

Novell iManager

1.5.2

ADMINISTRATION GUIDE

www.novell.com

September 29, 2003



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.

This product may require export authorization from the U.S. Department of Commerce prior to exporting from the U.S. or Canada.

You may not 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 © 2002 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.

U.S. Patent No. 5,157,663; 5,349,642; 5,455,932; 5,553,139; 5,553,143; 5,572,528; 5,594,863; 5,608,903; 5,633,931; 5,652,859; 5,671,414; 5,677,851; 5,692,129; 5,701,459; 5,717,912; 5,758,069; 5,758,344; 5,781,724; 5,781,724; 5,781,733; 5,784,560; 5,787,439; 5,818,936; 5,828,882; 5,832,274; 5,832,275; 5,832,483; 5,832,487; 5,850,565; 5,859,978; 5,870,561; 5,870,739; 5,873,079; 5,878,415; 5,878,434; 5,884,304; 5,893,116; 5,893,118; 5,903,650; 5,903,720; 5,905,860; 5,910,803; 5,913,025; 5,913,209; 5,915,253; 5,925,108; 5,933,503; 5,933,826; 5,946,002; 5,946,467; 5,950,198; 5,956,718; 5,956,745; 5,964,872; 5,974,474; 5,983,223; 5,983,234; 5,987,471; 5,991,771; 5,991,810; 6,002,398; 6,014,667; 6,015,132; 6,016,499; 6,029,247; 6,047,289; 6,052,724; 6,061,743; 6,065,017; 6,094,672; 6,098,090; 6,105,062; 6,105,132; 6,115,039; 6,119,122; 6,144,959; 6,151,688; 6,157,925; 6,167,393; 6,173,289; 6,192,365; 6,216,123; 6,219,652; 6,229,809. Patents Pending.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.

www.novell.com

Novell iManager 1.5.2 Administration Guide
September 29, 2003

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.

eDirectory is a trademark of Novell, Inc.

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

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

Third-Party Trademarks

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

About This Guide

This guide describes how to set up and use Novell® iManager 1.5.2. The guide is intended for network administrators and is divided into the following sections:

- ♦ Chapter 1, “Novell iManager Quick Start,” on page 7
- ♦ Chapter 2, “Installing Novell iManager,” on page 9
- ♦ Chapter 3, “Using Novell iManager,” on page 13
- ♦ Chapter 4, “Setting Up Roles and Tasks,” on page 17
- ♦ Appendix A, “Additional Resources,” on page 25
- ♦ Appendix B, “The eDirectory Management Toolbox,” on page 27
- ♦ Appendix C, “Configuring and Using SSL for LDAP Connections,” on page 39

Additional Documentation

For documentation on installing and running eDirectory, see the *Novell eDirectory 8.7 Administration Guide* on the Novell documentation web site (<http://www.novell.com/documentation>).

For information on installing Web services software (Apache, Tomcat, Windows Web Services), see the links in Appendix A, “Additional Resources,” on page 25.

Documentation Updates

For the most recent version of the *iManager 1.5.2 Administration Guide*, see the Novell documentation Web site (<http://www.novell.com/documentation/lg/imanager152>).

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.

User Comments

We want to hear your comments and suggestions about this manual and the other documentation included with Novell eDirectory and iManager. To contact us, send e-mail to proddoc@novell.com.

1

Novell iManager Quick Start

This chapter contains information on how to get started using Novell® iManager 1.5.2. More detailed information is included throughout this manual.

- 1** Install eDirectory™ 8.7.1. iManager is the way to get the most out of the new eDirectory 8.7.1 features.

For more information on eDirectory 8.7.1, see the Novell documentation Web site (<http://www.novell.com/documentation>).

- 2** Know your Web services setup.

iManager must be installed on a web or a middleware server. Your web/middleware server must have the necessary Web services: an HTTP server, a servlet container, and a Java* Virtual Machine. Refer to the installation instructions for each platform in Chapter 2, “Installing Novell iManager,” on page 9.

- 3** Install the iManager 1.5.2 software.

Make sure you have admin-equivalent rights.

- 4** Restart the server.

- 5** At a machine running Internet Explorer 5.5 or later (recommended) or Netscape* 6.2 or later, enter the following URL:

`https://server_ip_address:port_number/eMFrame/iManager.html`

IMPORTANT: This URL is case sensitive. The server IP address can also be a DNS name.

- 6** Set up your roles and tasks using the iManager Configuration Wizard.

The iManager Configuration Wizard will launch the first time you run iManager, but you can launch the wizard anytime by clicking **Configure > Plug-in Setup and Install > Configure iManager**.

2

Installing Novell iManager

This chapter describes how to install and initially set up Novell® iManager 1.5.2.

Novell iManager 1.5.2 must be installed on a web server or other middleware server. The person installing the iManager software should have admin-equivalent rights to the eDirectory™ tree.

Two steps are required before you can use iManager: you must install the software and you must configure the iManager roles and tasks. This chapter shows you how to complete both steps.

On NetWare

NOTE: If you are using a previous version of iManager, you must upgrade to version 1.5 if you want to use all of the latest roles and tasks.

Prerequisites

- ☐ NetWare® 6 server with Support Pack 3 or later installed

IMPORTANT: NetWare 5.1 is not supported.

- ☐ Novell International Cryptographic Infrastructure (NICI) 2.6.0 installed

NICI 2.6.0 is installed automatically with eDirectory 8.7.1. If you are installing iManager on a machine without eDirectory 8.7.1, you will need to install NICI manually. Run NWCONFIG and select the installs\nw\nici subdirectory from the iManager CD.

- ☐ A workstation with Internet Explorer 5.5 or later (recommended) or Netscape 6.2 or later installed
- ☐ The display settings on the server monitor set to at least 256 colors in order for the iManager installation program to run
- ☐ Admin-equivalent rights to the eDirectory tree (only necessary for the iManager Configuration Wizard)
- ☐ Web services

NetWare 6 already installs an Apache HTTP server, a Tomcat servlet container, and the Sun® JRE. No additional web services software is required.

Procedure

- 1** Mount the eDirWebApps CD as a NetWare volume.
- 2** Execute the webapp.ncf file.
- 3** Follow the prompts.
- 4** Reboot the server.

At a minimum, your Web services software (Apache, Tomcat. etc.) must be stopped and restarted before you can use iManager. The iManager installation program restarts Apache and Tomcat for you.

- 5 Upon the completion of the install, go to a workstation on your network.

NOTE: The browser software on the NetWare 6 console does not support iManager at this time.

- 6 From a workstation, launch either Internet Explorer 5.5 or later (recommended) or Netscape 6.2 or later, then enter the following URL:

https://server_ip_address:port_number/eMFrame/iManager.html

IMPORTANT: This URL is case sensitive. The server IP address can also be a DNS name.

- 7 Log in as someone with admin-equivalent rights to the eDirectory tree since the schema will be extended at this time.
- 8 Set up your roles and tasks using the iManager Configuration Wizard.

The iManager Configuration Wizard will launch the first time you run iManager, but you can launch the wizard anytime by clicking Configure > Plug-in Setup and Install > Configure iManager.

On Windows NT/2000

Prerequisites

- ☐ Windows* NT* Server with SP6a or later or Windows 2000 Server with SP3 or later
- ☐ 256MB memory on server
- ☐ Novell International Cryptographic Infrastructure (NICI) 2.6.0 installed

NICI 2.6.0 is installed automatically with eDirectory 8.7.1. If you are installing iManager on a machine without eDirectory 8.7.1, you will need to install NICI manually. Run wcniciu0.exe located in the installs\win\nici subdirectory on the iManager CD.

- ☐ A workstation with Internet Explorer 5.5 or later (recommended) or Netscape 6.2 or later installed
- ☐ The display settings on the server monitor set to at least 256 colors in order for the iManager installation program to run
- ☐ Admin-equivalent rights to the eDirectory tree (only necessary for the iManager Configuration Wizard)
- ☐ Web services

Windows servers can use Apache and Tomcat; they also can use Windows Web Services (IIS) and Tomcat. The iManager installation program will detect which Web services are already installed.

IMPORTANT: If the Windows server is using IIS and you want to use Apache and Tomcat, you must remove IIS first before installing Apache and Tomcat with the iManager installation program. Also, if no web services are currently installed on the Windows server, the iManager installation program will install and configure Apache and Tomcat.

For more information on Web services, see Appendix A, "Additional Resources," on page 25.

Procedure

- 1 Run the following executable on the Windows server:

installs\win\eDirWebAppsInstall.exe

- 2** Follow the prompts.
- 3** From a workstation, launch either Internet Explorer 5.5 or later (recommended) or Netscape 6.2 or later, then enter the following URL:

`https://server_ip_address:port_number/eMFrame/iManager.html`

IMPORTANT: This URL is case sensitive. The server IP address can also be a DNS name.

- 4** Log in as someone with admin-equivalent rights to the eDirectory tree since the schema will be extended at this time.
- 5** Set up your roles and tasks using the iManager Configuration Wizard.

The iManager Configuration Wizard will launch the first time you run iManager, but you can launch the wizard anytime by clicking Configure > Plug-in Setup and Install > Configure iManager.

On UNIX

Prerequisites

- ☐ Red Hat* Linux* 7.3 or Advanced Server 2.1; Solaris* 7, 8, or 9; and/or AIX 5L server
- ☐ A workstation with Internet Explorer 5.5 or later (recommended) or Netscape 6.2 installed
- ☐ Admin-equivalent rights to the eDirectory tree (only necessary for the iManager Configuration Wizard)
- ☐ Root rights to web server
- ☐ The display settings on the server monitor set to at least 256 colors in order for the iManager installation program to run
- ☐ Web services

UNIX platforms will most likely require a separate installation of Apache, Tomcat, and the JVM in order for iManager to run properly. For more information on Web services, see Appendix A, “Additional Resources,” on page 25.

Minimum web services requirements for UNIX platforms are JVM 1.3.1_02, Apache 1.3.20, and Tomcat 3.3a.

Procedure

- 1** Open a shell and change to the *install_directory*/installs/unix directory.
This path is relative to the directory where you copied or extracted the iManager files.
- 2** Enter the following command:
`sh eDirWebAppsInstall.bin`
- 3** Follow the prompts.
- 4** Stop and re-start Apache and Tomcat.
- 5** From a workstation, launch either Internet Explorer 5.5 or later (recommended) or Netscape 6.2 or later, then enter the following URL:

`https://server_ip_address:port_number/eMFrame/iManager.html`

IMPORTANT: This URL is case sensitive. The server IP address can also be a DNS name.

- 6** Log in as someone with admin-equivalent rights to the eDirectory tree since the schema will be extended at this time.
- 7** Set up your roles and tasks using the iManager Configuration Wizard.

The iManager Configuration Wizard will launch the first time you run iManager, but you can launch the wizard anytime by clicking Configure > Plug-in Setup and Install > Configure iManager.

Uninstalling iManager

NOTE: Uninstalling iManager doesn't remove the new Role-Based Services objects created in eDirectory. To remove the Role-Based Services objects in iManager, click the Configure tab > Collection Configuration > Delete Collection.

On NetWare

Uninstalling iManager using NWCONFIG is not supported in this release. Use the uninstall.ncf file located in the sys:\webapps\eMFrame\Web-inf directory.

On Windows

Use the Add/Remove Programs feature from the Windows Control Panel.

On UNIX

Execute the UninstalliManager file located in the \$tomcat_home/webapps/eMFrame/UninstallerData directory. The uninstall program will remove everything with the exception of log files and custom files that might have been created. These files will be left in their respective directories.

3

Using Novell iManager

This chapter describes how to access and use the Novell® iManager 1.5.2 software.

Opening Novell iManager

- 1 From a workstation, launch either Internet Explorer 5.5 or later (recommended) or Netscape 6.2 or later, then enter the following URL:

`https://server_ip_address:port_number/eMFrame/iManager.html`

IMPORTANT: This URL is case sensitive. Also, the server IP address can also be a DNS name.

For example:

`https://137.65.135.150:2200/eMFrame/iManager.html`

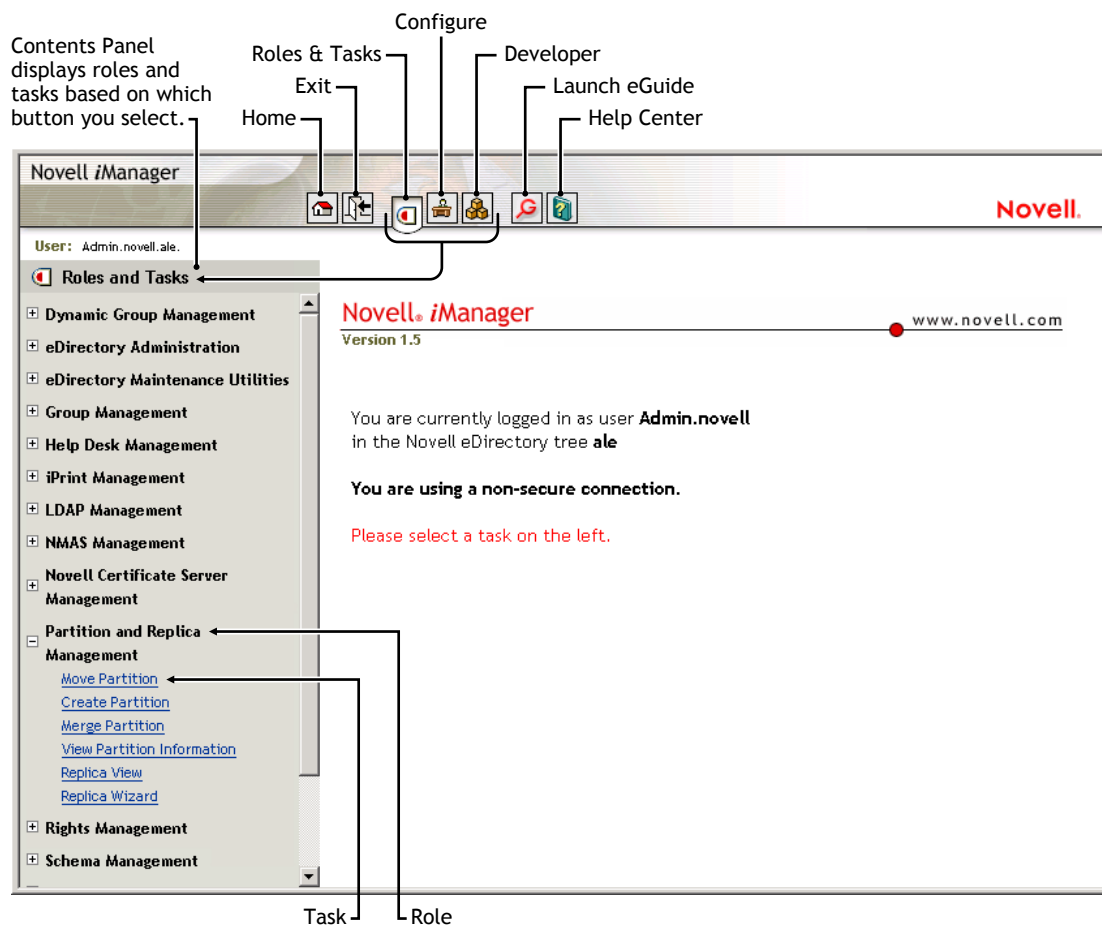
- 2 Log in using your username, context, password, and eDirectory tree name or IP address.

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

iManager Interface

The following figure describes the iManager interface.

Figure 1 iManager Interface



NOTE: When using iManager, make sure to use the buttons ("OK," "Next," etc.) within the interface. The browser's toolbar buttons ("Back," "Next", etc.) are not supported in iManager.

Simple Mode

Novell iManager 1.5.2 can also run in "simple mode" which provides similar functionality to the standard iManager program with a streamlined Web interface.

Simple mode can be also used with screen readers and provides accessibility features intended to accommodate persons with disabilities.

Simple mode is opened by default when running iManager in a Netscape browser. In order to use the accessibility features (screen readers, etc.) in iManager 1.5.2, you must use Internet Explorer 5.5 as your browser.

Opening Novell iManager in Simple Mode

- 1 From a workstation, launch either Internet Explorer 5.5 or later (recommended) or Netscape 6.2 or later, then enter the following URL:

https://server_IP_address:port_number/eMFrame/Simple.html

IMPORTANT: This URL is case sensitive. Also, the server IP address can also be a DNS name.

For example:

`https://137.65.135.150:2200/eMFrame/Simple.html`

- 2** Log in using your username, context, password, and eDirectory Tree name or IP address.

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

Advice about Using iManager

Don't Use Browser "Back" and "Forward" Buttons

Because iManager is a web-based application, it is important to navigate through the interface using the buttons inside the application and not the buttons located in the toolbar of your browser.

4

Setting Up Roles and Tasks

Novell® iManager 1.5.2 gives administrators the ability to assign specific responsibilities to users and to present them with only the tools (and their accompanying rights) necessary to perform those sets of responsibilities. This functionality is called *Role-Based Services (RBS)*.





Role-Based Services allows administrators to assign users a defined set of specific functions, called *tasks*, and objects as determined by the grouping of tasks, called *roles*. What users see when they access Novell iManager is based on their role assignments in Novell eDirectory™. Only the tasks assigned to the authenticated user are displayed. The user does not need to browse the tree to find an object to administer; the plug-in for that task presents the necessary tools and interface to perform the task.


You can assign multiple roles to a single user. You can also assign the same role to multiple users.

A default set of roles and tasks is included with iManager 1.5.2. You can use the default set or customize them to your liking.

Role Based Services is represented by objects defined in eDirectory. The base eDirectory schema gets extended while running the iManager Configuration Wizard. The new object types are listed in the following table.

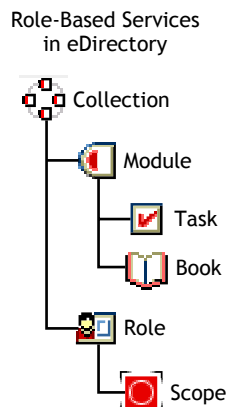
Table 1 **Role-Based Services Objects in eDirectory**

Object	Description
 rbsCollection	A container object that holds all RBS role and module objects.
 rbsRole	<p>Specifies the 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 can be created only in an rbsCollection container.</p>
 rbsTask	<p>Represents a specific function, such as resetting login passwords.</p> <p>rbsTask objects are located only in rbsModule containers.</p>
 rbsScope	<p>Represents the context in the tree where a role will be performed and is associated with rbsRole objects.</p> <p>This object is dynamically created when needed, then automatically deleted when no longer needed.</p> <p>WARNING: Never change the configuration of an rbsScope object. Doing so will have serious consequences and could possibly break the system.</p>

Object	Description
 rbsModule	Holds rbsTask objects. Each module corresponds to a product.

The Role-Based Services objects use the structure within the eDirectory tree as shown in the following figure.

Figure 2 Role-Based Services Objects Grouped in the eDirectory Tree



Installing Roles and Tasks for the First Time

Roles and tasks should be set up by a network administrator using the iManager Configuration Wizard.

The wizard will launch the first time you run iManager. You must be logged in as a user with admin-equivalency since the schema is extended at this time. It will step you through the creation of the Role-Based Services objects and will let you assign roles and tasks to the user that is currently logged in.

You can launch the iManager Configuration Wizard anytime by clicking **Configure > Plug-in Setup and Install > Configure iManager**.


Defining RBS Roles

RBS roles specify the tasks that users are authorized to perform. Defining an RBS role includes creating an rbsRole object and specifying the tasks that the role can perform and the User, Group, or container objects that can perform those tasks. In some cases, Novell iManager plug-ins (product packages) might provide a few predefined RBS roles that you can modify.

The tasks that RBS roles can perform are exposed as rbsTask objects in your eDirectory tree. These objects are added automatically during the installation of product packages. They are organized into one or more rbsModules, which are containers that correspond to the different functional modules of the product.

For information on assigning members to a role, see “Assigning RBS Role Membership and Scope” on page 20.

Creating an rbsRole Object

- 1** Verify that you are logged in as the owner of the rbsCollection you are creating this role in.
- 2** Click the Configure button .
- 3** Specify Role Configuration > Create iManager Role.
- 4** Enter a name for the role in the Role Name field.
- 5** Specify an rbsCollection to hold the object in the Collection field.
rbsRoles can be created only in an rbsCollection container.
- 6** (Optional) Enter a description for the role in the Description field.
- 7** Click Next.
- 8** Specify the tasks you want assigned to this role, then click Next.
- 9** Specify the name and context of the object (a User, Group, or container object) you want this role to be associated with, then click Add.

You can add as many users, groups, or containers as you want.

- 10** Add members.
- 11** Define the scope (i.e., areas of the tree where the role can be performed).

You can assign multiple objects to the same scope, or you can assign individual scopes for each object.


Uncheck the Inheritable check box if you want this role to be performed only in this context. If this box is checked, anyone who is a member of this role will be able to execute tasks in this container and its sub-containers.

- 12** Click Add.
- 13** Repeat Step 10 and Step 11 for each object you added in Step 9.
- 14** Click Next > Finish.

See “Assigning RBS Role Membership and Scope” on page 20 for information on adding members to roles.

Modifying the Tasks That rbsRole Objects Can Perform

Each RBS role has a set of available tasks associated with it. You can choose which tasks are assigned to a particular role, adding or removing tasks as necessary.

- 1** Click the Configure button .
- 2** Click Role Configuration > Modify iManager Roles.
- 3** Click the Modify Tasks button in the role you want to modify.
- 4** Add or remove tasks from the Assigned Task list.
- 5** Click OK.

Deleting a Pre-defined Role

If a predefined Role such as eDirectory Administration, Group Management, etc. is deleted using the Delete Role task, and then recreated by re-installing the iManager plug-in using the Install

plug-in task, the Role is recreated but no tasks are assigned to the Role. The Role should be recreated with all of the default tasks assigned to the Role.

Assigning RBS Role Membership and Scope

After you have defined the RBS roles needed in your organization, you can assign members to each role. In doing so, you specify the scope in which each member can exercise the functions of the role.

The scope is the location or context in the eDirectory tree where this role can be performed. Some tasks require multiple objects to be managed. In these cases you will need to assign a scope high enough in the tree to encompass all objects or make two associations with different scopes that will encompass all objects.

Roles can have the following members:

- ◆ User
- ◆ Group


You can create a Group object, assign Users to the Group, then associate the Group with the role. Every User object in the Group object is then automatically associated with that role. Groups or containers in the Group object are not associated with the role, however.

- ◆ Container

Associating an Organization or Organizational Unit object with a role automatically assigns every user in those containers to the role.

With this method, there is no way to exclude specific users in those containers from the role assignment.

A member can perform multiple roles and tasks. You can also assign the same task to multiple members.

- 1** Click the Configure button .
- 2** Click Role Configuration > Modify iManager Roles.
- 3** Click the Modify Members button in the role you want to modify.
- 4** Specify an object name (a User, Group, or container object) in the Name field, then click Add.
To assign this role to multiple objects, repeat this step as many times as necessary.
- 5** To assign the same scope to multiple members, select the names of all the members you want to have this scope in the Name column.
- 6** Specify a scope (Organization or Organizational Unit object name and context) in the Scope field for a selected name, then click Add.
Every object name you add must have a scope to designate the context in the tree that will be affected by that object.
- 7** Click OK.

User Self-Management

Novell iManager allows administrators to set up *user self-management* so users in the network can modify their own personal information when they are authenticated to the network as themselves.

User self-management is enabled with the [This] special trustee name in eDirectory. [This] is a special eDirectory trustee name that allows you to modify attributes on the authenticated object only.

The **Provider.eMFrame.This.enable=** flag in the eMFrame.cfg file must be set to "true" in order to enable user self-management. This file is located in the \$TOMCAT_HOME/webapps/eMFrame/WEB-INF directory.

To enable user self-management:

- 1** Make sure eGuide 2.1 is installed.

eGuide 2.1 software can be downloaded for free from the Novell download site (<http://download.novell.com>). It is also available on the eDirectory 8.7 WebApps CD.

- 2** Make sure eDirectory 8.7 is installed.

WARNING: User self-management will work only on eDirectory versions 8.6 and later. We recommend that you upgrade to version 8.7 before setting up user self-management.

Modifying the eMFrame.cfg file as described in this section will cause serious problems if you are not running eDirectory 8.6 or later on every server in your eDirectory tree.

- 3** Open the eMFrame.cfg file located in the eMFrame\web-inf directory on the web/middleware server where iManager was installed.

- 4** Find the following statement:

```
Provider.eMFrame.This.enable=false
```

- 5** Replace false with true.

- 6** Save the eMFrame.cfg file.

- 7** On the Web/middleware server where iManager is installed, then stop and restart the Tomcat servlet container.

- 8** In iManager, configure tasks and assign the eGuide self-management role to one or more containers in the tree.

NOTE: You can only assign the eGuide self-management role to Container objects, not User objects.

- 8a** Install the eGuide Configuration plug-in, if necessary by going to Configure > Plug-in Setup and Install > Install Plug-in.

NOTE: The eGuide Configuration plug-in can be installed to multiple RBS Collections if multiple eGuide Self-Management roles are needed.

- 8b** Click on the Role Configuration > Modify eGuide Roles task.

- 8c** On the Modify eGuide Roles page, find the eGuide Self-Management role.

- 8d** Click on the Modify Tasks button next to this role in order to add or remove tasks from the role.

You can also click on the Modify Members button that is next to this role in order to add or remove containers from the role.

All User objects in the container will inherit the ability to modify attributes on their own objects according to the tasks in the role.

Using Property Books

iManager also uses property books as used in the ConsoleOne™ utility. Property books can assist in the viewing and management of a large number of attributes.

Creating a Property Book

- 1** Create a new role that will hold the property book.
- 2** Create a property book.
 - 2a** Select name and rbsModule.
 - 2b** Select the objects that this property book will manage.
 - 2c** Select the individual attribute pages this property book will manage.

Example

In the Group Management > Modify Group task, there are two tabs: General and Security.

Under the General tab are three items: Identification, See Also, and Members.

Under the Security tab is one item: Security equal to me.

Any user that is an assigned member of the Modify Group task can administer these four items on any group within the eDirectory scope defined.

For some organizations that use a decentralized approach to administration, this level of responsibility assignment is not granular enough. This is where property books can be utilized to define administration responsibilities in a granular manner.

For example, you might want to allow certain users to only be able to modify the members of a group and not be able to modify the group identification information or security equivalent settings. To accomplish this

- 1** Create a role called "Group User Admin." Do not assign any tasks to the role when prompted. Assign members and scopes.
- 2** Create a new property book called "Group Users."
- 3** Select an rbsModule.
- 4** Select the objects the property book will manage.
- 5** Select the pages to assign to the property book. The pages that appear are dependent on what objects were selected. Only select "manageGroupUsersPage."
- 6** Assign the property book to the Group User Admin role you just created.
- 7** Select Finish.

Now, when a user assigned to the Group User Admin role logs in and selects this role, they will see the property book "Group Users." Selecting this and entering a group to manage will only allow the user to administer the group users and no other pages related to the Group Management role.

5

Dynamic Groups

A dynamic group can use an LDAP search filter to populate its 'member' attribute. Traditional or static groups require the 'member' attribute to be populated manually. A dynamic group, on the other hand, can use an LDAP URL to assign all users with a Title attribute of "IS" to its membership list. Members can be specified by a Filter on a Dynamic Group object, in addition to explicit members.

You can use the Dynamic Group Management role in Novell iManager to create and modify Dynamic Group objects. Dynamic Groups are supported with eDirectory 8.6 and above.

To make a dynamic group work properly after creation:

- 1 Setup SSL for LDAP connections.

For more information, see "Configuring and Using SSL for LDAP Connections" (<http://www.novell.com/documentation/lg/imanage15/index.html?page=/documentation/lg/imanage15/imanage/data/adbcvpt.html>) in the *iManager 1.5.2 Administration Guide*.

Alternately, if you want to use clear text passwords for LDAP communication: Run iManager, click the Roles and Tasks button > LDAP Management > LDAP Overview > View LDAP Group Objects > click on an LDAP Group object > click Information. Uncheck "Require TLS for Simple Binds with Password". Do this for each LDAP Group object in the tree.

- 2 In Novell iManager, click the Roles and Tasks button.

- 3 Click Dynamic Group Management > Modify Dynamic Group.

- 4 Specify the name and context of the Dynamic Group object you want to modify.

- 5 Enter the appropriate information on the Modify Dynamic Group page.

There are default values for the Identity object, Base dn, and Filter fields:

Identity object = [Public]

Base dn = [root]

Filter = (objectClass=*)

If nothing is entered in these fields, these default values will automatically be used. You will not be able to see a default value for Base dn or Filter. Leaving everything set to the default values will add every object in your tree as a member of this dynamic group. You can verify this by selecting the Unique member list, which will show you the current members of the dynamic group based on the filter that is set and any members that were explicitly added.

- 6 Set the Base dn to the search base. The search base is the point at which you want to begin searching for dynamic group members based on the Filter you have entered.

- 7 Set the Identity object or accept the default.

NOTE: [Public] may not have sufficient rights to read and compare attributes. 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. To perform a search, the server has to use a specific identity so that the results will always be consistent. The Identity object should have a password set so that the server can authenticate as the

Identity object. The Identity object must have sufficient rights to the Base dn level and below to determine dynamic group membership.

- 8** Specify a filter with the Advanced Selector or by typing one in.

For an overview of using dynamic groups with eDirectory, see the April 2002 edition (<http://developer.novell.com/research/appnotes/2002/april/05/a020405.htm>) of *Novell AppNotes*®.

A

Additional Resources

For more information on Novell® iManager, refer to the following Web sites.

Web Services

- ♦ Apache HTTP server (<http://httpd.apache.org>)
- ♦ Tomcat servlet container (<http://jakarta.apache.org/tomcat>)
- ♦ Java 2 Platform, Standard Edition, version 1.3 (<http://java.sun.com/j2se/1.3>)
- ♦ Windows Web Services (<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/iis/default.asp>)
- ♦ Novell eDirectory™ Cool Solutions community (<http://www.novell.com/coolsolutions/nds>)

eDirectory

- ♦ Novell eDirectory product home page (<http://www.novell.com/products/edirectory>)
- ♦ Novell eDirectory product documentation (<http://www.novell.com/documentation>)
- ♦ Novell eDirectory Cool Solutions community (<http://www.novell.com/coolsolutions/nds>)

B

The eDirectory Management Toolbox

The Novell® eDirectory™ Management Toolbox (eMBox) lets you access all of the eDirectory backend utilities remotely as well as on the server. eMBox works with Novell iManager to provide Web-based access to eDirectory utilities such as DSRepair and DSMerge. It also includes Web-based access to the new Backup and Restore and Service Manager functionalities.

All functions are accessible, either on the local server or remotely, through a command line client.

For all eDirectory Management Tools (eMTools)—such as Backup, DSRepair, DSMerge, Schema Operations, and eDirectory Service Manager—to run, eMBox must be loaded and running on the eDirectory server.

You can perform tasks for multiple servers from one server or workstation using the eMBox Client.

The eDirectory Maintenance role in iManager also has access to the eMTools.

In this section:

- ♦ “Using the eMBox Command Line Client” on page 27
- ♦ “Using the eMBox Logger” on page 36

Using the eMBox Command Line Client

One way to access eMBox is to use its Java command line client. The command line client has two modes: interactive and batch. In the interactive mode, you run the eMBox commands one at a time. In the batch mode, you can run a group of commands unattended. The command line client has logging service for both modes.

The command line client is a Java application. To run it, you must have access to the Java Runtime Environment, which is installed with eDirectory. You must also have access behind the firewall to the servers you want to manage. You can perform tasks for multiple servers from one server or workstation.

In this section:

- ♦ “Displaying the Command Line Help” on page 28
- ♦ “Running the eMBox Command Line Client in Interactive Mode” on page 28
- ♦ “Running the eMBox Command Line Client in Batch Mode” on page 32
- ♦ “eMBox Command Line Client Options” on page 33
- ♦ “Establishing a Secure Connection with the eMBox Client” on page 34
- ♦ “Finding Out eDirectory Port Numbers” on page 35

Displaying the Command Line Help

To display the eMBox general command line help before going in to the eMBox Client, do the following:

- ♦ NetWare and UNIX: At the command line, enter **edirutil -?**.
- ♦ Windows: Run
drive\novell\nds\embox\edirutil.exe -?

To display the eMBox interactive command line help while you are in the interactive mode, at the eMBox Client prompt enter a question mark (?). For example,
eMBox Client> ?

The help displays information on the command-line options like the information in “eMBox Command Line Client Options” on page 33.

Running the eMBox Command Line Client in Interactive Mode

Interactive mode lets you run eMBox commands one at a time.

In this section:

- ♦ “Running the eMBox Client on an eDirectory Server” on page 28
- ♦ “Running the eMBox Client on a Workstation” on page 28
- ♦ “Logging In to a Server” on page 30
- ♦ “Setting Preferred Languages, Timeout, and Log File” on page 30
- ♦ “Listing eMTools and Their Services” on page 30
- ♦ “Running a Particular Service” on page 31
- ♦ “Logging Out From the Current Server” on page 31
- ♦ “Exiting the Client” on page 32

Running the eMBox Client on an eDirectory Server

The eMBox Client and the Sun JVM 1.3.1 are installed with eDirectory. To open the eMBox Client in interactive mode on an eDirectory server, do the following:

- ♦ NetWare and UNIX: At the command line, enter **edirutil -i**.
- ♦ Windows: Run
drive\novell\nds\embox\edirutil.exe -i

The edirutil file gives you a shortcut to running the eMBox Client. It points to the Java executable and the default location where the eMBox Client is installed with eDirectory, and for NetWare, it includes the necessary -ns option (which is a Java option on NetWare meaning “new screen”). (You can also enter the information manually, as described in “Setting Up the Path and Classpath for eMBox Client” on page 29.)

You must have access behind the firewall to use the eMBox command line client for the servers you want to manage—so if you are remote, you’ll need VPN access.

Running the eMBox Client on a Workstation

To use the eMBox Client on a machine other than an eDirectory server:

- ♦ Copy the eMBoxClient.jar file from an eDirectory server to your machine.
 - ♦ NetWare: sys:\system\embox\eMBoxClient.jar
 - ♦ Windows: \novell\nds\embox\eMBoxClient.jar
 - ♦ UNIX: /usr/lib/nds-modules/embox/eMBoxClient.jar
- ♦ Make sure the machine has the Sun JVM 1.3.1 installed.
- ♦ Make sure you have access behind the firewall to use the eMBox command line client for the servers you want to manage.

You can't use the edirutil command on a workstation as a shortcut to getting in to the eMBox Client in interactive mode as you can on a server. You must either set up the environment once in your path and class path, or enter it manually each time. See "Setting Up the Path and Classpath for eMBox Client" on page 29.

Setting Up the Path and Classpath for eMBox Client

If you are running the eMBox Client on an eDirectory server and have not changed the location of Java or the eMBoxClient.jar file, you can use edirutil as a shortcut to running the eMBox Client. (See "Running the eMBox Client on an eDirectory Server" on page 28.)

But if you have changed the default locations, or you are running the eMBoxClient.jar file on a machine that is not a server, or you wish to enter the classpath manually, you need to set up the path and classpath for the eMBox Client as explained in this section.

You can run the eMBox Client from anywhere on your machine if you do the following:

- ♦ Add to your path the directory where the Java executable (for example, java.exe) is located, or make sure that Java is already running.

If you are on a server, this is probably already done for you. On Windows and UNIX servers, the directory needs to be in your path. On NetWare, instead of adding the directory to a path, Java needs to be running.

On a workstation, you might need to set it up yourself. For example, on Windows, click Start > Settings > Control Panel > System. On the Advanced tab, click Environment Variables and add the path to the Path variable.

To enter this manually: If the path to the Java executable has not been added to your path, at the command line you will need to first change to the directory containing the Java executable before running embox. For example, on Windows enter

```
cd c:\novell\nds\embox\jre\bin
```

- ♦ Add the path to the eMBoxClient.jar file to your classpath.

NetWare server:

```
set ENVSET=path\eMBoxClient.jar
```

Windows server or workstation:

```
set CLASSPATH=path\eMBoxClient.jar
```

UNIX server or workstation:

```
export CLASSPATH=path/eMBoxClient.jar
```

To enter this manually: An alternative way to specify the classpath is to use the -cp flag for Java each time you want to run eMBox:

```
java -cp path/eMBoxClient.jar embox -i
```

For example, on Windows enter

```
java -cp c:\novell\nds\embox\emBoxClient.jar embox -i
```

WARNING: On a NetWare server only, to avoid an abend you *must* include `-ns` (a Java option on NetWare for “new screen”). For example,

```
java -ns -cp sys:\system\embox\emBoxClient.jar embox -i
```

After doing both of these steps, you can run the client in interactive mode from anywhere on your machine using the following command:

```
java embox -i
```

WARNING: On a NetWare server only, to avoid an abend you *must* include `-ns` (a Java option on NetWare for “new screen”). For example,

```
java -ns embox -i
```

For information on Java commands, see the Java documentation on the Sun Web site (<http://java.sun.com>).

Logging In to a Server

To log in to a server, you need to specify the server name or IP address and the port number to connect to a particular server. A username and password are not needed for public logins.

For example, after opening the eMBox Client in interactive mode, enter:

```
login -s 137.65.123.244 -p 8008 -u admin.mycompany -w mypassword -n
```

For more information, see “Finding Out eDirectory Port Numbers” on page 35.

Setting Preferred Languages, Timeout, and Log File

The default language is the client system language, so in most cases you won't need to explicitly set a language. Similarly, the default timeout should work in most cases. To set the log file, specify the filename and the mode for opening it (append or overwrite).

See the following table for sample commands.

Command	Description
<code>set -L en,de</code>	Sets the language preference to English and German (in that order).
<code>set -T 100</code>	Sets the timeout to 100 seconds. The timeout setting specifies how long to wait for responses from the server.
<code>set -l mylog.txt -o</code>	Uses mylog.txt as the log file and overwrites when opening it.
	Default=append

Listing eMTools and Their Services

After logging in to a server, you can use the `list` command to display a list of the services available on that server.

The `list` command displays the following eMTools and their services dynamically:

eMTool	Description
backup	Novell eDirectory Backup eMTool
dsmerge	Novell eDirectory Merge eMTool
dsrepair	Novell eDirectory Repair eMTool
dsschema	Novell eDirectory Schema Operations eMTool
service	Novell eDirectory Service Manager eMTool

Use `-r` to force the refresh of the list. Use `-t` to list service details. Use `-f` to list just the command format.

See the following table for sample commands.

Command	Description
<code>list</code>	Lists the eMTools available on the server .
<code>list -r</code>	Refreshes the eMTool list.
<code>list -t backup</code>	Lists Backup services with details.
<code>list -t dsrepair</code>	Lists DSRepair services with details.
<code>list -t dsmerge -f</code>	Lists DSMerge services with command formats only.

Running a Particular Service

You can perform tasks using each of the eMTool services after you have logged in to a server. For example:

Command	Description
<code>dsrepair.rld</code>	Repair local database.
<code>backup.getconfig</code>	Get backup configuration information.

For more information, see the *eDirectory 8.7 Administration Guide* on the Novell documentation web site (<http://www.novell.com/documentation>).

Logging Out From the Current Server

To log out from the current session, use the following command:

logout

If you log in to a different server, you don't need to use this command; you are automatically logged out of the current server.

Exiting the Client

To exit the client, use either of the following commands:

exit

or

quit

Running the eMBox Command Line Client in Batch Mode

There are three ways you can run the eMBox Client in batch mode:

- ♦ “Single Tasks” on page 32
- ♦ “Internal Batch File” on page 32
- ♦ “System Batch File” on page 33

You can use a combination of the system and internal batch files for more flexibility and for organizing and reusing commands that you run often.

Single Tasks

You can perform a single eMBox task in batch mode at the command line, simply by entering the command using the **-t** option to specify the tool and task, and omitting the **-i** option (**-i** specifies interactive mode). For example,

```
java embox -s 137.65.123.244 -p 8008 -u admin.mycompany -w mypassword -l  
mylog.txt -t dsrepair.rld
```

For multiple tasks on different servers, or for tasks you perform often, a better alternative is to use an internal batch file. For more information, see “Internal Batch File” on page 32 below.

Internal Batch File

To run the eMBox Client in batch mode using an eMBox Client internal batch file, you need to create a file which contains a group of eMBox commands you would run in the interactive mode.

An eMBox Client internal batch file lets you run all the commands in the batch file without your attention. You can perform multiple tasks with multiple eMBox tools on the same server without having to log in and log out again for each task. From one server, you can also perform tasks with multiple eMBox tools on multiple servers.

Internal batch files can help you organize and reuse commands that you perform often, so you don’t have to enter them manually at the command line each time.

You can go to the command line and run the internal batch file using an eMBox Client command. For example, this command would log in to a server and run the commands listed in the **mybatch.mbx** file:

```
java embox -s 137.65.123.244 -p 8008 -u admin.mycompany -w mypassword -l  
mylog.txt -o -b mybatch.mbx -n
```

WARNING: On NetWare only, to avoid anabend you *must* include **-ns** (a Java option on NetWare for “new screen”). For example,

```
java -ns embox -s 137.65.123.244 -p 8008 -u admin.mycompany -w mypassword -l mylog.txt  
-o -b mybatch.mbx -n
```


Another option is to put the same kind of command in a system batch file, so that you can schedule it to run on the server unattended. See “System Batch File” on page 33 below.

Here is an example of an eMBox internal batch file. It contains examples of the commands you could run and an example of logging in to a different server. This example assumes that you logged in to a server when you opened the eMBox Client. (Each command must be on a separate line. Lines beginning with # are comments.)

```
# This file is named mybatch.mbx.
# This is an example of commands you could use in
# an eMBox internal command batch file.

# Backup commands
backup.getconfig
backup.backup -b -f mybackup.bak -l backup.log -t -e -w

# DSRepair commands
dsrepair.rld

# Log in to a different server
login -s 137.65.123.255 -p 8008 -u admin.mycompany -w mypassword -n

# DSMerge commands
dsmerge.pr -u admin.mycompany -p admin.mycompany -n mypassword

# Schema Operations
dsschema.rst
dsschema.dse
dsschema.rls
dsschema.gsu
dsschema.scc
dsschema.irs -n LocalTree

# DSService commands
service.serviceList

# End of example.
```

System Batch File

As with other command line tools, you can create system batch files containing eMBox Client commands and run them manually at the command line or schedule them to run on the server unattended.

From one server, you can perform tasks with multiple eMBox tools on multiple servers.

In a system batch file, you can use a combination of eMBox Client single commands and internal batch files for more flexibility and for organizing and reusing commands that you run often. For more information, see “Internal Batch File” on page 32 above.

eMBox Command Line Client Options

Option	Description
-? or -h	Display help information
-i	Interactively run eMBox commands one at a time.

Option	Description
-s <i>server</i>	Name or IP address of the eMBox server. Default=127.0.0.1
-p <i>port</i>	Port number of the eMBox server. Default=80
-u <i>user</i>	User DN. For example, admin.mycompany. Default=anonymous
-w <i>password</i>	Password associated with the user specified with -u.
-m <i>mode</i>	Login mode. Default=dclient
-n	Do not try to make a secure SSL connection. Use a nonsecure connection. If you do not use this option, the eMBox Client will try to establish an SSL connection, and you must have the JSSE files in your class path or it will return an error. See "Establishing a Secure Connection with the eMBox Client" on page 34 for more information.
-l <i>log file</i>	Name of the log file.
-o	Overwrite the log file when opening it.
-T <i>timeout</i>	How long (in seconds) to wait for responses from the server.
-L <i>language</i>	List of comma-delimited acceptable languages in order of preference, such as en-US,de_DE. This option defaults to the client system language.
-t [<i>tool.</i>] <i>task options</i>	Perform a single service with this connection. The string following -t should be a valid eMBox command.
-b <i>eMBox batch file</i>	Perform a group of services as specified in the batch file. The eMBox commands in the batch file should be put on separate lines. Lines preceded by # are comments.

Establishing a Secure Connection with the eMBox Client

If you use a nonsecure connection, all the information you enter, such as user names and passwords, is sent over the wire in clear text.

If you instead want to establish a secure connection using SSL, do the following:

- ♦ Make sure you don't use the -n option in your command. It specifies a nonsecure connection. A secure connection is the default.
- ♦ Make sure you have the following Java Secure Socket Extension (JSSE) files in your class path:
 - ♦ jsse.jar

- ♦ jnet.jar
- ♦ jcert.jar

If you don't, the eMBox Client will return an error.

You can get information about JSSE and these files from the Sun Web site (<http://java.sun.com/products/jsse>).

Finding Out eDirectory Port Numbers

When logging in to a server in the eMBox Client, you must specify a port number.

If you specified a port number when you installed eDirectory, use that number.

The default ports are as follows:

- ♦ For NetWare, the default nonsecure port is 8008, and the default secure port is 8009.
- ♦ For other platforms, the default nonsecure port is 80, unless you have a Web server running which is already using that port at the time you install eDirectory. In that case, the nonsecure port is usually 8008. The default secure port is 443.

Below are some additional tips for finding out the port that is assigned to eDirectory:

- ♦ “On Windows” on page 35
- ♦ “On NetWare” on page 35
- ♦ “On UNIX” on page 36

On Windows

- 1 Click Start > Settings > Control Panel.
- 2 Double-click the Novell eDirectory Services icon, then click the Transport tab.
- 3 Look up the secure or nonsecure port.
 - ♦ For the nonsecure port, click the plus sign next to HTTP.
 - ♦ For the secure port, click the plus sign next to HTTPS.

Click the plus sign next to Bound Transports to see the port number.

On NetWare

The Network Address property of a Server object will show you the ports.

You can look up the Network Address property of a server object in the following tools:

- ♦ In iManager, look at the server object using eDirectory Administration > Modify Object, and on the General tab read the drop down list for Network address.
- ♦ In ConsoleOne, right-click the server object or select it and click Object > Properties, and look for the Network Addresses drop-down list.

Look for the network addresses that begin with http: or https: and have “/portal” at the end. These are the nonsecure and secure ports used for eMBox tools.

Here's how to tell what the port number is:

- ♦ If a port number is displayed in the network address, that is the port number that has been assigned.

For example, `http://137.65.188.1:8008/portal` means that a Web server was probably using the default port 80 at the time eDirectory was installed on a non-NetWare platform, so instead port 8008 is being used.

- ◆ If a port number is not displayed, and you see only the IP address for the server, that means the default port numbers are being used.

For example, `https://137.65.188.1/portal` is displaying no port number after the IP address, which means that the default secure portal number is being used for eMBox tools: 8009 on NetWare, 443 on other platforms.

On UNIX

You can use this command to see a list of ports:

```
ndsconfig get | grep http
```

Look for the lines that say `http.server.interface` and then a port number.

You can also look up the port number in iManager or ConsoleOne using the same method described for NetWare. See “On NetWare” on page 35 for more information.

Using the eMBox Logger

The eMBox Logger is an infrastructure module that logs all the events for all the eDirectory Management Tools (eMTools) such as DSBackup, DSMerge, and DSRepair. In this release, only one log file is provided in which all eMTools log their operations.

The eMBox Logger is different than the client logging service, which is provided through the log files that you specify when you run the eMBox client (for example, when you specify `-l mylogfile.txt` in an eMBox client command or when you enter `mylogfile.txt` as a log file name in iManager). The eMBox Logger currently records all server messages for tasks that are performed by the eMBox, showing greater detail. By contrast, the client logging service records client messages and messages sent to the client, which give a general report of progress.

Logging is asynchronous, and all operations are logged by default.

This release of the eMBox Logger provides the following features:

- ◆ The ability to change the log file name and location.

By default, log files are created in the `embox\log` directory located in the same directory that eDirectory was installed in.

- ◆ The ability to change the maximum file size, after which the log file will reset.

The maximum file size is 8 MB.

- ◆ The ability to change the logging mode.

You can choose to append all new messages to the log file or to overwrite an existing log file. The Append option is set by default.

- ◆ The ability to start and stop the logging.

By default, the logger is in Start mode when the eMBox starts up. While in Stop mode, no messages are logged.

- ◆ The ability to reset the log file contents.
- ◆ The ability to read the log file from a client machine.

In This Section

- ♦ “Using the eMBox Logger Command Line Client” on page 37
- ♦ “Using the eMBox Logger Feature in Novell iManager” on page 37

Using the eMBox Logger Command Line Client

The following table lists the eMBox Logger command line client options:

Option	Description
logstart	Starts the eMBox logger.
logstop	Stops the eMBox logger.
readlog	Displays the current log file.
getlogstate	Displays the current state of the eMBox logger (Start/Stop).
getloginfo	Displays the name, logging mode(Append/Overwrite), maximum size and the current size of the eMBox log file.
setloginfo [-f <i>filename</i>] [-s <i>size in Kilo bytes</i>] [-a -o]	Lets you set the name, size, and logging mode (Append/Overwrite) of the eMBox log file using the following parameters: <ul style="list-style-type: none">♦ -f <i>filename</i> The eMBox log file name.♦ -s <i>size in Kilo bytes</i> The maximum size of the log file.♦ -a New log messages will be appended to the current one.♦ -o The log file will be overwritten.
emptylog	Clears the contents of the server log file.

Using the eMBox Logger Feature in Novell iManager

- 1** In Novell iManager, click the Roles and Tasks button.
- 2** Click eDirectory Maintenance Utilities > Log File.
- 3** Specify which server will perform the log file operation, then click Next.
- 4** Authenticate to the server, then click Next.
- 5** Select the log file operation to be performed.
Click Help for details.

C

Configuring and Using SSL for LDAP Connections

Follow these instructions if you want to use SSL connections between Novell® Web-based applications (for example, iManager and eGuide) and an LDAP data source rather than plain- or clear-text connections.

IMPORTANT: SSL connections are slower than plain- or clear-text connections. Using SSL may result in a noticeable degradation in performance.

This procedure varies depending on the server platform you are using (NetWare, Windows, UNIX). The specific platform is indicated under each step.

Step One: Download and Set Up the JSSE Package from Sun Microsystems

On NetWare

If you have NetWare® 6, JDK version 1.4, or iManager 1.5, you should already have the necessary software.

On Windows and UNIX

- 1** Verify if you have Java® Secure Socket Extension (JSSE) package on your server.
- 2** To download the JSSE, access the java.sun.com Web site (<http://java.sun.com/products/jsse>).
- 3** Add the following files to Java's jre\lib\ext folder:
 - ♦ JSSE.JAR
 - ♦ JNET.JAR
 - ♦ JCERT.JAR

Step Two: Set the Provider in the Security Object

On All Platforms

Setting the provider in the security object can be done statically in the security properties file (jre\lib\security\java.security).

To set this provider statically, find the following line in the security properties file:

```
security.provider.1=sun.security.provider.Sun
```

Add the following line immediately after:

```
security.provider.x=com.sun.net.ssl.internal.ssl.Provider
```

where x is equal to the next sequential number (for example, `security.provider.2=com.sun.net.ssl.internal.ssl.Provider`).

IMPORTANT: Both of these lines are required in order for SSL to work correctly.

Step Three: Configure the LDAP Server to Support SSL

On All Platforms

- 1 In iManager, select Roles and Tasks > LDAP Management > LDAP Overview > View LDAP Servers > Select the the desired LDAP Server > Select Connections.
- 2 Select an SSL Certificate object in the Server Certificate field.
NOTE: These objects were created at the time eDirectory™ was installed.
- 3 Make note of the SSL port (typically 636).
- 4 Save your changes.
- 5 Access the LDAP server's properties again and click Refresh on the Information tab.

Step Four: Configure the LDAP Group Object

On All Platforms

- 1 In iManager, select Roles and Tasks > LDAP Management > LDAP Overview > View LDAP Groups > Select the desired LDAP Group > Select information.
- 2 To require TLS, check the Require TLS for Simple Binds with Password checkbox.

Step Five: Export the Trusted Root Certificate

On All Platforms

- 1 In ConsoleOne, access the properties for the SSL Certificate object you just configured.
- 2 Click Certificates > Trusted Root Certificate.
- 3 Click Export and save the file in binary DER format (filename is typically `trustedrootcert.der`).

Step Six: Import the Trusted Root Certificate

For this step, you will need a JDK to use keytool. If a JRE was installed with iManager, you will need to download a JDK to use the keytool.

You now need to import the Trusted Root Certificate into your `cacerts` or `jssecacerts` trust store file.

- 1 Find the `cacerts` or `jssecacerts` file in the `lib\security` folder (relative to your Java home folder).
- 2 Find keytool in the `\bin` folder (relative to your Java home folder).

IMPORTANT: You must use keytool that comes with JVM 1.3 or later. The keytool that comes with JVM 1.2.2 or earlier will not work.

- 3 Execute the following keytool command (platform specific):

On NetWare

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

On Windows

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

On UNIX

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

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

IMPORTANT: You will be prompted for a keystore password. If you haven't changed it, the default is "changeit".

Step Seven: Edit the Tomcat Configuration File

On NetWare

This step is not necessary on NetWare.

On Windows and UNIX

To configure a secure (SSL) HTTP connector for Tomcat, verify that it is activated in the \$TOMCAT_HOME/conf/server.xml file (the standard version of this file, as shipped with Tomcat, contains a simple example which is commented-out by default).

Syntax for Tomcat 3.3:

```
<Http10Connector  
  port="8443"  
  secure="true"  
  keystore="/usr/java/jre/lib/security/cacerts"  
  clientAuth="false" />
```

Step Eight: Modify the eMFrame.cfg File

On All Platforms

- 1 Open the eMFrame.cfg file located in the eMFrame\WEB-INF directory on the Web/middleware server where iManager was installed.
- 2 Find the following statement:

```
Provider.eMFrame.ssl=false
```
- 3 Replace false with true.
- 4 Save and exit the file.
- 5 Restart Tomcat and your web server.

Step Nine (Optional): Configure eGuide to Use SSL

On All Platforms

- 1** From a web browser, open the Novell eGuide Administration Utility.
- 2** Click LDAP Data Sources > Edit (for the appropriate directory) > LDAP Settings.
- 3** Select Enable SSL.
- 4** For Secure Port, type the LDAP server port number you made note of when configuring the LDAP server.
- 5** Click Save.

If you receive an error message or hang when you click Save, go through all of the SSL configuration steps again to make sure the configuration is completely correct. The following are two examples of bad settings that will cause eGuide to hang:

- ♦ Trying to communicate with an SSL port using a plain-text connection
- ♦ Trying to communicate with a plain-text port using an SSL connection