

Installation Guide

Novell[®] Identity Manager

4.0

October 15, 2010

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 © 2007-2010 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.
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
Part I Planning	11
1 Setting Up a Development Environment	13
2 Creating a Project Plan	15
2.1 Discovery Phase	15
2.1.1 Defining Current Business Processes	16
2.1.2 Defining How the Identity Manager Solution Affects the Current Business Processes	17
2.1.3 Identifying the Key Business and Technical Stakeholders	18
2.1.4 Interviewing All Stakeholders	18
2.1.5 Creating a High-level Strategy and an Agreed Execution Path	18
2.2 Requirements and Design Analysis Phase	19
2.2.1 Defining the Business Requirements	20
2.2.2 Analyzing Your Business Processes	21
2.2.3 Designing an Enterprise Data Model	22
2.3 Proof of Concept	23
2.4 Data Validation and Preparation	23
2.5 Production Pilot	24
2.6 Production Rollout Planning	24
2.7 Production Deployment	25
3 Technical Guidelines	27
3.1 Management Tools Guidelines	28
3.1.1 Analyzer Guidelines	28
3.1.2 Designer Guidelines	29
3.1.3 iManager Guidelines	29
3.1.4 Role Mapping Administrator Guidelines	29
3.2 Metadirectory Server Guidelines	29
3.3 eDirectory Guidelines	30
3.3.1 Identity Manager Objects in eDirectory	31
3.3.2 Replicating the Objects that Identity Manager Needs on the Server	31
3.3.3 Using Scope Filtering to Manage Users on Different Servers	33
3.4 User Application	35
3.5 Auditing and Reporting Guidelines	36
Part II Installation	39
4 Basic Identity Manager System Checklist	41
4.1 Prerequisites	42
4.2 Planning	42
4.3 Installation	42
4.4 Driver Configuration with the Remote Loader	43

4.5	Driver Configuration without the Remote Loader	43
4.6	Additional Configuration	43
5	Where to Get Identity Manager	45
6	System Requirements	47
6.1	eDirectory and iManager	48
6.2	Metadirectory Server	49
6.2.1	Supported Processors	49
6.2.2	Server Operating Systems	50
6.3	Remote Loader	51
6.4	User Application	53
6.5	Auditing and Reporting	54
6.6	Workstations	54
6.6.1	Workstation Platforms	55
6.6.2	Web Browsers	56
6.7	Resource Requirements	57
7	Installing Identity Manager	59
7.1	Installing Analyzer	59
7.2	Installing Designer	60
7.3	Installing eDirectory	60
7.4	Installing iManager	61
7.5	Installing the Metadirectory Server	61
7.5.1	Non-root Installation of the Metadirectory Server	63
7.5.2	Silent Installation of the Metadirectory Server	64
7.6	Installing the Remote Loader	65
7.6.1	Requirements	65
7.6.2	Supported Drivers	65
7.6.3	Installation Procedure	66
7.6.4	Silent Installation of the Remote Loader	68
7.6.5	Installing the Java Remote Loader on UNIX or Linux	69
7.6.6	Coexistence of 32-bit and 64-bit Remote Loader	70
7.7	Installing the Driver Files	70
7.8	Installing the Roles Based Provisioning Module	71
7.9	Installing a Custom Driver	71
7.10	Installing the Role Mapping Administrator	71
7.11	Installing the Identity Reporting Module or Sentinel	72
8	Activating Novell Identity Manager Products	73
8.1	Purchasing an Identity Manager Product License	73
8.2	Installing a Product Activation Credential	73
8.3	Viewing Product Activations for Identity Manager and for Drivers	74
8.4	Activating Identity Manager Drivers	75
8.5	Activating Analyzer	75
8.6	Activating Designer and the Role Mapping Administrator	75

9 Troubleshooting Identity Manager	77
Part III Upgrading or Migrating	83
10 What's New	85
10.1 Identity Reporting Module	85
10.2 New Drivers	85
10.2.1 SharePoint Driver (.NET Remote Loader)	85
10.2.2 Salesforce.com Driver	86
10.3 Support for XDAS Auditing Included	86
10.4 Packages Replace Driver Configuration Files	86
10.5 Role Mapping Administrator	86
10.6 Analyzer	86
10.7 Integrated Installer	86
11 Upgrade Versus Migration	87
11.1 Upgrade	87
11.2 Migration	88
11.3 Multiple Servers Associated with a Single Driver Set	88
12 Supported Versions and System Requirements for Upgrades and Migrations	89
12.1 Upgrades	89
12.1.1 Supported Versions for Upgrades	89
12.1.2 System Requirements	89
12.2 Migrations	90
12.2.1 Supported Versions for Migrations	90
12.2.2 System Requirements	90
13 Performing an Upgrade	91
13.1 Upgrade Checklist	91
13.2 Creating a Backup of the Current Configuration	93
13.2.1 Ensuring that Your Designer Project is Current	93
13.2.2 Creating an Export of the Drivers	95
13.3 Upgrading iManager	95
13.4 Stopping the Drivers	96
13.4.1 Using Designer to Stop the Drivers	96
13.4.2 Using iManager to Stop the Drivers	96
13.5 Upgrading Analyzer	97
13.6 Upgrading Designer	97
13.7 Upgrading the Metadirectory Server and Driver Shim Files	98
13.8 Upgrading the Remote Loader	99
13.9 Upgrading Drivers to Packages	99
13.9.1 Creating a New Driver	100
13.9.2 Replacing Existing Content with Content from Packages	100
13.9.3 Keeping the Current Content and Adding New Content with Packages	101
13.10 Restoring Custom Policies and Rules to the Driver	101
13.10.1 Using Designer to Restore Custom Policies and Rules to the Driver	102
13.10.2 Using iManager to Restore Custom Policies and Rules to the Driver	103
13.11 Overlaying the Existing Driver Configuration File with the New Driver (Deprecated)	103

13.11.1	Using Designer to Overlay the Existing Driver Configuration File with the New Driver	104
13.11.2	Using iManager to Overlay the Existing Driver Configuration File with the New Driver	104
13.12	Deploying the Converted Project	105
13.13	Starting the Drivers	105
13.13.1	Using Designer to Start the Drivers	105
13.13.2	Using iManager to Start the Drivers	105
14	Performing a Migration	107
14.1	Migration Checklist	107
14.2	Adding the New Server to the Driver Set	108
14.3	Changing Server-Specific Information	109
14.3.1	Changing the Server-Specific Information in Designer	109
14.3.2	Changing the Server-Specific Information in iManager	110
14.4	Removing the Old Server from the Driver Set	110
14.4.1	Using Designer to Remove the Old Server from the Driver Set	110
14.4.2	Using iManager to Remove the Old Server from the Driver Set	111
14.4.3	Decommissioning the Old Server	111
Part IV	Uninstalling Identity Manager	113
15	Uninstalling the Identity Manager Components	115
15.1	Removing Objects from eDirectory	115
15.2	Uninstalling the Metadirectory Server	116
15.2.1	Uninstalling on Linux/UNIX	116
15.2.2	Uninstalling on Windows	116
15.2.3	Uninstalling a Non-root Installation	116
15.3	Uninstall the Remote Loader	116
15.3.1	Uninstalling on Linux/UNIX	117
15.3.2	Uninstalling on Windows	117
15.4	Uninstalling the Roles Based Provisioning Module	117
15.4.1	Deleting the Drivers	117
15.4.2	Uninstalling the User Application	117
15.4.3	Uninstalling the Application Server and the Database	118
15.5	Uninstalling the Identity Reporting Module Components	119
15.5.1	Deleting the Reporting Drivers	119
15.5.2	Uninstalling the Identity Reporting Module	119
15.5.3	Uninstalling the Event Auditing Service	119
15.6	Uninstalling iManager	119
15.7	Uninstalling eDirectory	120
15.8	Uninstalling Analyzer	121
15.9	Uninstalling Designer	121
15.10	Uninstalling the Role Mapping Administrator	122

About This Guide

Novell Identity Manager is a data sharing and synchronization service that enables applications, directories, and databases to share information. It links scattered information and enables you to establish policies that govern automatic updates to designated systems when identity changes occur. Identity Manager provides the foundation for account provisioning, security, single sign-on, user self-service, authentication, authorization, automated workflow, and Web services. It allows you to integrate, manage, and control your distributed identity information so you can securely deliver the right resources to the right people.

This guide contains information about how to plan, install, or upgrade an Identity Manager system that is useful for your environment.

- ◆ Part I, “Planning,” on page 11
 - ◆ Chapter 1, “Setting Up a Development Environment,” on page 13
 - ◆ Chapter 2, “Creating a Project Plan,” on page 15
 - ◆ Chapter 3, “Technical Guidelines,” on page 27
- ◆ Part II, “Installation,” on page 39
 - ◆ Chapter 4, “Basic Identity Manager System Checklist,” on page 41
 - ◆ Chapter 5, “Where to Get Identity Manager,” on page 45
 - ◆ Chapter 6, “System Requirements,” on page 47
 - ◆ Chapter 7, “Installing Identity Manager,” on page 59
 - ◆ Chapter 8, “Activating Novell Identity Manager Products,” on page 73
- ◆ Part III, “Upgrading or Migrating,” on page 83
 - ◆ Chapter 10, “What’s New,” on page 85
 - ◆ Chapter 11, “Upgrade Versus Migration,” on page 87
 - ◆ Chapter 12, “Supported Versions and System Requirements for Upgrades and Migrations,” on page 89
 - ◆ Chapter 13, “Performing an Upgrade,” on page 91
 - ◆ Chapter 14, “Performing a Migration,” on page 107
- ◆ Part IV, “Uninstalling Identity Manager,” on page 113

Audience

This guide is intended for administrators, consultants, and network engineers who plan and implement Identity Manager in a network environment.

Documentation Updates

For the most recent version of this document, see the [Identity Manager Documentation Web site \(http://www.novell.com/documentation/idm40/index.html\)](http://www.novell.com/documentation/idm40/index.html).

Additional Documentation

For additional Identity Manager Drivers documentation, see the [Identity Manager Drivers Documentation Web site](http://www.novell.com/documentation/idm40drivers/index.html) (<http://www.novell.com/documentation/idm40drivers/index.html>).

For User Application documentation, see the [Identity Manager Roles Based Provisioning Module Documentation Web site](http://www.novell.com/documentation/idmrpbm40/index.html) (<http://www.novell.com/documentation/idmrpbm40/index.html>).

Planning

Identity Manager 4.0 helps you manage the identities and resources in your business. It also automates many business processes for you that are currently manual tasks.

If you have any questions about the different components that make up an Identity Manager solution, see the *Identity Manager 4.0 Overview Guide* guide for more information about each component.

To create an effective Identity Manager solution for your environment, you first must take time to plan and design the solution. There are two major aspects to planning: setting up a test lab to become familiar with the products and creating a project plan to implement an Identity Manager solution. When you create a project plan, you define your business process and create an implementation plan. Most companies have many different business processes that are managed by many different people. A complete Identity Manager solution affects most of these processes. It is extremely important to take the time to plan an Identity Manager solution, so that it can be effectively implemented in your environment.

If you are creating a new Identity Manager solution where all of the components resides on the same server, use the *Identity Manager 4.0 Integrated Installation Guide* to help you with the installation. This is a simplified installer to help you get a system set up faster.

We strongly recommend that you engage an Identity Manager expert to assist in each phase of your Identity Manager implementation. For more information about partnership options, see the [Novell Solution Partner Web site \(http://www.novell.com/partners/\)](http://www.novell.com/partners/). Novell Education also offers courses that address Identity Manager implementation.

- ♦ Chapter 1, “Setting Up a Development Environment,” on page 13
- ♦ Chapter 2, “Creating a Project Plan,” on page 15
- ♦ Chapter 3, “Technical Guidelines,” on page 27

Setting Up a Development Environment

1

Before you begin the planning phase of the Identity Manager deployment, you must be familiar with the Identity Manager products so you can create a useful plan. Setting up a development environment where you can test, analyze, and develop your Identity Manager solution allows you to learn about each component of Identity Manager and find unforeseen issues that can arise.

For example, when you synchronize information between different systems, the information is presented differently for each system. Changing the data to see how it synchronizes between these two systems allows you to see if this change affects other systems that use this same information.

Another major reason to set up a development environment is to make sure your solutions work before you apply them to live data. Identity Manager manipulates and deletes data. Having the test environment allows you to make changes without any loss to the data in your production environment.

You should set up a development environment for each deployment of Identity Manager. Each deployment is different. There are different systems, business policies, and procedures that need to be included in the Identity Manager solution. The development environment allows you to create the solution that is best for each situation.

The most important tool to use when you are developing your Identity Manager solution is Designer. It allows you to capture all of the information about your environment and then use that information to create an Identity Manager solution that fits your needs. You should use Designer during all aspects of the planning to capture all of the information. Designer makes it much easier to create a project plan that includes the business information as well as the technical information. For more information about Designer, see [Designer 4.0 for Identity Manager 4.0 Administration Guide](#).

To set up your development environment, use the information in [Chapter 4, “Basic Identity Manager System Checklist,” on page 41](#). It is an installation checklist of all of the Identity Manager components. Use this list to make sure you have installed and configured all components for Identity Manager that you can use to develop a project plan. Use the information in [Chapter 3, “Technical Guidelines,” on page 27](#) as you set up your development environment, so you can learn about technical considerations as you install and configure each component of Identity Manager.

After your development environment is created, the next step is to create the project plan to implement the Identity Manager solution. Use the information in [Chapter 2, “Creating a Project Plan,” on page 15](#) to create the project plan.

Creating a Project Plan

2

This planning material provides an overview of the activities that are usually part of an Identity Manager project, from its inception to its full production deployment. Implementing an identity management strategy requires you to discover what all of your current business processes are, what are the needs for these processes, who the stakeholders are in your environment, and then design a solution, get buy-in from stakeholders, and test and roll out the solution. This section is intended to provide you with sufficient understanding of the process so that you can maximize the benefit from working with Identity Manager.

This section is not exhaustive; it is not intended to address all possible configurations, nor is it intended to be rigid in its execution. Each environment is different and requires flexibility in the type of activities to be used.

- ◆ [Section 2.1, “Discovery Phase,” on page 15](#)
- ◆ [Section 2.2, “Requirements and Design Analysis Phase,” on page 19](#)
- ◆ [Section 2.3, “Proof of Concept,” on page 23](#)
- ◆ [Section 2.4, “Data Validation and Preparation,” on page 23](#)
- ◆ [Section 2.5, “Production Pilot,” on page 24](#)
- ◆ [Section 2.6, “Production Rollout Planning,” on page 24](#)
- ◆ [Section 2.7, “Production Deployment,” on page 25](#)

2.1 Discovery Phase

The Identity Manager solution affects many aspects of your business. In order to create an effective solution, you must take time to define all of your current business processes, then identify how an implementation of Identity Manager changes these processes, who these changes affect, and how the changes are implemented.

The discovery phase provides a common understanding of the issues and solutions for all stakeholders. It creates a plan or road map that contains the key business and systems information that are affected by the Identity Manager solution. It also allows all stakeholders to participate in the creation of the Identity Manager solution so they understand how it can affect their area of the business.

The following list indicates the steps needed to have a successful discovery phase. There might be additional items you find that you need to add to the list as you proceed through the discovery and design phases.

- ◆ [Section 2.1.1, “Defining Current Business Processes,” on page 16](#)
- ◆ [Section 2.1.2, “Defining How the Identity Manager Solution Affects the Current Business Processes,” on page 17](#)
- ◆ [Section 2.1.3, “Identifying the Key Business and Technical Stakeholders,” on page 18](#)
- ◆ [Section 2.1.4, “Interviewing All Stakeholders,” on page 18](#)
- ◆ [Section 2.1.5, “Creating a High-level Strategy and an Agreed Execution Path,” on page 18](#)

2.1.1 Defining Current Business Processes

Identity Manager automates business processes to easily manage identities in your environment. If you do not know what the current business processes are, you cannot design an Identity Manager solution that automates those processes. You can use the Architecture mode of Designer to capture your current business processes and display them graphically. For more information, see “[Architect Mode](#)” in the *Designer 4.0 for Identity Manager 4.0 Administration Guide*.

For example, your company might identify the following business processes:

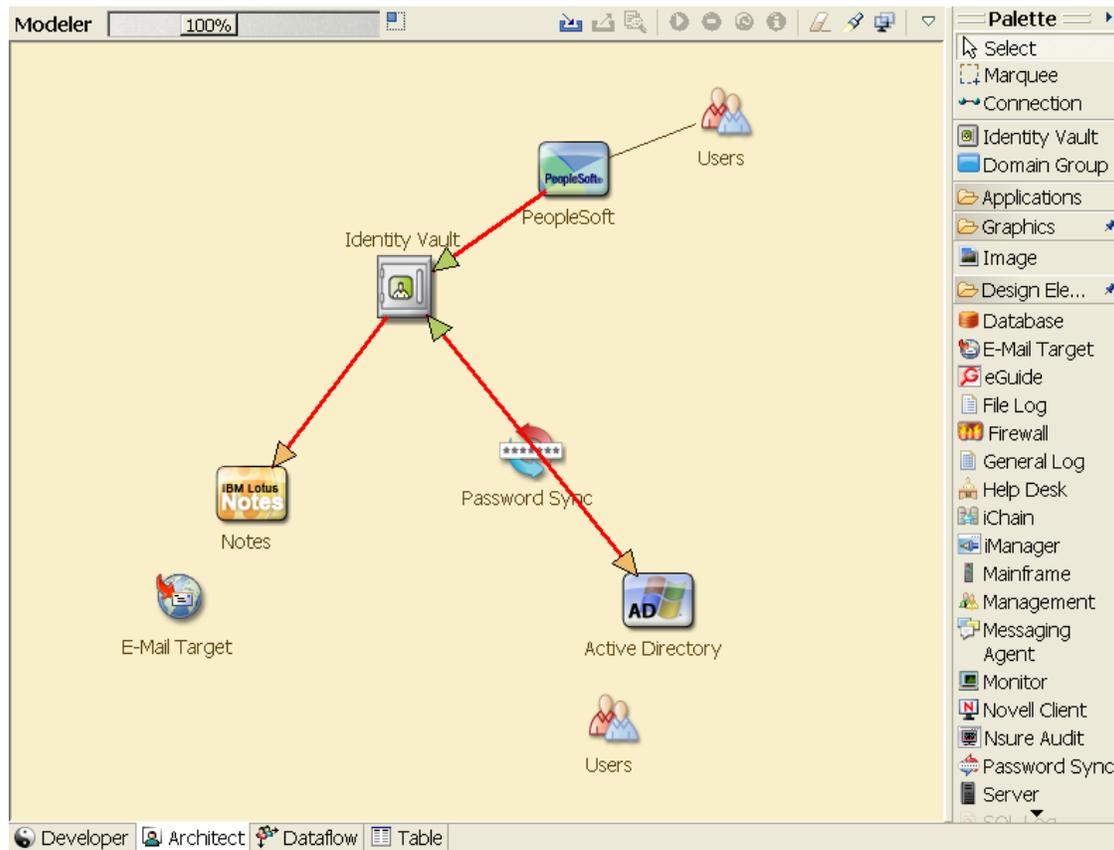
- ◆ When an employee is terminated, the user account in the e-mail system is deleted, but the user’s account in all other systems is disabled, not deleted.
- ◆ The format for a user’s e-mail address.
- ◆ The systems or resources that sales employees can access.
- ◆ The systems or resources that managers can access.
- ◆ What systems generate new accounts? Is it the human resource system or is it through a workflow request?
- ◆ A password policy for the company that defines how often a password changes, how complex the password is, and which systems are synchronizing the password.

As you define your business processes, use the following list of items to help you understand all of the processes:

- ◆ Define or clarify the current business issues.
- ◆ Determine what initiatives are required to address these issues.
- ◆ Determine which services and systems are affected by these initiatives.

This step allows you to create a high-level overview of what your business is currently doing and what processes need to be improved. For example, [Figure 2-1](#) uses Designer to show how new user accounts are generated from the PeopleSoft system. They are synchronized into the Identity Vault and then synchronized into Lotus Notes and Active Directory. Passwords are being synchronized between Active Directory and the Identity Vault. Accounts are synchronizing into the Notes system, but no accounts are synchronizing back to the Identity Vault.

Figure 2-1 Example of Business Processes



After you determine processes, you start to identify how Identity Manager can be involved. Continue with [Section 2.1.2, “Defining How the Identity Manager Solution Affects the Current Business Processes,”](#) on page 17.

2.1.2 Defining How the Identity Manager Solution Affects the Current Business Processes

After you have defined your current business processes, you need to decide which processes you want to incorporate into an Identity Manager solution.

It is best to look at the entire solution and then prioritize which processes should be implemented. Identity Manager encompasses so many aspects of your business, it is easier to plan the entire solution rather than approach each business process as its own solution.

Create a list of which business processes are a priority to automate, then identify which systems these changes will affect. Then continue with [Section 2.1.3, “Identifying the Key Business and Technical Stakeholders,”](#) on page 18.

2.1.3 Identifying the Key Business and Technical Stakeholders

Identifying all stakeholders involved in the Identity Manager solution is important for the success of the solution. In most companies, there is not just one person you can contact who understands all business and technical aspects of the business processes. You must identify which services and systems are going to be affected by the Identity Manager solution, and you must also identify the person who is responsible for that service or system.

For example, if you are integrating an e-mail system into your solution, you would need to list what the e-mail system is, who the e-mail system administrator is, and what the contact information is. You can add all of this information into the Designer project. Each application icon has a place where you can store information about the system and the system administrator. For more information, see “[Configuring Application Properties](#)” in the *Designer 4.0 for Identity Manager 4.0 Administration Guide*.

After you have identified all of the people involved in each business process, the next step is in [Section 2.1.4, “Interviewing All Stakeholders,”](#) on page 18.

2.1.4 Interviewing All Stakeholders

Interviews with key business and technical stakeholders allow you to gather information needed for a complete design of the Identity Manager solution. The interviews also allow you to educate each stakeholder about the Identity Manager solution and how the solution affects them. Here is a list of items to cover when you do the interviews:

- ♦ Define or clarify the business processes being addressed by the Identity Manager solution. The person you are interviewing might have information that can change the current plan.
- ♦ Determine how the solution will impact the stakeholders and address any concerns they have. Also ask the stakeholders how much time their part of the solution might take. They might or might not have an estimate, but gathering this information helps to determine the scope of the solution.
- ♦ Capture key business and systems information from the stakeholders. Sometimes a proposed plan might adversely affect a business process or a system. By capturing this information, you can make educated decisions about the Identity Manager solution.

After you have interviewed the key stakeholders, the next step is in [Section 2.1.5, “Creating a High-level Strategy and an Agreed Execution Path,”](#) on page 18.

2.1.5 Creating a High-level Strategy and an Agreed Execution Path

After all of the information is gathered, you need to create a high-level strategy or road map for the Identity Manager solution. Add all of the features you want to be included in the Identity Manager solution. For example, new user accounts are generated from a request through a workflow, but the type of user depends upon the resources the user is given access to.

Present this high-level strategy to all of the stakeholders in the same meeting, if possible. This allows you to accomplish several things:

- ♦ Verify that the included initiatives are the most correct and identify which ones have the highest priority.

- ◆ Identify planning activities in preparation for a requirements and design phase
- ◆ Determine what it would take to carry out one or more of these initiatives.
- ◆ Create an agreed execution path for the Identity Manager solution.
- ◆ Define additional education for stakeholders.

Discovery provides a common understanding of the issues and solutions for all stakeholders. It provides an excellent primer for the analysis phase, which is a phase that requires stakeholders to have a basic knowledge of directories, Novell eDirectory, Novell Identity Manager, and XML integration in general.

After you have completed the discovery phase, proceed to [Section 2.2, “Requirements and Design Analysis Phase,”](#) on page 19.

2.2 Requirements and Design Analysis Phase

Take the high-level road map that was created in the discovery phase as a starting point for this analysis phase. The document and the Designer project both need technical and business details added. This produces the data model and high-level Identity Manager architecture design used to implement the Identity Manager solution.

The focus of the design should be specifically on identity management; however, many of the elements traditionally associated with a resource management directory, such as file and print, can also be addressed. Identity Manager synchronizes user accounts to directories that do not have direct access to the operating system’s file system. For example, you can have a user account in Active Directory, but that does not grant you access to the file system on the Active Directory server.

Using the information gathered in the discovery phase, answer the following sample questions to see what other information needs to be gathered. This might require additional interviews with stakeholders.

- ◆ What versions of system software are being used?
- ◆ Is the eDirectory design appropriate? For example, does the Identity Manager server contain a Master or Read/Write replica of the user objects that are synchronizing? If it does not, the eDirectory design is not appropriate.
- ◆ Is the quality of the data in all systems appropriate? (If the data is not of usable quality, the business policy might not be implemented as desired.) For example, there might be duplicate accounts for the users in the systems that are synchronizing, or the format of the data might not be consistent throughout each system. Each system’s data must be evaluated before information is synchronized.
- ◆ Is data manipulation required for your environment? For example, a user’s hire date format in the human resource system can only be 2008/02/23 and the hire date in the Identity Vault is 02-23-2008. This requires that the date be manipulated for synchronization to occur.

Identity Manager contains a tool to help you simplify the process of analyzing and cleaning your data. For more information, see [Analyzer 1.2 for Identity Manager Administration Guide](#).

Review the information in [Chapter 3, “Technical Guidelines,”](#) on page 27 to help make the correct decisions for your environment.

After the requirements analysis, you can establish the scope and project plan for the implementation, and determine if any prerequisite activities need to occur. To avoid costly mistakes, be as complete as possible in gathering information and documenting requirements. Here is a list of possible requirements:

- ◆ Data model showing all systems, authoritative data sources, events, information flow, data format standards, and mapping relationships between connected systems and attributes within Identity Manager.
- ◆ Appropriate Identity Manager architecture for the solution.
- ◆ Details for additional system connection requirements.
- ◆ Strategies for data validation and record matching.
- ◆ Directory design to support the Identity Manager infrastructure.

The following tasks should be completed during the requirements and design assessment:

- ◆ [“Defining the Business Requirements” on page 20](#)
- ◆ [“Analyzing Your Business Processes” on page 21](#)
- ◆ [“Designing an Enterprise Data Model” on page 22](#)

2.2.1 Defining the Business Requirements

In the discovery phase, you gathered your organization’s business processes and the business requirements that define these business processes. Create a list of these business requirements and then start mapping these processes in Designer by completing the following tasks:

- ◆ Create a list of the business requirements and determine which systems are affected by this process. For example, a business requirement for terminating an employee might be that the employee’s network and e-mail account access must be removed the same day the employee is terminated. The e-mail system and the Identity Vault are affected by this termination process.
- ◆ Establish the process flows, process triggers, and data mapping relationships.

For example, if something is going to happen in a certain process, what other processes are triggered?

- ◆ Map data flows between applications. Designer allows you to see this information. For more information, see [“Managing the Flow of Data”](#) in the *Designer 4.0 for Identity Manager 4.0 Administration Guide*.
- ◆ Identify data transformations that need to take place from one format to another, such as 2/25/2007 to 25 Feb 2007, and use Analyzer to change the data. For more information, see the *Analyzer 1.2 for Identity Manager Administration Guide*.
- ◆ Document the data dependencies that exist.

If a certain value is changed, it is important to know if there is a dependency on that value. If a particular process is changed, it is important to know if there is a dependency on that process.

For example, selecting a “temporary” employee status value in a human resources system might mean that the IT department needs to create a user object in eDirectory with restricted rights and access to the network during certain hours.

- ◆ List the priorities.

Not every requirement, wish, or desire of every party can be immediately fulfilled. Priorities for designing and deploying the provisioning system will help plan a road map.

It might be advantageous to divide the deployment into phases that enable implementation of a portion of the deployment earlier and other portions of the deployment later, or use a phased deployment that is based on groups of people within the organization.

- ◆ Define the prerequisites.

The prerequisites required for implementing a particular phase of the deployment should be documented. This includes access to the connected systems that need to interface with Identity Manager.

- ◆ Identify authoritative data sources.

Learning early on which items of information that system administrators and managers feel belong to them can help in obtaining and keeping buy-in from all parties.

For example, the account administrator might want ownership over granting rights to specific files and directories for an employee. This can be accommodated by implementing local trustee assignments in the account system.

After you have defined your business requirements, proceed to [Section 2.2.2, “Analyzing Your Business Processes,” on page 21.](#)

2.2.2 Analyzing Your Business Processes

After you complete the analysis of your business requirements, there is more information you need to gather to help focus the Identity Manager solution. You need to interview essential individuals such as managers, administrators, and employees who actually use the application or system. Issues to be addressed include:

- ◆ Where does the data originate?
- ◆ Where does the data go?
- ◆ Who is responsible for the data?
- ◆ Who has ownership for the business function to which the data belongs?
- ◆ Who needs to be contacted to change the data?
- ◆ What are all the implications of the data being changed?
- ◆ What work practices exist for data handling (gathering and/or editing)?
- ◆ What types of operations take place?
- ◆ What methods are used to ensure data quality and integrity?
- ◆ Where do the systems reside (on what servers, in which departments)?
- ◆ What processes are not suitable for automated handling?

For example, you could use the following questions for an administrator for a PeopleSoft system in Human Resources:

- ◆ What data are stored in the PeopleSoft database?
- ◆ What appears in the various panels for an employee account?
- ◆ What actions must be reflected across the provisioning system (such as add, modify, or delete)?
- ◆ Which of these are required? Which are optional?
- ◆ What actions need to be triggered based on actions taken in PeopleSoft?

- ♦ What operations/events/actions are to be ignored?
- ♦ How is the data to be transformed and mapped to Identity Manager?

Interviewing key people can lead to other areas of the organization that can provide a more clear picture of the entire process.

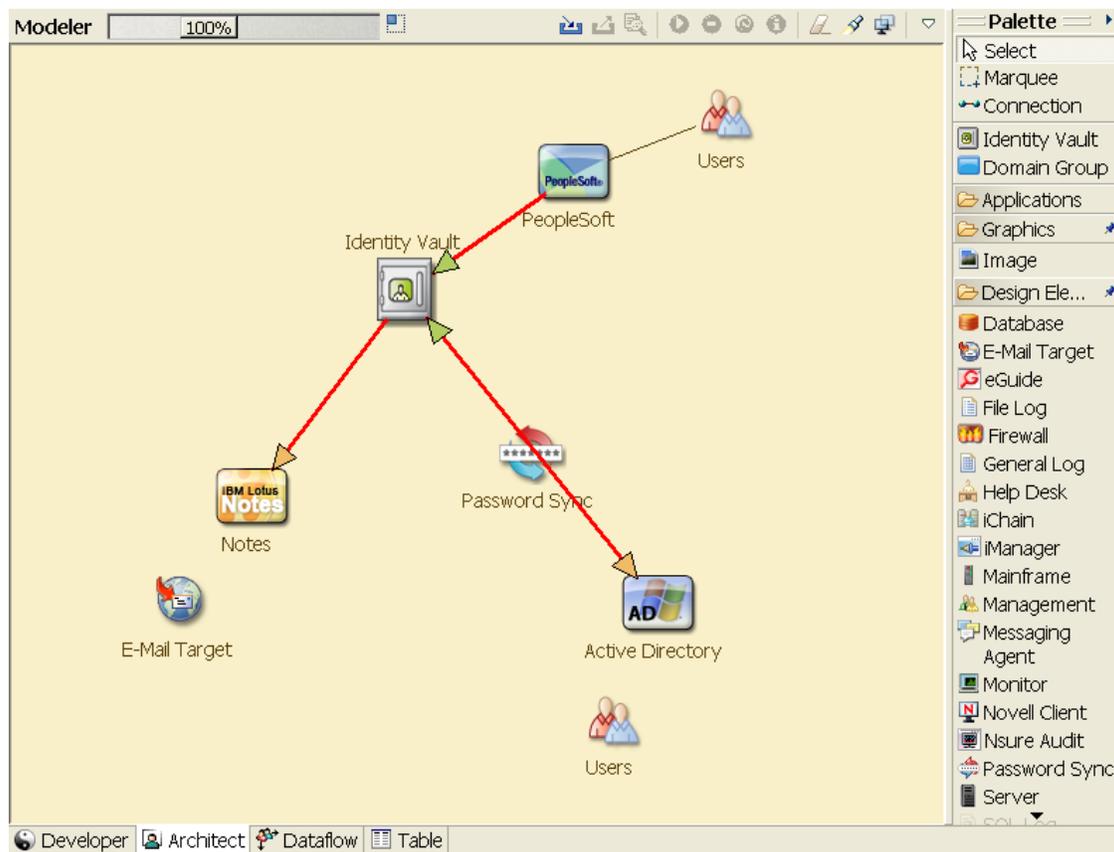
After you have gathered all of this information, you can design a correct enterprise data model for your environment. Proceed to [Section 2.2.3, “Designing an Enterprise Data Model,” on page 22](#) to start the design.

2.2.3 Designing an Enterprise Data Model

After your business processes have been defined, you can use Designer to begin to design a data model that reflects your current business processes.

The model in Designer illustrates where data originates, where it moves to, and where it can’t move. It can also account for how critical events affect the data flow. For example, [Figure 2-2](#) shows that the data flows from the PeopleSoft, but no data synchronizes back into PeopleSoft.

Figure 2-2 Data Flow through Designer



You might also want to develop a diagram that illustrates the proposed business process and the advantages of implementing automated provisioning in that process.

The development of this model begins by answering questions such as the following:

- ♦ What types of objects (users, groups, etc.) are being moved?
- ♦ Which events are of interest?
- ♦ Which attributes need to be synchronized?
- ♦ What data is stored throughout your business for the various types of objects being managed?
- ♦ Is the synchronization one-way or two-way?
- ♦ Which system is the authoritative source for which attributes?

It is also important to consider the interrelationships of different values between systems.

For example, an employee status field in PeopleSoft might have three set values: employee, contractor, and intern. However, the Active Directory system might have only two values: permanent and temporary. In this situation, the relationship between the “contractor” status in PeopleSoft and the “permanent” and “temporary” values in Active Directory needs to be determined.

The focus of this work should be to understand each directory system, how they relate to each other, and what objects and attributes need to be synchronized across the systems. After the design is complete, the next step is to create a proof of concept. Proceed to [Section 2.3, “Proof of Concept,” on page 23](#).

2.3 Proof of Concept

You create an test your proof of concept by using a sample implementation in a lab environment in order to reflect your company’s business policy and data flow. The implementation is based on the design of the data model developed during the requirement analysis and design and is a final step before the production pilot. You perform the tests in the lab you created in [Chapter 1, “Setting Up a Development Environment,” on page 13](#).

NOTE: This step is often beneficial in gaining management support and funding for a final implementation effort.

[Chapter 3, “Technical Guidelines,” on page 27](#) contains information that can help you validate your proof of concept. It contains technical guidelines to help make your Identity Manager deployment successful.

As you create the proof of concept, you need to also create a plan to validate the data that you have in your systems. This step helps you make sure that conflicts don’t occur between systems. Proceed to [Section 2.4, “Data Validation and Preparation,” on page 23](#) to make sure these conflicts do not occur.

2.4 Data Validation and Preparation

The data in production systems can be of varying quality and consistency and therefore might introduce inconsistencies when synchronizing systems. This phase presents an obvious point of separation between the resources implementation team and the business units or groups who “own” or manage the data in the systems to be integrated. At times, the associated risk and cost factors might not belong in a provisioning project.

You need to use the data model that you completed in the analysis and design phases. You should also have a possible record matching and data format strategy in order to prepare the data correctly. With the data model and format strategy defined, you can complete two important steps:

- ◆ Create production data sets appropriate for loading into the Identity Vault (as identified in the analysis and design activities). This includes the probable method of loading (either bulk load or via connectors). The requirement for data that is validated or otherwise formatted is also identified.
- ◆ Identify performance factors and validate these factors against equipment being used and the overall distributed architecture of the deployment of Identity Manager.

After the data is prepared, proceed to [Section 2.5, “Production Pilot,” on page 24](#).

2.5 Production Pilot

The production pilot is the first step in migrating into a production environment. During this phase, there might be additional customization that occurs. In this limited introduction, the desired outcomes of the preceding activities can be confirmed and agreement obtained for the production rollout. The pilot validates the plan that has been created to this point in the process.

NOTE: This phase can provide the acceptance criteria for the solution and the necessary milestone en route to full production.

The pilot solution provides live proof of concept and validation for the data model and desired process outcomes. After the pilot is completed, proceed to [Section 2.6, “Production Rollout Planning,” on page 24](#).

2.6 Production Rollout Planning

This phase is where the production deployment is planned. The plan should do several things:

- ◆ Confirm server platforms, software revisions, and service packs
- ◆ Confirm the general environment
- ◆ Confirm the design of the Identity Vault in a mixed coexistence
- ◆ Confirm that the business logic is correct
- ◆ Confirm that the data synchronization is occurring as planned
- ◆ Plan the legacy process cutover
- ◆ Plan a rollback contingency strategy

The plan needs to contain implementation and completion dates for each step in the rollout. Each stakeholder provides input for these dates and agrees that these dates work for them. This allows each person involved in the rollout to know when the changes are coming and when they should be completed.

With the production rollout plan completed, proceed to the [Section 2.7, “Production Deployment,” on page 25](#).

2.7 Production Deployment

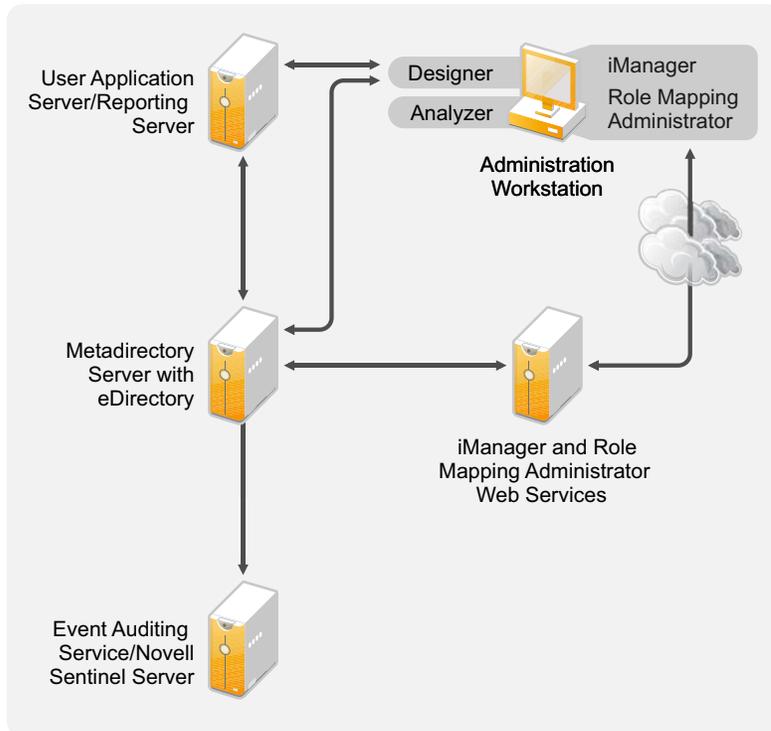
The production deployment phase puts all of the plans into action so that the Identity Manager solution is created in the live environment. Use the production rollout plan to put the different pieces of the Identity Manager solution into place. Depending on the complexity of the plan, this might be accomplished quickly or it might take some time to complete.

Technical Guidelines

3

The information that you gather in Designer allows you to make the technical decisions such as installation location and configuration options about each component of Identity Manager. For an introduction to each component, see the *Identity Manager 4.0 Overview Guide* guide. Figure 3-1 is one possible configuration of an Identity Manager solution.

Figure 3-1 Identity Manager Components



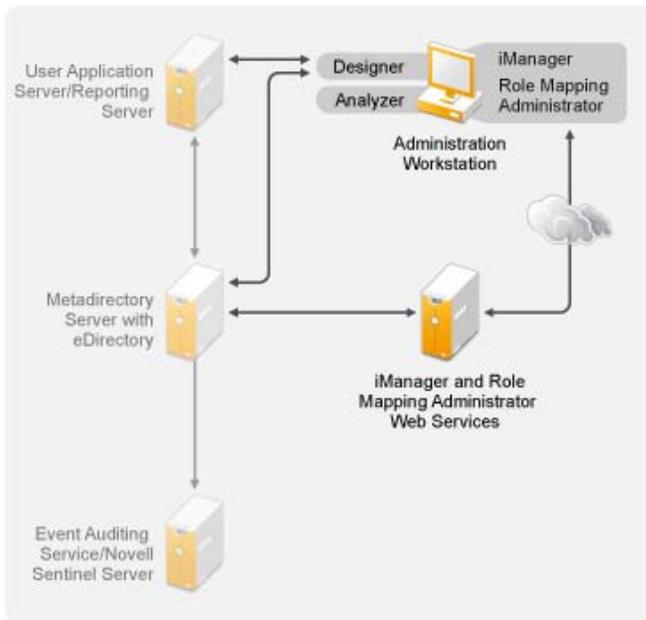
Identity Manager is very customizable. The following sections contain technical best practices guidelines to help set up and configure the Identity Manager solution that works best for your environment. Variables that affect how these guidelines apply to your environment include the type of hardware you have for your servers, how your WAN is configured, and how many objects are being synchronized.

- ◆ [Section 3.1, “Management Tools Guidelines,”](#) on page 28
- ◆ [Section 3.2, “Metadirectory Server Guidelines,”](#) on page 29
- ◆ [Section 3.3, “eDirectory Guidelines,”](#) on page 30
- ◆ [Section 3.4, “User Application,”](#) on page 35
- ◆ [Section 3.5, “Auditing and Reporting Guidelines,”](#) on page 36

3.1 Management Tools Guidelines

The two main management tools for the Identity Manager solution are Designer and iManager, as illustrated in [Figure 3-2](#). Designer is used during the planning and creation of the Identity Manager solution, and iManager is used for daily management tasks of the Identity Manager solution.

Figure 3-2 *Identity Manager Management Tools*



The User Application uses a Web-based administration page. For more information about the User Application, see “[Administering the User Application](#)” in the *Identity Manager Roles Based Provisioning Module 4.0 User Application: Administration Guide*.

- ♦ [Section 3.1.1, “Analyzer Guidelines,”](#) on page 28
- ♦ [Section 3.1.2, “Designer Guidelines,”](#) on page 29
- ♦ [Section 3.1.3, “iManager Guidelines,”](#) on page 29
- ♦ [Section 3.1.4, “Role Mapping Administrator Guidelines,”](#) on page 29

3.1.1 Analyzer Guidelines

Analyzer is a thick client that is installed on a workstation. Analyzer is used to examine and clean the data in the systems that you want to add to your Identity Manager solution. Using Analyzer during the planning phase helps you see what changes need to be made and how best to make those changes.

There are no major considerations for using Analyzer. For more information, see the [Analyzer 1.2 for Identity Manager Administration Guide](#).

3.1.2 Designer Guidelines

Designer is a thick client that is installed on a workstation. Designer is used to design, test, document, and then deploy your Identity Manager solution. Using Designer throughout the planning phase helps you capture information in one place. It also helps you see issues you might not be aware of as you look at all of the components of the solution together.

There are no major considerations for using Designer, unless you have multiple people working on the same project. Designer allows for version control of the project. For more information, see “[Version Control](#)” in the *Designer 4.0 for Identity Manager 4.0 Administration Guide*.

3.1.3 iManager Guidelines

iManager is a Web application that is the administration tool for Identity Manager. When you install Identity Manager, the installation expects that you already have an iManager server installed in your eDirectory tree.

If you have more than 10 administrators constantly working in iManager at one time, you should have a server that hosts only iManager. [Figure 3-2 on page 28](#) represents this configuration of your Identity Manager solution. If you have only one administrator, you can run iManager on your Metadirectory server without complications.

3.1.4 Role Mapping Administrator Guidelines

The Role Mapping Administrator is a Web application that discovers authorizations and permissions that can be granted within your major IT systems. It allows business analysts, not just IT administrators, to define and maintain which authorizations are associated with which business roles.

There are no major considerations for using the Role Mapping Administrator. You can run the Role Mapping Administrator on a separate server as show in [Figure 3-2 on page 28](#) or you can run it on the Metadirectory server. For more information, see the *Identity Manager Role Mapping Administrator 2.0 Installation and Configuration Guide*.

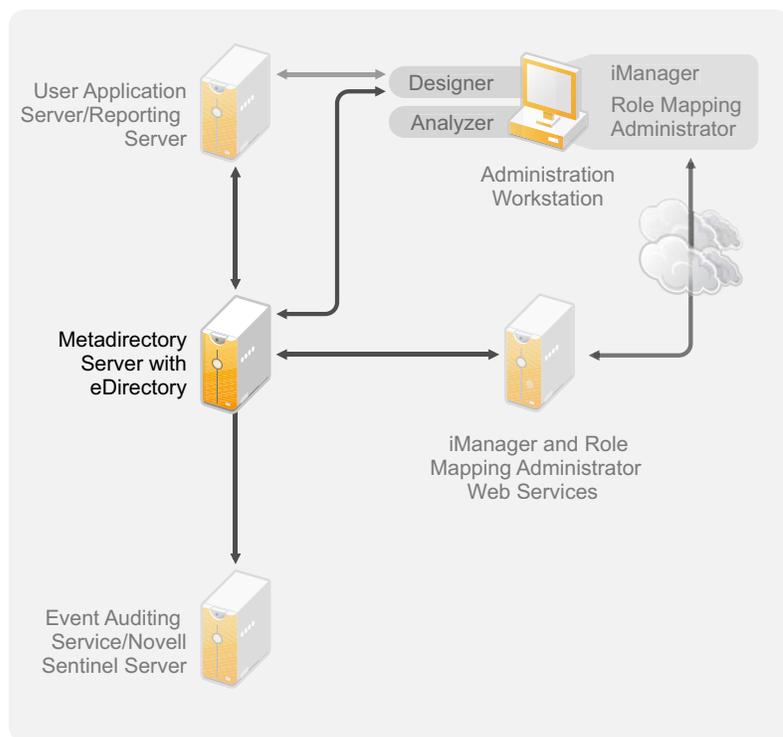
3.2 Metadirectory Server Guidelines

You can have one or more Metadirectory servers in your Identity Manager solution, depending on the server workload. The Metadirectory server requires that eDirectory be installed as shown in [Figure 3-3](#). You can add a Remote Loader server, not represented in the figure, to help with the workload or configuration of your environment.

Drivers must run on the same server as the connected application. For example, to configure the Active Directory driver, the server in [Figure 3-3](#) must be a member server or a domain controller. If you do not want to install eDirectory and Identity Manager on a member server or domain controller, then you can install the Remote Loader on a member server or a domain controller. The Remote Loader sends all of the events from Active Directory to the Metadirectory server. The Remote Loader receives any information from the Metadirectory server and passes that to the connected application.

The Remote Loader provides added flexibility for your Identity Manager solution. For more information, see the *Identity Manager 4.0 Remote Loader Guide*.

Figure 3-3 *Metadirectory Sever*



There are many variables that affect the performance of the server. The standard recommendation is that you have no more than ten drivers running on a Metadirectory server. However, if you are synchronizing millions of objects with each driver, you might not be able to run ten drivers on a server. On the other hand, if you are synchronizing 100 objects per driver, you can probably run more than ten drivers on one server.

Setting up the Identity Manager solution in a lab environment gives you the opportunity to test how the servers will perform. You can use the health monitoring tools in iManager to obtain a baseline and then be able to make the best decisions for your environment. For more information about the health monitoring tools, see “[Monitoring Driver Health](#)” in the *Identity Manager 4.0 Common Driver Administration Guide*.

For considerations for each driver, see the [Identity Manager Drivers documentation Web site \(http://www.novell.com/documentation/idm36drivers/index.html\)](http://www.novell.com/documentation/idm36drivers/index.html). Driver-specific information is provided in each driver guide.

3.3 eDirectory Guidelines

eDirectory is the Identity Vault that stores the objects that are synchronized through the Identity Manager solution. The follow sections contain guidelines that help you plan your deployment of eDirectory.

- ◆ [Section 3.3.1, “Identity Manager Objects in eDirectory,”](#) on page 31
- ◆ [Section 3.3.2, “Replicating the Objects that Identity Manager Needs on the Server,”](#) on page 31
- ◆ [Section 3.3.3, “Using Scope Filtering to Manage Users on Different Servers,”](#) on page 33

3.3.1 Identity Manager Objects in eDirectory

The following list indicates the major Identity Manager objects that are stored in eDirectory and how they relate to each other. No objects are created during the installation of Identity Manager. The Identity Manager objects are created during the configuration of the Identity Manager solution.

- ♦ **Driver Set:** A driver set is a container that holds Identity Manager drivers and library objects. Only one driver set can be active on a server at a time. However, more than one server might be associated to one driver set. Also, a driver can be associated with more than one server at a time. However, the driver should only be running on one server at a time. The driver should be in a disabled state on the other servers. Any server that is associated with a driver set must have the Metadirectory server installed on it.
- ♦ **Library:** The Library object is a repository of commonly used policies that can be referenced from multiple locations. The library is stored in the driver set. You can place a policy in the library so that every driver in the driver set can reference it.
- ♦ **Driver:** A driver provides the connection between an application and the Identity Vault. It also enables data synchronization and sharing between systems. The driver is stored in the driver set.
- ♦ **Job:** A job automates a recurring task. For example, a job can configure a system to disable an account on a specific day, or initiate a workflow to request an extension of a person's access to a corporate resource. The job is stored in the driver set.

3.3.2 Replicating the Objects that Identity Manager Needs on the Server

If your Identity Manager environment calls for multiple servers in order to run multiple Identity Manager drivers, your plan should make sure that certain eDirectory objects are replicated on servers where you want to run these Identity Manager drivers.

You can use filtered replicas, as long as all of the objects and attributes that the driver needs to read or synchronize are included in the filtered replica.

Keep in mind that you must give the Identity Manager Driver object sufficient eDirectory rights to any objects it is to synchronize, either by explicitly granting it rights or by making the Driver object security equivalent to an object that has the desired rights.

An eDirectory server that is running an Identity Manager driver (or that the driver refers to, if you are using the Remote Loader) must hold a master or read/write replica of the following:

- ♦ The Driver Set object for that server.

You should have one Driver Set object for each server that is running Identity Manager. Unless you have specific needs, don't associate more than one server with the same Driver Set object.

NOTE: When you create a Driver Set object, the default setting is to create a separate partition. Novell recommends creating a separate partition on the Driver Set object. For Identity Manager to function, the server is required to hold a full replica of the Driver Set object. If the server has a full replica of the location where the Driver Set object is installed, the partition is not required.

- ♦ The Server object for that server.

The Server object is necessary because it allows the driver to generate key pairs for objects. It is also important for Remote Loader authentication.

- ◆ The objects that you want this instance of the driver to synchronize.

The driver can't synchronize objects unless a replica of those objects is on the same server as the driver. In fact, an Identity Manager driver synchronizes the objects in *all* the containers that are replicated on the server unless you create rules for scope filtering to specify otherwise.

For example, if you want a driver to synchronize all user objects, the simplest way is to use one instance of the driver on a server that holds a master or read/write replica of all your users.

However, many environments don't have a single server that contains a replica of all the users. Instead, the complete set of users is spread across multiple servers. In this case, you have three choices:

- ◆ **Aggregate users onto a single server.** You can create a single server that holds all users by adding replicas to an existing server. Filtered replicas can be used to reduce the size of the eDirectory database if desired, as long as the necessary user objects and attributes are part of the filtered replica.
- ◆ **Use multiple instances of the driver on multiple servers, with scope filtering.** If you don't want to aggregate users onto a single server, you need to determine which set of servers holds all the users, and set up one instance of the Identity Manager driver on each of those servers.

To prevent separate instances of a driver from trying to synchronize the same users, you need to use scope filtering to define which users each instance of the driver should synchronize. Scope filtering means that you add rules to each driver to limit the scope of the driver's management to specific containers. See [“Using Scope Filtering to Manage Users on Different Servers” on page 33](#).

- ◆ **Use multiple instances of the driver on multiple servers, without scope filtering.** If you want to have multiple instances of a driver running on different servers without using filtered replicas, you need to define policies on the different driver instances that enable the driver to process different sets of objects within the same Identity Vault.
- ◆ The Template objects you want the driver to use when creating users, if you choose to use templates.

Identity Manager drivers do not require you to specify eDirectory Template objects for creating users. However, if you specify that a driver should use a template when creating users in eDirectory, the Template object must be replicated on the server where the driver is running.

- ◆ Any containers you want the Identity Manager driver to use for managing users.

For example, if you have created a container named Inactive Users to hold user accounts that have been disabled, you must have a master or read/write replica (preferably a master replica) of that container on the server where the driver is running.

- ◆ Any other objects that the driver needs to refer to (for example, work order objects for the Avaya PBX driver).

If the other objects are only to be read by the driver, not changed, the replica for those objects on the server can be a read-only replica.

3.3.3 Using Scope Filtering to Manage Users on Different Servers

Scope filtering means adding rules to each driver to limit the scope of the driver's actions to specific containers. The following are two situations in which you would need to use scope filtering:

- ◆ You want the driver to synchronize only users that are in a particular container.

By default, an Identity Manager driver synchronizes objects in all the containers that are replicated on the server where it is running. To narrow that scope, you must create scope filtering rules.

- ◆ You want an Identity Manager driver to synchronize all users, but you don't want all users to be replicated on the same server.

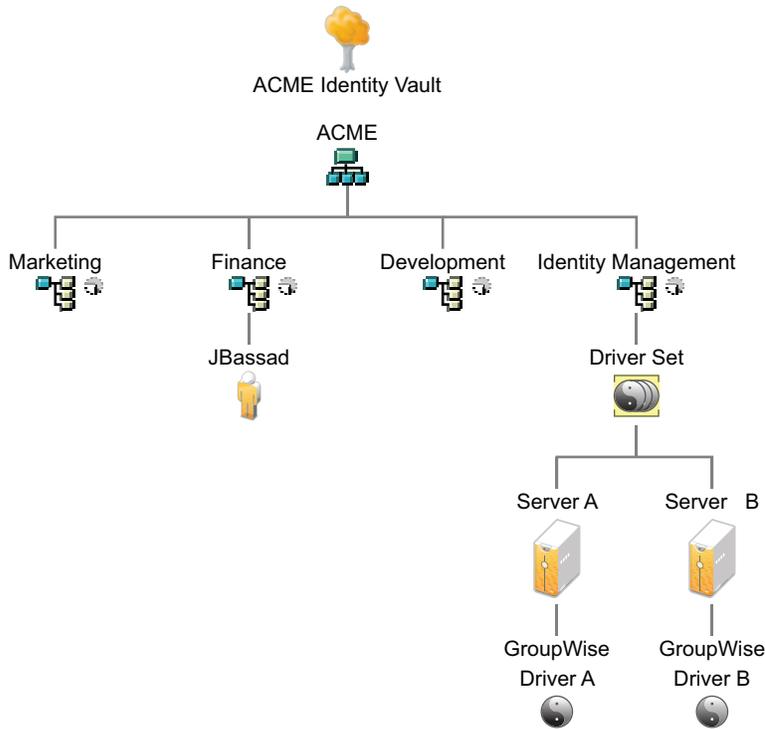
To synchronize all users without having them replicated on one single server, you need to determine which set of servers holds all the users, and then create an instance of the Identity Manager driver on each of those servers. To prevent two instances of the driver from trying to synchronize the same users, you need to use scope filtering to define which users each instance of the driver should synchronize.

NOTE: You should use scope filtering even if your server's replicas don't currently overlap. In the future, replicas could be added to your servers and an overlap could be created unintentionally. If you have scope filtering in place, your Identity Manager drivers do not try to synchronize the same users, even if replicas are added to your servers in the future.

Here's an example of how scope filtering is used:

The following illustration shows an Identity Vault with three containers that hold users: Marketing, Finance, and Development. It also shows an Identity Management container that holds the driver sets. Each of these containers is a separate partition.

Figure 3-4 Example Tree for Scope Filtering



In this example, the Identity Manager administrator has two Identity Vault servers, Server A and Server B, shown in [Figure 3-5 on page 35](#). Neither server contains a copy of all the users. Each server contains two of the three partitions, so the scope of what the servers hold is overlapping.

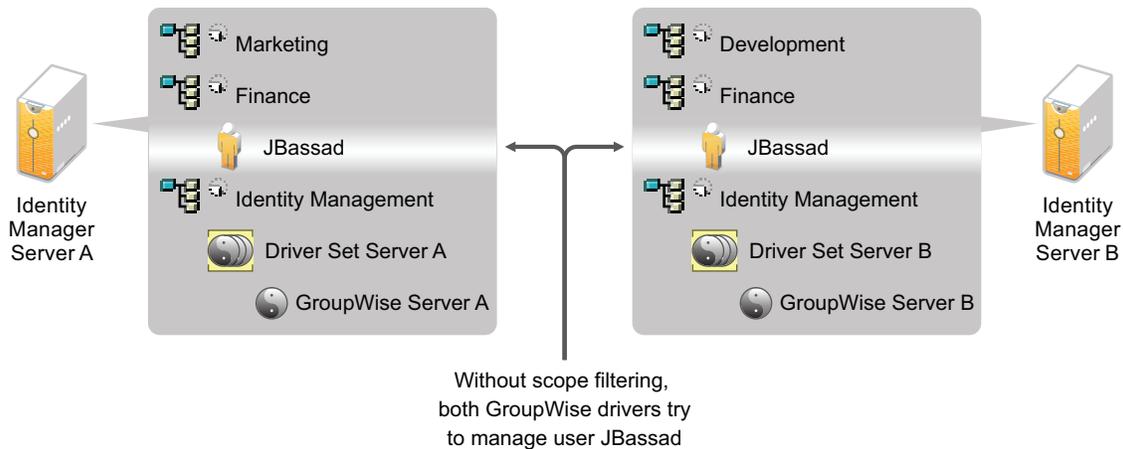
The administrator wants all the users in the tree to be synchronized by the GroupWise driver, but does not want to aggregate replicas of the users onto a single server. He chooses instead to use two instances of the GroupWise driver, one on each server. He installs Identity Manager and sets up the GroupWise driver on each Identity Manager server.

Server A holds replicas of the Marketing and Finance containers. Also on the server is a replica of the Identity Management container, which holds the driver set for Server A and the GroupWise Driver object for Server A.

Server B holds replicas of the Development and Finance containers, and the Identity Management container holding the driver set for Server B and the GroupWise Driver object for Server B.

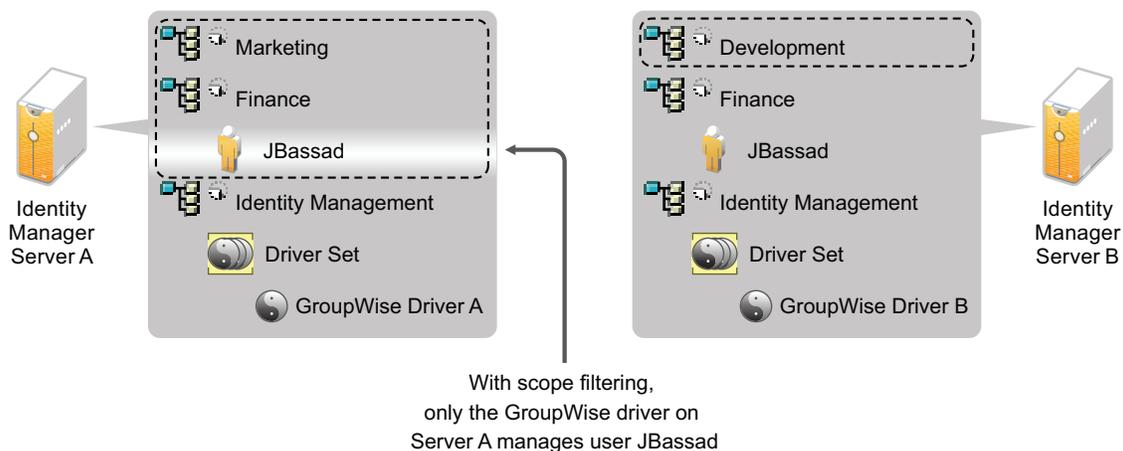
Because Server A and Server B both hold a replica of the Finance container, both servers hold the user JBassad, who is in the Finance container. Without scope filtering, both GroupWise Driver A and GroupWise Driver B would synchronize JBassad.

Figure 3-5 Two Servers with Overlapping Replicas, without Scope Filtering



The next illustration shows that scope filtering prevents both instances of the driver from managing the same user, because it defines which drivers synchronize each container.

Figure 3-6 Scope Filtering Defines Which Drivers Synchronize Each Container



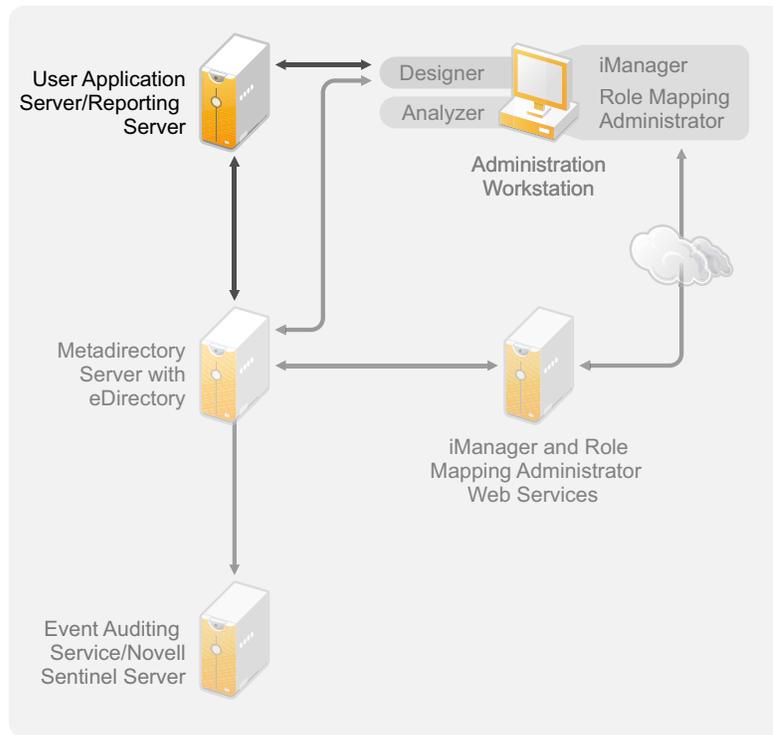
Identity Manager comes with predefined rules. There are two rules that help with scope filtering. “Event Transformation - Scope Filtering - Include Subtrees” and “Event Transformation - Scope Filtering - Exclude Subtrees” are documented in [Understanding Policies for Identity Manager 4.0](#).

For this example, you would use the Include Subtrees predefined rule for Server A and Server B. You would define the scope for each driver differently so that they would only synchronize the users in the specified containers. Server A would synchronize Marketing and Finance. Server B would synchronize Development.

3.4 User Application

The User Application should run on its own server, as shown in [Figure 3-7](#). You might need more than one User Application server.

Figure 3-7 *User Application*

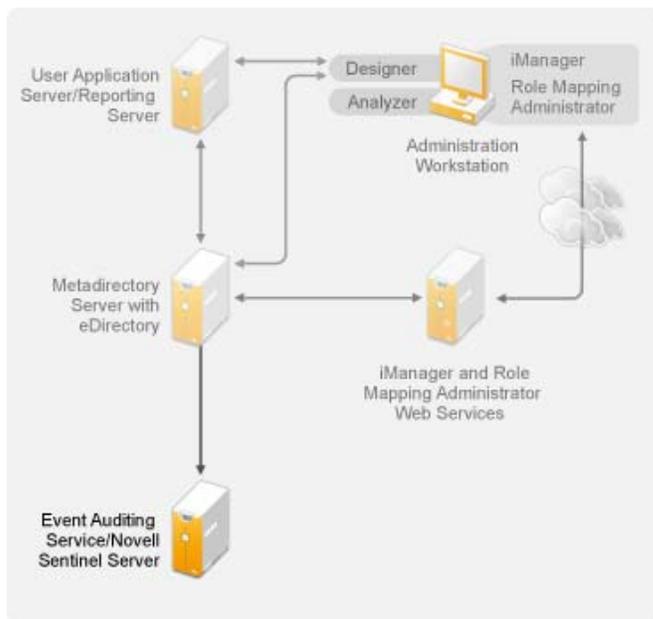


Use the information in the “Performance Tuning” (<http://www.novell.com/documentation/idmrpbm40/agpro/data/b2gx735.html>) section of the *User Application Administration Guide* to determine how best to configure the User Application server.

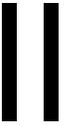
3.5 Auditing and Reporting Guidelines

If you need auditing and reporting as part of the Identity Manager solution, you need to implement Identity Audit or Novell Sentinel. You should run either the Event Auditing Service or Sentinel on its own server, as shown in Figure 3-8. The number of servers that are required for your solution depends on how many drivers you have in your environment and how many events you have defined to audit.

Figure 3-8 Sentinel



Installation



The following sections contain the information required to install an Identity Manager system without using the integrated installer. For simple installation and configuration you should use the new integrated installer instead of installing the components separately. For more information about the integrated installer, see the *Identity Manager 4.0 Integrated Installation Guide*.

However, if you need to install one or more of the Identity Manager components separately, use the information in these sections to complete those installations.

- ♦ [Chapter 4, “Basic Identity Manager System Checklist,” on page 41](#)
- ♦ [Chapter 5, “Where to Get Identity Manager,” on page 45](#)
- ♦ [Chapter 6, “System Requirements,” on page 47](#)
- ♦ [Chapter 7, “Installing Identity Manager,” on page 59](#)
- ♦ [Chapter 8, “Activating Novell Identity Manager Products,” on page 73](#)
- ♦ [Chapter 9, “Troubleshooting Identity Manager,” on page 77](#)

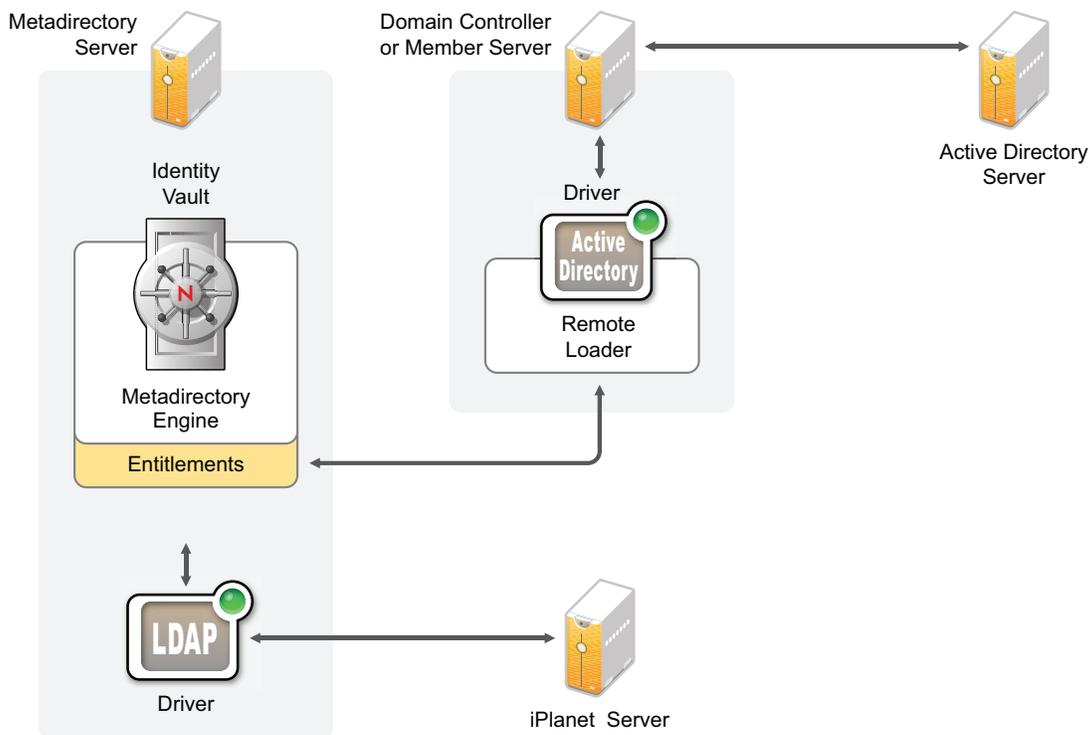
Basic Identity Manager System Checklist

4

There are many different ways to configure Identity Manager to take advantage of all of its features. [Figure 4-1](#) represents a basic configuration of Identity Manager. This configuration provisions users by synchronizing data. No matter how Identity Manager is configured, you always start with a basic system.

As you configure your Identity Manager system, use this checklist to make sure all steps are completed.

Figure 4-1 Basic Identity Manager System



- ◆ [Section 4.1, “Prerequisites,”](#) on page 42
- ◆ [Section 4.2, “Planning,”](#) on page 42
- ◆ [Section 4.3, “Installation,”](#) on page 42
- ◆ [Section 4.4, “Driver Configuration with the Remote Loader,”](#) on page 43
- ◆ [Section 4.5, “Driver Configuration without the Remote Loader,”](#) on page 43
- ◆ [Section 4.6, “Additional Configuration,”](#) on page 43

4.1 Prerequisites

- ❑ Verify that your system meets the system requirements listed in [Chapter 6, “System Requirements,”](#) on page 47.

4.2 Planning

Planning is the key to having a successful implementation and deployment of Identity Manager.

- ❑ Create a development environment. It is important to have access to an Identity Manager system to validate your Identity Manager solution. You want to do all testing and development in the development environment before changing the production environment. For more information, see [Chapter 1, “Setting Up a Development Environment,”](#) on page 13.
- ❑ Create a project plan for deploying Identity Manager. The project plan includes defining your key business processes, creating an Identity Manager solution that automates those processes, and creating a technical implementation plan. To have a successful deployment of Identity Manager, you must have a project plan. For more information, see [Chapter 2, “Creating a Project Plan,”](#) on page 15.
- ❑ After you have created a project plan, use Analyzer to clean and prepare your data for synchronization. For more information, see the [Analyzer 1.2 for Identity Manager Administration Guide](#).

4.3 Installation

- ❑ Install Analyzer. For more information, see [Section 7.1, “Installing Analyzer,”](#) on page 59.
- ❑ Install Designer. For more information, see [Section 7.2, “Installing Designer,”](#) on page 60.
- ❑ Install eDirectory. For more information, see [Section 7.3, “Installing eDirectory,”](#) on page 60.
- ❑ Install iManager. For more information, see [Section 7.4, “Installing iManager,”](#) on page 61.
- ❑ Install the Metadirectory server and drivers. For more information, see [Chapter 7, “Installing Identity Manager,”](#) on page 59.
- ❑ Activate Identity Manager. For more information, see [Chapter 8, “Activating Novell Identity Manager Products,”](#) on page 73.
- ❑ (Optional) Design and create entitlements for your Identity Manager system.

Entitlements are a set of defined criteria for a person or group that can be applied to multiple drivers. After the criteria are met, the entitlements initiate an event to grant or revoke access to business resources. Entitlements add an additional level of control and automation for granting and revoking resources.

The key benefit of entitlements is to create and define business logic, and then apply that logic to multiple drivers. If you need to make a change, you change it in the entitlement instead of in each driver.

Entitlements are implemented through three agents:

- ◆ Role-Based Entitlements using the Entitlements service driver
- ◆ Workflow
- ◆ Roles Based Provisioning Module

For more information about entitlements, see the [Identity Manager 4.0 Entitlements Guide](#).

4.4 Driver Configuration with the Remote Loader

The Remote Loader allows you to synchronize information to a connected system without having eDirectory installed on the connected system. The Remote Loader synchronizes the information to the Metadirectory server, which stores the data in the Identity Vault. Identity Manager uses eDirectory as the Identity Vault.

- Install the Remote Loader on a machine that communicates with the connected system. The Remote Loader communicates between the connected system and the Metadirectory server, and makes it possible for Identity Manager to communicate with a machine that does not have eDirectory installed. For more information, see “[Installing the Remote Loader](#)” in the *Identity Manager 4.0 Remote Loader Guide*.
- Configure the Remote Loader for a driver. You define a specific instance of the Remote Loader to communicate with a specific driver. For more information, see “[Configuring the Remote Loader](#)” in the *Identity Manager 4.0 Remote Loader Guide*.
- Configure the driver to communicate with the Remote Loader. There is a driver guide for each driver. For specific information about your driver, see the [Identity Manager 4.0 Drivers Documentation Web site \(http://www.novell.com/documentation/idm40drivers/\)](http://www.novell.com/documentation/idm40drivers/).
- (Optional) Enable entitlements on the driver. Verify that you have the correct policies in place to execute the entitlement. For more information, see the *Identity Manager 4.0 Entitlements Guide*.
- Repeat these steps for each driver you have in your environment.

4.5 Driver Configuration without the Remote Loader

- Create and configure your driver. There is a driver guide for each driver. For specific information about your driver, see the [Identity Manager 4.0 Drivers Documentation Web site \(http://www.novell.com/documentation/idm40drivers/\)](http://www.novell.com/documentation/idm40drivers/).
- (Optional) Enable entitlements on the driver. Verify that you have the correct policies in place to execute the entitlement. For more information, see the *Identity Manager 4.0 Entitlements Guide*.
- Repeat these steps for each driver you have in your environment.

4.6 Additional Configuration

With the basic Identity Manager system installed and configured, you can add the following features:

- Password Management:** If you want to manage passwords with Identity Manager, you need to do some additional configuration. Use the “[Password Management Checklist](#)” in the *Identity Manager 4.0 Password Management Guide* to verify that all configuration steps are completed.
- Roles Management:** If you want to manage roles across different systems from one location, Identity Manager contains a tool called the Roles Mapping Administrator. It allows you to map business roles from one system to another without understanding the IT infrastructure. For more information, see the *Identity Manager Role Mapping Administrator 2.0 Installation and Configuration Guide*.

- ❑ **Roles Based Provisioning:** If you want to add Roles Based Provisioning to your Identity Manager solution, use the “[Installation Checklist](#)” in the *Identity Manager Roles Based Provisioning Module 4.0 User Application: Installation Guide* to verify that all configuration steps are completed.
- ❑ **Auditing and Reporting:** Adding auditing and reporting to your Identity Manager solution provides a means to show that your business policies comply with the company’s policies. You can add the Identity Reporting Module or Novell Sentinel to your Identity Manager solution for auditing and reporting. For more information about the Identity Reporting Module, see the *Identity Reporting Module Guide*. For more information about Novell Sentinel, see the *Identity Manager 4.0 Reporting Guide for Novell Sentinel*.

Where to Get Identity Manager

5

You can download an evaluation copy of Identity Manager and use it for 90 days free of charge. However, the Identity Manager components 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 purchase a product license and activate Identity Manager. For more information, see [Chapter 8, “Activating Novell Identity Manager Products,”](#) on page 73.

To download Identity Manager and its services:

- 1 Go to the [Novell Downloads Web site \(http://download.novell.com\)](http://download.novell.com).
- 2 In the *Product or Technology* menu, select *Novell Identity Manager*, then click *Search*.
- 3 On the Novell Identity Manager Downloads page, click the *Download* button next to a file you want. [Table 5-1](#) contains a description of each file.
Based on your requirements, you can select an appropriate ISO image. Each ISO contains the 32-bit and 64-bit versions of the product.
- 4 Follow the on-screen prompts to download the file to a directory on your computer.
- 5 Repeat [Step 3](#) until you have downloaded all of the files you need.
- 6 Either mount the downloaded `.iso` file as a volume, or use the `.iso` file to create a DVD of the software. If you haven't already verified that the media you burned is valid, you can check it by using the *Media Check* option.

Table 5-1 Identity Manager ISO Images

ISO	Platform	Description
windows_identity_manager_enterprise_4.0.iso	Windows	Contains the DVD image for the Metadirectory server, Designer, iManager, Role Mapping Administrator, Analyzer, Identity Reporting Module, and Roles Based Provisioning Module.
linux_identity_manager_enterprise_4.0.iso	Linux	Contains the DVD image for the Metadirectory server, Designer, iManager, Role Mapping Administrator, Analyzer, Identity Reporting Module, and Roles Based Provisioning Module.
solaris_identity_manager_enterprise_4.0.iso	Solaris	Contains the DVD image for the Metadirectory server. Other components are not supported on the Solaris platform.

Your Identity Manager purchase includes activations for service drivers and several common drivers.

- ♦ **Service Drivers:** The following is a list of service drivers that are activated when you activate the Metadirectory server:
 - ♦ Data Collection Service
 - ♦ Entitlements Services
 - ♦ ID Provider

- ◆ Loopback Service
- ◆ Managed System Gateway
- ◆ Manual Task Service
- ◆ Null Service
- ◆ Role and Resource Service
- ◆ User Application
- ◆ WorkOrder
- ◆ **Common Drivers:** The following is a list of common drivers that are activated when you activate the Metadirectory server:
 - ◆ Active Directory
 - ◆ ADAM
 - ◆ eDirectory
 - ◆ GroupWise
 - ◆ LDAP
 - ◆ Lotus Notes

Activations for all other Identity Manager drivers must be purchased separately. The activations for the drivers are sold as Identity Manager Integration modules. An Identity Manager Integration module can contain one or more drivers. You receive a Product Activation Credential for each Identity Manager Integration module you purchase. For more information see, the [Identity Manager Drivers product Web page](http://www.novell.com/products/identitymanager/drivers/) (<http://www.novell.com/products/identitymanager/drivers/>).

The User Application Roles Based Provisioning Module is included with your Identity Manager purchase. It adds a powerful roles based approval workflow to managing your users' identities.

Your Identity Manager purchase also includes the several tools to help design, create, and manage your Identity Manager solution:

- ◆ Analyzer
- ◆ Designer
- ◆ iManager
- ◆ Role Mapping Administrator

The Identity Reporting Module is another component of Identity Manager that allows you to audit and create reports about your Identity Manager solution. You can use the reports to help meet compliance regulations for your business.

For more information about the Identity Manager components, see the [Identity Manager 4.0 Overview Guide](#).

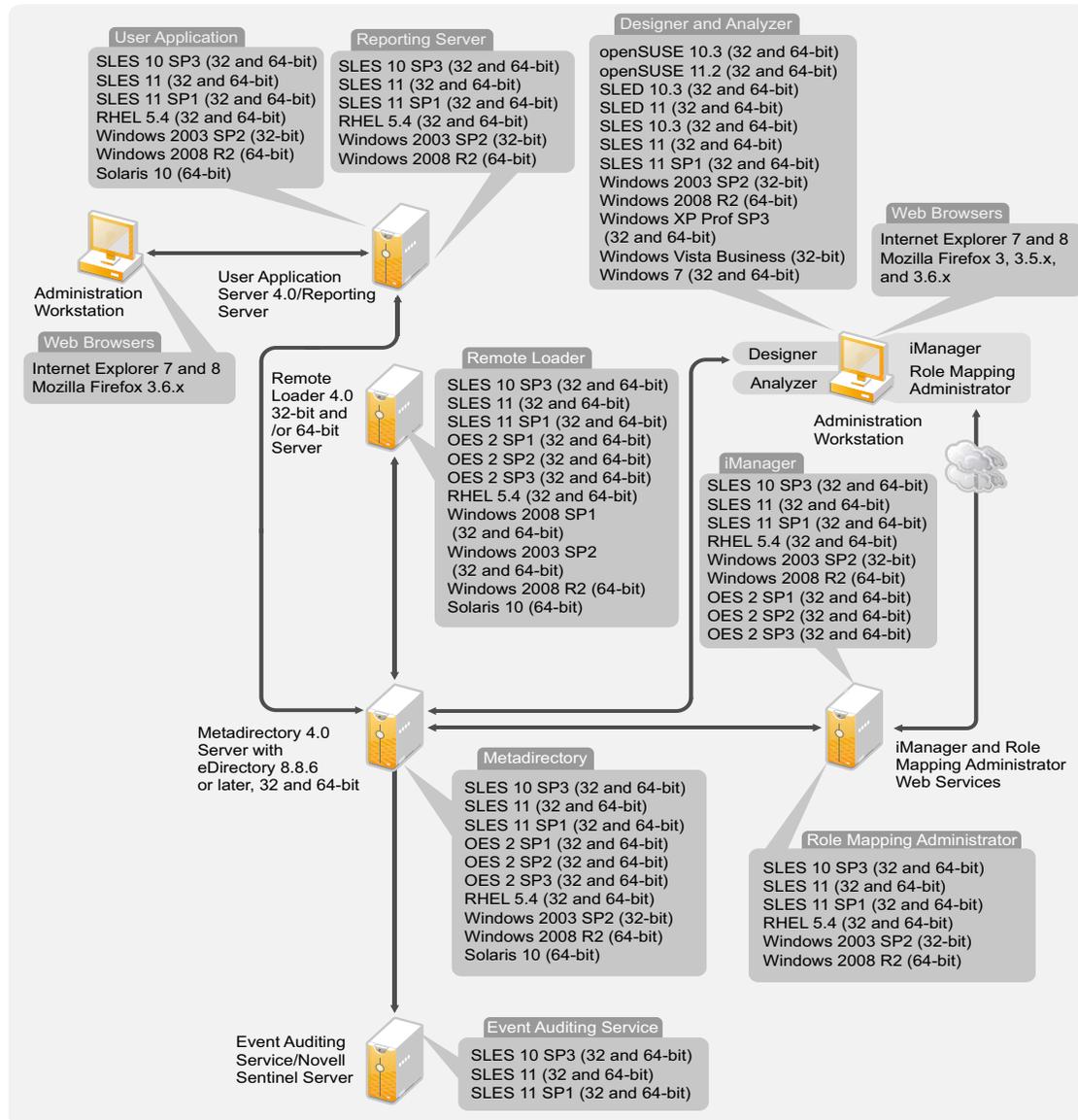
System Requirements

6

The components of Novell Identity Manager can be installed on multiple systems and platforms.

Figure 6-1 shows which platforms and systems are supported.

Figure 6-1 System Requirements for the Identity Manager Components



Depending on your system configuration, you might need to run the Identity Manager installation program several times to install Identity Manager components on the appropriate systems.

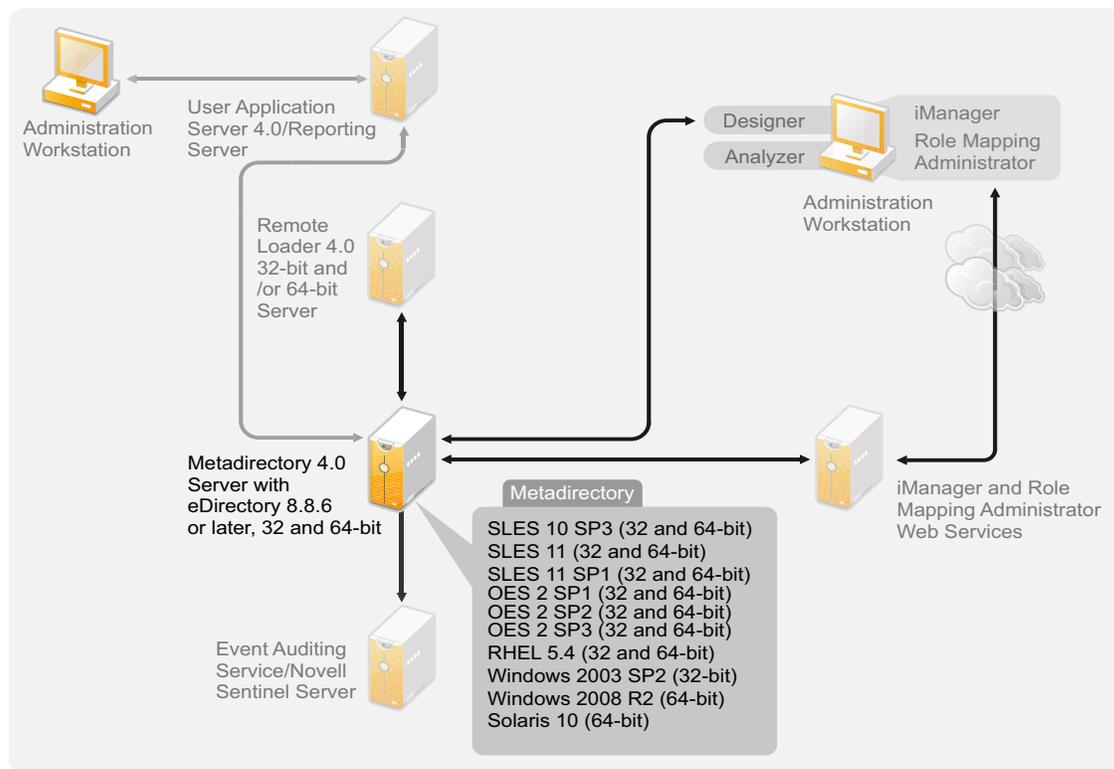
- ◆ [Section 6.1, “eDirectory and iManager,”](#) on page 48
- ◆ [Section 6.2, “Metadirectory Server,”](#) on page 49

- ◆ Section 6.3, “Remote Loader,” on page 51
- ◆ Section 6.4, “User Application,” on page 53
- ◆ Section 6.5, “Auditing and Reporting,” on page 54
- ◆ Section 6.6, “Workstations,” on page 54
- ◆ Section 6.7, “Resource Requirements,” on page 57

6.1 eDirectory and iManager

Identity Manager requires eDirectory and iManager to be installed. These products provide a base for Identity Manager, and they are included in the Identity Manager Advanced Edition ISO image. Figure 6-2 illustrates these components.

Figure 6-2 Base Products for Identity Manager



You need the following versions of these products:

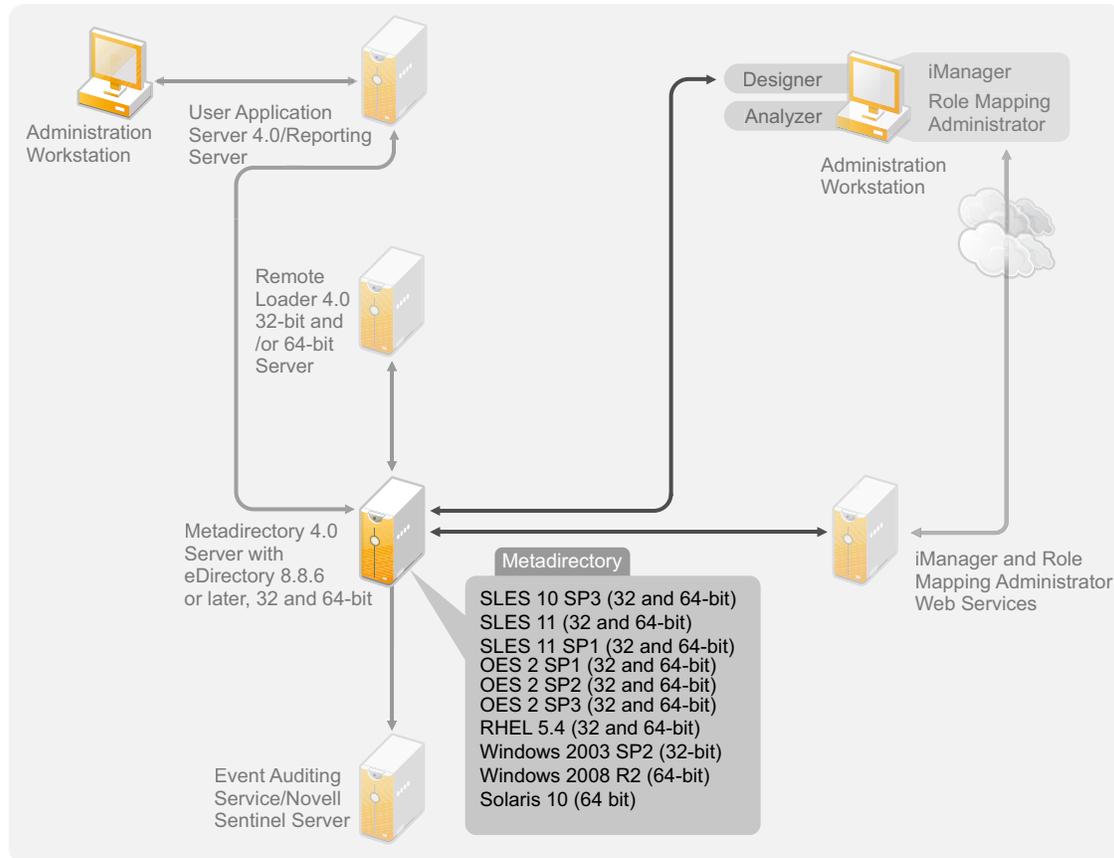
- ◆ eDirectory 8.8.6 or later (32-bit or 64-bit)
- ◆ iManager 2.7.4

For eDirectory system requirements, see the *Novell eDirectory 8.8 Installation Guide* (<http://www.novell.com/documentation/edir88/index.html>). For system requirements for iManager, see *Installing iManager* (http://www.novell.com/documentation/imanager27/imanager_install_274/data/alw39eb.html) section in the *iManager 2.7 Installation Guide* (<http://www.novell.com/documentation/imanager27/index.html>).

6.2 Metadirectory Server

The Metadirectory server processes the events from the drivers, whether they are configured using the Remote Loader or not. For a list of the supported operating systems, see [Figure 6-3](#).

Figure 6-3 Supported Operating Systems for the Metadirectory Server



During the installation of the Metadirectory server, the installation program detects what version of eDirectory is installed.

NOTE: You must have eDirectory 8.8.6 or later (32-bit or 64-bit) installed, or the installation program does not continue.

- ♦ [Section 6.2.1, “Supported Processors,”](#) on page 49
- ♦ [Section 6.2.2, “Server Operating Systems,”](#) on page 50

6.2.1 Supported Processors

The processors listed here are used during the testing of Identity Manager. The SPARC processor is used for Solaris testing.

The supported 32-bit processors for Linux (Red Hat and SUSE Linux Enterprise Server) and Windows operating systems are:

- ◆ Intel x86-32
- ◆ AMD x86-32

The supported 64-bit processors for Linux (Red Hat and SUES Linux Enterprise Server) and Windows operating systems are:

- ◆ Intel EM64T
- ◆ AMD Athlon64
- ◆ AMD Opteron

All operating systems should have the latest support packs.

6.2.2 Server Operating Systems

You can install the Metadirectory server as a 32-bit application on a 64-bit operating system. [Table 6-1](#) contains a list of the supported server operating systems that the Metadirectory server can run on.

Table 6-1 *Supported Server Operating Systems*

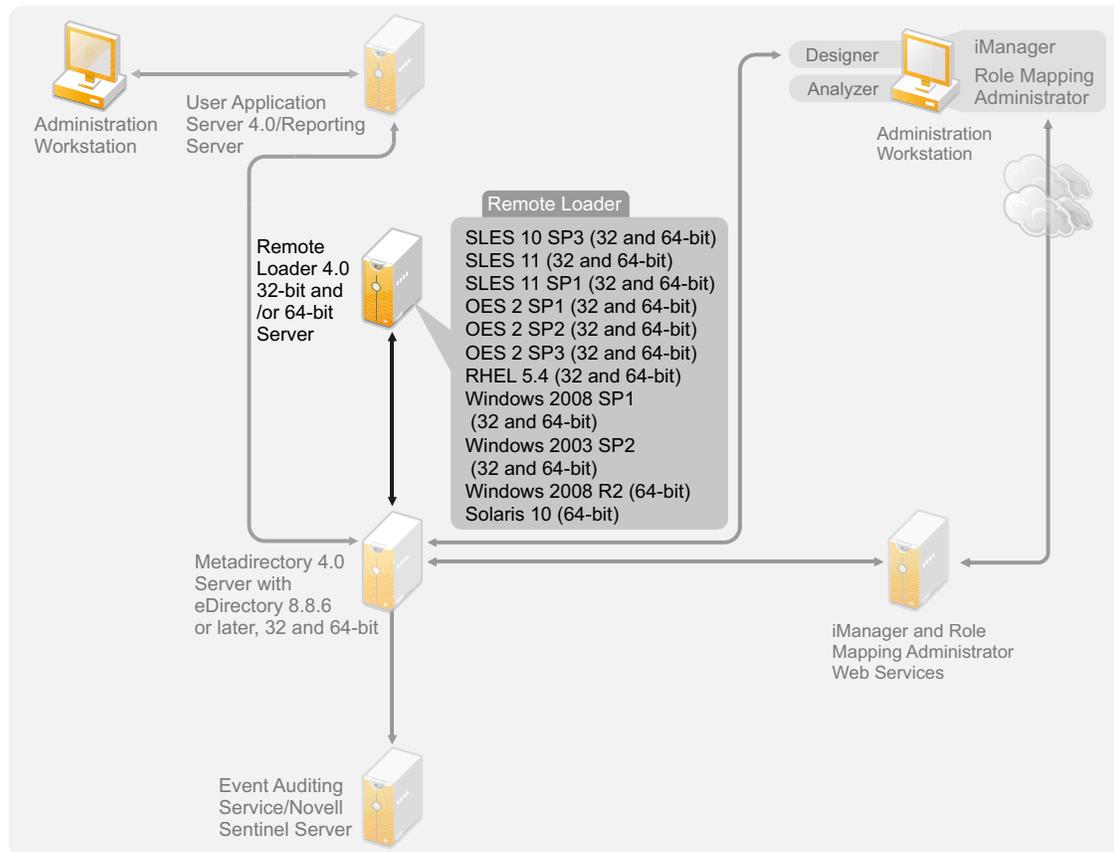
Server Operating System Version	Notes
Windows Server 2003 SP2 or later (32-bit)	The Metadirectory server runs only in 32-bit mode.
Windows Server 2008 R2 (64-bit)	The Metadirectory server runs only in 64-bit mode.
Red Hat 5.4 (32-bit and 64-bit)	The Metadirectory server runs in either 32-bit or 64-bit mode. Novell recommends that you apply the latest OS patches via the manufacturer's automated update facility before you install Identity Manager.
SUSE Linux Enterprise Server 10 SP3 or later support packs (32-bit and 64-bit)	The Metadirectory server runs in either 32-bit or 64-bit mode. Novell recommends that you apply the latest OS patches via the manufacturer's automated update facility before you install Identity Manager.
SUSE Linux Enterprise Server 11 (32-bit and 64-bit)	The Metadirectory server runs in either 32-bit or 64-bit mode. Novell recommends that you apply the latest OS patches via the manufacturer's automated update facility before you install Identity Manager.
SUSE Linux Enterprise Server 11 SP1 (32-bit and 64-bit)	The Metadirectory server runs in either 32-bit or 64-bit mode. Novell recommends that you apply the latest OS patches via the manufacturer's automated update facility before you install Identity Manager.

Server Operating System Version	Notes
OES 2 SP1 (32-bit and 64-bit)	The Metadirectory server runs in 32-bit and 64-bit mode.
OES 2 SP2 (32-bit and 64-bit)	The Metadirectory server runs in 32-bit and 64-bit mode.
OES 2 SP3 (32-bit and 64-bit)	The Metadirectory server runs in 32-bit and 64-bit mode.
Solaris 10 (64-bit)	The Metadirectory server runs only in 64-bit mode.
Xen	Xen is supported when the Xen Virtual Machine is running SLES 10/SLES 11 as the guest operating system in paravirtualized mode.
VMware ESX	The Metadirectory server runs in either 32-bit or 64-bit mode.
Red Hat Enterprise Linux 5 Virtualization	The Metadirectory server runs in either 32-bit or 64-bit mode.
Windows Server 2008 R2 Virtualization with Hyper-V	The Metadirectory server runs in either 32-bit or 64-bit mode.

6.3 Remote Loader

The Remote Loader gives you flexibility in your Identity Manager solution configuration. It provides both 32-bit and 64-bit support. By default, the installation program detects the version of the operating system and then installs the corresponding version of the Remote Loader.

Figure 6-4 Supported Operating Systems for the Remote Loader



If you have installed the Metadirectory server as a 32-bit application on a 64-bit operating system, you can install both a 32-bit and a 64-bit Remote Loader on the same machine.

Table 6-2 lists the supported operating systems for the Remote Loader.

Table 6-2 Supported Operating Systems for the Remote Loader

Server Operating System Version	Notes
Windows Server 2003 SP2 (32-bit and 64-bit)	The Remote Loader runs in 32-bit and 64-bit mode.
Windows Server 2008 SP1 (32-bit and 64-bit)	The Remote Loader runs in 32-bit and 64-bit mode.
Windows Server 2008 Server R2 (64-bit)	The Remote Loader runs only in 64-bit mode.
Red Hat 5.4 (32-bit and 64-bit)	The Remote Loader runs in 32-bit and 64-bit mode. Novell recommends that you apply the latest OS patches via the manufacturer's automated update facility before you install Identity Manager.

Server Operating System Version	Notes
SUSE Linux Enterprise Server 10 SP3 (32-bit and 64-bit)	The Remote Loader runs in 32-bit and 64-bit mode. Novell recommends that you apply the latest OS patches via the manufacturer's automated update facility before you install Identity Manager.
SUSE Linux Enterprise Server 11 (32-bit and 64-bit)	The Remote Loader runs in 32-bit and 64-bit mode. Novell recommends that you apply the latest OS patches via the manufacturer's automated update facility before you install Identity Manager.
SUSE Linux Enterprise Server 11 SP1 (32-bit and 64-bit)	The Remote Loader runs in 32-bit and 64-bit mode. Novell recommends that you apply the latest OS patches via the manufacturer's automated update facility before you install Identity Manager.
OES 2 SP1 (32-bit and 64-bit)	The Remote Loader runs in 32-bit and 64-bit mode.
OES 2 SP2 (32-bit and 64-bit)	The Remote Loader runs in 32-bit and 64-bit mode.
OES 2 SP3 (32-bit and 64-bit)	The Remote Loader runs in 32-bit and 64-bit mode.
Solaris 10 (64-bit)	The Remote Loader runs only in 64-bit mode.
Xen	Xen is supported when the Xen Virtual Machine is running SLES 10/SLES 11 as the guest operating system in paravirtualized mode.
VMware ESX (64-bit)	The Remote Loader runs in 32-bit and 64-bit mode.
Red Hat Enterprise Linux 5 Virtualization (64-bit)	The Remote Loader runs in 32-bit and 64-bit mode.
Windows Server 2008 R2 Virtualization with Hyper-V (64-bit)	The Remote Loader runs in 32-bit and 64-bit mode.

Java Remote Loader is supported on platforms where native Remote Loader is not available. .NET Remote Loader is supported on .NET platform version 2.

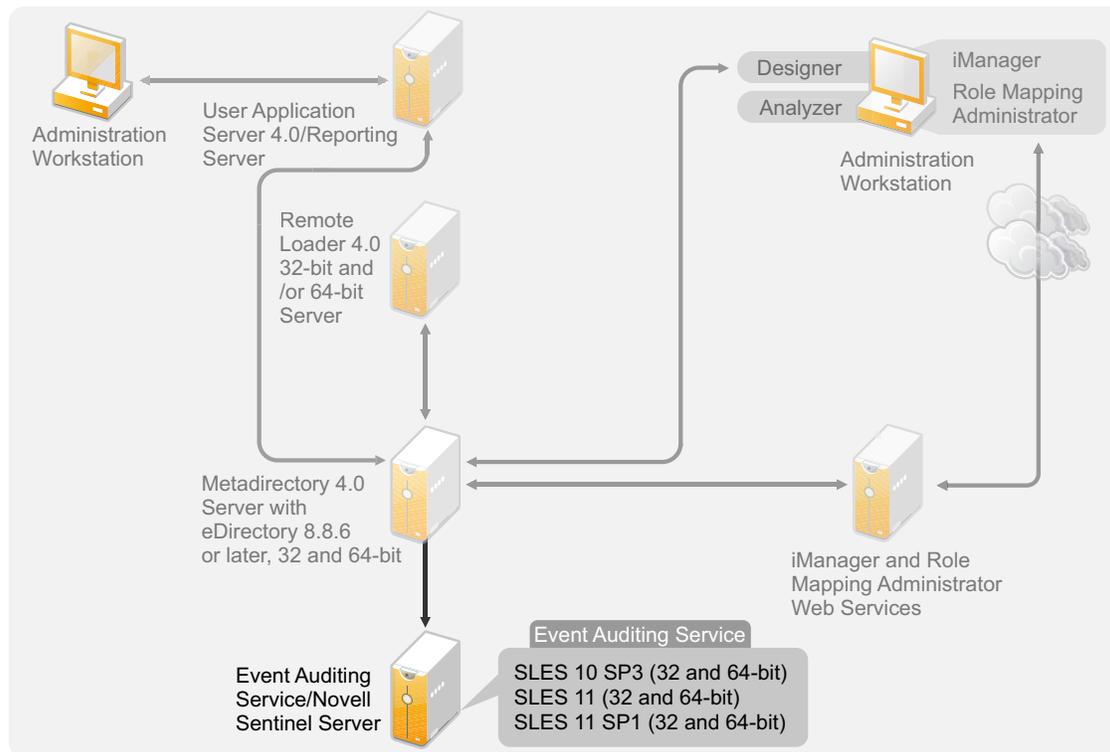
6.4 User Application

For User Application system requirements, see the “[System Requirements](#)” section in the *Identity Manager Roles Based Provisioning Module 4.0 User Application: Installation Guide*. The Roles Based Provisioning Module 4.0 uses JBoss 5.1 as the application server and PostgreSQL 8.4.3 as the database.

6.5 Auditing and Reporting

The Identity Reporting Module and Novell Sentinel are two different tools used to gather auditing and reporting information about Identity Manager. Figure 6-5 lists the supported version of Sentinel with Identity Manager 4.0.

Figure 6-5 Sentinel



The Identity Reporting Module is a component of the Identity Manager Advanced Edition. Novell Sentinel is an optional component you can add to your Identity Manager system, but Sentinel does not come with Identity Manager.

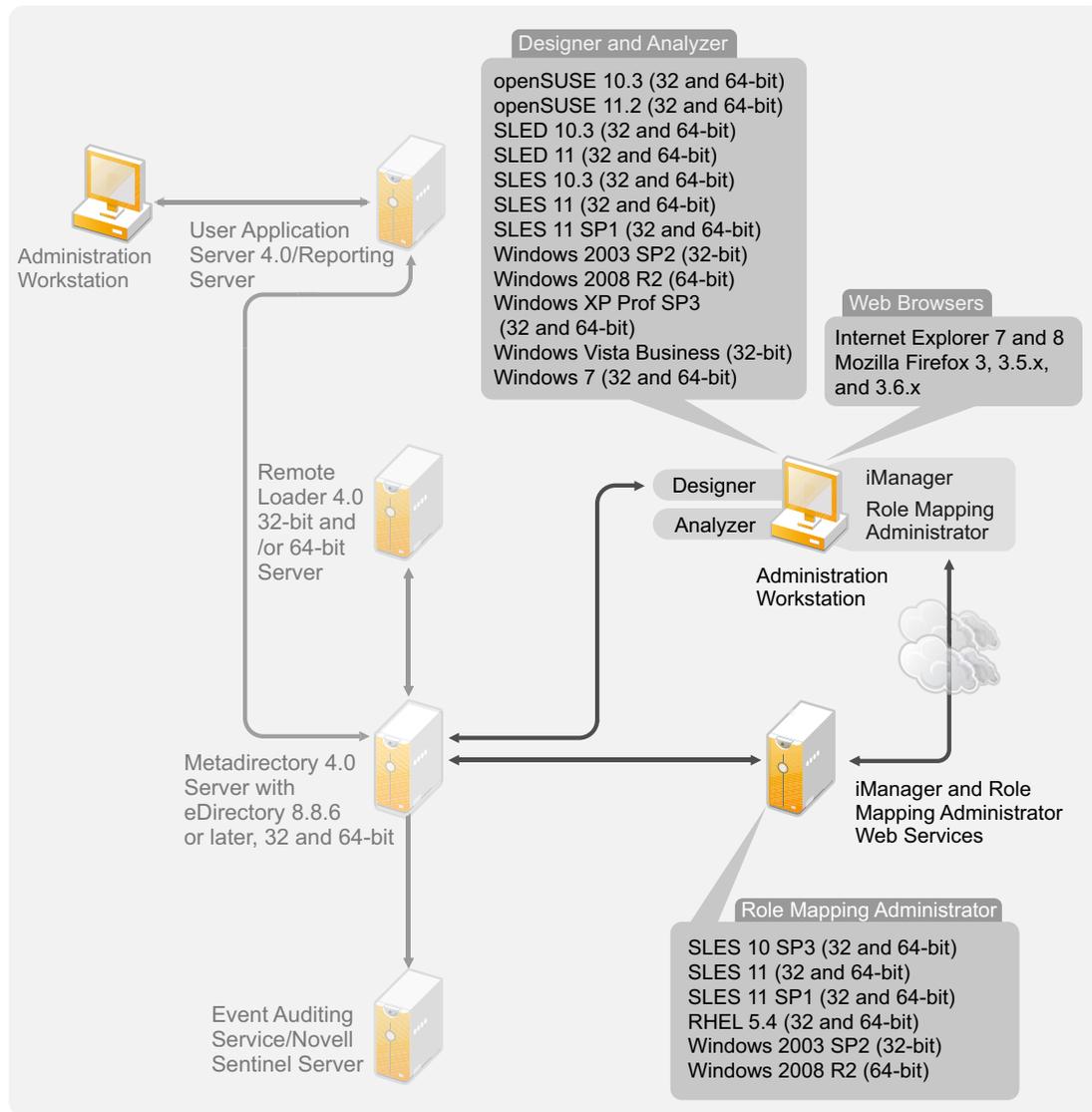
By adding auditing and reporting, you can meet compliance standards that many companies must abide by. You can create audit trails for any events you need to track, and you can generate reports to meet audit standards for your company.

For system requirements and configuration information about the Identity Reporting Module, see the “[System Requirements](#)” section the *Identity Reporting Module Guide*. For configuration information about Sentinel with Identity Manager, see the *Identity Manager 4.0 Reporting Guide for Novell Sentinel*. For system requirement information about Novell Sentinel, see the “Supported Platforms and Best Practices” chapter in the *Novell Sentinel Installation Guide* (<http://www.novell.com/documentation/sentinel6/index.html>).

6.6 Workstations

Workstations are used to access Designer, iManager, the Role Mapping Administrator, or the User Application administration Web page. Figure 6-6 lists the different components for workstations that are supported with Identity Manager 4.0.

Figure 6-6 Supported Components for Workstations



There are three different items that affect workstations:

- ♦ [Section 6.6.1, “Workstation Platforms,” on page 55](#)
- ♦ [Section 6.6.2, “Web Browsers,” on page 56](#)

6.6.1 Workstation Platforms

[Table 6-3](#) contains a list of the supported workstation platforms for Designer and iManager.

For system requirements information, refer to the individual component documentation.

- ♦ iManager: See the [Installing iManager \(http://www.novell.com/documentation/imanager27/imanager_install_274/data/alw39eb.html\)](http://www.novell.com/documentation/imanager27/imanager_install_274/data/alw39eb.html) section in the *Novell iManager 2.7 Installation Guide*.
- ♦ Designer: See the “System Requirements” section in the *Designer 4.0 for Identity Manager 4.0 Administration Guide*.

Table 6-3 Supported Workstation Platforms

Platforms	Details
Windows 7 (32 and 64-bit)	Both 32 and 64-bit versions are supported.
Windows Vista (32-bit)	Only the 32-bit version is supported.
Windows XP Professional SP3 (32 and 64-bit)	Both 32 and 64-bit versions are supported.
Windows 2003 SP2 (32-bit)	Only the 32-bit version is supported.
Windows 2008 R2 (64-bit)	Only the 64-bit Business Edition is supported.
openSUSE 10.3 (32 and 64-bit)	Apply the latest patches via the automated update facility.
openSUSE 11.2 (32 and 64-bit)	Apply the latest patches via the automated update facility.
SUSE Linux Enterprise Desktop 10 SP3 (32 and 64-bit)	Apply the latest patches via the automated update facility.
SUSE Linux Enterprise Desktop 11 (32 and 64-bit)	Apply the latest patches via the automated update facility.
SUSE Linux Enterprise Server 10 SP3 (32 and 64-bit)	Apply the latest patches via the automated update facility.
SUSE Linux Enterprise Server 11 (32 and 64-bit)	Apply the latest patches via the automated update facility.
SUSE Linux Enterprise Server 11 SP1 (32 and 64-bit)	Apply the latest patches via the automated update facility.

6.6.2 Web Browsers

iManager runs all of the plug-ins required to administer Identity Manager. The Role Mapping Administrator allows you to map business roles in different systems without having to understand the IT infrastructure. You access both application through a Web browser.

The supported Web browsers for iManager and the Role Mapping Administrator are:

- ♦ Internet Explorer 7 and 8
- ♦ Mozilla Firefox 3, 3.5.x, and 3.6.x

See the “System Requirements” section in the *Identity Manager Role Mapping Administrator 2.0 Installation and Configuration Guide* for a list of Role Mapping Administrator system requirements.

6.7 Resource Requirements

Table 6-4 *Identity Manager Resource Requirements*

Identity Manager Component	Minimum Requirement
Metadirectory Server	203 MB
Remote Loader	96 MB
Drivers	200 MB
iManager Plug-ins	80 MB

Installing Identity Manager

7

Identity Manager contains an integrated installer that simplifies the installation process and installs and configures all of the components at the same time. If you are installing your first Identity Manager system, use the integrated installer. For more information, see the [Identity Manager 4.0 Integrated Installation Guide](#).

If you have experience with Identity Manager and want to install each item separately, Identity Manager has separate installers for the different components.

It is important to install and use Analyzer and Designer during the planning phase of the Identity Manager implementation. For more information, see [Chapter 2, “Creating a Project Plan,” on page 15](#).

Install the components in the order listed. For an explanation of the different components, see the [Identity Manager 4.0 Overview Guide](#) guide.

- ◆ [Section 7.1, “Installing Analyzer,” on page 59](#)
- ◆ [Section 7.2, “Installing Designer,” on page 60](#)
- ◆ [Section 7.3, “Installing eDirectory,” on page 60](#)
- ◆ [Section 7.4, “Installing iManager,” on page 61](#)
- ◆ [Section 7.5, “Installing the Metadirectory Server,” on page 61](#)
- ◆ [Section 7.6, “Installing the Remote Loader,” on page 65](#)
- ◆ [Section 7.7, “Installing the Driver Files,” on page 70](#)
- ◆ [Section 7.8, “Installing the Roles Based Provisioning Module,” on page 71](#)
- ◆ [Section 7.9, “Installing a Custom Driver,” on page 71](#)
- ◆ [Section 7.10, “Installing the Role Mapping Administrator,” on page 71](#)
- ◆ [Section 7.11, “Installing the Identity Reporting Module or Sentinel,” on page 72](#)

7.1 Installing Analyzer

Analyzer is a workstation-based tool that allows you to analyze, clean, and prepare your data for synchronization with Identity Manager. You should install Analyzer and use it throughout the planning part of your Identity Manager implementation. For more information about planning, see [Part I, “Planning,” on page 11](#).

- 1** Verify that your workstation’s operating system is supported.
For more information, see [Section 6.6, “Workstations,” on page 54](#).
- 2** Ensure that you have downloaded the necessary Identity Manager files from the Novell Downloads Web site. For more information, see [Chapter 5, “Where to Get Identity Manager,” on page 45](#).
- 3** Start the installation by executing the correct program for your workstation’s platform.

Linux: `IDM4.0_Lin/products/Analyzer/install`

To execute the binary file, enter `./install`.

Windows: IDM4.0_Win:/products/Analyzer/install.exe

- 4 Use the following information to complete the installation:

Install Location: Specify a location on the workstation where to install Analyzer.

Create Short Cuts and Select a Language: Select where you want short cuts for Analyzer created on the desk top, and select the language you want to use to install Analyzer.

Analyzer is now installed. The first time you launch Analyzer you are prompted for an activation. Until you activate Analyzer, you cannot use it. For more information, see [Chapter 8, “Activating Novell Identity Manager Products,”](#) on page 73.

7.2 Installing Designer

Designer is a workstation-based tool that allows you to design your Identity Manager solution. You should install Designer and use it throughout the planning part of your Identity Manager implementation. For more information about planning, see [Part I, “Planning,”](#) on page 11.

- 1 Verify that your workstation’s operating system is supported. For a proper functioning of Designer, install 32-bit NCI package. For more information, see [Section 6.6, “Workstations,”](#) on page 54 and [Designer 4.0 for Identity Manager 4.0 Administration Guide](#).
- 2 Ensure that you have downloaded the necessary Identity Manager files from the Novell Downloads Web site. For more information, see [Chapter 5, “Where to Get Identity Manager,”](#) on page 45.
- 3 Start the installation by executing the correct program for your workstation’s platform.

Linux: IDM4.0_Lin/products/Designer/install

To execute the binary file, enter `./install`.

Windows: IDM4.0_Win:\products\Designer\install.exe

- 4 Use the following information to complete the installation:

Install Folder: Specify a location on the workstation where to install Designer.

Create Shortcuts: Select whether the shortcuts are placed on your desktop and in your Desktop Menu.

Before installing Designer, make sure that you have installed this package. You can use YaST to check for dependencies and installed packages. Refer to the [Designer 4.0 for Identity Manager 4.0 Administration Guide](#) for further information.

7.3 Installing eDirectory

Ensure that you have downloaded the necessary Identity Manager files from the Novell Downloads Web site. For more information, see [Chapter 5, “Where to Get Identity Manager,”](#) on page 45.

eDirectory 8.8.6 is provided on the Identity Manager media. There are installers for both 32-bit platforms and 64-bit platforms. The location of the installer depends on the platform:

- ♦ **Linux 32-bit:** IDM4.0_Lin/products/eDirectory/x86/setup/nds-install
- ♦ **Linux 64-bit:** IDM4.0_Lin/products/eDirectory/x64/setup/nds-install
- ♦ **Solaris 32-bit:** IDM4.0_Solaris/products/eDirectory/x86/setup/nds-install
- ♦ **Solaris 64-bit:** IDM4.0_Solaris/products/eDirectory/x64/setup/nds-install

To execute the binary file, enter `./nds-install`.

- ♦ **Windows 32-bit:** `IDM4.0_Win:\products\eDirectory\x86\nt\Setup.exe`
- ♦ **Windows 64-bit:** `IDM4.0_Win:\products\eDirectory\x64\windows\Setup.exe`

The instructions on how to install eDirectory vary depending on your platform. For installation instructions for your platform, see the corresponding section in the *Novell eDirectory 8.8 Installation Guide* (<http://www.novell.com/documentation/edir88/edirin88/data/a2iii88.html>).

NOTE: For Linux and Solaris, you must configure you eDirectory after it is installed before you can install the Metadirectory server. For configuration instructions, see “[Configuring Novell eDirectory on Linux, Solaris, or AIX Systems](http://www.novell.com/documentation/edir88/edirin88/data/bnn8z89.html)” (<http://www.novell.com/documentation/edir88/edirin88/data/bnn8z89.html>) in the *Novell eDirectory 8.8 Installation Guide*.

7.4 Installing iManager

Ensure that you have downloaded the necessary Identity Manager files from the Novell Downloads Web site. For more information, see [Chapter 5, “Where to Get Identity Manager,” on page 45](#).

iManager 2.7.4 is provided on the Identity Manager media. There are installers for Windows and Linux. iManager is not supported on Solaris. The location of the installer depends on the platform:

- ♦ **Linux:** `IDM4.0_Lin/products/iManager/installs/linux/iManagerInstallLinux.bin`

To execute the binary file, enter `./iManagerInstallLinux.bin`.

- ♦ **Windows:** `IDM4.0_Win:\products\iManager\installs\win\iManagerInstall.exe`

The instructions on how to install iManager vary depending on your platform. For installation instructions, see the corresponding section in the *iManager Installation Guide* (http://www.novell.com/documentation/imanager27/imanager_install_27/data/hk42s9ot.html).

7.5 Installing the Metadirectory Server

For Linux\UNIX platforms you can install the Metadirectory server as `root` or a non-`root` user. The installation procedure is different if you are using the non-`root` installation. See [Section 7.5.1, “Non-root Installation of the Metadirectory Server,” on page 63](#) for the installation instructions.

This procedure covers the GUI installation of the Metadirectory server, Web components, and utilities for the different platforms that Identity Manager supports. If you want to do a silent installation of these components, see [Section 7.5.2, “Silent Installation of the Metadirectory Server,” on page 64](#).

- 1 Verify that you have met the system requirement list in [Chapter 6, “System Requirements,” on page 47](#).
- 2 Ensure that you have downloaded the necessary Identity Manager files from the Novell Downloads Web site. For more information, see [Chapter 5, “Where to Get Identity Manager,” on page 45](#).
- 3 (Linux\UNIX only) To verify that the environment variables for eDirectory are exported before starting the installation on Linux/UNIX, go to a command prompt and enter:

```
set | grep PATH
```

The environment variables set the path for the eDirectory installation. The eDirectory installation path is listed if the environment variables are set. If the environment variables are not set, the installation of Identity Manager fails.

To set the environment variables for your current shell:

```
. /opt/novell/eDirectory/bin/ndspath
```

You must have the space between the . and the / for the command to work. For more information, see “Using the nds-install Utility to Install eDirectory Components” (<http://www.novell.com/documentation/edir88/edirin88/index.html?page=/documentation/edir88/edirin88/data/a79kg0w.html#ai39feq>).

- 4 Start the installation, by using the correct program for your platform.

Linux - GUI Install: IDM4.0_Lin/products/IDM/install.bin [-i gui]

Linux - Command Line Install: IDM4.0_Lin/products/IDM/install.bin -i console

Solaris - GUI Install: IDM4.0_Solaris/products/IDM/install.bin [-i gui]

Solaris - Command Line Install: IDM4.0_Solaris/products/IDM/install.bin -i console

To execute the binary files on Linux or Solaris, enter `./install.bin [-i {gui | console}]`.

Windows: IDM4.0_Win:\products\IDM\windows\setup\idm_install.exe

- 5 Use the following information to complete the installation:

Select Components: Select the Metadirectory server, iManager plug-ins, and utilities to install the Metadirectory server.

- ♦ **Novell Identity Manager Metadirectory Server:** This option requires the Identity Vault to be installed on this server and installs the 64-bit version of Identity Manager. It extends the schema for Identity Manager, installs the Metadirectory server, the Identity Manager drivers, and the Novell Audit Agent.
- ♦ **Novell Identity Manager Metadirectory Server (32-bit):** This option requires the Identity Vault to be installed on this server and installs the 32-bit version of Identity Manager. It extends the schema for Identity Manager, installs the Metadirectory server, the Identity Manager drivers, and the Novell Audit Agent.
- ♦ **Novell Identity Manager Connected System Server (64-bit):** This option does not require the Identity Vault to be installed on this server. Select this option only if you are installing the 64-bit Remote Loader. For more information, see [Section 7.6, “Installing the Remote Loader,”](#) on page 65.
- ♦ **Novell Identity Manager Connected System Server (.NET):** This option (Windows only) installs the .NET Remote Loader service and the SharePoint driver on this server.
- ♦ **Novell Identity Manager Plug-ins for Identity Manager:** Select this option if you have iManager installed on this server. It installs the iManager plug-ins for Identity Manager.
- ♦ **Utilities:** Installs utilities used to help configure the drivers for the connected systems. Not all drivers have utilities. If you are not sure if you need this, select it. It does not use much disk space.
- ♦ **Customize the selected components:** This option enables you to customize the components that you have selected to install. Before selecting this option, you should select the relevant components to install.

Authentication: Specify a user and password that has sufficient rights in eDirectory to extend the schema. Specify the username in the LDAP format. For example, `cn=idmadmin,o=company`.

- 6 Activate Identity Manager. For more information, see [Chapter 8, “Activating Novell Identity Manager Products,” on page 73](#).
- 7 Create and configure your driver objects. This information is contained in each driver guide. For more information, see [Identity Manager Drivers documentation \(http://www.novell.com/documentation/idm40drivers/\)](http://www.novell.com/documentation/idm40drivers/).

7.5.1 Non-root Installation of the Metadirectory Server

You can install Identity Manager as a non-root user to enhance the security of your UNIX/Linux server. You cannot install Identity Manager as a non-root user if eDirectory is installed by root.

The non-root installation does not install the following items:

- ♦ **Remote Loader:** Use the Java Remote Loader if you need to install the Remote Loader as a non-root user. For more information, see [Section 7.6.5, “Installing the Java Remote Loader on UNIX or Linux,” on page 69](#).
- ♦ **UNIX/Linux Account Driver:** Requires root privileges to function.
- ♦ **Novell Sentinel Platform Agent:** Install Novell Sentinel Platform Agent by root. Create `Dirxml.properties` in the `/etc/opt/novell/naudit/conf` directory. The location where the event log file is generated (`/var/opt/novell/naudit` is the default location) should have the write permission for a non-root user.

Use the following procedure to run the non-root installation of the Metadirectory server:

- 1 Ensure that you have downloaded the necessary Identity Manager files from the Novell Downloads Web site. For more information, see [Chapter 5, “Where to Get Identity Manager,” on page 45](#).
- 2 Install eDirectory 8.8.6 or later as a non-root user. For more information, see [“Non-root User Installing eDirectory 8.8.6” \(http://www.novell.com/documentation/edir88/edirin88/index.html?page=/documentation/edir88/edirin88/data/a79kg0w.html#bs6a3gs\)](http://www.novell.com/documentation/edir88/edirin88/index.html?page=/documentation/edir88/edirin88/data/a79kg0w.html#bs6a3gs).
- 3 Log in as the non-root user used to install eDirectory.
You should install Identity Manager as the same user you used to install the non-root version of eDirectory. The user who installs Identity Manager must have write access to the directories and files of the non-root eDirectory installation.
- 4 Execute the installation program for your platform.
Linux: `IDM4.0_Lin/products/IDM/linux/setup/idm-nonroot-install`
Solaris: `IDM4.0_Solaris/products/IDM/solaris/setup/idm-nonroot-install`
- 5 Use the following information to complete the installation:
Base Directory for the non-root eDirectory Installation: Specify the directory where the non-root eDirectory installation is. For example, `/home/user/install/eDirectory`.
Extend eDirectory Schema: If this is the first Identity Manager server installed into this instance of eDirectory, enter `Y` to extend the schema. If the schema is not extended, Identity Manager cannot function.

You are prompted to extend the schema for each instance of eDirectory owned by the non-root user that is hosted by the non-root eDirectory installation.

If you do select to extend the schema, specify the full distinguished name (DN) of the eDirectory user who has rights to extend the schema. The user must have the Supervisor right to the entire tree to extend the schema. For more information about extending the schema as a non-root user, see the `schema.log` file that is placed in the `data` directory for each instance of eDirectory.

Run the `/opt/novell/eDirectory/bin/idm-install-schema` program to extend the schema on additional eDirectory instances after the installation is complete.

Utilities: (Optional) If you need an Identity Manager driver utility, you must copy the utilities from the Identity Manager installation media to the Identity Manager server. All utilities are found in the `IDM4.0_platform/product/IDM/platform/setup/utilities` directory.

- 6 Activate Identity Manager. For more information, see [Chapter 8, “Activating Novell Identity Manager Products,”](#) on page 73.
- 7 Create and configure the driver objects. This information is contained in each driver guide. For more information, see the [Identity Manager Drivers documentation \(http://www.novell.com/documentation/idm40drivers/\)](http://www.novell.com/documentation/idm40drivers/).

7.5.2 Silent Installation of the Metadirectory Server

In order to run a silent installation of Identity Manager you must create a properties files with the parameters required to complete the installation. There is a sample file included on the Identity Manager media:

- ♦ **Linux:** `IDM4.0_Lin/products/IDM/linux/setup/silent.properties`
- ♦ **Solaris:** `IDM4.0_Solaris/products/IDM/solaris/setup/silent.properties`
- ♦ **Windows:** `IDM4.0_Win:\products\IDM\windows\setup\silent.properties`

Start the silent installation by using the correct program for your platform:

- ♦ **Linux:** `IDM4.0_Lin/products/IDM/install.bin -i silent -f <filename>.properties`
- ♦ **Solaris:** `IDM4.0_Solaris/products/IDM/install.bin -i silent -f <filename>.properties`
- ♦ **Windows:** `IDM4.0_Win:\products\IDM\windows\setup\idm_install.exe -i silent -f <filename>.properties`

Create a property file `<filename>.properties` with the following attributes, in the location from where you run the Identity Manger installer:

```
EDIR_USER_NAME=cn=admin,o=test
EDIR_USER_PASSWORD=test
METADIRECTORY_SERVER_SELECTED=true
CONNECTED_SYSTEM_SELECTED=false
X64_CONNECTED_SYSTEM_SELECTED=false
WEB_ADMIN_SELECTED=false
UTILITIES_SELECTED=false
```

For default installed locations, see `/tmp/idmInstall.log`.

If you have installed iManager, and you later want to install iManager plug-ins, you must set the `WEB_ADMIN_SELECTED` value to `true`.

If you want to do a silent installation of Identity Manager on multiple instances, you must make sure that the `<filename>.properties` file has the following lines:

```
EDIR_NCP_PORT=524
EDIR_NDS_CONF=/etc/opt/novell/eDirectory/conf
EDIR_IP_ADDRESS=<xxx.xx.xx.xx>
```

The password is stored in a file for the silent installation of Metadirectory. You can also use the `EDIR_USER_PASSWORD` environment variable to supply the password instead of writing it in a file. If the `EDIR_USER_PASSWORD` variable is not set in the properties file, the installer reads the value from the `EDIR_USER_PASSWORD` environment variable.

7.6 Installing the Remote Loader

The Remote Loader extends the functionality of Identity Manager by allowing the driver to access the connected system without having the Identity Vault and Metadirectory server installed on the same server as the connected system. As part of the planning process, you need to decide if you are going to use the Remote Loader or not. For more information about the planning process, see [Chapter 3, “Technical Guidelines,” on page 27](#).

- ◆ [Section 7.6.1, “Requirements,” on page 65](#)
- ◆ [Section 7.6.2, “Supported Drivers,” on page 65](#)
- ◆ [Section 7.6.3, “Installation Procedure,” on page 66](#)
- ◆ [Section 7.6.4, “Silent Installation of the Remote Loader,” on page 68](#)
- ◆ [Section 7.6.5, “Installing the Java Remote Loader on UNIX or Linux,” on page 69](#)
- ◆ [Section 7.6.6, “Coexistence of 32-bit and 64-bit Remote Loader,” on page 70](#)

If you want to install the Remote Loader through a non-`root` user, use the Java Remote Loader. The Java Remote Loader can also be used when you customize your environment and install the Java Remote Loader on a unsupported platform such as HP-UX. For more information, see [Section 7.6.5, “Installing the Java Remote Loader on UNIX or Linux,” on page 69](#).

7.6.1 Requirements

The Remote Loader requires that each driver’s connected system is available and the relevant APIs are provided. Refer to the [Identity Manager Driver documentation \(http://www.novell.com/documentation/idm40drivers\)](http://www.novell.com/documentation/idm40drivers) for operating system and connected system requirements that are specific to each driver.

7.6.2 Supported Drivers

Not all Identity Manager drivers are supported by the Remote Loader. The following is a list the drivers that have Remote Loader capability.

- ◆ Active Directory
- ◆ Avaya PBX
- ◆ Data Collection Services

- ◆ Delimited Text
- ◆ GroupWise (Available only for 32-bit Remote Loader)
- ◆ JDBC
- ◆ JMS
- ◆ LDAP
- ◆ Driver for Linux and UNIX
- ◆ LoopBack
- ◆ Lotus Notes
- ◆ Managed System Gateway
- ◆ Manual Task Services
- ◆ Null Services
- ◆ PeopleSoft 5.2
- ◆ Remedy ARS
- ◆ RACF
- ◆ Salesforce.com
- ◆ SAP Business Logic
- ◆ SAP GRC (CMP only)
- ◆ SAP HR
- ◆ SAP Portal
- ◆ SAP User Management
- ◆ Scripting
- ◆ SharePoint
- ◆ SOAP
- ◆ WorkOrder

The drivers listed below are not capable of using the Remote Loader.

- ◆ eDirectory
- ◆ Entitlements Services
- ◆ Role Service
- ◆ User Application

7.6.3 Installation Procedure

The Remote Loader has different programs for the different platforms, so it can communicate with the Metadirectory server.

- ◆ **Linux/UNIX:** `rdxml` is an executable that enables the Metadirectory server to communicate with the Identity Manager drivers running in Solaris or Linux environments.
- ◆ **Windows:** The Remote Loader Console uses `rlconsole.exe` to interface with `dirxml_remote.exe`, which is an executable that enables the Metadirectory server to communicate with the Identity Manager drivers running on Windows.

To install the Remote Loader:

- 1 Verify you have met the system requirements listed in [Chapter 6, “System Requirements,”](#) on [page 47](#).
- 2 Ensure that you have downloaded the necessary Identity Manager files from the Novell Downloads Web site. For more information, see [Chapter 5, “Where to Get Identity Manager,”](#) on [page 45](#).

- 3 Start the installation, using the correct program for your platform.

Linux - GUI Install: `IDM4.0_Lin/products/IDM/install.bin [-i gui]`

Linux - Command Line Install: `IDM4.0_Lin/products/IDM/install.bin -i console`

Solaris - GUI Install: `IDM4.0_Solaris/products/IDM/install.bin [-i gui]`

Solaris - Command Line Install: `IDM4.0_Solaris/products/IDM/install.bin -i console`

Windows: `IDM4.0_Win:\products\IDM\windows\setup\idm_install.exe`

To execute the binary files on Linux or Solaris, enter `./install.bin [-i {gui | console}]`.

- 4 Use the following information provided to complete the installation:

Select Components: Select the connected system server and utilities to install the Remote Loader.

- ♦ **Novell Identity Manager Metadirectory Server:** Select this option only if you are installing the Metadirectory server. This option requires the Identity Vault to be installed on this server. For more information, see [Section 7.5, “Installing the Metadirectory Server,”](#) on [page 61](#).
- ♦ **Novell Identity Manager Connected System Server 32-bit:** This option does not require the Identity Vault to be installed on this server. It installs the 32-bit version of the Remote Loader Service on your application server.
- ♦ **Novell Identity Manager Connected System Server 64-bit:** This option does not require the Identity Vault to be installed on this server. It installs the 64-bit version of the Remote Loader Service on your application server.
- ♦ **Novell Identity Manager Connected System Server (.NET):** This option (Windows only) installs the .NET Remote Loader service and the SharePoint driver on this server.
- ♦ **Novell Identity Manager Plug-ins for Identity Manager:** Select this option if you have iManager installed on this server. It installs the iManager plug-ins for Identity Manager.
- ♦ **Utilities:** Installs utilities used to help configure the drivers for the connected systems. Not all drivers have utilities. If you are not sure if you need this, select it. It does not use much disk space.
- ♦ **Custom:** Select this option if you want to customize the features that are installed. It allows you to select the options listed below. Before you select this option, you should select the components to install:
 - ♦ **Remote Loader Service 32-bit:** The service that communicates with the Metadirectory server.
 - ♦ **Remote Loader Service 64-bit:** The service that communicates with the Metadirectory server.

- ♦ **Drivers:** Select which driver files to install. You should install all of the driver files. If you need to add another Remote Loader instance, you do not need to run the installation again.
- ♦ **Novell Identity Manager Connected System Server (.NET):** (Windows Only) Installs the .NET Remote Loader service and the SharePoint driver.

Other options must be select when you select the customize for the installation to proceed.

(Windows Only) Install Location for Connected System Server: Specify the directory where the Connected System Server is installed.

(Windows Only) Install Location for .NET Remote Loader: Specify the directory where the .NET Remote Loader is installed.

(Windows Only) Install Location for Utilities: Specify the directory where the utilities are installed.

- 5 Create and configure your driver objects to use the Remote Loader. This information is contained in each driver guide. For more information, see the [Identity Manager Drivers documentation \(http://www.novell.com/documentation/idm40drivers/\)](http://www.novell.com/documentation/idm40drivers/).
- 6 Create a Remote Loader configuration file to work with your connected system. For more information, see “[Configuring the Remote Loader for Linux/UNIX by Creating a Configuration File](#)” in the *Identity Manager 4.0 Remote Loader Guide*.

7.6.4 Silent Installation of the Remote Loader

In order to run a silent installation of the Remote Loader you must create a properties file with the parameters required to complete the installation. There is a sample file included on the Identity Manager media:

- ♦ **Linux:** IDM4.0_Lin/products/IDM/linux/setup/silent.properties
- ♦ **Solaris:** IDM4.0_Solaris/products/IDM/solaris/setup/silent.properties
- ♦ **Windows:** IDM4.0_Win:\products\IDM\windows\setup\silent.properties

Start the silent installation by using the correct program for your platform:

- ♦ **Linux:** IDM4.0_Lin/products/IDM/install.bin -i silent -f <filename>.properties
- ♦ **Solaris:** IDM4.0_Solaris/products/IDM/install.bin -i silent -f <filename>.properties
- ♦ **Windows:** IDM4.0_Win:\products\IDM\windows\setup\idm_install.exe -i silent -f <filename>.properties

Create a property file <filename>.properties with the following attributes, in the location from where you run the Identity Manger installer:

```
METADIRECTORY_SERVER_SELECTED=false
CONNECTED_SYSTEM_SELECTED=true
X64_CONNECTED_SYSTEM_SELECTED=true
WEB_ADMIN_SELECTED=false
UTILITIES_SELECTED=false
```

For default installed locations, see /tmp/idmInstall.log.

If you have installed iManager, and you later want to install iManager plug-ins, you must set the `WEB_ADMIN_SELECTED` value to `true`.

7.6.5 Installing the Java Remote Loader on UNIX or Linux

`dirxml_jremote` is a pure Java Remote Loader. It is used to exchange data between the Metadirectory server running on one server and the Identity Manager drivers running in another location, where `rdxml` doesn't run. It should be able to run on any system with a compatible JRE (1.5.0 minimum) and Java Sockets. It is supported on the Linux/UNIX platforms the Identity Manager supports.

- 1 Verify that the Java 1.5.x JDK/JRE is available on the host system.
- 2 Ensure that you have downloaded the necessary Identity Manager files from the Novell Downloads Web site. For more information, see [Chapter 5, "Where to Get Identity Manager," on page 45](#).

- 3 Locate the Java Remote Loader installation files on the Identity Manager media:

Linux: `IDM4.0_Lin/products/IDM/java_remoteloader`

Solaris: `IDM4.0_Solaris/products/IDM/java_remoteloader`

- 4 Copy the `dirxml_jremote_dev.tar.gz` file to the desired location on the remote server.
- 5 Copy the `dirxml_jremote.tar.gz` or the `dirxml_jremote_mvs.tar` file to the desired location on the remote server.

For example: `/usr/idm`

For information on `mvs`, untar the `dirxml_jremote_mvs.tar` file, then refer to the `usage.html` document.

- 6 Unzip and extract the `dirxml_jremote.tar.gz` file and the `dirxml_jremote_dev.tar.gz` file.

For example: `gunzip dirxml_jremote.tar.gz` or `tar -xvf dirxml_jremote_dev.tar`

- 7 Copy the application `shim.jar` files to the `lib` subdirectory that was created when the `dirxml_jremote.tar` file was extracted.

Because the tar file doesn't contain the `.jar` files, you must manually copy these `.jar` files from the Metadirectory server into the `lib` directory. The `lib` directory is under the directory where the untarring occurred.

The default installation directory for `.jar` files on the Metadirectory server is `/opt/novell/eDirectory/lib/dirxml/classes`.

- 8 Customize the `dirxml_jremote` script by doing either of the following:

- ♦ Verify that the Java executable is reachable through the `PATH` environment variable by setting the environment variable `RDXML_PATH`. Enter the following commands to set the environment variable:
 1. `set RDXML_PATH=path`
 2. `export RDXML_PATH`
- ♦ Edit the `dirxml_jremote` script and prepend the path to the Java executable on the script line that executes Java.

- 9 Configure the sample `config8000.txt` file for use with your application `shim`. For more information, see ["Configuring the Remote Loader for Linux/UNIX by Creating a Configuration File"](#) in the *Identity Manager 4.0 Remote Loader Guide*.

7.6.6 Coexistence of 32-bit and 64-bit Remote Loader

Identity Manager 4.0 allows coexistence of 32-bit and 64-bit Remote Loader on a 64-bit operating system. If you are upgrading a 32-bit Remote Loader installed on a 64-bit operating system, it upgrades 32-bit Remote Loader and also installs 64-bit Remote Loader. You can have both 32-bit Remote Loader and 64-bit Remote Loader on the same machine.

7.7 Installing the Driver Files

You can install the driver files without installing the Metadirectory server or the Remote Loader. The driver files consists of driver shims and the driver utilities.

To install the driver files:

- 1 Ensure that you have downloaded the necessary Identity Manager files from the Novell Downloads Web site. For more information, see [Chapter 5, “Where to Get Identity Manager,” on page 45](#).

- 2 Start the installation, by using the correct program for your platform.

Linux - GUI Install: `IDM4.0_Lin/products/IDM/install.bin [-i gui]`

Linux - Command Line Install: `IDM4.0_Lin/products/IDM/install.bin -i console`

Solaris - GUI Install: `IDM4.0_Solaris/products/IDM/install.bin [-i gui]`

Solaris - Command Line Install: `IDM4.0_Solaris/products/IDM/install.bin -i console`

To execute the binary files on Linux or Solaris, enter `./install.bin [-i {gui | console}]`.

Windows: `IDM4.0_Win:\products\IDM\windows\setup\idm_install.exe`

- 3 Read and accept the license agreement, then click *Next*.

- 4 On the Select Components page, select the following options:

Novell Identity Manager Metadirectory Server: You can select this option or select the *Connected System Server* option. You don't need to select both options.

The driver files are included with this option.

Novell Identity Manager Connected System Server: You can select this option or select the *Metadirectory Server* option. You don't need to select both options.

The driver files are included with this option.

Novell Utilities Select this option to install utilities to help configure some drivers.

Customize the selected components: Allows you to select just the driver files without installing the Metadirectory server or the Remote Loader.

- 5 Click *Next*.

- 6 Unselect the *Metadirectory Engine* option and the *Remote Loader Service* option.

- 7 Verify that the *Drivers* option is selected under the *Metadirectory Server* option or the *Connected System Server* option.

You can expand the *Drivers* option and select the only the drivers you want to install. By default all drivers are selected.

- 8 Click *Next*.

- 9 On the *Authentication* page, specify a user and password that has sufficient rights in eDirectory to extend the schema. Specify the username in the LDAP format. For example, `cn=idmadmin,o=company`.
- 10 Click *Next*.
- 11 Review the installation summary, then click *Next*.
- 12 Review the installation complete message, then click *Done*.

The files for the drivers are now installed with the Remote Loader or the Metadirectory server.

7.8 Installing the Roles Based Provisioning Module

To install the Roles Based Provisioning Module, see the *Identity Manager Roles Based Provisioning Module 4.0 User Application: Installation Guide*.

7.9 Installing a Custom Driver

You can create a custom driver to use in your environment. For more information on creating a custom driver or installing one, see the [Novell Developer Kit \(http://developer.novell.com/wiki/index.php/Dirxml\)](http://developer.novell.com/wiki/index.php/Dirxml).

7.10 Installing the Role Mapping Administrator

The Role Mapping Administrator is a Web service that discovers authorizations and permissions that can be granted within your major IT systems. To install the Role Mapping Administrator:

- 1 Ensure that you have downloaded the necessary Identity Manager files from the Novell Downloads Web site. For more information, see [Chapter 5, “Where to Get Identity Manager,” on page 45](#).
- 2 Locate the Role Mapping Administrator installation file on the Identity Manager media located here:
Linux: `IDM4.0_Lin/products/RMA/IDMRMAP.jar`
Windows: `IDM4.0_Win:\products\RMA\IDMRMAP.jar`
- 3 From a command line, access the Role Mapping Administrator installation directory, then enter `java -jar IDMRMAP.jar`.

NOTE: For security reasons, you should install the Role Mapping Administrator as a non-root user, if you are using Linux.

- 4 Enter `Yes` to accept the license agreement.
- 5 Specify the installation directory for the Role Mapping Administrator. The default path is your current location.
- 6 Specify the portion of the URL representing the Role Impinging Administrator name. The default value is `IDMRMAP`.
- 7 Specify the HTTP port. The default value is `8081`.
- 8 Specify a password for the configuration administrator.

The Role Mapping Administrator is now installed. The application is not automatically started after the installation finishes. Use the following scripts to in the installation directory to stop and start the application.

- ♦ **Linux:** The start script is `start.sh` and the stop script is `stop.sh`.
- ♦ **Windows:** The start script is `start.bat` and the stop script is `stop.bat`.

After the Role Mapping Administrator is installed and started, you must configure it. See “[Configuring the Application](#)” in the *Identity Manager Role Mapping Administrator 2.0 Installation and Configuration Guide* for configuration information.

7.11 Installing the Identity Reporting Module or Sentinel

The Identity Reporting Module and Sentinel are optional addition to the Identity Manager solution. By adding auditing and reporting, you can meet compliance standards that many companies must abide by. You can create audit trails for any events you need to track, and you can generate reports to make sure you meet any audit standards for your company.

For installation and configuration information about the Identity Reporting Module, see the *Identity Reporting Module Guide*. For configuration information about Sentinel with Identity Manager, see the *Identity Manager 4.0 Reporting Guide for Novell Sentinel*. For system requirement information for Sentinel, see the *Novell Sentinel Installation Guide* (<http://www.novell.com/documentation/sentinel6/index.html>).

Activating Novell Identity Manager Products

8

The following information explains how activation works for products based on Novell Identity Manager. 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 the drivers by completing the following tasks:

- ♦ [Section 8.1, “Purchasing an Identity Manager Product License,” on page 73](#)
- ♦ [Section 8.2, “Installing a Product Activation Credential,” on page 73](#)
- ♦ [Section 8.3, “Viewing Product Activations for Identity Manager and for Drivers,” on page 74](#)
- ♦ [Section 8.4, “Activating Identity Manager Drivers,” on page 75](#)
- ♦ [Section 8.5, “Activating Analyzer,” on page 75](#)
- ♦ [Section 8.6, “Activating Designer and the Role Mapping Administrator,” on page 75](#)

8.1 Purchasing an Identity Manager Product License

To purchase an Identity Manager product license, so that you can activate the product, 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 Product Activation 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.). You can also [chat with us online \(http://support.novell.com/chat/activation\)](http://support.novell.com/chat/activation).

8.2 Installing a Product Activation Credential

You should install the Product Activation Credential via iManager.

- 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.
- 2 Click the license download link and 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 Open iManager.
- 4 Select *Identity Manager > Identity Manager Overview*.
- 5 Click  to browse for and select a driver set in the tree structure.
- 6 On the Identity Manager Overview page, click the driver set that contains the driver to activate.
- 7 On the Driver Set Overview page, click *Activation > Installation*.
- 8 Select the driver set where you want to activate an Identity Manager component, then click *Next*.
- 9 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*.
- 10 Click *Finish*.

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

8.3 Viewing Product Activations for Identity Manager and for Drivers

For each of your driver sets, you can view the Product Activation Credentials you have installed for the Metadirectory server and Identity Manager drivers:

- 1 Open iManager.
- 2 Click *Identity Manager > Identity Manager Overview*.
- 3 Click  to browse for and select a driver set in the tree structure, then click  to perform the search.
- 4 On the Identity Manager Overview page, click the driver set you want to view the activation information for.
- 5 On the Driver Set Overview page, click *Activation > Information*.

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

NOTE: 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.

8.4 Activating Identity Manager Drivers

Your Identity Manager purchase includes activations for service drivers and several common drivers.

- ◆ **Service Drivers:** The following service drivers are activated when you activate the Metadirectory server:
 - ◆ Data Collection Service
 - ◆ Entitlements Services
 - ◆ ID Provider
 - ◆ Loopback Service
 - ◆ Managed System Gateway
 - ◆ Manual Task Service
 - ◆ Null Service
 - ◆ Roles Service
 - ◆ User Application
 - ◆ WorkOrder
- ◆ **Common Drivers:** The following common drivers are activated when you activate the Metadirectory server:
 - ◆ Active Directory
 - ◆ ADAM
 - ◆ eDirectory
 - ◆ GroupWise
 - ◆ LDAP
 - ◆ Lotus Notes

Activations for all other Identity Manager drivers must be purchased separately. The activations for the drivers are sold as Identity Manager Integration modules. An Identity Manager Integration module can contain one or more drivers. You receive a Product Activation Credential for each Identity Manager Integration module that you purchase.

You must perform the steps in [Section 8.2, “Installing a Product Activation Credential,”](#) on page 73 for each Identity Manager Integration module to activate the drivers.

8.5 Activating Analyzer

The first time you launch Analyzer, you are prompted for an activation. If you do not enter the activation, you cannot use Analyzer. For more information, see “[Activating Analyzer](#)” in the *Analyzer 1.2 for Identity Manager Administration Guide*.

8.6 Activating Designer and the Role Mapping Administrator

Designer and the Role Mapping Administrator don’t require additional activations beyond activating the Metadirectory server or drivers.

Troubleshooting Identity Manager

9

Keep in mind the following information when you install Identity Manager:

- ♦ [“Lotus Notes driver issue while installing Identity Manager” on page 77](#)
- ♦ [“The Identity Manager installation might sporadically fail on Windows 2008 SP2 32-bit platform” on page 77](#)
- ♦ [“When two events occur on the syntax stream attribute, the first attribute change is lost” on page 81](#)

Lotus Notes driver issue while installing Identity Manager

Source: On Solaris 10, while installing Identity Manager 4.0 as non-root, you might encounter the following error message for Lotus Notes driver:

```
ln: cannot create /usr/lib/locale/ja/wnn//ndsrep: File exists
ln: cannot create
cp: cannot create /usr/lib/locale/ja/wnn//
libnotesdrvjni.so.1.0.0: Permission
denied
ln: cannot create /usr/lib/locale/ja/wnn//
libnotesdrvjni.so.1: File exists
ln: cannot create /usr/lib/locale/ja/wnn//libnotesdrvjni.so:
File exists
```

Action: Manually create the symbolic links. For information on checking and re-creating symbolic links, see [“Troubleshooting Installation Problems”](#) in the *Identity Manager 4.0 Driver for Lotus Notes Implementation Guide*.

The Identity Manager installation might sporadically fail on Windows 2008 SP2 32-bit platform

Source: The framework installer displays the following error:

```
Java Platform SE binary has stopped working.
```

Action: To work around this issue:

- 1 Run the Identity Manager installer with the `-DCLUSTER_INSTALL="true"` option. This installs only the Identity Manager files and not the eDirectory schema and other files.

```
<install_drive>:\windows\setup\idm_install.exe -
DCLUSTER_INSTALL="true"
```
- 2 Extend Identity Manager schema through iManager by using the *Import Convert Export Wizard* under *eDirectory Maintenance*.
- 3 Create the default objects by using the LDIF file.
 - ♦ Default password policy LDIF file

- 5 After installing the NMAS plug-ins on iManager, goto *NMAS > NMAS Login > Methods > New*. Browse to and install the configuration files from the desired NMAS methods.

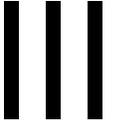
NOTE: Ensure that you refer the log file before applying the workaround. For example, the Role Based Provisioning Module schema is already extended, you don't need to extend it while installing the Role Based Provisioning Module driver.

When two events occur on the syntax stream attribute, the first attribute change is lost

- Source: The Identity Manager 4.0 engine does not store the STREAM and OCTET_STRING attributes in the cache. When an event is synchronized to the connected system, the engine reads these attributes from the Identity Vault and updates the connected system. If these attributes are modified before the engine reads them from the Identity Vault, the modified value is updated in the connected system and the intermediate change might be lost.
- Action: If the attribute is changed frequently, use an appropriate syntax other than SYN_STREAM.

For example, if an XML object is stored in the STREAM attribute, use XMLData syntax instead of SYN_STREAM.

Upgrading or Migrating



The following sections contain information about upgrading or migrating your existing Identity Manager solution:

- ♦ [Chapter 10, “What’s New,” on page 85](#)
- ♦ [Chapter 11, “Upgrade Versus Migration,” on page 87](#)
- ♦ [Chapter 12, “Supported Versions and System Requirements for Upgrades and Migrations,” on page 89](#)
- ♦ [Chapter 13, “Performing an Upgrade,” on page 91](#)
- ♦ [Chapter 14, “Performing a Migration,” on page 107](#)

Identity Manager 4.0 includes several new features and enhancements:

- ◆ [Section 10.1, “Identity Reporting Module,” on page 85](#)
- ◆ [Section 10.2, “New Drivers,” on page 85](#)
- ◆ [Section 10.3, “Support for XDas Auditing Included,” on page 86](#)
- ◆ [Section 10.4, “Packages Replace Driver Configuration Files,” on page 86](#)
- ◆ [Section 10.5, “Role Mapping Administrator,” on page 86](#)
- ◆ [Section 10.6, “Analyzer,” on page 86](#)
- ◆ [Section 10.7, “Integrated Installer,” on page 86](#)

10.1 Identity Reporting Module

The Identity Reporting Module gives you the ability to generate reports that show information about various aspects of your Identity Manager configuration, including information collected from one or more Identity Vaults or managed systems. The reporting module provides a set of predefined report definitions you can use to generate reports. In addition, it gives you the option to import custom reports defined in a third-party tool.

The Identity Reporting Module requires two new service drivers:

- ◆ Data Collection Service Driver
- ◆ Managed System Gateway Driver

For details on the reporting module and on the two reporting drivers, see the [Identity Reporting Module Guide](#). For details on the predefined reports, see [Using Identity Manager 4.0 Reports](#).

10.2 New Drivers

The following new drivers are included with Identity Manager 4.0:

- ◆ [Section 10.2.1, “SharePoint Driver \(.NET Remote Loader\),” on page 85](#)
- ◆ [Section 10.2.2, “Salesforce.com Driver,” on page 86](#)

10.2.1 SharePoint Driver (.NET Remote Loader)

The SharePoint driver for Novell Identity Manager enables user and group membership events to be synchronized between the Identity Vault and a SharePoint 2007 or SharePoint 2010 site collection. A single driver can process these events for a single site collection, which maintains user and group membership information for one or more SharePoint sites. For more information, see the [Identity Manager 4.0 Driver for SharePoint Implementation Guide](#).

10.2.2 Salesforce.com Driver

Identity Manager 4.0 offers automatic provisioning and synchronization of users to cloud applications. The new Salesforce.com driver for Novell Identity Manager can seamlessly provision and deprovision users to a Salesforce.com cloud application, which ensures that user identity information is consistent between the Identity Vault and the cloud application. The Salesforce.com driver also supports secure password synchronization between Identity Vault and Salesforce.com cloud and supports an authenticated proxy server and configurable user profile for automatic user provisioning. For more information, see the [Identity Manager 4.0 Driver for Salesforce.com Implementation Guide](#).

10.3 Support for XDAS Auditing Included

Identity Manager 4.0 supports XDAS-based auditing that augments the auditing capabilities of the Novell Audit Platform Agent. It uses common XDAS schema for Identity Manager, NMAS, eDirectory and the Role Mapping Administrator. The new auditing service also supports the syslog and file appenders. For more information, see the [Identity Reporting Module Guide](#) and the [Identity Manager 4.0 Reporting Guide for Novell Sentinel](#).

10.4 Packages Replace Driver Configuration Files

Identity Manager 4.0 introduces packages, which contain high-quality building blocks of Identity Manager policy content. Packages are now used to create drivers instead of using driver configuration files. For more information, see “[Managing the Identity Manager Content](#)” in the [Designer 4.0 for Identity Manager 4.0 Administration Guide](#).

10.5 Role Mapping Administrator

The Role Mapping Administrator is a new tool that analyzes the authorizations or permissions that can be granted in your IT systems, and allows you to grant those authorizations or permissions. The authorizations and permissions can be granted by a business analyst, not just IT staff or consultants. For more information, see the [Novell Identity Manager Role Mapping Administrator 2.0 User Guide](#).

10.6 Analyzer

Analyzer allows you to diagnose, clean, and prepare identity data for management with Identity Manager. For more information, see the [Analyzer 1.2 for Identity Manager Administration Guide](#).

10.7 Integrated Installer

Identity Manager 4.0 comes with an integrated installer that installs and configures all of the Identity Manager components through one installer. The installer is used for new installations in small to medium environments. For more information, see the [Identity Manager 4.0 Integrated Installation Guide](#).

Upgrade Versus Migration

11

You can update your Identity Manager software through either an upgrade or a migration. An upgrade is when you update the software on the existing hardware. A migration is when you move to new hardware and a new version of the software. Each method has advantages and disadvantages, and there are scenarios where only one method can be used.

- ◆ [Section 11.1, “Upgrade,” on page 87](#)
- ◆ [Section 11.2, “Migration,” on page 88](#)
- ◆ [Section 11.3, “Multiple Servers Associated with a Single Driver Set,” on page 88](#)

11.1 Upgrade

An upgrade is when you install the new version of Identity Manager on the existing server. To install Identity Manager, you must upgrade the current versions of the OS and eDirectory to the supported versions for Identity Manager 4.0. See [Chapter 6, “System Requirements,” on page 47](#) for a list of the supported platforms.

There are several advantages to performing an upgrade:

- ◆ No new hardware
- ◆ No migration of data

There are also disadvantages to performing an upgrade:

- ◆ Downtime when the OS is updated and the server is rebooted
- ◆ Downtime when eDirectory is updated and is restarted

There are certain scenarios when an upgrade is not feasible, or when multiple upgrades must be performed. Because Identity Manager 3.5.x and above are the only supported migration paths, these are the only versions that are described in the following scenarios:

The only supported situation for an upgrade is to have Identity Manager 3.5.x or Identity Manager 3.6.x on a supported operating system. But there are some scenarios where an upgrade is not feasible. The following are some examples where an upgrade is not feasible:

- ◆ **Unsupported OS:** If the current version of the OS is not supported by Identity Manager 4.0, the only supported upgrade path is to perform a migration to a new server.
- ◆ **Identity Manager 3.0.x:** If the current version of Identity Manager is 3.0.x, you cannot perform a direct upgrade. The two options are:
 - ◆ Perform an upgrade to Identity Manager 3.5.x, upgrade to eDirectory 8.8.6, then perform an upgrade to Identity Manager 4.0.
 - ◆ Perform a migration to a new server.
- ◆ **Roles Based Provisioning Module:** If you have the Roles Based Provisioning Module installed, you cannot perform an upgrade. You must perform a migration. For more information see the [Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide](#).

If you are performing an upgrade, proceed to [Chapter 13, “Performing an Upgrade,”](#) on page 91.

11.2 Migration

A migration is when you install Identity Manager 4.0 on a new server, then migrate the existing data to this new server. Follow the [Chapter 4, “Basic Identity Manager System Checklist,”](#) on page 41 to verify that the installation is complete.

The advantage of performing an upgrade is that there is minimal downtime for the drivers. The disadvantage is that it requires new hardware.

If you are performing a migration, proceed to [Chapter 14, “Performing a Migration,”](#) on page 107.

11.3 Multiple Servers Associated with a Single Driver Set

If you have multiple servers associated with a driver set, you can perform an upgrade or a migration on one server at a time. If you don't have time to upgrade the servers at the same time, the drivers continue to work with the different versions of Identity Manager until the upgrades for each server can be completed.

The Identity Manager engine is backward compatible, so the Identity Manager 4.0 engine can run Identity Manager 3.6.x drivers without problems.

IMPORTANT: If you enable features for drivers that are supported only on Identity Manager 4.0, the drivers stop working on the servers with mixed versions. The older engines cannot handle the new functionality. This breaks the drivers until all servers are upgraded to Identity Manager 4.0.

Supported Versions and System Requirements for Upgrades and Migrations

Use this information in this section to understand whether your version of Identity Manager is supported for an update or migration. An upgrade is when you update the software on the existing hardware. A migration is when you move to new hardware and a new version of the software.

- ♦ [Section 12.1, “Upgrades,” on page 89](#)
- ♦ [Section 12.2, “Migrations,” on page 90](#)

12.1 Upgrades

- ♦ [Section 12.1.1, “Supported Versions for Upgrades,” on page 89](#)
- ♦ [Section 12.1.2, “System Requirements,” on page 89](#)

12.1.1 Supported Versions for Upgrades

The following table indicates the supported upgrades for previous versions of Identity Manager.

Table 12-1 *Supported Versions for Upgrades*

Installed Version	Newest Version	Upgrade Supported
DirXML 1.1a	Identity Manager 4.0	No
Identity Manager 2.x	Identity Manager 4.0	No
Identity Manager 3.0.x	Identity Manager 4.0	No
Identity Manager 3.5.x*	Identity Manager 4.0	Yes
Identity Manager 3.6.x*	Identity Manager 4.0	Yes

*If you are running the Roles Based Provisioning Module, you cannot do an upgrade. You must do a migration. For more information, see the [Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide](#).

12.1.2 System Requirements

In order to upgrade to Identity Manager 4.0, the servers running the Identity Manager services need to meet the minimum requirements. See [Chapter 6, “System Requirements,” on page 47](#) for the list of minimum requirements for each platform.

12.2 Migrations

- ♦ [Section 12.2.1, “Supported Versions for Migrations,” on page 90](#)
- ♦ [Section 12.2.2, “System Requirements,” on page 90](#)

12.2.1 Supported Versions for Migrations

The following table indicates the supported migration paths for earlier versions of Identity Manager.

Table 12-2 *Supported Versions for Migrations*

Installed Version	Newest Version	Upgrade Supported
DirXML 1.1a*	Identity Manager 4.0	No
Identity Manager 2.x*	Identity Manager 4.0	No
Identity Manager 3.0.x*	Identity Manager 4.0	No
Identity Manager 3.5.x	Identity Manager 4.0	Yes
Identity Manager 3.6.x	Identity Manager 4.0	Yes

*You can perform migrations from versions prior to Identity Manager 3.5.x, but they have not been tested. There might be additional steps that are not documented to convert the data from these older versions to the current version.

12.2.2 System Requirements

In order to migrate to Identity Manager 4.0, the servers running the Identity Manager services need to meet the minimum requirements. See [Chapter 6, “System Requirements,” on page 47](#) for the list of minimum requirements for each platform.

Before beginning, make sure you have reviewed the differences between an upgrade and a migration. See [Chapter 11, “Upgrade Versus Migration,”](#) on page 87.

- ◆ [Section 13.1, “Upgrade Checklist,”](#) on page 91
- ◆ [Section 13.2, “Creating a Backup of the Current Configuration,”](#) on page 93
- ◆ [Section 13.3, “Upgrading iManager,”](#) on page 95
- ◆ [Section 13.4, “Stopping the Drivers,”](#) on page 96
- ◆ [Section 13.5, “Upgrading Analyzer,”](#) on page 97
- ◆ [Section 13.6, “Upgrading Designer,”](#) on page 97
- ◆ [Section 13.7, “Upgrading the Metadirectory Server and Driver Shim Files,”](#) on page 98
- ◆ [Section 13.8, “Upgrading the Remote Loader,”](#) on page 99
- ◆ [Section 13.9, “Upgrading Drivers to Packages,”](#) on page 99
- ◆ [Section 13.10, “Restoring Custom Policies and Rules to the Driver,”](#) on page 101
- ◆ [Section 13.11, “Overlaying the Existing Driver Configuration File with the New Driver \(Deprecated\),”](#) on page 103
- ◆ [Section 13.12, “Deploying the Converted Project,”](#) on page 105
- ◆ [Section 13.13, “Starting the Drivers,”](#) on page 105

13.1 Upgrade Checklist

Use the following checklist to verify that all of the steps are completed in the correct order for a successful upgrade of the Identity Manager system. Follow these steps for each Identity Manager server in your environment.

- Make sure you have downloaded the Identity Manager ISO files. For more information, see [Chapter 5, “Where to Get Identity Manager,”](#) on page 45.
- Create a backup of the current configuration of your Identity Manager solution. This is done by creating exports of your drivers or creating a Designer project of your Identity Manager solution. For more information, see [Section 13.2, “Creating a Backup of the Current Configuration,”](#) on page 93.
- Verify that the operating system on the servers running Identity Manager is a supported version. See [Chapter 6, “System Requirements,”](#) on page 47 for a list of supported operating systems. If the operating system requires only a service pack to meet the system requirements, then proceed with the upgrade.

If your operating system is listed below, you cannot use this procedure. You must perform a migration instead of an upgrade.

- ◆ NetWare
- ◆ Windows NT
- ◆ Windows 2000
- ◆ Red Hat Linux 3

- ◆ SLES 8
- ◆ Solaris 8 or 9
- ❑ Upgrade your iManager server to iManager 2.7.3. For more information, see [Section 13.3, “Upgrading iManager,”](#) on page 95.
- ❑ Stop the drivers that are associated with the server you are upgrading. For more information, see [Section 13.4, “Stopping the Drivers,”](#) on page 96.
- ❑ Upgrade eDirectory to 8.8.6 or later on the server running Identity Manager. For more information, see the *Novell eDirectory 8.8 Installation Guide* (<http://www.novell.com/documentation/edir88/>).
- ❑ Start the drivers and verify that the drivers start. This also verifies that the upgrade to eDirectory 8.8.6 is successful. For more information, see [Section 13.13, “Starting the Drivers,”](#) on page 105.

For more information on running Identity Manager and Identity Manager drivers successfully after upgrading to eDirectory 8.8.6, see [TID 7007184](http://www.novell.com/support/viewContent.do?externalId=7007184&sliceId=1) (<http://www.novell.com/support/viewContent.do?externalId=7007184&sliceId=1>).

- ❑ (Conditional) If you are using Analyzer, upgrade to Analyzer 1.2. For more information, see [Section 13.5, “Upgrading Analyzer,”](#) on page 97.
- ❑ Upgrade to Designer 4.0. For more information, see [Section 13.6, “Upgrading Designer,”](#) on page 97.
- ❑ Convert the Designer project. For more information, see “[Converting Earlier Projects](#)” in *Designer 4.0 for Identity Manager 4.0 Administration Guide*.
- ❑ Stop the drivers that are associated with the server you are upgrading. For more information, see [Section 13.4, “Stopping the Drivers,”](#) on page 96.
- ❑ Upgrade the Metadirectory server. For more information, see [Section 13.7, “Upgrading the Metadirectory Server and Driver Shim Files,”](#) on page 98.
- ❑ (Conditional) If any of the drivers in the driver set for this server are Remote Loader drivers, upgrade the Remote Loader servers for each driver. For more information, see [Section 13.8, “Upgrading the Remote Loader,”](#) on page 99.
- ❑ (Conditional) If this server is your User Application server, perform the following additional steps:
 - ❑ The User Application driver must be migrated in Designer. For more information, see the *Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide*.
 - ❑ Create a new Role and Resource Service driver. The Role and Resource Service driver is not migrated. If you have an existing Role and Resource Service driver, you must create a new driver for Identity Manager 4.0. For more information, see the *Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide*.
 - ❑ Deploy the migrated User Application driver into the Identity Vault. For more information, see the *Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide*.
 - ❑ Upgrade the User Application. For more information, see the *Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide*.

- ❑ (Optional) For the new policies to take effect on the existing drivers, install the new driver packages. This is required only if there is new functionality included in the driver packages that you want to add to your existing driver. For more information, see [Section 13.9, “Upgrading Drivers to Packages,” on page 99](#).
- ❑ (Optional) Restore custom policies and rules to the drivers. When the new driver packages are installed, the existing driver policies are overwritten, so you must restore these policies. For more information, see [Section 13.10, “Restoring Custom Policies and Rules to the Driver,” on page 101](#).
- ❑ Deploy the converted Designer project into the Identity Vault. For more information, see the “Deploying and Exporting” in *Designer 4.0 for Identity Manager 4.0 Administration Guide*.
- ❑ Start the drivers associated with this server. For more information, see [Section 13.13, “Starting the Drivers,” on page 105](#).
- ❑ (Conditional) If you are using Novell Sentinel, you must update to Novell Sentinel 6.1. For more information about upgrading Sentinel, see the *Sentinel Installation Guide* (http://www.novell.com/documentation/sentinel6/pdfdoc/sentinel60_installationguide.pdf).
- ❑ Activate the Metadirectory server and any upgraded driver. For more information, see [Chapter 8, “Activating Novell Identity Manager Products,” on page 73](#).

13.2 Creating a Backup of the Current Configuration

Before upgrading, it is important to create a backup of the current configuration of your Identity Manager system. There are no additional steps required if you are using the User Application. All User Application configuration is stored in the User Application driver. There are two ways to create a backup:

- ◆ [Section 13.2.1, “Ensuring that Your Designer Project is Current,” on page 93](#)
- ◆ [Section 13.2.2, “Creating an Export of the Drivers,” on page 95](#)

13.2.1 Ensuring that Your Designer Project is Current

A Designer project contains the schema and all driver configuration information. Creating a project of your Identity Manager solution allows you to export all of the driver in one step instead of creating a separate export file for each driver.

- ◆ [“Exporting the Current Project” on page 93](#)
- ◆ [“Creating a New Project from the Identity Vault” on page 94](#)

Exporting the Current Project

If you already have a Designer project, verify that the information in the project is synchronized with what is in the Identity Vault:

- 1 In Designer, open your project.
- 2 In the Modeler, right-click the Identity Vault, then select *Live > Compare*.
- 3 Evaluate the project and reconcile any differences, then click *OK*.

For more information, see “Using the Compare Feature When Deploying” in *Designer 4.0 for Identity Manager 4.0 Administration Guide*.

- 4 On the toolbar, select *Project > Export*.
- 5 Click *Select All* to select all resources to export.
- 6 Select where to save the project and in what format, then click *Finish*.

Save the project in any location, other than the current workspace. When you upgrade to Designer, you must create a new workspace location. For more information, see “[Exporting a Project](#)” in *Designer 4.0 for Identity Manager 4.0 Administration Guide*.

Creating a New Project from the Identity Vault

If you don't have a Designer project of your Identity Manager solution, use the following procedure:

- 1 Install Designer 3.5.
You can create a Identity Manager 3.6.x project with Designer 3.5. For more information, see [Section 7.2, “Installing Designer,” on page 60](#).
- 2 Launch Designer, then specify a location for your workspace.
- 3 Select whether you want to check for online updates, then click *OK*.
- 4 On the Welcome page, click *Run Designer*.
- 5 On the toolbar, select *Project > Import Project > Identity Vault*.
- 6 Specify a name for the project, then either use the default location for your project or select a different location.
- 7 Click *Next*.
- 8 Specify the Identity Vault connection information:
 - ♦ **Host Name:** Specify the IP address or DNS name of the Identity Vault server.
 - ♦ **User name:** Specify the DN of the user used to authenticate to the Identity Vault.
 - ♦ **Password:** Specify the password of the authentication user.
- 9 Click *Next*.
- 10 Leave the Identity Vault Schema and the Default Notification Collection selected.
- 11 Expand the Default Notification Collection, then deselect the languages you don't need.
The Default Notification Collections are translated into many different languages. You can import all languages or select only the languages that you use.
- 12 Click *Browse*, then browse to and select a driver set to import.
- 13 Repeat [Step 12](#) for each driver set in this Identity Vault, then click *Finish*.
- 14 Click *OK* after the project is imported.
- 15 If you only have one Identity Vault, you are finished. If you have multiple Identity Vaults, proceed with [Step 16](#).
- 16 Click *Live > Import* on the toolbar.
- 17 Repeat [Step 8](#) through [Step 14](#) for each additional Identity Vault.

13.2.2 Creating an Export of the Drivers

Creating an export of the drivers makes a backup of your current configuration.

- ♦ “Using Designer to Create an Export of the Driver” on page 95
- ♦ “Using iManager to Create an Export of the Driver” on page 95

Using Designer to Create an Export of the Driver

- 1 Verify that your project in Designer has the most current version of your driver. For instructions, see “Importing a Library, a Driver Set, or a Driver from the Identity Vault” in the *Designer 4.0 for Identity Manager 4.0 Administration Guide*.
- 2 In the Modeler, right-click the driver line of the driver you are upgrading.
- 3 Select *Export to a Configuration File*.
- 4 Browse to a location to save the configuration file, then click *Save*.
- 5 Click *OK* on the results page.
- 6 Repeat [Step 1](#) through [Step 5](#) for each driver.

Using iManager to Create an Export of the Driver

- 1 In iManager, select *Identity Manager > Identity Manager Overview*.
- 2 Browse to and select the location in the tree to search for Driver Set objects, then click the search icon .
- 3 Click the Driver Set object that holds the driver you want to upgrade.
- 4 Click the driver you want to upgrade, then click *Export*.
- 5 Click *Next*, then select *Export all contained policies, linked to the configuration or not*.
- 6 Click *Next*, then click *Save As*.
- 7 Select *Save to Disk*, then click *OK*.
- 8 Click *Finish*.
- 9 Repeat [Step 1](#) through [Step 8](#) for each driver.

13.3 Upgrading iManager

You must upgrade iManager to be able to use the updated functionality in the Identity Manager plugins.

iManager can only be installed on Windows or Linux. If your Metadirectory server is installed on Solaris, you must have iManager installed on a separate server.

If you have iManager 2.6 or earlier installed, you cannot use these steps to upgrade iManager. Use the correct upgrade procedure in the *Novell iManager 2.7 Installation Guide* (http://www.novell.com/documentation/imanager27/imanager_install_27/data/bhxda4r.html).

To upgrade iManager:

- 1 (Conditional) If you are installing on Linux, log in as `root` before launching the installation.
- 2 Access the Identity Manager installation media on your platform.

- 3 Launch the appropriate iManager install for your platform:
 - ♦ **Linux:** IDM4.0_Lin/products/iManager/installs/linux/iManagerInstallLinux.bin
To execute the binary, enter `./iManagerInstallLinux.bin` from the installation directory.
 - ♦ **Windows:** IDM4.0_Win:\product\iManager\installs\win\iManagerinstall.exe
- 4 Select the language you want to install iManager in.
- 5 Read and accept the license agreement.
- 6 Select to install Novell iManager 2.7, Tomcat, and JVM.
- 7 Select OK to remove the older version of Tomcat that is installed with the older version of iManager.
- 8 Select Yes to download plug-ins.
- 9 Access the default location to download plug-ins.
- 10 Select to install the default selected plug-ins.
- 11 Select No when you are asked to install plug-ins from a local directory.
- 12 Specify the HTTP port for Tomcat to run on. By default, it is 8080.
- 13 Specify the SSL port for Tomcat to run on. By default, it is 8443.
- 14 Review your selections, then select *OK* to run the upgrade.
- 15 After the installation finishes, restart Tomcat to see the changes.

13.4 Stopping the Drivers

Before you upgrade any files, it is important to stop the drivers.

- ♦ [Section 13.4.1, “Using Designer to Stop the Drivers,” on page 96](#)
- ♦ [Section 13.4.2, “Using iManager to Stop the Drivers,” on page 96](#)

13.4.1 Using Designer to Stop the Drivers

- 1 In Designer, select the Identity Vault  object in the *Outline* tab.
- 2 In the Modeler toolbar, click the *Stop All Drivers* icon .
This stops all drivers that are part of the project.
- 3 Set the drivers to manual start to ensure that the drivers do not start until the upgrade process is complete:
 - 3a Double-click the driver icon  in the *Outline* tab.
 - 3b Select *Driver Configuration > Startup Options*.
 - 3c Select *Manual*, then click *OK*.
 - 3d Repeat [Step 3a](#) through [Step 3c](#) for each driver.

13.4.2 Using iManager to Stop the Drivers

- 1 In iManager, select *Identity Manager > Identity Manager Overview*.

- 2 Browse to and select the location in the tree to search for Driver Set objects, then click the search icon .
- 3 Click the Driver Set object.
- 4 Click *Drivers > Stop all drivers*.
- 5 Repeat [Step 2](#) through [Step 4](#) for each Driver Set object.
- 6 Set the drivers to manual start to ensure that the drivers do not start until the upgrade process is complete:
 - 6a In iManager, select *Identity Manager > Identity Manager Overview*.
 - 6b Browse to and select the location in the tree to search for Driver Set objects, then click the search icon .
 - 6c Click the Driver Set object.
 - 6d In the upper right corner of the driver icon, click *Edit properties*.
 - 6e On the Driver Configuration page under *Startup Options*, select *Manual*, then click *OK*.
 - 6f Repeat [Step 6a](#) through [Step 6e](#) for each driver in your tree.

13.5 Upgrading Analyzer

If you have Analyzer installed, you must upgrade it to work with Identity Manager 4.0. If you don't have Analyzer installed, skip this section and proceed with [Section 13.6, "Upgrading Designer,"](#) on page 97.

Analyzer can only be installed on Windows or Linux. If your Metadirectory server is installed on Solaris, you must have Analyzer installed on a separate server.

To upgrade Analyzer:

- 1 Launch the Analyzer installer from the Identity Manager media:
 - ♦ **Linux:** `IDM4.0_Lin/products/Analyzer/install`
To execute the binary file, enter `./install`.
 - ♦ **Windows:** `IDM4.0_Win:\products\ANALZYER\install.exe`
- 2 Select the language you want to run Analyzer in, then read and accept the license agreement.
- 3 Specify the directory where Analyzer is installed, then click *Yes* in the message stating you already have Analyzer installed.
- 4 Select whether the shortcuts should be placed on your desktop and in your desktop menu.
- 5 Review the summary, then click *Install*.
- 6 Review the installation summary, then click *Done*.

13.6 Upgrading Designer

Before upgrading Designer, make sure you export your projects to create a backup of them. For instructions on how to export your project, see "[Exporting a Project](#)" in the *Designer 4.0 for Identity Manager 4.0 Administration Guide*.

Designer can only be installed on Windows or Linux. If your Metadirectory server is installed on Solaris, you must have Designer installed on a separate server.

To upgrade Designer:

- 1 Launch the Designer installer from Identity Manager media:
 - ♦ **Linux:** IDM4.0_Lin/products/Designer/install
To execute the binary file, enter `./install`.
 - ♦ **Windows:** IDM4.0_Win:\products\Designer\install.exe
- 2 Select the language to install Designer in, then read and accept the license agreement.
- 3 Specify the directory where Designer is installed, then click *Yes* in the message stating you already have Designer installed.
- 4 Select whether the shortcuts should be placed on your desktop and in your desktop menu.
- 5 Review the summary, then click *Install*.
- 6 Review the Readme, then click *Next*.
- 7 Select to launch Designer, then click *Done*.
- 8 Specify a location for your Designer workspace, then click *OK*.
- 9 Click *OK* in the warning message stating that your project needs to be closed and converted.
- 10 In the Project view, expand the project, then double-click *Project needs conversion*.
- 11 Review the steps that the Project Converter Wizard performs, then click *Next*.
- 12 Specify a name for the backup of your project, then click *Next*.
- 13 Review the summary of what happens during the conversion, then click *Convert*.
- 14 Review the summary after the conversion finishes, then click *Open*.

Designer is upgraded and the project is converted to the current format.

13.7 Upgrading the Metadirectory Server and Driver Shim Files

After the supporting components have been upgraded, you upgrade the Metadirectory server. During the upgrade process, the driver shim files that are stored in the file system are updated.

- 1 Verify that the drivers are stopped. For instructions, see [Section 13.4, “Stopping the Drivers,” on page 96](#).
- 2 Launch the Metadirectory server installer from the Identity Manager media:
 - ♦ **Linux:** IDM4.0_Lin/products/IDM/install.bin
 - ♦ **Solaris:** IDM4.0_Solaris/products/IDM/install.bin
To execute the binary file, enter `./install.bin`.
 - ♦ **Windows:** IDM4.0_Win:\products\IDM\Windows\setup\idm_install.exe
- 3 Select the language to install in, then read and accept the license agreement.
- 4 Select the *Novell Identity Manager Metadirectory Server*, *Novell iManager Plug-ins for Identity Manager*, and *Utilities* options to update the Metadirectory server and driver shim files.
- 5 Specify a user and the user password with administrative rights to eDirectory in LDAP format.

- 6 Review the summary, then click *Install*.
- 7 Read the installation summary, then click *Done*.

NOTE: After upgrading Identity Manager from 32-bit to 64-bit, the GroupWise driver and the native custom drivers do not work.

13.8 Upgrading the Remote Loader

If you are running the Remote Loader, you also need to upgrade the Remote Loader files.

- 1 Create a backup of the Remote Loader configuration files. The default location of the files is as follows:
 - ♦ **Windows:** `C:\Novell\RemoteLoader\remoteloadername-config.txt`
 - ♦ **Linux:** Create your own configuration file in the path of `rdxml`.
- 2 Verify that the drivers are stopped. For instructions, see [Section 13.4, “Stopping the Drivers,” on page 96](#).
- 3 Stop the Remote Loader service or daemon for each driver.
 - ♦ **Windows:** In the Remote Loader Console, select the Remote Loader instance, then click *Stop*.
 - ♦ **Linux:** `rdxml -config path_to_configfile -u`
 - ♦ **Java Remote Loader:** `dirxml_jremote -config path_to_configfile -u`
- 4 Run the installation programs for the Remote Loader.

The installation process updates the files and binaries to the current version. For more information, see [Section 7.6, “Installing the Remote Loader,” on page 65](#).
- 5 After the installation finishes, verify that your configuration files contain your environment’s information.
- 6 (Conditional) If there is a problem with the configuration file, copy the backup file you created in [Step 1](#). Otherwise, continue with [Step 7](#).
- 7 Start the Remote Loader service or daemon for each driver.
 - ♦ **Windows:** In the Remote Loader Console, select the Remote Loader instance, then click *Start*.
 - ♦ **Linux:** `rdxml -config path_to_config_file -sp password password`
 - ♦ **Java Remote Loader:** `dirxml_jremote -config path_to_config_file -sp password password`

NOTE: After upgrading Remote Loader from 32-bit to 64-bit, the GroupWise driver and the native custom drivers do not work.

13.9 Upgrading Drivers to Packages

Packages are a new content management feature in Identity Manager 4.0. All new driver content is delivered through packages instead of through driver configuration files.

Packages are managed, maintained, and created through Designer. iManager is package aware, but any changes to driver content through iManager are not maintained in Designer. For more information about managing packages, see “[Managing the Identity Manager Content](#)” in the *Designer 4.0 for Identity Manager 4.0 Administration Guide*.

There are three different ways to upgrade your drivers to packages:

- ♦ [Section 13.9.1, “Creating a New Driver,” on page 100](#)
- ♦ [Section 13.9.2, “Replacing Existing Content with Content from Packages,” on page 100](#)
- ♦ [Section 13.9.3, “Keeping the Current Content and Adding New Content with Packages,” on page 101](#)

13.9.1 Creating a New Driver

The simplest and cleanest way to upgrade drivers to packages is to delete your existing driver and create a new driver with packages. Add all the functionality you want in the new driver. The steps are different for each driver. For instructions, see the individual driver guides on the [Identity Manager Drivers documentation Web site \(http://www.novell.com/documentation/idm40drivers/\)](http://www.novell.com/documentation/idm40drivers/).

WARNING: When you delete an existing driver, your customized policies to the driver are also lost.

13.9.2 Replacing Existing Content with Content from Packages

If you need to keep the associations created by the driver, you shouldn’t delete and re-create the driver. This option allows you to keep the associations, but still create the driver content with packages.

To replace the existing content with content from packages:

- 1 Create a backup of the driver and all of the customized content in the driver.

For instructions, see [Section 13.2.2, “Creating an Export of the Drivers,” on page 95](#).

IMPORTANT: Make sure that your customized policies have different names than the default policies so that you do not lose any data.

- 2 In Designer, delete all objects stored inside of the driver. Delete the policies, filters, entitlements, and all other items stored inside of the driver.
- 3 Import the driver packages into the package catalog.
For instructions, see “[Importing Packages into the Package Catalog](#)” in the *Designer 4.0 for Identity Manager 4.0 Administration Guide*.
- 4 Install the packages to the driver.
For instructions, see each driver guide at the [Identity Manager Drivers documentation Web site \(http://www.novell.com/documentation/idm40drivers/\)](http://www.novell.com/documentation/idm40drivers/).
- 5 Add the base, mandatory, and optional packages to the driver to get the desired functionality. These steps are specific per driver.

For instructions, see each driver guide at the [Identity Manager Drivers documentation Web site \(http://www.novell.com/documentation/idm40drivers/\)](http://www.novell.com/documentation/idm40drivers/).

- 6 Restore any custom policies and rules to the driver. For instructions, see [Section 13.10, “Restoring Custom Policies and Rules to the Driver,”](#) on page 101.

The driver now functions as before, but with content from packages instead of from a driver configuration file.

13.9.3 Keeping the Current Content and Adding New Content with Packages

You can keep the driver as it currently is and add new functionality to the driver through packages, as long as the functionality in packages does not overlap the current functionality of the driver. When you install a package, it can overwrite existing policies, which might cause the driver to not work.

To add new content to the driver with packages:

- 1 Create a backup of the driver and all of the customized content in the driver.
For instructions, see [Section 13.2.2, “Creating an Export of the Drivers,”](#) on page 95.
- 2 Import the driver packages into the package catalog.
For instructions, see [“Importing Packages into the Package Catalog”](#) in the *Designer 4.0 for Identity Manager 4.0 Administration Guide*.
- 3 Install the packages on the driver.
For instructions, see each driver guide at the [Identity Manager Drivers documentation Web site \(http://www.novell.com/documentation/idm40drivers/\)](http://www.novell.com/documentation/idm40drivers/).
- 4 Add the desired packages to the driver. These steps are specific for each driver.
For instructions, see the [Identity Manager Drivers documentation Web site \(http://www.novell.com/documentation/idm40drivers/\)](http://www.novell.com/documentation/idm40drivers/).

The driver contains the new functionality added by the packages.

13.10 Restoring Custom Policies and Rules to the Driver

If you have custom policies or rules, they must be restored to the driver after you overlay the new driver configuration file. If these policies have different names, they are still stored in the driver, but the links are broken and need to be reestablished.

- ♦ [Section 13.10.1, “Using Designer to Restore Custom Policies and Rules to the Driver,”](#) on page 102
- ♦ [Section 13.10.2, “Using iManager to Restore Custom Policies and Rules to the Driver,”](#) on page 103

13.10.1 Using Designer to Restore Custom Policies and Rules to the Driver

You can add policies into the policy set in two different ways:

- ♦ [“Adding a Customized Policy through the Outline View” on page 102](#)
- ♦ [“Adding a Customized Policy through the Show Policy Flow View” on page 102](#)

Adding a Customized Policy through the Outline View

Perform these steps in a test environment before you move the upgraded driver to your production environment.

- 1 In the *Outline* view, select the upgraded driver to display the *Policy Set* view.
- 2 Right-click the policy set  icon where you need to restore the customized policy to the driver, then select *New > From Copy*.
- 3 Browse to and select the customized policy, then click *OK*.
- 4 Specify the name of the customized policy, then click *OK*.
- 5 Click *Yes* in the file conflict message to save your project.
- 6 After the Policy Builder opens the policy, verify that the information is correct in the copied policy.
- 7 Repeat [Step 2](#) through [Step 6](#) for each customized policy you need to restore to the driver.
- 8 Start the driver and test the driver.

For more information on starting the driver, see [Section 13.13, “Starting the Drivers,” on page 105](#). For more information on testing the driver, see [“Testing Policies with the Policy Simulator” in *Policies in Designer 4.0*](#).

- 9 After you verify that the policies work, move the driver to the production environment.

Adding a Customized Policy through the Show Policy Flow View

Perform these steps in a test environment before you move the upgraded driver to your production environment.

- 1 In the *Outline* view, select the upgraded driver, then click the *Show Policy Flow* icon .
- 2 Right-click the policy set where you need to restore the customized policy to the driver, then select *Add Policy > Copy Existing*.
- 3 Browse to and select the customized policy, then click *OK*.
- 4 Specify the name of the customized policy, then click *OK*.
- 5 Click *Yes* in the file conflict message to save your project.
- 6 After the Policy Builder opens the policy, verify that the information is correct in the copied policy.
- 7 Repeat [Step 2](#) through [Step 6](#) for each customized policy you need to restore to the driver.
- 8 Start the driver and test the driver.

For more information on starting the driver, see [Section 13.13, “Starting the Drivers,” on page 105](#). For more information on testing the driver, see “[Testing Policies with the Policy Simulator](#)” in *Policies in Designer 4.0*.

- 9 After you verify that the policies work, move the driver to the production environment.

13.10.2 Using iManager to Restore Custom Policies and Rules to the Driver

Perform these steps in a test environment before you move the upgraded driver to your production environment.

- 1 In iManager, select *Identity Manager > Identity Manager Overview*.
- 2 Browse to and select the location in the tree to search for Driver Set objects, then click the search icon .
- 3 Click the Driver Set object that contains the upgraded driver.
- 4 Click the driver icon, then select the policy set where you need to restore the customized policy.
- 5 Click *Insert*.
- 6 Select *Use an existing policy*, then browse to and select the custom policy.
- 7 Click *OK*, then click *Close*.
- 8 Repeat [Step 3](#) through [Step 7](#) for each custom policy you need to restore to the driver.
- 9 Start the driver and test the driver.

For information on starting the driver, see [Section 13.13, “Starting the Drivers,” on page 105](#). There is no policy simulator in iManager. To test the policies, cause events to happen that make the policies execute. For example, create a user, modify a user, or delete a user.

- 10 After you verify that the policies work, move the driver to the production environment.

13.11 Overlaying the Existing Driver Configuration File with the New Driver (Deprecated)

Identity Manager 4.0 uses packages instead of driver configuration files. There are no new configuration files for this release. All new driver content is delivered in packages from now on.

Before you begin, make sure that any customized policies have different policy names than the default policies. When a driver configuration is overlaid with a new driver file, the existing policies are overwritten. If your custom policies do not have a unique name, you lose those custom policies.

You overlay the new driver configuration file over your existing driver to update the driver with any new policies or functionality that are in the driver configuration file.

- ♦ [Section 13.11.1, “Using Designer to Overlay the Existing Driver Configuration File with the New Driver,” on page 104](#)
- ♦ [Section 13.11.2, “Using iManager to Overlay the Existing Driver Configuration File with the New Driver,” on page 104](#)

13.11.1 Using Designer to Overlay the Existing Driver Configuration File with the New Driver

IMPORTANT: Make sure that your customized policies have different names than the default policies, so you do not lose any data.

- 1 In the Modeler, right-click the driver line of the driver you are upgrading.
- 2 Select *Run Configuration Wizard*.
- 3 Click *Yes* on the warning page.
The warning informs you that all of the driver settings and policies will be reset.
- 4 Browse to and select the driver configuration for the driver you are upgrading, then click *Run*.
- 5 Specify the information for the driver, then click *Next*.
There might be more than one page of information to specify.
- 6 Click *OK* on the results page.
- 7 Look at the driver parameters and policies to make sure everything is set how you want it.
- 8 If you have custom policies, proceed to [Section 13.10, “Restoring Custom Policies and Rules to the Driver,” on page 101](#). Otherwise, proceed to [Section 13.13, “Starting the Drivers,” on page 105](#).

13.11.2 Using iManager to Overlay the Existing Driver Configuration File with the New Driver

IMPORTANT: Make sure that any customized policies have a different name than the default, so you do not lose any data.

- 1 In iManager, select *Identity Manager > Identity Manager Overview*.
- 2 Browse to and select the location in the tree to search for Driver Set objects, then click the search icon .
- 3 Click the Driver Set object.
- 4 Click *Drivers > Add driver*, then click *Next* on the New Driver Wizard page.
- 5 Select the driver configuration you want to overlay, then click *Next*.
- 6 In the *Existing drivers* field, browse to and select the driver you want to upgrade.
- 7 Specify the information for the driver, then click *Next*.
- 8 On the summary page, select *Update everything about that driver and policy libraries*.
- 9 Click *Next*, then click *Finish* on the Summary page.
- 10 Look at the driver parameters and policies to make sure everything is set how you want it.
- 11 If you have custom policies, proceed to [Section 13.10, “Restoring Custom Policies and Rules to the Driver,” on page 101](#). Otherwise, proceed to [Section 13.13, “Starting the Drivers,” on page 105](#).

13.12 Deploying the Converted Project

Deploy the converted Designer project into the Identity Vault. For more information, see “[Deploying and Exporting](#)” in the *Designer 4.0 for Identity Manager 4.0 Administration Guide*.

13.13 Starting the Drivers

After all of the Identity Manager components are upgraded, the drivers must be restarted. It is important to test the drivers after they are running to verify that all of the policies still work.

- ♦ [Section 13.13.1, “Using Designer to Start the Drivers,”](#) on page 105
- ♦ [Section 13.13.2, “Using iManager to Start the Drivers,”](#) on page 105

13.13.1 Using Designer to Start the Drivers

- 1 In Designer, select the Identity Vault  object in the *Outline* tab.
- 2 Click the *Start All Drivers* icon  in the Modeler toolbar. This starts all of the drivers in the project.
- 3 Set the driver startup options:
 - 3a Double-click the driver icon  in the *Outline* tab.
 - 3b Select *Driver Configuration > Startup Option*.
 - 3c Select *Auto start* or select your preferred method of starting the driver, then click *OK*.
 - 3d Repeat [Step 3a](#) through [Step 3c](#) for each driver.
- 4 Test the drivers to verify the policies are working as designed. For information on how to test your policies, see “[Testing Policies with the Policy Simulator](#)” in *Policies in Designer 4.0*.

13.13.2 Using iManager to Start the Drivers

- 1 In iManager, select *Identity Manager > Identity Manager Overview*.
- 2 Browse to and select the location in the tree to search for Driver Set objects, then click the search icon .
- 3 Click the Driver Set object.
- 4 Click *Drivers > Start all drivers* to start all of the drivers at the same time.
or
In the upper right corner of the driver icon, click *Start driver* to start each driver individually.
- 5 If you have multiple drivers, repeat [Step 2](#) through [Step 4](#).
- 6 Set the driver startup options:
 - 6a In iManager, select *Identity Manager > Identity Manager Overview*.
 - 6b Browse to and select the location in the tree to search for Driver Set objects, then click the search icon .
 - 6c Click the Driver Set object.
 - 6d In the upper right corner of the driver icon, click *Edit properties*.

- 6e** On the Driver Configuration page, under *Startup Options*, select *Auto start* or select your preferred method of starting the driver, then click *OK*.
- 6f** Repeat [Step 6b](#) through [Step 6e](#) for each driver.
- 7** Test the drivers to verify the policies are working as designed.
There is no policy simulator in iManager. To test the policies, cause events to happen that make the policies execute. For example, create a user, modify a user, or delete a user.

Before beginning, make sure you have reviewed the differences between an upgrade and a migration. See [Chapter 11, “Upgrade Versus Migration,”](#) on page 87.

- ♦ [Section 14.1, “Migration Checklist,”](#) on page 107
- ♦ [Section 14.2, “Adding the New Server to the Driver Set,”](#) on page 108
- ♦ [Section 14.3, “Changing Server-Specific Information,”](#) on page 109
- ♦ [Section 14.4, “Removing the Old Server from the Driver Set,”](#) on page 110

14.1 Migration Checklist

Use the following checklist to verify that all of the steps are completed in the correct order for a successful migration of the Identity Manager system. Follow these steps for each Identity Manager server in your environment.

- Make sure that you have downloaded the Identity Manager ISO files. For more information, see [Chapter 5, “Where to Get Identity Manager,”](#) on page 45.
- Create a backup of the current configuration of your Identity Manager solution. You do this by creating exports of your drivers or creating a Designer project of your Identity Manager solution. For more information, see [Section 13.2, “Creating a Backup of the Current Configuration,”](#) on page 93.
- Install the desired operating system. For a list of supported platforms, see [Chapter 6, “System Requirements,”](#) on page 47.
- Install eDirectory 8.8.6 on the server. For more information, see the *Novell eDirectory 8.8 Installation Guide* (<http://www.novell.com/documentation/edir88/index.html>).
- Add the same eDirectory replicas that are on the current Identity Manager server to this new server. For more information, see “[Administering Replicas](#)” (<http://www.novell.com/documentation/edir88/edir88/data/fbgciaad.html>) in the *eDirectory Administration Guide* (<http://www.novell.com/documentation/edir88/pdfdoc/edir88/edir88.pdf>).
- Install Identity Manager 4.0. Use [Chapter 4, “Basic Identity Manager System Checklist,”](#) on page 41 to verify that all steps are completed.
- If any of the drivers in the driver set are Remote Loader drivers, upgrade the Remote Loader server for each driver. For more information, see [Section 13.8, “Upgrading the Remote Loader,”](#) on page 99.
- (Conditional) If the old server is your User Application server, perform the following additional steps:
 - Run the NrfCaseUpdate utility. For more information, see “[Running the NrfCaseUpdate Utility](#)” in the *Identity Manager Roles Based Provisioning Module 4.0 User Application: Installation Guide*.
 - The User Application driver must be migrated in Designer. For more information, see the *Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide*.

- ❑ Create a new Role and Resource Service driver. The Role and Resource Service driver is not migrated. If you have an existing Role and Resource Service driver, you must create a new driver for Identity Manager 4.0. For more information, see the *Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide*.
- ❑ Deploy the migrated User Application driver into the Identity Vault. For more information, see the *Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide*.
- ❑ Install the User Application on this new server. For more information, see the *Identity Manager Roles Based Provisioning Module 4.0 User Application: Migration Guide*.
- ❑ Add the new server to the driver set. For more information, see [Section 14.2, “Adding the New Server to the Driver Set,” on page 108](#).
- ❑ Change the server-specific information for each driver. If you use iManager, it is a manual process. You should use iManager if you are migrating from an Identity Manager server earlier than 3.5 version to an Identity Manager server greater than or equal to 3.5. For all other supported migration paths, you can use Designer. For more information, see [Section 14.3, “Changing Server-Specific Information,” on page 109](#).
- ❑ (Conditional) Run `configupdate.sh` or `configupdate.bat` to change server-specific information from the old server to the new server for the User Application configuration. For more information, see “[IDM User Application Configuration Reference](#)” in the *Identity Manager Roles Based Provisioning Module 4.0 User Application: Installation Guide*.
- ❑ (Optional) Upgrade your drivers to use packages. All content for drivers is delivered through packages instead of a driver configuration file. For more information, see [Section 13.9, “Upgrading Drivers to Packages,” on page 99](#).
- ❑ (Optional) Restore custom policies and rules to the drivers. When you update your drivers to packages, the policies are overwritten, so restoring policies is required only if you upgraded your driver to use packages. For more information, see [Section 13.10, “Restoring Custom Policies and Rules to the Driver,” on page 101](#).
- ❑ Remove the old server from the driver set. For more information, see [Section 14.4, “Removing the Old Server from the Driver Set,” on page 110](#).
- ❑ If you are using Novell Sentinel, you must update to Novell Sentinel 6.1. For more information about upgrading Sentinel, see the *Sentinel Installation Guide* (http://www.novell.com/documentation/sentinel6/pdfdoc/sentinel60_installationguide.pdf).
- ❑ Activate the Metadirectory server and any upgraded driver. For more information, see [Chapter 8, “Activating Novell Identity Manager Products,” on page 73](#).

14.2 Adding the New Server to the Driver Set

If you are using iManager, you must add the new server to the driver set. Designer contains a Migration Wizard for the server that does this step for you. If you are using Designer, skip to [Section 14.3, “Changing Server-Specific Information,” on page 109](#). If you are using iManager, complete the following procedure:

- 1 In iManager, click  to display the Identity Manager Administration page.
- 2 Click *Identity Manager Overview*.
- 3 Browse to and select the container that holds the driver set.
- 4 Click the driver set name to access the Driver Set Overview page.

- 5 Click *Servers > Add Server*.
- 6 Browse to and select the new Identity Manager 4.0 server, then click *OK*.

14.3 Changing Server-Specific Information

You must change all server-specific information that is stored in each driver to the new server's information. The server-specific information is contained in:

- ♦ Global configuration values
- ♦ Engine control values
- ♦ Named passwords
- ♦ Driver authentication information
- ♦ Driver startup options
- ♦ Driver parameters
- ♦ Driver set data

You can do this in Designer or iManager. If you use Designer, it is an automated process. If you use iManager, it is a manual process. You should use iManager if you are migrating from an Identity Manager server earlier than 3.5 version to an Identity Manager server greater than or equal to 3.5. For all other supported migration paths, you can use Designer.

- ♦ [Section 14.3.1, “Changing the Server-Specific Information in Designer,” on page 109](#)
- ♦ [Section 14.3.2, “Changing the Server-Specific Information in iManager,” on page 110](#)

14.3.1 Changing the Server-Specific Information in Designer

The procedure affects all drivers stored in the driver set.

- 1 In Designer, open your project.
- 2 In the *Outline* tab, right-click the server, then select *Migrate*.
- 3 Read the overview to see what items are migrated to the new server, then click *Next*.
- 4 Select the target server from the list available servers, then click *Next*.

The only servers listed are servers that are not currently associated with a driver set and are equal to or newer than the source server's Identity Manager version.

- 5 Select *Make the target server active*.

There are three options, but *Make the target server active* is recommended.

- ♦ **Make the target server active:** Copies the settings from the source server to the target server and disables the drivers on the source server.
- ♦ **Keep the source server active:** Does not copy the settings and disables all drivers on the target server.
- ♦ **Makes both target and source servers active:** Copies settings from the source server to the target server without disabling the drivers on the source or target servers. This option is not recommended. If both drivers are started, the same information is written to two different queues and this can cause corruption.

- 6 Click *Migrate*.

7 Deploy the changed drivers to the Identity Vault.

For more information, see “[Deploying a Driver to an Identity Vault](#)” in the *Designer 4.0 for Identity Manager 4.0 Administration Guide*.

8 Start the drivers.

For more information, see [Section 13.13, “Starting the Drivers,”](#) on page 105.

14.3.2 Changing the Server-Specific Information in iManager

1 In iManager, click  to display the Identity Manager Administration page.

2 Click *Identity Manager Overview*.

3 Browse to and select the contain that holds the driver set.

4 Click the driver set name to access the Driver Set Overview page.

5 Click the upper right corner of the driver, then click *Stop driver*.

6 Click the upper right corner of the driver, then click *Edit properties*.

7 Copy or migrate all server-specific driver parameters, global configuration values, engine control values, named passwords, driver authentication data, and driver startup options that contain the old server’s information to the new server’s information. Global configuration values and other parameters of the driver set, such as max heap size, Java settings, and so on, must have identical values as those of the old server.

8 Click *OK* to save all changes.

9 Click the upper right corner of the driver to start the driver.

10 Repeat [Step 5](#) through [Step 9](#) for each driver in the driver set.

14.4 Removing the Old Server from the Driver Set

After the new server is running all of the drivers, the old server must be removed from the driver set.

- ♦ [Section 14.4.1, “Using Designer to Remove the Old Server from the Driver Set,”](#) on page 110
- ♦ [Section 14.4.2, “Using iManager to Remove the Old Server from the Driver Set,”](#) on page 111
- ♦ [Section 14.4.3, “Decommissioning the Old Server,”](#) on page 111

14.4.1 Using Designer to Remove the Old Server from the Driver Set

1 In Designer, open your project.

2 In the Modeler, right-click the driver set, then select *Properties*.

3 Select *Server List*.

4 Select the old Identity Manager server in the *Selected Servers* list, then click the < to remove the server from the *Selected Servers* list.

5 Click *OK* to save the changes.

- 6 Deploy the change to the Identity Vault.

For more information, see “Deploying a Driver Set to an Identity Vault” in *Designer 4.0 for Identity Manager 4.0 Administration Guide*.

14.4.2 Using iManager to Remove the Old Server from the Driver Set

- 1 In iManager, click  to display the Identity Manager Administration page.
- 2 Click *Identity Manager Overview*.
- 3 Browse to and select the container that holds the driver set.
- 4 Click the driver set name to access the Driver Set Overview page.
- 5 Click *Servers > Remove Server*.
- 6 Select the old Identity Manager server, then click *OK*.

14.4.3 Decommissioning the Old Server

At this point, the old server is not hosting any drivers. If you no longer need this server, you must complete additional steps to decommission it:

- 1 Remove the eDirectory replicas from this server.

For more information, see “Deleting Replicas” (<http://www.novell.com/documentation/edir88/edir88/data/fbgciaad.html>) in the *eDirectory Administration Guide* (<http://www.novell.com/documentation/edir88/pdfdoc/edir88/edir88.pdf>).

- 2 Remove eDirectory from this server.

For more information, see TID 10056593, “Removing a Server From an NDS Tree Permanently” (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=10056593&sliceId=&docTypeID=DT_TID_1_1&dialogID=35218849&stateId=0%20%202035214815).

Uninstalling Identity Manager

IV

If you need to uninstall any of the Identity Manager, you must uninstall each component.

- ♦ [Chapter 15, “Uninstalling the Identity Manager Components,” on page 115](#)

Uninstalling the Identity Manager Components

15

Uninstall the Identity Manager components in the order listed.

- ♦ Section 15.1, “Removing Objects from eDirectory,” on page 115
- ♦ Section 15.2, “Uninstalling the Metadirectory Server,” on page 116
- ♦ Section 15.3, “Uninstall the Remote Loader,” on page 116
- ♦ Section 15.4, “Uninstalling the Roles Based Provisioning Module,” on page 117
- ♦ Section 15.5, “Uninstalling the Identity Reporting Module Components,” on page 119
- ♦ Section 15.6, “Uninstalling iManager,” on page 119
- ♦ Section 15.7, “Uninstalling eDirectory,” on page 120
- ♦ Section 15.8, “Uninstalling Analyzer,” on page 121
- ♦ Section 15.9, “Uninstalling Designer,” on page 121
- ♦ Section 15.10, “Uninstalling the Role Mapping Administrator,” on page 122

15.1 Removing Objects from eDirectory

The first step in uninstalling Identity Manager is to delete all Identity Manager objects from the Identity Vault. If any driver set objects are partition root objects in eDirectory, the partition must be merged into the parent partition before the driver set object can be deleted. When the driver set is created, the wizard prompts you to make the driver set a partition.

- 1 Perform a health check on the eDirectory database. If any errors occur, fix the errors before proceeding.

For more information, see [Keeping eDirectory Healthy \(http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html\)](http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html) in the *Novell eDirectory 8.8 Administration Guide*.

- 2 Log in to iManager as an administrator user with full rights to the eDirectory tree.
- 3 Select *Partitions and Replica > Merge Partition*.
- 4 Browse to and select the driver set object that is the partition root object, then click *OK*.
- 5 Wait for the merge process to complete, then click *OK*.
- 6 Delete the driver set object.

When you delete the driver set object, it deletes all of the driver objects associated with that driver set.

- 7 Repeat [Step 3](#) through [Step 6](#) for each driver set object that is in the eDirectory database, until they are all deleted.
- 8 Repeat [Step 1](#) to make sure all merges completed and all of the objects have been deleted.

15.2 Uninstalling the Metadirectory Server

When Identity Manager is installed, there is an uninstall script that is placed on the Identity Manager server. It allows you to remove all services, packages, and directories that were created when Identity Manager was installed.

- ♦ [Section 15.2.1, “Uninstalling on Linux/UNIX,” on page 116](#)
- ♦ [Section 15.2.2, “Uninstalling on Windows,” on page 116](#)
- ♦ [Section 15.2.3, “Uninstalling a Non-root Installation,” on page 116](#)

15.2.1 Uninstalling on Linux/UNIX

To uninstall Identity Manager on Linux/UNIX, run the uninstall script located at `/root/idm/Uninstall_Identity_Manager/Uninstall_Identity_Manager`. To execute the script, enter `./Uninstall_Identity_Manager`.

If you installed Identity Manager as a non-`root` user, the `idm` directory is placed in the directory of the user that installed Identity Manager.

15.2.2 Uninstalling on Windows

The procedure to uninstall the Metadirectory server is different for each of the supported Windows platforms.

- ♦ **Windows 2003 SP2 (32-bit and 64-bit):** In the Control Panel select *Add or Remove Programs > Identity Manager*, then click *Change/Remove*.
- ♦ **Windows 2008 SP1 (32-bit and 64-bit):** Click *Programs and Features > Identity Manager*, then right-click and select *Uninstall*.

15.2.3 Uninstalling a Non-root Installation

To uninstall a non-root installation of Identity Manager, you need to run the uninstall script as the user that installed Identity Manager. It is located `/eDirectory_Base_Directory/opt/novell/eDirectory/bin/idm-uninstall`.

The script cleans up the user rpm database created during the installation of Identity Manager.

15.3 Uninstall the Remote Loader

When the Remote Loader is installed, there is an uninstall script that is placed on the Remote Loader server. It allows you to remove all services, packages, and directories that are created when the Remote Loader is installed.

- ♦ [Section 15.3.1, “Uninstalling on Linux/UNIX,” on page 117](#)
- ♦ [Section 15.3.2, “Uninstalling on Windows,” on page 117](#)

15.3.1 Uninstalling on Linux/UNIX

To uninstall the Remote Loader on Linux/UNIX, run the uninstall script located at `/root/idm/Uninstall_Identity_Manager/Uninstall_Identity_Manager`. To execute the script, enter `./Uninstall_Identity_Manager`.

If you installed the Remote Loader as a non-`root` user, the `idm` directory is placed in the directory of the user that installed the Remote Loader.

15.3.2 Uninstalling on Windows

The procedure to uninstall the Remote Loader is different for each of the supported Windows platforms.

- ♦ **Windows 2003 SP2 (32-bit and 64-bit):** In the Control Panel, select *Add or Remove Programs > Identity Manager*, then click *Change/Remove*.
- ♦ **Windows 2008 SP1 (32-bit and 64-bit):** Click *Programs and Features > Identity Manager*, then right-click and select *Uninstall*.

15.4 Uninstalling the Roles Based Provisioning Module

There are multiple components for the Roles Based Provisioning Module and each component must be uninstalled.

- ♦ [Section 15.4.1, “Deleting the Drivers,” on page 117](#)
- ♦ [Section 15.4.2, “Uninstalling the User Application,” on page 117](#)
- ♦ [Section 15.4.3, “Uninstalling the Application Server and the Database,” on page 118](#)

15.4.1 Deleting the Drivers

You must delete the User Application driver and the Role and Resource Service driver.

- 1 Stop the User Application driver and the Role and Resource Service driver.
 - ♦ **Designer:** Right-click the driver line, then click *Live > Stop Driver*.
 - ♦ **iManager:** On the Driver Set Overview page, click the upper right corner of the driver, then click *Stop Driver*.
- 2 Delete the User Application driver and the Role and Resource Service driver.
 - ♦ **Designer:** Right-click the driver line, then click *Delete*.
 - ♦ **iManager:** On the Driver Set Overview page, click *Drivers > Delete drivers*, then click the driver you want to delete.

15.4.2 Uninstalling the User Application

- ♦ **Linux/UNIX:** Execute the uninstall script located at `/root/Roles_Based_Provisioning_Module_for_Novell_Identity_Manager/Uninstall_Roles_Based_Provisioning_Module_for_Novell_Identity_Manager`.

To execute the script, enter `./Uninstall\ Roles\ Based\ Provisioning\ Module\ for\ Novell\ Identity\ Manager`.

- ♦ **Windows:** The procedure to uninstall the User Application is different for each of the supported Windows platforms.
 - ♦ **Windows 2003 SP2 (32-bit and 64-bit):** In the Control Panel, select *Add or Remove Programs > Roles Based Provisioning Module*, then click *Change/Remove*.
 - ♦ **Windows 2008 SP1 (32-bit and 64-bit):** Click *Programs and Features > Roles Based Provisioning Module*, then right-click and select *Uninstall*.

15.4.3 Uninstalling the Application Server and the Database

The User Application runs on the following application servers and database.

Table 15-1 Supported Application Servers and Databases

Application Server	Database
JBoss 5.1.0	<ul style="list-style-type: none"> ♦ MS SQL 2008 ♦ MySQL Version 5.1 ♦ Oracle 11gR2 ♦ PostgreSQL 8.4.3
WebSphere 7.0	<ul style="list-style-type: none"> ♦ DB2 9.5b ♦ MS SQL 2008 ♦ Oracle 11gR2 ♦ PostgreSQL 8.4.3
WebLogic 10.3	<ul style="list-style-type: none"> ♦ MS SQL 2008 ♦ Oracle 11gR2 ♦ PostgreSQL 8.4.3

The following procedure explains how to uninstall JBoss and PostgreSQL. If you are using another application server and database, refer that product's documentation for instructions.

- ♦ **Linux/UNIX:** Execute the uninstall script located at `/opt/novell/idm/Postgres/JBossPostgreSQL_Uninstaller/Uninstall_JBossPostgreSQL`.
To execute the script, enter `./Uninstall_JBossPostgreSQL`.
- ♦ **Windows:** The procedure to uninstall JBoss and PostgreSQL is different for each of the supported Windows platforms.
 - ♦ **Windows 2003 SP2 (32-bit and 64-bit):** In the Control Panel, select *Add or Remove Programs > JBossPostgreSQL*, then click *Change/Remove*.
 - ♦ **Windows 2008 SP1 (32-bit and 64-bit):** Click *Programs and Features > JBossPostgreSQL*, then right-click and select *Uninstall*.

15.5 Uninstalling the Identity Reporting Module Components

The Identity Reporting Module consists of multiple components. Each component must be uninstalled in order to uninstall the Identity Reporting Module.

- ♦ [Section 15.5.1, “Deleting the Reporting Drivers,” on page 119](#)
- ♦ [Section 15.5.2, “Uninstalling the Identity Reporting Module,” on page 119](#)
- ♦ [Section 15.5.3, “Uninstalling the Event Auditing Service,” on page 119](#)

15.5.1 Deleting the Reporting Drivers

You must delete the Data Collection driver and the Managed System Gateway driver.

- 1 Stop the Data Collection driver and the Managed System Gateway driver.
 - ♦ **Designer:** Right-click the driver line, then click *Live > Stop Driver*.
 - ♦ **iManager:** On the Driver Set Overview page, click the upper right corner of the driver, then click *Stop Driver*.
- 2 Delete the Data Collection driver and the Managed System Gateway driver.
 - ♦ **Designer:** Right-click the driver line, then click *Delete*.
 - ♦ **iManager:** On the Driver Set Overview page, click *Drivers > Delete drivers*, then click the driver you want to delete.

15.5.2 Uninstalling the Identity Reporting Module

- ♦ **Linux:** Execute the uninstall script located at `/opt/novell/IdentityReporting/Uninstall_Identity Reporting`.

To execute the script, enter `./Uninstall\ Identity\ Reporting`.

- ♦ **Windows:** The procedure to uninstall the Identity Reporting Module is different for each of the supported Windows platforms.
 - ♦ **Windows 2003 SP2 (32-bit and 64-bit):** In the Control Panel, select *Add or Remove Programs > Identity Reporting*, then click *Change/Remove*.
 - ♦ **Windows 2008 SP1 (32-bit and 64-bit):** Click *Programs and Features > Identity Reporting*, then right-click and select *Uninstall*.

15.5.3 Uninstalling the Event Auditing Service

The Event Auditing Service (EAS) is supported only on Linux. Execute the uninstall script located at `/opt/novell/sentinel_eas/Uninstall_Event Auditing Service/Uninstall Event Auditing Service`. To execute the script, enter `./Uninstall\ Event\ Auditing\ Service`.

15.6 Uninstalling iManager

- ♦ **Linux:** As root, execute the uninstall script located at `/var/opt/novell/iManager/nps/UninstallerData/UninstalliManager`.

To execute the script, enter `./UninstalliManager`.

- ♦ **Windows:** The procedure to uninstall iManager is different for each of the supported Windows platforms.
 - ♦ **Windows 2003 SP2 (32-bit and 64-bit):** In the Control Panel, select *Add or Remove Programs > Novell iManager*, then click *Change/Remove*.
 - ♦ **Windows 2008 SP1 (32-bit and 64-bit):** Click *Programs and Features > Novell iManager*, then right-click and select *Uninstall*.

Tomcat and NICI are listed as separate entries in the Control Panel. If you are no longer using these programs, you can uninstall each program. If eDirectory is installed on this same server, NICI is required for eDirectory to continue to run. If you are not uninstalling eDirectory, do not uninstall NICI.

15.7 Uninstalling eDirectory

Before you uninstall eDirectory, you need to understand your eDirectory tree structure and replica placements, so you don't cause problems in the eDirectory tree.

Answer the following questions before uninstalling eDirectory:

- Is there more than one server in your tree?

If the answer is yes, proceed with the other questions in this list. If the answer is no, you can remove eDirectory.

- Does this server hold any master replicas?

If the answer is yes, you need to promote another server in the replica ring to be a master before you remove eDirectory. For more information, see “[Managing Partitions and Replicas](http://wwwtest.provo.novell.com/documentation/edir88/edir88/data/a2iiiik.html)” (<http://wwwtest.provo.novell.com/documentation/edir88/edir88/data/a2iiiik.html>) in the *Novell eDirectory 8.8 Administration Guide*.

- Does this server hold the only copy of a partition?

If the answer is yes, you must either merge this partition into the parent partition or add a replica of this partition to another server and make it the master replica holder. For more information, see “[Managing Partitions and Replicas](http://wwwtest.provo.novell.com/documentation/edir88/edir88/data/a2iiiik.html)” (<http://wwwtest.provo.novell.com/documentation/edir88/edir88/data/a2iiiik.html>) in the *Novell eDirectory 8.8 Administration Guide*.

After you make sure your eDirectory tree is ready, use the following procedure to uninstall eDirectory:

- 1 If this is a single-server tree, skip to [Step 2](#). Otherwise, perform a health check on the eDirectory database. If any errors occur, fix the errors before proceeding. For more information, see “[Keeping eDirectory Healthy](http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html)” (<http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html>) in the *Novell eDirectory 8.8 Administration Guide*.
- 2 Uninstall eDirectory.
 - ♦ **Linux/UNIX:** Execute the uninstall script located at `/opt/novell/eDirectory/sbin/nds-uninstall`.
To execute the script, enter `./nds-uninstall`.

- ♦ **Windows:** The procedure to uninstall eDirectory is different for each of the supported Windows platforms.
 - ♦ **Windows 2003 SP2 (32-bit and 64-bit):** In the Control Panel, select *Add or Remove Programs* > *Novell eDirectory*, then click *Change/Remove*.
 - ♦ **Windows 2008 SP1 (32-bit and 64-bit):** Click *Programs and Features* > *Novell eDirectory*, then right-click and select *Uninstall*.
- 3 (Conditional) If this is a multiple-server tree, delete any server-specific objects left in the tree, then perform another health check. This verifies that the server was properly removed from the tree.

For more information, see “Keeping eDirectory Healthy” (<http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html>) in the *Novell eDirectory 8.8 Administration Guide*.

15.8 Uninstalling Analyzer

- 1 Make sure Analyzer is closed.
- 2 Uninstall Analyzer:
 - ♦ **Linux:** Execute the uninstall script located at `<installation_directory>/analyzer/UninstallAnalyzer/Uninstall Analyzer for Identity Manager`.
To execute the script, enter `./Uninstall\ Analyzer\ for\ Identity\ Manager`.
 - ♦ **Windows:** The procedure to uninstall Analyzer is different for each of the supported Windows platforms.
 - ♦ **Windows 2003 SP2 (32-bit and 64-bit):** In the Control Panel, select *Add or Remove Programs* > *Analyzer for Identity Manager*, then click *Change/Remove*.
 - ♦ **Windows 2008 SP1 (32-bit and 64-bit):** Click *Programs and Features* > *Analyzer for Identity Manager*, then right-click and select *Uninstall*.

15.9 Uninstalling Designer

- 1 Make sure that Designer is closed.
- 2 Uninstall Designer.:
 - ♦ **Linux/UNIX:** Execute the uninstall script located at `<installation_directory>/designer/UninstallDesigner/Uninstall Designer for Identity Manager`.
To execute the script, enter `./Uninstall\ Designer\ for\ Identity\ Manager`.
 - ♦ **Windows:** The procedure to uninstall Designer is different for each of the supported Windows platforms.
 - ♦ **Windows 2003 SP2 (32-bit and 64-bit):** In the Control Panel, select *Add or Remove Programs* > *Designer for Identity Manager*, then click *Change/Remove*.
 - ♦ **Windows 2008 SP1 (32-bit and 64-bit):** Click *Programs and Features* > *Designer for Identity Manager*, then right-click and select *Uninstall*.

15.10 Uninstalling the Role Mapping Administrator

- 1 Access the installation directory of the Role Mapping Administrator.
This directory is defined during the installation, so it can be different for each installation.
- 2 From the command line, stop the Role Mapping Administrator by running the `stop` script.
 - ♦ **Linux:** `stop.sh`
To execute the script, enter `./stop.sh`
 - ♦ **Windows:** `stop.bat`
- 3 From the command line, run the `uninstall` script.
 - ♦ **Linux:** `rma-uninstall.sh [-h] [-s]`
 - ♦ `[-h]`: Specifies help.
 - ♦ `[-s]`: Specifies silent mode.To execute the script, enter `./rma-uninstall.sh`.
 - ♦ **Windows:** `rma-uninstall.bat [-h] [-s]`
- 4 Delete the installation directory.