any custom plug-ins you want to use with iManager 2.7 must be re-compiled in the iManager 2.7 environment.

6.4.8 Misc

The *Misc* tab lets you configure the following settings:

Enable [this]: You can safely ignore this option. Enable [this] was added to iManager to allow some internal teams to modify their own objects. [this] is an attribute in the tree that enables specific self-management functionality. If [this] is enabled, all eDirectory servers in the tree must be version 8.6.2 or later.

eGuide URL: Specifies the URL to eGuide. This is used in the eGuide launch button in the header and in the eGuide role and task management tasks. This must be a full URL, (for example, <https://my.dns.name/eGuide/servlet/eGuide>) or the keyword EMFRAME_SERVER. Using EMFRAME_SERVER causes eMFrame to look for eGuide on the same server on which eMFrame is located.

For more information on eGuide, see the [Novell eGuide documentation Web site](http://www.novell.com/documentation/eguide212/index.html) (<http://www.novell.com/documentation/eguide212/index.html>).

6.5 Object Creation List

When you create an object, a preconfigured list of object classes is registered with the Create Object task. The Object Creation List Category contains the following tasks:

- ♦ [Section 6.5.1, “Adding an Object Class to the Creation List,” on page 74](#)
- ♦ [Section 6.5.2, “Deleting an Object Class from the Creation List,” on page 74](#)

6.5.1 Adding an Object Class to the Creation List

Use this task to add more objects to the Object Creation List, which is the list of objects that can be created in iManager, using the Directory Administration > Create Object task.

- 1 In the Configure view, select *Object Creation List > Add Object Class to Creation List*.
- 2 Select the object to add, then click *Next*.
- 3 Review the XML definition information, then click Finish to create the .xml file.

6.5.2 Deleting an Object Class from the Creation List

Use this task to delete an object from the Object Creation List, which is the list of objects that can be created in iManager, using the Directory Administration > Create Object task.

- 1 In the Configure view, select *Object Creation List > Delete Object Class from Creation List*.
- 2 Select the object to delete, then click *Next*.
- 3 Review the XML definition information, then click Finish to delete the object from the Object Creation List.

6.6 Plug-In Module Installation

If you do not see this role in your iManager interface, you are probably not an authorized user. See [“Authorized Users” on page 70](#).

There are two types of modules used in iManager:

Novell Plug-in Module (NPM): These are archives that contain the files for plug-ins to iManager. When you install an NPM using the Available Novell Plug-in Modules task, you are installing a plug-in to iManager to add to its functionality.

RBS Module: These are objects in eDirectory that contain RBS Tasks and RBS Book objects. When Role-Based Services has been configured in an eDirectory tree, click *Configure > RBS Configuration* to install the RBS Module after the NPM in order for the new tasks associated with the plug-in to become available for use.

Module Installation relates to NPMs only. For information about installing NPMs during the iManager installation process, see [“Downloading and Installing Plug-Ins During Installation”](#) in the *iManager 2.7 Installation Guide*.

6.6.1 Available Novell Plug-in Modules

The Available Novell Plug-in Modules (NPM) page lists all the available NPMs contained in the packages directory/download site. (See “[Plug-In Download](#)” on page 73.) The name, version, and description of each module are in their respective manifest files.

6.6.2 Installed Novell Plug-in Modules

This list contains the NPMs that have been installed in iManager. Each NPM is listed by name, local version, and description found in the current manifest files.

iManager 2.7 does not include all plug-in modules as part of the base product. Most iManager 2.7 plug-ins must be downloaded separately. However, the following plug-ins are included in the *base.npm* module that ships with iManager 2.7:

- ♦ Directory Administration
- ♦ Partitions and Replicas
- ♦ Help Desk
- ♦ Schema
- ♦ Rights
- ♦ Users
- ♦ Groups

For more information, see [Chapter 5, “Roles and Tasks,”](#) on page 35.

IMPORTANT: To function properly, a plug-in module's version must be compatible with the version of iManager on which it is running. Refer to the specific product documentation for information about iManager version requirements for a particular plug-in module.

For example, iManager 2.7 plug-ins are not compatible with previous versions of iManager. Additionally, any custom plug-ins you want to use with iManager 2.7 must be re-compiled in the iManager 2.7 environment.

6.7 Downloading and Installing Plug-in Modules

iManager 2.7 lets you download and install updates to existing and new plug-ins from within iManager. iManager automatically queries the Novell Download Web site once a week for plug-ins.

NOTE: Plug-in modules are not replicated between iManager servers. We recommend that you install the plug-in modules you want on each iManager server.

To download and install one or more plug-in modules:

- 1 Launch iManager and log in.
- 2 In the Configure view, select *Plug-in Installation > Available Novell Plug-in Modules*.

The Content frame lists all the available iManager plug-ins. iManager automatically checks the Novell download site once a week for updated plug-ins. However, you can update the list at any time by clicking the *Refresh* link.

- 3 (Optional) If you have downloaded a plug-in, or have one locally that you want to install, click *Add*, then browse for the appropriate plug-in NPM file.
- 4 Click *OK*.

This returns you to the Available Novell Plug-in Modules page.
- 5 Select the plug-in you want, then click *Install*.

The file location shows whether the plug-in is local or from download. Installing a plug-in from the Novell download site can take several minutes, depending on your connection speed and how many plug-ins are being installed. A status bar indicates the download time.
- 6 Restart Tomcat.

Tomcat sometimes requires several minutes to fully initialize. Wait at least 5 minutes before trying to log in to iManager.

For information about restarting Tomcat, see “Starting and Stopping Tomcat” on page 90.
- 7 Verify that the new Role appears in the Roles and Tasks page.

To add members to the new Role, use the Modify Member Association task.

6.7.1 If RBS is Configured

IMPORTANT: In order to reinstall an existing plug-in, you must first delete the rbsModule object for that plug-in from eDirectory using the *Module Configuration > Delete RBS Module* task.

- 1 From the Configure view, select *Role-Based Services > RBS Configuration*.

The table on the 2.x Collections tab displays any out-of-date modules.
- 2 To update them, select the number in the Out-of-Date column for the Collection you want to update.

The list of outdated modules is displayed.
- 3 Select the modules you want to update, then click Update at the top of the table.

6.7.2 Uninstalling a Plug-in Module

- 1 In the Configure view, select *Plug-in Installation > Installed Novell Plug-in Modules*.
- 2 Select the plug-in, then click Uninstall.
- 3 Restart Tomcat.

For information about restarting Tomcat, see “Starting and Stopping Tomcat” on page 90.

The steps for manually removing a plug-in module are available in [TID #10096957 \(http://support.novell.com/cgi-bin/search/searchtid.cgi?/10096957.htm\)](http://support.novell.com/cgi-bin/search/searchtid.cgi?/10096957.htm).

6.7.3 Customizing the Plug-In Download Location

You can create a plug-in download repository if a proxy server or firewall prevents iManager 2.7 from contacting the Novell download Web site. This lets you host plug-in modules on a local Web server or a common file system location.

The best way to do this is to use the XML descriptor file from the [Novell download Web site \(http://www.novell.com/products/containers/imanager/iman_mod_desc.xml\)](http://www.novell.com/products/containers/imanager/iman_mod_desc.xml) as a template. For more

information about the iManager descriptor file, see “[Downloading and Installing Plug-Ins During Installation](#)” in the *iManager 2.7 Installation Guide*.

To set up a local plug-in repository, save the descriptor file locally; then open the file and copy the URL for each plug-in module you want to make available locally, and paste it in a Web browser address bar to download the file. After downloading all desired plug-in modules, edit the local copy of the descriptor file to reflect the new URL for each downloaded plug-in module.

A plug-in module URL can be an HTTP link or a file system location. For example:

Windows File System

```
<url><![CDATA[file:///c:\iManager_plugins\NMA5.npm]]></url>
```

Linux File System

```
<url><![CDATA[file:///home/admin/iManager_plugins/NMA5.npm]]></url>
```

HTTP Link

```
<url><![CDATA[http://192.168.0.136/iManager_plugins/NMA5.npm]]></url>
```

Specifying a Local Descriptor File

You can specify a custom descriptor file either during the iManager 2.7 installation, or after iManager 2.7 has been installed.

During the installation process, the iManager 2.7 plug-in download URL can be redirected to a custom descriptor file. To do this, simply change the URL on the Select Plug-ins to Download and Install page to the location of the custom descriptor file and click *Go*.

NOTE: If the message `No plug-ins found or server not available` appears in the Plug-in download area, one or both of the following conditions can exist: There are no updated plug-ins available on the Novell download site, or the connection to download. novell.com from the install program was not successful. Verify your Internet connection.

When iManager 2.7 is installed, you can change the plug-in module download URL by modifying `<TOMCAT_HOME>\webapps\nps\WEB-INF\config.xml`. For example:

Windows File System

```
<setting>
  <name><![CDATA[ModuleDownloadDescriptorURL]]></name>
  <value><![CDATA[file:///c:\iManager_plugins\custom.xml]]></value>
</setting>
```

Linux File System

```
<setting>
  <name><![CDATA[ModuleDownloadDescriptorURL]]></name>
  <value><![CDATA[file:///home/admin/iManager_plugins/custom.xml]]></value>
</setting>
```

HTTP Link

```
<setting>
  <name><![CDATA[ModuleDownloadDescriptorURL]]></name>
  <value><![CDATA[http://192.168.0.136/iManager_plugins/
custom.xml]]></value>
</setting>
```

IMPORTANT: If you use iManager Workstation to access a custom plug-in URL over an SSL connection (HTTPS), make sure to import the target Web server's certificate or you won't be able to set up a secure connection.

6.8 E-Mail Notification

This role enables you to select plug-in-specific tasks that users want to be notified of whenever that specific task occurs. The tasks are set up by the plug-in itself. You decide whether or not to be notified, and specify who should be notified of selected events. Your first task is to set up the mail server.

TIP: Depending on what you select, you could receive a *lot* of e-mail!

6.8.1 Mail Server Configuration

The mail server configuration specifies the SMTP server settings for event notification.

- 1 In the Configure view, select Email Notification > Mail Server Configuration.
- 2 Specify the mail server settings, then click *OK*.
 - From Address:** Specifies the address that appears in the From field of the iManager e-mail message.
 - Primary Mail Server:** Specifies an IP address or server name (for example: smtp.novell.com) of a mail server. You must also provide the username and password for iManager to use to access the SMTP server.
 - Secondary Mail Server:** Specifies an optional backup mail server. Provide the same information as that for the primary mail server.

6.8.2 Task Event Notification

Plug-ins whose tasks are listed in their .xml files automatically register task events on this page.

- 1 In the Configure view, select *Email Notification > Task Event Notification*.
- 2 In the *Email Address* field, specify the E-mail addresses you want to receive this notification, separated by commas.
- 3 Select an event.

The Task Event Properties screen appears.
- 4 Specify the e-mail subject and the E-mail message in the appropriate fields.
- 5 In the *Additional Email Addresses* field, type any additional e-mail addresses (separated by commas) you want to notify.

- 6 Select *Override Default and Notify Only These Addresses* if you want the message to ignore the E-mail list in step 2 and go only to the e-mail addresses specified on this page.

6.9 Views

If you do not see this role in your iManager interface, you are probably not an authorized user. See [“Authorized Users” on page 70](#).

iManager Views are management pages accessed from buttons in iManager’s Header frame. You might want to prevent users from accessing certain views, such as *View Objects* or *Configure*.

By default, all views inherit the settings of the parent set.

6.9.1 Showing and Hiding iManager Views

- 1 In the Configure view, select *Views > iManager Views*.
- 2 Specify, or use the Object Selector to find, a container at which you want to restrict access to Views, then click OK.
- 3 Specify the appropriate view settings, then click *OK*.

There are three view settings from which you can choose:

- ♦ Do not set: Does not explicitly set the view state. This is the default setting.
- ♦ Hide: Hides the view.
- ♦ Show: Displays the view.

Select *Read parent containers of this object* to use the settings of the object's parent container for this object. When selected, the parent settings take precedence over the object’s local settings.

Preferences

7

The Preferences view lets you configure iManager settings related to the application's look and feel. It provides access to the following tasks:

- ♦ [Section 7.1, “Manage Favorites,” on page 81](#)
- ♦ [Section 7.2, “Object Selector,” on page 81](#)
- ♦ [Section 7.3, “Object View,” on page 82](#)
- ♦ [Section 7.4, “Set Initial View,” on page 82](#)
- ♦ [Section 7.5, “Language,” on page 82](#)

7.1 Manage Favorites

Configures the Favorites view, which displays a custom set of often-used tasks together in a special view.

- 1 From the Preferences view, select *Manage Favorites*.
- 2 Select the desired tasks from the *Tasks* field and move them to the *Favorites* field.
Double click tasks to move them, or select them and use the arrow icons to move them.
Select *Make favorites my initial view* to use the Favorites view as your iManager “Home page”.
- 3 Click *OK*.

7.2 Object Selector

Configures the Object Selector settings:

Window Size: Specify Object Selector's window width, height, and left column width, in pixels.

User-Specified Defaults: Specify Object Selector's default settings, including

- ♦ **Startup Mode:** Specifies whether the *Browse* tab or *Search* tab is displayed initially.
- ♦ **Results per Page:** Specifies the number of results to display per page.
- ♦ **Starting Context:** Specifies the default container to which Object Selector opens.
- ♦ **Search on Startup:** Specifies initial search actions when Object Selector opens to the *Search* tab.
- ♦ **Show Subordinate Count:** Enables/disables displaying the total number of objects next to each container object displayed in the Object Selector. When selected, iManager displays the subordinate object count, in parentheses, next to the container name.

NOTE: The subordinate count does not take into account your assigned rights when calculating the subordinate object count, so the number of objects you can see might differ from the count specified.

7.3 Object View

Configures the Object View settings:

Column Width: Specifies Object View's column width, in pixels.

Startup Mode: Specifies whether the *Browse*, *Search*, or *Tree* tab is displayed initially.

Selection Mode: Specifies Object View's initial object selection mode: single object, or multiple objects.

Navigation Pane (Left Side): Specifies the number of results to display in the Navigation frame. This setting applies to all tabs in the Object View. Valid settings include 1 - 500.

Tree Content Pane (Right Side): Specifies the number of results to display on one page in the Content frame. This setting applies only to the Tree tab in the Object View. Valid settings include 1 - 500.

Starting Context: Specifies the default directory container to which Object View opens. You can have it open to the last container used, or have it always open to the same container.

Search on Startup: Specifies initial search actions when Object View opens to the *Search* tab.

Show Subordinate Count: Enables/disables displaying the total number of objects next to each container object displayed in the Object Selector. When selected, iManager displays the subordinate object count, in parentheses, next to the container name.

This applies to the Navigation frame in the Tree tab, and the results window in the Browse and Search tabs in the Object View.

NOTE: The subordinate count does not take into account your assigned rights when calculating the subordinate object count, so the number of objects you can see might differ from the count specified.

7.4 Set Initial View

Specifies the view that displays when you first log in to iManager. If nothing is selected, the *Roles and Tasks* view defaults to the initial view. You select determines what appears after you log in to iManager.

7.5 Language

Specifies the language in which you want iManager to display. You must select the check box to remember the language will remember the language setting between iManager sessions. To make the language setting permanent, set your preferred default language in the Web browser.

NOTE: Plug-ins cannot work properly if the first language (top position) listed in your Web browser's Language setting is not set to a supported language for iManager.

To avoid problems, in your Web browser, click *Tools > Options > Languages* or a sequence similar to this, then set the first language preference in the list to a supported language.

This section provides some troubleshooting tips resulting from Novell's testing of iManager. These tips are arranged alphabetically in the following topics:

- ♦ Section 8.1, "Authentication Issues," on page 83
- ♦ Section 8.2, "Deleting and Re-creating User Accounts with the Same Name (Windows XP/2000)," on page 86
- ♦ Section 8.3, "DNS 630 Error Message Appears When Creating a Property Book with Invalid Characters in Name," on page 86
- ♦ Section 8.4, "eDirectory Maintenance Task Errors," on page 86
- ♦ Section 8.5, "Enabling Debug Messages for Install and Configure," on page 86
- ♦ Section 8.6, "History Does Not Automatically Sync Across Multiple Simultaneous User Logins," on page 87
- ♦ Section 8.7, "iManager Doesn't Work after Installing Groupwise 7.0 WebAccess (Windows Server 2000/2003)," on page 87
- ♦ Section 8.8, "Missing Attribute, Object, or Value Errors," on page 87
- ♦ Section 8.9, "Missing Roles or Tasks in the Configure View," on page 87
- ♦ Section 8.10, "Performing a System Restore from Image Software," on page 88
- ♦ Section 8.11, "Running eDirectory and iManager on the Same Machine (Windows only)," on page 88
- ♦ Section 8.12, "'Service Unavailable' Message Appears During Multiple Plug-In Installs," on page 89
- ♦ Section 8.13, "Tomcat," on page 89
- ♦ Section 8.14, "'Unable to Determine Universal Password Status' Error," on page 90
- ♦ Section 8.15, "(Windows) iManager workstation does not display information," on page 91

8.1 Authentication Issues

Authentication is a complex topic, and your existing network infrastructure can affect your ability to successfully perform an initial iManager login. The following facts can help you minimize authentication-related difficulties. For more information about authentication-related topics, see Novell's [NMA3 documentation \(http://www.novell.com/documentation/nmas30/index.html\)](http://www.novell.com/documentation/nmas30/index.html) and [eDirectory documentation \(http://www.novell.com/documentation/edir88/index.html\)](http://www.novell.com/documentation/edir88/index.html).

- ♦ iManager authentication is a platform-dependent operation, meaning that it functions differently depending on the platform on which iManager is running

NetWare servers: When iManager runs on a NetWare server (including OES NetWare) it utilizes eDirectory's legacy authentication mechanism and the regular eDirectory password. This mechanism does not support eDirectory's Simple Password or Universal Password options.

Linux and Windows servers: When iManager runs on a Linux or Windows server it utilizes eDirectory's legacy authentication mechanism and the regular eDirectory password. This mechanism does not support eDirectory's Simple Password or Universal Password options.

iManager Workstation: iManager Workstation runs on a client workstation, either Linux or Windows, and leverages the NMAS client that allows it to use Universal Password, if configured.

- ♦ iManager does not use LDAP for the initial iManager authentication process. It utilizes eDirectory's proprietary authentication protocol. However, following initial authentication, iManager can, create LDAP connections to eDirectory as needed to support directory access for the installed plug-ins that require LDAP access.
- ♦ iManager does not support authenticating with eDirectory's Simple Password.

You might encounter the following error messages when authenticating to iManager. Each error message section discusses possible causes.

- ♦ [Section 8.1.1, "HTTP 404 Errors," on page 84](#)
- ♦ [Section 8.1.2, "HTTP 500 Errors," on page 84](#)
- ♦ [Section 8.1.3, "601 Error Messages," on page 85](#)
- ♦ [Section 8.1.4, "622 Error Messages," on page 85](#)
- ♦ [Section 8.1.5, "632 Error Messages," on page 85](#)
- ♦ [Section 8.1.6, "634 Error Messages," on page 85](#)
- ♦ [Section 8.1.7, "669 Error Messages," on page 85](#)

8.1.1 HTTP 404 Errors

If you receive a 404 error the first time you attempt to access iManager, you need to verify the ports that Apache is running on. Depending on how you installed iManager and whether you chose to use Apache or IIS, the configuration file locations vary. Apache uses either the `httpd.conf` file or the `ssl.conf` file. Refer to the Microsoft documentation for information on IIS port settings.

8.1.2 HTTP 500 Errors

If you receive an internal server error or servlet container error (either unavailable or being upgraded), iManager is having one of two problems with Tomcat:

- ♦ Tomcat has not fully initialized after a reboot.
- ♦ Tomcat has failed to start.

Wait a few minutes and try again to access iManager. If you still receive the same errors, verify the status of Tomcat.

Checking the Status of Tomcat

- 1 Restart Tomcat.

For information about restarting Tomcat, see ["Starting and Stopping Tomcat" on page 90](#).

- 2 Check the Tomcat logs for any errors.

The log file is located in the `$tomcat_home$/logs` directory on the UNIX, Linux, and Windows platforms. On UNIX and Linux, the logs are named `catalina.out` or `localhost_log.date.txt`; on Windows, the log files are named `stderr` and `stdout`. On NetWare, errors appear on the logger screen.

8.1.3 601 Error Messages

The object name entered could not be found in the context specified.

Some possible causes:

- ♦ Contextless login might be disabled.
- ♦ Your User object might not be in the configured search containers list. Either ask your administrator to add your user location to the contextless login search containers or log in with a full context.

8.1.4 622 Error Messages

The NDS password has been disabled in the Universal Password policy. This may also manifest itself with a 222 Error Message.

You can avoid this error with iManager Workstation by installing the NMAS client, which allows iManager to utilize the Universal Password authentication mechanism rather than eDirectory's legacy authentication process.

8.1.5 632 Error Messages

This error is a system failure with several [possible causes](http://www.novell.com/documentation/nwec/nwec_enu/nwec_ids_t_err_system_failure.html) (http://www.novell.com/documentation/nwec/nwec_enu/nwec_ids_t_err_system_failure.html).

8.1.6 634 Error Messages

The target server does not have a copy of what the source server is requesting, or the source server has no objects that match the request and has no referrals on which to search for the object.

Some possible causes:

- ♦ You entered an incorrect tree or IP address. If you are using the IP address, make sure you include the port if eDirectory™ is installed on a nonstandard (524) port.
- ♦ iManager cannot locate your tree or IP address before timing out. If the tree name fails, use the IP address.

8.1.7 669 Error Messages

An invalid password was used, authentication failed, one server tried to synchronize with another one but the target server's database was locked, or a problem exists with the remote ID or public key.

Some possible causes:

- ♦ You typed an incorrect password

- ♦ There are multiple users with the same username in the tree. Contextless login tries to log in using the first user account it finds with the supplied password. In this case, provide a full context when you log in or limit the search containers that contextless login searches.

8.2 Deleting and Re-creating User Accounts with the Same Name (Windows XP/2000)

If you have deleted one or more Windows user accounts, and then re-created them with the same name, do the following to use iManager Workstation with the re-created account:

- 1 Log in as a member of the Administrator group.
- 2 Take ownership of the `\system32\novell\nici\username` directory. The absolute path varies between Windows 2000 and Windows XP.
- 3 Delete the folder.

When the user next logs in, this folder is automatically recreated using NCI keys of the re-created user account, and the user can then run iManager Workstation.

8.3 DNS 630 Error Message Appears When Creating a Property Book with Invalid Characters in Name

If you create a Property Book and name it using special characters that are invalid, a DNS Error 603 message might be returned. For more information about naming a Property Book, see [“Creating a New Property Book” on page 61](#).

8.4 eDirectory Maintenance Task Errors

Running eDirectory Maintenance Tasks requires that Role-Based Services (RBS) must be configured through iManager for the tree that is being administered. For RBS configuration information, see [Chapter 4, “Browsing Objects,” on page 25](#).

For additional information, see the [Novell eDirectory documentation \(http://www.novell.com/documentation/lg/edir871/index.html?page=/documentation/lg/edir871/edir871/data/agabn4a.html\)](http://www.novell.com/documentation/lg/edir871/index.html?page=/documentation/lg/edir871/edir871/data/agabn4a.html).

8.5 Enabling Debug Messages for Install and Configure

If installation fails, you must enable some debugging messages to help determine what is wrong.

- ♦ Linux: Export `LAX_DEBUG=true` in the terminal session that you start the iManager InstallAnywhere program from.
- ♦ Windows: Hold the Ctrl key down as you start the iManager InstallAnywhere program and continue holding it until the debugging screen appears.

8.6 History Does Not Automatically Sync Across Multiple Simultaneous User Logins

Using two instances of the same browser (such as two Firefox or two Mozilla browsers but not Internet Explorer) avoids the problem. The history book is shared by the two instances.

8.7 iManager Doesn't Work after Installing Groupwise 7.0 WebAccess (Windows Server 2000/2003)

On Windows 2000 and 2003 Server with IIS 5 or 6, installing Groupwise 7.0 WebAccess to IIS automatically installs Tomcat 5.5.

As the iManager installation begins, the iManager installer program detects that IIS and Tomcat are available for use. The installer reports the inability to stop the iisadmin service. Near the end of the install, the installer reports the inability to start Tomcat.

After the install is completed, Groupwise WebAccess still works, but iManager does not (HTTP 404: Page not found).

Workaround: Do not install iManager and Groupwise on the same server.

8.8 Missing Attribute, Object, or Value Errors

If you have a large installation with synchronization delays, you can force iManager to communicate with the master replica. This ensures that you have access to any attributes, objects, or values that have been recently added or modified. This is not recommended for regular use of iManager, but can be helpful when you are experiencing synchronization delays.

To use this parameter when logging in to iManager, add `&forceMaster=true` to the end of the URL after you have loaded the login page. This setting can also be enabled in `TOMCAT_HOME\webapps\nps\WEB-INF\config.xml`. For example: `https://127.0.0.1/nps/servlet/webacc?taskId=fw.Startup&forceMaster=true`.

You must restart Tomcat after making any changes to the `config.xml` file. For information about restarting Tomcat, see [“Starting and Stopping Tomcat” on page 90](#).

8.9 Missing Roles or Tasks in the Configure View

If the following Roles or Tasks are not present on the Configure view, you need to verify that you are an authorized user. For more information, see [“Authorized Users” on page 70](#).

8.9.1 Possible Missing Roles or Tasks

- ◆ Configure iManager task
- ◆ Object Creation List role
- ◆ Plug-in Installation role
- ◆ Email Notification role
- ◆ View role

8.9.2 Possible Reasons Why You Are Not an Authorized User

- ♦ You renamed your tree.

Edit the `configiman.properties` file and change the tree name for each user.

- ♦ Information entered during the iManager installation for the authorized user was incorrect.

Edit the `configiman.properties` file and add the correct username including the tree name.

- ♦ The `configiman.properties` file has become corrupt for some unknown reason.

Delete the `configiman.properties` file and either re-create the file with the correct information or log in to iManager and go to *Configure view > iManager Server > Configure iManager*. On the Security page, add the Authorized Users for the system by browsing the tree, or if you are sure of the full path to the user, you can manually enter it.

- ♦ The permissions on the `configiman.properties` file have been changed to prevent iManager from reading the file.

Change the permissions on the file to match the files in the same directory.

- ♦ Your administrator has not added you as an authorized user.

Request to be added to the Authorized Users list. For more information, see [“Authorized Users” on page 70](#).

8.10 Performing a System Restore from Image Software

If you perform a system restore from image software such as Ghost, the `sys:\tomcat5\conf\NPS-APACHE.CONF` file could become truncated in the process.

If this file is truncated to `NPS-APACHE~1.CON` or some other corrupt filename, rename the file and then stop and restart Tomcat.

For information about restarting Tomcat, see [“Starting and Stopping Tomcat” on page 90](#).

8.11 Running eDirectory and iManager on the Same Machine (Windows only)

If iManager was installed before eDirectory, you might experience any of the following errors when using iManager, LDAP(S), or HTTP(S) to access eDirectory.

-340 error when trying to access encrypted attributes with iManager

```
LDAP : SSL_CTX_use_KMO failed. Error stack: error:1412D0D4:SSL
routines:SSL_CTX_use_KMO:read wrong packet type (err = -1418)
HTTP : 0016 TLS operation failed, err: 1, result: -1 --
HTTP : -- error:1408A0C1:SSL routines:SSL3_GET_CLIENT_HELLO:no
shared cipher
HTTP : 0017 TLS operation failed, err: 1, result: -1 --
HTTP : -- error:1406B0BD:SSL routines:GET_CLIENT_MASTER_KEY:no p
rivatekey
```



```
HTTP : Unable to access server certificate and key, handshakes
will fail -- HTTP : -- error:1412D0D4:SSL
routines:SSL_CTX_use_KMO:read wrong packet type
Limber : Error while setting NCP Key Material Name SSL
CertificateDNS to server, Err: failed, -340 (0xfffffeac)...
Limber : Error During syncKeyMaterialInfo -340 (0xfffffeac)
```

It could be that eDirectory's initial system configuration has not occurred. The user who installed eDirectory and the user who is running the eDirectory server must coordinate the eDirectory configuration. Generally, eDirectory is installed as administrator and is run as SYSTEM. You can manually correct this issue, but an understanding of eDirectory, iManager, NICI, and other currently installed products is necessary. You must determine if the following steps are safe to perform. You should also check the product's documentation and dependencies to see if any long-term encrypted data or secrets are used.

If eDirectory and iManager are installed on the same physical machine, you can manually configure eDirectory after eDirectory installation.

NOTE: You should not do this if eDirectory was installed at a previous time and has been successfully running on the current machine.

- 1 Log in as an administrator.
- 2 Stop the eDirectory server and the Tomcat service.
Also stop any other service that may be using NICI.
- 3 Take ownership of the %systemroot%\system32\novell\NICI\SYSTEM directory.
Do this from the file properties' *Security > Advanced Options*.
- 4 Save the contents of the SYSTEM directory in a backup directory.
- 5 Delete the contents of the SYSTEM directory.
- 6 Copy the contents of %systemroot%\system32\novell\NICI\Administrator to
%systemroot%\system32\novell\NICI\SYSTEM
- 7 You can reset the permissions of %systemroot%\system32\novell\NICI\SYSTEM
and its contents so that only SYSTEM has access.
- 8 Restart the NDS Server and Tomcat services and any other service you may have stopped.

8.12 “Service Unavailable” Message Appears During Multiple Plug-In Installs

This situation occurs when you select several plug-ins to install, all at the same time. While the plug-in installation continues over several minutes, the browser page times out and returns a 503 Error.

Although you probably don't need to do anything but wait, you can monitor plug-in installations through the Tomcat log files or on the NetWare logger screen.

8.13 Tomcat

The following general Tomcat information can be useful in your troubleshooting efforts.

8.13.1 Starting and Stopping Tomcat

The following tables describe how to start and stop Tomcat on the platforms supported by iManager 2.7.

Table 8-1 *Stopping and Starting Tomcat*

Platform	Restart Command
Linux	Enter <code>/etc/init.d/novell-tomcat5 stop</code> , then enter <code>/etc/init.d/novell-tomcat5 start</code> .
NetWare® 6.5	Enter <code>TC5STOP</code> to stop Tomcat. Wait at least one minute, then enter <code>TOMCAT5</code> to start Tomcat again.
iManager Workstation	Shut down and restart iManager Workstation.
Windows	Stop and start the Tomcat service.

8.13.2 Tomcat Ports

If you experience port conflicts while upgrading to iManager 2.7, or need to know the ports that Tomcat is using, consult the platform-specific information in this section.

NetWare

View Tomcat ports in the `sys:\tomcat\5.0\conf\server.xml` file.

Linux

View Tomcat ports in the `/var/opt/novell/tomcat5/conf/server.xml` file.

The non-SSL port section of the file begins with `Define a non-SSL Coyote HTTP/1.1 Connector on port n`, while the SSL port section begins with `Define an SSL Coyote HTTP/1.1 Connector on port n`.

Windows

Windows allows for relocation of all files. If you accept the defaults in the iManager installation, look for Tomcat configuration files in the `rootdir\novell\tomcat5\conf\server.xml` file.

If you can't find a configuration file, search the Windows registry for the Tomcat settings.

8.14 “Unable to Determine Universal Password Status” Error

If an eDirectory for UNIX server is configured to use SSL for LDAP communications, you might receive the following error when you select the option in iManager to set a Simple Password:

Unable to determine universal password status

To resolve this error, run the `/usr/bin/nmasinst/nmasinst` utility on the eDirectory for UNIX server. This utility lets you install login methods into eDirectory from a UNIX machine and is required to run the Universal Password feature. The `nmasinst` utility is located in the `directory` directory.

For more information, see the *Universal Password Deployment Guide* (http://www.novell.com/documentation/lg/nw65/universal_password/data/front.html).

8.15 (Windows) iManager workstation does not display information

iManager workstation might not display error messages, and load pages like *Tree View*, *Object Browse*, and *Create Objects*. This happens when the XULRunner browser cache contains old data of the previous build of iManager 2.7 workstation.

Work around: You must manually clear the data from browser cache.

1. Exit iManager
2. Browse for
C:\Users\<username>\AppData\<Profile>\Mozilla\eclipse\Cache (the path varies depending on the configuration and OS)
3. Delete that data in this Cache directory
4. Restart iManager

Configuring for iManager Auditing

9

Use Novell® Audit for iManager auditing tasks. For more information, see the *Novell Audit 2.0 Administration Guide* (<http://www.novell.com/documentation/novellaudit20/index.html>).

Novell Audit has the following prerequisites:

- ☐ A server (NetWare®, Solaris*, Windows*, Linux*) in your directory tree with Novell Audit 2.0.x.
- ☐ Novell Audit Platform Agent installed on the iManager server or iManager Workstation desktop and configured to point to the Secure Logging Server.

Novell Audit captures data about the following events:

- ♦ Added authorized user
- ♦ Successful login
- ♦ Successful NPM install
- ♦ Startup iManager
- ♦ Failed SSL connection
- ♦ Logout
- ♦ Changed configuration
- ♦ Failed login
- ♦ Failed NPM install
- ♦ Shutdown iManager

The `IMAN_EN.LSC` file which contains this data is distributed under `nps/support/audit` and is installed via the Novell Audit process. It can also be installed manually via the Novell Audit iManager plug-in as described in the following section.

9.1 Installing the IMAN_EN.LSC File in iManager

Install Novell Audit *before* you install the `IMAN_EN.LSC` file.

- 1 Log in to iManager.
- 2 Select the Auditing and Logging role.
- 3 Select the Logging Server Options task.
- 4 Browse to and select the Logging Server object, then click OK.
- 5 Click the Log Applications tab.
- 6 Select Applications.
- 7 Click the Applications Actions link, then click New.
- 8 Click OK to create a new Log Application in the container.
- 9 Specify a Log Application name.
- 10 To import the `IMAN_EN.LSC` file, click Browse and select the file found in the `TOMCAT_HOME\webapps\nps\support\audit` directory, then click OK.

The new log application should now appear under the Applications container.

9.2 Enabling Auditing in iManager

- 1** Log in to iManager.
- 2** In the Configure view, click iManager Configuration > Configure iManager.
- 3** Select Enable Novell Audit, select the events you want to record, then click Save.

Best Practices and Common Questions

10

This section contains recommendations about the following topics from some of our experts. If you find something that works well for you, please share it at [Cool Solutions \(http://www.novell.com/cool solutions\)](http://www.novell.com/cool solutions).

- ♦ [Section 10.1, “Backup and Restore Options,” on page 95](#)
- ♦ [Section 10.2, “Coexistence with previous versions of iManager 2.x and Role-Based Services,” on page 95](#)
- ♦ [Section 10.3, “Collections,” on page 96](#)
- ♦ [Section 10.4, “Failed Installs,” on page 96](#)
- ♦ [Section 10.5, “High Availability: Running iManager in a Clustered Environment,” on page 97](#)
- ♦ [Section 10.6, “Patching iManager,” on page 98](#)
- ♦ [Section 10.7, “Performance Tuning,” on page 98](#)
- ♦ [Section 10.8, “iManager AppArmor Profile,” on page 99](#)

10.1 Backup and Restore Options

There is no automatic backup and restore feature included with iManager. iManager is composed of two parts: the local files on the server and the Role-Based Services objects in eDirectory™.

To make a full backup of iManager, make sure you have a valid backup of the RBS collection and all subordinate objects in the tree, either through replica redundancy or with an eDirectory backup solution.

All local iManager files on the file system are stored in the Tomcat directory. As long as you have a backup of the Tomcat directory, all iManager content is preserved. If the Tomcat directory is somehow compromised on the server, shutting down Tomcat and recopying the directory allows you to recover iManager. If you are not using RBS, backing up the Tomcat directory is all that is needed.

10.2 Coexistence with previous versions of iManager 2.x and Role-Based Services

You should update your RBS collection to version 2.7. Otherwise, if you use iManager to access a tree that has an RBS collection from a previous version of iManager 2.x, you won't see all of the roles and tasks that should display.

- 1 In the Configure view, click *Role Based Services > RBS Configuration*.
- 2 Click the link in the *Out-of-Date* column for a module that needs updating.
- 3 On the Out-Of-Date Modules page, select a module, then click *Update*.

A message appears that confirms a successful update.

Updated plug-ins are visible in all versions of iManager 2.x.

10.3 Collections

It is important to recognize that one configuration is not ideal for all companies. We recommend multiple collections in a tree only if you use a hierarchical structure using geographical or functional organizations with different administrators in each location. Following are the most common situations together with suggestions for managing their respective collections:

- ♦ A hierarchical tree organized to reflect a geographical organization
Create a collection in every geographical location and have one or more iManager servers per location. Login time is faster and tree navigation is simplified. Each geographical administrator manages the collection of a specified location.
- ♦ A hierarchical tree that reflects the company's organizational structure
Create one collection at the same level as the organization and have one or more iManager servers as company size requires. You manage only one collection.
- ♦ A flat tree in which all objects are in a unique container
Create one collection as a sibling of the unique container and have one or more iManager servers as company size requires. You manage only one collection.

10.4 Failed Installs

To avoid failed installs, make sure that your operating system is updated to the most current version and that all system requirements are met. For more information, see “**Installing iManager**” in the *iManager 2.7 Installation Guide*.

To recover from a failed install, assess the problem from the error message generated during installation.

- ♦ **Section 10.4.1, “Windows,” on page 96**
- ♦ **Section 10.4.2, “Linux,” on page 97**

10.4.1 Windows

- 1** If the error involves one of these components, check the specified log files for errors:

NICI: *installed directory\temp\wcniciu0.log*

Tomcat: *tomcat install directory\Apache_Tomcat_InstallLog.log*. For example, C:\Program Files\Novell\Tomcat\Apache_Tomcat_InstallLog.log.

- 2** Check the iManager install log file (*servlet root\WEB_INF\log\iManager_Install_2.7_InstallLog.log*) for any errors.
- 3** If the log file does not give sufficient information to identify the problem, rerun the install in debug mode.

To view or capture the debug output from an installer, open and copy the console output to a text file for later review.

- 3a** Immediately after launching the installer, hold down the Ctrl key until a console window appears.

- 3b** After the install has completed, click the icon in the upper left corner of the console window and select *Properties > Layout*.
- 3c** Change the buffer size to 3000, then click *OK*.
- 3d** In the Layout window, select *Edit > Select All > Edit > Copy*.
- 3e** Open a text editor and paste the output of the debug in it.
- 4** Identify and correct any errors or stack traces, then rerun the install.

10.4.2 Linux

- 1** Check the iManager install log file (`/var/log/Novell/iManager_Install_2.7_InstallLog.log`) for any errors.
- 2** If the log file does not give sufficient information to identify the problem, rerun the install in debug mode.
At the command line, type the following:
`export LAX_DEBUG=true`
- 3** Identify and correct any errors or stack traces, then rerun the install.

10.5 High Availability: Running iManager in a Clustered Environment

Although iManager is a session-based tool that ships without any failover features, you can run it in a clustered environment. For more information about clustering, see the [OES Clustering documentation](http://www.novell.com/documentation/oes/cluster-services.html#cluster-services) (<http://www.novell.com/documentation/oes/cluster-services.html#cluster-services>).

- 1** Install and configure iManager on the nodes in the cluster where the virtual IP is moved to (that is, an Active/Active cluster).

If the node running iManager fails, Novell Cluster Services[®] detects the node failure and moves (reloads) the virtual IP address on another node in the cluster.

- 2** Using the `Generic_IP_Service` template that ships with Novell Cluster Services, create a new cluster resource called iManager.

This cluster resource uses a virtual IP address that moves between nodes in the cluster. When creating a new cluster resource, the wizard steps you through the creation of a load script and an unload script.

- 3** Verify the load and unload scripts.

The load script should contain only the following lines (any other lines should be commented out):

```
. /opt/novell/ncs/lib/ncsfuns
exit_on_error add_secondary_ipaddress xxx.xxx.xxx.xxx
exit 0
```

The unload script should contain only the following lines (any other lines should be commented out):

```
. /opt/novell/ncs/lib/ncsfuns
ignore_error del_secondary_ipaddress xxx.xxx.xxx.xxx
exit 0
```

- 4** Browse to the **iManager URL**.

iManager services are now highly available; however, any live sessions are not failed over. If a service fails in the middle of user operations, users must reauthenticate and restart whatever operations were interrupted.

Because iManager and Tomcat are already running (Active/Active) on the other nodes, there is no load time for these applications if Novell Cluster Services has to migrate (move) the virtual IP to another node.

There is little benefit in using an Active/Passive cluster because it requires much more configuration and makes you wait the entire load time for each failover. If you really want iManager configured as an Active/Passive clustered resource, you must create a cluster resource that loads and unloads iManager and its dependencies (such as Tomcat). This identical configuration of iManager then needs to be done on all nodes where you want iManager highly available.

10.6 Patching iManager

Patching a server is as easy as installing a module. Any updates for iManager are packaged into an plug-in package (NPM) file. This file is installed like any other plug-in.

- 1 In the Configure view, select *Plug-in Module Installation*.
- 2 Select *Available Novell Plug-in Modules*.
- 3 Select the patch from the download list or Click *Add*.
- 4 Browse to the location of the patch file, then click *OK*.
- 5 Select the patch from the list, then click *Install*.
The server is patched with the latest code.
- 6 Restart Tomcat when the install is finished.

10.7 Performance Tuning

The following are tips for enhancing speed and efficiency.

10.7.1 Using Dynamic Groups with RBS

Disable Dynamic Group support for RBS if you are not using this feature. By default, Dynamic Group support is enabled and, when used, significantly taxes resources because of the extensive searches it conducts.

- 1 In the Configure view, click *iManager Server > Configure iManager*.
- 2 Select the *RBS* tab, then deselect *Enable Dynamic Groups*.

10.7.2 Role Assignments

If you have assigned more than five users to a role within the same scope, consider using Group objects to reduce the number of role assignments and make RBS administration more efficient. By doing so, you have fewer objects to update and you can manage the Group object by adding and removing members.

Also, consider using Dynamic Group objects. You can set up User objects to match a Dynamic Group search criteria.

10.8 iManager AppArmor Profile

Novell Open Enterprise Server 2—Linux includes an AppArmor profile for iManager 2.7. The profile name is `etc.opt.novell.tomcat5.init.d.tomcat5` and is installed at `/etc/apparmor/profiles/extras/iManager`.

The iManager AppArmor profile is not enabled by default. To enable it, copy the profile into the `/etc/apparmor.d` folder.

For more information about AppArmor and AppArmor profiles, see the [Novell AppArmor documentation \(http://www.novell.com/documentation/apparmor/index.html\)](http://www.novell.com/documentation/apparmor/index.html).

iManager Security Issues

A

This section provides information about potential security issues related to iManager, and includes information about the following topics:

- ♦ [Section A.1, “Secure LDAP Certificates,” on page 101](#)
- ♦ [Section A.2, “Self-Signed Certificates,” on page 102](#)
- ♦ [Section A.3, “iManager Authorized Users,” on page 102](#)
- ♦ [Section A.4, “Preventing Username Discovery,” on page 103](#)
- ♦ [Section A.5, “Tomcat Settings,” on page 103](#)
- ♦ [Section A.6, “Encrypted Attributes,” on page 104](#)
- ♦ [Section A.7, “Secure Connections,” on page 104](#)

A.1 Secure LDAP Certificates

iManager can create secure LDAP connections behind the scenes without any user intervention. If the LDAP server’s SSL certificate is updated for any reason (for example, new Organizational CA), iManager should automatically retrieve the new certificate using the authenticated connection and import it into its own keystore database.

If this does not happen correctly, you must delete the private key store that iManager uses, in order to force iManager and Tomcat to re-create the database and reacquire the certificate:

- 1 Shut down Tomcat.
- 2 Delete the `TOMCAT_HOME\webapps\nps\WEB-INF\iMKS` file.
- 3 Restart Tomcat.

For information about restarting Tomcat, see [“Starting and Stopping Tomcat” on page 90](#).

- 4 Open iManager in a browser and log back in to the tree, to automatically reacquire the new certificate and re-create the database store.

Alternately, you can also manually import the required certificate into Tomcat’s JVM default keystore using the keytool certificate management utility available in the JDK*. When creating secure SSL connections, iManager first tries the JVM default keystore, then uses the iManager specific keystore database.

After you have an eDirectory™ certificate saved in DER format, you must import the trusted root certificate into the iManager keystore. To do this, you need a JDK to use keytool. If a JRE was installed with iManager, you must download a JDK to use the keytool.

NOTE: For information about creating a `.der` certificate file, see [Exporting a Trusted Root or Public Key Certificate \(http://www.novell.com/documentation/crt32/crtadmin/data/a2ebopb.html\)](http://www.novell.com/documentation/crt32/crtadmin/data/a2ebopb.html) in the *Novell Certificate Server Admin Guide*. You will want to export the trusted root certificate.

- 1 Open a command window.
- 2 Change to the `\bin` directory where you have installed the JDK.

For example, on a Windows system, you would enter the following command:

```
cd j2sdk1.5.0_11\bin
```

- 3 Import the certificate into the keystore with the keytool, executing the following keytool commands (platform specific):

- ♦ NetWare

```
keytool -import -alias [alias_name] -file  
[full_path]\trustedrootcert.der -keystore  
sys:java\lib\security\cacerts
```

- ♦ Windows

```
keytool -import -alias [alias_name] -file  
[full_path]\trustedrootcert.der -keystore  
[full_path]\jre\lib\security\cacerts
```

- ♦ Linux

```
keytool -import -alias [alias_name] -file [full_path]/  
trustedrootcert.der -keystore [full_path]/jre/lib/security/  
cacerts
```

Replace *alias_name* with a unique name for this certificate and make sure you include the full path to trustedrootcert.der and cacerts.

The last path in the command specifies the keystore location. This varies from system to system because it is based on where iManager is installed. The default location for iManager on a Windows server, for example, is C:\Program Files\Novell\jre\lib\security\cacerts.

- 4 Enter `changeit` for the keystore password.

- 5 Click *Yes* to trust this certificate.

NOTE: This process must be repeated for each eDirectory tree you will be accessing with iManager. If LDAP has been configured to use a certificate not signed by the tree's Organizational CA, you must import that certificate's Trusted Root. This is necessary, for example, if LDAP is configured to use a VeriSign*-signed certificate.

A.2 Self-Signed Certificates

iManager includes a temporary, self-signed certificate that you use when installing iManager on any platform except NetWare. It has an expiration date of one year. For more information, see “[Self-Signed Certificates](#)” in the *iManager 2.7 Installation Guide*.

A.3 iManager Authorized Users

Authorized Users are those that iManager permits to perform its various administrative tasks. For more information about specifying and configuring Authorized Users, see “[Authorized Users](#)” on [page 70](#).

Authorized User data is stored in the `configiman.properties` file, which must be secured to prevent unauthorized modification. To do this, modify the access controls for `configiman.properties` to restrict those users authorized to manually edit the file.

NOTE: Not specifying an Authorized User, which prevents the `configiman.properties` file from being created, or specifying an Authorized User of `AllUsers`, allows any user to install

iManager plug-ins and modify iManager server settings. This is a security risk for server-based iManager environments.

A.4 Preventing Username Discovery

In some installations, the eDirectory server is protected behind a firewall, but the iManager server is open to the outside world to allow management from home or on the road. Access to iManager is controlled with Username, Password, and Treename fields on the login screen. In such installations, it is often desirable to tighten security to avoid revealing any information about the system.

Standard iManager configurations pass through eDirectory messages related to invalid usernames and passwords during iManager authentication. These messages can inadvertently provide too much information to potential crackers. To avoid this, iManager 2.7 includes a configuration option to hide the specific reason for login failure. When enabled, the following error messages are replaced with a generic error message that reads: `Login Failure. Invalid Username or Password.`

- ♦ Invalid Username (-601)
- ♦ Incorrect password (-669)
- ♦ Expired password or disabled account (-220)

To enable this setting, open the *Configure* view and select *iManager Server > Configure iManager*. On the *Authentication* tab, select *Hide specific reason for login failure*. This sets `Authenticate.Form.HideLoginFailReason=true` in iManager's `config.xml` file.

Additionally, iManager 2.7 does not support the asterisk (*) character as a wildcard in the Username field. This prevents unauthorized users from discovering valid usernames. It also prevents possible denial-of-service attacks that attempt to overload the eDirectory server by continually attempting a login using only the wildcard (*), which forces eDirectory to search for and return all matching usernames.

A.5 Tomcat Settings

Because iManager makes use of Tomcat Servlet Container, iManager administrators should be aware of the encryption-related configuration options of those resources as part of their overall security strategy. Of particular interest are cipher suites and trusted certificates, which directly impact the quality of your wire-level encryption. Consider the following rules when configuring your Tomcat environment:

- ♦ Do not use SSL 2.0 cipher suites, which are outdated and not guaranteed to be secure.
- ♦ Do not use the NULL cipher suite in a production environment.
- ♦ Do not use any cipher suite classified as LOW or EXPORT quality, because these are less secure.
- ♦ Regularly review the list of trusted certificates, and limit the list of accepted Certificate Authorities to only those you are actually using

More information for Tomcat is available at the [Tomcat Documentation Web site \(http://tomcat.apache.org/tomcat-4.1-doc/index.html\)](http://tomcat.apache.org/tomcat-4.1-doc/index.html).

NOTE: Because of the way that iManager interprets and uses data, there are no known risks of HTML-based attacks such as cross-site scripting.

A.6 Encrypted Attributes

iManager is able to securely read eDirectory 8.8 encrypted attributes. However, because of the way it determines if an attribute is encrypted, iManager does not securely modify or delete these encrypted attributes. The impact of this, which can result in some wire-level data exposure, can be mitigated through normal network security practices such as the following:

- ♦ Locating all iManager servers behind the firewall
- ♦ Locating iManager servers physically near their associated eDirectory servers
- ♦ Physically securing iManager and eDirectory servers
- ♦ Requiring remote administrators to use a VPN to access iManager and eDirectory servers

A.7 Secure Connections

Although iManager leverages secure HTTP (SSL) for client communications, and secure LDAP connections between iManager and eDirectory servers, iManager does not, with the exception of reading encrypted attributes, utilize secure NCP connections for communications between iManager servers and eDirectory servers.

This is also true for the NCP connection used by Mobile iManager. The impact of this, which can result in some wire-level data exposure, can be mitigated through normal network security practices such as the following:

- ♦ Locating all iManager servers behind the firewall
- ♦ Locating iManager servers physically near their associated eDirectory servers
- ♦ Physically securing iManager and eDirectory servers
- ♦ Requiring remote administrators to use a VPN to access iManager and eDirectory servers

NOTE: Regardless of the wire-level encryption being used, passwords are always encrypted and protected as part of the iManager authentication process.

Novell Plug-in Modules

B

iManager 2.7 ships with the following roles as part of the `base.npm` plug-in. Additional plug-in modules must be downloaded separately.

- ♦ Directory Administration
- ♦ Partitions and Replicas
- ♦ Help Desk
- ♦ Schema
- ♦ Rights
- ♦ Users
- ♦ Groups

The best place to locate and download iManager plug-ins is within iManager on the *Available Novell Plug-in Module* page. Alternately, you can download plug-ins from the [Novell download site \(http://download.novell.com\)](http://download.novell.com). Select iManager as the product in the search criteria.

Additionally, Novell occasionally releases iManager plug-in updates. These updates are available on the [Novell Patches download site \(http://support.novell.com/filefinder/20544/index.html\)](http://support.novell.com/filefinder/20544/index.html).

iManager base plug-ins are only available as part of the complete iManager software download (for example, eDirectory™ administrative plug-ins). Unless there are specific updates to these plug-ins, they can only be downloaded and installed with the entire iManager product.

For more information about downloading iManager plug-ins, see “**Downloading and Installing Plug-Ins During Installation**” in the *iManager 2.7 Install Guide*.

NOTE: By default, the plug-in modules are not replicated between iManager servers. We recommend that you install the plug-in modules you want on each iManager server.
