

Novell iManager

2.5

March 15, 2006

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.

You may not use, export, or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

Copyright © 2004-2005 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 at <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 online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

ConsoleOne is a registered trademark of Novell, Inc. , in the United States and other countries.

DirXML is a registered trademark of Novell, Inc. , in the United States and other countries.

eDirectory is a trademark of Novell, Inc.

exteNd is a trademark of Novell, Inc.

exteNd Director is a trademark of Novell, Inc.

NetWare is a registered trademark of Novell, Inc. , in the United States and other countries.

NMAS is a trademark of Novell, Inc.

Novell is a registered trademark of Novell, Inc. , in the United States and other countries.

Novell Directory Services and NDS are registered trademarks of Novell, Inc. in the United States and other countries.

Nterprise is a trademark of Novell, Inc.

SUSE is a registered trademark of SUSE LINUX AG, a Novell company.

Novell Distributed Print Services is a tradement of Novell, Inc. , in the United States and other countries.

NDPS is a registered trademark of Novell, Inc. , in the United States and other countries.

Nsure is a registered trademark of Novell, Inc. , in the United States and other countries.

Novell Certificate Server is a trademark of Novell, Inc. , in the United States and other countries.

Third-Party Materials

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

About This Guide

This guide describes how to administer Novell® iManager 2.5. It is intended for network administrators and contains the following sections:

- [Chapter 1, “Overview,” on page 7](#)
- [Chapter 2, “Accessing iManager,” on page 9](#)
- [Chapter 3, “Navigating the iManager Interface,” on page 13](#)
- [Chapter 4, “Roles and Tasks,” on page 17](#)
- [Chapter 5, “Configuring for iManager Auditing,” on page 37](#)
- [Chapter 6, “Configuring and Customizing iManager,” on page 39](#)
- [Chapter 7, “Preferences,” on page 57](#)
- [Chapter 8, “Troubleshooting,” on page 59](#)
- [Chapter 9, “Best Practices and Common Questions,” on page 65](#)

Additional Documentation

Documentation for all Novell software products is available at www.novell.com/documentation (<http://www.novell.com/documentation>).

For documentation on installing and using NetWare®, see the [Novell NetWare documentation Web site](http://www.novell.com/documentation/NetWare.html) (<http://www.novell.com/documentation/NetWare.html>).

For documentation on installing and running eDirectory™, see the [Novell eDirectory documentation Web site](http://www.novell.com/documentation/eDirectory.html) (<http://www.novell.com/documentation/eDirectory.html>).

For additional information on current iManager 2.5 issues, please see TID #10097429, [Novell iManager 2.5 Readme Addendum](http://support.novell.com/cgi-bin/search/searchtid.cgi?/10097429.htm) (<http://support.novell.com/cgi-bin/search/searchtid.cgi?/10097429.htm>).

For support documentation, see <http://support.novell.com> (<http://support.novell.com>).

For other documentation resources, see [Section 1.2, “Additional Resources,” on page 7](#).

Documentation Updates

For the latest iManager documentation, see the [Novell documentation Web site](http://www.novell.com/documentation) (<http://www.novell.com/documentation>).

Documentation Conventions

In this documentation, a greater-than symbol (>) is used to separate actions within a step and items within 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

1.1 What's New in Version 2.5

Novell iManager 2.5 contains the following new features:

- Improved installation programs
- Enhanced group management capabilities
- Backward compatibility with most iManager 2.0.x plug-ins
- Enhanced Role-Based Services (RBS) management and reporting
- Improved interface customization options
- Mobile iManager software, which allows you to run iManager locally on a Linux* or Microsoft* Windows* workstation

1.2 Additional Resources

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

- Apache HTTP server (<http://httpd.apache.org>)
- Tomcat servlet container (<http://jakarta.apache.org/tomcat>)
- 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/coolsolutions/nds>)

Accessing iManager

2

Novell® iManager is accessed via a Web browser. This section includes the following topics:

- Section 2.1, “Using a Supported Web Browser,” on page 9
- Section 2.2, “Accessing iManager,” on page 9
- Section 2.3, “Accessing iManager with a Screen Reader and Other Accessibility Options,” on page 10
- Section 2.4, “Access Modes,” on page 10
- Section 2.5, “Authenticating,” on page 11
- Section 2.6, “iManager Session Timeouts,” on page 11

2.1 Using a Supported Web Browser

For iManager access and complete use of all its features, you must use a computer running one of the following Web browsers:

- Microsoft Internet Explorer 6.0 SP1
- Mozilla* 1.7
- Mozilla Firefox* 1.0

IMPORTANT: 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 those listed above.

2.2 Accessing iManager

To access Novell iManager:

- 1 Enter the following in the address (URL) field from a supported Web browser:

```
http://server_IP_address/nps/iManager.html
```

For example:

```
http://127.0.0.1/nps/iManager.html
```

NOTE: You might be redirected to an https secure page, depending on your platform.

- 2 Log in using your username and password.

You will have access only to those features you have rights to. To have full access to all Novell iManager features, you must log in as Supervisor of the tree.

2.3 Accessing iManager with a Screen Reader and Other Accessibility Options

iManager includes a simple display that can be effectively used with screen readers in Internet Explorer on a Windows* platform (client side).

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

```
http://server_IP_address/nps/Simple.html
```

For example:

```
http://127.0.0.1/nps/Simple.html
```

- 2 Log in using your username, context, password, and eDirectory™ tree name.

You will have access only to those features you have rights to. To have full access to all Novell iManager features, you must log in as Supervisor of the tree.

Complete accessibility statements are available on the [Novell Web site \(http://www.novell.com/accessibility\)](http://www.novell.com/accessibility).

2.4 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 in the upper left corner of the iManager interface.

- 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 in *<tomcat location>\webapps\nps\WEB-INF* which forces Unrestricted Access, even if Role Based Services is installed. Add the following setting to config.xml and restart Tomcat:

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

- 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 rights have not been assigned. Role-Based Services must be installed in order to use this mode.

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

2.5 Authenticating

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. If you use the tree name to log in, you do not have to specify a port. (Example: 127.0.0.1: 1080)

2.5.1 The Tree Name Field

Possible values for the tree name field are: Tree name, Server IP Address, and Server DNS name.

2.5.2 Single Sign-on

Single Sign-on functionality (including Forward authentication, OLAC, and Form Fill) is not compatible with iManager 2.5. iManager 2.5 requires a username, password, and tree name for login, so Single Sign-on using Forward authentication or OLAC will not work. Form Fill also fails because the Exit button in the iManager toolbar directs you back to the initial login form. When FormFill is active, you are simply logged back in to iManager.

2.5.3 Logging into a Server without a Replica

You can log in to a server without a replica if you have previously logged in to the tree using the tree name, or if you have logged in to the tree using a server that contains a replica.

2.5.4 Unsuccessful Authentication

Login failures occur for a variety of reasons. [Authentication Error Messages](#) are addressed in the Troubleshooting chapter.

2.6 iManager Session Timeouts

iManager session timeouts are controlled by a timeout setting in the web.xml file located in webapps/nps/WEB-INF/. Remove the comment tags to change the timeout from the default of 30 minutes.

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


Navigating the iManager Interface

3

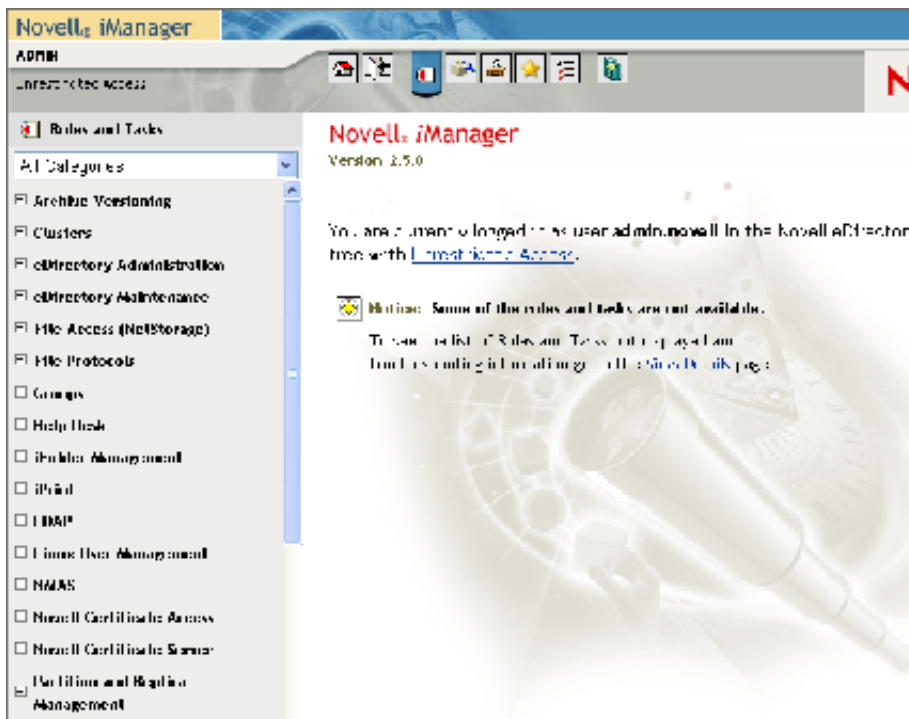
This section describes how to navigate through the Novell® iManager 2.5 interface.

- Section 3.1, “iManager Interface,” on page 13
- Section 3.2, “Special Characters,” on page 14
- Section 3.3, “Using the Object Selector,” on page 15
- Section 3.4, “Enable Pop-ups,” on page 15

3.1 iManager Interface




Use only the buttons within the interface when you are navigating in iManager. The Web browser's toolbar buttons (Back, Next, etc.) are not supported.




Figure 3-1 By default, the iManager Interface displays Roles and Tasks



3.1.1 Views

iManager 2.5 has several views that you access using the icons at the top of the iManager interface:

-  Roles and Tasks: contains all the tasks you are authorized to perform
-  View Objects: contains browsing and searching functionality to find objects
-  Configure: contains Role-Based Services, iManager Server, Object Creation List, Module Installation, E-mail Notification, and Views, all of which you can configure as you want

-  Favorites: displays your most frequent tasks, selected from the Preferences > Favorites page
-  Preferences: Set 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: Applicable information related to the page you are on appears when you select this icon

Roles and Tasks is the default view. For information on how to change the default view, see [Chapter 6, “Configuring and Customizing iManager,” on page 39.](#)

3.1.2 Contents Panel

The Contents Panel displays a navigation pane. Its contents vary, depending on which view you have selected.

New in iManager 2.5 is the Category selector, which provides groups of roles and tasks specific to a particular function. Categories include the following:

- All Categories
- Authentication & Passwords
- Collaboration
- Directory
- File Management
- Identity Manager
- Infrastructure
- Install & Upgrade
- Network
- Nsure Audit
- Printing
- Security
- Servers
- Software Licenses & Network Usage
- Users and Groups

Tasks under categories are listed in order of probable use.

3.2 Special Characters

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

NDAP (NDS):

- period (.)
- equal sign (=)
- plus (+)

- backslash (\)

LDAP:

- DNs: , = + \ @; < >
- Leading #
- Leading or trailing spaces

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

3.3 Using the Object Selector

Follow these guidelines when using the iManager search feature, Object Selector:

1. In dotted NDS[®] names, you must escape the following characters with a backslash (\):
 - period (.)
 - equal (=)
 - plus (+)
 - backslash (\)
2. You don't need escape characters in most values, but you do need them when the name is a Distinguished Name or R Distinguished Name.
3. In a search filter, you must escape these characters with a backslash:
 - asterisk (*)
 - backslash (\)

For example:

To search for all objects containing a period, the search filter = *.*

To search for all objects containing a plus the search filter = *+*

However, to search for all objects containing a backslash, the search filter = **

3.4 Enable Pop-ups

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

The Roles and Tasks icon displays all of the roles and tasks that you have set up; some are part of iManager and others are plug-ins. This chapter describes only those roles and tasks that are intrinsic to iManager.

- [Section 4.1, “eDirectory Administration,” on page 17](#)
- [Section 4.3, “Groups,” on page 21](#)
- [Section 4.4, “Help Desk,” on page 23](#)
- [Section 4.5, “Partitions and Replicas,” on page 24](#)
- [Section 4.6, “Passwords,” on page 28](#)
- [Section 4.7, “Rights,” on page 31](#)
- [Section 4.8, “Schema,” on page 32](#)
- [Section 4.9, “Users,” on page 35](#)

4.1 eDirectory Administration

eDirectory™ administration involves the management of objects in your directory tree. You can create, edit, and organize objects. You can also set up user accounts and assign rights, grant equivalence, and block inheritance. When you configure Role-Based Services, you can define administrator roles for specific administrative applications through the Role-Based Services object.

4.1.1 Copy 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, select *eDirectory Administration > Copy Object*.
- 2 In the Object to Copy From field, type the name and context of the object or use the search feature 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 the *Copy ACL Rights* check box if you want to copy access control list rights to this object. This step might take additional processing time, depending on your system and networking environment.

4.1.2 Create Object

- 1 In Roles and Tasks, select *eDirectory Administration > Create Object*.
- 2 Select the object class from the list that appears and click *OK*.

- 3 Enter the requested information that appears according to the object class you selected, and click *OK*.
- 4 A confirmation message appears: “The Create Object request succeeded.” Click *OK*, *Repeat Task*, or *Modify*.

4.1.3 Delete Object

- 1 In Roles and Tasks, select *eDirectory Administration > Delete Object*.
- 2 Type the name and context of the object, or use the search feature to find it, and click *OK*.
- 3 A confirmation message appears: The Delete Object request succeeded.

4.1.4 Modify Object

- 1 In Roles and Tasks, select *eDirectory Administration > Modify Object*.
- 2 Type the name and context of the object, or use the search feature to find it, and click *OK*. The Modify Objects screen appears, displaying a set of tabs which are specific to the object you selected. Tabs and their features are described below this task.
- 3 Complete the modification based on the tabs you select and click *OK*.

General

The General tab displays the Identification page.

- 1 Complete the form with the following information:
 - *Other Name*
 - *Owner*
 - *Location*
 - *Department*
 - *Organization*
 - *Description*Modify your description using the add, delete, and edit features.

- 2 Click *OK*.

The See Also page displays the search feature (Object Selector) to help you locate the object to modify.

The Other page displays the Valued Attributes and Unvalued Attributes list boxes. You can move, edit, or delete attributes for the object.

Security

The Security tab displays one or both of the following options, according to the object selected. The following attributes are used in rights calculation for eDirectory.

- *Security Equal To Me*

This attribute specifies other objects that are security equivalent to this object.
- *Security Equal To*

This attribute specifies objects that this object is security equivalent to.

Restrictions

Use the *Limit Grace Login* option to force users to change their passwords after a number of logins using an expired password.

Set the maximum number of concurrent connections a user is allowed.

Dynamic

Use the Member Query page to specify the search criteria when looking for members of a Dynamic Group object.

- 1 Select the *Dynamic Group* check box to make a static group dynamic.

After a static group becomes dynamic, it can be converted back to static status by clearing the Dynamic Group check box.

- 2 Complete the *Start Search at* (Base dn) text box with the location that you are searching from.
- 3 Specify the search scope. If you do not specify, the base scope is assumed.
 - *Search Base DN*, searches only the base object.
 - *Search One Level*, searches the direct subordinates of the base object, but the base object itself is not searched.
 - *Search Sub Containers*, searches the base object and all objects in the subtree below it.
- 4 Choose whether the search for Dynamic Members should involve multiple servers or only the server containing the Dynamic Group object.
 - *Yes*, the server communicates with other servers while searching for Dynamic Members.
 - *No*, the search for Dynamic Members returns only local results.
- 5 Use the two Search Filter icons to refine the search and manually edit the string if you know the syntax.
- 6 Click *Apply* to update the Query Results.

Use the Settings page to establish an identity object and other object-related search parameters.

- 1 Select the Identity Object. This is the object that the LDAP server uses to log in to the tree as, to query.
- 2 Leave the *Time Out* blank unless you give iManager a reasonable amount of time to load the objects it finds.

If you do not allow enough time for iManager to load and it times out, the object becomes unusable. You must delete the object and start over.
- 3 Select *Allow Duplicates* to reduce the load on the server while listing dynamic group members. Unless you fully understand the implications of this feature, leave it unchecked.
- 4 Leave *Allow Unknowns* unselected unless you fully understand the implications of this feature. Allow Unknowns determines the inclusion or exclusion of members in the dynamic group when the membership cannot be correctly determined.

RPM

This configuration task applies only to NDPS[®] printers. iPrint printers are not affected.

- 1 Select *Do Not Update Workstations* if Remote Printer Management is disabled and printers are not installed or removed from workstations.
- 2 Select *Allow Only Specified Printers to Reside on Workstations* to allow only the printers specified in Remote Printer Management.
All other NDPS printers on the workstation are removed. This does not remove any iPrint printers.
- 3 Select *Show the Results Window on Workstations* to display a window on the workstation that shows the printers that were installed and removed.
- 4 Select the printers to install.
- 5 Set a default printer.
- 6 Indicate printers to be removed, if, any, and click *OK*, or *Apply*.

4.1.5 Move Object

- 1 In Roles and Tasks, select *eDirectory Administration > Move Object*.
- 2 Type the name and context of the object, or use the search feature (Object Selector) to find it, and click *OK*.
- 3 In the *Move To* field, select the container you want to move the object to.
- 4 Select *Create an Alias in Place of Moved Object* if you want to create an alias in an old location for each object being moved.
- 5 Click *OK*. A confirmation message appears: `The Move Object request succeeded.`

4.1.6 Rename Object

- 1 In Roles and Tasks, select *eDirectory Administration > Rename Object*.
- 2 Type the name and context of the object, or use the search feature to find it.
- 3 Type only the name of the new object; do not include a context.
- 4 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 General Identification tab for that object.
- 5 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 reflect the new name.
- 6 Click *OK*. A confirmation message appears: `The Rename Object request succeeded.`

4.2 eDirectory Maintenance

4.2.1 Repair Sync

- 1 In Roles and Tasks, select *Partitions and Replicas > Repair Sync*.
- 2 Use the Sync Repair wizard to do the following tasks:
 - Synchronize the selected replica on the current server
 - Report the synchronization status on the current server
 - Report the synchronization status on all servers
 - Perform a time synchronization
 - Schedule an immediate synchronization

For more information, see [Performing Synchronization Operations \(http://www.novell.com/documentation/edir873/edir873/data/aew13qs.html#aew13qs\)](http://www.novell.com/documentation/edir873/edir873/data/aew13qs.html#aew13qs) in the *eDirectory Administration Guide*.

4.2.2 Replica Repair

Repairing a replica consists of checking each object in the replica for consistency with the schema, and checking each attribute of the object for consistency with the schema and the data, according to the syntax of the attribute. Other internal data structures associated with the replica are also checked.

- 1 In Roles and Tasks, select *Partitions and Replicas > Replica Repair*.
- 2 Use the Replica Repair wizard to do any of the following tasks:
 - Repair all replicas
 - Repair a selected replica
 - Repair time stamps
 - Designate this server as the new master replica
 - Destroy a selected replica

For more information, see [Repairing Replicas \(http://www.novell.com/documentation/edir873/edir873/data/aew0b5f.html#aew0b5f\)](http://www.novell.com/documentation/edir873/edir873/data/aew0b5f.html#aew0b5f) in the *eDirectory Administration Guide*.

4.2.3 Replica Ring Repair

The Replica Ring Repair wizard lets you repair all or selected replica rings, send all objects to every server in the ring, receive all objects from the master to the selected replica, and remove the current server from the replica ring, if necessary.

To repair a replica ring, check the replica ring information on each server that contains a replica and validate the remote ID information. For more information, see [Replica Ring Repair \(http://www.novell.com/documentation/edir873/edir873/data/af0lnik.html#af0lnik\)](http://www.novell.com/documentation/edir873/edir873/data/af0lnik.html#af0lnik) in the *eDirectory Administration Guide*.

4.3 Groups

Any user who creates a group automatically becomes the owner of the group. Groups are either static or dynamic, depending on the option that you select.

4.3.1 Create Group

If you select the *Dynamic Group* check box on the Create Group page, the group is dynamic, of the class `dynamicGroup`.

If you create a Group on this page and leave the *Dynamic Group* check box blank, your group is static, of the class `group`. You can manually edit this group.

If you create a group initially as a static group on this page, and later make it dynamic (*Modify Group > Dynamic* tab > *Dynamic Group* check box), iManager extends the object to belong to the class `dynamicGroupAux`.

NOTE: If you take the third option and if you are using RBS, you must enable `dynamicGroupAux` class support. Select *Configure > iManager Server > Configure iManager > RBS > Dynamic Group Search Type*. Select *DynamicGroupObjects&AuxClasses* from the drop-down menu and click *Save*.

4.3.2 Delete Group

Specify the objects to delete, from *Select a Single Object*, *Select Multiple Objects*, *Simple Selection*, or *Advanced Selection*, then click *OK*.

4.3.3 Modify Group

Use the Settings tab to establish Identity objects and other object-related search parameters. In order to perform the search, the server uses a specific identity so that the results will always be consistent. The Identity object must have authentication credentials so the server can authenticate as the Identity object. The Identity object must have a password set.

For example, if you set the Filter to `(&(title=manager))`, the [Public] identity might not be able to read or compare the title or many other attributes. The Identity object must have sufficient rights to the Base dn level and below to determine dynamic group membership.

NOTE: If you create a Dynamic Group on this page, and if you are using RBS, you must enable `dynamicGroupAux` class support. Select *Configure > iManager Server > Configure iManager > RBS > Dynamic Group Search Type*. Select *DynamicGroupPbjects&AuxClasses* from the drop-down menu and click *Save*.

Use the Member Query page for specifying the search criteria when you are looking for members of a group.

- *Start Search At:* The search base is the location that you are searching from (the starting point).
- *Search Scope:* The search scope defines the depth and breadth of the search.
- *Search Multiple Servers:* Use this option to indicate whether the search for Dynamic Members should span multiple servers, or should be done only on the server containing the Dynamic Group object. If Search Multiple Servers is set to Yes, then the server, if necessary, communicates with other servers while searching for Dynamic Members. If Search Multiple Servers is set to No, then the search for Dynamic Members will not chain across other servers,

and return only local results. Use this extension with care because it can result in lengthy operations.

- *Search Filter*: The Search filter has two buttons, one for advanced search criteria and the other for editing. For more information on search criteria, go to: [The String Representation of LDAP Search Filters \(http://ietf.org/rfc/rfc2254.txt\)](http://ietf.org/rfc/rfc2254.txt).
- *Query Results*: Click *Apply* to update results.

4.3.4 Modify Members of Group

This feature allows spontaneous modification of members of a specified group.

4.3.5 View My Groups

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

4.4 Help Desk

Help Desk is a limited role that permits a small number of user-related tasks. The user who owns this role can clear a user lockout, create a user, and set a new password.

4.4.1 Clear 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 To clear the lockout, type the username and click *OK*.

4.4.2 Create User

The Create User task also appears from *Users > Create User*.

- 1 In Roles and Tasks, select *Help Desk > Create User*.
- 2 Complete the form with the following information:
 - *Username* (required)
 - *First Name*
 - *Last Name* (required)
 - *Full Name*
 - *Context* (required)
 - *Password* (twice)

IMPORTANT: Failure to enter a password will allow the user to login without a password.

- 3 Select *Simple Password* according to your configuration.

NOTE: Simple Password is required for native file access for Windows* and Macintosh* users. It is not required when Universal Password is enabled.

- 4 Select to *Copy from template or user object*, according to your configuration.

NOTE: iManager prevents users from receiving the same rights as the administrator. They can use the same directory as the Administrator, but iMan sets up different rights for them.

- 5 If you select to *Create home directory*, enter the volume and path.

NOTE: If you enter an existing path, a user directory will be created. If you enter a path that doesn't exist, nothing happens; no error message appears.

- 6 Fill in the remainder of the form with appropriate information and click *OK*.

4.4.3 Set Password

- 1 In Roles and Tasks, select *Help Desk > Set Password*.
- 2 Type the context of the user object, or use the search feature to find it.
- 3 Type the new password twice.
- 4 Select *Simple Password*.

NOTE: Simple Password is required for native file access for Windows and Macintosh users. It is not required when Universal Password is enabled.

4.5 Partitions and Replicas

Partitions are logical divisions of the Novell® eDirectory database that form a distinct unit of data in the eDirectory tree for administrators to store and replicate eDirectory information. Each partition consists of a Container object, all objects contained in it, and information about those objects. Partitions do not include any information about the file system or the directories and files contained there.

Instead of storing a copy of the entire eDirectory database on each server, you can make a copy of the eDirectory partition and store it on many servers across the network. Each copy of the partition is known as a replica. You can create any number of replicas for each eDirectory partition and store them on any server. There are different types of replicas:

- Master, read/write, and read-only

These contain all objects and attributes for a particular partition.

- Subordinate references

These are used for tree connectivity.

- Filtered replicas

Filtered replicas contain a subset of information from the entire partition, consisting of only the desired classes and attributes which are defined by the server's replication filter. This filter is used to identify the classes and attributes allowed to pass during inbound synchronization and local changes.

Filtered replicas allow administrators to create sparse and fractional replicas.

- Sparse replicas contain only the object classes that you specify
- Fractional replicas contain only the attributes you specify

The functionality of filtered replicas enables fast response when the data stored in eDirectory is procured by applications. Filtered replicas also allow more replicas to be stored on a single server.

- Read/write filtered replicas

These replicas allow local modifications to classes and attributes that are a subset of the server's replication filter. However, these replicas can create objects only if all mandatory attributes for the class are within the replication filter.

- Read-only filtered replicas

These replicas do not allow local modifications.

For more information, see [Managing Partitions and Replicas \(http://www.novell.com/documentation/edir873/index.html?page=/documentation/edir873/edir873/data/a2iiiiik.html\)](http://www.novell.com/documentation/edir873/index.html?page=/documentation/edir873/edir873/data/a2iiiiik.html) in the *eDirectory Administration Guide*.

4.5.1 Create Partition

When you create partitions, you make logical divisions of your tree. These divisions can be replicated and distributed among different eDirectory servers in your network. When you create a new partition, you split the parent partition and then have two partitions. The new partition becomes a child partition. 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 Type the name and context of the container or use the search feature to find it, and click *OK*.
- 3 After a few seconds, a confirmation message appears: "Complete: Create Partition."

4.5.2 Merge Partition

When you merge a partition with its parent partition, the chosen partition and its replicas combine with the parent partition. You do not delete partitions; you only merge and create partitions to define how the directory tree is split into logical divisions.

There are several reasons to merge a partition with its parent:

- The directory information in the two partitions is closely related.
- You want to delete a subordinate partition, but you don't want to delete the objects in it.
- You're going to delete the objects in the partition.
- You want to delete all replicas of the partition. (Merging a partition with its parent is the only way to delete the partition's master replica.)
- After moving a container (which must be a partition root with no subordinate partitions), you don't want the container to be a partition anymore.

- You experience changes in your company organization, so you want to redesign your directory tree by changing the partition structure.

Before merging a partition, check the partition synchronization of both partitions and fix any errors before proceeding. By fixing the errors, you can isolate problems in the directory and avoid propagating the errors or creating new ones. Make sure that all servers which have replicas (including subordinate references) of the partition you want to merge, are up before attempting to merge a partition. If a server is down, eDirectory won't be able to read the server's replicas and won't be able to complete the operation.

If you receive errors in the process of merging a partition, resolve the errors as they appear. Don't try to fix the error by continuing to perform operations; doing so only results in more errors.

To merge a child partition with its parent partition:

- 1 In Roles and Tasks, select *Partitions and Replicas > Merge Partition*.
- 2 Type the name and context of the partition or use the search feature to find it, and click *OK*.
- 3 After a few seconds, a confirmation message appears: "Complete: Merge Partition."

4.5.3 Move Partition

Moving a partition lets you move a subtree in your directory tree. You can move a partition root object (which is a Container object) only if it has no subordinate partitions.

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 current tree, because the root's containment rules allow Locality, Country, or Organization, but not Organizational Unit.

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.

- 1 In Roles and Tasks, select *Partitions and Replicas > Move Partition*.
- 2 Type the name and context of the object or use the search feature to find it.
- 3 Type the location you want to move the partition to in the Move to text box.
- 4 Select the *Create an alias in place of moved object* check box and click *OK*.

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.

The Alias object that is created has the same common name as the moved container and references the new complete name of the moved container.

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.

4.5.4 Replica View

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

To view information about a replica:

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

A table appears listing the replica Partition, Type, Filter, and State. The following list describes the replica states that you might see in iManager:

- *On*: Currently not undergoing any partition or replication operations
- *New*: Being added as a new replica on the server
- *Dying*: Being deleted from the server
- *Dead*: Done being deleted from the server
- *Master Start*: Being changed to a master replica
- *Master Done*: Done being changed to a master replica
- *Change Type*: Being changed to a different type of replica
- *Locked*: Locked in preparation for a partition move or repair operation
- *Transition Move*: Starting in to a partition move operation
- *Move*: In the midst of a partition move operation
- *Transition Split*: Starting in to a partition split operation (creation of a child partition)
- *Split*: In the midst of a partition split operation (creation of a child partition)
- *Join*: Being merged into its parent partition
- *Transition On*: About to return to an On state
- *Unknown*: In a state not known to iManager

For more information, see [Replica View \(http://www.novell.com/documentation/edir873/edir873/data/fbgeaaeg.html#fbgeaaeg\)](http://www.novell.com/documentation/edir873/edir873/data/fbgeaaeg.html#fbgeaaeg) in the *eDirectory Administration Guide*.

4.5.5 View Partition Information

Viewing information about a [partition \(http://www.novell.com/documentation/edir873/edir873/data/fbgeaaeg.html#a2iijy\)](http://www.novell.com/documentation/edir873/edir873/data/fbgeaaeg.html#a2iijy) (from the *eDirectory Administration Guide*) displays its synchronization information: last successful synchronization and last attempted synchronization.

- 1 In Roles and Tasks, select *Partitions and Replicas > View Partition Information*.
- 2 Type the name and context of the partition object, or use the search feature to find it, and click *OK*.

4.5.6 Filtered Replica Wizard

Administrators generally use the filtered replica capability to create an eDirectory server that holds a set of filtered replicas that contain only specific objects and attributes that they want synchronized. 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 Type the name and context of the server on which you want to configure a filtered replica, or use the search feature to find it, and click *Next*.
- 3 Click *Define the Filter Set* to define the classes and attributes for a filter set on the selected server.
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 *Next*, then click *Finish*.

For more information, see [Setting Up and Managing Filtered Replicas \(http://www.novell.com/documentation/edir873/edir873/data/a5lhibw.html\)](http://www.novell.com/documentation/edir873/edir873/data/a5lhibw.html) in the *eDirectory Administration Guide*.

4.6 Passwords

Password management is a core eDirectory feature that can be enhanced by adding DirXML/Identity Manager.

4.6.1 Challenge Sets

A Challenge Set is a set of questions that can be answered by a user to prove his or her identity, instead of using a password.

When you create a Password Policy, you can enable Forgotten Password self-service so that users can get help without calling the help desk. To make self-service more secure, you can create a Challenge Set and require that users answer the Challenge Set questions before obtaining password help.

To create a Challenge Set:

- 1 In Roles and Tasks, select *Passwords > Challenge Sets*.
- 2 Click *New*.
- 3 Type a *Challenge Set Name*.
- 4 Select *Required Questions and/or Random Questions*, then click *OK*.

IMPORTANT: You can manage Challenge Sets and Password Policies from iManager 2.5, but the forgotten password self-provisioning portal where users go if they have forgotten their passwords is not supported on iManager 2.5. Users must access an iManager 2.0.2 server to access the self-provisioning portal.

4.6.2 Password Policies

Make sure you have completed the steps in Prerequisites for Using Password Policies. The information there prepares you to use all the features of Password Policies.

- 1 In Roles and Tasks, select *Passwords > Password Policies*.
- 2 Click *New* to create a new Password Policy.

- 3 Follow the steps in the wizard to create Advanced Password Rules, Universal Password Configuration Options, and Forgotten Password selections for the policy.

See the online help for information about each step, as well as the information in [Managing Passwords by Using Password Policies \(http://www.novell.com/documentation/dirxml20/admin/data/ampxjj0.html#ampxjj0\)](http://www.novell.com/documentation/dirxml20/admin/data/ampxjj0.html#ampxjj0) and in [Password Self-Service \(http://www.novell.com/documentation/dirxml20/admin/data/bqf5d1r.html#bqf5d1r\)](http://www.novell.com/documentation/dirxml20/admin/data/bqf5d1r.html#bqf5d1r) in the *eDirectory Deployment Guide*.

4.6.3 Policy Assignments

You can assign a Password Policy to users in eDirectory by assigning the policy to the whole tree (using the Login Policy object), specific partitions or containers, or specific users. To simplify administration, assign a default policy to the whole tree, and assign any other policies you use as high up in the tree as possible.

A policy is not in effect until you assign it to one or more objects. You can assign a password policy to the following objects:

- Login Policy object

We recommend that you create a default Password Policy for all users in the tree, which you do by creating a policy and assigning it to the Login Policy object. The Login Policy object is located in the Security container just below the root of the tree.

- A container that is a partition root

If you assign a policy to a container that is the root of a partition, the policy assignment is inherited by all users in that partition, including users in subcontainers. To determine whether a container is a partition root, browse for the container and note whether a partition icon is displayed beside it.

- A specific user

Only one policy is effective for a user at a time. Novell Modular Authentication Services (NMAS) determines which policy is effective for a user by looking for policies in the following order, and applying the first one it finds.

1. Specific user assignment: If a password policy has been assigned specifically to the user, that policy is applied.
2. Container: If the user has no specific assignment, NMAS applies the policy that is assigned to the container which holds the user.
3. Partition root container: If no policy is assigned to the user or to the container directly above the user, the policy assigned to the partition root container is applied.
4. Login Policy object: If no policy is assigned to the user or other containers, the policy assigned to the Login Policy object is applied. It is the default policy for all users in the tree.

NOTE: Special Password Policies are automatically created for Driver Set objects.

4.6.4 Set Universal Password

Universal Password is the new password capability in eDirectory 8.7.3. You must enable Universal Password for your users if you want to use Advanced Password Rules, Password Synchronization, and many of the Forgotten Password features. To allow you or help desk personnel to set the

Universal Password for a user, an iManager plug-in is provided. This plug-in displays the Advanced Password Rules from the users' Password Policy, to help you or a help desk user create a compliant Universal Password.

Universal Password allows or provides:

- One password for all access to eDirectory
- Use of extended characters in password
- Advanced password policy enforcement
- Synchronization of passwords from eDirectory to other systems

Universal Password is managed by the Secure Password Manager (SPM), a component of the NMAS™ module (nmas.nlm on NetWare). To set it:

- 1 In Roles and Tasks, select *Passwords > Set Universal Password*.
- 2 Specify a user for the Universal Password change text box and click *OK*.
The current setting for the user should read Disabled.
- 3 Select *Enable*.
- 4 Click *OK*.

IMPORTANT: When you enable Universal Password on a container, it is enabled on all existing subcontainers as well. If you enable Universal Password at the Tree level, all subcontainers you create after enabling Universal Password will be enabled for Universal Password. However, if you enable Universal Password on a container below the Tree level, such as an Organization (O) or an Organizational Unit (OU), and then create a new subcontainer, you must enable Universal Password on that subcontainer. It is not automatically enabled.

4.6.5 E-mail Server Options

E-mail Server Options lets you specify the e-mail server settings.

- 1 In Roles and Tasks, select *Passwords > E-mail Server Options*.
- 2 Type the Host Name and From settings for your e-mail notification server.
- 3 Select *Authenticate to Server Using Credentials* and supply the credentials.
- 4 Click *OK*.

4.6.6 Edit E-mail Templates

You can customize these templates with your own text. The name of the template indicates what it is used for.

- 1 In Roles and Tasks, select *Passwords > Edit E-mail Templates*.

A list of templates appears, including the following:

- *Your request for your password hint*
- *Your request for your current password*
- *Notice of Password Reset Failure*
- *Notice of Password Set Failure*

- *Notice of Password Synchronization Failure*

- 2 Edit the templates. If you want to add any replacement tags, some additional tasks might be required. Follow the instructions in [Adding Your Own Replacement Tags to E-Mail Notification Templates \(http://www.novell.com/documentation/dirxml20/admin/data/bnpdcy4.html#bnwjtmu\)](http://www.novell.com/documentation/dirxml20/admin/data/bnpdcy4.html#bnwjtmu) in the *eDirectory Administration Guide*.
- 3 Restart DirXML drivers that need to be updated with the changes.

The driver reads the templates and SMTP server information only at startup time.

For more information see [Setting Up E-mail Templates \(http://www.novell.com/documentation/dirxml20/admin/data/bnpdcy4.html#anlaiv8\)](http://www.novell.com/documentation/dirxml20/admin/data/bnpdcy4.html#anlaiv8) in the *eDirectory Administration Guide*.

4.7 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. Some of the default assignments are as follows:

- User Admin has the Supervisor right to the top of the tree, giving the Admin complete control over the entire directory. Admin also has the Supervisor right to the NetWare™ Server object, giving complete control over any volumes on that server.
- [Public] has the Browse right to the top of the tree, giving all users the right to view any objects in the tree.
- Objects created through an upgrade process such as a NetWare migration, printing upgrade, or Windows NT* user migration receive trustee assignments appropriate for most situations.

The assignment of rights involves a trustee and a target object. The trustee represents the user or set of users that are receiving the authority. The target represents those network resources the users have authority over.

4.7.1 Modify Inherited Rights Filter

In eDirectory, rights assignments on containers can be inheritable or non-inheritable. In the NetWare file system, all rights assignments on folders are inheritable. In both eDirectory and NetWare, you can block such inheritance on individual subordinate items so that the rights aren't effective on those items, no matter who the trustee is. One exception is that the Supervisor right can't be blocked in the NetWare file system.

To block rights from flowing down the eDirectory tree:

- 1 In Roles and Tasks, select *Rights > Modify Inherited Rights Filter*.
- 2 Specify the name and context of the object whose inherited rights filter you want to modify, 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.
- 4 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, and click *OK*.

NOTE: These filters won't block rights that are explicitly granted a trustee on this object, because such rights aren't inherited.

4.7.2 Modify Trustees

To modify trustee rights:

- 1 In Roles and Tasks, select *Rights > Modify Trustees*.
- 2 Specify the name of the trustee whose rights you want to view, then click *OK*.
- 3 Click *Assigned Rights* to view and change.
- 4 Click *Add Trustee* or *Delete Trustee*, according to your task.
- 5 Click *OK*.

4.7.3 Rights to Other Objects

Fill in the *Trustee Name* and *Context to Search from* fields. iManager searches for the Trustee Name within the scope of the container defined in the Context field.

4.7.4 View Effective Rights

Users can receive rights in a number of ways, such as explicit trustee assignments, inheritance, and security equivalence. Rights can also be limited by inherited rights filters and changed or revoked by lower trustee assignments. The net result of all these actions—the rights a user can employ—are called effective rights.

A user's effective rights to an object are calculated each time the user attempts an action. To view effective rights:

- 1 In Roles and Tasks, select *Rights > View Effective Rights*.
- 2 Specify the name of the trustee whose rights you want to view, then click *OK*.

4.8 Schema

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. Every object has a defined schema class for that type of object. A class is like a set of rules for an object. An object is a new record with data built according to the rules of its class. The class has a class name, an inheritance class (unless it is at the top of the class hierarchy), class flags, and a group of attributes. Classes are named like objects—User, Printer, Queue, Server—yet they are just structure and rules, no content.

The schema that ships with eDirectory is the base schema. After the base schema is modified in any way, such as adding a new class or a new attribute, then it is considered to be the extended schema.

You aren't required to extend the schema, but you have the ability to do so. The Schema role in iManager lets you extend the schema to meet organizational needs. For example, you might want to extend your schema if your organization requires special footwear for employees and you need to keep track of employee shoe sizes. You might want to create a new attribute called Shoe Size and then add it to the User class.

4.8.1 Add Attribute

You can add optional attributes to existing classes if your organization's information needs change, or if you are preparing to merge trees.

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

1 In Roles and Tasks, Click *Schema > Add Attribute*.

2 Select the class you want to add an attribute to, then click *OK*.

3 In the *Available Optional Attributes* list, select the attributes you want to add, then click the right-pointing arrow to add these attributes to the *Add These Optional Attributes* list.

If you add an attribute by mistake or change your mind, select the attribute in the *Add These Optional Attributes* list, then click the left-pointing arrow to remove it from the list of attributes you want to add.

4 Click *OK*.

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

TIP: You can modify an existing class by using this page to add to the Current Attributes list. You can remove only attributes you have added prior to clicking *OK*. You cannot remove any attribute that has been previously added and saved.

4.8.2 Attribute Information

1 In Roles and Tasks, select *Schema > Attribute Information*.

2 Select the attribute you want information on, then click *View*.

4.8.3 Class Information

The Class Information page displays information about the selected class and lets you add attributes. Most of the information displayed on the page was specified when the class was created. Some optional attributes might have been added later.

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.

1 In Roles and Tasks, select *Schema > Attribute Information*.

2 Select the class you want information on, then click *View*.

4.8.4 Create Attribute

If a class is like a form, then the attribute is one field on the form. When an attribute is created, it is named (such as "surname" or "employee number") and given a syntax type (such as "string A-Z, 0-9" or "number -999 to 999"). From then on, it is available in the attribute list.

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.

- 1 In Roles and Tasks, click *Schema > Create Attribute*.
- 2 The Create Attribute wizard steps you through the attribute creation procedure.

4.8.5 Create Class

A class is like a set of rules for an object. An object is a new record with data built according to the rules of its class. The class has a class name, an inheritance class (unless it is at the top of the class hierarchy), class flags, and a group of attributes. Classes are named like objects—User, Printer, Queue, Server—yet they are just structure and rules, no content.

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.

- 1 In Roles and Tasks, click *Schema > Create Class*.
- 2 Specify a class name and (optional) ASN1 ID, then click *Next*.
- 3 Select *Auxiliary Class* when setting the class flags, then click *Next*.
- 4 Follow the instructions in the Create Class Wizard to define the new auxiliary class.

4.8.6 Delete Attribute

You can delete unused attributes that aren't part of the base schema of your eDirectory tree.

Two situations in which to consider deleting a class are:

- After merging two trees and resolving attribute differences.
- Whenever an attribute has become obsolete.

- 1 In Roles and Tasks, click *Schema > Delete Attribute*.
- 2 Select the attribute you want to delete.
Only attributes that can be deleted are shown.
- 3 Click *Delete*.

4.8.7 Delete Class

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

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

4.8.8 Extend 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 rights to the entire tree.

- 1 In Roles and Tasks, select *Schema > Extend Schema*.

The ICE* wizard steps you through the import, export, migration of data or schema update and compare operations.

4.8.9 Object Extensions

- 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, complete the appropriate action:
 - *Yes*: Quit this procedure. See [Modifying an Object's Auxiliary Properties \(http://www.novell.com/documentation/edir873/edir873/data/fbbdchgh.html#a3olrac\)](http://www.novell.com/documentation/edir873/edir873/data/fbbdchgh.html#a3olrac) in the *eDirectory Administration Guide* instead.
 - *No*: Click *Add*, select the auxiliary class, then click *OK*.
- 4 Click *Close*.

4.9 Users

A good source of general information is [Plan Users and Groups \(http://www.novell.com/documentation/nw312/instlenu/data/a4qsie4.html\)](http://www.novell.com/documentation/nw312/instlenu/data/a4qsie4.html).

4.9.1 Create User

- 1 In Roles and Tasks, click *Users > Create User*.
- 2 Complete the form with the following information:
 - *Username* (required)
 - *First Name*
 - *Last Name* (required)
 - *Full Name*
 - *Context* (required)
 - *Password* (twice)
- 3 Select *Set Simple Password*. (optional)

Simple Password is required for native file access for Windows and Macintosh users; it is not required when Universal Password is enabled.
- 4 Select *Copy from Template or User Object*.

The template or user object is only used if the corresponding Create user fields are left blank. When copying from a user object, iManager only allows a copy of the New object NDS Rights and prevents a copy of NDS rights.
- 5 Select *Create Home Directory*.

All rights except Administrator rights are given. Volume and Path fields are required. Enter the existing path and only the user directory will be created.

6 Click *OK*.

A confirmation appears: “Complete: The Create User request succeeded.”

4.9.2 Delete User

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, and click *OK*.

3 Click *Delete*.

A confirmation appears: “Complete: The Delete User request succeeded .”

4.9.3 Disable Account

1 In Roles and Tasks, select *Users > Disable Account*.

2 Type the name and context of the object, or use the search feature to find it, and click *OK*.

3 Click *Disable*.

4.9.4 Enable Account

1 In Roles and Tasks, select *Users > Enable Account*.

2 Type the name and context of the object, or use the search feature to find it, and click *OK*.

3 Click *Enable*.

4.9.5 Modify User

1 In Roles and Tasks, select *Users > Modify User*.

2 Type the name and context of the object, or use the search feature to find it, and click *OK*.

Tabs appear that display various properties as you select each tab or one of its links:

- *General*
- *NMAS Login Methods*
- *NMAS Login Sequences*
- *Security*
- *Restrictions*

3 Make your changes and click *Apply* to preview or *OK* to save.

Configuring for iManager Auditing

5

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

Nsure has the following prerequisites:

- A server (NetWare[®], Solaris*, Windows*, Linux*) in your directory tree with Nsure Audit 1.0.3. Use the [installation instructions](http://www.novell.com/documentation/nsureaudit/index.html) (<http://www.novell.com/documentation/nsureaudit/index.html>).
- Nsure Audit Platform Agent installed on the iManager server or Mobile iManager desktop and configured to point to the Secure Logging Server.

Nsure Audit captures data about the following events:

- Login successes
- Login failures
- Logouts
- Startups
- Shutdowns
- NPM installs

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

Additional Nsure Audit information is available in the [Novell[®] Nsure Audit white paper](http://www.novell.com/collateral/4621347/4621347.html#3) (<http://www.novell.com/collateral/4621347/4621347.html#3>).

5.1 Installing the IMAN_EN.LSC File in iManager

Install Nsure Audit 1.0.3 before you install the IMAN_EN.LSC file.

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

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

5.2 Enabling Auditing in iManager

To enable auditing:

- 1 Log in to iManager.
- 2 In Configure, select *iManager Configuration > Configure iManager*.
- 3 Select the *Enable Nsure Audit* check box and click *Save*.

Configuring and Customizing iManager

6

This section of the Administration Guide takes a systematic approach in describing the various features of Novell® iManager configuration. Topics are presented in the order that they appear on the interface.

Access iManager, then select the Configure icon. The Configure menu in the left pane of the interface lists the following tasks:

- [Section 6.1, “Role-Based Services,” on page 39](#)
- [Section 6.2, “Using RBS Reporting,” on page 45](#)
- [Section 6.3, “Configure iManager,” on page 49](#)
- [Section 6.4, “Object Creation List,” on page 53](#)
- [Section 6.5, “Module Installation,” on page 53](#)
- [Section 6.6, “E-mail Notification,” on page 54](#)
- [Section 6.7, “iManager Views,” on page 55](#)

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 only with iManager.

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 only those sets of responsibilities. This functionality is called Role-Based Services (RBS).

Role-Based Services (RBS) 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.

Use RBS to create specific roles within your organization; the roles contain tasks that a user performs. You can assign a role to a user who then performs the tasks 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

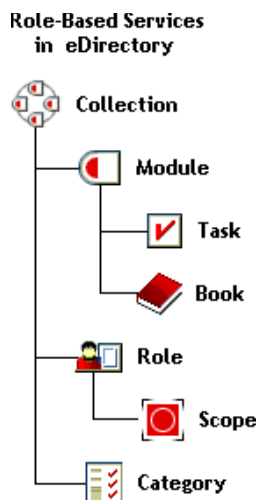
The following table lists the RBS objects. iManager extends the eDirectory schema to include these objects when you install RBS. For more information, see [Section 6.1.2, “Installing RBS,” on page 42](#).

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
 rbsRole	<p>Tasks that users (members) are authorized to perform. 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, or Organizational Units, and they 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>

Object	Description
 rbsBook	<p>A leaf object that contains a list of pages assigned to the book. An rbsBook can be assigned to one or more Roles and to one or more Object class types.</p> <p>rbsBook objects are located only in rbsModule containers.</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>
 rbs Module	<p>Represents a container object that holds rbsTask and rbsBook objects.</p> <p>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, Nsure Audit, Printing, Security, Servers, Software Licenses & Network, Usage, 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



6.1.2 Installing RBS

RBS is installed using the iManager Configuration wizard.

- 1 In iManager, click the *Configure* icon.
- 2 Select *Role Based Services > RBS Configuration*.
- 3 Select the *Configure iManager* link in the Notice.
- 4 Follow the onscreen instructions.

6.1.3 RBS Configuration

The RBS Configuration task provides complete control over RBS objects. It is a central place for managing and configuring RBS objects. This task enables you to list and modify RBS objects by type. This 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. For some operations you can operate on multiple objects at the same time. For example, you can associate or disassociate multiple members from a role at the same time.

In *Configure > Role-Based Services > RBS Configuration*, the RBS Configuration window appears. If RBS Services has not yet been configured on iManager, click the link in the window and follow the onscreen instructions.

Two tabs appear on the RBS Configuration screen:

- *2.x Collection* - The current collection of RBS objects
- *1.x Collection* - The older collection of RBS objects that you can either Delete or Migrate to 2X. If you select Migrate, a wizard steps you through the migration process.

You only see the collections you own.

- *Module* indicates the number of modules on the Web server that you are logged into.
- *Installed* lists the modules that are currently installed. Outdated modules are listed, as well as modules that are available but not installed.

From the RBS Configuration page you can create roles.

Creating a Role

To create a new iManager or eGuide role:

- 1 Select a collection by clicking it.
- 2 Click the *Role* tab.
A list displays the roles belonging to the collection.
- 3 Click *New > iManager Role*.
The Create iManager Role wizard appears.
- 4 Complete the steps in the wizard.

You can also delete roles. Under *Actions*, you can set a member association, define its scope, and set rights (Inherited) from that scope down to that subtree. If this option is not selected, then rights are limited to the container.

6.1.4 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 also cleans up all user role associations and scopes in the tree automatically. Do not delete the RBS collection using other utilities, such as ConsoleOne®.

Remove RBS by using the RBS Configuration task.

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

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

Changing to Unrestricted Mode

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

- 1 In *Configure*, select *iManager Server > Configure iManager*.
- 2 Select the *RBS* tab.
- 3 Remove the tree name in the *RBS Tree List* field by selecting the minus button to the right of the field.
- 4 Click *Save*.
- 5 Log out of iManager and log in again.

6.1.5 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. (Your Web Server may differ if you use a different Web server program.)

NOTE: The language in which a task is rendered is determined by the language in use by the Web browser. A task can be displayed in any language supported by iManager, since the text strings used to create tasks in Plug-In Studio have already been translated into all of iManager's supported languages. The Web browser automatically displays the task's text strings for its currently selected language.

Creating a New Task

To create a new task:

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

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

- 3 Choose an object type and platform by populating the following fields:
 - *Available classes*: (any class in eDirectory)
 - *Target Device*: Default (supported browsers), Browser (IE)
 - *Plug-in Type*: Task for Modify, Property Book Page, Task for Create, Task for Delete
 - *Add Auxiliary Classes*: (eDirectory)

- 4 In the Plug-in Fields screen, select or populate the following and click Install.

- *Attributes*

Select an attribute from the list of available attributes for the selected object class.

Click the attribute to list all available controls for the selected attribute. Double-click to accept the default control and move it into the plug-in field.

There are three icons beside a selected control:

- The flashing red icon indicates a required field.
Click it to add available values, then click OK, and the icon stops flashing.
- The down arrow allows you to change a control.
This is the same control that displayed when you clicked the attribute. Change it to any available control for the selected attribute.
- The third icon deletes the attribute.

- *Controls*

This box lists your attribute selection.

- *Plug-in Properties*

Below Plug-in Properties, in the left area of the page, give the plug-in an ID and assign the task to an RBS collection. Open the Object Selector to find the RBS collection. Assign the task to a role. The role you assign determines where it appears in the Roles and Tasks screen.

For example, if you choose User Management, click *Preview* and a new browser window opens. Preview the task to verify your design choices. Close the preview. Click *Install*, and iManager dynamically builds the .xml file, the .jsp file, and the Java* files that execute the task, and installs it into the system.

Editing a Task

- 1 In Configure, select *Role-Based Services > Plug-in Studio*.
- 2 Select the task and click *Edit*.
- 3 Modify the settings described in the create procedure and click *Install*.

A confirmation message appears: “The plug-in was successfully created and installed.”

Deleting a task

- 1 In Configure, select *Role-Based Services > Plug-in Studio*.
- 2 Select the task and click *Delete*.

A message appears: “Are you sure you want to delete this plug-in?”

3 Click *OK*.

A confirmation message appears. “The plug-in has been successfully deleted.”

6.1.6 Edit Member Association

There are two ways to associate members with roles: either go to a member and assign it to a role within a scope, or go to the role, and assign members and scope to it. The Edit Member Association feature assigns a role to a selected member.

1 In Roles and Tasks, select *Configure > Role Based Services > Edit Member Association*.

2 Specify a member and click *OK*.

A list appears displaying the roles this member is assigned to.

3 Specify a role.

When specifying the role to use in the Member Association, you can type in the full name of the RBS Role object. However, it is much easier to use the Object Selector (the magnifying glass button), from which you can either Browse to the desired Role, or Search for the desired Role from those available in the current eDirectory tree.

4 Specify the scope and click *OK*.

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

6.1.7 Edit Owner Collections

Use this feature to allow administration of RBS objects by assigned owners.

1 Specify a collection owner and click *OK*.

2 Add or remove collections this person can own, and click *OK*.

6.1.8 Create Server Administration Task

Step through the wizard to build custom tasks to access a server’s services. Before you do this, verify that the service is available on the server.

6.2 Using RBS Reporting

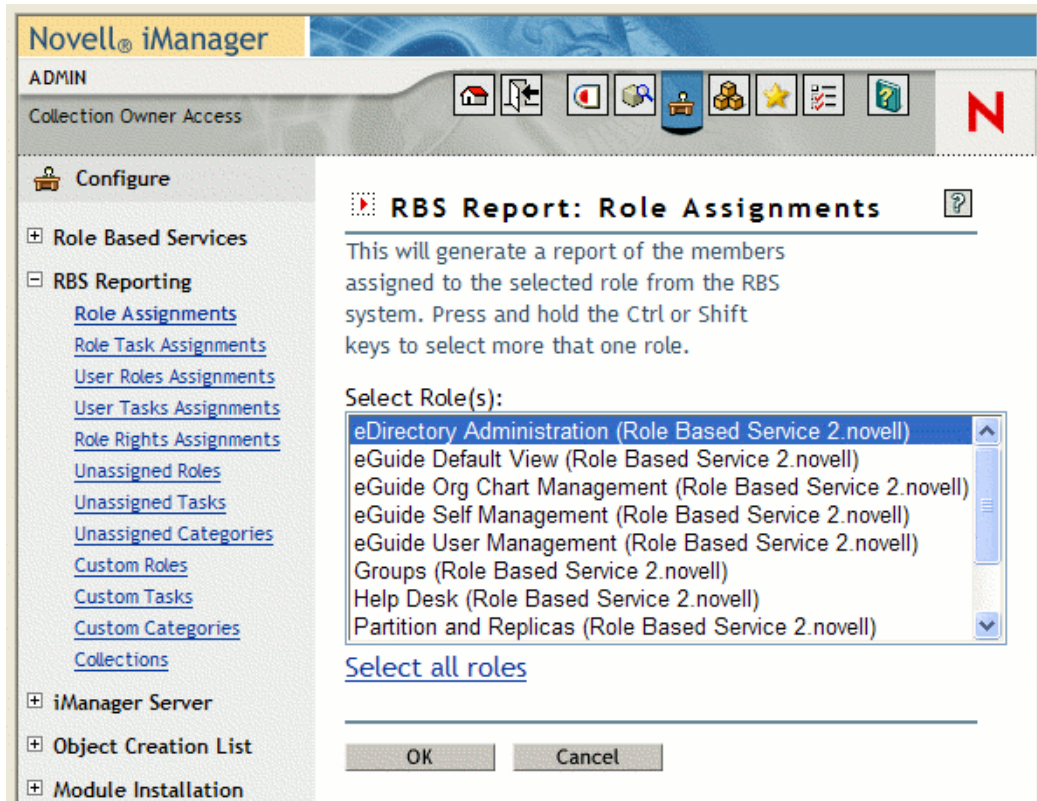
The RBS Reporting feature lets you generate reports about RBS objects in the directory and their configuration. Reports are in chart format and can be exported to other formats and printed. RBS Reporting generates the following reports:

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

6.2.1 Creating Reports

To access RBS Reporting, select the Configure view, then select the RBS Reporting role. Each report is implemented as a task. To generate a report, click the report task and follow the onscreen instructions. For example, to get a report listing all members assigned to a role, click *RBS Reporting > Role Assignments*.

Figure 6-2 iManager Configure View Showing the Role Assignments Task



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

6.2.2 Using Reports

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

Figure 6-3 *Members Assigned to a Role.*

Role Name	Role Object	Type	Member	Scope	Assigned	Inherit
eDirectory Administration	eDirectory Administration.Role Based Service 2.novell		admin.novell	.MY_TREE.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
eDirectory Administration	eDirectory Administration.Role Based Service 2.novell		jdoe.novell	novell	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

OK Print Export

Sorting Reports

By default, the items listed in a report are sorted alphabetically in ascending order on the first column. To indicate the column on 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 on which items are sorted, click the name of the column on which you want to sort. To change the sort order, click the name of the column on 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, which you can 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.

To export the data in a report:

- 1 Click *Export*.
- 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, CVS, 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
-----

```


6.3 Configure iManager

If you do not see this task, you are not an authorized user. See [“Authorized Users” on page 50](#).

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](#) on the interface (Configure iManager > Security).

- Security.Keystore.UpdateAllowAll

When Security.Keystore.UpdateAllowAll is true, then any successful user login imports/updates a certificate into the iManager certificate keystore. If the setting=false, only an [authorized user](#) login imports/updates certificates.

- Security.Keystore.Priority

The keystore.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 by switching “system” and “iManager,” or remove 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 be inside of 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.

6.3.1 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 on the various tabbed pages.

Warn When Using a Nonsecure Connection

Select if you want the following message to warn users: “You are using a non-secure connection.” This setting applies to the connection between the browser and the Web server.

Enable Nsure Audit

Assumption: you have met the Nsure[®] Audit [prerequisites](#). Select the Enable Nsure Audit option to send iManager logging events data to Nsure Audit.

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 users who can run various administrative tasks. Authorized user data is saved in `webapps/nps/WEB-INF/configiman.properties`. This file automatically gets created at install time, and the installing administrator's name is added to this file.

Using this option, you can modify the `configiman.properties` file. The tree name must be included with the names specified for example: `admin.novell.mytree`. To designate all users as authorized users, type `AllUsers`.

6.3.2 Look and Feel

Use this screen to customize the appearance of the iManager interface. Information about look and feel is saved in `webapps/nps/WEB-INF/configiman.xml`.

Title Bar Name

Type your organization name in this text box. It will appear 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 on the interface.

Store these files in `nps/portal/modules/fw/images`. Type 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 change your color selections.

6.3.3 Logging Events

Select a logging level for Web server debugging, from No Logging to Errors, Warnings, and Information messages.

To set your logging options, follow the onscreen instructions on the *Configure iManager > Logging Events* page.

6.3.4 Log Output

The log file path and log file size both appear on this page. Select to view the log file and it appears in html format. Select to clear the log file and all data in it is deleted; then the Log File Size resets to 0 (zero).

6.3.5 Authentication

Authentication configuration affects the iManager login page.

Remember Login Credentials

If you select this option, you will enter only your password to login.

Use Secure LDAP when Auto Connect

This setting specifies whether iManager communicates via LDAP SSL or LDAP clear text. Some plug-ins, such as Dynamic Groups and NMAS, will not work if this option is not selected. This setting will not take effect until you logout of iManager.

Allow Tree Selection on Login Page

If you select this option, the Tree text box appears on the login page. If you do not select this option, you must have a default tree name. Otherwise, you will not be able to log in.

Contextless Login

Select this option to allow users to type usernames on the login page without specifying a context.

Populating the following boxes is optional.

- Tree Name

The values you specify in the following text boxes depend on the tree name that you type here. The tree name is the tree that the contextless configuration will be applied to.

- Containers to Search

Which containers (for the selected tree) iManager must search to find a specific user. If you do not specify a container by default, iManager searches from the root of the tree down through the entire tree. The search to find the user object can take several minutes, depending on the size of the tree.

- Public Username

By default, iManager connects with public access, requiring no specific credentials. If you want, you can specify a user with specific credentials to do the search for the contextless lookup. The iManager public user will be used if you don't specify a user.

- Public User Password

The password (for the selected tree) for the user specified in Public Username.

6.3.6 RBS

Role-Based Services (RBS) assigns the rights within eDirectory to perform tasks. In order to do certain things, you must have rights in the eDirectory tree. When you assign a role to a user, RBS assigns the rights necessary to perform the tasks of that role.

Enable Dynamic Groups

Select this option to allow RBS to allow dynamic groups to be members of a role.

For more information on dynamic groups, see the *Novell eDirectory Administration Guide* (<http://www.novell.com/documentation/edir873/index.html?page=/documentation/edir873/edir873/data/fbabihtml>)

Show Roles in Owned Collection

If you select this option, collection owners will see all roles and tasks whether they are members of them or not. If you do not select it, owners will see only their assigned roles.

Click the drop-down arrows for lists of the following:

- *Role Discovery Domain*

This option indicates where in the tree iManager is to search for roles that are assigned to a member.

- *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 Discovery Domain*

This option indicates where in the tree iManager is to search for Dynamic Group membership. Role membership will then be checked in the Dynamic Groups found.

- *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 the entire tree for Dynamic Groups, up to root.

- *Dynamic Group Search Type*

This option selects which type of Dynamic Groups should be searched for role membership

- *Dynamic Group Objects 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*

When a collection owner or a Role member authenticates, this setting is auto-populated with the eDirectory tree's name. This effectively keeps track of the eDirectory trees where RBS has been configured. If RBS is removed from an eDirectory tree, remove that tree's entry in this list in order to return to Unassigned Access mode.

6.3.7 Miscellaneous

- *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 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 that eMFrame is located on.

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)

6.4 Object Creation List

When you create an object a preconfigured list of object classes are registered with the Create Object task.

6.4.1 Add Object Class to Creation List

Use this screen to add more objects to the Object Creation List. For example, if you add Device and click *Next*, the following information is created in an xml file: object type name, ID, version, required version, class name, and merge-template. Click *Finish*. If you click *Create Object*, Device is there. You can now create Device objects in eDirectory.

6.4.2 Delete Object Class From Creation List

This shows only the list of the objects that are registered.

6.5 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 50](#).

There are two types of Modules used in iManager: Novell Plug-in Modules (NPMs) and RBS Modules.

- Novell Plug-in Modules (NPMs)

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

- RBS Modules

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

Module Installation relates to NPMs. For more information, see [“Installing, Using, and Uninstalling Novell Plug-In Modules”](#) in the *iManager 2.5 Installation Guide*.

6.5.1 Available Novell Plug-in Modules

The Available Novell Plug-in Modules (NPM) page lists the NPMs contained in the packages directory and available for install. The name, version, and description of each module are in their respective manifest files.

6.5.2 Installed Novell Plug-in Modules

The Installed Novell Plug-in Modules 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.

6.6 E-mail Notification

This feature 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.

6.6.1 Mail Server Configuration

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

- 1 Configure the SMTP server settings to use for Task Event Notification and click *OK*.
 - *From Address*
The address that will appear in the From field of the e-mail message.
 - *Primary mail server*
An IP address or server name (example: smtp.novell.com)
The username and password that are required to send through the SMTP server.
 - *Secondary mail server*
Optional, used in case of failover.

6.6.2 Task Event Notification

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

- 1 Select an event.
The Task Event Properties screen appears.
- 2 Type the e-mail subject. (for example: Create User)
- 3 Type the message.
- 4 In the Additional e-mail addresses text box, type any additional e-mail addresses (separated by commas) you want to notify.
- 5 Select to *Override Default and Notify Only These Addresses* if you want the message to go only to the e-mail addresses specified on this page.
Otherwise, the message will go to the address on the Task Event Notification screen as well as the additional addresses.

6.7 iManager Views

iManager Views are management pages accessed from the top frame of iManager. You might not want users to see certain views, such as Object or Configure.

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

You can show or hide the views that are available to users of iManager.

- 1 Change the flag for a specific icon from *Do Not Set to Hide*.
- 2 Select the Read Parent Containers of this Object check box to impose the settings of the object's parent container on this object.

When an object's parent container is selected, this will take precedence.

Do not select the *Read Parent Containers of this Object* check box if you are selecting settings exclusively for this particular object.

6.7.1 Read-only Views

Read-only views are not created by iManager, but are a result of a user's eDirectory rights to the iManager attributes being viewed. If the user only has read rights to the attribute, then iManager only allows the user to see the fields, but not edit them.

NOTE: By default, iManager automatically grants edit rights to attributes related to a user's assigned roles.

For example, iManager does not provide a mechanism to create a read-only view of password restrictions. Members of the 'Held Desk' role receive write rights to the password restrictions attributes by default, so the password restriction attributes are editable to members of the 'Help Desk' role.

To avoid this, disable the automatic granting of rights in support of an assigned iManager role and grant user rights manually. To do this, complete the following steps:

- 1 Go to *Configure > Role Based Services > RBS Configuration*, and select the collection to modify.
- 2 Open the *Role* tab
- 3 Select the box next to the role to which the users are assigned, and select *Actions > Member Associations*.
- 4 In the list of members for the role, uncheck *Assign Rights*. This removes the rights assigned to the users automatically by the role. You must now assign rights manually to the attributes that users should be permitted to edit.

Preferences

7

Select the Preferences icon and set your personal preferences.

7.1 General

This section has the following features:

- [Section 7.1.1, “Manage Favorites,” on page 57](#)
- [Section 7.1.2, “Object Selector,” on page 57](#)
- [Section 7.1.3, “Object View,” on page 57](#)
- [Section 7.1.4, “Set Initial View,” on page 58](#)
- [Section 7.1.5, “Language,” on page 58](#)

7.1.1 Manage Favorites

Select and direct the tasks you perform most frequently. You can choose to make Favorites your initial view after login.

7.1.2 Object Selector

Set your Object Selector preferences for the following features:

- *Window Size* (window width, height, and Left column width) in pixels
- User-Specified Defaults
 - *Startup Mode*
 - *Results per Page*
 - *Starting Context*
 - *Search on Startup*

7.1.3 Object View

Set your Object View preferences for the following features:

- *Column Width*
Measured in pixels
- *Startup Mode*
Select Browse or Search.
- *Selection Mode*
Select Single or Multiple.
- *Results per Page*
How many results to display on a page, in *Single-select Mode* or *Multi-select Mode*.

- *Starting Context*

Where in the tree the search begins, and if that place should be used every time.

- *Search on Startup*

When the Object View opens in Search mode, select to either: *Wait for the user to enter search criteria* and click *Apply*, or *Automatically do an initial search based on task-specified search criteria*.

7.1.4 Set Initial View

The view that you select determines what will appear after you log in to iManager.

7.1.5 Language

Select the language you want iManager to display and click *OK*. The language setting is not persistent; you must set it on a per session basis.

This section provides some troubleshooting tips resulting from iManager testing in Novell® test labs. These tips are arranged alphabetically in the following topics:

- [Section 8.1, “Authentication Error Messages,” on page 59](#)
- [Section 8.2, “Debugging Settings for Install and Configure,” on page 60](#)
- [Section 8.3, “Dynamic Group Auxillary Class Support,” on page 60](#)
- [Section 8.4, “Firefox 1.0 Issue Incompatible with iManager Plug-in Functionality,” on page 60](#)
- [Section 8.5, “eDirectory Maintenance Task Errors,” on page 61](#)
- [Section 8.6, “HTTP 404 Errors,” on page 61](#)
- [Section 8.7, “HTTP 500 Errors,” on page 61](#)
- [Section 8.8, “Missing Attribute, Object, or Value Errors,” on page 62](#)
- [Section 8.9, ““Page not found” Error on a Windows Server,” on page 62](#)
- [Section 8.10, ““Unable to Determine Universal Password Status” Error,” on page 63](#)
- [Section 8.11, “\(SuSE\) History does not automatically Sync across Multiple Simultaneous Use Logins,” on page 63](#)
- [Section 8.12, “iManager 2.5 Remote Install for NetWare 6.5,” on page 63](#)
- [Section 8.13, “Apache and Tomcat Ports,” on page 63](#)
- [Section 8.14, “Performing a System Restore from Image Software,” on page 64](#)

8.1 Authentication Error Messages

Authentication errors most often return 669, 634, or 601 error messages.

8.1.1 669 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 user name in the tree. Contextless login will try 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.

8.1.2 634 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 in a timely manner.

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. Ask your administrator to add your user location to the contextless login search containers or log in with a full context.

8.2 Debugging Settings for Install and Configure

If installation fails, you can run some debugging tools to help determine what is wrong.

You can run the installation program in debugging mode for Windows*, HP*-UX*, and Solaris* installations.

- Solaris and HP-UX: 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.

The Linux* installation program does not have a debugging mode, but the program creates the imanager_install.log and iManagerConfigWizard.log during the install for informational and troubleshooting purposes. These are located in /var/log. The imanager_install.log contains informational/error messages logged during the general install. The iManagerConfigWizard.log contains informational error messages logged during the configuration of iManager.

8.3 Dynamic Group Auxillary Class Support

If you try to add an object that is extended to be a Dynamic Group as a member of a role, the following message appears: “Dynamic Group support is not enabled. The selected Dynamic Group object cannot be used as a role member.” The object cannot be added because Dynamic Group auxiliary class support is not enabled.

8.4 Firefox 1.0 Issue Incompatible with iManager Plug-in Functionality

Using the shipping version of Firefox* 1.0 to run iManager 2.5, you can get 404 errors when you select a task. This is a bug in Firefox. It occurs when you use iManager plug-ins that utilize the clipboard, and you choose “Remember this decision” in the security window that displays when the clipboard is accessed. You can monitor this bug at the [Mozilla* bug tracking system \(https://bugzilla.mozilla.org/show_bug.cgi?id=269270\)](https://bugzilla.mozilla.org/show_bug.cgi?id=269270).

There are two things you can do if you find yourself in this state:

- Run iManager in simple mode by replacing “iManager.html” with “Simple.html” in the URL that runs iManager
- or
- Edit your Mozilla prefs.js file by doing the following:
- 1 Close the Firefox browser.
 - 2 In a folder below the Mozilla/Profiles folder, located in your account's Application Data folder, find your browser profile's prefs.js file and delete the following two lines: `user_pref("capability.principal.codebase.pX.denied", "UniversalXPConnect");` `user_pref("capability.principal.codebase.pX.id", "<iManager URL Root>");` where “<iManager URL Root>” is the root of the URL of the version of iManager you are using; and “X” in the “...pX...” of the two settings match
 - 3 Restart the browser.
 - 4 The Internet Security will continue to annoy you. Select *Allow*, but *do not* select the *Remember this Decision* check box.

8.5 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, “Roles and Tasks,” on page 17](#).

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).

8.6 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 will vary. Apache uses either the httpd.conf file or the ssl.conf file. Please refer to Microsoft’s documentation for information on IIS port settings.

8.7 HTTP 500 Errors

If you receive an internal server error or servlet container error (either unavailable or being upgraded), iManager is having 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, you need to verify the status of Tomcat and, if the error persists, the status of Apache.

8.7.1 Checking the Status of Tomcat

- 1 Restart Tomcat.
- 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[®], any errors are sent to the logger screen.

8.7.2 Checking the Status of Apache

- 1 Restart Apache.
- 2 Check the Apache log files for errors.

The files are located in the \$apache_home\$/logs directory.

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 config.xml located in webapps/nps/WEB-INF/. You must restart Tomcat after making any changes to the config.xml file. For example: https://127.0.0.1/nps/servlet/webacc?taskId=fw.Startup&forceMaster=true

8.9 “Page not found” Error on a Windows Server

If your server is running multiple Web sites, the iManager installation program selects the first site that meets its criteria, mostly likely the default Web site that uses port 80. If you want iManager to run from a different Web site, you need to create a virtual directory on the desired Web site.

- 1 From Control Panel > *Administration Tools* > *Computer Management*, click *Services and Applications* > *Internet Information Services* in the left-hand navigation frame.
- 2 Select the Web site icon that you want to configure for iManager.
- 3 From the Action menu, select *New* > *Virtual Directory*.
- 4 In the Virtual Directory Creation Wizard, type *jakarta* in the Alias box.
- 5 In the Directory box, browse to the ISAPI redirector directory, which is found in the Tomcat home directory (\bin\win32\1386) and click *OK*.
- 6 For access permissions, select *Read*, *Run scripts* (such as ASP), *Execute* (such as ISAPI applications or CGI) and *Write*.
- 7 Click *Next* to create the virtual directory and return to the Computer Manager window.
- 8 In the left-hand frame, select the *Default Web Site* > *jakarta*, then delete *jakarta*.

iManager creates this jakarta directory. If this Web site does not contain the jakarta directory, browse the other Web sites until you find the one with the jakarta directory.

8.10 “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 `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 `\usr\bin\nmasinst` directory.

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

8.11 (SuSE) History does not automatically Sync across Multiple Simultaneous Use Logins

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

8.12 iManager 2.5 Remote Install for NetWare 6.5

If the iManager 2.5 remote install for NetWare 6.5 behaves unexpectedly, try deleting the Novell Installation Service temporary files. Delete the entire Novell directory located in `C:\Program Files\Common Files\`.

8.13 Apache and Tomcat Ports

If you are experiencing port conflicts or need to know what ports Apache and Tomcat are using, see the platform-specific information below:

8.13.1 HP-UX

For the Apache http port, see the file, `/opt/hpws/apache/conf/httpd.conf`, or the location you put it.

For the Apache https port, see the file, `/opt/hpws/apache/conf/ssl.conf`, or the location you put it.

For Tomcat ports, see the file, `/opt/hpws/tomcat/conf/server.xml`.

IMPORTANT: Find the section that reads, “Define a coyote 1AK2AJP1.3 connector.” Set the redirect port to be the same as the Apache SSL. For example, if Apache is on port 443, Tomcat should be, also.

8.13.2 Linux

For the Apache http port, see the file, `/etc/opt/novell/httpd/gconf.d/vhost.conf`.

For the Apache https port, see the file, `/etc/opt/novell/httpd/gconf.d/sshhost.conf`.

For the Tomcat ports, see the file, `/var/opt/novell/tomcat4/conf/server.xml`.

The non-SSL port section begins with, “Define a non-SSL Coyote HTTP/1.1 Connector on port *n*.”

The SSL port section begins with, “Define an SSL Coyote HTTP/1.1 Connector on port *n*.”

IMPORTANT: Find the section that reads, “Define a coyote 1AK2AJP1.3 connector.” Set the redirect port to be the same as the Apache SSL. For example, if Apache is on port 443, Tomcat should be, also.

8.13.3 NetWare

For the Apache HTTP port, see the httpd.conf file in sys:\apache2\conf.

For the Apache HTTPS port, see the httpd.conf file in sys:\apache2\conf.

For the Tomcat ports, see the server.xml file in sys:\tomcat\4\conf.

8.13.4 Solaris

For the Apache HTTP port, see the httpd.conf file in /var/opt/novell/httpd/conf/ (or the location you put it).

For the Apache HTTPS port, see the ssl.conf file in /var/opt/novell/httpd/conf (or the location you put it).

For the Tomcat ports, see the server.xml file in /var/opt/novell/tomcat4/conf.

8.13.5 Windows

Windows allows for relocation of all files. If you accept the defaults in the iManager installation, look in the following places for Apache and Tomcat configuration files:

For the Apache HTTP port, see the httpd.conf file in *rootdir*\novell\apache\conf.

For the Apache HTTPS port, see the ssl.conf file in *rootdir*\novell\apache\conf.

For the Tomcat ports, see the server.xml file in *rootdir*\novell\tomcat4\conf.

If you can't find a configuration file, search the Registry.

8.14 Performing a System Restore from Image Software

If you perform a system restore from image software such as Ghost, the NPS-APACHE.CONF could become truncated in the process. (This file is located in SYS:\tomcat\4\conf.)

If the NPS-APACHE.CONF file is truncated to NPS-APACHE~1.CON or some other corrupt filename, use bash or another text editor to rename the file, then stop and restart Apache and Tomcat.

Best Practices and Common Questions

9

This chapter contains recommendations 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 9.1, “Backup and Restore Options,” on page 65](#)
- [Section 9.2, “Coexistence with iManager 2.0.2 Role-Based Services,” on page 65](#)
- [Section 9.3, “Collections,” on page 66](#)
- [Section 9.4, “Failed Installs,” on page 66](#)
- [Section 9.5, “High Availability: Running iManager in a Clustered Environment,” on page 67](#)
- [Section 9.6, “Logging In to an xref Server,” on page 68](#)
- [Section 9.7, “Multiple Collection Objects,” on page 68](#)
- [Section 9.8, “Patching Servers,” on page 68](#)
- [Section 9.9, “Role Assignments,” on page 69](#)

9.1 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 RBS 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 will be preserved. If the Tomcat directory is somehow compromised on the server, shutting down Tomcat and recopying the directory will allow you to recover iManager. If you are not using Role-Based Services, backing up the Tomcat directory is all that is needed.

9.2 Coexistence with iManager 2.0.2 Role-Based Services

You should update your RBS collection to version 2.5. Otherwise, if you use iManager to access a tree that has an RBS collection from iManager 2.0.2, you won't see all of the roles and tasks that should display.

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

A message appears that confirms a successful update.

Updated Plug-ins will be visible in both iManager 2.0.2 and 2.5.

9.3 Collections

It is important to recognize that one configuration is not ideal for all companies. The most common situations together with suggestions for managing their respective collections are:

- 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.

9.4 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. See “[Prerequisites](#)” in the *iManager 2.5 Installation Guide*.

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

9.4.1 Windows

- 1 If the error involves one of these components, check the specified log files for errors:
 - NCI - wnciu0.log, located in the install's temp directory
 - Apache - apache_install.log, located in the root of the directory where iManager is being installed; for example: C:\Program Files\Novell <system.drive>\Program Files\Novell
 - Tomcat - Apache_Tomcat_InstallLog.log, located in the root of Tomcat's install directory; for example: Program Files\Novell\Tomcat

- 2 Check the iManager install log file, iManager_Install_2.5_InstallLog.log, for any errors.

This file is located in the <servlet root>/WEB_INF/log directory.

- 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.

1. Immediately after launching the installer, hold down the <CTRL> key until a console window appears.
2. After the install has completed, click the icon in the upper left corner of the console window and select Properties > Layout.
3. Change the Buffer Size to be 3000 and click OK.
4. In the Layout window, click Edit > Select All.

5. Again, in the Layout window, click Edit > Copy.
 6. Open a text editor and paste the output of the debug in it.
- 4 Identify and correct any errors or stack traces and rerun the install.

9.4.2 HP UX and Solaris

- 1 Check the iManager install log file, `iManager_Install_2.5_InstallLog.log`, for any errors.

This file is located in the `<servlet root>/WEB_INF/log` directory.

- 2 If the log file does not give sufficient information to identify the problem, rerun the install in debug mode.

In the command line, type the following: .

```
export LAX_DEBUG=true
```

- 3 Identify and correct any errors or stack traces and rerun the install.

9.4.3 Linux

- 1 Check the iManager install log file, `iManager_Install_2.5_InstallLog.log`, for any errors.

This file is located in the `<servlet root>/WEB_INF/log` directory.

- 2 If the log file does not give sufficient information to identify the problem, rerun the install in debug mode.

In the command line, type the following:

```
/var/log/manager_install.log
```

- 3 Identify and correct any errors or stack traces and rerun the install.

9.5 High Availability: Running iManager in a Clustered Environment

Although iManager is a session-based tool that ships without any failover feature, you can run it in a clustered environment (http://www.novell.com/documentation/oes/index.html?page=/documentation/oes/cluster_admin_lx/data/h4r4bw6c.html).

- 1 Install and configure iManager on the nodes in the cluster where the virtual IP is moved to (i.e., an Active/Active cluster). If the node running iManager were to fail, Novell Cluster Services (NCS) detects the node failure and will move (re-load) the virtual IP address on another node in the cluster.
- 2 Using the `Generic_IP_Service` template that ships with NCS, 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/ncsfuncs
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/ncsfuncs
ignore_error del_secondary_ipaddress xxx.xxx.xxx.xxx
exit 0
```

- 4 Point your Web browser to: `http://web_server/nps/iManager.html` (*web_server* is the IP address used in the iManager cluster resource).

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 re-authenticate and re-start whatever operations were interrupted.

Because iManager/tomcat/apache is already running (Active/Active) on the other nodes, there is no load time of these applications in the event that NCS has to migrate (move) the virtual IP to another node.

There is little benefit in using an Active/Passive cluster as 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 (i.e., Apache and Tomcat). This identical configuration of iManager then needs to be done on all nodes where you want iManager highly available.

9.6 Logging In to an xref Server

See [Section 8.1, “Authentication Error Messages,”](#) on page 59 in the “Troubleshooting” chapter of this guide.

9.7 Multiple Collection Objects

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.

- Create a collection in every geographical or functional location as high in the location as possible.
- Have one or more iManager servers per location.

The benefits of this setup are faster login time and simplified tree navigation.

9.8 Patching Servers

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

- 1 In the Configure view, select *Module Installation*.
- 2 Select *Available Novell Plug-in Modules*.
- 3 Click *New*.
- 4 Browse to the location of the patch file, and click *OK*.
- 5 Select the patch from the list and click *Install*.

The server will be patched with the latest code.

9.9 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 will 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 the user objects to match a Dynamic Group search criteria.