

Installation Guide for the Identity Manager Components

Novell® Identity Manager Resource Kit

1.2

August 29, 2008

www.novell.com



Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2007-2008 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

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

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

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

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide	9
1 Overview	11
2 Preparing the Environment	13
2.1 Downloading Prerequisite Software	13
2.1.1 Downloading ISO Files	13
2.1.2 Downloading SUSE Linux Enterprise Server (SLES) 10 SP2	14
2.1.3 Downloading eDirectory 8.8.3	14
2.1.4 Downloading iManager 2.7	14
2.1.5 Downloading Identity Manager 3.6	14
2.1.6 Downloading Designer 3.0 for Identity Manager	15
2.1.7 Downloading Novell Audit 2.0.2 FP5	15
2.1.8 Downloading the MySQL JDBC Driver (Connector/J)	15
2.1.9 Downloading XPOZ	15
2.1.10 Downloading the Resource Kit Designer Project	16
2.2 Creating an Identity Manager Service User and Group	16
3 Installing eDirectory	17
3.1 Before Installing eDirectory	17
3.1.1 Enabling the SLES Server for Multicast Routing	17
3.1.2 Network Time Protocol Configuration	18
3.1.3 Installing the SLP User Agent and Server Agent	19
3.1.4 Validating Entries in the /etc/hosts File	20
3.2 Installing eDirectory 8.8.3	21
3.3 Configuring Your Environment	21
3.4 Configuring eDirectory	22
3.5 Tuning the eDirectory Database Cache Settings	23
4 Installing iManager	25
4.1 Installing iManager 2.7 SP1	25
4.2 Post-Installation Tasks for iManager 2.7 SP1	26
4.2.1 Granting File Access Rights to the Novell Service Group	26
4.2.2 Installing Additional Plug-Ins	27
4.2.3 Configuring eDirectory and iManager for Role-Based Services	28
4.2.4 Configuring iManager With a Trusted Certificate	33
4.2.5 Converting the Certificate File to the Appropriate File Type	38
5 Installing Designer 3.0 for Identity Manager	41
6 Installing the Identity Manager Metadirectory Engine and Drivers	43
7 Configuring the Environment for the Resource Kit	45
7.1 Importing the Resource Kit Designer Project	45
7.2 Loading the Resource Kit Structure into the Identity Vault	48

7.3	Populating the Identity Vault with the Resource Kit Data	49
7.3.1	Deploying the Resource Kit Project into the Identity Vault	49
7.3.2	Loading Sample Schema Extensions and Data	53
7.4	Prerequisites for the Delimited Text Driver	53
7.5	Making eDirectory Visible on the External IP Address	54
8	Installing XPOZ and Executing XPOZ Scripts	55
8.1	Installing XPOZ	55
8.2	Executing XPOZ Scripts	55
8.2.1	XPOZ Console	56
8.2.2	XPOZ GUI	56
8.3	Accessing the Resource Kit XPOZ Scripts	57
9	Configuring a Secure Mail Relay for Identity Manager	59
9.1	Enabling postfix and saslauthd to Start at Boot	59
9.2	Configuring saslauthd to Use LDAP Authentication	61
9.3	Configuring postfix to Use saslauthd	61
9.4	Testing saslauthd and postfix	62
9.5	Configuring Identity Manager to Use Your postfix MTA Service	63
10	Password Configuration	65
10.1	Creating a Required Password Policy	65
10.2	Enabling the Password Expiration Notification Job	68
11	Installing and Configuring the User Application	71
11.1	Preparing to Install the Identity Manager User Application	71
11.2	Using the Identity Manager Service Account	74
11.3	Installing the JBoss Application Server and the MySQL Database	74
11.4	Exporting the Correct Path to the Java Installation	75
11.4.1	Setting the Correct Path in the Current Shell	76
11.4.2	Adding the Commands to the /etc/profile.local Script	76
11.4.3	Configuring JRE for the IDMSA Service Account	76
11.5	Installing the Identity Manager User Application	77
11.6	Making JBoss shutdown.sh Executable	80
11.7	Configuring the User Application for Automatic Startup	80
11.8	Configuring the User Application for HTTPS	82
11.9	Importing the Custom Portal Page	84
11.10	Configuring the Organization Chart to Only Display Active Users	87
12	Installing and Configuring Novell Audit	89
12.1	Before Installing Novell Audit	89
12.2	Installing Novell Audit	89
12.3	Creating the Novell Audit Database	91
12.4	Installing the Novell Audit Plug-Ins	91
12.5	Installing the MySQL Connector	92
12.6	Granting the User Application Access to the Cache Directory	93
12.7	Configuring Novell Audit	93
12.7.1	Creating a Channel	93

12.7.2	Configuring the Platform Agent	95
12.7.3	Connecting to the Novell Audit Database	96
12.8	Enabling Audit Events for the User Application	97
13	Removing Temporary Files after Installation	99
14	Initializing the Resource Kit	101
14.1	Final Configuration for the Workflow Process	101
14.2	Starting the Drivers	102
14.3	Getting a Baseline of Business Logic.	103
15	Activating the Resource Kit	105
15.1	Purchasing an Identity Manager Product License	105
15.2	Using a Credential to Activate Identity Manager Products.	105
15.3	Installing a Product Activation Credential.	106
15.4	Viewing Product Activations for Identity Manager and Drivers.	107
A	Documentation Updates	109
A.1	August 29, 2008	109
A.1.1	Installing and Configuring Novell Audit	109

About This Guide

This guide describes the Resource Kit for Novell® Identity Manager and how to create your own Identity Manager images for deployment.

This guide contains the following sections:

- ♦ Chapter 1, “Overview,” on page 11
- ♦ Chapter 2, “Preparing the Environment,” on page 13
- ♦ Chapter 3, “Installing eDirectory,” on page 17
- ♦ Chapter 4, “Installing iManager,” on page 25
- ♦ Chapter 5, “Installing Designer 3.0 for Identity Manager,” on page 41
- ♦ Chapter 6, “Installing the Identity Manager Metadirectory Engine and Drivers,” on page 43
- ♦ Chapter 7, “Configuring the Environment for the Resource Kit,” on page 45
- ♦ Chapter 8, “Installing XPOZ and Executing XPOZ Scripts,” on page 55
- ♦ Chapter 9, “Configuring a Secure Mail Relay for Identity Manager,” on page 59
- ♦ Chapter 10, “Password Configuration,” on page 65
- ♦ Chapter 11, “Installing and Configuring the User Application,” on page 71
- ♦ Chapter 12, “Installing and Configuring Novell Audit,” on page 89
- ♦ Chapter 13, “Removing Temporary Files after Installation,” on page 99
- ♦ Chapter 14, “Initializing the Resource Kit,” on page 101
- ♦ Chapter 15, “Activating the Resource Kit,” on page 105

Audience

This guide is intended for Identity Manager administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the Resource Kit guides, visit the [Novell Compliance Management Platform Documentation Web site](http://www.novell.com/documentation/ncmp10/) (<http://www.novell.com/documentation/ncmp10/>).

Additional Documentation

For documentation on Identity Manager and drivers, see the [Identity Manager Documentation Web site](http://www.novell.com/documentation/idm36/index.html) (<http://www.novell.com/documentation/idm36/index.html>).

For documentation on the Roles Based Provisioning Module, see the [Identity Manager Roles Based Provisioning Module Documentation Web site](http://www.novell.com/documentation/idmrbpm361/index.html) (<http://www.novell.com/documentation/idmrbpm361/index.html>).

For documentation on Novell Audit, see the [Novell Audit Documentation Web site](http://www.novell.com/documentation/novellaudit20/index.html) (<http://www.novell.com/documentation/novellaudit20/index.html>).

Documentation Conventions

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

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

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

Overview

1

The Resource Kit comes with a VMware* image that contains a complete Identity Manager system with all of the products already installed and configured. This guide walks you through creating the same Identity Manager system that comes on the VM. You can follow these instructions to set up your own system to get a better understanding of all of the components that make up an Identity Manager system.

You can also follow these steps to create your own system on hardware instead of on a VM. You can use this system as a starting point for a customer, or use it as a proof of concept to show what Identity Manager can do.

It is important to make sure you install and configure the components in the order listed. If you do not, then the Identity Manager system does not work as designed. Use the following checklist to make sure you install and configure the components in the correct order.

- ❑ Download the correct versions of the products used in the Resource Kit 1.2.
 - ♦ SUSE® Linux Enterprise Server (SLES) 10 SP2
 - ♦ eDirectory™ 8.8.3
 - ♦ iManager 2.7 SP1
 - ♦ Designer 3.0
 - ♦ Identity Manager 3.6
 - ♦ Novell® Audit 2.0.2 FP5
 - ♦ Sentinel™ 6.1
- Section 2.1, “[Downloading Prerequisite Software](#),” on page 13 tells you how to access the software.
- ❑ Create an Identity Manager service account on the SLES server. For security purposes you should avoid logging in to the SLES server as root. Section 2.2, “[Creating an Identity Manager Service User and Group](#),” on page 16 contains these instructions.
- ❑ Enable the SLES server for multicast routing. This is an eDirectory requirement. For more information, see Section 3.1.1, “[Enabling the SLES Server for Multicast Routing](#),” on page 17.
- ❑ Enable Network Time Protocol (NTP). eDirectory and Identity Manager are event-driven systems and rely heavily on time stamps. For more information, see Section 3.1.2, “[Network Time Protocol Configuration](#),” on page 18.
- ❑ Install the Service Location Protocol (SLP). This is an eDirectory requirement. For more information, see Section 3.1.3, “[Installing the SLP User Agent and Server Agent](#),” on page 19.
- ❑ Install eDirectory. For more information, see Section 3.2, “[Installing eDirectory 8.8.3](#),” on page 21.
- ❑ Set the ndspath variable for each shell that is executed. This points the shell to the binary files that must be executed for eDirectory to work and it also enables the man pages for eDirectory. For more information, see Section 3.3, “[Configuring Your Environment](#),” on page 21.
- ❑ Configure eDirectory. For more information, see Section 3.4, “[Configuring eDirectory](#),” on page 22.
- ❑ Install iManager. For more information, see Chapter 4, “[Installing iManager](#),” on page 25.

- ❑ Install Designer. For more information, see [Chapter 5, “Installing Designer 3.0 for Identity Manager,” on page 41](#).
- ❑ Install the Metadirectory engine and the Identity Manager drivers. For more information, see [Chapter 6, “Installing the Identity Manager Metadirectory Engine and Drivers,” on page 43](#).
- ❑ Configure your environment for the Resource Kit. This includes importing LDIF files into eDirectory to extend the schema and to create the eDirectory structure for the Resource Kit. For more information, see [Chapter 7, “Configuring the Environment for the Resource Kit,” on page 45](#).
- ❑ Install the XPOZ test harness, which is used to test the solutions in the Resource Kit. For more information, see [Chapter 8, “Installing XPOZ and Executing XPOZ Scripts,” on page 55](#).
- ❑ (Optional) Configure a secure mail relay for the Identity Manager system, so you can send e-mail without configuring an e-mail system. For more information, see [Chapter 9, “Configuring a Secure Mail Relay for Identity Manager,” on page 59](#).
- ❑ Install and configure the User Application. For more information, see [Chapter 11, “Installing and Configuring the User Application,” on page 71](#).
- ❑ Install and configure Novell Audit. This allows you to track events that occur in the Identity Manager system for compliance. For more information, see [Chapter 12, “Installing and Configuring Novell Audit,” on page 89](#).
- ❑ Initialize the Resource Kit. This includes starting all of the drivers and then migrating the information that is in the Identity Vault into other systems. For more information, see [Chapter 14, “Initializing the Resource Kit,” on page 101](#).
- ❑ Activate the Resource Kit. For more information, see [Chapter 15, “Activating the Resource Kit,” on page 105](#).

Preparing the Environment

2

This section explains the tasks to prepare your Identity Manager Resource Kit environment.

- ♦ [Section 2.1, “Downloading Prerequisite Software,” on page 13](#)
- ♦ [Section 2.2, “Creating an Identity Manager Service User and Group,” on page 16](#)

2.1 Downloading Prerequisite Software

The Resource Kit requires prerequisite software. This section guides you through the process of downloading the software required for installing the Identity Manager Resource Kit. We recommend that you create a `/tmp` directory in the admin user’s home directory and save the prerequisite software there.

- ♦ [Section 2.1.1, “Downloading ISO Files,” on page 13](#)
- ♦ [Section 2.1.2, “Downloading SUSE Linux Enterprise Server \(SLES\) 10 SP2,” on page 14](#)
- ♦ [Section 2.1.3, “Downloading eDirectory 8.8.3,” on page 14](#)
- ♦ [Section 2.1.4, “Downloading iManager 2.7,” on page 14](#)
- ♦ [Section 2.1.5, “Downloading Identity Manager 3.6,” on page 14](#)
- ♦ [Section 2.1.6, “Downloading Designer 3.0 for Identity Manager,” on page 15](#)
- ♦ [Section 2.1.7, “Downloading Novell Audit 2.0.2 FP5,” on page 15](#)
- ♦ [Section 2.1.8, “Downloading the MySQL JDBC Driver \(Connector/J\),” on page 15](#)
- ♦ [Section 2.1.9, “Downloading XPOZ,” on page 15](#)
- ♦ [Section 2.1.10, “Downloading the Resource Kit Designer Project,” on page 16](#)

2.1.1 Downloading ISO Files

If the product that you are downloading is stored as an ISO file, we recommend that you download the ISO file to your local host machine instead of directly in the VM. The reason for this is that the ISO files make the VM very large. You can access the ISO file from the local host as a mounted CD-ROM or DVD in the VM by doing the following:

- 1 Disconnect the CD-ROM device from your VM by selecting *Removable Devices > CD-ROM 1 > Disconnect* from the VM menu.
- 2 Reconfigure your VM to load the ISO file as a CD-ROM or DVD in your virtual CD-ROM/DVD device by selecting *Removable Devices > CD-ROM 1 > Edit*.
- 3 From the VM menu, browse to and select the ISO file in the *Connection -- Use ISO image* section.
- 4 From the VM menu, select *Removable Devices > CD-ROM 1 > Connect* to reconnect the CD-ROM device to your VM.

This causes the OS in your VM to automatically mount the CD-ROM and open it in a file browser.

2.1.2 Downloading SUSE Linux Enterprise Server (SLES) 10 SP2

Information about downloading and installing SLES 10 SP2 is available in “[Downloading the SLES Software](#)” section of the *Identity Manager Resource Kit 1.2 Installation Guide for SUSE Linux Enterprise Server 10 SP2*.

2.1.3 Downloading eDirectory 8.8.3

- 1 From your host machine (not from within the VM), browse to the [Novell® Download Web site \(http://download.novell.com\)](http://download.novell.com).
- 2 In the *Product or Technology* drop-down list, select *eDirectory*, then click *Search*.
- 3 In the list of files, click *Novell eDirectory 8.8.3 CD (ISO) Images*.
- 4 Click *proceed to download*.
- 5 Download the `eDir_88_SP3_Linux.iso` file to a temporary directory on your host machine. For example, `/tmp`.

The file you download is an ISO file. For more information, see “[Downloading ISO Files](#)” on [page 13](#).

2.1.4 Downloading iManager 2.7

When you install iManager, it checks for the latest updates. Support pack 1 is installed during this update.

- 1 From within the VM, browse to the [Novell Download Web site \(http://download.novell.com\)](http://download.novell.com).
- 2 In the *Product or Technology* drop-down list, select *iManager*, then click *Search*.
- 3 In the list of files, click *iManager 2.7*.
- 4 Click *proceed to download*.
- 5 Download the `iMan_27_linux.tgz` file to the `/tmp` directory.

2.1.5 Downloading Identity Manager 3.6

The Identity Manager product contains the Metadirectory engine, Identity Manager driver, and the User Application.

- 1 From your host machine (not from within the VM), browse to the [Novell Download Web site \(http://download.novell.com\)](http://download.novell.com).
- 2 In the *Product or Technology* drop-down list, select *Identity Manager*, then click *Search*.
- 3 In the list of files, click *Identity Manager 3.6 (90-day evaluation until enabled)*.
- 4 Click *proceed to download*.
- 5 Download the `Identity_Manager_3_6_DVD.iso` file to a temporary directory on your host machine. For example, `/tmp`.

NOTE: If you have difficulty downloading large files, you can download the following separate ISO files:

- ♦Identity_Manager_3_6_Linux.iso
 - ♦Identity_Manager_3_6_User_Application.iso
-

For more information, see [Section 2.1.1, “Downloading ISO Files,” on page 13](#).

2.1.6 Downloading Designer 3.0 for Identity Manager

You download Designer 3.0 from the Cool Solutions Web site.

- 1 From within the VM, browse to the [Novell Cool Solutions Web site \(http://www.novell.com/coololutions/dirxml/designer\)](http://www.novell.com/coololutions/dirxml/designer).
- 2 Download the Linux version of Designer 3.0 to the /tmp directory.

2.1.7 Downloading Novell Audit 2.0.2 FP5

- 1 From your host machine (not from within the VM), browse to the [Novell Download Web site \(http://download.novell.com\)](http://download.novell.com).
- 2 In the *Product or Technology* drop-down list, select *Audit*, then click *Search*.
- 3 In the results section, switch to the tab labeled *patches*.
- 4 From the list of files, click *Novell Audit 2.0.2 FP5*.
- 5 Click *proceed to download*.
- 6 Download the `Novell_Audit_202_SP5.iso` file to a temporary directory on your host machine. For example, /tmp.

The file you download is an ISO file. For more information, see [“Downloading ISO Files” on page 13](#).

2.1.8 Downloading the MySQL JDBC Driver (Connector/J)

- 1 From within the VM, browse to [MySQL* Connector/J 5.1 Web site \(http://dev.mysql.com/downloads/connector/j/5.1.html\)](http://dev.mysql.com/downloads/connector/j/5.1.html).
- 2 At the bottom of the page, select *Pick a mirror* for Source and Binaries (`tar.gz`).
- 3 Select a mirror and download the most recent version of the `mysql-connector-java-5.1.6.tar.gz` file to the /tmp directory.

2.1.9 Downloading XPOZ

- 1 From within the VM, browse to the [Identity Manager Resource Kit Download Web site \(http://download.novell.com/index.jsp\)](http://download.novell.com/index.jsp).
- 2 Download the `xpozv61_install.zip` file to the /tmp directory.

2.1.10 Downloading the Resource Kit Designer Project

- 1 From within the VM, browse to the [Identity Manager Resource Kit download Web site \(http://download.novell.com/index.jsp\)](http://download.novell.com/index.jsp).
- 2 Download the `RK12_Project.zip` file to the `/tmp` directory.

The additional project files are included in the Designer project .zip file. “**Designer Project Files**” in the *Identity Manager Resource Kit 1.2 Overview Guide* contains a list of all of the additional files and a description of those files.

2.2 Creating an Identity Manager Service User and Group

As a best practice for security when working with Linux, it is recommended that you do not log in as `root` to the server. For security purposes, run installations and do configurations as an administrative user rather than `root`, if possible. There are many tasks that must be completed when you are logged in as `root`.

If you are logged in as `root`, your server is more vulnerable to external attack. For the Resource Kit, you should create a new administrative user and group. To create an administrative user and group:

- 1 From the *Computer* menu, open the *Control Center*.
- 2 From the *System* section, select *User Management* to launch the *User and Group Administration* tool.
- 3 Authenticate with your `root` password when prompted.
- 4 Select *Add*, then use the following information to create a user:
User’s Full Name: Identity Manager Service Account
Username: `idmsa`
Password: `n0v3ll`
- 5 Click *Accept*.
- 6 Select *Group* to switch from user into group administration mode, then click *Add* to create a new group.
- 7 Name the group *novell*.
- 8 From the *Group Members* list, select *admin*, *idmsa*, and *root*.
- 9 Leave the Group ID set to the default value.
- 10 Do not set a password.
- 11 Click *Accept*.
- 12 Click *Finish* to close the *User and Group Administration Tool*.
- 13 Close the *Control Center*.
- 14 Log out and log back in to inherit the new settings.
- 15 Proceed to **Chapter 3, “Installing eDirectory,” on page 17**.

Installing eDirectory

3

Novell® eDirectory™ installation and configuration is covered in detail in the [eDirectory product documentation \(http://www.novell.com/documentation/edir88/index.html\)](http://www.novell.com/documentation/edir88/index.html); however, the following sections contain information specific to your Metadirectory server setup.

- ♦ [Section 3.1, “Before Installing eDirectory,” on page 17](#)
- ♦ [Section 3.2, “Installing eDirectory 8.8.3,” on page 21](#)
- ♦ [Section 3.3, “Configuring Your Environment,” on page 21](#)
- ♦ [Section 3.4, “Configuring eDirectory,” on page 22](#)
- ♦ [Section 3.5, “Tuning the eDirectory Database Cache Settings,” on page 23](#)

3.1 Before Installing eDirectory

The following sections explain the necessary steps you must take for the Resource Kit to be properly configured before installing eDirectory.

- ♦ [Section 3.1.1, “Enabling the SLES Server for Multicast Routing,” on page 17](#)
- ♦ [Section 3.1.2, “Network Time Protocol Configuration,” on page 18](#)
- ♦ [Section 3.1.3, “Installing the SLP User Agent and Server Agent,” on page 19](#)
- ♦ [Section 3.1.4, “Validating Entries in the /etc/hosts File,” on page 20](#)

3.1.1 Enabling the SLES Server for Multicast Routing

In order for eDirectory to function correctly, multicast routing must be enabled on the SUSE® Linux Enterprise Server (SLES) server.

- 1 From the Computer menu, select *Gnome Terminal* to verify your broadcast address range.
- 2 Enter `netstat -nr` to retrieve the current routing table.
- 3 If you have an entry for 224.0.0.0, you have the correct address range and you can proceed to [“Network Time Protocol Configuration” on page 18](#). If not, continue with Step 4.
- 4 Log in as `root` at the terminal by entering `su`, then enter the `root` password.
- 5 To add the 224.0.0.0 network, enter the following:
`route add -net 224.0.0.0 netmask 255.0.0.0 dev eth0`
- 6 Enter `netstat -nr` again to verify that you now have a network entry for the 224.0.0.0 network.
- 7 Enter `exit` twice to close the Gnome Terminal.
- 8 Proceed to [Section 3.1.2, “Network Time Protocol Configuration,” on page 18](#).

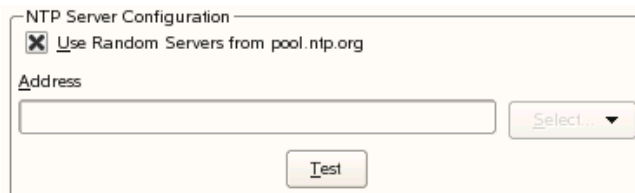
3.1.2 Network Time Protocol Configuration

Both eDirectory and Identity Manager are event-driven systems that rely heavily on time stamps. It is critical to have an accurate common source of time in your Identity Manager solution. Network Time Protocol (NTP) provides this functionality.

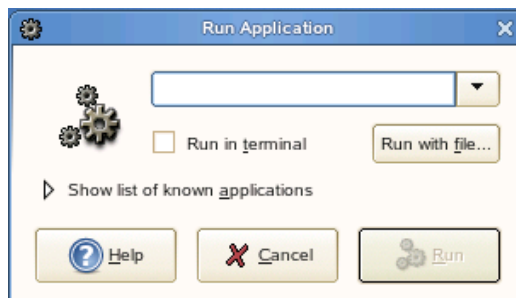
- 1 From the *Computer* menu, open the *Control Center*.
- 2 Select *Open Administrator Settings* to launch YaST.
- 3 Enter the `root` password.
- 4 From *Network Services*, select *NTP Configuration*.
- 5 Select the *During Boot* option to start your NTP Client.



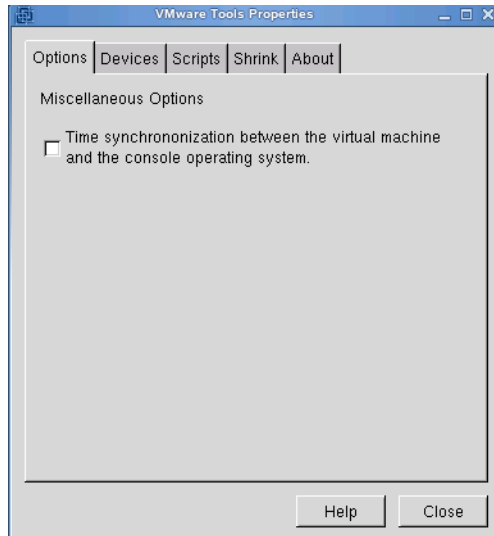
- 6 Click *Continue* in the warning message about the NTP daemon taking a long time to start if you do not have an Internet connection.
- 7 Select *Use Random Servers from pool.ntp.org.*, then click *Finish*.



- 8 Close the YaST Control Center.
- 9 Press Alt+F2 to launch the Run Application dialog box.



- 10 Type `vmware-toolbox`, then click *Run*.
- 11 Click the *Options* tab, then deselect the *Time Synchronization between the virtual machine and host operating system* option.

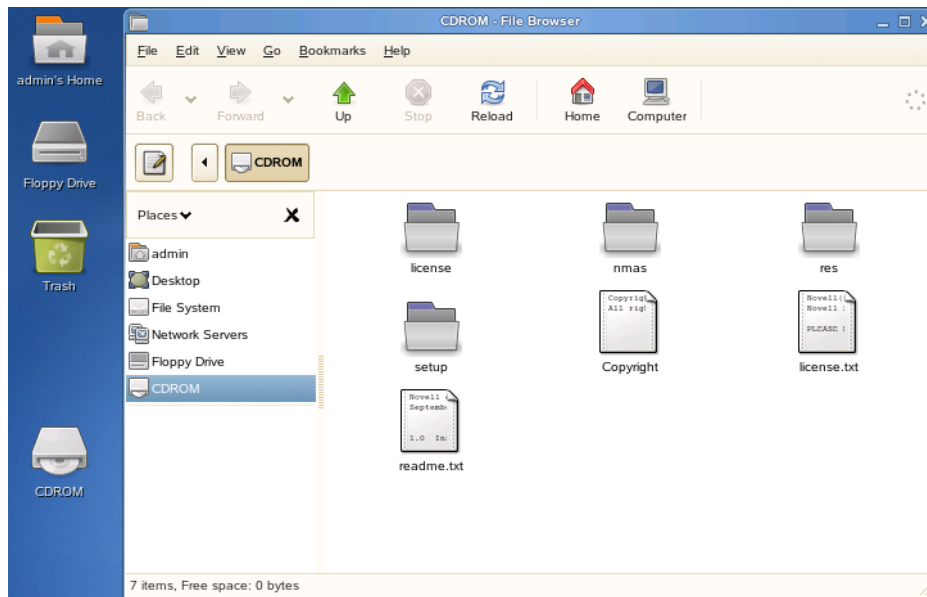


- 12 Click *Close*.
- 13 Proceed to [Section 3.1.3, “Installing the SLP User Agent and Server Agent,”](#) on page 19.

3.1.3 Installing the SLP User Agent and Server Agent

eDirectory Service Lookup Protocol (SLP) must be enabled for searching the network for other eDirectory trees and servers. eDirectory communicates with others servers, and SLP allows communication to occur faster.

- 1 If you are planning on using a physical DVD or CD-ROMs to install eDirectory, insert the installation media into your drive, which must be accessible from with your VM. Continue with [Step 6](#).
- 2 If you are using ISO files, disconnect the CD-ROM device from your VM by selecting *Removable Devices > CD-ROM 1 > Disconnect from the VM menu*.
- 3 Reconfigure your VM to use the eDirectory 8.8.3 for Linux ISO file (`eDir_88_SP3_Linux.iso`) by selecting *Removable Devices > CD-ROM 1 > Edit*.
- 4 From the VM menu, browse to the ISO file in the *Connection -- Use ISO image* section.
- 5 From the VM menu, reconnect the CD-ROM device to your VM by selecting *Removable Devices > CD-ROM 1 > Connect*. This causes SLES to automatically mount the CD-ROM and open a file browser.



- 6 Browse to the `Setup` directory and double-click the `novell-NDSSlp-8.8.2-1.i386.rpm` file to install the package with the Software Installer.
- 7 Authenticate as `root` when prompted, then click *Continue*.
- 8 Verify that the *novell-NDSSlp* package is selected, then click *Install* to start the installation.
- 9 Select *Close* when the installation ends.
- 10 To start the SLP User Agent and Server Agent, go to the *Computer* menu, select *Gnome Terminal*, then complete the following steps:
 - 10a Log in as `root` by entering `su`.
 - 10b Enter the `root` password.
 - 10c Issue the command to start the SLP service: `/etc/init.d/slpuasa start`.
 - 10d If you want to stop the SLP service, issue the command `/etc/init.d/slpuasa stop`.
- 11 Enter `exit` twice to log out as `root` and close the Gnome Terminal.
- 12 Proceed to [Section 3.1.4, “Validating Entries in the /etc/hosts File,” on page 20](#).

3.1.4 Validating Entries in the /etc/hosts File

If your `/etc/hosts` file has the entry `127.0.0.2 metaserver1.idm metaserver1`, then the installation can fail. This entry is placed in the `/etc/hosts` file by the SUSE installation. Many utilities such as `ndsconfig` or `ndssch` do a quick lookup in `/etc/hosts` for the hostname. The utilities read the line indicating that `metaserver1 = 127.0.0.2` and try to connect. This is a dummy address and the utilities cannot connect. The line must be removed or commented out before running any installation.

- 1 From the *Computer* menu, select *Gnome Terminal*.
- 2 Log in as `root` by entering `su`, then enter the `root` password.
- 3 Enter `gedit /etc/hosts`.

- 4 Find the entry `127.0.0.2 metaserver1.idm metaserver1` (your server's DNS name), place a `#` in the front of the line to comment the entry, or delete the line entirely.
- 5 Select *File > Save* to save the changes, then click *File > Quit* to close the utility.
- 6 Enter `exit` twice to log out as `root` and close the Gnome Terminal.
- 7 Proceed to [Section 3.2, “Installing eDirectory 8.8.3,” on page 21.](#)

3.2 Installing eDirectory 8.8.3

Installing eDirectory installs the necessary files and sets up the required daemons. The installation process does not contain any configuration steps.

- 1 From the *Computer* menu, select *Gnome Terminal*.
- 2 Log in as `root` by entering `su`, then enter the `root` password.
- 3 Access the `/media/CROM/setup` directory by entering `cd /media/CDROM/setup/`.
- 4 Enter `./nds-install` to run the eDirectory installation script.
- 5 Press `Enter` to continue the installation.
- 6 Read the license agreement, then press the `Spacebar` until you are asked to accept the license agreement.
- 7 Accept the license agreement by entering `Y`.
- 8 Select to install the eDirectory server and administration utilities by entering `1, 2`.
- 9 Verify that the eDirectory software is now successfully installed on your server. Make sure no errors occurred during the installation.
- 10 Enter `exit` twice to log out as `root` and close the Gnome Terminal.
- 11 Proceed to [Section 3.3, “Configuring Your Environment,” on page 21.](#)

3.3 Configuring Your Environment

Before configuring eDirectory, you need to configure the shell for eDirectory by executing `ndspath` when launching a shell. This points the shell to the eDirectory binary files, and it enables the man pages for eDirectory.

To do this, you add this command to the `/etc/profile.local` file. The following procedure creates the `profile.local` script file in the `/etc` directory and adds the command to this file.

- 1 From the *Computer* menu, select *Gnome Terminal*.
- 2 Log in as `root` by entering `su`, then enter the `root` password.
- 3 Enter the following command: `echo . /opt/novell/eDirectory/bin/ndspath >> /etc/profile.local`.

The entry in the `/etc/profile.local` file is not applied until the server is rebooted, or until you do the following to apply the script to the shell:

- 1 Enter `. /opt/novell/eDirectory/bin/ndspath` to execute the script in your current shell.
or
Enter `source /etc/profile.local` to execute the script file.

- 2 Enter `exit` twice to log out as `root` and close the Gnome Terminal.
- 3 Proceed to [Section 3.4, “Configuring eDirectory,” on page 22.](#)

3.4 Configuring eDirectory

Now that eDirectory is installed, use the values listed in [Table 3-1](#) to configure eDirectory properly for the Resource Kit.

A password for the admin user is listed in the table. It is the same password used in the VM of the Resource Kit. You can use any password you choose.

When a server is installed, there are many objects that are created and associated with the server. As a best practice, each server is installed into a separate container. The container has the same name as the server to keep track of all of the objects associated with the server.

If you have ten server objects in the same container, you automatically get over 100 objects added to that container. It becomes very difficult to manage all of these objects. If each server has its own container, managing the objects becomes an easy task.

Another best practice is to not install eDirectory into the default location. You can install multiple instances of eDirectory on the same server. It is easier to keep track of each installation if the folder that contains the eDirectory files has the same name as the tree.

Table 3-1 *eDirectory Values for the Resource Kit*

Parameter	Value
Tree Name	META
Server Name	metaserver1
Server Context	dc=metaserver1.dc=servers.dc=system
Admin User	cn=admin.dc=admins.dc=system
NCP Port number to listen on	524
eDirectory dib location	/var/opt/novell/eDirectory/META/data/dib
Configuration File	/var/opt/novell/eDirectory/META/nds.conf
Admin User's Password	n0v3ll

- 1 From the *Computer* menu, select *Gnome Terminal* to configure your eDirectory server.
- 2 Log in as `root` by entering `su`, then enter the `root` password.
- 3 Type `ndsconfig new -t META -S metaserver1 -n dc=metaserver1.dc=servers.dc=system -a cn=admin.dc=admins.dc=system -w n0v3ll -i -d /var/opt/novell/eDirectory/META/data/dib -D /var/opt/novell/eDirectory/META/ -b 524 -e --config-file /var/opt/novell/eDirectory/META/nds.conf`
 This command creates a new instance of eDirectory on this server. Here are of all of the options specified and what they mean:

Option	Description
<code>new</code>	Creates a new instance of eDirectory on this server.
<code>-t</code>	Specifies the tree name.
<code>-S</code>	Specifies the server name.
<code>-n</code>	Specifies the server's context.
<code>-a</code>	Specifies the administrator's user name and context.
<code>-w</code>	Specifies the administrator's password.
<code>-i</code>	Ignores looking on the network for a duplicate tree name.
<code>-d</code>	Specifies the path for the eDirectory database files.
<code>-D</code>	Specifies the path for the eDirectory installation files.
<code>-b</code>	Specifies the NCP™ port number.
<code>-e</code>	Disables the TLS authentication via LDAP.
<code>--config-file</code>	Specifies the path for the <code>nds.conf</code> file.

If you receive the message `command not found`, the `ndspath` is not set. See [Section 3.3, “Configuring Your Environment,” on page 21](#) for steps on how to set the `ndspath`.

- 4 Review the message that the eDirectory instance is successfully configured.
- 5 Enter `exit` twice to log out as `root` and close the Gnome Terminal.
- 6 Proceed to [“Tuning the eDirectory Database Cache Settings” on page 23](#).

3.5 Tuning the eDirectory Database Cache Settings

- 1 From within your VM, access [iMonitor \(https://172.17.2.117:8030/\)](https://172.17.2.117:8030/).
- 2 When prompted to *Accept the SSL Certificate for 172.17.2.117*, select *Accept this certificate permanently*, then click *OK*.
- 3 Click the *NDS iMonitor* link.
- 4 Authenticate as *admin.admins.system* and use the password you chose during the eDirectory configuration process.
- 5 In the navigation panel, select *Agent Configuration > Database Cache*.
- 6 Scroll down to the Database Cache Configuration and click the *Hard Limit* button, then specify *128000* for the *Cache Maximum Size*.
- 7 Set the *Block Cache Percentage* to *40%*.
- 8 Select the option *Cache Settings Permanent*.

NDS™ iMonitor Tue Nov 27 11:14:21 2007

Agent Configuration

Novell.

.CN=metaserver1. dc=metaserver1. dc=servers. dc=system. T=META.

Identity: [.CN=admin. dc=admins. dc=system. META.](#)

Refresh Settings:

Refresh On

Refresh Interval

15 seconds

Agent Configuration:

[Agent Information](#)

[Partitions](#)

[Replication Filters](#)

[Agent Triggers](#)

[Background Process Settings](#)

[Agent Synchronization](#)

[Schema Synchronization](#)

Database Cache

[Login Settings](#)

Permanent Settings

Dynamic Adjust

Cache Adjust Percentage 51 % of Available Memory

Cache Size Constraints > 16384 KB < Total Available Memory - 24576 KB

Hard Limit

Cache Maximum Size 128000 KB

Block Cache Percentage 40 %

Cache Adjust Interval 15 secs

Cache Cleanup Interval 15 secs

Cache Settings Permanent ☒

Submit

Done 172.17.2.117:8030

- 9 Select *Submit* to save your changes.
- 10 Close your browser to exit iMonitor.
- 11 Proceed to **Chapter 4, “Installing iManager,”** on page 25.

Installing iManager

4

Now that you have installed eDirectory™ 8.8.3, you should install iManager to manage eDirectory and the Identity Manager system.

- ♦ [Section 4.1, “Installing iManager 2.7 SP1,” on page 25](#)
- ♦ [Section 4.2, “Post-Installation Tasks for iManager 2.7 SP1,” on page 26](#)

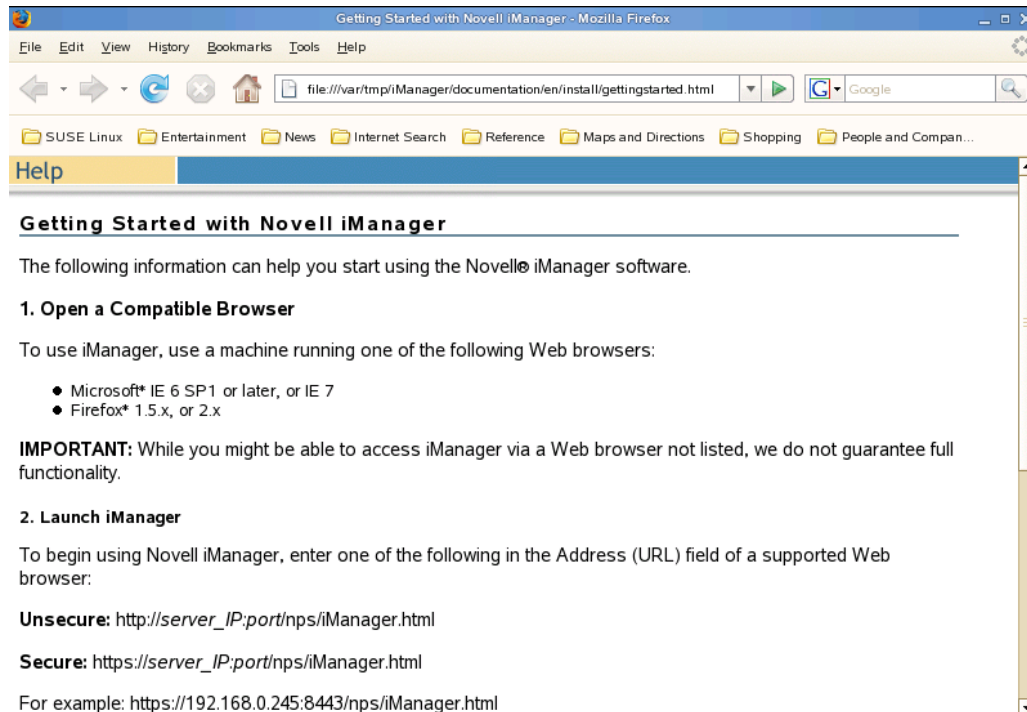
4.1 Installing iManager 2.7 SP1

NOTE: As part of the iManager installation, you will install the iManager plug-ins. You should have an active Internet connection (verify by pinging the gateway, then the Novell download site) before starting the installation process.

- 1 From the *Computer* menu, select *Gnome Terminal*.
- 2 Access the directory where you downloaded the iManager installation file by entering `cd /usr/tmp`.
- 3 Untar the installation file by entering `tar -xzf iMan_27_linux.tgz`.
- 4 Log in as `root` by entering `su`, then enter the `root` password.
- 5 Change to the installation directory by entering `cd iManager/installs/linux/`.
- 6 Start the iManager installation by entering `./iManagerInstallLinux.bin`.
- 7 Enter 2 to select English and the installation language.
- 8 Read the introduction message, then press Enter to continue.
- 9 Read the license agreement, then press Enter until you are prompted to accept the license agreement.
- 10 Enter Y to accept the license agreement.
- 11 Press Enter to select the default components to install: iManager 2.7, Tomcat, and the JVM*.
- 12 Press Enter to download plug-ins.
- 13 Press Enter to accept the default network URL to download plug-ins from.
- 14 Press Enter to select the default plug-ins to install.
The number of available plug-ins changes with product releases. We recommend that you accept the default value.
- 15 Enter 2 to not install the plug-ins from a local directory.
It is easier to install additional plug-ins after iManager is installed.
- 16 Enter 8081 for the Tomcat port number.
- 17 Press Enter to accept the default value (8443) for the SSL port.
- 18 Specify the admin user's full context of `admin.admins.system`.
- 19 Specify the name of the eDirectory tree `META`.
- 20 Review the summary of the installation information specified, then enter 1 to proceed or 2 to make any necessary changes.

- 21 Press Enter after iManager has been successfully installed.

The installation wizard launches your browser and points it to a local Getting Started with Novell iManager page.



- 22 Enter `exit` twice to log out as `root` and close the Gnome Terminal.
- 23 Proceed to [Section 4.2.1, “Granting File Access Rights to the Novell Service Group,” on page 26](#). The file access rights need to be granted before launching iManager.

4.2 Post-Installation Tasks for iManager 2.7 SP1

This section explains how to add additional plug-ins and how to configure iManager with a permanent certificate. You must also grant administrator user’s rights to the `/opt/novell` directory.

- [Section 4.2.1, “Granting File Access Rights to the Novell Service Group,” on page 26](#)
- [Section 4.2.2, “Installing Additional Plug-Ins,” on page 27](#)
- [Section 4.2.3, “Configuring eDirectory and iManager for Role-Based Services,” on page 28](#)
- [Section 4.2.4, “Configuring iManager With a Trusted Certificate,” on page 33](#)
- [Section 4.2.5, “Converting the Certificate File to the Appropriate File Type,” on page 38](#)

4.2.1 Granting File Access Rights to the Novell Service Group

After the graphical installer quits, use the following procedure to restart the Tomcat Web server and to grant the new novell services group file access rights to `/opt/novell`.

- 1 From the *Computer* menu, select *Gnome Terminal*.
- 2 Log in as `root` by entering `su`, then enter the `root` password.


- 3 Stop the Tomcat Web server by entering `/etc/init.d/novell-tomcat5 stop`.
- 4 Enter `chmod 775 /opt/novell/` to change the rights to the `/opt/novell` directory.
- 5 Enter `chown idmsa:novell /opt/novell` to grant any user that is a member of the `novell` group the rights that the user `idmsa` has to the `/opt/novell` directory.
- 6 To verify that the changes took place, enter `ls -l /opt`.
The `novell` directory rights should be `drwxrwxr-x 10 idmsa novell`.
- 7 Start the Tomcat Web server by entering `/etc/init.d/novell-tomcat5 start`.
- 8 Enter `exit` twice to log out as `root` and close the Gnome Terminal.
- 9 Proceed to [Section 4.2.2, “Installing Additional Plug-Ins,” on page 27](#).

4.2.2 Installing Additional Plug-Ins

iManager can detect if there are additional plug-in updates that need to be installed.

- 1 Launch iManager by pointing your browser to `https://172.17.2.117:8443/nps/iManager.html`.
 - 2 Select *Accept this certificate permanently* in the temporary certificate message, then click *OK*.
 - 3 Click *OK* in the security error.
- [Section 4.2.4, “Configuring iManager With a Trusted Certificate,” on page 33](#) explains how to set up a permanent certificate for iManager to use.
- 4 Use the following information to log in, then click *Login*.
 - ♦ **Username:** admin
 - ♦ **Password:** n0v3ll (or the password you chose)
 - ♦ **Tree:** 172.17.2.117



- 5 Select *Configure*  in the iManager header frame.
- 6 Select *Plug-in Installation > Available Novell Plug-in Modules*. All of the plug-ins that are available to install and that need to be updated are listed here.
- 7 Click the box by the *Name* column to select all of the plug-ins, then click *Install*.

Novell Plug-in Modules	
Add Install Remove Refresh	
<input checked="" type="checkbox"/>	Name

This can take a long time, depending upon how many plug-ins need to be installed.

- 8 Click *Close* twice after all of the modules have been successfully installed, then close the Web browser.

Support pack 1 is installed during this update.

Tomcat must be restarted for iManager to display the new plug-ins.

- 1 From the *Computer* menu, select *Gnome Terminal*.
- 2 Log in as `root` by entering `su`, then enter the `root` password.
- 3 Enter `/etc/init.d/novell-tomcat5 stop`.
- 4 When the prompt is returned, enter `/etc/init.d/novell-tomcat5 start`.
- 5 Enter `exit` twice to log out as `root` and close the Gnome Terminal.

The next time you launch iManager, all of the new plug-ins are displayed.

- 6 Proceed to [Section 4.2.3, “Configuring eDirectory and iManager for Role-Based Services,” on page 28](#).

4.2.3 Configuring eDirectory and iManager for Role-Based Services

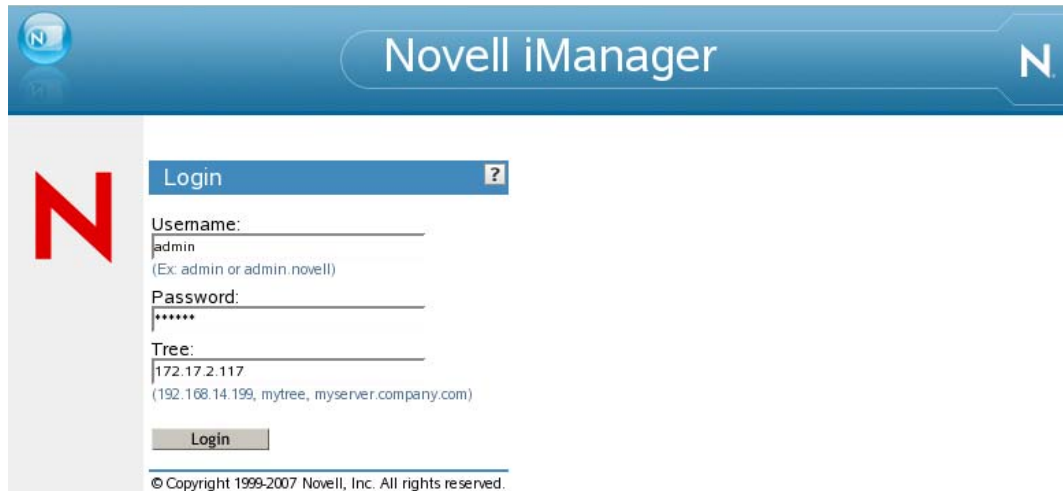
Role-Based Services allows you control who has access to features in iManager. For security reasons, it is best practice to use iManager with the Role-Based Services enabled.


In order for your system to be like the Resource Kit image, a container needs to be created before enabling the Role-Based Services.

- ♦ [“Creating the Services Container” on page 28](#)
- ♦ [“Enabling Role-Based Services” on page 30](#)

Creating the Services Container

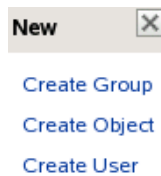
- 1 Launch iManager by pointing your browser to `https://172.17.2.117:8443/nps/iManager.html`.
- 2 Click *OK* in the security error.
[Section 4.2.4, “Configuring iManager With a Trusted Certificate,” on page 33](#) explains how to set up a permanent certificate for iManager to use.
- 3 Use the following information to log in, then click *Login*.
 - ♦ Username: `admin`
 - ♦ Password: `n0v3ll`
 - ♦ Tree: `172.17.2.117`



- 4 Select *View Objects*  in the iManager header frame.
- 5 Select the system container. The objects that are stored under the system container are displayed on the right.



- 6 Click *New*, then select *Create Object*.



- 7 Select *domain*, then click *OK*.

Select the object class to create.


Available object classes:

Alias
Computer
Country
Domain
Dynamic Group
Group
Locality
Organization
Organizational Person
Organizational Role

☐ Show all object classes
Note: This option is only available to authorized users.

OK Cancel

- 8 In the *domain name* field, specify *services* as the name of the domain.
- 9 Leave the context as *system*, then click *OK*.

 **Create domain**


Specify the object name to be created.

domain name:
services

Context:
system

OK Cancel

- 10 Click *OK* in the completion message.

 **Complete: The Create domain request succeeded**


The new domain was created: services.system.META.

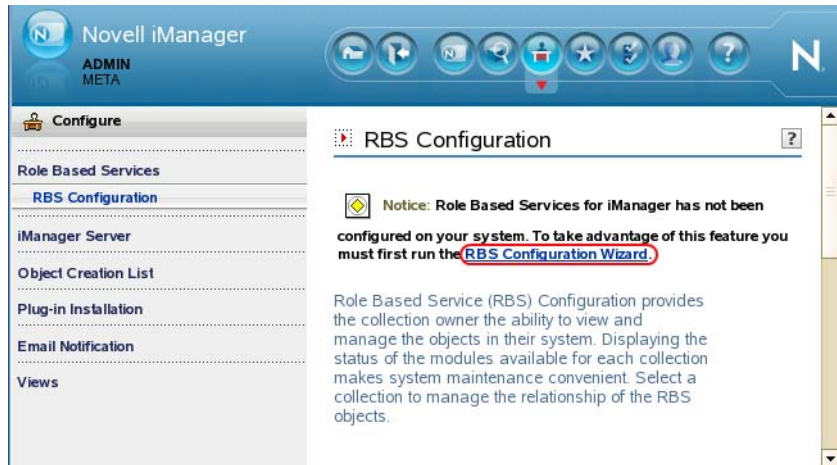
OK Repeat Task Modify

The container is now created, and the Role-Based Services can now be enabled.

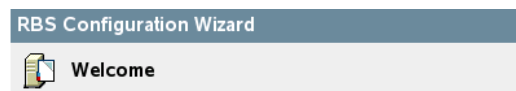
- 11 Proceed to **“Enabling Role-Based Services”** on page 30.

Enabling Role-Based Services

- 1 Select *Configure*  in the iManager header frame.
- 2 Select *Role Based Services > RBS Configuration*.
- 3 Select the *RBS Configuration Wizard* link.



- 4 Read the welcome message, then click *Next*.



Either the RBS schema definitions have not been installed or they are out of date. Select Next to extend the schema and continue with iManager configuration.

- 5 Leave the default value of Role Based Service 2 in the *Name* field.

- 6 Browse to and select the services.system container for the *Container* field, then click *Next*.

RBS Configuration Wizard

Collection Information

In order to use iManager, a collection object must be created. You currently do not own any collections. The collection should be created by a qualified iManager administrator. If you are not qualified, please select Close now and contact your iManager administrator.

Name:

Container:  



<< Back Next >> Close Start

- 7 Leave all of the modules selected so that they can be installed.

Modules to be installed:

Service Manager	 	Select All
SMS Backup and Restore		Deselect All
SNMP		
Storage Content		
WAN Traffic Manager Plugin		

- 8 Browse to and select the tree .META for the *Scope* field.

Scope:  

☒ Assign Rights


☒ Inheritable

A scope is a container in which members of a role can perform tasks. 'Inheritable' scopes allow tasks to be performed in all subcontainers of the scope you specify.

- 9 Leave *Assign Rights* and *Inheritable* selected, then click *Start*.

- 10 After the wizard completes, click *Close*.

RBS Configuration Wizard

 **Completed:** Module Update

Update Update Interval... Cancel

The following messages were returned from the configuration process.

```

Creating collection (Role Based Service 2)
----Updating collection (Role Based Service 2.services.syste

```

<< Back Next >> Close Start

- 11 Proceed to [Section 4.2.4, “Configuring iManager With a Trusted Certificate,”](#) on page 33.


4.2.4 Configuring iManager With a Trusted Certificate

When iManager 2.7 SP1 is installed on a Linux server and that server does not have the Apache Web service installed, the server is using iManager 2.7 SP1's Tomcat Web service for HTTP/HTTPS. A certificate and keystore are used for secure HTTPS traffic between a client Web browser and iManager's Tomcat service. This certificate must be accepted by all client browsers connecting to iManager.

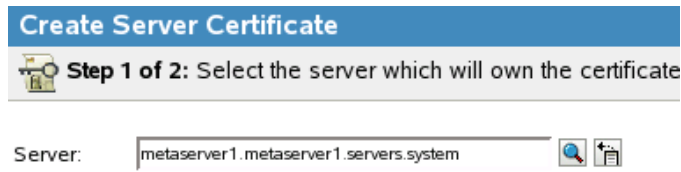
By default, a temporary non-trusted CA signed certificate is generated once during the installation of iManager. This non-trusted signed certificate has a CN of Temporary Certificate and an expiration date of one year. You can replace this certificate with a certificate signed by a trusted CA. If you configure Access Manager to authenticate to iManager, a certificate chained to a CA must be used or the Access Manager to iManager authentication fails.

The following steps were taken from TID 3092268 with minor modifications to adapt to the Resource Kit requirements.

- 1 Launch iManager by pointing your browser to <https://172.17.2.117:8443/nps/iManager.html>
- 2 Click *OK* in the security error.
- 3 Use the following information to log in, then click *Login*.
 - ♦ Username: admin
 - ♦ Password: n0v3ll (or the password you chose)
 - ♦ Tree: 172.17.2.117

The image shows the Novell iManager login interface. At the top is a blue header bar with the Novell logo on the left, the text "Novell iManager" in the center, and another Novell logo on the right. Below the header is a login form. On the left side of the form is a large red "N" logo. The form has a "Login" button at the top right. Below it are fields for "Username:" (with a help icon), "Password:" (with a masked password "*****"), and "Tree:" (with a dropdown menu showing "172.17.2.117" and a list of other options). A "Login" button is at the bottom of the form. At the very bottom, there is a copyright notice: "© Copyright 1999-2007 Novell, Inc. All rights reserved."

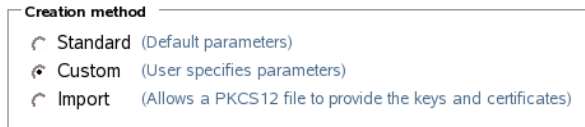
- 4 Select *Novell Certificate Server > Create Server Certificate*.
- 5 Browse to and select the server `metaserver1.metaserver1.servers.system` for the *Server* field.

The image shows the "Create Server Certificate" wizard, specifically "Step 1 of 2: Select the server which will own the certificate". The title bar says "Create Server Certificate". Below the title bar is a key icon and the text "Step 1 of 2: Select the server which will own the certificate". There is a "Server:" label followed by a text box containing "metaserver1.metaserver1.servers.system". To the right of the text box are two icons: a magnifying glass and a folder icon.

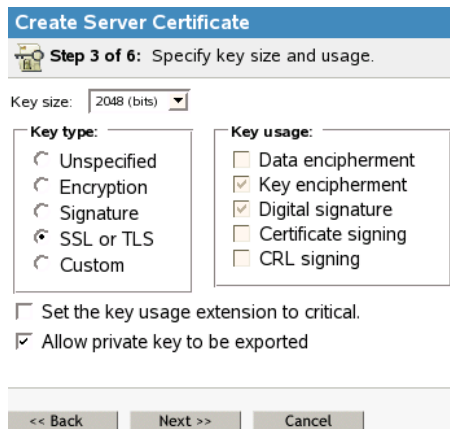
- 6 Specify a meaningful name in the *Nickname* field, such as *imanager*.

Nickname:

- 7 Choose *Custom* for the *Creation method*, then click *Next*.

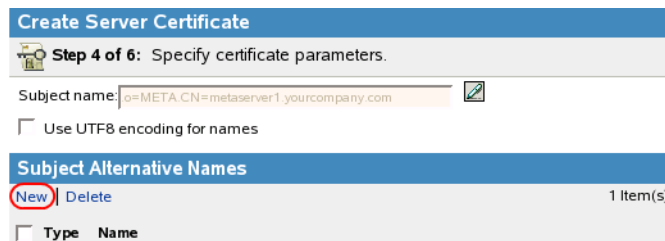


- 8 Select *Organizational certificate authority* to have the eDirectory tree's certificate authority sign the certificate, then click *Next*.
- 9 In Step 3 of the wizard, accept the defaults, then click *Next*.

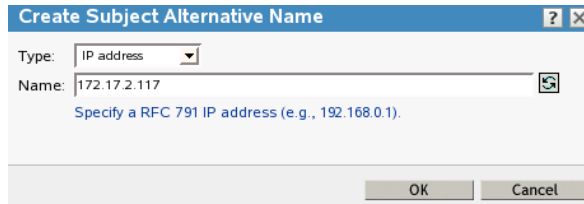


The default values are:

- ♦ Key type: *SSL or TLS*
 - ♦ Key usage: *Key encipherment* and *Digital signature*
 - ♦ *Allow private key to be exported*
 - ♦ *Enable extended key usage*
 - ♦ Extended key type: *Server*
 - ♦ Extended key usage: *Server authentication*
- 10 Click *New* to add a new *Subject Alternative Name*.



- 11 For *Type*, select *IP address*. In the *Name* field, specify *172.17.2.117*, then click *OK*.



Create Subject Alternative Name

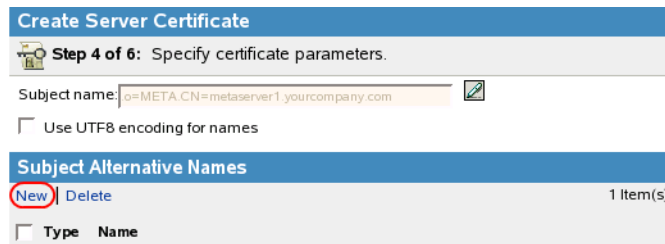
Type: IP address

Name: 172.17.2.117

Specify a RFC 791 IP address (e.g., 192.168.0.1).

OK Cancel

- 12 Create a second *Subject Alternative Name* by clicking *New* again.



Create Server Certificate

Step 4 of 6: Specify certificate parameters.

Subject name: o=META.CN=metaserver1.yourcompany.com

☐ Use UTF8 encoding for names

Subject Alternative Names

New Delete 1 Item(s)

☐ Type Name

- 13 For *Type*, select *DNS name*. In the *Name* field, specify `metaserver1.idm`, then click *OK*.



Create Subject Alternative Name

Type: DNS name

Name: metaserver1.idm

Specify a Domain Name Service (DNS) name (e.g., www.YourCompany.com).

OK Cancel

- 14 Verify that only the two alternative names are listed.



Create Server Certificate

Step 4 of 6: Specify certificate parameters.

Subject name: o=META.CN=metaserver1.yourcompany.com


☐ Use UTF8 encoding for names

Subject Alternative Names

New Delete 2 Item(s)

Type	Name
IP	172.17.2.117
DNS	metaserver1.idm

- 15 Set the *Signature algorithm* to *SHA1-RS*.



Create Server Certificate

Step 4 of 6: Specify certificate parameters.

Signature algorithm:

SHA1-RSA

SHA-1 (Secure Hash Algorithm version 1) is a message digest function proposed by the National Institute of Standards and Technology (NIST). Novell recommends SHA-1 for all generated public key certificates.

- 16 Set the *Validity period* to *Maximum*.

Create Server Certificate

Step 4 of 6: Specify certificate parameters.

Validity period:

Validity period: Maximum

Effective date: Monday, December 10, 2007 2:13:00 PM

Expiration date: Thursday, December 07, 2017 10:35:00 AM

The maximum validity period is ten years. Certificates should expire intermittently to increase the level of security. Depending upon your company's policies, a ten-year validity period might be too long.

- 17** There are no *Custom Extensions* to add, so click *Next*.

Custom Extensions

[New](#) | [Delete](#) 0 Item(s)

☐ Extension File

No items

[<< Back](#) [Next >>](#) [Cancel](#)

- 18** In Step 5 of the wizard, select *Your organization's certificate*, then click *Next*.

Create Server Certificate

Step 5 of 6: Select the trusted root certificate to be associated with this server certificate.

☒ **Your organization's certificate**

The server certificate will chain back to the self-signed certificate of the organizational certificate authority.

☐ **Novell Root Certifier's certificate**

The server certificate will chain back to the global root for Novell Inc. Select this option only if the certificate will be used with software capable of processing the Novell Security Attributes(TM).

- 19** Review the Summary page, then click *Finish*.

- 20** Read the success message, then click *Close*.

Create Server Certificate

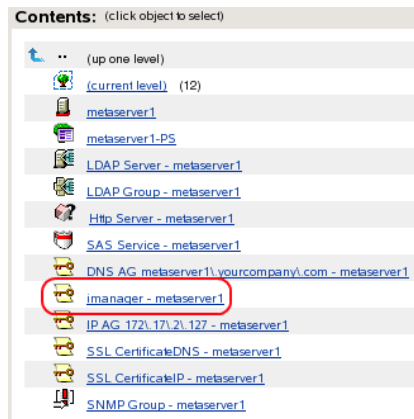
The following are the results of the Create Server Certificate request.

1 Item(s)

Name	Result
.o=META.CN=metaserver1.yourcompany.com	<input checked="" type="checkbox"/> Success

- 21** Under *Roles and Tasks*, select *Directory Administration > Modify Object*.

- 22** Browse to and select the KMO object named imanager-metaserver1, then click *OK*.

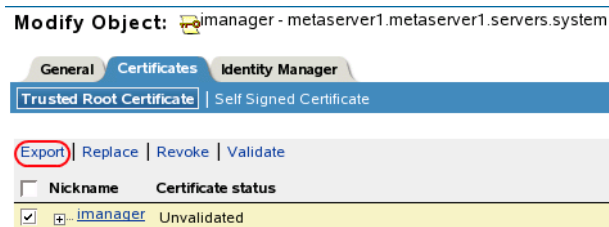


The context of the object is metaserver1.servers.system.

- 23** Click the *Certificates* tab, then select *Trusted Root Certificate*.

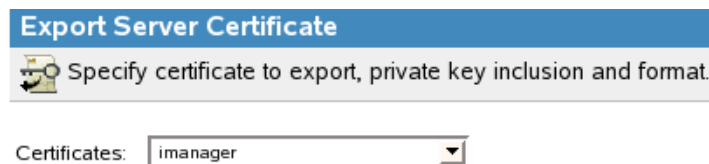


- 24** Select the certificate check box, then click *Export*.



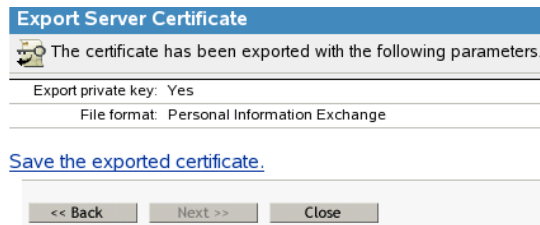
The certificate is listed by the nickname.

- 25** In the *Certificates* field, select *imanager*.



- 26** Leave the *Export private key* option selected and specify a password (the Resource Kit uses the password changeit), then click *Next*.

- 27** Select *Save the exported certificate*.



- 28 Click *Save File*.
- 29 Close Web the browser window after the file is saved.
- 30 Click *OK* to close the export wizard.
- 31 Exit iManager.
- 32 Proceed to [Section 4.2.5, “Converting the Certificate File to the Appropriate File Type,” on page 38](#).

4.2.5 Converting the Certificate File to the Appropriate File Type

You must convert the `pkcs12.pfx` file to a `.pem`, then finally to a `.p12` file so that it can be consumed by Tomcat.

NOTE: The example uses *changeit* for every password and passphrase.

- 1 From the *Computer* menu, select *Gnome Terminal*.
- 2 Log in as `root` by entering `su`, then enter the `root` password.
- 3 Change to the directory where the `cert.pfx` certificate file was saved.
- 4 Enter `openssl pkcs12 -in cert.pfx -out imanagercert.pem`.
- 5 Specify an import password.
- 6 Specify a PEM passphrase twice.
- 7 Enter `openssl pkcs12 -export -in imanagercert.pem -out imanagercert.p12 -name "iManager"`.
- 8 Specify the passphrase for `imanagercert.pem`.
- 9 Specify the export password twice.
- 10 Move the `imanagercert.p12` file by entering:

```
mv imanagercert.p12 /var/opt/novell/novlwww/
```
- 11 Change the owner of the new directory `novlwww` by entering:

```
chown novlwww /var/opt/novell/novlwww/imanagercert.p12
```
- 12 Change the permission on the `imanagercer.p12` file by entering:

```
chmod 654 /var/opt/novell/novlwww/imanagercert.p12
```
- 13 Remove the files from the working directory by entering:

```
rm cert.pfx imanagercert.pem
```
- 14 Stop Tomcat by entering `/etc/init.d/novell-tomcat5 stop`.

15 To edit the Tomcat configuration file, enter `gedit /etc/opt/novell/tomcat5/server.xml`.

16 Locate the `clientAuth="false" protocol="TLS"` line.

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->

<Connector port="8443" maxThreads="150" minSpareThreads="25"
maxSpareThreads="75" enableLookups="true" disableUploadTimeout="true"
acceptCount="100" debug="0" scheme="https" secure="true" clientAuth="false"
sslprotocol="TLS" />
```

17 Add the following statements regarding `keystoreType` and `keystoreFile`, substituting the applicable p12 filename.

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<Connector port="8443" maxThreads="150" minSpareThreads="25"
maxSpareThreads="75" enableLookups="true" disableUploadTimeout="true"
acceptCount="100" debug="0" scheme="https" secure="true" clientAuth="false"
sslprotocol="TLS"
keystoreType="PKCS12" keystoreFile="/var/opt/novell/novlwww/imanagercert.p12"
/>
```

When the keystore type is changed to PKCS12, you must specify the entire path because Tomcat no longer defaults to using the Tomcat home path.

18 Select *File > Save* to save the changes, then select *File > Quit* to exit the editor.

19 Restart Tomcat by entering `/etc/init.d/novell-tomcat5 start`.

The next time you log into iManager, it prompts you to accept this certificate.

20 Enter `exit` twice to log out as `root` and close the Gnome Terminal.

21 Proceed to [“Installing Designer 3.0 for Identity Manager” on page 41](#).

Installing Designer 3.0 for Identity Manager

5

Designer is a client-based tool that is used to design and develop an Identity Manager solution. The Resource Kit contains a completed Identity Manager solution that is imported into Designer, then deployed into the Identity Vault. To install Designer:

- 1 From the *Computer* menu, select *Gnome Terminal*.
- 2 Do not log in as `root`.
If the steps in [Section 4.2.1, “Granting File Access Rights to the Novell Service Group,” on page 26](#) have been completed, you can run the installation as the admin user.
- 3 Change to the `/usr/tmp` directory where the installation files are stored by entering `cd /usr/tmp`.
- 4 Untar the Designer installation file by entering `tar -zxf designer_linux_.tar.gz`.
- 5 Change to the installation directory by entering `cd designer_install`.
- 6 Start the Designer installation by entering `./install`.
- 7 Use the following information to complete the installation:

Installation Screen	Fields
Designer for Identity Manager	Select the language for the installation program to use. The default is <i>English</i> .
Introduction	Read the introduction.
License Agreement	Read the License Agreement, then select <i>I accept the terms of the License Agreement</i> .
Designer for Identity Manager Install Folder	Change the installation location to <code>/opt/novell/designer</code> .
Select Language	Select a language you want Designer to use. The default value is <i>English</i> .
Pre-Installation Summary	Review the summary, then start the installation.
Important Information	Read the Readme.
Install Complete	Read the message about the successful installation.

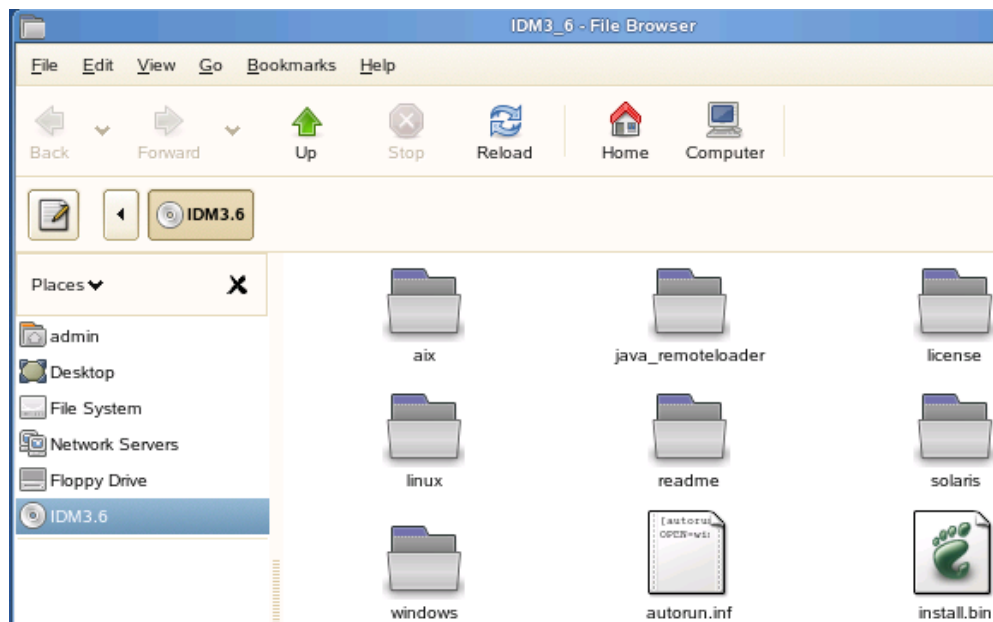
- 8 Proceed to [Chapter 6, “Installing the Identity Manager Metadirectory Engine and Drivers,” on page 43](#).

Installing the Identity Manager Metadirectory Engine and Drivers

6

Identity Manager contains many components. The Metadirectory engine and drivers need to be installed before installing the User Application.

- 1 If you are planning on using a physical DVD or CD-ROMs to install Identity Manager, insert the installation media into your drive, which must be accessible from within your VM. Continue with **Step 6**.
- 2 If you are using ISO files, disconnect the CD-ROM device from your VM by selecting *Removable Devices > CD-ROM 1 > Disconnect from the VM menu*.
- 3 Reconfigure your VM to use the Identity Manager 3.5.1 ISO file (*Identity_Manager_3_5_1_DVD.iso*) by selecting *Removable Devices > CD-ROM 1 > Edit*.
- 4 From the VM menu, browse to the ISO file in the *Connection -- Use ISO image* section.
- 5 From the VM menu, reconnect the CD-ROM device to your VM by selecting *Removable Devices > CD-ROM 1 > Connect*. This causes the Identity Manager 3.5.1 ISO to automatically mount the CD-ROM and open a file browser.



- 6 From the *Computer* menu, select *Gnome Terminal*.
- 7 Log in as `root` by entering `su`, then specify `root`'s password.
- 8 Access the Identity Manager installation directory by entering `cd /media/IDM3_6/`.
- 9 Start the installation by entering `./install.bin`.
This launches the graphical installer.
- 10 Use the following information to complete the installation:

Installation Screen	Description
Novell Identity Manager	Select the language you want the install program to use.
Introduction	Read the introduction information.
License Agreement	Read the license agreement, then select <i>I accept the terms of the License Agreement</i> .
Select Components	Select <i>Novell Identity Manager Metadirectory Server</i> , <i>Novell Identity Manager Web-based Administrator Server</i> , and <i>Utilities</i> . This installs the Metadirectory engine, the driver configurations files, and the iManager plug-ins for Identity Manager.
Identity Manager Activation Notice	Read the activation information. NOTE: If the error <code>LD_LIBRARY_PATH</code> is not set occurs, the <code>ndspath</code> variable has not been set for the current shell. For more information, see Section 3.3, "Configuring Your Environment," on page 21. Set the <code>ndspath</code> variable and start the installation again.
Authentication	Enter <code>cn=admin,dc=admins,dc=system</code> for the username, then enter <code>n0v3l1</code> for the password.
Pre-Installation Summary	Review the summary, then start the installation.
Installation Complete	Read the installation completed successfully message.

- 11** Restart Tomcat to display the new plug-ins.
 - 11a** Enter `/etc/init.d/novell-tomcat5 stop`.
 - 11b** When the prompt is returned, enter `/etc/init.d/novell-tomcat5 start`.
- 12** Enter `exit` twice to log out as `root` and close the Gnome Terminal.
- 13** Proceed to [Chapter 7, "Configuring the Environment for the Resource Kit,"](#) on page 45.

Configuring the Environment for the Resource Kit

7

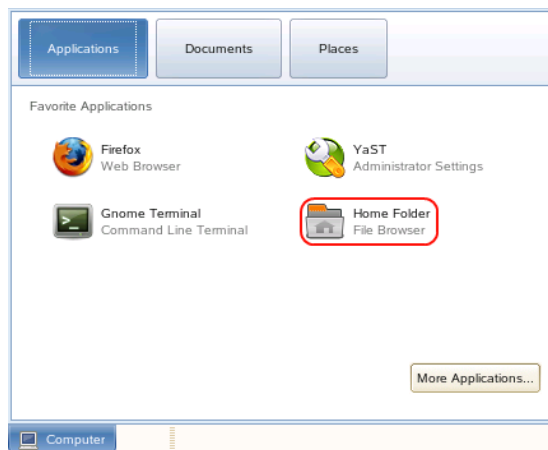
For your environment to be configured exactly like the Resource Kit VM, there are certain tasks that must be completed. These tasks must be completed before the installation of the User Application.

- ♦ [Section 7.1, “Importing the Resource Kit Designer Project,” on page 45](#)
- ♦ [Section 7.2, “Loading the Resource Kit Structure into the Identity Vault,” on page 48](#)
- ♦ [Section 7.3, “Populating the Identity Vault with the Resource Kit Data,” on page 49](#)
- ♦ [Section 7.4, “Prerequisites for the Delimited Text Driver,” on page 53](#)
- ♦ [Section 7.5, “Making eDirectory Visible on the External IP Address,” on page 54](#)

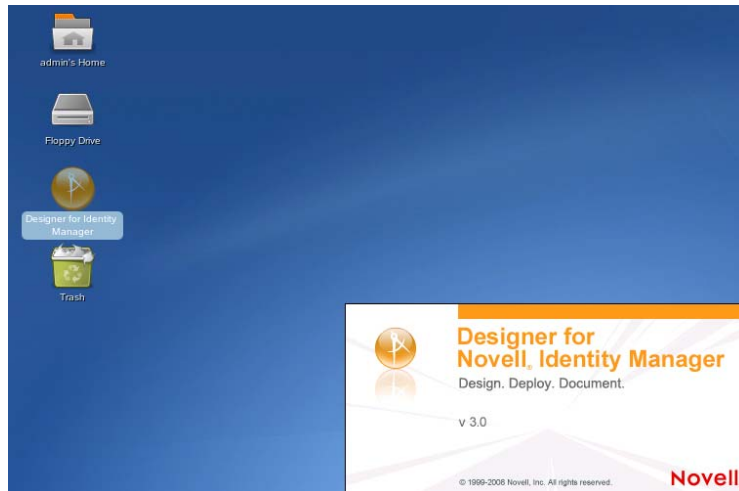
7.1 Importing the Resource Kit Designer Project

There are many configuration files for the Resource Kit that are stored as part of the Designer project. Use the following procedure to import the project into Designer and gain access to these files.

- 1 From the *Computer* menu, select *Home Folder*.

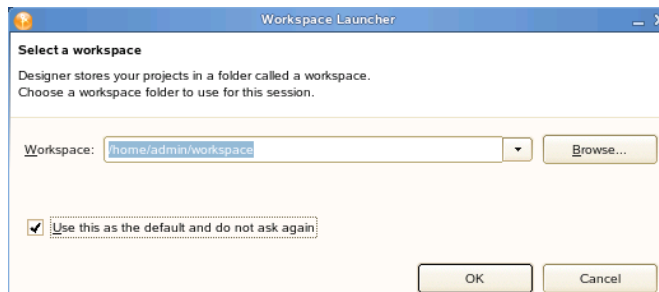


- 2 Select *File System* on the left.
- 3 Browse to and select the `/usr/tmp` folder.
- 4 Right-click the `RK12_Project.zip` file, then select *Extract Here*.
This creates a directory named `RK12` in the `/usr/tmp` directory.
- 5 Launch Designer by double-clicking the Designer icon on the desktop.



6 Accept `/home/admin/workspace` as the default location for the Designer workspace.

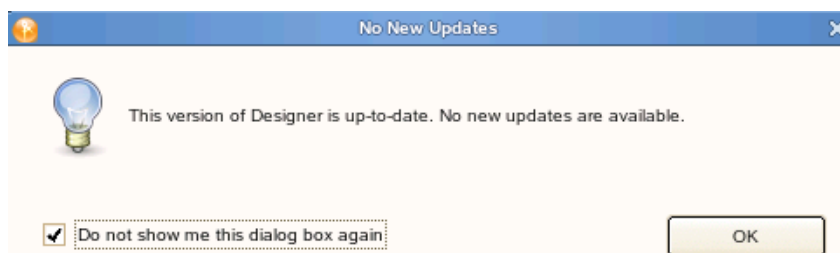
7 Select *Use this as the default and do not ask again*, then click *OK*.



8 When you are prompted to check for updates to Designer, select *Yes* if you have Internet connectivity, or select *No* if you do not.

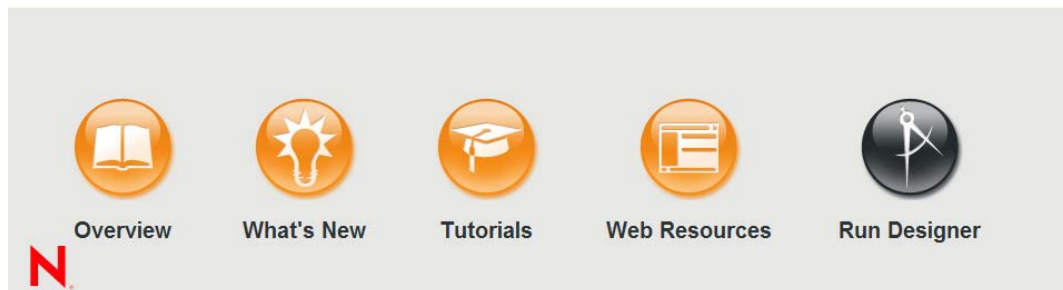
9 To save the setting, select *Remember this selection each time Designer starts*, then click *OK*.

10 If you chose to check for online updates and no updates are found, you see the following dialog box. If you don't want to see the dialog box again, select *Do not show me this dialog box again*, then click *OK*.

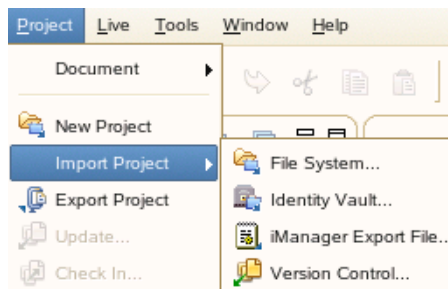


11 Explore the welcome page.

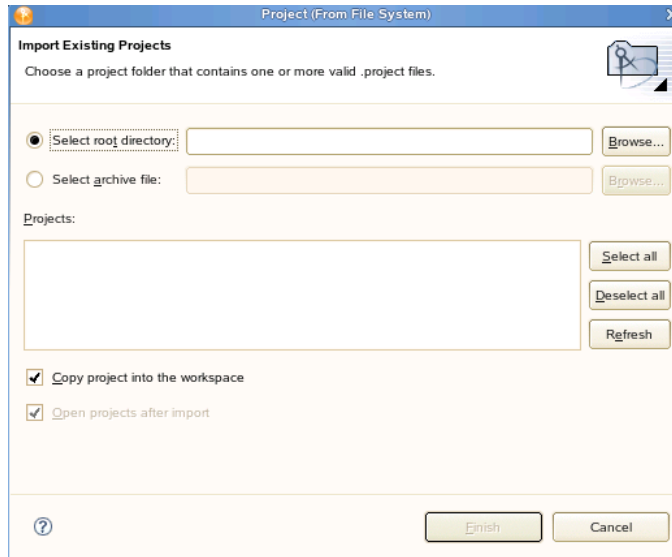
Click the *Overview* section if you are not familiar with Designer. Use the *Tutorials* to get started. If you have used Designer before, read the *What's New* section to see the latest enhancements to Designer.



- 12** When you are ready to proceed, select *Run Designer*.
- 13** Select *Project > Import Project > File System* to import the Resource Kit project.



- 14** Make sure that *Select root directory* is selected, then click *Browse*.



- 15 Browse to and select `/usr/tmp/RK12`, then click *OK*.
- 16 Verify that the Resource Kit project is listed under *Projects*, and that the *Copy project into the workspace* option is selected.
- 17 Click *Finish*.
- 18 After the project is imported, click the *Project* tab, then browse to *RK12/Designer/Documents/Resources*.
All of the files that are needed for the following sections are stored in Designer. The files are located at `/home/admin/designer_workspace/RK12/Designer/Documents/Resources`.
- 19 Proceed to [Section 7.2, “Loading the Resource Kit Structure into the Identity Vault,” on page 48](#).

7.2 Loading the Resource Kit Structure into the Identity Vault

The Resource Kit contains a specific structure for the Identity Vault that is required for the solution provided to work.

- 1 From the *Computer* menu, select *Gnome Terminal*.
- 2 Login in as `root` by entering `su`, then enter the `root` password.
- 3 Verify that your current directory is `/home/admin/designer_workspace/RK12/Designer/Documents/Resources/config`.
- 4 Enter the following command to import the `ResourceKitConfiguration.ldif` file:


```
ice -S LDIF -f ResourceKitConfiguration.ldif -D LDAP -s 172.17.2.117 -p 389 -d cn=admin,dc=admins,dc=system -w n0v3ll -F -l error.log -v
```

See [Table 7-1 on page 49](#) for a description of each option.
- 5 Enter `exit` twice to log out as `root` and close the Gnome Terminal.
- 6 Proceed to [Section 7.3, “Populating the Identity Vault with the Resource Kit Data,” on page 49](#).

Table 7-1 ICE Command Line Options

Option	Description
-S	Source handler specifies where the source information comes from.
-f	The LDIF file that contains the source information.
-c	Prevents the source handler from stopping if there are errors.
-D	Destination handler specifies where the destination information goes to.
-s	The server's name or IP address for the destination information.
-p	The LDAP port that is being used by the LDAP server.
-d	The DN of the user making the bind to the LDAP server.
-w	The password for the user making the bind to the LDAP server.
-F	Allows forward referencing in eDirectory. If the option is not specified, the file import fails.
-P	Enables the LBURP protocol.
-l	Creates a log file to see the results of the LDIF file import.
-v	Enables the verbose mode.

7.3 Populating the Identity Vault with the Resource Kit Data

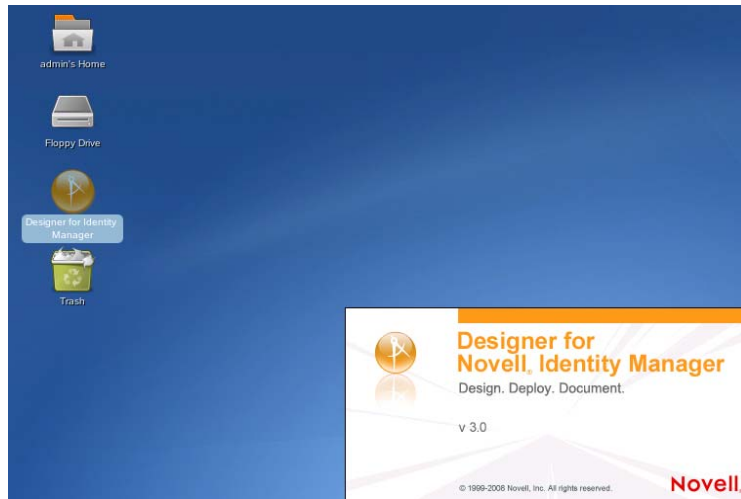
This section explains how to populate the Identity Vault with the information from the Resource Kit Designer project. This prepares the Identity Vault for the installation of the User Application.

There are two separate tasks to complete:

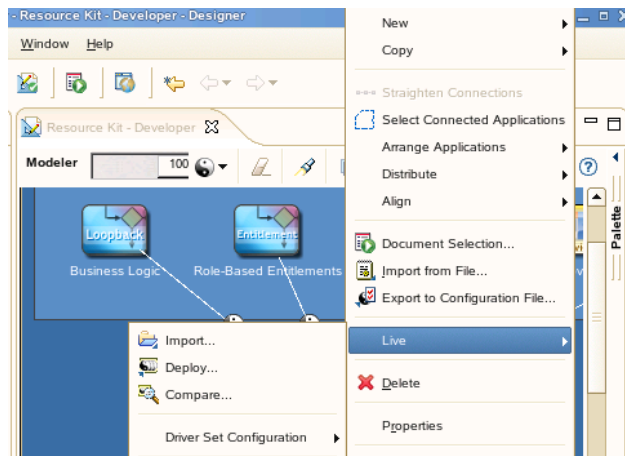
- ♦ [Section 7.3.1, “Deploying the Resource Kit Project into the Identity Vault,” on page 49](#)
- ♦ [Section 7.3.2, “Loading Sample Schema Extensions and Data,” on page 53](#)

7.3.1 Deploying the Resource Kit Project into the Identity Vault

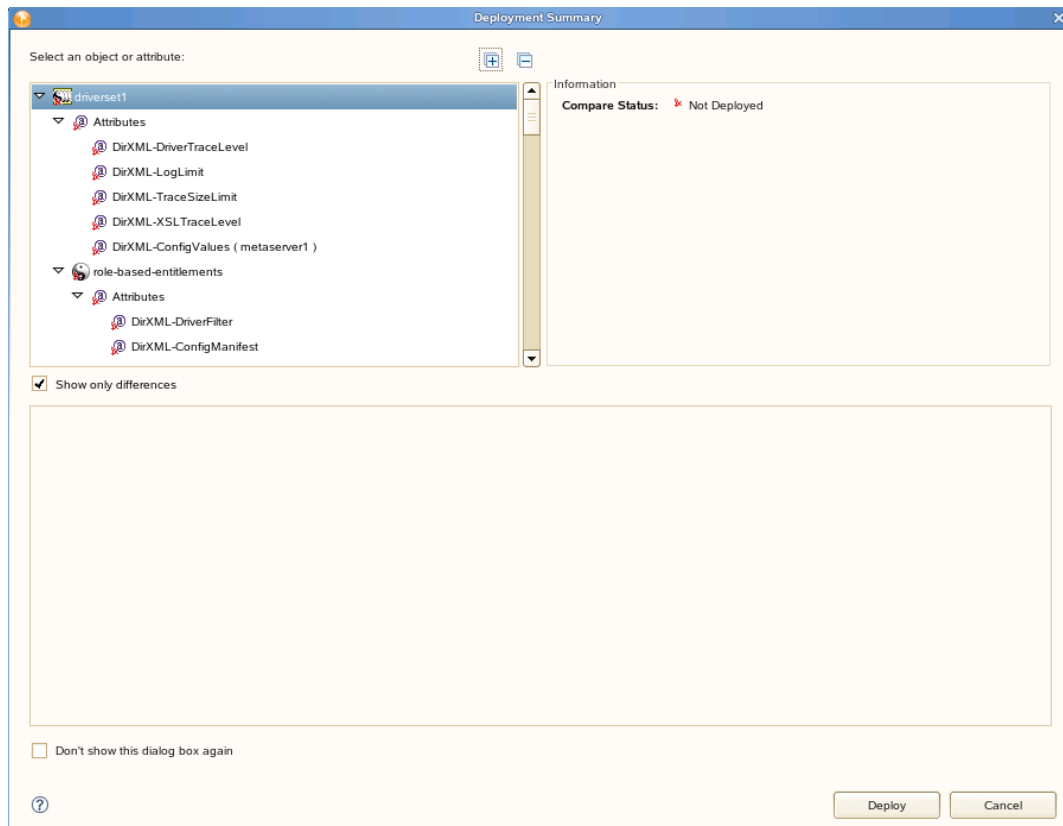
- 1 Launch Designer by clicking the icon on the desktop.



- 2 To deploy the configuration to the Identity Vault, right-click the driver set in the META Identity Vault, then select *Live > Deploy*.



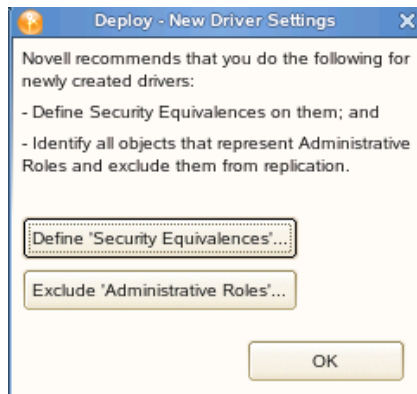
- 3 The deployment summary dialog box comes up. If you don't want to see this dialog box every time you deploy, select *Don't show this dialog box again*, then select *Deploy*.



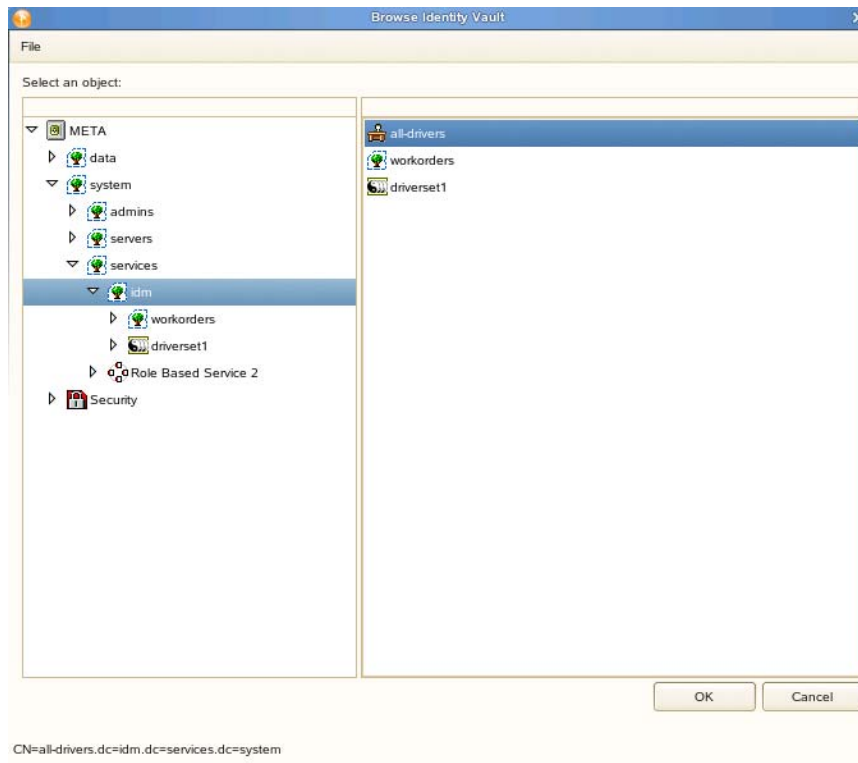
You can always use *Compare* instead of *Deploy* to use the full compare and reconciliation capabilities of Designer. Most people prefer to have the deploy process smooth and silent.

The deploy process ends with a Deployment Results dialog box.

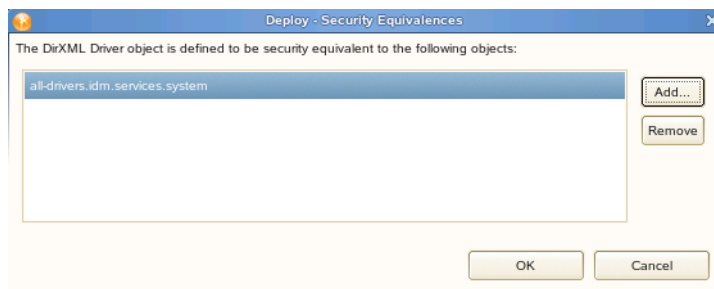
- 4 Select *Define Security Equivalences* to define the rights for the drivers.



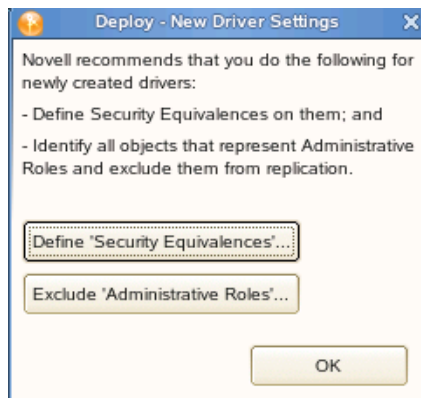
- 5 Click *Add*, browse to and select the *all-drivers.idm.services.system Organizational Role*, then click *OK*.



6 Click *OK* to close the Security Equivalences dialog box.



7 Do not click *Exclude Administrative Roles* in the New Driver Settings dialog box.



If you exclude administrative roles, this is a static list that must be maintained if there are changes in your environment. The Resource Kit uses Entitlements and Role-Based Services to manage this information.

- 8 Click *OK* to deploy the project.
- 9 Select the Default Notification Collection container in the Outline tab.
The e-mail notification templates are not deployed when you select the driver set.
- 10 Right-click the container, then select *Live > Deploy*.
- 11 Select *Deploy*.
- 12 Read the summary, then click *OK*.
- 13 Exit Designer.
- 14 Proceed to [Section 7.3.2, “Loading Sample Schema Extensions and Data,”](#) on page 53.

7.3.2 Loading Sample Schema Extensions and Data

The best way to explore the Resource Kit and its capabilities is to install our sample schema extensions and sample data, so you have real data in the system and can use that to demonstrate or test the kit.

The passwords for the user accounts are set to the user’s name. For example, the password for the `ablake.users.company.data` is `ablake`.

NOTE: You can usually use the ICE utility through iManager. However, there is currently an issue with it and it does not function. You must use the ICE command line utility instead.

- 1 From the *Computer* menu, select *Gnome Terminal*.
- 2 Login in as `root` by entering `su`, then enter the `root` password.
- 3 Verify you current directory is `/home/admin/designer_workspace/RK12/Designer/Documents/Resources/config`.
- 4 Enter the following command to extend the schema:

```
ice -S LDIF -f ResourceKitSampleSchema.ldif -c -D LDAP -s 172.17.2.117 -p 389  
-d cn=admin,dc=admins,dc=system -w n0v3l1 -F -P -l error.log -v
```

See [Table 7-1](#) for a description of each option used.

- 5 Enter the following command to import the sample data:

```
ice -S LDIF -f ResourceKitSampleData.ldif -c -D LDAP -s 172.17.2.117 -p 389 -d  
cn=admin,dc=admins,dc=system -w n0v3l1 -F -P -l error.log -v
```

See [Table 7-1](#) for a description of each option used.

- 6 Enter `exit` twice to log out as `root` and close the Gnome Terminal.
- 7 Proceed to [Section 7.4, “Prerequisites for the Delimited Text Driver,”](#) on page 53.

7.4 Prerequisites for the Delimited Text Driver

You must create the input and output directories for the Delimited Text driver to use.

- 1 From the *Computer* menu, select *Gnome Terminal*.

- 2 Log in as root by entering `su`, then enter the root password.
- 3 Enter `mkdir -p /var/novell/idm/users/input/images` to create the input directory for the Delimited Text driver.
- 4 Enter `mkdir -p /var/novell/idm/users/output/images` to create the output directory for the Delimited Text driver.
- 5 Enter `exit` twice to log out as root and close the Gnome Terminal.
- 6 Proceed to [Section 7.5, “Making eDirectory Visible on the External IP Address,”](#) on page 54.

7.5 Making eDirectory Visible on the External IP Address

The Resource Kit VM is set for DHCP on the external IP address. eDirectory might not be visible to any other machines on the external IP address. If you want to make the Resource Kit eDirectory visible externally, you need to apply a script that comes with the Resource Kit. For more information, see “[Solution for Making eDirectory Visible on the External IP Address](#)” in the *Identity Manager Resource Kit 1.2 Business Solutions Reference Guide*.

The script is named `setndsconf`.

- 1 From the *Computer* menu, select *Gnome Terminal*.
- 2 Log in as root by entering `su`, then enter the root password.
- 3 Enter `cd designer_workspace/RK12/Designer/Documents/Resources/bootscripts/` to access the directory where the `setndsconf` script file is located.
- 4 Enter `cp setndsconf /etc/init.d/` to copy the `setndsconf` script to the correct directory.
- 5 Enter `chmod 775 /etc/init.d/setndsconf` to change the access rights to the file.
- 6 Enter `yast2 runlevel`.
- 7 Select the *Expert Mode* radio button.
- 8 Verify that `setndsconf` is set to run levels 3 and 5.
 - 8a If it is not set, select 3 and 5, then click *Set/Reset*.
 - 8b Select *Enable the service*, then click *Finish*.
 - 8c Click *Yes* to save the changes.
- 9 Enter `exit` twice to log out as root and close the Gnome Terminal.

Proceed to [Chapter 8, “Installing XPOZ and Executing XPOZ Scripts,”](#) on page 55.

Installing XPOZ and Executing XPOZ Scripts

8

The Resource Kit comes with a test harness program called XPOZ (pronounced “expose”). It allows you to test many aspects of the Resource Kit and Identity Manager.

- ♦ [Section 8.1, “Installing XPOZ,” on page 55](#)
- ♦ [Section 8.2, “Executing XPOZ Scripts,” on page 55](#)
- ♦ [Section 8.3, “Accessing the Resource Kit XPOZ Scripts,” on page 57](#)

8.1 Installing XPOZ

The only prerequisite is to have NCI (Novell International Cryptographic Infrastructure) installed. NCI is installed when you install eDirectory.

To install XPOZ:

- 1 From the *Computer* menu, select *Home Folder*.
- 2 Browse to and select the `/usr/tmp` directory.
- 3 Right-click the `xpozv61_install.zip` file, then select *Extract*.
- 4 From the *Computer* menu, select *Gnome Terminal*.
- 5 Log in as `root` by entering `su`, then enter the `root` password.
- 6 Access the XPOZ installation file by entering `cd /usr/tmp/xpoz_install`.
- 7 Enter `sh ./xpoz_install_linux.bin` to start the installation.
- 8 Read the license agreement, then enter `Y` to accept the license agreement.
- 9 Specify the installation location as `/opt/novell/xpoz`, then press `Enter` to start the installation.
- 10 Press `Enter` when the installation completes successfully.

8.2 Executing XPOZ Scripts

XPOZ executes test scripts that test your Identity Manager solution. The Resource Kit contains XPOZ scripts you can run. If you want to create your own test scripts, see the *Novell Compliance Management Platform 1.0 Integration Guide*. It contains detailed information about the XPOZ scripting language.

XPOZ contains two utilities that execute the XPOZ test scripts:

- ♦ [Section 8.2.1, “XPOZ Console,” on page 56](#)
- ♦ [Section 8.2.2, “XPOZ GUI,” on page 56](#)

8.2.1 XPOZ Console

The XPOZ Console is a command line utility. You can create additional scripts to automate running of the XPOZ test scripts. The XPOZ Console can be executed remotely via Telnet or ssh.

To run the XPOZ Console, enter:

```
XPOZConsole scriptfile [localEnvironmentFileName]
```

Linux is case sensitive. The `scriptfile` name is the name of the XPOZ script that you want to execute. The `localEnvironmentFileName` allows you to pass in an environment file if needed.

8.2.2 XPOZ GUI

The XPOZ GUI is a graphical utility that executes the XPOZ scripts. It gives you the ability to change variables during script execution and view results in the tool.

To run the XPOZ GUI utility, run the XPOZGui program. The default location for the program is `/opt/novell/xpoz/XPOZGui`. To run the XPOZGui program:

```
./XPOZGui
```

Figure 8-1 XPOZ GUI

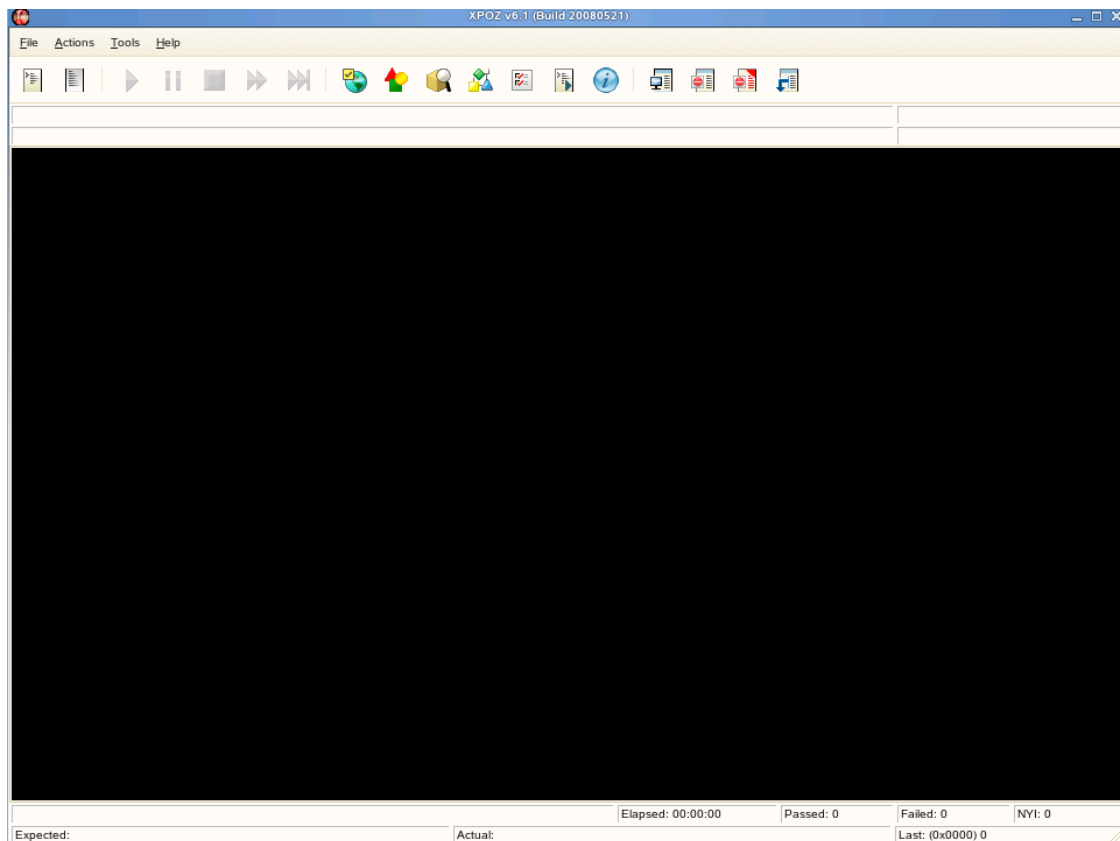

















Table 8-1 describes the different features of the XPOZ GUI tool. It is much more flexible and powerful than the XPOZ Console.

Table 8-1 XPOZ GUI Features

Feature	Description
 Open Script File	Browse to and select the XPOZ script file to execute.
 Open Log File	This feature is not implemented.
Play	Executes the XPOZ script.
Pause	Pauses the XPOZ script file execution.
Stop	Stops the execution of the XPOZ script file.
FFWD Retry	If errors occur during the execution of the XPOZ script, it skips the current delay before recalling the function.
FFWD Retry Count	Makes one more retry of the script, before continuing with the execution of the function.
 Environment Browser	Browse to an environment variable.*
 Symbol Table Browser	Browse to a symbol defined in the symbol table.*
 Object Browser	Browse to a specific eDirectory™ object. The <i>Object Browser</i> lists each eDirectory tree you are authenticated to.*
 Schema Browser	Browse to the eDirectory schema. The <i>Schema Browser</i> lists each eDirectory tree you are authenticated to.*
 Options Browser	Browse to common environment variables, such as log to screen or retrydelay.
 Execute Script Command	Inserts additional script commands into the XPOZ script that is running.
 Script Information Dialog	Lists the information about the script being executed.
 Results Admin	Allows you to access and reuse the results of the XPOZ script.
 Turn Results Off	Turns off the results. The results are no longer recorded.
 Turn Results On	Turns on the results. The results are recorded.
 Turn Defect Tracking Off	This feature is not implemented.
 Turn Defect Tracking On	This feature is not implemented.
 Select Results System	Allows you to select the type of results tracking system. Currently the only supported system is Results Tracking System v1 (RTS).

*The browsers allow you to view specific information to see why a script failed.

8.3 Accessing the Resource Kit XPOZ Scripts

The Resource Kit contains XPOZ scripts in the Designer project. You can use these XPOZ scripts to test the quality of the Resource Kit. To access the XPOZ scripts:

- 1 Launch the XPOZ GUI from `/opt/novell/xpoz/XPOZGui`.
- 2 Click *Open Script File*.

- 3** Browse to and select the XPOZ script file located in `/home/admin/designer_workspace/RK12/Designer/Documents/Resources/quality`.
- 4** Click *Play* to execute the XPOZ script.

Proceed to [Chapter 9, “Configuring a Secure Mail Relay for Identity Manager,”](#) on page 59.

Configuring a Secure Mail Relay for Identity Manager

9

In order to implement the Resource Kit, a mail server is required. It is required for things such as events from an Identity Manager driver policy, password change notification, or workflow events for the Identity Manager User Application.

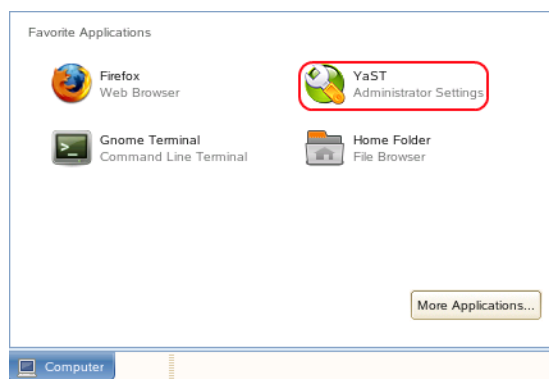
Instead of setting up a complete e-mail server, the Resource Kit has a secure mail relay that allows an authorized Identity Manager User Application user to send e-mail when required. The secure mail relay uses the postfix smtpd MTA agent as a secure e-mail relay with cyrus-sasl-sasauthd, using LDAP authentication against eDirectory™ for smtp_auth.

To set up a secure mail relay, the Server Base System install for SUSE® Linux Enterprise Server (SLES) 10 SP2 needs to contain cyrus-sasl, cyrus-sasl-saslauthd, and postfix. If you followed the steps in *Identity Manager Resource Kit 1.2 Installation Guide for SUSE Linux Enterprise Server 10 SP2*, these options were installed.

- ♦ Section 9.1, “Enabling postfix and saslauthd to Start at Boot,” on page 59
- ♦ Section 9.2, “Configuring saslauthd to Use LDAP Authentication,” on page 61
- ♦ Section 9.3, “Configuring postfix to Use saslauthd,” on page 61
- ♦ Section 9.4, “Testing saslauthd and postfix,” on page 62
- ♦ Section 9.5, “Configuring Identity Manager to Use Your postfix MTA Service,” on page 63

9.1 Enabling postfix and saslauthd to Start at Boot

- 1 From the *Computer* menu, select *YaST*.



- 2 Log in as `root` when prompted.
- 3 Under the *System* category, select *System Services (Runlevel)*.

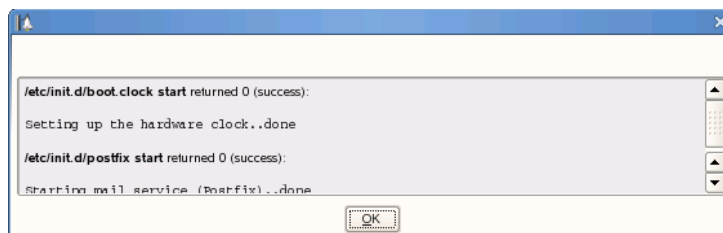


4 Browse to and select *postfix*, then click *Enable*.

Service	Enabled	Description
novell-zmd	Yes	ZMD, the ZENworks Management Daemon, allows users to manage \ software on their systems
nscd	Yes	Start Name Service Cache Daemon
ntp	Yes	Start network time protocol daemon (NTPD).
nxdm	No*	Novell IDM for Linux and UNIX
openct	No*	Start smart card readers
pcscd	No	PCSC daemon handling smart card readers
portmap	Yes	DARPA port to RPC program number mapper
post_nsd_start	No*	
postfix	Yes	start the Postfix MTA
powerd	No	Start the UPS monitoring daemon
powersaved	Yes	optimises power consumption, specially for laptops
random	Yes	Script to snapshot random state and reload it at boot time.
raw	No	raw-devices
rdxml	Yes*	Novell DirXML Remote Loader
resmgr	Yes	Start resource manager for device file access
rpasswdd	No	Start rpasswdd to allow secure remote password updates
rpmconfigcheck	No*	rpm config file scan
rsyncd	No	Start the rsync server daemon
running-level	Yes	Kernel source configuration switch

5 Click *Continue* in the message that states the default runlevels are set to 3 and 5.

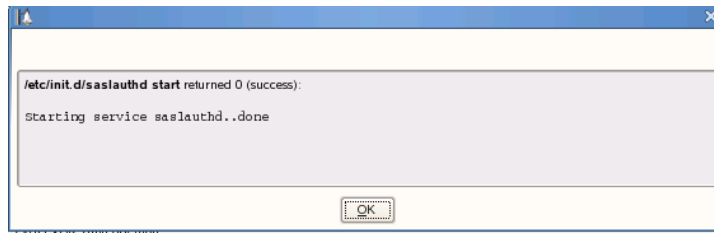
6 Click *OK* in the message screen.



7 Browse to and select *saslauthd*, then click *Enable*.

Service	Enabled	Description
rpasswdd	No	Start rpasswdd to allow secure remote password updates
rpmconfigcheck	No*	rpm config file scan
rsyncd	No	Start the rsync server daemon
running-level	Yes	Kernel source configuration switch
saslauthd	No	start the cyrus-sasl2 auth daemon
slpd	Yes	slpd - OpenSLP daemon for the Service Location Protocol
slpua	Yes	Start/Stop Script for NDS SLP Daemon
smartd	No	Monitors disk and tape health via S.M.A.R.T.

- 8 Click *OK* in the message screen.



- 9 Click *Finish*, then click *Yes* to save the changes.
- 10 Close YaST.
- 11 Proceed to [Section 9.2, “Configuring saslauthd to Use LDAP Authentication,”](#) on page 61.

9.2 Configuring saslauthd to Use LDAP Authentication

- 1 From the *Computer* menu, select *Gnome Terminal*.
- 2 Log in as `root` by entering `su`, then enter the `root` password.
- 3 Enter `gedit /etc/sysconfig/saslauthd`.
- 4 Change the line `SASLAUTHD_AUTHMECH=pam` to `SASLAUTHD_AUTHMECH=ldap`.
- 5 Add a new line: `CONFIG_FILE="/etc/saslauthd.conf"`.
- 6 Select *File > Save* to save the file, then select *File > Quit* to exit.
- 7 Enter `gedit /etc/saslauthd.conf`.
- 8 Add a new line: `ldap_servers: ldaps://172.17.2.117:636/`
This entry is the LDAP server that saslauthd does an LDAP authentication against. It could be the Identity Manager server or another LDAP server. If you want to use clear text instead of secure text, enter `ldap://172.17.2.117`. The port number is optional.
- 9 Add another line: `ldap_search_base: dc=admins,dc=system`.
This is the LDAP context where the user resides that authenticates (binds) to your LDAP server. For the Resource Kit, this is the admin user. If you want other users in the tree to be able to receive and send e-mail, you must specify the users container `ou=users,o=company,dc=data`.
- 10 Select *File > Save* to save the file, then select *File > Quit* to exit.
- 11 For the changes to take effect, restart saslauthd by entering `/etc/init.d/saslauthd restart`.
- 12 Verify that saslauthd is using LDAP by entering `ps -ef | grep saslauthd`.
If saslauthd is using LDAP, it returns `/usr/sbin/saslauthd -a ldap`.
- 13 Enter `exit` twice to log out as `root` and close the Gnome Terminal.
- 14 Proceed to [Section 9.3, “Configuring postfix to Use saslauthd,”](#) on page 61.

9.3 Configuring postfix to Use saslauthd

- 1 From the *Computer* menu, select *Gnome Terminal*.

- 2 Log in as root by entering `su`, then enter the root password.
- 3 Enter `gedit /etc/postfix/main.cf`.
- 4 Change the line `smtpd_sasl_auth_enable =` from `no` to `yes`.
- 5 Find the line `smtpd_recipient_restrictions =`, then add the option `permit_sasl_authenticated`.
The options are comma-separated, for example: `smtpd_recipient_restrictions=permit_mynetworks,reject_unauth_destination,permit_sasl_authenticated`
- 6 Add the line `smtpd_sasl_security_options = noanonymous`.
- 7 Add the line `smtpd_sasl_local_domain =`.
- 8 Add the line `broken_sasl_auth_clients = yes`.
- 9 Click *File > Save* to save the changes, then click *File > Quit* to exit.
- 10 For the changes to take effect, restart postfix by entering `/etc/init.d/postfix restart`.
- 11 Enter `exit` twice to log out as root and close the Gnome Terminal.
- 12 Proceed to [Section 9.4, “Testing saslauthd and postfix,” on page 62](#).

9.4 Testing saslauthd and postfix

Before configuring Identity Manager to use the postfix MTA server, you need to test saslauthd and postfix.

- 1 To test saslauthd, select *Gnome Terminal* from the *Computer* menu, then enter `testsaslauthd -u admin -p n0v3ll`.
The message `0:OK success` is displayed if it is working.
- 2 To test postfix, enter `telnet 172.17.2.117 25`.
If you can telnet to port 25 on the server, postfix is running and has authentication enabled. If it connects, the following message is displayed:

```
Trying 172.14.2.117
Connected to 172.17.2.117
Escape character is '^]'
220 metaserver1.yourcompany.com ESMTP Postfix
```
- 3 After you are connected, enter `ehlo localhost`.
It displays the following message:

```
250-mail.example.edu
250-PIPELINING
250-SIZE 31457280
250-VRFY
250-ETRN
250-AUTH NTLM LOGIN PLAIN DIGEST-MD5 CRAM-MD5
250-AUTH=NTLM LOGIN PLAIN DIGEST-MD5 CRAM-MD5
250 8BITMIME
```
- 4 The AUTH line contains LOGIN, which show the postfix requires a login before forwarding mail.
- 5 Enter `quit` to close the telnet session.

- 6 Enter `exit` to close the Gnome Terminal.
- 7 Proceed to [Section 9.5, “Configuring Identity Manager to Use Your postfix MTA Service,”](#) on [page 63](#).

9.5 Configuring Identity Manager to Use Your postfix MTA Service

- 1 Log in to iManager as admin. (<https://172.17.2.117:8443/nps/iManager.html>)
- 2 Select *Workflow Administration > Email Server Options*.
- 3 Specify the server’s IP address of 172.17.2.117 in the *Host Name* field.
- 4 Specify `idmadmin@company.com` in the *From* field.
- 5 Select *Authenticate to server using credentials*.
- 6 In the *User Name* field, specify `admin` as the user to authenticate.
- 7 Specify admin’s password twice, then click *OK*.

Enter the settings for your e-mail notification server.

Host Name:	<input type="text" value="172.17.2.117"/> <small>(for example: mail.novell.com or 137.89.119.5)</small>
From:	<input type="text" value="idmadmin@company.com"/> <small>(for example: admin@novell.com)</small>

☒ **Authenticate to server using credentials:**

User Name:	<input type="text" value="admin"/>
Password:	<input type="password" value="*****"/>
Retype password:	<input type="password" value="*****"/>

- 8 Click *OK* in the success message.

☒ **Complete: Success**

Your changes have been saved.

- 9 (Optional) You can view e-mail being processed by the postfix MTA by entering the following command in a *Gnome Terminal*: `tail -f /var/log/mail.info`.
- 10 Exit iManager.
- 11 Proceed to [Chapter 10, “Password Configuration,”](#) on [page 65](#).

Password Configuration

10

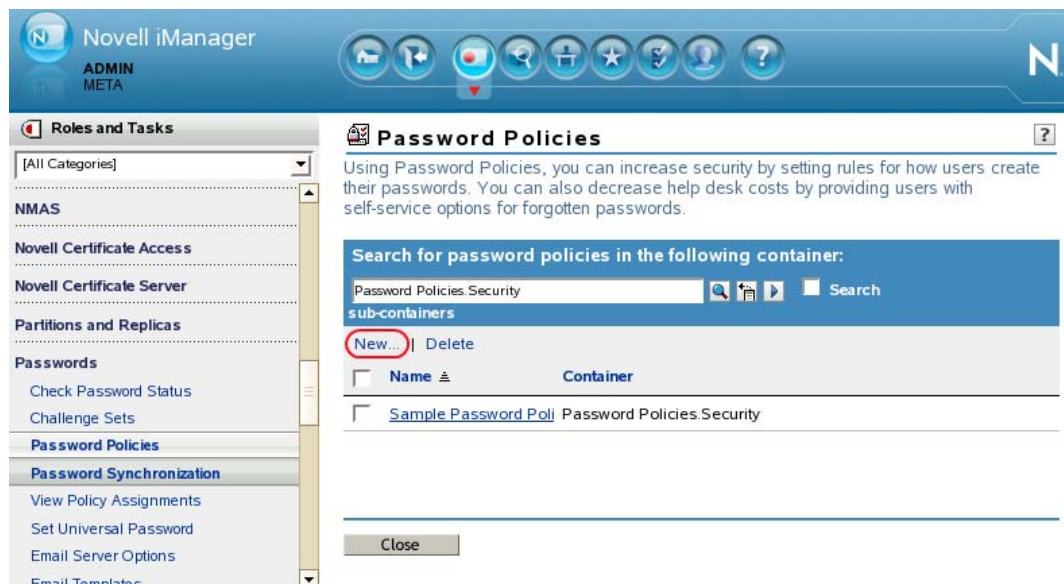
The Resource Kit helps you manage different password issues for your company. This section contains additional configuration steps to help address these issues.

- ♦ [Section 10.1, “Creating a Required Password Policy,” on page 65](#)
- ♦ [Section 10.2, “Enabling the Password Expiration Notification Job,” on page 68](#)

10.1 Creating a Required Password Policy

In order for the Resource Kit scenarios to work properly, you need to create a password policy.

- 1 Log in to iManager as admin. (<https://172.17.2.117:8443/nps/iManager.html>)
- 2 Click *Passwords* > *Password Policies*, then click *New*.



- 3 Leave the default value of Password Policies.Security for the container value.

Container to create the policy in:

Password Policies.Security

- 4 Specify Default Security in the *Policy Name* field.

Policy Name:

Default Security (ex. Engineering Dept)

- 5 Specify Password policy for the Resource Kit for the *Description*.

Description:
Password policy for the Resource Kit

- 6 For the *Password Change Message* field, specify `Please change your password.`

Password Change Message:
Please change your password.

- 7 Select the option to *Create a new Password Policy based on default settings*, then click *Next*.

☒ Create a new Password Policy based on the default settings
(Click Next to see summary)

- 8 Read the summary of the policy, then click *Finish*.

Password Policy Wizard [?]

Step 8 of 8: Summary of the Password Policy

Your policy has the following settings:

Password Policy Summary		Last Modified:
Name	Default Security	
Description	Password policy for the IDM Resource Kit	
Universal Password		
Options	Enable Universal Password	true
	Enable the Advanced Password Rules	true
	Synchronize NDS password when setting Universal Password	true

<< Back Next >> Close Finish

- 9 Click *Close* in the success message.

Success

☒ Complete: Your Password Policy was successfully created.

Click Close to return to the Password Policy List.

- 10 Click in the policy you created to edit it.



- 11 Click the *Universal Password* tab, then click *Advanced Password Rules*.



- 12 Verify that the following options are set:
- ♦ Under *Change Password* settings, select *Allow user to initiate password change*.
 - ♦ Under *Password Syntax* settings, select *Use Novell Syntax*.
 - ♦ Under *Password Length* settings, select and specify the *minimum value* (4) and *maximum value* (12).
 - ♦ Under *Case Sensitive* settings, select the *Allow password to be case sensitive* option.
 - ♦ Under *Numeric Character* settings, select *Allow numeric characters in password*.
 - ♦ Under *Special Character* settings, select *Allow special characters in the password* and *Allow non-US ASCII characters*.
- 13 Click *Apply*.
- 14 Click the *Policy Assignment* tab, then click the *Object Selector* icon.

You can assign this policy to multiple individuals, organizations or to an entire company. To assign a policy, type in a value and press the Enter key or search for the object in the tree. To remove an assignment, select an item in the list and press the Delete key on your keyboard or click the Remove button below the list.

Assign to:

Remove

- 15 Browse to and select the `users.company.data` container for the policy assignment, then click *OK*.

Contents: (shift-click to start a selection range)

.. (up one level)
 (current level) (3)
 users
 groups
 devices

<< Previous
 Next >>
 14

Selected Objects: 1 (click object to unselect)

users.company.data

OK
 Clear All

- 16 Click *OK* to save the change, then click *Close* to exit the Password Policy task.
- 17 Exit iManager.
- 18 Proceed to [Section 10.2, “Enabling the Password Expiration Notification Job,”](#) on page 68.

10.2 Enabling the Password Expiration Notification Job

The Resource Kit uses the Password Expiration Notification job to automatically send an e-mail to the users when their passwords are going to expire. This is a default job that ships with Identity Manager. For more information about jobs, see the *Identity Manager 3.6 Jobs Guide*.

In order for this feature to function, the secure mail relay must be configured. Verify that the procedures in [Chapter 9, “Configuring a Secure Mail Relay for Identity Manager,” on page 59](#) have been completed before proceeding.

The job is part of the Designer project. When the project is deployed into the Identity Vault, the job is created. However, the job is set to manual. To enable the job:

- 1 Log in to iManager as admin. (<https://172.17.2.117:8443/nps/iManager.html>)
- 2 Select *Identity Manager > Identity Manager Overview*.
- 3 Browse to and select the `driverset1.idm.services.system` object.
- 4 Click the driver set object.

Identity Manager Overview

Specify the container you want to search, then press the search button.

Search in:   

Driver Sets Libraries	
New... Delete	
<input type="checkbox"/> Name	Container
<input type="checkbox"/> driverset1	idm.services.system

- 5 Select the *Jobs* tab, then click the Password Expiration Notification job.
- 6 In the Job page, verify the job is enabled. If is not, select *Enable*.

Driver Set Overview

Driver Set:   

Overview Libraries Jobs Dashboard			
New... Run Now Stop Enable Disable Get Status Delete			
<input type="checkbox"/> Job Name	Enabled	Next scheduled run	Description
<input type="checkbox"/> Password Expiration Notification	<input checked="" type="checkbox"/>	Not scheduled	This job uses LDAP to look for objects whos

- 7 Click the *Password Expiration Notification* link to edit the job.
- 8 In the *Email server* field, browse to and select *Default Notification Collection.Security*.

Identity Manager

Job | Misc

General | Schedule | Scope | Parameters | Results

Java class name: com.novell.nds.dirxml.job.pwdexp.PasswordExpirationJob

☒ Enable job

☐ Delete the job after it runs once

Servers

Select the server(s) this job should run on:

☒ metaserver1.metaserver1.servers.system

Email server

Default Notification Collection: Security

Display name:

Password Expiration Notification

Description:

This job uses LDAP to look for objects whose password will expire in some number of days. An email is sent to the address contained by the "mail" LDAP attribute value.

9 Click the *Parameters* tab.

10 In the *Notification email template* field, verify the *Password Expiration Notification* e-mail template is selected, then click *OK*.

Notification email

Notification email template  Password Expiration Notifica 

If you are having difficulty finding the *Password Expiration Notification* e-mail template, you can search for the template by name in the Object Selector page.

11 Exit iManager.

12 Enter `exit` twice to log out as `root` and close the Gnome Terminal.

13 Proceed to [Chapter 11, “Installing and Configuring the User Application,”](#) on page 71.

Installing and Configuring the User Application


11

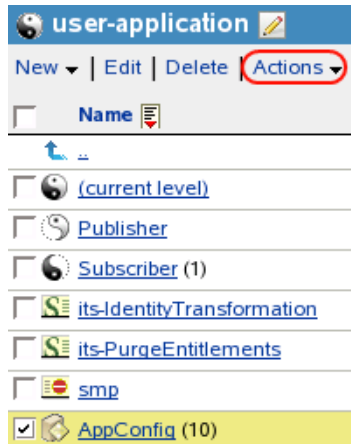
The User Application is a workflow-based provisioning tool. It simplifies the process of managing user access to secure resources in an organization. These resources can include digital entities such as user accounts, computers, and databases. It provides a Web interface for the user to request the resources.

All of the tasks listed in **Chapter 7, “Configuring the Environment for the Resource Kit,”** on page 45 must be completed before proceeding. The User Application requires that your environment be configured before you can run the installation.

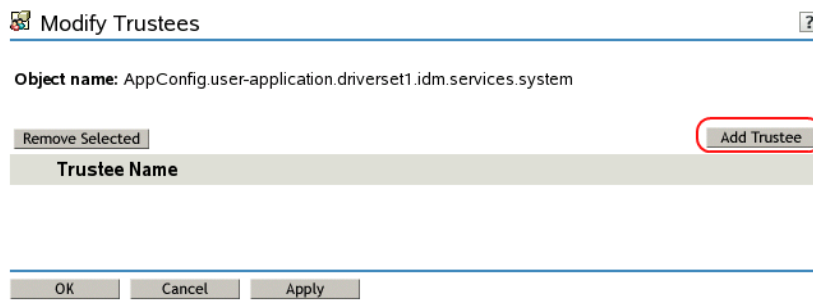
- ♦ **Section 11.1, “Preparing to Install the Identity Manager User Application,”** on page 71
- ♦ **Section 11.2, “Using the Identity Manager Service Account,”** on page 74
- ♦ **Section 11.3, “Installing the JBoss Application Server and the MySQL Database,”** on page 74
- ♦ **Section 11.4, “Exporting the Correct Path to the Java Installation,”** on page 75
- ♦ **Section 11.5, “Installing the Identity Manager User Application,”** on page 77
- ♦ **Section 11.6, “Making JBoss shutdown.sh Executable,”** on page 80
- ♦ **Section 11.7, “Configuring the User Application for Automatic Startup,”** on page 80
- ♦ **Section 11.8, “Configuring the User Application for HTTPS,”** on page 82
- ♦ **Section 11.9, “Importing the Custom Portal Page,”** on page 84
- ♦ **Section 11.10, “Configuring the Organization Chart to Only Display Active Users,”** on page 87

11.1 Preparing to Install the Identity Manager User Application

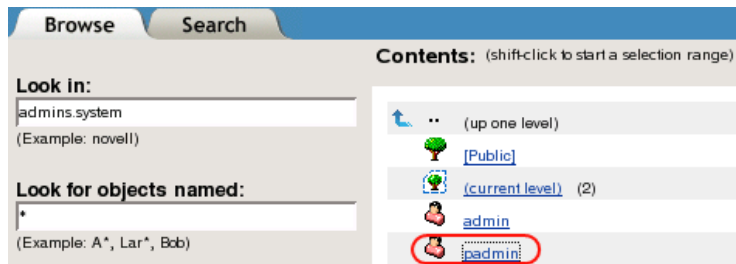
- 1 Log in to iManager as admin. (<https://172.17.2.117:8443/nps/iManager.html>)
- 2 Select *View Objects*  in the iManager header, then browse to the user application driver `UserApplication.driverset1.idm.services.system`.
- 3 Select the AppConfig container in the list of objects stored in the user application driver, then click *Actions*.




- 4 Select *Modify Trustee* from the list of actions.
- 5 Select *Add Trustee*.




- 6 Browse to and select the padmin.admins.system user, then click *OK*.



- 7 Select *Assigned Rights*.



Modify Trustees
?

Object name: AppConfig.user-application.driverset1.idm.services.system

 **Notice:** Unsaved changes exist for this trustee.


Select OK or Apply to save the changes to the directory.

Remove Selected
Add Trustee

Trustee Name	Assigned Rights
<input type="checkbox"/>  padmin.admins.system	

OK
Cancel
Apply

- 8 Select *Supervisor* for the *[Entry Rights]*, then click *Done*.


Modify Trustees
?

Object name: AppConfig.user-application.driverset1.idm.services.system


Trustee name: padmin.admins.system

Remove Selected
Add Property


Property Name	Assigned Rights	Inherit
<input type="checkbox"/> [All Attributes Rights]	<input type="checkbox"/> Supervisor <input checked="" type="checkbox"/> Compare <input checked="" type="checkbox"/> Read <input type="checkbox"/> Write <input type="checkbox"/> Self <input type="checkbox"/> Dynamic	<input checked="" type="checkbox"/>
<input type="checkbox"/> [Entry Rights]	<input checked="" type="checkbox"/> Supervisor <input checked="" type="checkbox"/> Browse <input type="checkbox"/> Create <input type="checkbox"/> Rename <input type="checkbox"/> Delete <input type="checkbox"/> Dynamic	<input checked="" type="checkbox"/>

Done
Cancel

- 9 Click *OK* to save your changes.



Modify Trustees
?

Object name: AppConfig.user-application.driverset1.idm.services.system

 **Notice:** Unsaved changes exist for this trustee.

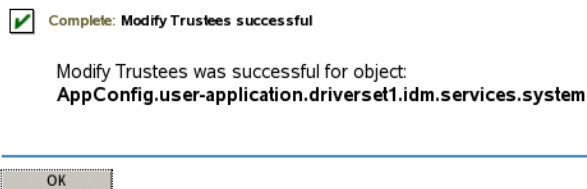
Select OK or Apply to save the changes to the directory.

Remove Selected
Add Trustee

Trustee Name	Assigned Rights
<input type="checkbox"/>  padmin.admins.system	

OK
Cancel
Apply

- 10 Click *OK* in the success message.



11 Exit iManager.

12 Proceed to [Section 11.2, “Using the Identity Manager Service Account,” on page 74.](#)

11.2 Using the Identity Manager Service Account

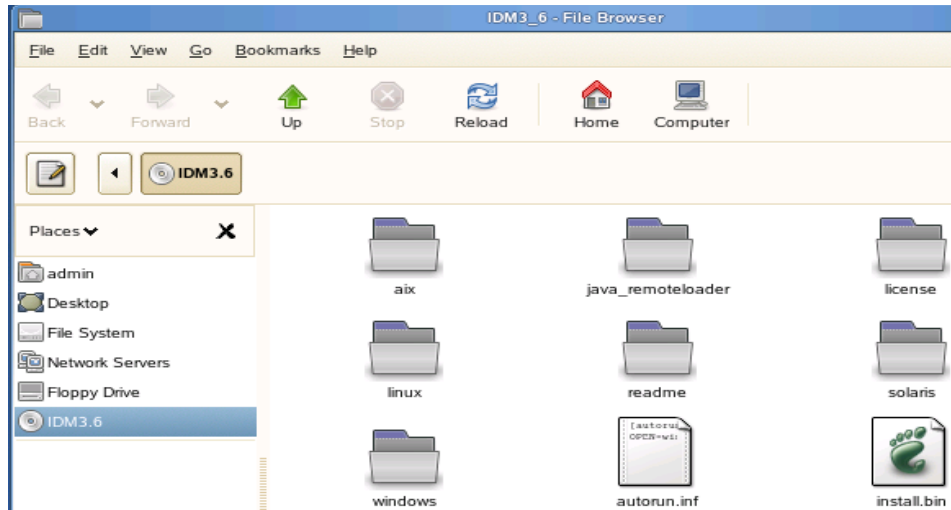
The MySQL and the User Application installations work better if you are not logged in as `root`. It is best to log in as the `idmsa` user. If you have not created the `idmsa` user, see [Section 2.2, “Creating an Identity Manager Service User and Group,” on page 16](#) for instructions.

If you are logged into the SLES server, log out, then log back in as the `idmsa` user. Make sure you have completed [Section 4.2.1, “Granting File Access Rights to the Novell Service Group,” on page 26](#) before starting the installation. The `idmsa` user needs write rights to the `/opt/novell` directory.

Proceed to [Section 11.3, “Installing the JBoss Application Server and the MySQL Database,” on page 74.](#)

11.3 Installing the JBoss Application Server and the MySQL Database

- 1 If you are planning on using a physical DVD or CD-ROMs to install the Identity Manager User Application, insert the installation media into your drive, which must be accessible from within your VM. Continue with [Step 6](#).
- 2 If you are using ISO files, disconnect the CD-ROM device from your VM by selecting *Removable Devices > CD-ROM > Disconnect from the VM menu*.
- 3 Reconfigure your VM to use the Identity Manager 3.5.1 ISO file (`Identity_Manager_3_5_1_DVD.iso`) by selecting *Removable Devices > CD-ROM 1 > Edit*.
- 4 From the VM menu, browse to and select the ISO file in the *Connection -- Use ISO image* section.
- 5 From the VM menu, reconnect the CD-ROM device to your VM by selecting *Removable Devices > CD-ROM 1 > Connect*. This causes the Identity Manager 3.5.1 ISO to automatically mount the CD-ROM and open a file browser.



- 6 From the *Computer* menu, select *Gnome Terminal*.
- 7 Access the User Application installation directory by entering `cd /media/IDM3_6_1_UA/linux/jboss/`.
- 8 Launch the JbossMsql utility by entering `./JbossMysql.bin`.
- 9 Use the following information to complete the installation:

Installation Screen	Description
Introduction	Read the introduction information.
Choose Install Set	Select <i>JBoss</i> and <i>MySQL</i> .
Choose JBoss parent folder	Specify <code>/opt/novell/idm</code> for the JBoss* parent folder.
MySQL Info	Defines the MySQL database with the following information. <ul style="list-style-type: none"> ♦ Database Name: idmuserappdb ♦ root user password: n0v3ll ♦ root user password (confirm): n0v3ll
Pre-Installation Summary	Review the summary, then start the installation.
Install Complete	Review the installation complete message.

- 10 Enter `exit` to close the Gnome Terminal.
- 11 Proceed to [Section 11.4, “Exporting the Correct Path to the Java Installation,” on page 75](#).

11.4 Exporting the Correct Path to the Java Installation

The User Application is tested with the Java* that is installed at `/opt/novell/idm/jre`. You must make sure the correct path is set. You can either execute the commands each time the shell starts, or add this information to the `/etc/profile.local` script.

- ♦ [Section 11.4.1, “Setting the Correct Path in the Current Shell,” on page 76](#)

- [Section 11.4.2, “Adding the Commands to the /etc/profile.local Script,” on page 76](#)
- [Section 11.4.3, “Configuring JRE for the IDMSA Service Account,” on page 76](#)

11.4.1 Setting the Correct Path in the Current Shell

Follow these steps to set the correct path in the current shell:

- 1 From the *Computer* menu, select *Gnome Terminal*.
- 2 Enter the following commands:


```
export JAVA_HOME=/opt/novell/idm/jre
export JRE_HOME=$JAVA_HOME/jre
export PATH=$JAVA_HOME/bin:$PATH
```
- 3 Do not exit the Gnome Terminal, or the path is no longer set.

11.4.2 Adding the Commands to the /etc/profile.local Script

Follow these steps to add these commands to the `/etc/profile.local` script.

- 1 From the *Computer* menu, select *Gnome Terminal*.
- 2 Log in as `root` by entering `su`, then enter the `root` password.
- 3 Enter `gedit /etc/profile.local`.
- 4 Add the following lines to the file:


```
export JAVA_HOME=/opt/novell/idm/jre
export JRE_HOME=$JAVA_HOME/jre
export PATH=$JAVA_HOME/bin:$PATH
```
- 5 Select *File > Save* to save the file, then select *File > Quit* to exit.
- 6 Enter `source /etc/profile.local` to execute the script file without rebooting the server.
- 7 Log out of the shell as `root` by entering `exit` at the command prompt.
- 8 Proceed to [Section 11.5, “Installing the Identity Manager User Application,” on page 77](#).

11.4.3 Configuring JRE for the IDMSA Service Account

Follow these steps to configure the JRE security and default keystore to be owned by the `idmsa` service account:

- 1 From the *Computer* menu, select *Gnome Terminal*.
- 2 Log in as `root` by entering `su`, then enter the `root` password.
- 3 Enter `chown idmsa:novell /opt/novell/idm/jre/lib/security`.
- 4 Enter `chown idmsa:novell /opt/novell/idm/jre/lib/security/cacerts`.
- 5 Enter `chmod 775 /opt/novell/idm/jre/lib/security`.
- 6 Enter `chmod 775 /opt/novell/idm/jre/lib/security/cacerts`.

11.5 Installing the Identity Manager User Application

- 1 In the Gnome Terminal, look at the prompt to verify that you are not logged in as `root`.

NOTE: If you are not logged in as `root`, the prompt is a `>`. If you are logged in as `root`, the prompt is a `#`.

- 2 Access the User Application installation directory by entering `cd /media/IDM3_6_1-UA/user_app_install/`.
- 3 Enter `java -jar IdmUserApp.jar` to start the User Application installation.
- 4 Use the following information to complete the installation:

Installation Screen	Description
Novell Identity Manager	Select the language for the installation program to use. The default is <i>English</i> .
License Agreement	Read the License Agreement, then select <i>I accept the terms of the License Agreement</i> .
Application Server Platform	Select <i>JBoss</i> for the application server.
Standard or Provisioning	Select <i>Roles Based Provisioning</i> to install the correct version of the User Application for the Resource Kit.
Data Migration	There is no data to migrate. Make sure that <i>Yes</i> is not selected.
Choose Install Folder	Specify <code>/opt/novell/idm</code> for the installation folder.
Database platform	Select <i>MySQL</i> for the database platform.
Database Host & Port	Specify the following information for the database connection. <ul style="list-style-type: none">♦ Host: localhost♦ Port: 3306
Database Name & Privileged User	Specify the following information for the database. <ul style="list-style-type: none">♦ Database name (or sid): idmuserappdb♦ Database user: root♦ Database user password: n0v3ll♦ Database user password (confirm): n0v3ll
Java Install	Specify the Java root folder as <code>/opt/novell/idm/jre</code> .
JBoss Configuration	Specify the following information for the JBoss configuration. <ul style="list-style-type: none">♦ Base folder: <code>/opt/novell/idm/jboss</code>♦ Host: localhost♦ Port: 8080

Installation Screen	Description
IDM Configuration	<p>Specify the following information for the Identity Manager configuration</p> <ul style="list-style-type: none"> ♦ The Resource Kit does not use clustering. Select <i>default</i>. ♦ Specify <code>IDMProv</code> for the <i>Application Name</i>. ♦ The <i>Workflow Engine ID</i> is only required if clustering is enabled. The Resource Kit does not use clustering.
Novell Audit	Select <i>Yes</i> to enable auditing for the User Application.
Audit Logging	Select <i>Novell Audit</i> to enable auditing for the User Application.
Novell Audit	<p>Specify the following information:</p> <ul style="list-style-type: none"> ♦ Server: 172.17.2.117 ♦ Log cache folder: <code>/opt/novell/idm</code>
Security - Master Key	Select <i>No</i> for a new master key to be generated.
User Application Configuration	Read the message.

Installation Screen	Description
User Application Configuration	<p>Specify the following values for each field:</p> <ul style="list-style-type: none"> ♦ eDirectory Connections Settings: Use the values provided. <ul style="list-style-type: none"> ♦ LDAP Host: 172.17.2.117 ♦ LDAP Non-Secure Port: 389 ♦ LDAP Secure Port: 636 ♦ LDAP Administrator: cn=admin,dc=admins,dc=system ♦ LDAP Administrator Password: n0v3ll ♦ Use Public Anonymous Account: Leave it selected. ♦ LDAP Guest: Do not specify a value. ♦ LDAP Guest Password: Do not specify a value. ♦ Secure Admin Connection: Leave it selected. ♦ Secure User Connection: Leave it selected. ♦ eDirectory DNs: Specify the following values for each field or browse to and select the desired objects. <ul style="list-style-type: none"> ♦ Root Container DN: dc=data ♦ Provisioning Driver DN: cn=UserApplication,cn=driverset1,dc=idm,dc=services,dc=system ♦ User Application Admin: cn=padmin,dc=admins,dc=system ♦ Provisioning Application Admin: cn=padmin,dc=admins,dc=system ♦ Compliance Admin: cn=padmin,dc=admins,dc=system ♦ Roles Admin: cn=padmin,dc=admins,dc=system ♦ User Container DN: ou=users,o=company,dc=data ♦ Group Container DN: dc=groups,o=company,dc=data ♦ eDirectory Certificates: Leave the default values. ♦ Email: Leave all of the fields blank. ♦ Password Management: Leave the default values.
Pre-Installation Summary	Review all of the values specified for the installation to make sure they are correct. Make any changes if needed.
Install Complete	Read the installation complete message.

5 Enter `exit` to close the Gnome Terminal.

6 Proceed to [Section 11.6, “Making JBoss shutdown.sh Executable,” on page 80.](#)

- ♦ `export MYSQLUSER='mysqlshutdown';`
- ♦ `export MYSQLPASS='n0v3l1';`

Make sure the `MYSQLPASS` variable is set to the password you assigned to the `mysqlshutdown` user in [Step 7](#).

- 13 Select *File > Save* to save your changes, then select *File > Quit* to exit.
- 14 Copy the startup script to `/etc/init.d` directory by entering `cp /home/admin/designer_workspace/RK12/Designer/Documents/Resources/bootscripts/userapp /etc/init.d`.
- 15 Enter `ls -l /etc/init.d/userapp` to verify the file copied.
- 16 Enter `chown root:sys /etc/init.d/userapp` to change the owner of the file.
- 17 Enter `chmod 700 /etc/init.d/userapp` to change access to the file.
- 18 Enter `chkconfig -add userapp` to add the script as a system service.
- 19 Use the following two commands to verify whether `userapp` runs before or after `ndsd` in run-level 3 during the system start procedure.

Ultimately, you must ensure that `userapp` starts after `ndsd`.

NOTE: The first command uses a lowercase letter `l` twice. It is not the number 11.

```
metaserver1:/home/admin # ll /etc/init.d/rc3.d/ |grep userapp
lrwxrwxrwx 1 root root 10 2008-05-16 16:26 K12userapp -> ../userapp
lrwxrwxrwx 1 root root 10 2008-05-16 16:26 S10userapp -> ../userapp
```

```
metaserver1:/home/admin # ll /etc/init.d/rc3.d/ |grep ndsd
lrwxrwxrwx 1 root root 7 2008-05-16 13:23 K11ndsd -> ../ndsd
lrwxrwxrwx 1 root root 7 2008-05-16 13:23 S11ndsd -> ../ndsd
```

Watch the `SXX` numbers (`S10userapp` and `S11ndsd`) that are prefixed to the script name. They indicate the start order. A higher number means the service is started after a lower number. If the numbers are the same, both services are started at the same time.

In this case, `userapp` runs before `ndsd`, which is the opposite of what you want. Enter the following commands as a corrective action if the `userapp` number is the same or lower than the `ndsd` number:

```
metaserver1:/home/admin # mv /etc/init.d/rc3.d/S10userapp /etc/init.d/rc3.d/S12userapp
```

- 20 Verify the startup order for run-level 5 (the same commands as [Step 19](#), but instead of `rc3.d`, you now use `rc5.d`):

```
metaserver1:/home/admin # ll /etc/init.d/rc5.d/ |grep userapp
lrwxrwxrwx 1 root root 10 2008-05-16 16:26 K12userapp -> ../userapp
lrwxrwxrwx 1 root root 10 2008-05-16 16:26 S10userapp -> ../userapp
```

```
metaserver1:/home/admin # ll /etc/init.d/rc5.d/ |grep ndsd
lrwxrwxrwx 1 root root 7 2008-05-16 13:23 K11ndsd -> ../ndsd
lrwxrwxrwx 1 root root 7 2008-05-16 13:23 S11ndsd -> ../ndsd
```

Enter the following commands as a corrective action if the `userapp` number is the same or lower than the `ndsd` number:

```
metaserver1:/home/admin # mv /etc/init.d/rc5.d/S10userapp /etc/init.d/rc5.d/S12userapp
```

- 21 Stop and start the User Application by entering `/etc/init.d/userapp stop`, then entering `/etc/init.d/userapp start`.
- 22 Enter `exit` twice to log out as `root` and close the Gnome Terminal.
- 23 Proceed to [Section 11.8, “Configuring the User Application for HTTPS,”](#) on page 82.

11.8 Configuring the User Application for HTTPS

As first installed, the User Application can be reached only by using HTTP. The following steps configure the User Application so that it can also be reached by using HTTPS. TID 10100226 describes how to accomplish this. Most of the steps below follow the content of the TID, but some have been adapted to comply with Resource Kit requirements.

To enable SSL for JBoss, you must first create an SSL certificate. This is done easily with the `keytool` command. Follow the steps shown below to generate a new certificate for the User Application to use. You might want to adapt some of the parameters to better reflect your environment. The parameters provided here serve as an example.

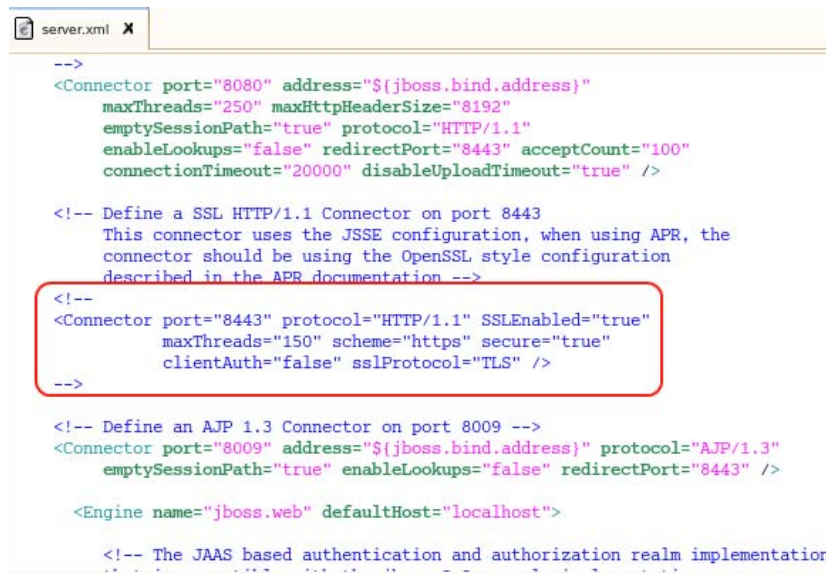
- 1 From the *Computer* menu, select *Gnome Terminal*.
- 2 Log in as `root` by entering `su`, then enter the `root` password.
- 3 Enter `/etc/init.d/userapp stop` to stop the User Application.
- 4 Enter `su idmsa` to log in as the `idmsa` user.
- 5 Enter `cd /opt/novell/idm/jre/bin` to access the directory where the `keytool` is stored.
- 6 Enter `./keytool -genkey -alias userAppKey -keyalg RSA -keystore userapp.keystore -validity 3650` to generate the key.

The following values can be set to any values you choose. The the values listed are examples.

- ♦ **Keystore Password:** Specify a password for the keystore.
 - ♦ **What is your first and last name?** Specify `User Application` for the first and last name.
 - ♦ **What is the name of your organizational unit?** Specify `IDM` for the name of the organizational unit.
 - ♦ **What is the name of your organization?** Specify `company` as the name of your organization.
 - ♦ **What is the name of your City or Locality?** Specify the city you are currently in.
 - ♦ **What is the name of your State or Province?** Specify the state you reside in.
 - ♦ **What is the two-letter country code for this unit?** Specify the country you reside in.
 - ♦ **Is CN=User Application, OU=IDM, O=company, L=Provo, ST=Utah, C=US correct?** Specify `yes` if the information is correct.
 - ♦ **Enter key password for <userAppkey>:** Specify the same password used for the keystore password.
- 7 Enter `mv userapp.keystore ../../jboss/server/IDMProv/conf/` to move the file to the correct location.
 - 8 Enter `chmod 700 ../../jboss/server/IDMProv/conf/userapp.keystore` to change the access rights to the file.

- 9 Enter `chown idmsa:novell ../../jboss/server/IDMPProv/conf/userapp.keystore` change the owner of the file.
- 10 Enter `gedit /opt/novell/idm/jboss/server/IDMPProv/deploy/jboss-web.deployer/server.xml` to edit the `server.xml` file.
- 11 In gedit, find the following section:

```
<!--
  <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
    maxThreads="150" scheme="https" secure="true"
    clientAuth="false" sslProtocol="TLS" />
-->
```



- 12 To enable TLS communication, remove the remarks, change the Connector port to 8444, add the `keystoreFile` parameter, and add the `keystorePass` parameter.

```
<Connector port="8444" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="150"
scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
keystoreFile="${jboss.server.home.dir}/conf/userapp.keystore"
keystorePass="changeit" />
```

```

server.xml x
enableUploads="false" redirectPort="8443" acceptCount="100
connectionTimeout="20000" disableUploadTimeout="true" />

<!-- Define a SSL HTTP/1.1 Connector on port 8443
This connector uses the JSSE configuration, when using APR, the
connector should be using the OpenSSL style configuration
described in the APR documentation -->

<Connector port="8444" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="${jboss.server.home.dir}/conf/userapp.keystore"
keystorePass="changeit" />

<!-- Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009" address="${jboss.bind.address}" protocol="AJP/1.3"
emptySessionPath="true" enableLookups="false" redirectPort="8443" />

<Engine name="jboss.web" defaultHost="localhost">

<!-- The JAAS based authentication and authorization realm implementation
that is compatible with the jboss 3.2.x realm implementation.
- certificatePrincipal : the class name of the
org.jboss.security.auth.certs.CertificatePrincipal impl

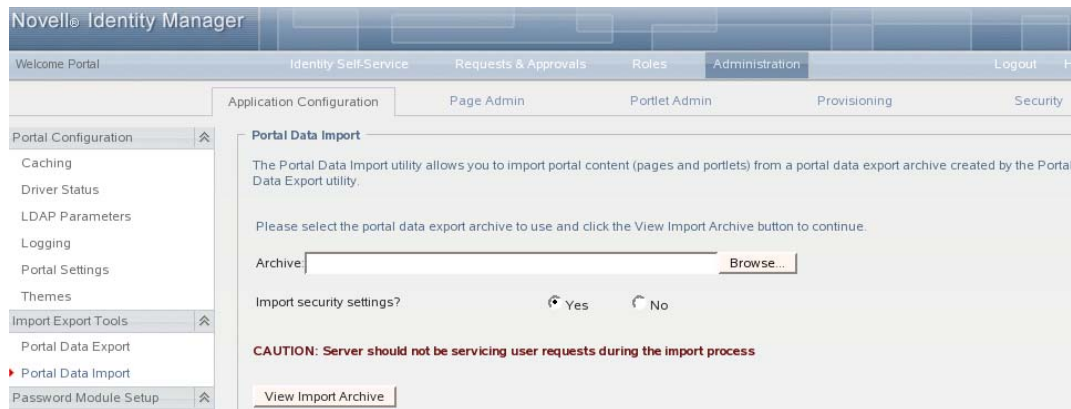
```

- 13 Select *File > Save* to save the changes, then select *File > Quit* to exit gedit.
- 14 Restart the User Application by entering `sudo /etc/init.d/userapp restart`, then enter the root password.
This might take a couple of minutes.
- 15 Enter `exit` to close the Gnome Terminal.
- 16 Log out of the SLES server as idmsa.
- 17 Proceed to [Section 11.9, “Importing the Custom Portal Page,”](#) on page 84.

11.9 Importing the Custom Portal Page

The Resource Kit contains a custom portal page as part of the workflow solution. Use the following information to create the custom portal page.

- 1 Log in to the SLES server as the admin user.
- 2 Access the User Application Portal through the Web browser at `https://172.17.2.117:8444/IDMProv`.
- 3 On the Welcome page, click *Login* in the upper right corner, then log in to the User Application Portal as:
 - ♦ **Username:** cn=padmin,dc=admins,dc=system
 - ♦ **Password:** n0v3ll
- 4 Click *Administration > Application Configuration*, then in the list on the left side click *Import Export Tools > Portal Data Import*.



5 Browse to and select the `PortalData_XXXXXX_XX_XX_XX.zip` file, then click *Open*.

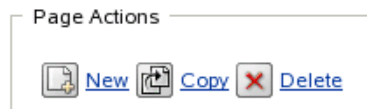
The `PortalData_XXXXXX_XX_XX_XX.zip` file is located `/home/admin/designer_workspace/RK12/Designer/Documents/Resources/UAPortal/` directory as part of the Designer project.

6 Click *View Import Archive*.

7 Use the default settings, then click *Import Portal Data*.

8 Click the *Page Admin* tab.

9 Click *New* in the Page Actions box in the lower left corner of the page.



10 Specify *Register New User* in the *Page Link Name (URI)* field.

11 Select *Information Management* for the Assign Categories, then click *Save Page*.

Page Properties

Page Link Name (URI):

Page Name: [Localize](#)

Navigation Priority (higher number = lower priority):

☒ none ☐ Set value

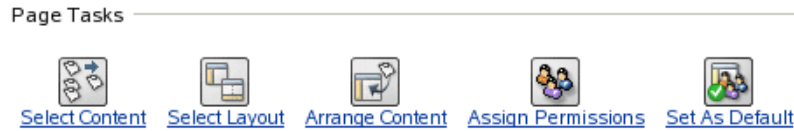
Parent Page: [Select Parent](#)

Assign Categories:

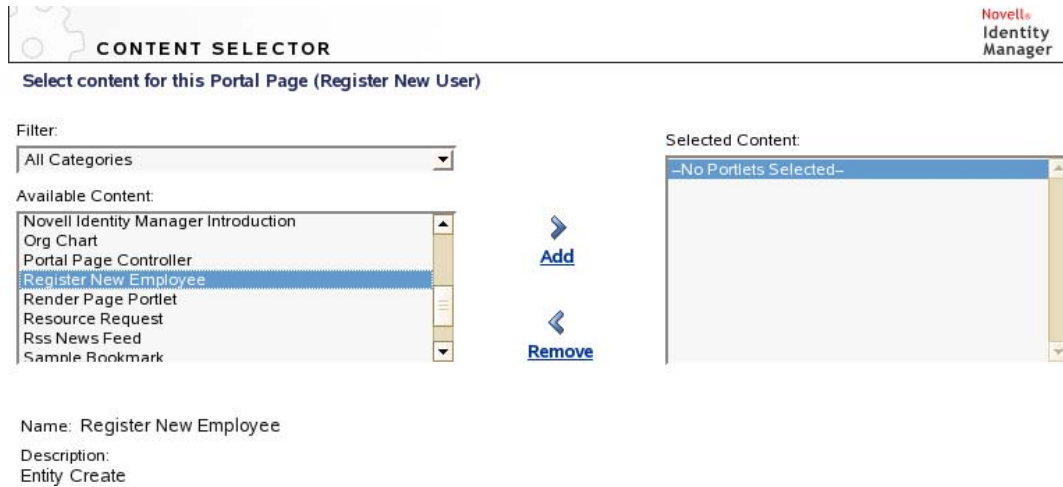
<input type="checkbox"/> Administration	<input type="checkbox"/> Directory Management
<input type="checkbox"/> General	<input type="checkbox"/> Guest Pages
<input checked="" type="checkbox"/> Information Management	<input type="checkbox"/> Password Management

Description:

12 From the Page Tasks, click *Select Content*.

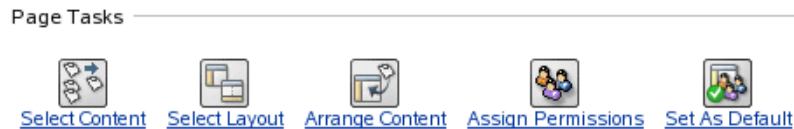


- 13** In the Available Content, scroll to and select *Register New Employee*, then click *Add*.



- 14** Click *Save Contents*.

- 15** From the Page Tasks, select *Assign Permissions*.



- 16** Deselect *View Permission Set to Admin Only*, then click *Save*.

PAGE PERMISSIONS

Please select the users and groups that can access this Page(Register New User)

View Ownership

Search for:
Users

Starts with:
a Go
(e.g. 'smi')

Results (Displaying 1 to 5 of 5 users):

- cn=ablake,ou=users,o=company,dc=...
- cn=achung,ou=users,o=company,dc=...
- cn=apalani,ou=users,o=company,dc=...
- cn=asmith,ou=users,o=company,dc=...
- cn=aspencer,ou=users,o=company,dc=...

Current Assignments:

Containers selected
no containers selected

Groups selected
no groups selected

Users selected
no users selected

☐ View Permission Set to Admin Only

Save Close

This allows all users to see this page link in the User Application.

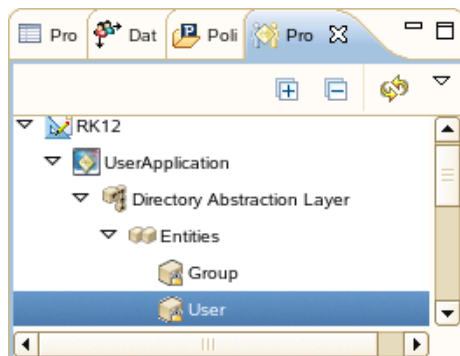
- 17 Click *Close* to close the page.
- 18 Click *Logout* to log out of the User Application Portal as the padmin user.
- 19 To verify the new page is available, log in to the User Portal as a user. The Register New User link is listed under the Information Management category in the User Application Portal.

11.10 Configuring the Organization Chart to Only Display Active Users

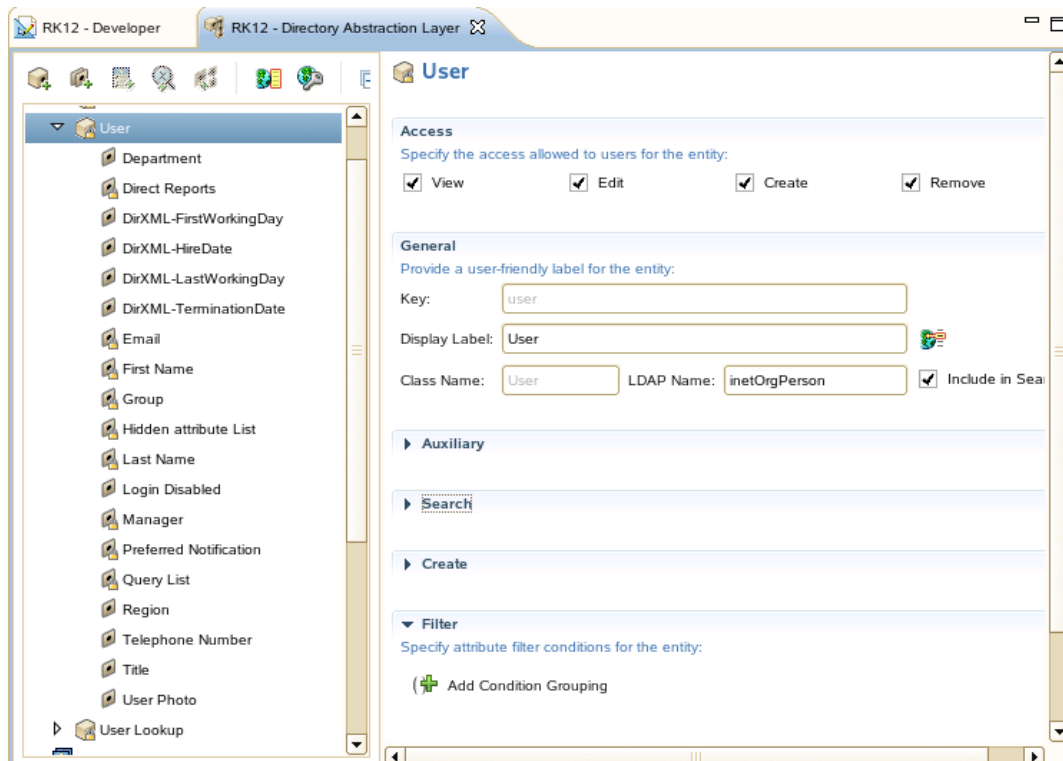
The Resource Kit provides the business logic for active and inactive users. You can configure the Organizational Chart and the Employee Search to only display active users.

- 1 In Designer, select Window > Show View > Provisioning View from the toolbar.
- 2 In the Provisioning view, expand the Resource Kit project to access the User Entity.

The User Entity is located RK12 > UserApplication > Directory Abstraction Layer > Entities > User.



- 3 Right-click User, then click *Edit*.
- 4 In the right pane, scroll down to the Filter heading, then select *Add Condition Grouping*.



- 5 In the attribute drop-down list, browse to and select the *employeeStatus* attribute.
- 6 In the operators drop-down list, browse to and select *equals*.
- 7 Specify add active in the input field.
- 8 Press ctrl+S to save the changes.
- 9 To update the Identity Vault, deploy the saved project. For more information, see “[Deploying a Project to an Identity Vault](#)” in the *Designer 3.0 for Identity Manager 3.6 Administration Guide*.
- 10 Proceed to [Chapter 12, “Installing and Configuring Novell Audit,”](#) on page 89.

Installing and Configuring Novell Audit

12

Enabling Identity Manager to use Novell® Audit provides an event tracking and notification system. It allows you to create audit trails for compliance with business policies. The following tasks must be completed in order for Novell Audit to be installed and configured correctly.

- [Section 12.1, “Before Installing Novell Audit,” on page 89](#)
- [Section 12.2, “Installing Novell Audit,” on page 89](#)
- [Section 12.3, “Creating the Novell Audit Database,” on page 91](#)
- [Section 12.4, “Installing the Novell Audit Plug-Ins,” on page 91](#)
- [Section 12.5, “Installing the MySQL Connector,” on page 92](#)
- [Section 12.6, “Granting the User Application Access to the Cache Directory,” on page 93](#)
- [Section 12.7, “Configuring Novell Audit,” on page 93](#)
- [Section 12.8, “Enabling Audit Events for the User Application,” on page 97](#)

12.1 Before Installing Novell Audit

If you have a secure logging server with more than one IP address, you need to configure the server to run Novell Audit. Secure logging servers with more than one IP address have problems running Novell Audit because MDB does not know which IP address to use with eDirectory™. You can point Novell Audit to a specific IP address by using an MDB configuration file.

To point Novell Audit to a specific IP address for eDirectory:

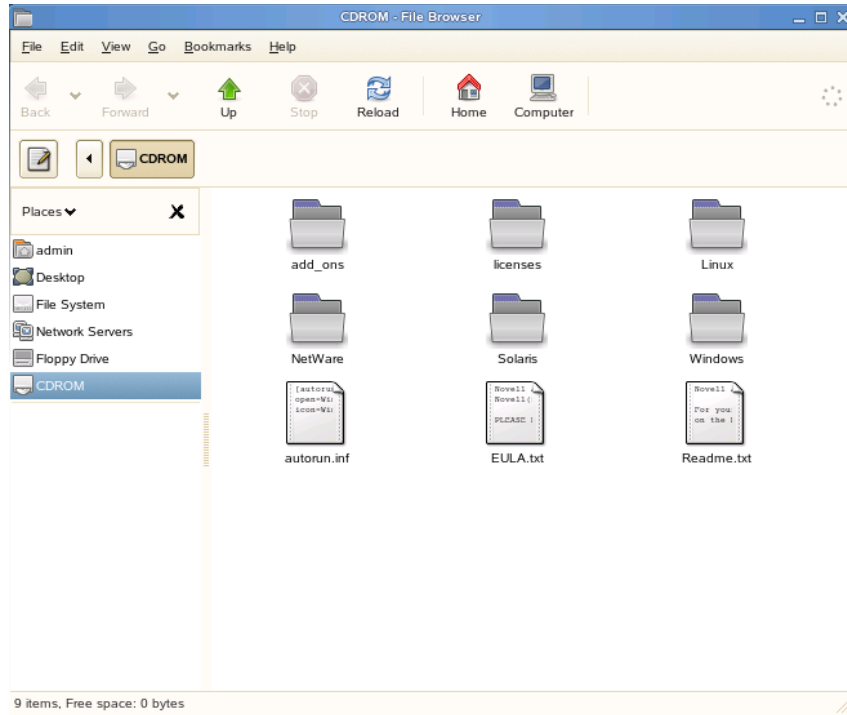
- 1 Log in to the SLES server as admin.
- 2 From the *Computer* menu, select *Gnome Terminal*.
- 3 Log in as root by entering `su`, then enter the root password.
- 4 To create the file, enter `gedit /etc/mdb.conf`.
- 5 Add the following line: `driver=mdbds referral=172.17.2.117`.
- 6 Click *File > Save* to save the file, then click *File > Quit* to exit.
- 7 Enter `exit` twice to log out as root and close the Gnome Terminal.
- 8 Proceed to [Section 12.2, “Installing Novell Audit,” on page 89](#).

12.2 Installing Novell Audit

- 1 If you are planning on using a physical DVD or CD-ROMs to install Novell Audit, insert the installation media into your drive, which must be accessible from within your VM. Continue with [Step 5](#).
- 2 If you are using ISO files, disconnect the CD-ROM device from your VM by selecting *Removable Devices > CD-ROM 1 > Disconnect from the VM* menu.

- 3 Reconfigure your VM to use the Novell Audit ISO `naudit202p3.iso` file by selecting *Removable Devices > CD-ROM 1 > Edit* from the VM menu and browsing to the ISO file in the *Connection – Use ISO image* section.
- 4 Reconnect the CD-ROM device to your VM by selecting *VM > Removable Devices > CD-ROM 1 > Connect*.

This causes the Novell Audit ISO to automatically mount the CD-ROM and open a file browser.



- 5 From the *Computer* menu, select *Gnome Terminal*.
- 6 Log in as `root` by entering `su`, then enter the `root` password.
- 7 Access the Novell Audit installation program by entering `cd /media/CDROM/Linux/`.
- 8 Enter `./pinstall.lin` to start the installation.
- 9 Read and accept the license agreement.
- 10 Enter `S` to install the Secure Logging Server with instrumentation, the Platform Agent, and the schema extensions.
- 11 Specify the administrator's name as `admin.admins.system`, then press the Tab key.
- 12 Specify the administrator's password, then press Enter.
- 13 Select *Add Schema Extensions*, then press Enter.
- 14 Tab to *Configure This Server*, then press Enter.
- 15 Leave the default value for the Secure Logging Server as `Metaserver1 Logging Server`.
- 16 Press the Tab key to accept using the default container, then press Enter.
- 17 Press the Tab key to select *Exit AuditExit* to start the installation, then press Enter.
- 18 If you see a message stating that there was an old configuration file found, press any key other than `Y` to overwrite the old file.

- 19 Press Y to start the eDirectory Instrumentation Agent, then press Enter.
- 20 Enter `exit` twice to log out as `root` and close the Gnome Terminal.
- 21 Proceed to [Section 12.3, “Creating the Novell Audit Database,”](#) on page 91.

12.3 Creating the Novell Audit Database

Novell Audit requires a database to store all of the collected events.

- 1 From the *Computer* menu, select *Gnome Terminal*.
- 2 Enter `cd /opt/novell/idm/mysql/` access the MySQL client.
- 3 Enter `./start-mysql-client.sh root n0v3ll` to launch the MySQL client.
- 4 Enter `create database naudit;` to create the database.
- 5 Enter `use mysql`
- 6 Enter `grant all on naudit.* to auditusr@'%' identified by 'n0v3ll';` to give users access to the naudit database.
- 7 Enter `select host,user from user;` to specify the users that have access to the database.
- 8 Enter `flush privileges;` to save the changes.
- 9 Enter `quit` to exit.
- 10 Enter `exit` to close the Gnome Terminal.
- 11 Proceed to [Section 12.4, “Installing the Novell Audit Plug-Ins,”](#) on page 91.

12.4 Installing the Novell Audit Plug-Ins


If the iManager plug-ins for Novell Audit are not installed, they must be installed.

To verify the Novell Audit plug-ins are installed in iManager:

- 1 Log in to iManager using the following information:
 - ♦ **Username:** admin.admins.system
 - ♦ **Password:** n0v3ll (or the password you chose)
 - ♦ **Tree:** 172.17.2.117
- 2 Verify that there is an Auditing and Reporting entry under the Roles and Tasks.

If there entry is there, the Novell plug-ins are installed. If there is no entry, use the following steps to install the plug-ins:

- 1 In iManager, click *Configure* in the iManager header.
- 2 Select *Plug-in Installation > Available Novell Plug-in Modules*.
- 3 Select the Novell Audit entry, then click *Install*.
- 4 Click *Close* after the plug-in is installed.
- 5 Select *Role Based Services > RBS Configuration*.
- 6 Click the number under *Modules*.

iManager 2.x Collections		iManager 1.x Collections				
New Edit Delete Actions						
<input type="checkbox"/>	Type	Name	Modules	Installed	Out-Of-Date	Not-Installed
<input type="checkbox"/>		Role Based Service 2.services.system	3	1	0	2

- 7 Select *Novell Audit*, then click *Install*.
- 8 Click *OK* to continue with the installation of the module into the collection object.
- 9 Click *OK* after the module is installed.
- 10 Exit iManager.

Tomcat must be restarted for the Novell Audit plug-ins to be displayed in iManager:

- 1 From the *Computer* menu, select *Gnome Terminal*.
- 2 Log in as root by entering `su`, then enter the root password.
- 3 Enter `/etc/init.d/novell-tomcat 5 stop` to stop the Web server.
- 4 Enter `/etc/init.d/novell-tomcat 5 start` to start the Web server.
- 5 Enter `exit` twice to log out as root and to close the Gnome Terminal.
- 6 Proceed to [Section 12.5, “Installing the MySQL Connector,” on page 92](#).

12.5 Installing the MySQL Connector

- 1 From the *Computer* menu, select *Gnome Terminal*.
- 2 Enter `cd /usr/tmp` to access the folder where the `mysql-connector-java-5.1.6.tar.gz` file is stored.
- 3 Enter `tar -xzf mysql-connector-java-5.1.6.tar.gz` to extract the file.
- 4 Enter `sudo cp mysql-connector-java-5.1.6/mysql-connector-java-5.1.6-bin.jar /var/opt/novell/tomcat5/common/lib/` to copy the file to the correct directory.
- 5 Enter the root password.
- 6 Enter `exit` to close the Gnome Terminal.

Tomcat must be restarted for this to take effect.

- 1 From the *Computer* menu, select *Gnome Terminal*.
- 2 Log in as root by entering `su`, then enter the root password.
- 3 Enter `/etc/init.d/novell-tomcat 5 stop` to stop the Web server.
- 4 Enter `/etc/init.d/novell-tomcat 5 start` to start the Web server.
- 5 Enter `exit` twice to log out as root and close the Gnome Terminal.
- 6 Proceed to [Section 12.7, “Configuring Novell Audit,” on page 93](#).

12.6 Granting the User Application Access to the Cache Directory

For Novell Audit or the User Application to write audit events to the cache directory, they must have access. To grant access:

- 1 From the *Computer* menu, select *Gnome Terminal*.
- 2 Log in as `root` by entering `su`, then enter the `root` password.
- 3 Enter `chown -R idmsa:novell /var/opt/novell/naudit`.
- 4 Enter `chmod -R 775 /var/opt/novell/naudit`.
- 5 Enter `chown -R idmsa:novell /opt/novell/idm/naudit`.
- 6 Enter `chmod -R 775 /opt/novell/idm/naudit`.
- 7 Enter `exit` twice to log out as `root` and close the Gnome Terminal.

12.7 Configuring Novell Audit

There are three separate tasks to complete in order to configure Novell Audit.

- ♦ [Section 12.7.1, “Creating a Channel,” on page 93](#)
- ♦ [Section 12.7.2, “Configuring the Platform Agent,” on page 95](#)
- ♦ [Section 12.7.3, “Connecting to the Novell Audit Database,” on page 96](#)

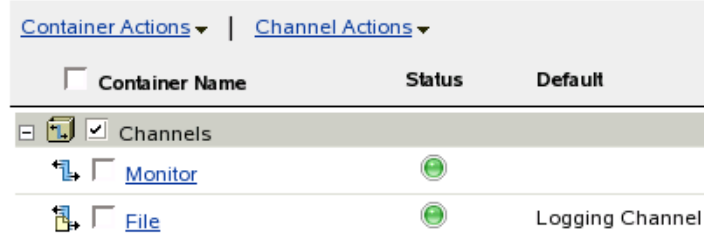
12.7.1 Creating a Channel

- 1 Log in to iManager by using the following information:
 - ♦ **Username:** `admin.admins.system`
 - ♦ **Password:** `n0v3ll` (or the password you chose)
 - ♦ **Tree:** `172.17.2.117`
- 2 Select *Auditing and Logging > Logging Server Options*.
- 3 Browse to and select the Metaserver1 Logging Server object in the Logging Services container, then click *OK*.

The full context of the object is Metaserver1 Logging Server.Logging Services.
- 4 Select the *Channels* tab, then select Channels container.



The logging server only scans these containers at startup. Therefore, if you new Channel container, creating or editing a Channel object, and so forth), changes. For more information on restarting the logging server, refer to the



- 5 Select *Channel Actions* > *New*.
- 6 Specify the channel name as *naudit* and the channel type as *MySQL Channel*, then click *OK*.
- 7 Click the *naudit* channel object.
- 8 Configure the new channel by entering the following information into the fields:

Fields	Information
<i>Host</i>	172.17.2.117 Make sure to use a real IP address here and not localhost. If you enter localhost, the SLS tries to connect through a local socket rather than the IP address, which would require additional configuration steps.
<i>Name</i>	naudit This is the name you specified in the Audit database.
<i>Table</i>	NAUDITLOG
<i>User</i>	auditusr This is the user you created when setting up the database.
<i>Password</i>	n0v3ll This is the password you specified when you created the database and granted the user access to it.
<i>Create Table Options</i>	Leave this field empty.
<i>SQL Expiration Commands</i>	clienttimestamp<(unix_timestamp()-259200); This expires records older than 3 days (259200 seconds.)
<i>Expire at specified time or interval</i>	00:00

- 9 Click *OK* to save the information.
- 10 Select the *General* tab, then select *Configuration*.
- 11 In the *Log Channel* field, browse to and select the *naudit* channel object.
The full context for the object is *naudit.Channels.Logging Services*.

- 12 Select the *Sign Events* option, then click *OK* to save the configuration changes.
- 13 Leave iManager open.
- 14 Proceed to [Section 12.7.2, “Configuring the Platform Agent,” on page 95](#).

12.7.2 Configuring the Platform Agent

- 1 To configure the platform agent, select *Gnome Terminal* from the *Computer* menu.
- 2 Log in as `root` by entering `su`, then enter the `root` password.
- 3 Use the following commands to verify whether the Secure Logging Server (SLS) runs before or after the user application and `ndsd` in run-level 3 during the system start procedure.

Ultimately, you must ensure that `naudit` starts after `ndsd` and `userapp`.

NOTE: The first command uses the lowercase letter `l` twice. It is not the number 11.

```
metaserver1:/home/admin # ll /etc/init.d/rc3.d/ |grep naudit
lrwxrwxrwx 1 root root 10 2008-05-16 16:26 K11novell-naudit -> ../novell-naudit
lrwxrwxrwx 1 root root 10 2008-05-16 16:26 S11novell-naudit -> ../novell-naudit
```

```
metaserver1:/home/admin # ll /etc/init.d/rc3.d/ |grep userapp
lrwxrwxrwx 1 root root 10 2008-05-16 16:26 K12userapp -> ../userapp
lrwxrwxrwx 1 root root 10 2008-05-16 16:26 S10userapp -> ../userapp
```

```
metaserver1:/home/admin # ll /etc/init.d/rc3.d/ |grep ndsd
lrwxrwxrwx 1 root root 7 2008-05-16 13:23 K12ndsd -> ../ndsd
lrwxrwxrwx 1 root root 7 2008-05-16 13:23 S10ndsd -> ../ndsd
```

Watch the SXX numbers (`S11novell-naudit`, `S10userapp`, and `S10ndsd`) that are prefixed to the script name. They indicate the start order. A higher number means the service is started after a lower number. If the numbers are the same, both services are started at the same time.

In this case, `naudit` runs after `userapp` and `ndsd`, which is what you want. Enter the following commands as a corrective action if the `userapp` number is the same or lower than the `ndsd` number:

```
metaserver1:/home/admin # mv /etc/init.d/rc3.d/S10novell-naudit /etc/init.d/rc3.d/S12novell-naudit
```

- 4 Verify the startup order for run-level 5 (the same commands as [Step 3](#), but instead of `rc3.d`, you now use `rc5.d`):

```
metaserver1:/home/admin # ll /etc/init.d/rc5.d/ |grep userapp
lrwxrwxrwx 1 root root 10 2008-05-16 16:26 K11novell-naudit -> ../novell-naudit
lrwxrwxrwx 1 root root 10 2008-05-16 16:26 S11novell-naudit -> ../novell-naudit
```

```
metaserver1:/home/admin # ll /etc/init.d/rc5.d/ |grep userapp
lrwxrwxrwx 1 root root 10 2008-05-16 16:26 K12userapp -> ../userapp
lrwxrwxrwx 1 root root 10 2008-05-16 16:26 S10userapp -> ../userapp
```

```
metaserver1:/home/admin # ll /etc/init.d/rc5.d/ |grep ndsd
lrwxrwxrwx 1 root root 7 2008-05-16 13:23 K12ndsd -> ../ndsd
lrwxrwxrwx 1 root root 7 2008-05-16 13:23 S10ndsd -> ../ndsd
```

Enter the following commands as a corrective action if the novell-naudit number is the same or lower than the ndsd number:

```
metaserver1:/home/admin # mv /etc/init.d/rc5.d/S10novell-naudit /etc/init.d/rc5.d/S12novell-naudit
```

- 5 Enter `gedit /etc/logevent.conf` to edit the platform agent configuration file.
- 6 Change the *LogHost* parameter from `LogHost=Not Configured` or `127.0.0.1` to `LogHost=172.17.2.117`.
- 7 Select *File > Save* to save the changes, then select *File > Quit* to exit.
- 8 Restart your Secure Logging Server by entering `/etc/init.d/novell-naudit restart`.
- 9 Enter `exit` twice to log out as `root` and to close the Gnome Terminal.

12.7.3 Connecting to the Novell Audit Database

- 1 To configure the Audit plug-ins to connect to your naudit database so you can look at the logged events from within iManager, select *Auditing and Logging > Query Options*, then click *New*.
- 2 Provide the necessary connection information in the fields:

Fields	Information
<i>Name</i>	Audit Log This is how you want this data source to be listed in iManager
<i>JDBC Class</i>	com.mysql.jdbc.Driver
<i>JDBC URL</i>	jdbc:mysql://172.17.2.117/naudit Make sure to use a real IP address here.
<i>Table</i>	NAUDITLOG
<i>Username</i>	auditusr
<i>Password</i>	n0v3ll
<i>Store Password</i>	Select this option if you don't want to enter the password every time you run a query. However, by selecting this option you also allow others the ability to run queries. Carefully consider your choice.

- 3 Test the database connectivity and make sure there are logged events in the NAUDITLOG table.
 - 3a Select *Auditing and Logging > Queries* from the Roles and Tasks list.
 - 3b Select the check box next to *All*, then select *Run Query* to return records from the last Secure Logging Server restart.
- 4 Exit iManager.
- 5 Proceed to **Chapter 13, “Removing Temporary Files after Installation,” on page 99**.

12.8 Enabling Audit Events for the User Application

The following procedure allows User Application events to be logged to Novell Audit or to Sentinel.

- 1 Select *Gnome Terminal* from the *Computer* menu.
- 2 Enter `ls /opt/novell/idm/NAuditPA.jar` to verify the `NAuditPA.jar` exists in the `/opt/novell/idm/` directory.
- 3 Log in as `root` by entering `su`, then enter the `root` password.
- 4 Enter `gedit /etc/logevent.conf` to edit the audit configuration file.
- 5 At the end of the file, add the following lines:
 - ♦ `LogJavaClass=/opt/novell/idm/NAuditPA.jar`
 - ♦ `LogCacheDir=/opt/novell/idm/naudit/cache`
 - ♦ `LogCachePort=1233`
 - ♦ `LogMaxBigData=8192`
- 6 Select *File > Save* to save the changes, then select *File > Quit* to exit.
- 7 Enter `/etc/init.d/novell-naudit restart` to restart Novell Audit to pick up the changes to the `logevent.conf` file.
- 8 Log into the User Application portal (<https://172.17.2.117:8444/IDMProv>) as the portal administrator (`cn=padmin,dc=admins,dc=system password n0v3ll`).
- 9 Click the *Administration* tab.
- 10 Select *Portal Configuration > Logging* in the menu on the left.
- 11 Select the following two options:
 - ♦ *Also send logging messages to Novell Audit*
 - ♦ *Persist the logging changes*
- 12 Click *Submit* to save the changes.
- 13 Exit the User Application portal Web page.
- 14 Restart the User Application by entering the following in the Gnome Terminal:
`/etc/init.d/userapp restart`
- 15 Enter `exit` twice to log out as `root` and to close the Gnome Terminal.

Removing Temporary Files after Installation

13

Now that you have completed the installation of the Identity Manager components, clean up the installation files. If you followed the example, all you need to do is to remove the `~/tmp` directory and all of its subdirectories and files.

- 1 From the *Computer* menu, select *Gnome Terminal*.
- 2 Make sure that there are no files you need in the `/usr/tmp` directory.
- 3 Log in as `root` by entering `su`, then enter the `root` password.
- 4 Enter `cd /usr`, then enter `rm -r /tmp`.
That removes the `/tmp` directory and all subdirectories and files.
- 5 Enter `exit` twice to log out as `root` and close the Gnome Terminal.
- 6 Proceed to [Chapter 14, “Initializing the Resource Kit,”](#) on page 101.

Initializing the Resource Kit

14

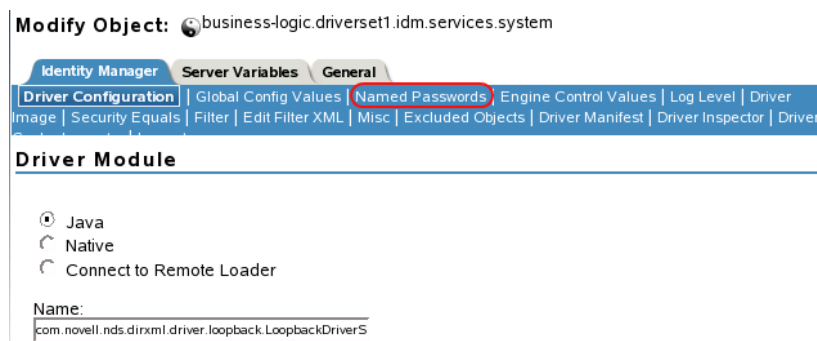
To finalize the initialization of the Resource Kit, you must start all of the drivers. This enables all of the business logic so the kit can function as designed. The following sections guide you through the initialization process:

- ♦ [Section 14.1, “Final Configuration for the Workflow Process,” on page 101](#)
- ♦ [Section 14.2, “Starting the Drivers,” on page 102](#)
- ♦ [Section 14.3, “Getting a Baseline of Business Logic,” on page 103](#)

14.1 Final Configuration for the Workflow Process

In order for the workflow process to work properly, a Named Password must be set on the business-logic driver.

- 1 In iManager select *Identity Manager > Identity Manager Overview* from the list of Roles and Tasks.
- 2 Browse to and select the driver set. The context is `driverset1.idm.services.system`.
- 3 Click the driver set to display all of the drivers stored in the driver set.
- 4 Click the upper right corner of the business-logic driver, then select *Edit Properties*.
- 5 Select the *Named Password* tab.



- 6 Select the Workflow User Password to edit it.



Named Passwords lets you securely store multiple passwords for a driver. Instead of including a password in clear text in a driver policy, you can configure the policy to request a Named Password.

Named Passwords

For server: metaserver1.metaserver1.servers.system

☐ [Workflow User](#)

The Named Password has been created, but there is no password set.

- 7 Specify the password n0v3ll in the password fields, then click *OK* to save the changes.

Named Password

Named Passwords lets you securely store multiple passwords for a driver. Instead of including a password in clear text in a driver policy, you can configure the policy to request a Named Password.

Name:
workflow-user

Display name:
Workflow User Password


Enter password:

Reenter password:

- 8 Click *OK* to exit the properties of the business-logic driver.
- 9 Proceed to [Section 14.2, “Starting the Drivers,”](#) on page 102.

14.2 Starting the Drivers

You must use Designer to start all of the drivers at the same time. If you want to start each driver individually, you can do it from iManager.

- 1 Log in to the SLES server as admin, then double-click the Designer icon on the desktop to launch Designer.
- 2 In Designer, select the driver set, then click the Start All Drivers icon  on the Modeler toolbar.

This displays an information dialog box that lists the status for each driver in the driver set.

- 3 Verify that the Notes, Active Directory*, and Sentinel™ drivers are the only drivers not running, then click *OK*.

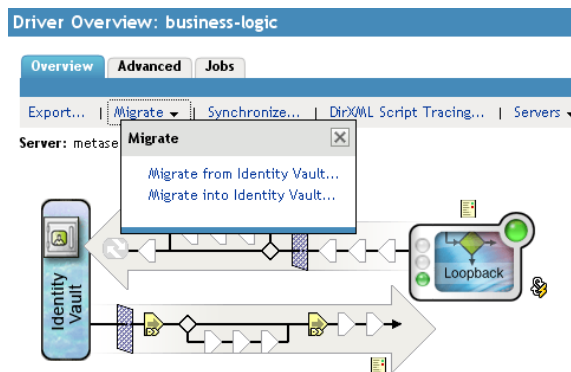
You must configure the Notes driver, the Active Directory driver, and the Sentinel driver for your environment. If there are other drivers that are not running, see “[Viewing Identity Manager Processes](#)” in the *Identity Manager 3.6 Common Driver Administration Guide*, which shows you how to enable tracing on the driver so you can troubleshoot why they are not starting.

- 4 Proceed to [Section 14.3, “Getting a Baseline of Business Logic,”](#) on page 103.

14.3 Getting a Baseline of Business Logic

Now that all the of drivers are running, you can complete the last initialization step, which is to get a baseline of the business logic and export your user data by using the import/export drivers.

- 1 In iManager, select *Identity Manager > Identity Manager Overview*.
If the iManager session timed out, you need to log in to iManager again.
- 2 Browse to and select the `driverset1.idm.services.system` driver set, then click *Search*.
- 3 Click the business-logic driver.
- 4 Select *Migrate > Migrate from Identity Vault*.



- 5 Click *Add*, then browse to and select the `user.company.data` container.
- 6 Click *OK* to add the container, then click *OK* to start the migration.
- 7 Click *OK* in the success message.
- 8 Click *Identity Manager Overview* at the top of the screen to return to the Overview page.
- 9 Repeat **Step 3** through **Step 8** for the `user-import-export` driver, then continue with **Step 10**.
- 10 Check the `/var/novell/idm/users/output` directory for the `<timestamp>.csv` file.
This file contains all the users in the `users.company.data` container.
- 11 Modify this file and copy it to the `/var/novell/idm/users/input` folder to update the objects in the Identity Vault.
- 12 Repeat **Step 1** through **Step 8** for the `image-import-export` driver, then continue with **Step 13**.
- 13 Check the `/var/novell/idm/users/output/images` directory for `workforceID.png` files. These are all the employees' photos. Replace one of the photos with a different photo and copy it into the `/var/novell/idm/users/input/images` folder to update the photo for the user identified by the `workforce ID` in the Identity Vault.
- 14 Proceed to **Chapter 15, “Activating the Resource Kit,”** on page 105.

Activating the Resource Kit

15

The following information explains how activation works for products based on Novell® Identity Manager. All components of the Resource Kit (Identity Manager, Integration Modules, and the Provisioning Module) must be activated within 90 days of installation, or they will shut down. At any time during the 90 days, or afterward, you can choose to activate Identity Manager products.

You can activate Identity Manager and drivers by completing the following tasks:

- ♦ [Section 15.1, “Purchasing an Identity Manager Product License,” on page 105](#)
- ♦ [Section 15.2, “Using a Credential to Activate Identity Manager Products,” on page 105](#)
- ♦ [Section 15.3, “Installing a Product Activation Credential,” on page 106](#)
- ♦ [Section 15.4, “Viewing Product Activations for Identity Manager and Drivers,” on page 107](#)

15.1 Purchasing an Identity Manager Product License

To purchase an Identity Manager product license, see the [Novell Identity Manager How to Buy Web page \(http://www.novell.com/products/identitymanager/howtobuy.html\)](http://www.novell.com/products/identitymanager/howtobuy.html)

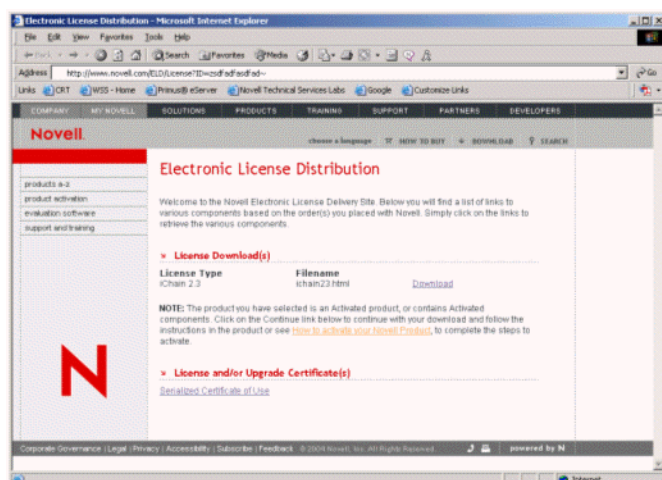
After you purchase a product license, Novell sends you a Customer ID via e-mail. The e-mail also contains a URL to the Novell site where you can obtain a credential. If you do not remember or do not receive your Customer ID, call the Novell Activation Center at 1-800-418-8373 in the U.S. In all other locations, call 1-801-861-8373. (You will be charged for calls made using the 801 area code.)

15.2 Using a Credential to Activate Identity Manager Products

- 1 After you purchase a license, Novell sends you an e-mail with your Customer ID. The e-mail also contains a link under the Order Detail section to the site where you can obtain your credential. Click the link to go to the site.

IMPORTANT: The e-mail is not required to activate the product. If the e-mail was sent to someone else within your company, contact the Novell Activation Center for more information.

After clicking the link, you should see a page similar to the one below:



- 2 Click the license download link and either save (download) or open the .html file.

After the file is opened, its content should be similar to the content shown in the illustration below:



- 3 Proceed to **Section 15.3, “Installing a Product Activation Credential,”** on page 106 for instructions on how to activate Identity Manager components.

15.3 Installing a Product Activation Credential

You should install the Product Activation Credential via iManager.

- 1 Open the Novell e-mail that contains the Product Activation Credential.

2 Do one of the following:

- ♦ Save the Product Activation Credential file.
or
- ♦ Open the Product Activation Credential file, then copy the contents of the Product Activation Credential to your clipboard.

Carefully copy the contents, and make sure that no extra lines or spaces are included. You should begin copying from the first dash (-) of the credential (----BEGIN PRODUCT ACTIVATION CREDENTIAL) through the last dash (-) of the credential (END PRODUCT ACTIVATION CREDENTIAL-----).

3 Log in to iManager as admin. (<https://172.17.2.117:8443/nps/iManager.html>)

4 Choose *Identity Manager > Identity Manager Overview*.

5 Select the driver set or browse to a driver set, then click *Next*.

6 On the Identity Manager Overview page, locate the driver set, click the red *Activation required* by link, then click *Install Activation*.

7 Select the driver set where you want to activate an Identity Manager component.

8 Do one of the following:

- ♦ Specify where you saved the Identity Manager Activation Credential, then click *Next*.
or
- ♦ Paste the contents of the Identity Manager Activation Credential into the text area, then click *Next*.

9 Click *Finish*.

You need to activate each driver set that has a driver. You can activate any tree with the credential.

10 Proceed to [Section 15.4, “Viewing Product Activations for Identity Manager and Drivers,” on page 107](#).

15.4 Viewing Product Activations for Identity Manager and Drivers

For each of your driver sets, you can see the Product Activation Credentials you have installed for the Metadirectory engine and Identity Manager drivers.

1 Log in to iManager as admin. (<https://172.17.2.117:8443/nps/iManager.html>)

2 Click *Identity Manager > Identity Manager Overview*.

3 Browse to and select the driver set or the driver you want to view activation information for.

4 Select the *Activation* tab.

You can view the text of the activation credential or, if an error is reported, you can remove an activation credential.

After installing a valid Product Activation Credential for a driver set, you might still see “Activation Required” next to the driver name. If this is the case, restart the driver and the message should then disappear.

The Identity Manager portion of the Resource Kit is ready to use. You can modify the current setup for your customers or you can use it as a demo for the customer.

Documentation Updates

A

The documentation was updated on the following dates:

- ♦ Section A.1, “August 29, 2008,” on page 109

A.1 August 29, 2008

Updates were made to the following sections. The changes are explained below.

A.1.1 Installing and Configuring Novell Audit

Location	Change
Section 12.8, “Enabling Audit Events for the User Application,” on page 97	Added this new section.