Novell
iManager

2.0.x

ADMINISTRATION GUIDE

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 © 2002-2003 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; 5,652,854; 5,671,414; 5,677,851; 5,692,129; 5,701,459; 5,717,912; 5,758,069; 5,758,344; 5,781,724; 5,781,733; 5,784,560; 5,787,439; 5,818,936; 5,828,882; 5,832,274; 5,832,275; 5,832,483; 5,832,487; 5,859,978; 5,870,561; 5,870,739; 5,873,079; 5,878,415; 5,884,304; 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; 5,956,718; 5,956,745; 5,964,872; 5,974,474; 5,983,223; 5,983,234; 5,987,471; 5,991,810; 6,002,398; 6,014,667; 6,016,499; 6,023,586; 6,029,247; 6,052,724; 6,061,726; 6,061,740; 6,061,743; 6,065,017; 6,081,774; 6,081,814; 6,094,672; 6,098,090; 6,105,062; 6,105,069; 6,105,132; 6,115,039; 6,119,122; 6,144,959; 6,151,688; 6,157,925; 6,167,393; 6,173,289; 6,216,123; 6,219,652; 6,233,859; 6,247,149; 6,269,391; 6,286,010; 6,308,181; 6,314,520; 6,324,670; 6,338,112; 6,345,266; 6,353,898; 6,424,976; 6,466,944; 6,477,583; 6,477,648; 6,484,186; 6,496,865; 6,510,450; 6,516,325; 6,519,610; 6,532,451; 6,532,491; 6,539,381; RE37,178. Patents Pending.

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

www.novell.com

Novell iManager 2.0.x Administration Guide
February 24, 2004

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Contents

About This Guide

This guide describes how to set up and use Novell® iManager 2.0.*x*. The guide is intended for network administrators and is divided into the following sections:

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).

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

For other documentation resources, see "Additional Resources" on page 11.

Documentation Updates

For the most recent version of the *iManager 2.0.x Administration Guide* and the latest readme file, see the Novell iManager documentation Web site (http://www.novell.com/documentation/lg/imanager20).

For information on additional iManager issues for this release, refer to Solution #10089040, titled "Novell iManager 2.0.*x* Readme Addendum," in the Novell Knowledge Base (http://support.novell.com).

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 UNIX*, should use forward slashes as required by your software.

1 Overview

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

iManager includes the following:

- All the functionality of its predecessor, ConsoleOne®
- 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 through a Web browser and various handheld devices
- Role-Based Services (RBS) for delegated administration

iManager is based on Novell exteNd Director™ Standard Edition software, which provides a portal through which iManager presents its interface. iManager functionality can be extended through software components called plug-ins. Many plug-ins are provided with iManager, and others are available from third parties.

New for 2.0.*x*

iManager 2.0.*x* includes the following new and upgraded features:

- Support for NetWare, Linux*, Windows*, Solaris* and HP-UX*
- New Plug-in Studio for custom task creation
- Expanded browser support, including Netscape* 7.1 and Mozilla 1.4
- iManager Migration Kit for moving custom tasks from iManager 1.*x* to 2.*x*
- Improved speed and performance

Additional Resources

For more information on topics relevant to Novell iManager 2.0.*x*, 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)

What's Next

- To install iManager, see Chapter 2, "Installing iManager," on page 13.
- To start the iManager program, see Chapter 3, "Accessing iManager," on page 27.
- To set up iManager, see Chapter 7, "Configuring and Customizing iManager," on page 45.

2 Installing iManager

This section includes the following:

Prerequisites

The following prerequisites apply to all platforms. Additional platform-specific prerequisites are listed in the next section by platform.

❑ **Supported Browsers.** To run iManager, you will need a workstation with Internet Explorer 6 SP1 or later (recommended), Netscape 7.1 or later, or Mozilla 1.4 or later installed.

❑ **eDirectory LDAP Server.** You must have a Novell® eDirectory™ LDAP server in a secure configuration. If eDirectory is on a different machine than iManager, the configuration of the iManager portal (typically performed during the installation) prompts you for credentials to perform and LDAP bind to a server in the tree. The server must have eDirectory 8.6.2 or later installed.

❑ **Admin-Equivalent Rights.** For the initial installation of iManager into the eDirectory tree, you must have admin-equivalent rights to run the iManager Configuration Wizard. For subsequent installations, you must have container admin rights.

❑ **Server Memory.** You must have a minimum of 512 MB of RAM in the server where you are installing iManager. 1024 MB is recommended.

❑ **Port Setup.** To avoid port conflicts, find out which ports are in use on the server where you will install iManager and determine whether they will conflict with ports used by iManager. Versions of Apache and Tomcat installed with iManager attempt to use ports 80, 443, 8009, 8080, 8005. If these ports are in use by another service, such as eDirectory, a problem is likely. See the installation instructions for each platform for more information.

Installing a New Version of iManager

Novell iManager 2.0.2 can be installed on the platforms covered in this section. In general, you should apply the latest service packs for your platform and have met the prerequisites listed in the preceding section before installing iManager. This section provides instructions for installing iMangager on the following platforms:

- ◆ Installing iManager on Windows 2000/XP/2003 (page 16)
- ◆ Installing iManager on Linux (page 17)
- ◆ Installing iManager on Solaris (page 19)
- ◆ Installing iManager on HP-UX (page 20)

IMPORTANT: The instructions in this guide do not apply when installing iManager with Novell Nterprise™ Linux Services. Please follow the prerequisites and installation instructions provided in the Novell Nterprise Linux Services Installation Guide (http://www.novell.com/documentation/lg/nnls/install/data/front.html).

Installing iManager on NetWare 6.5

You can install iManager 2.0.x from the NetWare® 6.5 product CD or from a standalone installation file.

Prerequisites

In addition to the general prerequisites listed in "Prerequisites" on page 13, the following prerequisites apply to iManager on NetWare 6.5:

- ❑ NetWare 6.5 server (iManager 2.0.2 is supported on Support Pack 1 or later only)
- ❑ eDirectory 8.7.1 or later
- ❑ Novell JVM 1.4.1 or later installed

Procedure

iManager 2.0.*x* is installed with the NetWare 6.5 installation program. For more information, see the *NetWare 6.5 Overview and Installation Guide* (http://www.novell.com/documentation/lg/nw65/index.html?page=/documentation/lg/nw65/install/data/hz8pck9v.html). If you have already installed NetWare 6.5 without iManager, you can install the program separately using the NetWare 6.5 product CD.

NOTE: The NetWare 6.5 SP1 CDs are required to install iManager 2.0.2.

To install iManager using the NetWare 6.5 product CD:

1 Verify that LDAP SSL is running. Run TCPCON from the NetWare console. Select Protocol Information > TCP > TCP Connections. Verify that port 636 is shown in the list of open ports.

2 Run PKI Diag Utility (PKIDIAG). For more information, see Technical Information Document #2963420 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/2963420.htm).

3 Insert the *Products* CD (disk 2) from the NetWare 6.5 product CD set.

4 From the NetWare 6.5 GUI, click the Novell button, then select Install > Add.

5 Browse for the postinst.ni file located on the *Products* CD.

6 Select iManager 2.0.*x*.

7 Follow the on-screen instructions.

Installing iManager on NetWare 6

Prerequisites

In addition to the general prerequisites listed in "Prerequisites" on page 13, the following prerequisites apply to iManager on NetWare 6.0:

- ❑ NetWare 6 server with Support Pack 3 or later installed

    NOTE: NetWare 5.1 is not supported.

- ❑ eDirectory 8.7.1 or later

- ❑ Novell JVM 1.4.1 or later installed

- ❑ Tomcat 3.3

- ❑ Tomcat 4 (included in the iManager 2.0.x installation program for NetWare 6.0)

- ❑ Web services

    Apache 1.3 HTTP server (installed with NetWare 6)

    NOTE: Apache 2.0 is not supported.

- ❑ 200 MB of disk space for a local installation

Procedure

1 Determine whether Tomcat 3.3 is listening on port 8080 (for Tomcat 3.3, this is disabled by default, but may have been enabled for debugging purposes). If the port is enabled, disable it by commenting out the Http10Interceptor tag in sys:\tomcat\33\nwserver.xml, then restart Tomcat 3.3 (at the command NetWare command prompt, type **tomcat stop** followed by **tomcat33**).

2 Verify that LDAP SSL is running. Run TCPCON from the NetWare console. Select Protocol Information > TCP > TCP Connections. Verify that port 636 is shown in the list of open ports.

3 Run PKI Diag Utility (PKIDIAG). For more information, see Technical Information Document #2963420 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/2963420.htm).

4 Verify that there is adequate disk space on the volume. You will need approximately 200 MB of free disk space.

5 Verify that Tomcat 3.3 is installed. The server should have a sys:\tomcat\33\ folder, and when you type JAVA -SHOW at the NetWare command line, org.apache.tomcat.startup.Main should appear in the list of Java processes.

6 Determine the ports that Apache is listening on. Open the sys:\Apache\conf\adminserv.conf file and find the following line:

    # Start Apache Services Port Configuration

    Note the ports for both HTTP and HTTPS (Listen and SecureListen directives).

7 Download the iMan_20x_NW60.exe file from Novell Product Downloads (http://download.novell.com).

8 Create a directory on your server (for example, sys:\imanager202).

9 Run the iMan_20x_NW60.exe file and extract its contents to the directory you've created on the sys: volume on your NetWare 6 server.

10 From the NetWare 6 GUI, click the Novell button, then select Install > Add.

11 Select the product.ni file (that was copied to the directory on the sys: volume) for iManager 2.0.x and complete the installation program.

12 (iManager 2.0.1 only) Modify the sys:\tomcat\4\webapps\nps\WEB-INF\PortalServlet.properties file. Find the line Custom_Backend_Renderer_Portal_Location=http\://127.0.0.1/nps. Replace 127.0.0.1 with the actual IP address and non-secure HTTP port (see Step 6) of the Web server where iManager is running.

If there are problems with the back end renderer location, you might encounter a blank screen when attempting to access iManager. One troubleshooting technique that may be useful is to turn off XML rendering in the URL, for example:

`https://IP:SecureListen port/nps/servlet/portal?render=off`

For more information on the back end renderer blank screen condition, see Technical Information Document #10070553 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10070553.htm).

13 Modify the connector redirect ports in server.xml.

    13a Open the sys:\tomcat\4\conf\server.xml file.

    13b Find the Connector element that defines the HTTP/1.1 connector. The port is typically set to 8080. Change the redirectPort attribute from the default of 8443 to the port number you found in Step 6.

    13c Find the Connector element that defines the AJP 1.3 connector. The port is typically set to 9009. Change the redirectPort attribute from the default of 8443 to the port number you found in Step 6.

    13d Save your changes to server.xml and close the file.

14 Restart Tomcat 4. Type **`TC4STOP`** at the NetWare console and wait for Tomcat to stop (the logger screen shows "java: Class org.apache.catalina.startup.Bootstrap exited successfully" when Tomcat 4 is down). Type **`TOMCAT4`** to restart Tomcat.

15 Open a Web browser and connect to iManager at the port discovered in Step 6. For example:

https://*IP*:*SecureListen port*/nps/iManager.html

Installing iManager on Windows 2000/XP/2003

Prerequisites

In addition to the general prerequisites listed in "Prerequisites" on page 13, the following prerequisites apply to iManager on Windows:

❑ Windows* 2000 Server, 2000 Advanced Server, 2000 Professional, XP Professional, or 2003 Server with the latest service pack installed

❑ Pentium* III 800 MHz or higher processor

❑ 200 MB of disk space for a local installation

❑ 512 MB of RAM (1024 MB recommended)

❑ eDirectory 8.6.2 or later installed on your Windows server or another available server

❑ Web services

Windows servers can use Apache and Tomcat or Windows Web Services (IIS) and Tomcat. The iManager installation program determines which Web services are already installed. If the Windows server is using IIS and you want to use Apache and Tomcat, you must remove IIS before installing Apache and Tomcat with the iManager installation program. The iManager installation program does not configure IIS to use SSL.

IMPORTANT: iManager 2.0.2 does not support IIS 6 on Windows 2003 Server. Apache 2 is supported on Windows 2003 Server.

The iManager 2.0.1 installation program installs and configures the following items if it does not detect a compatible version:

- Apache 2.0.47 (installed if Apache and IIS are not detected)

- Tomcat 4.1.27

- Sun JVM* 1.4.2_01

- Novell International Cryptographic Infrastructure (NICI) 2.6.0

The iManager 2.0.2 installation program installs and configures the following items if it does not detect a compatible version:

- Apache 2.0.48 (installed if Apache and IIS are not detected)

- Tomcat 4.1.27

- Sun JVM 1.4.2_02

- NICI 2.6.0

If you are installing iManager on the same machine as eDirectory, verify that you have Require TLS for Simple Binds with Password checked on the LDAP Group object for the server that you are using to set up iManager. If this check box is not checked, iManager is installed in non-secure mode and plug-ins that require secure mode will fail.

Procedure

1 Download the iMan_20x_win.exe file from Novell Product Downloads (http://download.novell.com).

2 Run the iMan_20x_win.exe file and extract its contents to a temporary directory.

3 Run iManagerInstall.exe.

4 Follow the on-screen instructions.

5 After the installation completes, your Web server is restarted. You might need to wait several seconds for the Web server to initialize before iManager will be available.

TIP: You can view the debug output of the installation program by holding down the Ctrl key immediately after launching the installer. Continue to hold down the key until a console window appears.

Installing iManager on Linux

IMPORTANT: The instructions in this guide do not apply when installing iManager with Novell Nterprise™ Linux Services. Please follow the prerequisites and installation instructions provided in the Novell Nterprise Linux Services Installation Guide (http://www.novell.com/documentation/lg/nnls/install/data/front.html).

Prerequisites

In addition to the general prerequisites listed in "Prerequisites" on page 13, the following prerequisites apply to iManager on Linux:

❑ SuSE* Linux Enterprise Server 8.*x* (SLES 8 for x86), Red Hat* Linux 8, Red Hat Linux 9, or Red Hat Advanced Server 2.1

❑ Sun JVM 1.4.1 or later installed

❑ Pentium III 800 MHz or higher processor

❑ 360 MB of disk space

❑ Root rights to the Web server

❑ eDirectory setup

If you are installing iManager on a server with eDirectory already installed on it, the eDirectory version needs to be 8.7.1 for iManager 2.0.1 and 8.7.3 for iManager 2.0.2 to avoid conflicts with packages that are shared between both eDirectory and iManager.

If you are installing iManager on a server without eDirectory, you must have eDirectory 8.6.2 or later installed on another available server.

❑ Port setup

Be aware of possible port conflicts. Apache, Tomcat, and a JVM are installed with the iManager installation program, which determines whether port 80 and 443 are in use (for example, eDirectory uses port 80 by default with its HTTP stack). If they are in use, the install prompts you for different ports for Apache to run on. Tomcat ports are not detected. Tomcat uses ports 8080, 8005, and 8009. If another version of Tomcat is running, it is not detected, and a port conflict might occur.

❑ Make sure you have a recent version of gettext on your server. To check if you have gettext, enter the following command from a shell:

`gettext -V`

If gettext exists, the command displays the version number.

If you do not have gettext, you must obtain it from the vendor of your Linux distribution and install it before installing iManager.

IMPORTANT: On Linux, iManager only works with the versions of Apache and Tomcat that are installed with iManager.

Procedure

1 Extract the iMan_20*x*_linux.tgz file to a directory on your server. Use the following command:

`tar -zxvf iMan_202_linux.tgz`

2 Open a shell and change to the *install_directory*/iManager_linux directory.

This path is relative to the directory where you copied or extracted the iManager files.

3 Enter the following command:

`./install.sh`

4 Follow the on-screen prompts. The text within the brackets at the prompt is the default selection. Press Enter to accept the default.

5 When prompted to enter the iManager server addresses or DNS host name, the IP address gets auto-detected.

6 For the admin name, you must use dot notation (for example, cn=admin.o=novell).

7 (Conditional) If you are installing iManager 2.0.1, set the PCO (Portal Configuration Object) password:

   7a In an eDirectory tree with an existing PCO, you need to use the existing password. The password is located in the PortalServlet.properties file located in the TOMCAT_HOME\webapps\nps\WEB-INF directory. Search for the System.Password=[password] field.

   7b To set a new password, make sure you do not use your admin password. The default password is novell. We recommend that you change this password.

8 LDAP server IP address or DNS hostname defaults to the local machine. Make sure you use the IP address of eDirectory LDAP server in the eDirectory tree where you want to install iManager.

9 Launch a supported browser and go to:

https://*server_ip_address*:*port_number*/nps/iManager.html

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

Installing iManager on Solaris

Prerequisites

In addition to the general prerequisites listed in "Prerequisites" on page 13, the following prerequisites apply to iManager on Solaris:

❑ Sun Solaris* 8 or 9 (SPARC* processors only) with the latest patches installed from the SunSolve Web site (http://sunsolve.sun.com)

IMPORTANT: If you are using Solaris 8, make sure that you have installed patch 112438.02 and that the OS version is dated October 2001 or later.

❑ Sun JVM 1.4.1 or later installed

❑ Root rights to Web server

❑ eDirectory setup

If you are installing iManager on a server with eDirectory already installed on it, the eDirectory version needs to be 8.7.1 for iManager 2.0.1 and 8.7.3 for iManager 2.0.2 to avoid conflicts with packages that are shared between both eDirectory and iManager.

If you are installing iManager on a server without eDirectory, you must have eDirectory 8.6.2 or later installed on another available server.

❑ Port setup

Be aware of possible port conflicts. Apache, Tomcat and JVM are installed with the iManager installation program. The iManager installation program looks to see if port 80 or 443 are in use (for example, eDirectory uses port 80 by default with its HTTP stack). If they are in use, the install prompts you for different ports for Apache to run on.

❑ Verify that you have a random device installed

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:

./iManagerInstallSolaris.bin

For text only, enter the following command:

./iManagerInstallSolaris.bin -i console

3 Follow the prompts.

4 Stop and re-start Tomcat, then Apache by entering the following commands:

```
/var/opt/novell/tomcat4/bin/shutdown.sh
/var/opt/novell/tomcat4/bin/startup.sh
/var/opt/novell/httpd/bin/apachectl stop
/var/opt/novell/httpd/bin/apachectl startssl
```

These services are not configured to start at boot-up.

5 Launch a suppored browser and go to:

https://*server_ip_address*:*port_number*/nps/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, because the schema will be extended at this time.

7 To access the Getting Started help screen, open the gettingstarted.html file located in the /var/opt/novell/tomcat4/webapps/nps/help/en/install directory.

Installing iManager on HP-UX

IMPORTANT: You must be ROOT to perform the iManager install and configuration on HP-UX.

Prerequisites

In addition to the general prerequisites listed in "Prerequisites" on page 13, the following prerequisites apply to iManager on HP-UX:

❑ HP-UX 11i operating system with the latest patches installed

Ensure that the OS is updated with patch PHSS_26560. You can download this patch from the HP IT Resource Center Web site (http://www.itrc.hp.com).

❑ PA-RISC 2.0 Processor

❑ 400 MB of disk space

❑ eDirectory setup

If you are installing iManager on a server with eDirectory already installed on it, the eDirectory version needs to be 8.7.1 for iManager 2.0.1 and 8.7.3 for iManager 2.0.2 to avoid conflicts with packages that are shared between both eDirectory and iManager.

If you are installing iManager on a server without eDirectory, you must have eDirectory 8.6.2 or later installed on another available server.

❑ gettext-0.12 installed

You can download the gettext-0.12 depot from the HP-UX Porting and Archive Centre Web site (http://hpux.connect.org.uk/hppd/hpux/Gnu/gettext-0.12).

❑ libiconv-1.9 installed

You can download the libiconv-1.9 depot from the HP-UX Porting and Archive Centre Web site (http://hpux.connect.org.uk/hppd/hpux/Development/Libraries/libiconv-1.9).

❑ Java 2 SDK for HP-UX version 1.4.1.01 or 1.4.1.02 (version 1.4.1.02 recommended)

Procedure

1 Install the HP-UX Web Server Suite version 1.0.06.01 from the HP Software Depot Web site (http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=HPUXWSSUITE). The suite contains the official versions of Apache and Tomcat that are supported for HP-UX. If you are installing iManager 2.0.2, you can update to version 1.0.10.01 after you create a new Apache SSL certificate in Step 4. If you are installing iManager 2.0.1, you must use version 1.0.06.01.

NOTE: The version of openssl (0.9.7b) included with the HP-UX Web Server Suite versions A100901 and A101001 has problems generating certificates through Webmin. Install HP-UX Web Server Suite version A100601, which contains openssl version 0.9.6i, create a new SSL certificate for Apache through Webmin, and then update your HP-UX Web Server Suite to a newer version if you are installing iManager 2.0.2. If you would like to create certificates with openssl through Webmin in the future, back up /opt/hpws/Apache/bin/openssl before updating your HP-UX Web Server Suite from version A100601.

Select the download with all components:

HP-UX Apache-based Web Server
HP-UX Tomcat-based Servlet Engine
HP-UX Webmin-based Admin

2 Install Java 1.4.1_02 from the HP Java for HP-UX Web site (http://www.hp.com/go/java) and update your path to find the new Java.

3 Add and export the following environment variables in the environment setting for the user that will be running Tomcat (usually located in the .bashrc file): JAVA_HOME, CATALINA_HOME, APACHE_HOME, SHLIB_PATH.

For example:

```
JAVA_HOME=/opt/java
APACHE_HOME=/opt/hpws/apache
CATALINA_HOME=/opt/hpws/tomcat
SHLIB_PATH=/usr/lib:/usr/lib/nds-modules:$SHLIB_PATH
export JAVA_HOME APACHE_HOME CATALINA_HOME SHLIB_PATH
```

4 Install a new certificate for Apache. You must complete this step before continuing the installation. The certificate that is installed with Apache on HP-UX does not have the correct information for your server. You can install a certificate that you purchase from a trusted authority or a self-signed certificate.

The Webmin administration tool can generate keys, certificates, and certificate requests for Apache. Webmin is installed with the HP-UX Web Server Suite. For more information, see the HP-UX Web Server Suite documentation, which is accessible from your Apache installation (http://*IP_ADDRESS*). For information on using Webmin to generate keys, certificates, and certificate requests, go to http://*IP_ADDRESS*/hp_docs/faq/#security11.

IMPORTANT: Make sure you use the correct DNS name or IP address for the common name when you create a new certificate.

Copy the certificates to the Apache directory: /opt/hpws/apache/conf/ssl.crt/ and /opt/hpws/apache/conf/ssl.key/.

5 Download the iMan_20*x*_hp.tgz file from Novell Product Downloads (http://download.novell.com).

6 Extract the iMan_20*x*_hp.tgz file (for example, gzip -dc iMan_20*x*_hp.tgz | tar xvf -).

7 Logout or close the terminal session to load the environment variables.

8 Install iManager from the location you extracted the install files:

```
./iManagerInstallHPUX.bin
```

or

```
sh iManagerInstallHPUX.bin
```

For text only, enter the following command:

```
./iManagerInstallHPUX.bin -i console
```

IMPORTANT: The iManager installer detects the HP-UX Web Server Suite. Do not change the install path for iManager.

9 (Optional) If you are having trouble with Apache SSL support or would like to connect on non-secure ports, turn off forcing SSL connections between the browser and the servlet engine. Edit the /opt/hpws/tomcat/webapps/nps/WEB-INF/web.xml file and comment the following lines at the bottom of the file:

```
<!--
<security-constraint>
  <web-resource-collection>
    <web-resource-name>SSL-requiring Area</web-resource-name>
    <url-pattern>/servlet/*</url-pattern>
  </web-resource-collection>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>
-->
```

10 Start Tomcat and Apache. The command you use depends on your iManager configuration:

```
/opt/hpws/tomcat/bin/startup.sh
/opt/hpws/apache/bin/apachectl start
```

or

```
/opt/hpws/apache/bin/apachectl startssl
```

NOTE: Tomcat might take 60 seconds or longer to load before you can access iManager, depending on the performance of your server.

11 Run the extenNd Director™ Configuration Wizard. Follow the instructions in .

Upgrading Your Existing Version of iManager

This section explains how to upgrade your existing version of iManager.

Special Considerations when Upgrading from iManager 1.5.*x*

When you install iManager 2.0.*x*, the installation program leaves all existing 1.*x* (1.2.2 and 1.5.*x*) files in place. If you have set up a Role-Based Services (RBS) collection in 1.*x*, all existing 1.*x* RBS objects will continue to reside in your Novell eDirectory tree.

If you choose to set up RBS using iManager 2.0.*x*, use the iManager Configuration Wizard. By using the Configuration Wizard, you can migrate your 1.*x* RBS collection into your 2.0.*x* RBS collection. After the migration has completed, your 1.*x* RBS collection will still exist but all of existing 1.*x* RBS data will also reside in 2.0.*x*.

IMPORTANT: Before you migrate your 1.*x* RBS collection, you must create placeholders in 2.0.*x* using the same names for the roles and tasks that you used in 1.*x*.

Also, any custom tasks or property book pages created with the 1.*x* Create iManager Task task are not migrated. You can either re-create them using the Plug-In Studio or you can migrate them with a utility that will be made available for download on the Novell Web site.

Third-party roles and property book pages, and those created using the iManager 1.*x* SDK, are not migrated. The iManager 2.0 SDK provides utilities that assist in the migration of these plug-ins to iManager 2.0.*x*.

For more information on the iManager 2.0.*x* Configuration Wizard, see .

Upgrading iManager on Windows

Upgrading from iManager 1.x

The 2.0.*x* installation program checks to determine whether a version of 1.*x* is already installed on the target server. If the 2.0.*x* installation program finds an instance of 1.*x* on the server, it asks you whether you want to remove the older version.

If you choose to remove the 1.*x* version, all of the files in the file system are removed with the exception of any custom files you have created. However, 1.*x* RBS objects are not removed from the eDirectory tree and the schema remains in the same state.

If you choose not to remove the 1.*x* version, the 2.0.*x* installation program quits.

Upgrading from iManager 2.0.1

The 2.0.*x* installation program checks to determine whether a version of 2.0.*x* is already installed on the target server. If the 2.0.*x* installation program finds an instance of 2.0.*x* on the server, it asks you whether you want to remove the older version.

If you choose to remove the earlier 2.0.*x* version, only a portion of the files in the file system are removed. The installation programs asks whether you want to remove all iManager files. If you choose Yes, all iManager files are removed, including custom content. The earlier 2.0.*x* RBS objects are not removed from the eDirectory tree and the schema remains in the same state.

If you choose not to remove the earler 2.0.*x* version, the 2.0.2 installation program quits.

Upgrading iManager on Linux

Upgrading from iManager 1.x

On Linux, there is no application that upgrades iManager 1.*x* to iManager 2.0.*x*. The iManager installation program attempts to detect version 1.*x*. If it finds a previous version, you are prompted to uninstall. The uninstall only removes files; it doesn't remove any custom content on the file system or eDirectory RBS objects. To migrate custom content and objects, use the iManager Migration Wizard and Migration Utility.

Upgrading from iManager 2.0.1

If you are performing an upgrade from version 2.0.1 to 2.0.2, the installer displays "(upgradeable)" next to the components available to install. To upgrade to version 2.0.2:

1 Proceed through the installation as explained in "Installing iManager on Linux" on page 17. The installer will install the iManager 2.0.2 files.

2 Run the iManager Configuration Wizard as explained in "Installing RBS" on page 36.

Upgrading iManager on HP-UX

To upgrade iManager 2.0.1 to 2.0.2, follow instructions for installing HP-UX in "Installing iManager on HP-UX" on page 20. Verify that you have satisfied all installation prerequisites. The iManager installation program automatically detects and installs the components that need to be updated.

Uninstalling iManager

IMPORTANT: When uninstalling iManager 2.0.2 on NetWare, the uninstall program will delete all iManager files, regardless of whether they were installed by the iManager installation program or not. Before running the uninstall on NetWare platforms, make sure to back up any custom content or other special iManager files that you would like to preserve.

There is no specific sequence in which iManager or the associated third-party components must be uninstalled.

There are, of course, ramifications to uninstalling any of them. For example, if you uninstall either the Web server or the servlet container, you will not be able to run iManager. Also, on all platforms except for NetWare (see "Important" above), uninstall will only remove files that it installed in the first place. If there are files that were created by the application, for example, the log files and auto-generated configuration files that are created while Tomcat runs, these will not be deleted by the uninstall because it did not install them.

Likewise, if you have created new files or modified existing files within the directory structure that was originally laid down during the install, these files are not removed by the uninstall. This is a safeguard so that data is not unintentionally deleted when a product is uninstalled.

Uninstalling iManager on NetWare 6.0

IMPORTANT: When uninstalling iManager 2.0.2 on NetWare, the uninstall program will delete all iManager files, regardless of whether they were installed by the iManager installation program or not. Before running the uninstall on NetWare platforms, make sure to back up any custom content or other special iManager files that you would like to preserve.

1 Run the iManager 2.0.*x* uninstall.

    1a In the NetWare GUI, click Novell > Install.

    1b In the installed products list, select iManager 2.0.1 or iManager 2.0.2, then click the Remove button.

    1c (Conditional) If you encounter a fatal error message after running the uninstall the first time, select iManager 2.0.1 or iManager 2.0.2, then click the Remove button again.

2 Reset the iManager 1.*x* URL in Web Manager.

    2a Open sys:\webapps\WebAdmin\servers.xml.

2b Change the AdminUrl on the iManager Service tag back to iManager 1.*x*. Change

AdminUrl='https://$(host)/nps/iManager.html'

to

AdminUrl='https://$(host):2200/eMFrame/iManager.html'

2c Change the id attribute from

id='iManager'

to

id='eMFrame'

3 Remove the iManager Tomcat startup parameters. In the sys:\tomctat\4\bin\tomcat4.ncf file, remove the following lines:

; NetWare iManager Config
setenv CATALINA_OPTS=-server -vm160m -Xmx256m
setenv CATALINA_OPTS=-Xmx256m

4 (iManager 2.0.1 only) Delete the following file and directories:

- SYS:\tomcat\4\webapps\platform.xar

- SYS:\tomcat\4\webapps\nps*

- SYS:\tomcat\4\work\Standalone\localhost\nps*

IMPORTANT: If you have created custom tasks and pages that you would like to save, be sure to back up the sys:\tomcat\4\webapps\nps\packages\Custom.npm file before deleting the webapps\nps\ directory.

Uninstalling iManager on Windows

iManager can be uninstalled from Windows using the Add or Remove Programs applet in the Control Panel. If the iManager installation installed Apache, Tomcat, or NICI, they are listed separately in Add or Remove Programs. You must uninstall each program separately.

WARNING: If eDirectory is installed on the same machine as iManager, NICI might be required to continue to run eDirectory.

When you remove iManager 2.0.*x*, only a portion of the files in the file system are removed. You are asked if you want to remove all iManager files. If you choose Yes, all iManager files are removed, including all custom content. The 2.0.*x* RBS objects are not removed from the eDirectory tree, and the schema remains in the same state.

Uninstalling iManager on Linux

1 Open a shell and go to the iManager_linux directory created when you extracted the installation files from the iMan_20*x*_linux.tgz file.

2 Run the installation script:

./install.sh

3 The script prompts you to install or uninstall. Enter u to uninstall.

4 The script will pause to display the products to uninstall. Enter **a** to uninstall all.

5 When prompted, enter the eDirectory admin credentials.

NOTE: The uninstall procedure does not remove configuration and log files.

Uninstalling iManager on Solaris

1 Log in as root.

2 Run the following command:

`/var/opt/novell/tomcat4/nps/UninstallerData/UninstalliManager`

3 When asked if you want to remove all iManager files, choose Yes if you want to remove all files, including all custom content; otherwise, choose No.

Uninstalling iManager on HP-UX

1 Log in as root.

2 Run the following command:

`/opt/hpws/tomcat/webapps/nps/UninstallerData/`
`UninstalliManager`

3 When asked if you want to remove all iManager files, choose Yes if you want to remove all files, including all custom content; otherwise, choose No.

NOTE: Only some of the files in the file system are removed. The uninstall procedure does not remove iManager 2.0.*x* RBS objects from the eDirectory tree, and the schema remains in the same state.

3 Accessing iManager

This section gives instructions on the following tasks for accessing iManager:

- "Using a Supported Web Browser" on page 27
- "Logging in to iManager" on page 27
- "Accessing iManager with a Screen Reader and Other Accessibility Options" on page 28
- "Logging in to a Different Tree" on page 28

Using a Supported Web Browser

To access iManager, you must use a machine running Internet Explorer 6 SP1 or above, Netscape 7.1 or above, or Mozilla 1.4 or above.

The following issues will occur when using Netscape and Mozilla browsers:

- The tool tips functionality for the iManager buttons might not always work.
- The multi-select feature in iManager cannot be used.
- The object view cannot be used.
- The Repair Through iMonitor task does not work.
- The Install and Upgrade Plug-in task does not work.

Logging in to iManager

To access Novell® iManager:

1 From a supported Web browser (see Using a Supported Web Browser), type the following in the address (URL) field:

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

For example:

```
http://137.65.135.150/nps/iManager.html
```

2 Log in using your username and password.

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

Accessing iManager with a Screen Reader and Other Accessibility Options

iManager includes a "simple" display that can be effectively used with screen readers. To access this display:

1 In a Web browser, type the following in the address (URL) field:

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

For example:

`http://137.65.135.150/nps/Simple.html`

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

You will have access to only 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).

Logging in to a Different Tree

You can log into a different tree from iManager, but when you do, the following restrictions apply:

- Only the Unrestricted Access mode of authentication is available. For more information on available modes, see "Access Modes" on page 30.
- You cannot configure Role-Based Services (RBS).
- eDirectory Maintenance tasks are not available unless RBS has been installed in that tree by iManager 2.0.x.
- iManager Configuration tasks are not available.
- The Monitor button is not available.

To log into a different tree:

1 In iManager, click the Log into a Different Tree button .

2 Enter your login information for the tree, then click Login.

What's Next

- To set up Role-Based Services (RBS), see Chapter 5, "Setting Up Role-Based Services," on page 33.
- To customize iManager, see Chapter 7, "Configuring and Customizing iManager," on page 45.

4 Navigating the iManager Interface

This section describes how to navigate through the Novell® iManager 2.0.*x* interface.

iManager Interface

The following figure describes the iManager interface.

Figure 1   iManager Interface
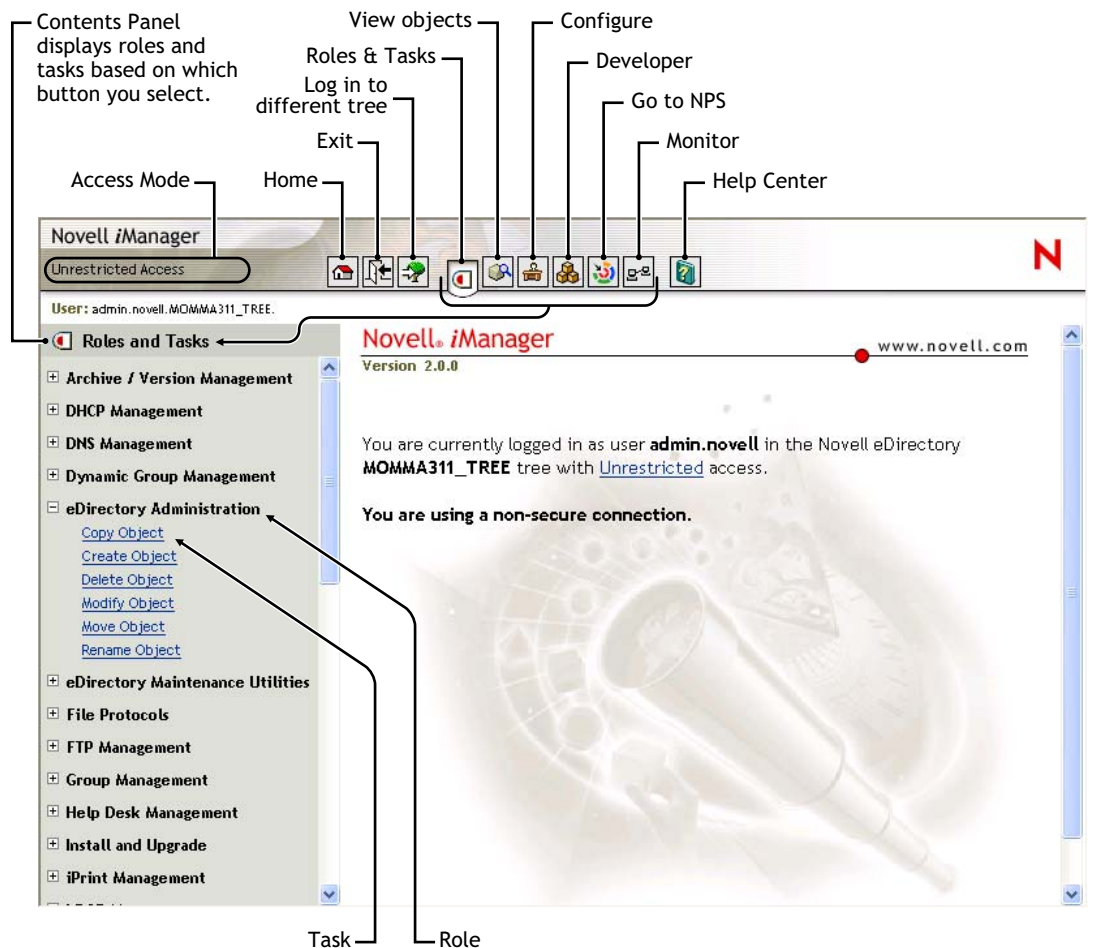
NOTE: When using iManager, make sure to use the buttons (OK, Next, etc.) within the interface. The browser's toolbar buttons (Back, Next, etc.) are not supported in iManager.

Contents Panel

The Contents Panel displays a navigation pane. Its contents vary, depending on which button is selected from the tool bar.

When the Roles and Tasks ⬜, Configure ⬜, Favorites ⬜, or Developer ⬜ button is selected, the Contents Panel lists the roles to which the user is assigned. The tasks associated with each role are listed under the role.

When the View Objects ⬜ button is selected, the Contents Panel displays the iManager Object Selector, which enables users to browse or search for objects in the eDirectory tree.

Using the Object Selector

Use the following guidelines when using the iManager 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, just when the name is a DN or RDN.

3. In a search filter, you must escape these characters with a backslash:

   ◆ asterisk (*)

   ◆ backslash (\)

For example:

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

To search for all objects containing plus, search filter = *+*

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

Access Modes

When you start iManager, you are granted an *access mode* based on the rights you've been assigned. iManager has four access modes. The mode you are in is displayed in the top-left corner of the iManager interface.

◆ Unrestricted

This mode displays all of the roles and tasks installed. Although all roles and tasks are visible, the authenticated user will still need the necessary rights to use the tasks.

◆ Assigned

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

◆ Collection owner

This mode displays all of the roles and tasks installed in the collection. It allows user Admin 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.

◆ Tree down

This is a troubleshooting mode that should be used only when eDirectory services on your network are unavailable. Tomcat must be stopped and restarted to access this mode.

Special Characters

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

NDAP (NDS): . = + \

LDAP:

◆ DNs: , = + \ ; < >

◆ Leading #

◆ Leading or trailing spaces

For LDAP, any character can be specified with \xx (RFC2253).

5 Setting Up Role-Based Services

This chapter defines Role-Based Services (RBS) and describes how to implement RBS with Novell® iManager. The instructions in the following sections assume that you have successfully installed iManager.

Overview

iManager gives administrators 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 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.

Default Roles and Tasks

A default set of roles and tasks is included with iManager. You can use the default set or customize them to your liking. The following base set of roles and their associated tasks are included with iManager 2.0.*x*:

- Dynamic Groups

  Create Dynamic Group
  Create Extended Object
  Delete Dynamic Group
  Modify Dynamic Group

- eDirectory Administration

  Copy Object
  Create Object
  Delete Object
  Modify Object
  Move Object
  Rename Object

- Groups

  Create Group

Delete Group
Modify Group

- ◆ Help Desk

  Clear Lockout
  Create User
  Set Password

- ◆ Partition and Replicas

  Create Partition
  Merge Partition
  Move Partition
  Replica View
  View Partition Information

- ◆ Rights

  Modify Inherited Rights Filter
  Modify Trustees
  Rights To Other Objects
  View Effective Rights

- ◆ Schema

  Add Attribute
  Attribute Information
  Class Information
  Create Attribute
  Create Class
  Delete Attribute
  Delete Class
  Object Extensions

- ◆ Servers

  Launch NetWare Remote Manager

- ◆ Users

  Create User
  Delete User
  Disable Account
  Enable Account
  Modify User

RBS Objects in eDirectory

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

Table 1   **RBS Objects in eDirectory**

Object	Description
rbsCollection	Represents a container object that holds all RBS Role and Module objects.
	rbsCollection objects are the topmost 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.
	rbsCollection objects can be created in any of the following containers:
	◆ Country
	◆ Domain
	◆ Locality
	◆ Organization
	◆ Organizational Unit
rbsRole	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.
	rbsRoles are container objects that can be created only in an rbsCollection container.
	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.
rbsTask	Represents a leaf object that holds a specific function, such as resetting login passwords.
	rbsTask objects are located only in rbsModule containers.
rbsBook	Represents a leaf object that containing 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.
	rbsBook objects are located only in rbsModule containers.
rbsScope	Represents 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 will be 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.
	This object is dynamically created when needed, then automatically deleted when no longer needed. They are located only in rbsRole containers.
	WARNING: Never change the configuration of an rbsScope object. Doing so will have serious consequences and could possibly break the system.

Object	Description
rbsModule	Represents a container object that holds rbsTask and rbsBook objects. rbsModule objects have a module name attribute that represents the name of the product that defines the tasks or books (for example, eDirectory Maintenance Utilities, NMAS Management, or Novell Certificate Server Access).
	rbsModule objects can be created only in rbsCollection containers.

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

Figure 2   RBS Objects in the eDirectory Tree

Role-Based Services
in eDirectory
- Collection
  - Module
    - Task
    - Book
  - Role
    - Scope
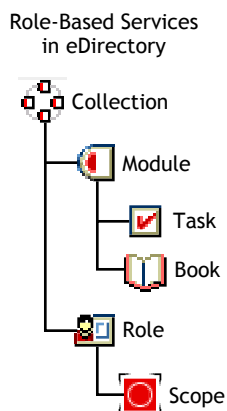
Installing RBS

Role-Based Services (RBS) is installed using the iManager Configuration Wizard.

IMPORTANT: Using RBS is optional, although we recommend setting it up for the optimal use of the iManager software.

To launch the iManager Configuration Wizard:

1 In iManager, click the Configure button .

2 Select RBS Configuration > Configure iManager.

3 Select one of the following available options:

 ◆ Create a New Collection (iManager 2.*x*)

   Use this to create a new iManager 2.*x* Collection object. We recommend that you run this first before choosing the other options.

 ◆ Migrate a Previous Collection

   Use this to migrate iManager 1.*x* collection information to iManager 2.0.*x*.

   IMPORTANT: Before you migrate your 1.*x* RBS collection, you must install any 1.*x* modules you want to use in the 2.0.*x* container using the same names for the roles and tasks that you used in 1.*x*.

   Custom roles and custom property books can be migrated to iManager 2.0.*x*, but any custom tasks or custom pages that you created with the iManager 1.*x* Task Builder or iManager 1.*x* third-party plug-in cannot be migrated. You need to re-create them using iManager 2.0.*x*.

 ◆ Migrate Previous Role Association

Use this to migrate iManager 1.*x* role associations to iManager 2.0.*x*.

- ◆ Upgrade Collection

    Use this to upgrade any Collection object that you have rights to.

4 After you've made your selection, click Next and follow the on-screen instructions.

Some tasks assign supervisor rights to the container specified in the scope for the user. To become familiar with such tasks, see "Rights" on page 37.

IMPORTANT: Do not use Novell ConsoleOne® to modify or delete any Role-Based Services (RBS) objects. RBS objects should only be managed using iManager.

Rights

Several tasks in iManager require supervisor rights to the container to perform the required tasks for that role. When assigning roles to users or groups, the administrator is prompted for a scope. The scope defines how far up (or down) the tree rights are assigned. If, for instance, the iPrint role is assigned to a user and the scope is set at the top of the tree, the user that was assigned to that role has supervisor Object Entry rights to the entire tree.

NOTE: *Assigned rights* and *scope* are separate and rights do not necessarily need to be assigned with tasks.

If you have the Assigned Rights checkbox checked, the following roles contain tasks that assign supervisor rights to the container specified in the scope for the user:

- ◆ Archive/Version Management
- ◆ DHCP
- ◆ DNS
- ◆ eDirectory Administration
- ◆ eDirectory Maintenance
- ◆ iPrint
- ◆ NetStorage
- ◆ Novell Certificate Access
- ◆ Novell Certificate Server
- ◆ Partition and Replicas
- ◆ Schema
- ◆ Storage
- ◆ WAN Traffic

As new modules become available, they might have Supervisor rights. For more information, see the "Novell iManager: Planning Security for Delegated Administration" (http://www.novell.com/collateral/4621360/4621360.html) white paper.

Defining RBS Roles

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

The following sections explain how to manage role objects:

- "Creating a Role Object" on page 38
- "Modifying the Tasks Associated with a Role" on page 38
- "Assigning RBS Role Membership and Scope" on page 38
- "Deleting a Role-Based Services Object" on page 39
- "Defining Custom RBS Tasks" on page 39

Creating a Role Object

Use the Create iManager Role Wizard to create a new rbsRole object. We recommend creating the new rbsRole object in the same rbsCollection container where the other rbsRole objects reside (for example, the Role-Based Services Collection container).

1 In Novell iManager, click the Configure button 📛.

2 Click Role Configuration > Create iManager Role.

3 Follow the instructions in the Create iManager Role Wizard.

4 See "Defining Custom RBS Tasks" on page 39 for information on adding members to roles.

Modifying the Tasks Associated with a Role

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 In Novell iManager, click the Configure button 📛.

2 Click Role Configuration > Modify iManager Roles.

3 To add or remove tasks from a role, click the Modify Tasks button to the left of the role you want to modify.

4 Add or remove tasks from the Assigned Task list.

5 Click OK.

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.

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

- Directly
- 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. You can also assign the same task to multiple members.

To assign role membership and scope:

1 In Novell iManager, click the Configure button .

2 Click Role Configuration > Modify iManager Roles.

3 To add or remove members from a role, click the Modify Members button to the left of the role you want to modify.

4 In the Name field, specify an object name (a User, Group, or Container object) and context.

5 In the Scope field, specify an Organization or Organizational Unit object name and context.

6 Click Add, then click OK.

Deleting a Role-Based Services Object

1 In Novell iManager, click the Configure button .

2 Click Role Configuration > Delete Role.

3 Specify the name and context of the RBS role you want to delete.

4 Click OK.

Defining Custom RBS Tasks

The following sections explain how to defining custom RBS tasks and manage them:

- "Creating an iManager Task" on page 39
- "Creating a Server Administration Task" on page 39
- "Modify Role Assignment" on page 40
- "Deleting a Task" on page 40

Creating an iManager Task

1 In Novell iManager, click the Configure button .

2 Click Task Configuration > Plug-in Studio.

3 Follow the instructions in the online help to create a custom task.

Creating a Server Administration Task

Use the Create Server Administration Task Wizard to build custom tasks to access a server's services. The system administrator should verify that the service is available on the server.

1 In Novell iManager, click the Configure button .

2 Click Task Configuration > Create Server Administration Task.

3 Follow the instructions in the Create Server Administration Task Wizard.

Modify Role Assignment

1 In Novell iManager, click the Configure button .

2 Click Task Configuration > Modify Role Assignment.

3 Specify the name and context of the task you want to modify, then click Next.

4 Move the roles you want from the Available Roles column to the Assigned Roles column.

5 Click OK.

Deleting a Task

1 In Novell iManager, click the Configure button .

2 Click Task Configuration > Delete Task.

3 Specify the name and context of the task you want to delete, then click OK.

6 Installing and Using iManager Plug-ins

iManager ships with a core set of plug-ins including eDirectory Administration, Partition and Replicas, and Dynamic Groups. But many Novell® products include additional product-specific plug-ins. For example, DirXML® includes plug-ins that allow you to manage and configure all of your DirXML objects in Novell eDirectory™.

Typically, you will install plug-ins as part of the iManager or product installation. However, you can download and install plug-ins separate from a product installation.

Downloading and Installing a Plug-in

iManager plug-ins are available for download on the Novell Product Downloads Web site (http://download.novell.com/pages/PublicSearch.jsp?filter=category&filterselection=180).

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

The process you use to download and install plug-ins will vary depending upon whether or not you have RBS configured. For more information about RBS, see Chapter 5, "Setting Up Role-Based Services," on page 33.

- If RBS is not configured, all tasks appear in the Contents Panel regardless of your access rights, and no additional setup is required beyond plug-in installation. See "Installing a Plug-in When RBS Is Not Configured" on page 41.
- If RBS is configured, the new plug-in is not available for use until you upgrade your collections. See "Installing a Plug-In When RBS Is Configured" on page 42.

Installing a Plug-in When RBS Is Not Configured

1 At the Product Downloads Web site, mark Search by Category, select the iManager Plug-Ins category, then click Submit Search.

A list of available plug-ins organized by product is displayed.

2 Click the plug-in you want to download and review information specific to that plug-in, then close the text windows.

NOTE: Plug-ins are packaged in modules (NPMs). Those modules are capable of containing one or more plug-ins.

3 Click the Download button, log in, and review the download agreement.

If you haven't registered yet, you can register for free.

4 On the system where iManager is installed, download the *plug-in*.npm.

5 Log in to iManager.

6 Click the Configure button .

7 Click iManager Configuration > Modules, then click Install to install the module package.

8 Select the *plug-in*.npm file to install.

This install will take a few minutes.

9 Restart Tomcat.

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

Platform	Restart Command
NetWare® 6 or later	Enter **TC4STOP**. Wait at least 1 minute, then enter **TOMCAT4** to start the service again.
Windows	Stop and start the Tomcat service.
Solaris	Enter /var/opt/novell/tomcat4/bin/shutdown.sh, then enter /var/opt/novell/tomcat4/bin/startup.sh.
HP-UX	Enter /opt/hpws/tomcat/bin/shutdown.sh, then enter /opt/hpws/tomcat/bin/startup.sh.
Linux	Enter /etc/init.d/novell-tomcat4 stop, then enter /etc/init.d/novell-tomcat4 start.

10 Verify that the new Role appears in the Roles and Tasks page.

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

Installing a Plug-In When RBS Is Configured

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

1 At the Product Downloads Web site, mark Search by Category, select the iManager Plug-Ins category, then click Submit Search.

A list of available plug-ins organized by product is displayed.

2 Click the plug-in you want to download and review information specific to that plug-in, then close the text windows.

NOTE: Plug-ins are packaged in modules (NPMs). Those modules are capable of containing one or more plug-ins.

3 Click the Download button, log in, and review the download agreement.

If you haven't registered yet, you can register for free.

4 On the system where iManager is installed, download the *plug-in*.npm.

5 Log in to iManager.

6 Click the Configure button .

7 Click iManager Configuration > Modules, then click Install to install the module package.

8 Select the *plug-in*.npm file to install.

This install will take a few minutes.

9 Restart Tomcat.

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

Platform	Restart Command
NetWare 6 or later	Enter `TC4STOP`. Wait at least 1 minute, then enter `TOMCAT4` to start the service again.
Windows	Stop and start the Tomcat service.
Solaris	Enter /var/opt/novell/tomcat4/bin/shutdown.sh, then enter /var/opt/novell/tomcat4/bin/startup.sh.
HP-UX	Enter /opt/hpws/tomcat/bin/shutdown.sh, then enter /opt/hpws/tomcat/bin/startup.sh.
Linux	Enter /etc/init.d/novell-tomcat4 stop, then enter /etc/init.d/novell-tomcat4 start.

10 Log in to iManager, then click the Configure button.

11 Under RBS Configuration, select Configure iManager.

12 Choose Upgrade collections, then click Next.

13 Verify that the correct collection is selected, then click Next.

The new plug-ins should be displayed under Modules to Be Installed.

14 Select the plug-in you want, assign a scope, then click Start.

15 Wait for the Completed message, then click Close.

16 Verify that the new Role appears in the Roles and Tasks page.

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

7 Configuring and Customizing iManager

This section discusses how to customize the following features of Novell® iManager 2.0.*x*:

Configuring Contextless Login

Contextless login allows users to log in without specifying their directory context. By default, iManager enables this feature and sets users up for contextless login if the users meet the following criteria:

- They are in the same container as the iManager PCO object or the Admin User object for the server. Any subcontainers are automatically searched also.
- They use the CN attribute for logging in.
- They have inetOrgPerson as their user class. inetOrgPerson is the LDAP name for this class. The eDirectory name for this class is User.

If you have users who do not meet this profile, you need to configure contextless login to add additional containers, attributes, or user classes. See the following sections:

Adding Portal Containers

By default, the context of the iManager PCO object and the context of the Admin user are set up as Portal containers for contextless logins. If your user objects exist in other containers, you need to add these containers to the Contextless Login search path.

To add other containers for contextless logins:

1 In iManager, click the Configure button ![icon].

2 In the Contents panel, click iManager Configuration > Portal.

3 In the right pane, click Properties.

4 Use the Add and Remove buttons to select and add additional containers.

You only have to set up top level containers as Portal containers. Subcontainers under Portal containers automatically work with contextless logins.

5 Save your changes.

The portal should automatically refresh to use the new settings. If you want to refresh the portal manually, click Refresh Portal > Refresh All > Refresh.

Adding Other Attributes

The portal also has the capability for contextless login with other attributes than the CN attribute of the user object (such as e-mail address, fullname, etc.).

To add other attributes for contextless logins:

1 In iManager, click the Configure button .

2 In the Contents panel, click iManager Configuration > Portal.

3 In the right pane, click Configuration.

4 In the Attributes to Use for Contextless Login line, click Edit.

In the window, add the attributes to the list. All attributes are in LDAP format. CN is assumed if no attributes are set. If you set any attributes, you must also specify CN.

5 Save your changes.

Modifying the User Object Class

The portal also has the capability for contextless login with object classes other than inetOrgPerson such as Person, Organizational Person, etc. For example, to have contextless login search for all objects that inherit from the Person class which includes the Organizational Person and User classes, you would add the following line to the PortalServlet.properties file located in $TOMCAT_HOME$/webapps/nps/WEB-INF:

```
System.UserClass=person
```

NOTE: In eDirectory, User is the class name for the LDAP inetOrgPerson class.

Enabling or Disabling Contextless Login

When contextless login is disabled, users must enter their fully distinguished name (for example, cn=user,o=container) in order to log in. When enabled, users do not need to include their directory context, but can log in using just the log in attribute, usually CN. By default, contextless login is enabled.

To enable or disable contextless login:

1 In iManager, click the Configure button .

2 In the Contents panel, click iManager Configuration > Portal.

3 In the right pane, click Configuration.

4 In the Enable Contextless Login line, select either the Off or the On radio button.

5 Save your changes.

Configuring iManager for SSL/TLS Connection to eDirectory

Some plug-ins require secure LDAP access to function properly. To set up secure access, you must import an root certificate into iManager by completing the following tasks:

- "Exporting a Root Certificate" on page 47
- "Importing an eDirectory Certificate into the Keystore" on page 47

Exporting a Root Certificate

1 Log in to iManager.

2 In the Contents panel, click eDirectory Administration > Modify Object.

3 In the right pane, enter the distinguished name of the LDAP server in the Object Name box, then click OK.

If you do not know the name, click the Object Selector button that allows you to browse the tree for objects. In the left pane, enter the container in which to begin browsing, select the other criteria for the object, then click Apply. In the right pane, select the object. When the object appears in the Object Name box, click OK.

4 Select the Connections tab and note the name of the server certificate listed in the Server Certificate box.

5 In the Contents panel, click Modify Object.

6 In the right pane, enter the name of the server certificate, then click OK.

7 Select the Certificates tab, select Trusted Root Certificate, then click Export.

8 Select not to export the private key with the certificate.

9 Select to save the certificate in DER format.

10 Select to save the certificate to a file.

11 Click Close.

Importing an eDirectory Certificate into the Keystore

After you have an eDirectory certificate saved in DER format, you need to import the certificate into the iManager keystore.

1 Open a command window.

2 Change to the bin directory where you have installed the JDK*. For example, on a Windows system, you would enter the following command:

cd j2sdk1.4.1_02\bin

3 Import the certificate into the keystore with the keytool. For example, to import the certificate to iManager on a NetWare server from a Windows machine, you would enter the following command:

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

The first path in the command, c:\eDirectory.cer, specifies the location and name of the certificate you exported.

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

4 Enter **changeit** for the keystore password.

5 Select Yes to Trust this certificate.

Customizing Available Buttons

The iManager Views task allows an administrator to hide the different buttons that are in the top frame of iManager from the users that access iManager. By default all of the buttons are available to everyone, but some let you perform configuration operations that you might not want all users to be able to access or even see. This task allows you to hide these buttons from users. The settings can be applied to Containers (applies to all users in the container), Users, Persons, or Organizational Persons.

To limit the buttons available to users:

1 In iManager, click the Configure button .

2 In the Contents panel, click View Configuration > iManager Views Access.

3 In the right pane, enter the distinguished name of the object to restrict, then click OK.

If you do not know the name, click the Object Selector button that allows you to browse the tree for objects. In the left pane, enter the container in which to begin browsing, select the other criteria for the object, then click Apply. In the right pane, select the object. When the object appears in the Object Name box, click OK.

4 Change the flag to limit which buttons are available to users at the selected object in the directory:

   ◆ The Do Not Set flag either allows the button to show (the default) or takes the setting applied to a container above the object if one has been set.

   ◆ The Show flag shows the button, even if the button was hidden at container above the object.

   ◆ The Hide flag hides the button regardless of any other settings in a container above the object.

   ◆ The Read Parent Containers Above This Object setting applies the button settings that have been configured for container above the object to take effect on that object.

NOTE: Portal administrators and rbsCollection owners cannot be restricted from seeing the Configure button. Even if you use iManager to hide the button, these users can see and use the Configure button.

Manually Running the exteNd Director Configuration Wizard

iManager version 2.x runs on top of the exteNd Director™, Standard Edition (DEX) portal framework. For iManager to function properly, configuration of DEX needs to be performed in both eDirectory and on the Web server where iManager is running.

The DEX configuration is typically performed silently during the iManager 2.x install on most platforms. However, you might find it necessary to manually configure these settings if there were errors during the silent configuration or if you require custom configuration. iManager provides

the exteNd Director Configuration Wizard to allow easy configuration or reconfiguration of these settings.

The eDirectory configuration information is largely stored on the CN=PCO,OU=Extend object, which is usually found in your servers container. The Web server configuration information is stored in the PortalServlet.properties file located in $TOMCAT_HOME$/webapps/nps/WEB-INF.

The PCO object allows multiple iManager Web servers (Portal Heads) to synchronize content and to share Role-Based Services configuration and other settings. While running the exteNd Director Configuration Wizard, if one or more iManager servers have previously been installed into the tree, you are prompted to select to Install into an Existing PCO Object or to Create a New PCO Object. Be aware that if you select to create a new PCO object, the configured iManager cannot be associated in any way with the other iManager servers in the tree.

WARNING: Running the exteNd Director Configuration Wizard can destroy data. Do not complete the steps in the following sections unless you have been instructed to do so in either Chapter 2, "Installing iManager," on page 13 or Chapter 8, "Troubleshooting," on page 53.

Preparing to Run the Wizard

1 Get the PCO password seed.

If you are configuring to an existing PCO object, you are required to know the password seed for that PCO object. The password seed can be found in the System.Password entry in the PortalServlet.properties file of any iManager that has been configured to that PCO.

To find the list of all iManagers that are configured to an existing PCO, look at the bhLocation attribute on the PCO object.

2 Unconfigure the portal on the web server by renaming the PortalServlet.properties file. For example:

```
PortalServlet.properties.OLD
```

The exteNd Director Configuration Wizard contains an Unconfigure feature; however, in case you ever need to revert to the previous configuration, we recommend that you rename the PortalServlet.properties file instead of using the Unconfigure feature.

3 Restart Tomcat.

Running the Wizard

1 Run exteNd Director Configuration Wizard, based upon your iManager configuration. Enter

http://*server_ip_address*/nps/servlet/configure

or

https://*server_ip_address*/nps/servlet/configure

2 Click Start.

3 Type the IP address or DNS name of your eDirectory LDAP server and credentials for administration access.

You need to authenticate to the LDAP directory with admin rights before you install iManager. Use LDAP syntax for the authentication credentials. Passwords are case sensitive.

LDAP syntax refers to only the Distinguished name. For example, cn=admin,ou=mydepartment,o=mycompany.

IMPORTANT: If you select SSL, you must use an SSL port such as 636. The port number 389 is not an SSL port. We recommend you use SSL; otherwise, your password information will be sent over the wire in a clear text format.

4 Select the platform.xar from the list or browse for the platform.xar file.

5 Accept the license agreement, then click Next.

6 Select Typical, then click Next.

If a previous install exists, there is an option to connect to the existing PCO or create a new one.

IMPORTANT: Be aware that if you select to create a new PCO object, the configured iManager cannot be associated in any way with the other iManager servers in the tree.

7 Click Next.

8 After the configure is completed, restart Tomcat.

9 Log in to iManager, based upon your iManager configuration:

http://*server_ip_address*/nps/iManager.html

or

https://*server_ip_address*/nps/iManager.html

Setting Up Load Balancing and Failover

If you have multiple servers in your tree, you can configure how LDAP connections are handled. You can configure iManager so that the same server does not establish all or most of the LDAP connections or so that one server handles all the LDAP connections unless it fails. For configuration instructions, see the following sections:

IMPORTANT: Either load balancing or failover can be active at a time, never both.

Configuring Load Balancing

Load balancing is performed in a round-robin style. The first server is used for the first connection established. The second server is used for the second connection and so on until the last server has been accessed and the loop returns to the first server in the active servers list. As the server list is accessed, if one of the servers goes down, it is removed from the list of active servers and placed in a inactive servers queue. A process runs at periodic intervals to recheck the inactive server to see if it is now active. If it is active, it is appended to the end of the active servers list. The interval for rechecking inactive servers is configurable. See .

The LDAP connection stays with the same server it started with unless that server goes down. It can be thought of as a sticky connection as far as which server is used.

Load balancing supports up to three additional servers to use for load balancing. Therefore, a maximum of four servers can be used for load balancing purposes. This is accomplished by adding additional server address as listed below to your PortalServlet.properties file located in $TOMCAT_HOME/webapps/nps/WEB-INF/:

```
System.DirectoryAddress=137.65.1.2:636
System.DirectorySSL=true

System.Directory1Address=137.65.1.7:389
System.Directory1SSL=false

System.Directory2Address=137.65.1.14:389
System.Directory2SSL=false

System.Directory3Address=137.65.1.21:636
System.Directory3SSL=true
```

Load balancing supports up to four total server addresses with any combination of SSL and non-SSL LDAP connections. If the DirectorySSL line is omitted for any server address, false is assumed. False means that SSL is not used for communication.

Configuring Failover

Failover is implemented in much the same fashion as load balancing. The only significant difference is that the active server list stays with the first server in the list. If the first server goes down for some reason, it is removed from the active server list and the new server that is now first in the list is used for all new connections.

To enable failover mode, add the following line to the PortalServlet.properties file located in $TOMCAT_HOME/webapps/nps/WEB-INF/:

```
System.FailoverOnly=true
```

With this line in the file, the list of servers in the PortalServlet.properties file are used in a failover fashion and are not used for load balancing.

When an inactive server comes back up, it is appended to the end of the active servers list. If you want it to become the primary server again, you need refresh the iManager configuration. See "Refreshing the Load Balancing or Failover Configuration" on page 51.

Configuring the Server Check Interval

By default, the servers in the inactive server list are checked every 180 seconds. You can change this interval by adding the following line to the PortalServlet.properties file located in $TOMCAT_HOME/webapps/nps/WEB-INF/:

```
System.ServerCheckInterval=180000
```

The number specified is in milliseconds.

Refreshing the Load Balancing or Failover Configuration

To reset the server list for load balancing or failover:

1 In iManager, click the Configure button ![icon].

2 In the Contents panel, click iManager Configuration > Portal.

3 In the right pane, click Refresh Portal.

When the iManager configuration is refreshed, the bad servers list is thrown away and the active servers list is re-read from PortalServlet.properties.

Adding Classes of Objects to the Create Object Task

The eDirectory Administration role contains a task called Create Object. This task enables you to create an object of any class in the schema that uses one of the standard eDirectory syntaxes. When you select the Create Object task, it presents a list of available object classes. By default, the Create Object task lists only the most commonly-used object classes in the list. You can add additional object classes to the list, enabling users to create corresponding objects.

IMPORTANT: Role-based Services must be configured before you can use the iManager Development role.

To add additional items to the Available object classes list:

1 Click the Developer button .

2 Click iManager Development > Add Object Class To Creation List.

3 Select an object class from the list of available object classes, then click Next.

4 At the summary page, verify that the value of the <class-name> entry is com.novell.emframe.fw.GenericCreator, then click Finish.

5 To add another object class, click Repeat Task; otherwise, click OK.

6 Return to the Create Object task by clicking the Roles and Tasks button , then clicking eDirectory Administration > Create Object.

7 Verify that the object classes you added are in the list of available object classes.

TIP: If you want to have a separate task to create an object instead of using the Create Object task, use the Plug-In Studio to create a task for that class.

8 Troubleshooting

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

Blank Page

There are many causes for a blank page:

- You are running NetWare® 6 with a Novonyx server.
- You installed Apache as a standalone product on a nonstandard port.
- The Custom_Backend_Renderer_Portal_Location directive is not set in the PortalServlet.Properties file.

To correct these problems:

1 Stop Tomcat.

2 Edit the PortalServlet.properties file located in $TOMCAT_HOME/webapps/nps/WEB-INF:

- If you did not install Apache, modify the following line to use the specified port and replace <ip_address> with the IP address of your server.

```
Custom_Backend_Renderer_Portal_Location=http\://<ip_address>:8080/
nps
```

- If you installed Apache but used a nonstandard port, for example 81, modify this line to reflect the configured port and replace <ip_address> with the IP address of your server.

```
Custom_Backend_Renderer_Portal_Location=http\://<ip_address>:81/nps
```

- If the Custom_Backend_Renderer_Portal_Location directive is not set, add this line, making sure the port specified is correct. Replace <ip_address> with the IP address of your server

  ```
  Custom_Backend_Renderer_Portal_Location=http\://<ip_address>:80/nps
  ```

3 Restart Tomcat.

4 Log in to iManager.

If the blank page persists, you might need to manually reconfigure the iManager portal. See for instructions.

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.

- On Solaris and HP-UX, export LAX_DEBUG=true in the terminal session from which you start the iManager InstallAnywhere program.
- On 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 information/error messages logged during the configuration of iManager.

On all platforms, you can run the iManager servlet in debugging mode. Add ?DEBUG=LOG_LOW to the end of your iManager URL. For example:

```
https://<ip_address>/nps/servlet/configure?DEBUG=LOG_LOW
```

Replace <ip_address> with the IP address of your server. This command generates debug information in your Tomcat log files.

Dynamic Group LDAP Errors

After you have logged in using the Login to a Different Tree button ![icon], you might receive the following messages when modifying a dynamic group:

```
LDAP Error
Unable to obtain a valid LDAP context.

Creating secure SSL LDAP context failed:
simple bind failed: 151.155.159.49:636
```

The Dynamic Groups role requires secure LDAP access to function properly. To set up secure access, see .

eDirectory Maintenance Task Errors

In order to run eDirectory Maintenance Tasks, Role-Based Services must be configured through iManager to the tree that is being administered. For RBS configuration information, see Chapter 5, "Setting Up Role-Based Services," on page 33.

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 404 Error

If you receive this error the first time you attempt to access iManager, you need to unconfigure NPS for iManager and then reconfigure it.

1 Use a Web browser to connect to the exteNd Director™ Configuration wizard. Enter the following URL

https://<ip_address>/nps/servlet/configure

Replace <ip_address> with the IP address of the server where you installed iManager.

2 In the Welcome page, click the Current Configuration button.

3 Click the Unconfigure button.

You are asked for the credentials of the user that installed iManager (the Portal Admin). Follow any other on-screen instructions.

4 Run the exteNd Director Configuration Wizard to manually configure NPS. For instructions, see "Manually Running the exteNd Director Configuration Wizard" on page 48.

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.

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/Linux, the logs are named catalina.out or localhost_log.<date>.txt, and on Windows, the log files are named stderr and stdout.

On NetWare, any errors are sent to the logger screen.

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.

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 first logging in to iManager, add ?forceMaster=true to the end of the URL. For example:

http://*ip_address*/nps/iManager.html?forceMaster=true

NPS Is an Unrecognized Context Error

When installing iManager without Tomcat4 on NetWare 6.0, Tomcat needs to be manually restarted after the installation completes. If you try to access iManager without restarting Tomcat, you receive an error that NPS is an unrecognized context.

To solve this problem, restart Tomcat.

NOTE: This problem does not happen if you select both Tomcat4 and iManager during the iManager 2.0.2 install. It only happens if Tomcat is already installed.

"There Was a Problem Starting the Servlet" Errors

Most errors that begin with "There was a problem starting the servlet" indicate that information is missing from the PortalServlet.properties file, located in $TOMCAT_HOME/webapps/nps/WEB-INF. The error message also contains suggestions on possible causes and solutions.

If this is the second iManager portal you are installing into the same eDirectory tree, please copy the PortalServlet.properties file from another server to remedy the problem. Make sure to update IP addresses of settings to match the new server such as the Custom_Backend_Renderer_Portal_Location directive.

If the suggested solution fails, you might need to rerun the exteNd Director Configuration wizard. For instructions, see "Manually Running the exteNd Director Configuration Wizard" on page 48.

"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. The nmasinst 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).

A Configuration Settings in the PortalServlet.properties File

Various settings can be configured for Novell® iManager. These settings affect the way that iManager and the Web server behave. PortalServlet.properties is the configuration file for iManager 2.0.*x*, it is located in the "...\webapps\nps\WEB-INF\" directory of the Tomcat servlet engine.

Many of these settings can also be configured through iManager 2.0.*x* in the iManager Configuration role. Be aware that, upon restarting the Tomcat servlet engine, directives in the PortalServlet.properties file will override any of the same settings that have been configured through the iManager Configuration role in iManager 2.0.*x*.

The following are descriptions and examples of many of the directives that can be configured for iManager 2.0.*x*.

Default Tree Setting

System.AllowiManagerDefaultLogin

Turns on or off the default tree feature. By default, the feature is off.

true - Turns on default tree feature.

false - Turns off default tree feature (default).

For example:

System.AllowiManagerDefaultLogin=true

LDAP Server Settings

System.DirectoryAddress

Specifies the IP address and port of the LDAP server. The LDAP server is where the portal configuration object is located.

For example:

System.DirectoryAddress=127.1.1.1:389

System.DirectorySSL

Specifies that iManager should attempt to connect to LDAP securely.

NOTE: If set to true, the System.DirectoryAddress will use the default LDAP SSL port of 636.

true - SSL connection to LDAP server (default).

false - Clear text connection to LDAP server.

For example:

System.DirectorySSL=false

System.Directory#Address

Specifies the IP address and port of the secondary LDAP server(s). iManager is designed to have up to three secondary addresses specified. Replace # with number 1 - 3.

For example:

System.Directory1Address=127.1.1.1

System.Directory2Address=127.1.1.2

System.Directory3Address=127.1.1.3

NOTE: All Directory Addresses specified must be in the same tree as the System.DirectoryAddress.

System.Directory#SSL

Specifies if iManager attempts to connect to the secondary LDAP server(s) securely. Replace # with number 1 - 3.

NOTE: If this setting is true, the System.Directory#Address will need to use the LDAP SSL port (Default LDAP SSL port is 636).

true - SSL connection to LDAP server.

false - Clear text connection to LDAP server (default).

For example:

System.Directory1SSL=true

System.Directory2SSL=true

System.Directory3SSL=false

System.FailoverOnly

Enable fail over mode for LDAP directory access. If disabled, load balancing is used. This setting requires System.Directory#Address to be specified in order to work correctly.

true - Failover between LDAP servers.

false - Load balance between LDAP servers (default).

For example:

System.FailoverOnly=true

Portal Configuration Object Settings

System.PortalConfigurationObjectDN

Full LDAP directory name of the portal configuration object.

For example:

System.PortalConfigurationObjectDN=cn=portal,o=nps

System.GUID

Globally Unique Identifier (GUID) for the portal configuration object.

For example:

System.GUID={E5BAE001-0000-00F1-1D4E-C6AB89419537}

System.Password

Password seed of the portal configuration object.

For example:

System.Password=MyPassword

Custom_Backend_Renderer_Portal_Location

Specifies where iManager will retrieve the style sheets for backend rendering. For more information on this setting, refer to TID #10070553 on the Novell Support Web site (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10070553.htm).

NOTE: This setting should be considered as required when running iManager behind Novell iChain™ or any other reverse proxy.

For example:

Custom_Backend_Renderer_Portal_Location=http://127.1.1.1/nps

Session Manager Settings

System.SessionManager.Render
System.SessionManager.RenderOverride

These settings are used to force rendering on the iManager server.

true - Information is always returned as html to the browser.

false - Information can be returned as html or xml/xsl (default).

NOTE: These settings are commented out by default.

For example:

!System.SessionManager.Render=true

Render DontCacheStylesheets Settings

System.Render.DontCacheStylesheets

This setting is used for development purposes.

true - Style sheets are read from the file system on every request. This setting should only be used in development because of the impact on performance.

false - Style sheets are read from iManagers cache (default).

For example:

System.renderer.DontCacheStylesheets=true

Log Settings

Logging Enabled

Enables iManager to keep a log of debug, error, and informational output.

true - Information is logged (default).

false - Information is not logged.

For example:

System.Logging=true

Logging Priority

This determines the type and amount of information written to the output.

NOTE: This flag is only used if System.Logging is set to true.

high - Very little information is logged to the output (default).

medium - A moderate amount of information logged to the output.

low - All information is written to the output.

For example:

System.Logging.Priority=high

Logging Output

This determines the location where logger information is output to.

NOTE: This flag is only used if System.Logging is set to true.

err - Information is sent to Standard Error for the system (default).

out - Information is sent to Standard Output for the system.

file - Information is written to the …\webapps\nps\WEB-INF\Debug.xml file by default.

For example:

System.Logging.Output=err

NOTE: Logger output may be configured to be sent to multiple locations. For example: System.Logging.Output=err,file,out

Logging Output File

This allows the user to specify a output log file other than the default.

For example:

System.Logging.File=myDebugFile.xml

NOTE: This flag is only used if System.Logging.Output is set to "file".

SSL Settings

Warning on Non-Secure Connection

Shows a warning message when accessing iManager with a non-secure connection (using http instead of https).

true - Show a warning for non-secure connections (default).

false - Do not show a warning for non-secure connections.

For example:

Security.Warn.nonSecure=true

Require Secure eDirectory Communication

Specifies to iManager that it should use SSL when establishing JNDI/LDAP contexts.

NOTE: This only applies to the LDAP connections that are made by iManager tasks, not gadgets.

Additional configuration of the web server and eDirectory is typically required in order to allow secure communication between eDirectory and the web server.

This setting only applies when authenticated to a secondary tree.

Use the System.DirectorySSL directive for specifying a SSL connection to the tree where Portal has been configured.

true - When receiving a JNDI/LDAP context from the authentication broker, the connection will be secure.

false - The connection will be clear text (default).

For example:

Provider.eMFrame.ssl=false

Role-Based Services (RBS)

Show All Roles to Collection Owners

Specifies whether or not to show all of the roles in the administrator's owned collections in their roles and tasks view.

`true` - Show all roles in the Roles and Tasks view to authenticated User objects who are designated owners of an rbsCollection (default).

`false` - Show only assigned roles in the roles and tasks view.

For example:

Provider.eMFrame.ShowRolesInOwnedCollections.enable=true

Enable Self Provisioning

Specifies whether to enable the [this] keyword in iManager. This allows the assignment of rights for a user specifically to its own eDirectory object.

IMPORTANT: All servers in the tree must be running eDirectory version 8.62 or higher.

For example:

Provider.eMFrame.This.enable=false

RBS Discovery Domain

Specifies how far to traverse up the tree looking for roles that are assigned to a container.

Valid values are *parent*, *partition* and *root*. A value of parent will discover roles only assigned to the immediate parent container of the user logging in. A value of partition will discover roles assigned to the containers from the parent of the user to the first parent partition. A value of root will discover roles assigned to any container from the user to the root of the tree.

`parent` - Search from the parent container of the logged in user and all subdirectories (default).

`partition` - Search from the parent partition of the logged in user and all subdirectories.

`root` - Search from the root of the tree and all subdirectories.

For example:

Provider.eMFrame.Role.discoveryDomain=parent

Allow Dynamic Group Role Members

Specifies whether or not a dynamic group can be assigned as the member of a RBS role.

`true` - Dynamic groups can be assigned as a member of a role.

`false` - Dynamic groups cannot be assigned as a member of a role (default).

For example:

Provider.eMFrame.DynamicGroup.enable=true

Dynamic Group RBS Discovery Domain

Specifies how far to traverse up the tree looking for Dynamic Groups that are assigned to roles for a container.

Valid values are *parent*, *partition* and *root*. A value of parent will discover Dynamic Groups in the immediate parent container of the user logging in. A value of partition will discover Dynamic Groups in the containers from the parent of the user to the first parent partition. A value of root will discover roles assigned to any container from the user to the root of the tree.

NOTE: This flag is only used if Provider.eMFrame.DynamicGroup.enable is set to true.

parent - Search from the parent container of the logged in user and all subdirectories(default).

partition - Search from the parent partition of the logged in user and all subdirectories.

root - Search from the root of the tree and all subdirectories.

For example:

Provider.eMFrame.DynamicGroup.discoveryDomain=parent

Dynamic Group Search Types

Specifies the types of objects to allow as members of RBS roles.

This flag is only used if Provider.eMFrame.DynamicGroup.enable is set to true.

DynamicGroupObjectsOnly - Search for dynamic group objects only (default).

DynamicGroupObjects&AuxClasses - Search for dynamic group objects and any object that has the dynamic group auxiliary class.

For example:

Provider.eMFrame.DynamicGroup.Searchtype=DynamicGroupObjectsOnly

System.UserClass

By default, the only class searched for contextless login is inetOrgPerson (this is the User object in eDirectory). If you subclass inetOrgPerson it will work in contextless login. However, if you want to use something else, you must specify this setting to over-ride that behavior.

For example:

System.UserClass=person

NOTE: The example setting would cause contextless login to search for "person" objects instead of inetOrgPerson objects.

eGuide Administration

eGuide Server Location

Specifies the URL to eGuide. This is used in the eGuide launch button on 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 example:

Provider.eMFrame.eGuide.location=EMFRAME_SERVER

Sample PortalServlet.properties File

This section provides an example of the PortalServlet.properties file included with iManager 2.0.*x*.

```
#=================================================================================
# LDAP Server Settings:
#=================================================================================
#---------------------------------------------------------------------------------
# System.DirectoryAddress:
# Specifies the IP address and port of the LDAP server. The LDAP server is where
# the portal configuration object is located.
#---------------------------------------------------------------------------------
System.DirectoryAddress=137.65.150.253:389
#---------------------------------------------------------------------------------
# System.DirectorySSL:
# Specifies that iManager should attempt to connect to LDAP securely.
# NOTE: If this setting is true, the System.DirectoryAddress will need to use
# the LDAP SSL port (Default LDAP SSL port is 636).
#    true -  SSL connection to LDAP server.
#    false - Clear text connection to LDAP server (default).
#---------------------------------------------------------------------------------
System.DirectorySSL=false
#---------------------------------------------------------------------------------
# System.Directory#Address:
# Specifies the IP address and port of the secondary LDAP server(s). iManager is
# designed to have up to three secondary addresses specified. Replace # with
# number 1 - 3.
# EXAMPLE:
#System.Directory1Address=137.65.1.1
#System.Directory2Address=137.65.1.2
#System.Directory3Address=137.65.1.3
# NOTE: All Directory Addresses specified must be in the same tree as the
#        System.DirectoryAddress.
#---------------------------------------------------------------------------------
```

```
#-----------------------------------------------------------------------
# System.Directory#SSL:
# Specifies if iManager attempts to connect to the secondary LDAP server(s)
# securely. Replace # with number 1 - 3.
# NOTE: If this setting is true, the System.Directory#Address will
# need to use the LDAP SSL port (Default LDAP SSL port is 636).
#    true -  SSL connection to LDAP server.
#    false - Clear text connection to LDAP server (default).
# EXAMPLE:
#System.Directory1SSL=true
#System.Directory2SSL=true
#System.Directory3SSL=false
#-------------------------------------------------------------------------
#-------------------------------------------------------------------------
# System.FailoverOnly:
# Enable fail over mode for LDAP directory access. If disabled, load balancing
# is used. This setting requires System.Directory#Address to be specified in order to work
# correctly.
#    true -  Failover between LDAP servers.
#    false - Load balance between LDAP servers (default).
# EXAMPLE:
#System.FailoverOnly=true
#-------------------------------------------------------------------------
#=========================================================================
# Portal Configuration Object Settings:
#=========================================================================
#-------------------------------------------------------------------------
# System.PortalConfigurationObjectDN:
# Full LDAP directory name of the portal configuration object.
#-------------------------------------------------------------------------
System.PortalConfigurationObjectDN=cn=portal,o=nps
#-------------------------------------------------------------------------
# System.GUID:
# Globally Unique Identifier (GUID) for the portal configuration object.
#-------------------------------------------------------------------------
System.GUID={E5BAE001-0000-00F1-1D4E-C6AB89419537}
#-------------------------------------------------------------------------
```

```
# System.Password:

# Password seed of the portal configuration object.

#-------------------------------------------------------------------------------

System.Password=DiscoNNected

#-------------------------------------------------------------------------------

# Custom_Backend_Renderer_Portal_Location:

# Specifies where iManager will retrieve the style sheets for backend rendering.

# Please review http://support.novell.com/cgi-bin/search/searchtid.cgi?/10070553.htm

# for additional information.

# EXAMPLE:

#Custom_Backend_Renderer_Portal_Location=http://137.65.147.1/nps

#

# NOTE: This setting should be considered as required when running iManager behind Novell

#       iChain or any other reverse proxy.

#-------------------------------------------------------------------------------

#===============================================================================

# Session Manager Settings:

#===============================================================================

#-------------------------------------------------------------------------------

# System.SessionManager.Render:

# System.SessionManager.RenderOverride:

# These settings are used to force rendering on the iManager server.

#     true  - Information is always returned as html to the browser.

#     false - Information can be returned as html or xml/xsl (default).

# NOTE: These settings are commented out by default.

#-------------------------------------------------------------------------------

!System.SessionManager.Render=true

!System.SessionManager.RenderOverride=true

#===============================================================================

# Render DontCacheStylesheets Settings:

#===============================================================================

#-------------------------------------------------------------------------------

# System.Render.DontCacheStylesheets:

# This setting is used for development purposes.

#     true  - Stylesheets are read from the file system on every request (This

#             setting should only be used in development because of the

#             performance hit).
```

```
#       false - Stylesheets are read from iManagers cache (Default).

#------------------------------------------------------------------------------

System.renderer.DontCacheStylesheets=true

#==============================================================================

# Log Settings:

#==============================================================================

#------------------------------------------------------------------------------

# Logging Enabled:

# Enables iManager to keep a log of debug, error, and informational output.

#    true -  Information is logged (default).

#    false - Information is not logged.

#------------------------------------------------------------------------------

System.Logging=true

#------------------------------------------------------------------------------

# Logging Priority:

# This determines the type and amount of information written to the output.

# NOTE: This flag is only used if System.Logging is set to true.

#    high -   Very little information is logged to the output (default).

#    medium - A moderate amount of information logged to the output.

#    low -    All information is written to the output.

#------------------------------------------------------------------------------

System.Logging.Priority=high

#------------------------------------------------------------------------------

# Logging Output:

# This determines the location where logger information is output to.

# NOTE: This flag is only used if System.Logging is set to true.

# NOTE: Logger output may be configured to be sent to multiple locations.

#        Example:  System.Logging.Output=err,file,out

#    err -  Information is sent to Standard Error for the system (default).

#    out -  Information is sent to Standard Output for the system.

#    file - Information is written to the …\webapps\nps\WEB-INF\Debug.xml file

#        by default.

#------------------------------------------------------------------------------

System.Logging.Output=err

#------------------------------------------------------------------------------

# Logging Output File:

# This allows the user to specify a output log file other than the default.
```

```
# NOTE: This flag is only used if System.Logging.Output is set to "file".
#-------------------------------------------------------------------------------
System.Logging.File=myDebugFile.xml
#===============================================================================
# SSL Settings:
#===============================================================================
#-------------------------------------------------------------------------------
# Warning on Non-Secure Connection:
# Show a warning message when accessing iManager with a non-secure connection
# (using http instead of https)
#    true  - Show a warning for non-secure connections (default).
#    false - Do not show a warning for non-secure connections.
#-------------------------------------------------------------------------------
Security.Warn.nonSecure=true
#-------------------------------------------------------------------------------
# Require Secure eDirectory Communication:
# Specifies to iManager that it should use SSL when establishing JNDI/LDAP
# Contexts.
#  NOTE: This ONLY applies to the LDAP connections that are
#     made by iManager tasks, not gadgets.
#  NOTE: Additional configuration of the web server and eDirectory is
#     typically required in order to allow secure communication between
#     eDirectory and the web server.
#  NOTE: This setting only applies when authenticated to a secondary tree.
#     Use the System.DirectorySSL directive for specifying a SSL connection
#     to the tree where Portal has been configured.
#    true -  When receiving a JNDI/LDAP context from the authentication broker,
#             the connection will be secure.
#    false - The connection will be clear text (default).
#-------------------------------------------------------------------------------
Provider.eMFrame.ssl=false
#===============================================================================
# Role Based Services:
#===============================================================================
#-------------------------------------------------------------------------------
# Show All Roles to Collection Owners:
# Specify whether or not to show all of the roles in the administrator's owned
```

```
# collections in their roles and tasks view.
#    true   - Show all roles in the Roles and Tasks view to authenticated
#             Users who are designated owners of an rbsCollection (default).
#    false  - Show only assigned roles in the roles and tasks view.
#-----------------------------------------------------------------------------
Provider.eMFrame.ShowRolesInOwnedCollections.enable=true
#-----------------------------------------------------------------------------
# Enable Self Provisioning:
# Specifies whether to enable [this] in iManager.  This allows the assignment
# of rights for a user specifically to its own eDirectory object.
# Note that all servers in the tree must be version 8.62 or higher.
#-----------------------------------------------------------------------------
Provider.eMFrame.This.enable=false
#-----------------------------------------------------------------------------
# RBS Discovery Domain:
# Specifies how far to traverse up the tree looking for roles that are assigned
# to a container.  Valid values are parent, partition and root.  A value of
# parent will discover roles only assigned to the immediate parent container of
# the user logging in.  A value of partition will discover roles assigned to
# the containers from the parent of the user to the first parent partition.
# A value of root will discover roles assigned to any container from the user
# to the root of the tree.
#   parent    - Search from the parent container of the logged in user and all
#               subdirectories(default).
#   partition - Search from the parent partition of the logged in user and all
#               subdirectories.
#   root      - Search from the root of the tree and all subdirectories.
#-----------------------------------------------------------------------------
Provider.eMFrame.Role.discoveryDomain=parent
#-----------------------------------------------------------------------------
# Allow Dynamic Group Role Members:
# Specify whether or not a dynamic group can be assigned as the member of a
# RBS role.
#    false - Dynamic groups cannot be assigned as a member of a role (default).
#    true  - Dynamic groups can be assigned as a member of a role.
#-----------------------------------------------------------------------------
Provider.eMFrame.DynamicGroup.enable=true
```

```
#--------------------------------------------------------------------------
# Dynamic Group RBS Discovery Domain:
# Specifies how far to traverse up the tree looking for Dynamic Groups that
# are assigned to roles for a container.  Valid values are parent, partition
# and root.  A value of parent will discover Dynamic Groups in the immediate
# parent container of the user logging in.  A value of partition will discover
# Dynamic Groups in the containers from the parent of the user to the first
# parent partition.  A value of root will discover roles assigned to any
# container from the user to the root of the tree.
# Note that this flag is only used if Provider.eMFrame.DynamicGroup.enable is
# set to true.
#   parent    - Search from the parent container of the logged in user and all
#               subdirectories(default).
#   partition - Search from the parent partition of the logged in user and all
#               subdirectories.
#   root      - Search from the root of the tree and all subdirectories.
#--------------------------------------------------------------------------
Provider.eMFrame.DynamicGroup.discoveryDomain=parent
#--------------------------------------------------------------------------
# Dynamic Group Search Types:
# Specifies the types of objects to allow as members of RBS roles.
# Note that this flag is only used if Provider.eMFrame.DynamicGroup.enable is
# set to true.
#    DynamicGroupObjectsOnly - Search for dynamic group objects only (default).
#    DynamicGroupObjects&AuxClasses - Search for dynamic group objects and any
#     object that has the dynamic group auxiliary class
#--------------------------------------------------------------------------
Provider.eMFrame.DynamicGroup.Searchtype=DynamicGroupObjectsOnly
#--------------------------------------------------------------------------
# System.UserClass:
# By default, the only class searched for contextless login is "inetOrgPerson" (this is
# the User object in eDirectory). If you subclass inetOrgPerson it will work in
# contextless login.
# However, if you want to use something else, you must specify this setting to over-ride
# that behavior.
# EXAMPLE:
#System.UserClass=person
```

```
#
# NOTE: The example setting would cause contextless login to search for "person" objects
#        instead of inetOrgPerson objects
#------------------------------------------------------------------------------
#==============================================================================
# eGuide Administration:
#==============================================================================
#------------------------------------------------------------------------------
# eGuide Server Location:
# Specifies the url to eGuide.  This is used in the eGuide launch button on
# the header and in the eGuide role and task management tasks.  This must be
# a full url, (ie. 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.
#------------------------------------------------------------------------------
Provider.eMFrame.eGuide.location=EMFRAME_SERVER
```