

Novell Identity Manager

3.0.1

www.novell.com

INSTALLATION GUIDE

November 12, 2006



Novell[®]

Legal Notices

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

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

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. Please refer to 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 © 2005 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.novell.com/company/legal/patents/> and one or more additional patents or pending patent applications in the U.S. and in other countries.

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

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see [Novell's online documentation \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

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

eDirectory is a trademark of Novell, Inc.

exteNd is a trademark of Novell, Inc.

exteNd Director is a trademark of Novell, Inc.

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

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

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

NMAS is a trademark of Novell, Inc.

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

Novell Certificate Server is a trademark of Novell, Inc.

Novell Client is a trademark of Novell, Inc.

SUSE is a registered trademark of SUSE AG, a Novell business.

Third-Party Materials

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

Contents

About This Guide	7
1 Overview	9
1.1 An Introduction to Identity Manager	9
1.2 Changes in Terminology	11
1.3 What's New in Identity Manager?	11
1.3.1 Fixes included in Identity Manager 3.0.1	12
1.3.2 Designer for Identity Manager	12
1.3.3 Eclipse-based tools to customize the User Application	15
1.3.4 Entitlements for Workflow-Based Provisioning and Enhancements to Role-Based Entitlements	15
1.3.5 Novell Identity Manager User Application and Workflow-Based Provisioning	16
1.3.6 Novell Credential Provisioning Policies	17
1.4 Identity Manager Installation Programs and Services	17
1.4.1 Installation Programs	18
1.4.2 Services	19
1.5 System Requirements for Identity Manager	26
1.6 Recommended Deployment Strategies	33
1.7 Where To Get Identity Manager and Its Services	34
1.7.1 Installing Identity Manager 3	36
1.7.2 Activating Identity Manager 3 Products	36
2 Planning	37
2.1 Common Installation Scenarios	37
2.1.1 New Installation of Identity Manager	37
2.1.2 Using Identity Manager and DirXML 1.1a in the Same Environment	39
2.1.3 Upgrading from the Starter Pack to Identity Manager	41
2.1.4 Upgrading from Password Synchronization 1.0 to Identity Manager Password Synchronization	43
2.2 Planning the Project Management Aspects of Identity Manager Implementation	45
2.2.1 Novell Identity Manager Deployment	45
2.3 Planning the Technical Aspects of Identity Manager Implementation	51
2.3.1 Using Designer	51
2.3.2 Replicating the Objects that Identity Manager Needs on the Server	51
2.3.3 Managing Users on Different Servers Using Scope Filtering	53
3 Upgrading	57
3.1 Upgrade Paths	57
3.2 Upgrade Procedure	57
3.2.1 Exporting Drivers	57
3.2.2 Verifying Minimum Requirements	58
3.2.3 Upgrading the Engine	58
3.2.4 Upgrading the Remote Loader	59
3.3 Upgrading Password Synchronization	59
3.4 Upgrading from RNS to Novell Audit	60
3.5 Upgrading DirXML 1.1a Driver Configurations	60
3.6 Activating Identity Manager	60

4	Installing Identity Manager	61
4.1	Before You Install	61
4.2	Identity Manager Components and System Requirements	61
4.3	Installing Identity Manager on NetWare	61
4.4	Installing Identity Manager on Windows	68
4.5	Installing the Connected System Option on Windows	73
4.6	Installing Identity Manager on UNIX/Linux Platforms	76
4.7	Installing the Connected System Option on UNIX/Linux	80
4.8	Post-Installation Tasks	83
4.9	Installing a Custom Driver	83
5	Installing the User Application	85
5.1	Prerequisites	85
5.2	Installation and Configuration	86
5.3	Creating the User Application Driver	87
5.4	Installing the User Application	92
5.4.1	About the Installation Program	92
5.4.2	Selecting an Install Folder	95
5.4.3	Specifying MySQL Details	96
5.4.4	Specifying the Database Host and Port	97
5.4.5	Specifying the JBoss Server Settings	98
5.4.6	Selecting the JBoss Server Configuration Type	99
5.4.7	Enabling Novell Audit Logging	99
5.4.8	Configuring the User Application	101
5.4.9	Choosing a Database Platform	106
5.4.10	Specifying the Database Name and Privileged User	107
5.4.11	Post-Install Tasks	108
5.4.12	Testing the Install	108
5.5	Troubleshooting	108
6	Activating Novell Identity Manager Products	111
6.1	Purchasing an Identity Manager Product License	111
6.2	Activating Identity Manager Products Using a Generic Credential	111
6.3	Installing a Product Activation Credential	113
6.4	Viewing Product Activations for Identity Manager and Drivers	113

About This Guide

Novell® Identity Manager, formerly DirXML®, 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 provides an overview of the Identity Manager technologies, and also describes installation, administration, and configuration functions.

In this guide:

- ♦ Chapter 1, “Overview,” on page 9
- ♦ Chapter 2, “Planning,” on page 37
- ♦ Chapter 3, “Upgrading,” on page 57
- ♦ Chapter 4, “Installing Identity Manager,” on page 61
- ♦ Chapter 5, “Installing the User Application,” on page 85
- ♦ Chapter 6, “Activating Novell Identity Manager Products,” on page 111

Documentation Updates

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

Documentation Conventions

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

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

- ◆ [Section 1.1, “An Introduction to Identity Manager,” on page 9](#)
- ◆ [Section 1.2, “Changes in Terminology,” on page 11](#)
- ◆ [Section 1.3, “What’s New in Identity Manager?,” on page 11](#)
- ◆ [Section 1.4, “Identity Manager Installation Programs and Services,” on page 17](#)
- ◆ [Section 1.5, “System Requirements for Identity Manager,” on page 26](#)
- ◆ [Section 1.6, “Recommended Deployment Strategies,” on page 33](#)
- ◆ [Section 1.7, “Where To Get Identity Manager and Its Services,” on page 34](#)

1.1 An Introduction to Identity Manager

Novell® Identity Manager is an award-winning data-sharing and synchronization solution that revolutionizes how you manage data. This service leverages a central datastore, your Identity Vault, to synchronize, transform, and distribute information across applications, databases, and directories.

When data from one system changes, the Metadirectory engine included in Identity Manager detects and propagates these changes to other connected systems based on the business rules you define. This solution enables you to enforce authoritative data sources for any particular piece of data (for example, an HR application owns a user's ID, while a messaging system might own a user's e-mail account information).

Identity Manager lets a connected system (such as SAP*, PeopleSoft*, Lotus Notes*, Microsoft* Exchange, Active Directory*, and others) do the following:

- ◆ Share data with the Identity Vault.
- ◆ Synchronize and transform shared data with the Identity Vault when it is modified in connected systems.
- ◆ Synchronize and transform shared data with connected systems when the data is modified in the Identity Vault.

Identity Manager does this by providing a bidirectional framework that allows administrators to specify which data flows from the Identity Vault to the application and from the application to the Identity Vault. The framework uses XML to provide data and event translation capabilities that convert Identity Vault data and events into the specified application-specific format. It also converts application-specific formats into a format that can be understood by the Identity Vault. All interactions with the application take place using the application’s native API.

Identity Manager lets you select only the attributes and classes that correspond to relevant connected system-specific records and fields. For example, a directory datastore can choose to share User-type objects with a Human Resources datastore, but not share network resource objects such as Servers, Printers, and Volumes. The Human Resources datastore can in turn share users’ given names, surnames, initials, telephone numbers, and work locations with a but not share the users’ family information and employment history.

If the Identity Vault doesn’t have classes or attributes for data you want to share with other applications, you can extend the eDirectory schema to include them. In this case, your Identity Vault becomes a repository of information that it does not need, but which other applications can use. The

application-specific datastore maintains the repository for the information that is required only by the application.

Identity Manager accomplishes the following tasks:

- ◆ Uses events to capture changes in the Identity Vault.
- ◆ Centralizes or distributes data management by acting as a hub to pull all data together.
- ◆ Exposes directory data in XML format, allowing it to be used and shared by XML applications or applications integrated through Identity Manager.
- ◆ Controls the flow of data using specific filters that govern data elements defined in the system.
- ◆ Enforces authoritative data sources by using permissions and filters.
- ◆ Applies rules to datastore data that is in an XML format. These rules govern the interpretation and transformation of the data as changes flow through Identity Manager.
- ◆ Transforms the data from XML into virtually any data format. This provides Identity Manager the ability to share data with any application.
- ◆ Carefully maintains associations between Identity Vault objects and objects within all other integrated systems, in order to ensure that data changes are appropriately reflected across all connected systems.

With Identity Manager, your business can simplify HR processes, reduce data management costs, build customer relationships through highly customized service, and remove interoperability barriers that inhibit success. Below are several example activities that Identity Manager enables:

Table 1-1 *What Identity Manager Can Do For You*

Activity	Identity Manager Solution
Manage User Accounts	<p>With a single operation:</p> <p>Identity Manager almost immediately grants or removes access for an employee to resources.</p> <p>Identity Manager provides automated employee provisioning capability, to give a new employee access to network, e-mail, applications, resources, and so forth.</p> <p>Identity Manager can also restrict or disable access upon termination or leave.</p>
Track and Integrate Asset Inventory	<p>Identity Manager can add profiles for all asset inventory items (computers, monitors, phones, library resources, chairs, desks, etc.) to the Identity Vault and integrate them with user profiles such as individuals, departments, or organizations.</p>
Automate White/Yellow Page Directories	<p>Identity Manager can create unified directories with varying levels of information for internal and external use. External directories might contain only e-mail addresses; internal directories might include location, phone, fax, cell, home address, etc.</p>
Enhance User Profiles	<p>Identity Manager augments user profiles by adding or synchronizing information such as e-mail address, phone number, home address, preferences, reporting relationships, hardware assets, phone, keys, inventory, and more.</p>

Activity	Identity Manager Solution
Unify Communications Access	Identity Manager simplifies network, phone, pagers, Web, or wireless access for individual users or groups by synchronizing directories for each to a common management interface.
Strengthen Partner Relationships	Identity Manager strengthens partnerships by creating profiles (employee, customer, etc.) in partner systems outside the firewall to enable partners to provide immediate service as needed.
Improve the Supply Chain	Identity Manager improves customer services by recognizing and consolidating instances of multiple accounts per customer.
Build Customer Loyalty	Identity Manager offers new services in response to recognizing customer needs as a result of viewing data in one place that was previously isolated in separate applications or areas.
Customize Service	<p>Identity Manager provides users (employees, customers, partners, etc.) with profiles complete with synchronized information, including relationships, status, and service records.</p> <p>These profiles can be used to provide varying levels of access to services and information, and offer real-time, customized services based on a customer's standing.</p>

1.2 Changes in Terminology

The following terms have changed from earlier releases:

Table 1-2 *Changes in Terminology*

Earlier Terms	New Terms
DirXML®	Identity Manager
DirXML Server	Metadirectory server
DirXML engine	Metadirectory engine
eDirectory	Identity Vault (except when referring to eDirectory attributes or classes)

1.3 What's New in Identity Manager?

Identity Manager has the following new features:

- ◆ [Section 1.3.1, “Fixes included in Identity Manager 3.0.1,” on page 12](#)
- ◆ [Section 1.3.2, “Designer for Identity Manager,” on page 12](#)
- ◆ [Section 1.3.3, “Eclipse-based tools to customize the User Application,” on page 15](#)
- ◆ [Section 1.3.4, “Entitlements for Workflow-Based Provisioning and Enhancements to Role-Based Entitlements,” on page 15](#)

- ◆ Section 1.3.5, “Novell Identity Manager User Application and Workflow-Based Provisioning,” on page 16
- ◆ Section 1.3.6, “Novell Credential Provisioning Policies,” on page 17

1.3.1 Fixes included in Identity Manager 3.0.1

For a list of defect fixes included in Identity Manager 3.0.1, see [TID 3351724 \(http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3351724&sliceId=SAL_Public&dialogID=9004727&stateId=0%200%209012373\)](http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3351724&sliceId=SAL_Public&dialogID=9004727&stateId=0%200%209012373).

1.3.2 Designer for Identity Manager

Identity Manager includes an extremely flexible and powerful modeling tool, Designer 1.2. Designer is a standalone client application that enables you to design, deploy, and document Identity Manager-based solutions in a highly productive environment.

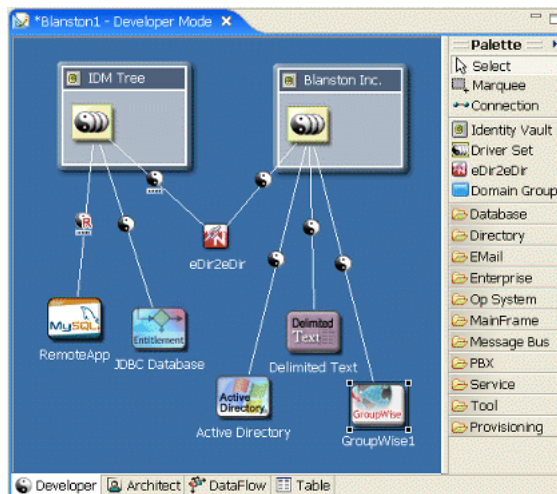
Using Designer, you can do the following:

- ◆ Design solutions locally, test them, then deploy solutions to the network.
- ◆ Import existing solutions from the network into Designer and work on them.
- ◆ Interact with your deployed solution to update any setting and view the state of any driver or system.

Designer has most of the configuration capabilities that are available in Novell iManager, plus new capabilities and advantages for designers. Some of the tasks you can perform in Designer include:

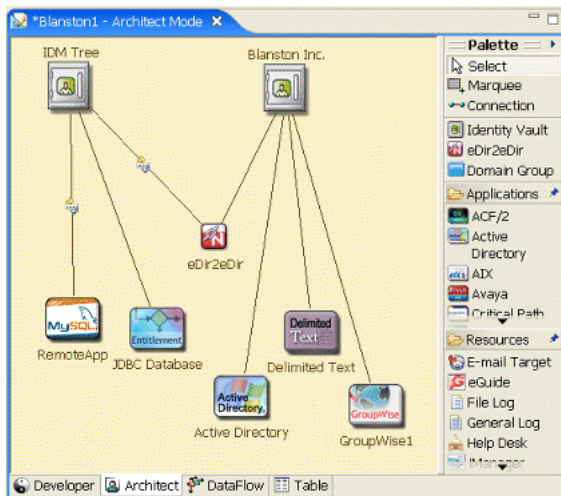
- ◆ Use powerful modeling to create the big picture of Identity management for your enterprise, with all Identity Manager components, end-systems and applications, and other visual elements. Divide the big picture into smaller connected pictures by organizing the systems into groups. Pan, scan, and zoom. Model application subsystems, eDir-to-eDir, and multiple drivers connecting to one system, in a way never possible before.

Figure 1-1 *Creating the Big Picture Is Simple In Designer*



- ◆ Work in different modes as either a high-level architect or a low-level developer, and easily transition from one to the other.

Figure 1-2 Choose Between Developer and Architect Modes



- ◆ Visually see and manipulate how data flows across the entire enterprise.
- ◆ With the push of a button, document your solution with detailed tables, charts, and graphics of all of your systems. You can document policies, schema, Identity Manager components, custom content, and project information, including a table of contents, appendix, and page numbering. You can strongly customize both the content and format of your document.
- ◆ Use the built-in policy simulator and Identity Manager engine to test your policies off-line.
- ◆ Easily create, copy, move, and share projects that span an entire enterprise. Because projects are local and file based, you can easily back up and version your entire solution.
- ◆ Use instant project-wide search and edit capabilities.
- ◆ Work in a highly productive rich-client environment, with a native look and feel.
- ◆ Work well in a disconnected mobile environment for when you're “on the go.”
- ◆ Use strong visual editors, minimal pop-ups, and well-synchronized views laid out to maximize productivity.
- ◆ Use wizards to help you get started and configure projects.
- ◆ Auto-create of objects, auto-value, auto-connection, auto-layouts.
- ◆ Use strong copy/paste within and across editors, as well as full undo/redo in most editors and views.
- ◆ Set many preferences and options that tailor the UI to how you want to use the product.
- ◆ Get help thorough contextual help and a powerful searchable help system.
- ◆ Auto-update installation notifies you of any updates and easily pulls them in.

Designer also comes with a number of features for developers:

- ◆ You can easily add and model something not in the shipping version. For example, you can add your own applications, drivers, resources, and icons.
- ◆ You can configure Designer to use a different editor. Configure all file types (for example, .xml and .txt) to use your editor of choice. Eclipse-based editors work best, but you can

also include various artifacts (for example, word processing documents and spreadsheets). The native editor is automatically integrated into Designer if the platform supports it.

- ◆ You can develop and debug in Java. If you install Designer plug-ins into a full Eclipse install, you can do Java development and debugging, ANT, C#, and UML modeling, all in the same tool alongside Designer. This has particular value to Identity Manager driver writers (Java or C) who want the tools all together.
- ◆ You can use public APIs. Novell is using fully published public Eclipse APIs, an underlying project data model that is consistent with open industry standards in its format, and also using published Eclipse extension points.

Audiences

Designer was created for the following audiences:

- ◆ Enterprise IT developers
- ◆ Consultants
- ◆ Sales engineers
- ◆ Architects or system designers
- ◆ System administrators

This tool is aimed at information technology professionals who:

- ◆ Have a strong understanding of directories, databases, and their information environment
- ◆ Act in the role of a designer or architect of identity-based solutions

You don't need to be a developer or programmer to fully make use of every aspect of this tool. We provide many capabilities for developers to extend this tool to suit their own needs. Wizards make this tool easy to learn and use in building Identity Management solutions. Experienced users can bypass the wizards and interact directly at any level of detail.

You can also use Designer as an effective and valuable tool to help communicate key Identity Solution concepts and design to strategic decision-makers in the organization. You can use both the visual Modeler and documentation that captures and displays Designer data.

How Designer Relates to the iManager Tools

iManager's primary use is for administration. iManager continues to be updated with new functionality for managing and monitoring deployed solutions. iManager's Web-based environment continues to have the following advantages:

- ◆ Remote access
- ◆ Centralized administration
- ◆ Support for roles
- ◆ Integration with other Web-based tools

iManager and Designer have similarities, but their features and end-user experience are optimized for their respective target users and environments. They are compatible. You can export information (for example, a driver set or a driver) from one application to the other. Also, several key common User Interface elements have been made similar so that you can move between the tools effectively.

1.3.3 Eclipse-based tools to customize the User Application

Identity Manager 3.0.1 also includes Designer 1.2. The latest version of Designer provides a powerful set of Eclipse-based design tools that can be used to customize the Identity Manager User Application. These tools include the directory abstraction layer editor and the provisioning request definition editor.

The directory abstraction layer editor allows you to modify the user applications behavior by:

- ◆ Adding new entities (Identity Vault objects)
- ◆ Defining the set of attributes for an entity
- ◆ Specifying the contents of lists
- ◆ Modeling relationships among entities
- ◆ Defining automatic lookups between entities

The provisioning request definition editor gives you complete control over the workflow design for a provisioning request. It lets you model the flow of user interactions needed to handle the provisioning request and its approvals. The provisioning editor allows you to:

- ◆ Define the basic characteristics of the provisioning request
- ◆ Design the associated workflow
- ◆ Define the request and approval forms
- ◆ Configure the activities and flow paths

Identity Manager ships with a set of provisioning request templates you can use to create your definitions. The templates model some common workflow design patterns. However, if you want to exercise complete control over the behavior of your workflows, you can create your provisioning request definitions from scratch.

For more information on designing user application components, see the *Identity Manager User Application Design Guide* (<http://www.novell.com/documentation/idm/dgpro/data/bookinfo.html>).

1.3.4 Entitlements for Workflow-Based Provisioning and Enhancements to Role-Based Entitlements

Identity Manager allows you to synchronize data between connected systems. Entitlements allow you to set up criteria for a person or group that, once met, initiate an event to grant or revoke access to business resources within the connected system. This gives you one more level of control and automation for granting and revoking resources.

There are two aspects to making entitlements work: creating the entitlement and managing the entitlement. You create entitlements through iManager or through Designer. To create an entitlement through iManager, select the *Create Entitlement* Option under the *Identity Manager Utilities* heading in iManager. For more information, see “**Creating and Using Entitlements**” in the *Novell Identity Manager 3.0.1 Administration Guide*.

You can also use Designer to create entitlements and deploy them into existing Identity Manager drivers. Designer allows you to create entitlements through the Entitlement Wizard, which gives you a graphical interface through which to create the entitlement, and steps you through the process. In iManager, you create entitlements through a simple interface, but you add additional properties

through an XML editor. Because it has a graphical interface, we recommend using Designer for creating and editing entitlements.

After you create entitlements (or use entitlements that come preconfigured with certain Identity Manager drivers), you need to manage them. Entitlements are managed by two packages or agents: iManager through Role-Based Entitlement Policies or with workflow-based provisioning through the User Application.

Role-Based Entitlement policies allow you to grant business resources if the criteria are met. For example, if a user meets criteria 1, 2, and 3, then a Role-Based Entitlement policy can add the user to Group H; but if the user meets criteria 4 and 5, he or she becomes a member of Group I. In order for this entitlement to work through workflow-based provisioning, approval is first required.

Entitlements created in Designer 1.2 won't work on Identity Manager engines earlier than Identity Manager 3.0. In Designer, you can access the Entitlements Wizard from the Modeler or from the Outline view.

- ◆ In the Outline view, right-click an Identity Manager driver. Select *Add Entitlement*.
- ◆ In the Modeler view, right-click a Driver object and select *Entitlements > Add Entitlement*.

1.3.5 Novell Identity Manager User Application and Workflow-Based Provisioning

The Novell Identity Manager User Application is a powerful Web application with supporting tools for provisioning. Workflow-based provisioning is the process of managing user access to secure resources in an organization. Users request resources and one or more individuals (including delegates or proxies) with approval rights can approve or deny the request. Users can also view the status of requests.

When used in conjunction with the Provisioning Module for Identity Manager and Novell Audit, the Identity Manager User Application provides a complete, end-to-end provisioning solution that's secure, scalable, and easy to manage.

The User Application offers the following Web-based end user functionality:

- ◆ White pages
- ◆ Organizational charts
- ◆ User search (with ability to save custom search configurations)
- ◆ Self-service password management
- ◆ Lightweight user administration tools
- ◆ Initiation and monitoring of provisioning requests (if the Provisioning Module is installed)
- ◆ Management of personal and/or team tasks (if the Provisioning Module is installed)
- ◆ Delegation and proxy capabilities
- ◆ Self-Service User Profile management (users can edit selected information on their public profiles)
- ◆ E-mail notification of provisioning tasks
- ◆ More than 85 portlets to create customized intranet pages for users as part of the Identity portal
- ◆ Support for self-provisioning and approval based provisioning workflows

For the system administrator, the User Application offers a rich assortment of configuration and administration capabilities, including:

- ◆ iManager plug-ins to allow setup and management of proxy and delegation rights
- ◆ Access to logging tools and customized Crystal Reports
- ◆ Wizard-based configuration of workflows (if the Provisioning Module is installed)
- ◆ Workflow management (if the Provisioning Module is installed), including enabling and disabling of workflows and suspension of flows in progress

Support for workflow-based provisioning is a key feature of Identity Manager 3 and is a separate purchase. Workflow-based provisioning is not supported in Identity Manager 2.

1.3.6 Novell Credential Provisioning Policies

Novell Credential Provisioning Policies for Identity Manager have been developed to enhance the user provisioning capabilities of any Identity Manager driver by providing the capability to simultaneously provision application credentials to the Novell SecretStore[®] and Novell SecureLogin credential repositories. Additionally, the product can provision the SecureLogin Passphrase question and answer in environments where non-repudiation capability is desired. These product capabilities enhance the User Single Sign-On (SSO) experience and increase the return on investment of SSO technologies by eliminating the initial setup of SecureLogin account information, providing additional security to application credentials, and reducing the replication of effort normally associated with provisioning SSO credential stores for users. It is important to note that the product can use IDM policies to automatically de-provision application credentials to prevent access to application data. For more information see “[Novell Credential Provisioning Policies](#)” in the *Policy Builder and Driver Customization Guide*.

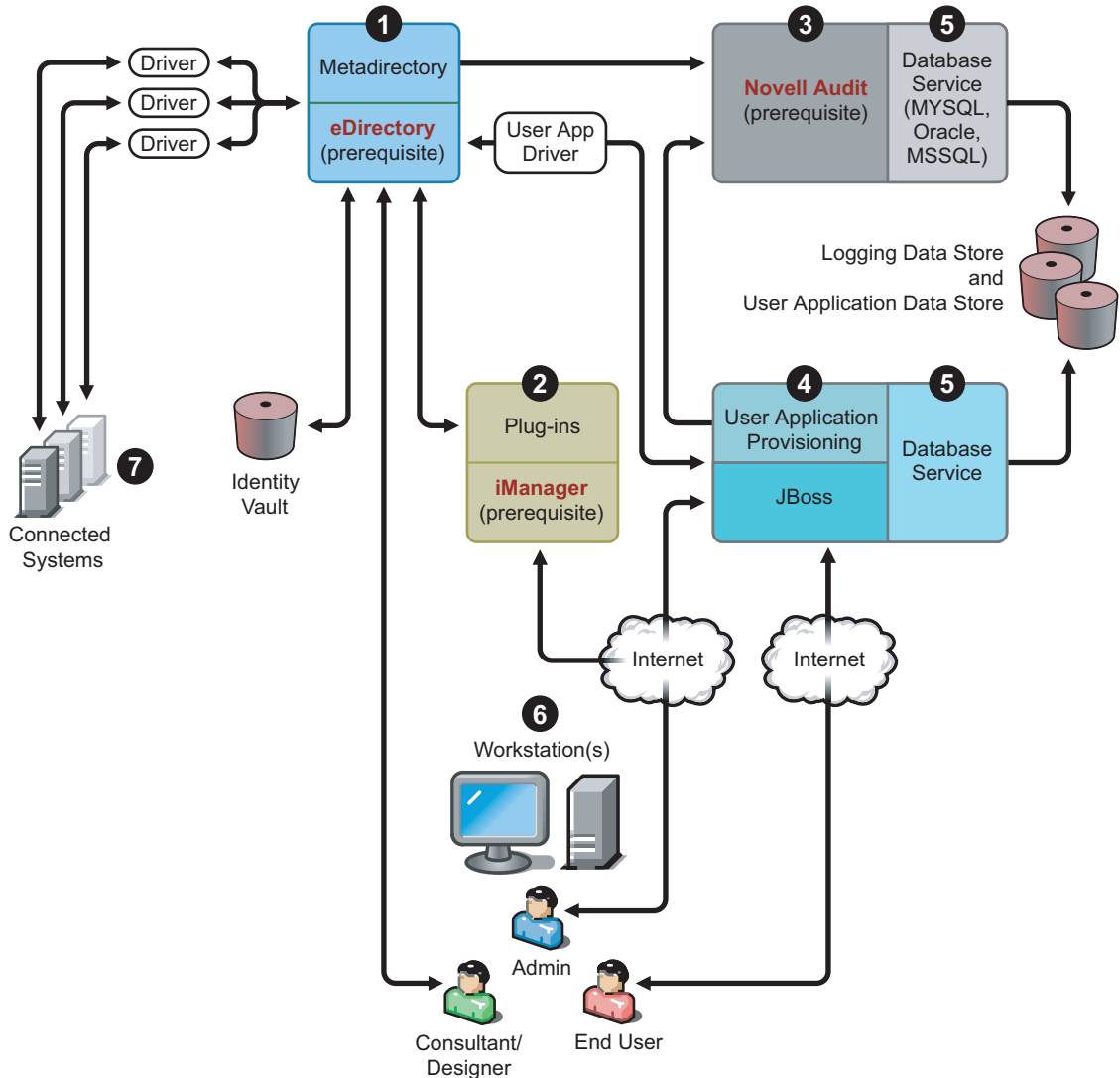
1.4 Identity Manager Installation Programs and Services

The following sections explain Identity Manager’s [Installation Programs](#) and [Services](#).

1.4.1 Installation Programs

Identity Manager has three distinct installation programs with seven services to install and configure.

Figure 1-3 Graphic Overview of the Seven Services That Identity Manager Offers



Below is the list of the installation programs and what each installation does:

- ♦ “Identity Manager Metadirectory System Installation” on page 19
- ♦ “User Application and Workflow Services for Provisioning Installation” on page 19
- ♦ “Designer Installation” on page 19

NOTE: Before installing Identity Manager components, you need to install prerequisite software including eDirectory 8.7.3 or later, iManager 2.5 or later, and Novell Audit 1.0.3 Starter Pack. You can get the prerequisite software from [Novell’s Download Web site \(http://download.novell.com\)](http://download.novell.com).

Identity Manager Metadirectory System Installation

The installation process performs the following functions:

- ◆ Extends the eDirectory schema for the Identity Manager product as a whole.
- ◆ Installs the Metadirectory engine and system service.
- ◆ Installs the Identity Manager plug-ins for iManager.
- ◆ Installs the Metadirectory system Remote Loader (if selected).
- ◆ Installs the connected system drivers. (The drivers are installed, but dormant until initiated for use).
- ◆ Installs the Identity Manager reports, and any of the Metadirectory system utilities, and tools.

User Application and Workflow Services for Provisioning Installation

The following services are installed on Linux and Windows:

- ◆ JBoss and MySQL (if selected).
- ◆ The lightweight portal software and the directory abstraction layer software.
- ◆ The User Application portlets, and supporting software, including work flow end user tasks.
- ◆ The Workflow engine.

Designer Installation

There is an installer for Linux and one for Windows:

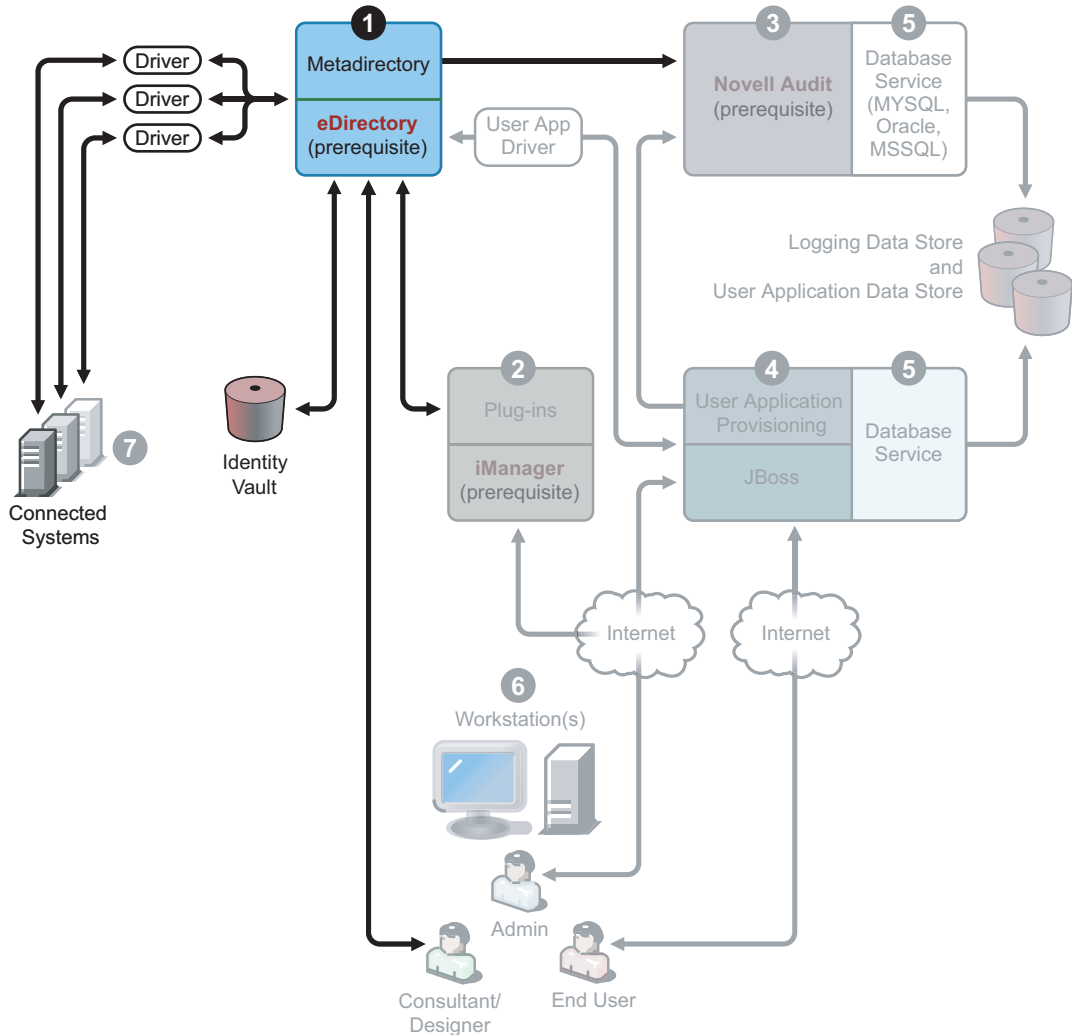
- ◆ Installs the Eclipse framework.
- ◆ Installs the foundational plug-ins.
- ◆ Installs the Metadirectory plug-ins.

1.4.2 Services

Identity Manager comes with seven services that you can install and configure. Although it's not recommended for a production environment, you can install and configure all seven services on a single computer. Or you can deploy one service per computer, or anything in between. The

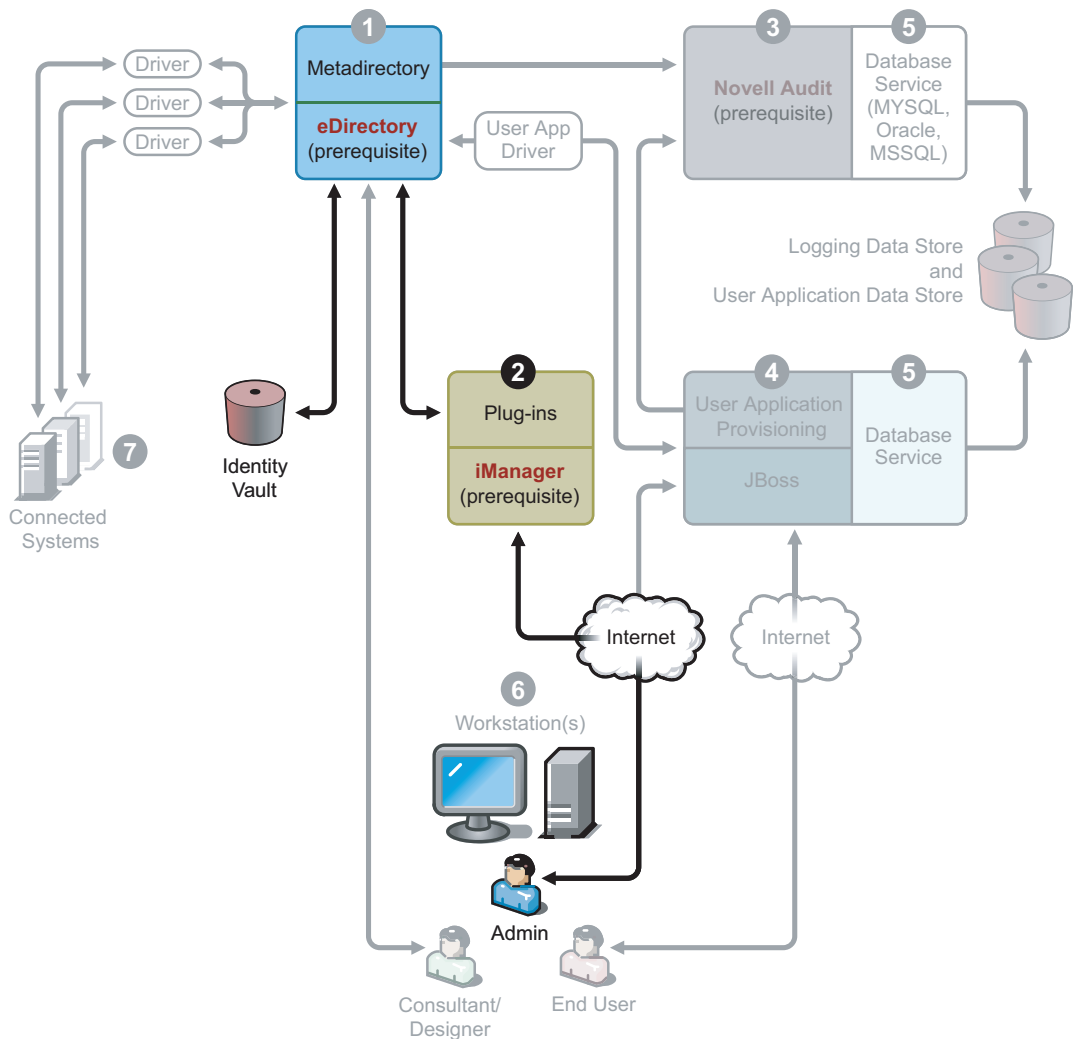
supported hardware and software prerequisites for each service are covered in [Section 1.5, “System Requirements for Identity Manager,”](#) on page 26.

Figure 1-4 *Metadirectory System Service*



1. The Metadirectory system service. This system is used as the Identity Vault, and you only need one instance of the Metadirectory engine in a production environment. To install Identity Manager and this service, see [Chapter 4, “Installing Identity Manager,”](#) on page 61.

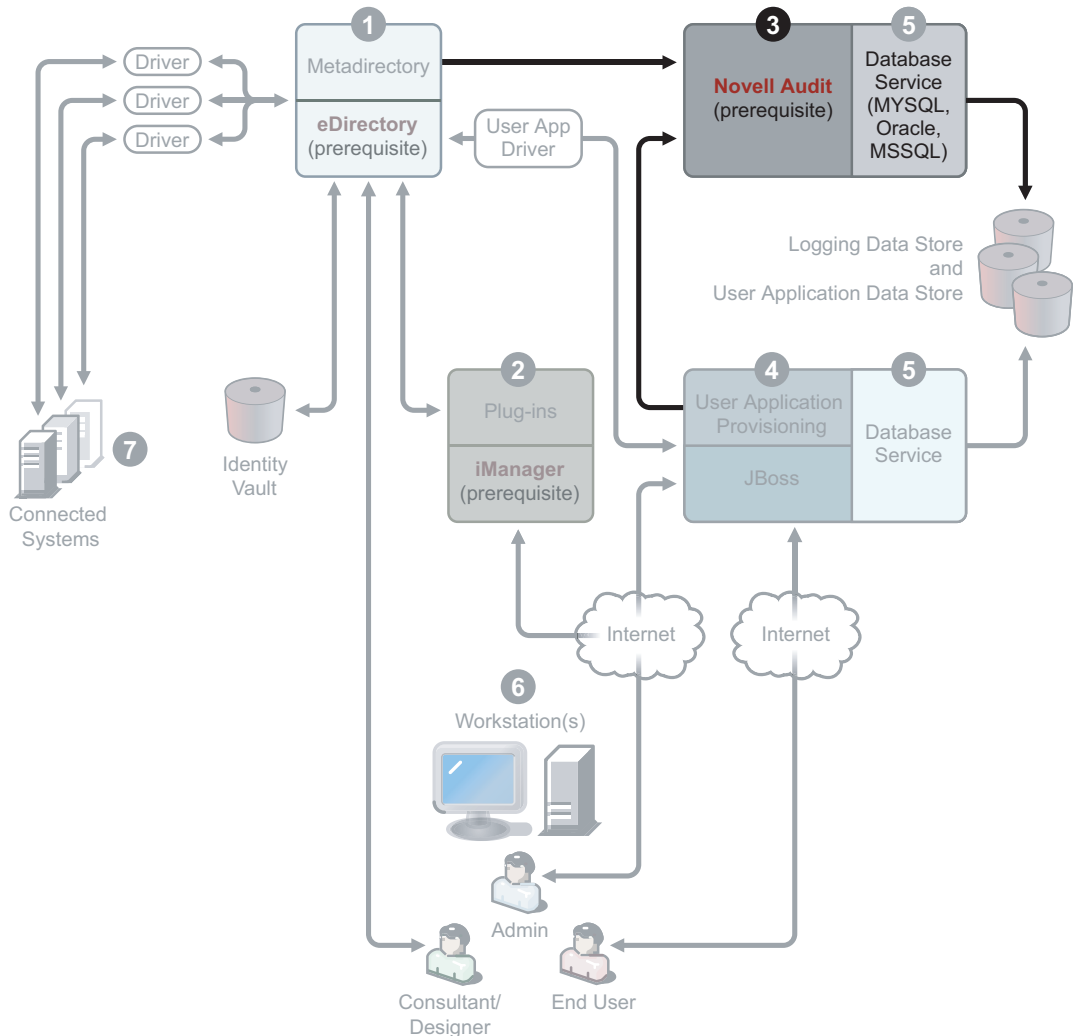
Figure 1-5 *Web-Based Administration Service*



2. The Web-based administration service. Use this service for the administration of eDirectory and the Metadirectory system using iManager 2.5 and above with Identity Manager and User Application plug-ins installed. You install Identity Manager plug-ins into iManager on the

server where you install Identity Manager. To install Identity Manager plug-ins and this service, see **Chapter 4, “Installing Identity Manager,”** on page 61.

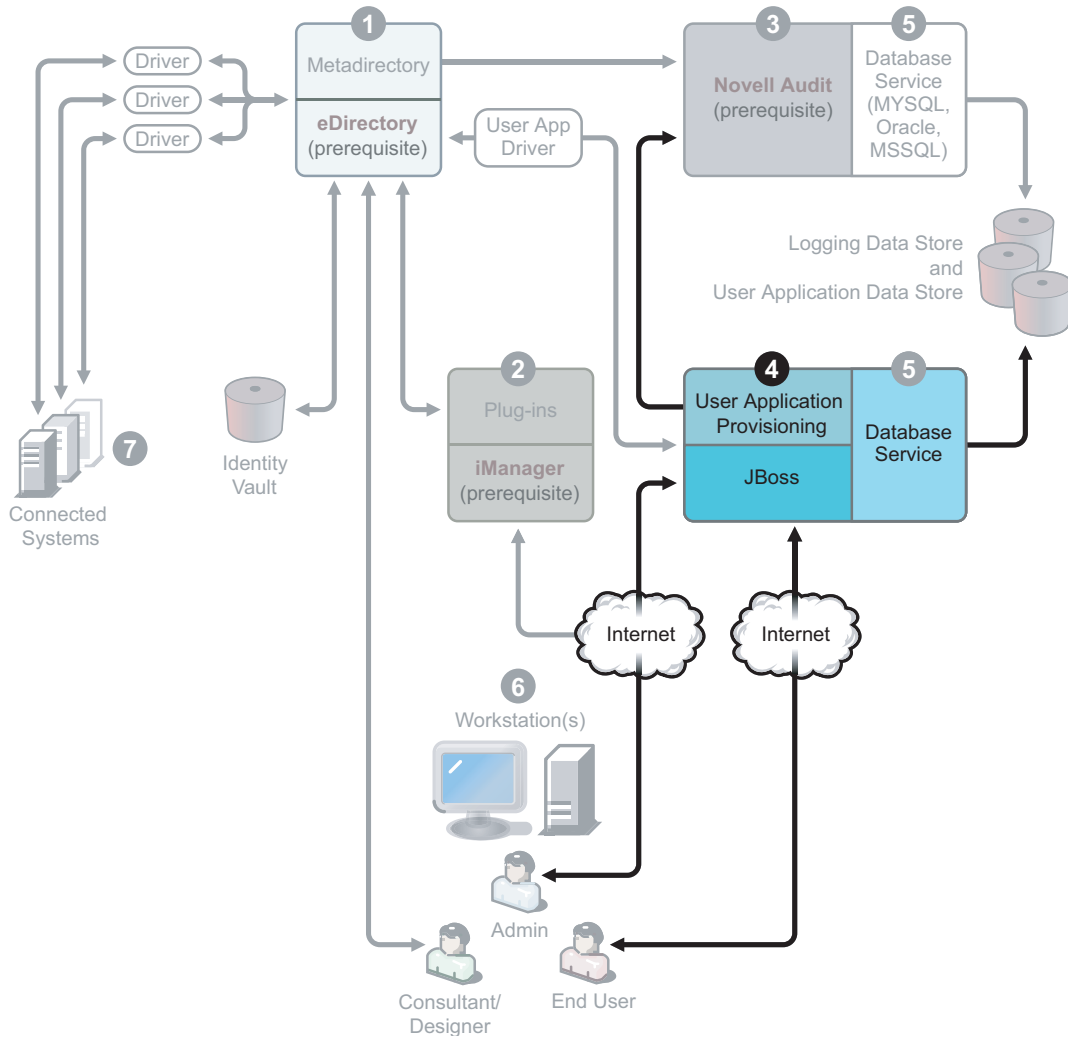
Figure 1-6 Secure Logging Service



3. The secure logging service. Repository for logging events (Identity Manager software is not installed on this server, but having a secure logging service is mandatory). This is a central service that is used by Identity Manager and the end-user application and workflow system services and is downloaded separately from Novell’s Download Web site (<http://download.novell.com>).

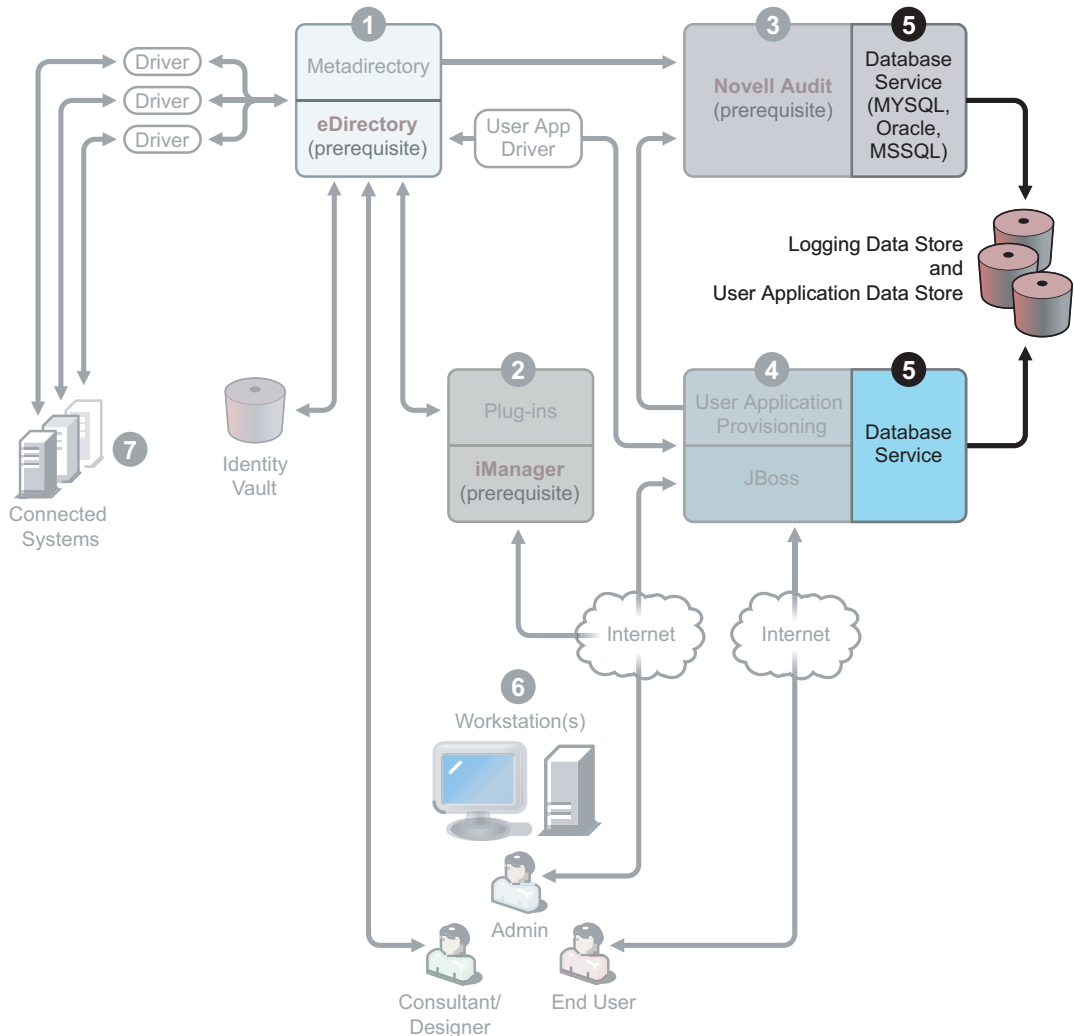
From the Product or Technology pull-down menu on the Download Web site, select *Novell Audit* and click *Search*. Click the *Novell Nsure Audit 1.0.3 Starter Pack*. Follow the installation instructions included with the Starter Pack.

Figure 1-7 User Application and Workflow-Based Provisioning Services



- The User Application and workflow-based provisioning services. To install this service, see Chapter 5, “Installing the User Application,” on page 85.

Figure 1-8 Database Service

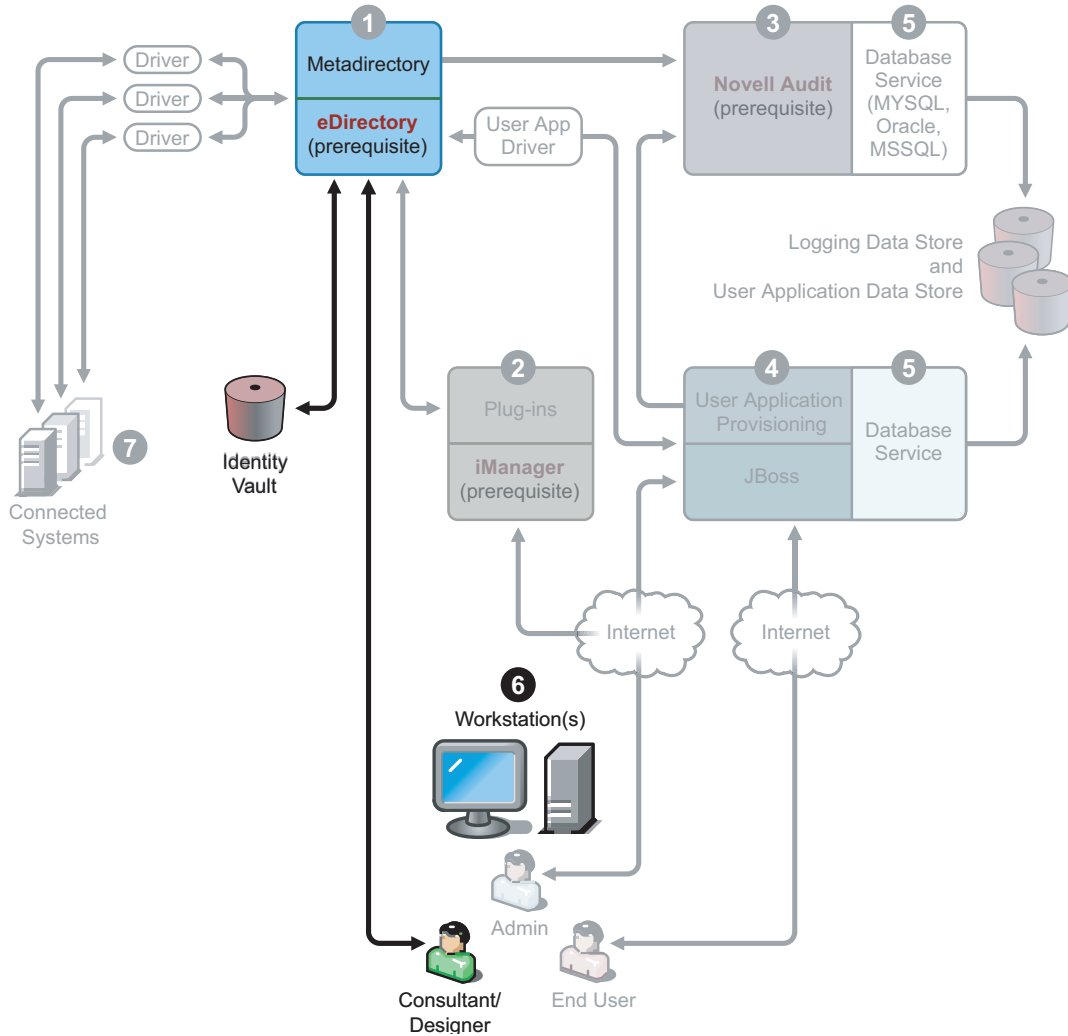


- The database service. Both the secure logging service and the end-user application/work flow system require a database. You can set up one database to serve both applications, or you can set up independent databases for each one.

The secure logging service does not include a specific database. However, you can use the MySQL database that comes with the User Application and Provisioning. The User Application comes with the JBoss Application Server Version 4.0.2, as well as with MySQL

Version 4.1.12. To install this service, see [Section 5.2, “Installation and Configuration,”](#) on page 86.

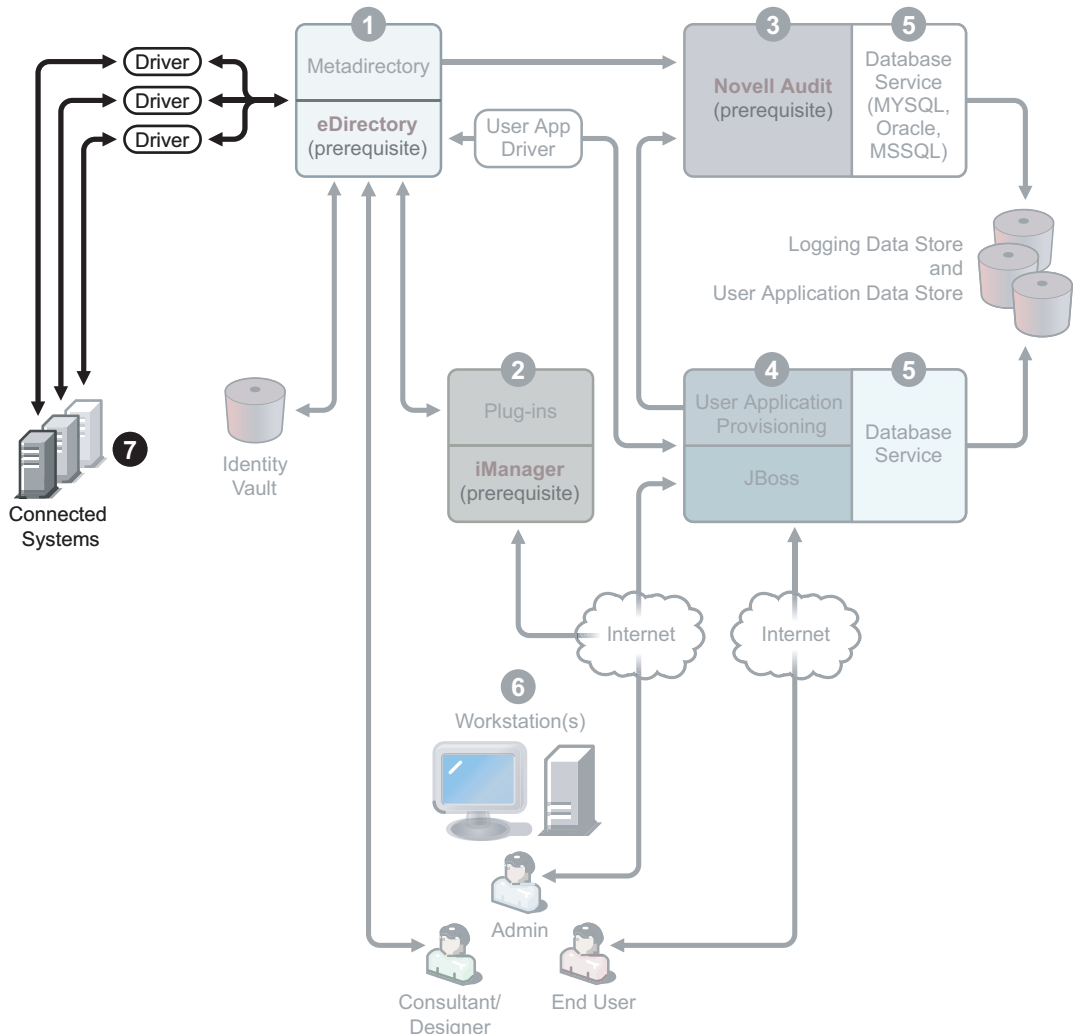
Figure 1-9 Workstation Services for Designer



6. Workstations. Used for Designer to design, deploy, and document the Identity Manager system and for utilities, reports, and tools included with the product. To install Designer on a

workstation, see “**Installing Designer**” in the *Designer for Identity Manager 3: Administration Guide*.

Figure 1-10 Connected Systems



7. Connected systems. This is where the drivers are hosted and these connected systems can be applications, databases, servers, and other services. Each connected application requires individuals with application-specific knowledge and responsibility. Each driver requires that the connected system be available and the relevant APIs provided.

You install the drivers as part of the Identity Manager installation process. To install Identity Manager and this service, see **Chapter 4, “Installing Identity Manager,”** on page 61. To learn more about configuring drivers, you should read the driver-specific documentation on the [Identity Manager Drivers Documentation Web site \(http://www.novell.com/documentation/idmdrivers\)](http://www.novell.com/documentation/idmdrivers).

1.5 System Requirements for Identity Manager

Novell Identity Manager contains components that can be installed within your environment on multiple systems and platforms. 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.

The following table lists the installation components of Identity Manager and requirements for each.

Table 1-3 *Identity Manager System Components and Requirements*

System Component	System Requirements	Notes
Metadirectory System	One of the following operating systems:	Using VMWare in your implementation is supported if you use a Metadirectory system platform.
<ul style="list-style-type: none"> ◆ Metadirectory engine ◆ Novell Audit agent ◆ Service drivers ◆ Identity Manager Drivers ◆ Utilities (including Application Tools, and the Novell Audit Setup tool) 	<ul style="list-style-type: none"> ◆ NetWare® 6.5 with the latest Support Pack ◆ Novell Open Enterprise Server (OES) 1.0 with the latest Support Pack ◆ Windows* NT ◆ Windows 2000 Server with the latest Service Pack (32-bit) ◆ Windows Server 2003 R2 with the latest Service Pack (2003 64-bit is not supported) ◆ Linux Red Hat* AS 3.0 ◆ Linux Red Hat AS 4.0 for AMD 64/EM64T ◆ SUSE® Linux Enterprise Server 8, 9, or 10 with the latest Support Pack ◆ Solaris 8, 9, or 10 ◆ AIX 5.2L 	<p>Unless specified otherwise, OES, NetWare, Windows, and Linux platforms (Red Hat and SUSE) support all of the following processors in 32-bit mode:</p> <ul style="list-style-type: none"> ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 and Opteron <p>eDirectory 8.8 and later supports these advanced features:</p> <ul style="list-style-type: none"> ◆ Multiple instances of eDirectory on the same server ◆ Encrypted attributes <p>Non-root installations of eDirectory are not currently supported with Identity Manager.</p> <p>eDirectory 8.8.1 supports 64-bit Red Hat Linux AS and ES 4.0. However, eDirectory 8.8.x does not support Solaris 8.</p>
	One of the following versions of eDirectory.:	Be sure to completely back up the eDirectory database before installing eDirectory 8.8.1. eDirectory 8.8.1 upgrades portions of the database structure and won't allow it to be rolled-back after the upgrade process.
	<ul style="list-style-type: none"> ◆ eDirectory 8.7.3 with the latest Support Pack (SP8 or later) ◆ eDirectory 8.8 with the latest Support Pack ◆ eDirectory 8.8.1 with the latest Support Pack 	<p>Xen virtualization is now supported on SUSE Linux Enterprise Server 10 when the Xen Virtual Machine (VM) is running SLES 10 as the guest operating system in paravirtualized mode. An Xen patch for SLES 10 is needed (see TID #3915180 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3915180&sliceId=SAL_Public&dialogID=20406933&stateId=0%20%2020414606)).</p>
	We recommend upgrading eDirectory 8.8 to 8.8.1.	Novell expects to drop support for SLES 8 and Solaris 8 after Identity Manager 3.0.1.

System Component	System Requirements	Notes
Web-based Administration Server	<p>One of the following operating systems:</p> <ul style="list-style-type: none"> ◆ Identity Manager and Password Management ◆ iManager 2.5 or 2.6 and plug-ins ◆ Driver configurations <ul style="list-style-type: none"> ◆ Novell Open Enterprise Server (OES) with the latest Support Pack ◆ NetWare 6.5 with the latest Support Pack ◆ Windows 2000 Server with the latest Service Pack (32-bit) ◆ Windows Server 2003 R2 with the latest Service Pack (2003 64-bit is not supported) ◆ Windows XP Professional (Mobile iManager only) ◆ Red Hat Linux AS 3.0 (Glibc version 2.1.1 or later and kernel version 2.2.xx or later.) ◆ Red Hat Linux AS 4.0 for AMD 64/EM64T (iManager 2.6 SP1 only) ◆ Red Hat Linux 8 (iManager 2.5 FP3 only) ◆ Red Hat Linux 9 (iManager 2.5 FP3 only) ◆ Solaris 9 ◆ Solaris 10 (iManager 2.6 SP1 only) ◆ SUSE Linux Enterprise Server 8, 9, or 10 with the latest Support Pack <p>Operating systems supported via iManager Workstation:</p> <ul style="list-style-type: none"> ◆ Windows 2000 Professional with latest Service Pack ◆ Windows XP ◆ Red Hat Enterprise Linux Workstation (Mobile iManager 2.5 FP3 only) ◆ SUSE Linux 9.1 (Mobile iManager 2.5 FP3 only) ◆ SUSE Linux 9.3 (Mobile iManager 2.6 SP1 only) <p>The following software.</p> <ul style="list-style-type: none"> ◆ Novell iManager 2.5 with latest Support Pack or iManager 2.6 Support Pack 2 or greater (includes Apache 2.0.52 or later and Tomcat 	<p>Unless stated otherwise, OES, NetWare, Windows, and Linux platforms (Red Hat and SUSE) support all of the following processors in 32-bit mode:</p> <ul style="list-style-type: none"> ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 and Opteron <p>◆ Browser support is determined by iManager 2.5 or 2.6. This list presently includes:</p> <ul style="list-style-type: none"> ◆ Internet Explorer 6, SP1 and above ◆ Firefox 1.5.0.x and above ◆ Mozilla 1.7 and above <ul style="list-style-type: none"> ◆ You must go through the iManager Configuration Wizard or the Designer utility to install or deploy portal content into eDirectory. ◆ If you install iManager 2.6 on the same server where eDirectory is installed, the version of eDirectory must be 8.7.3 or higher. ◆ (Windows) The Novell Client™ 4.9 is available from Novell Software Downloads (http://download.novell.com/index.jsp). ◆ When logging into other trees with iManager to manage remote Identity Manager servers, you might encounter errors if you use the server name instead of the IP address for the remote server. ◆ Novell expects to drop support for iManager 2.5 after Identity Manager 3.0.1.

System Component	System Requirements	Notes
Secure Logging Service	For the Secure Logging Server, one of the following operating systems:	OES, NetWare, Windows, and Linux platforms (Red Hat and SUSE) support all of the following processors in 32-bit mode:
<ul style="list-style-type: none"> ◆ The Secure Logging Server ◆ The Platform Agent (client component) 	<ul style="list-style-type: none"> ◆ Novell Open Enterprise Server (OES) with the latest Support Pack ◆ NetWare 6.5 with the latest Support Pack, NetWare 6.0 with latest Support Pack ◆ Windows 2000 Server with the latest Service Pack ◆ Linux Red Hat AS 3.0, AS, and ES 2.1 (Glibc version 2.1.1 or later and kernel version 2.2.xx or later.) ◆ Linux Red Hat AS 4.0 for AMD 64/EM64T ◆ Solaris 8, 9, or 10 ◆ SUSE Linux Enterprise Server 8, 9, or 10 ◆ Novell eDirectory 8.5 or later <p>For the Platform Agent, one of the following operating systems:</p> <ul style="list-style-type: none"> ◆ NetWare 5.1 and later (with the latest Support Pack) ◆ Windows 2000 or 2000 Server, XP, or Windows Server 2003 with the latest Service Pack (2003 64-bit is not supported) ◆ Linux Red Hat 7.3, 8, AS, and ES 2.1 ◆ Solaris 8, 9, or 10 ◆ SUSE Linux Enterprise Server 8 	<ul style="list-style-type: none"> ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 and Opteron <p>Minimum Secure Server requirements include:</p> <ul style="list-style-type: none"> ◆ A single processor, server-class PC with a Pentium* II 400 MHz ◆ A minimum of 40 MB disk space ◆ 512 MB RAM <p>The eDirectory Instrumentation, which allows eDirectory events to be logged, supports the following versions of eDirectory:</p> <ul style="list-style-type: none"> ◆ NDS® 8.x <p>eDirectory 8.6 (NetWare, Windows, Linux, and Solaris)</p> <ul style="list-style-type: none"> ◆ eDirectory 8.7 (NetWare, Windows, Linux, and Solaris) <p>The NetWare Instrumentation, which allows NetWare events to be logged, supports the following versions of NetWare:</p> <ul style="list-style-type: none"> ◆ NetWare 5.1 with the latest Support Pack ◆ NetWare 6.0 with the latest Support Pack ◆ NetWare 6.5 or NetWare 6.5 with the latest Support Pack ◆ Novell Open Enterprise Server (OES) with the latest Support Pack

System Component	System Requirements	Notes
User Application and Workflow System Service	SUSE Linux Enterprise Server 9 and 10 Windows Server 2000 SP4	Unless otherwise stated, SUSE Linux Enterprise Server supports all of the following processors in 32-bit mode:
<ul style="list-style-type: none"> ◆ Identity Vault access ◆ IDM User Application storage 	Windows Server 2003 SP1	<ul style="list-style-type: none"> ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 and Opteron <p>The User Application requires credentials to log in to the Identity Vault. The credentials used to access the Identity Vault must:</p> <ul style="list-style-type: none"> ◆ Have full rights to the Identity Vault ◆ Must exist in the Identity Vault before you install the Identity Manager 3 User Application. <p>You are prompted for these credentials during installation. This user is referred to as the User Application Administrator.</p> <p>The computer where you install the User Application must have 320 MB of storage available.</p> <p>Xen virtualization is now supported on SUSE Linux Enterprise Server 10 when the Xen Virtual Machine (VM) is running SLES 10 as the guest operating system in paravirtualized mode. An Xen patch for SLES 10 is needed (see TID #3915180 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3915180&sliceId=SAL_Public&dialogID=20406933&statelD=0%200%2020414606)).</p> <p>For Linux:</p> <ul style="list-style-type: none"> ◆ Runlevel. The User Application installer needs X Server (X Windows), so your Linux runlevel must be set to 5 or higher. ◆ It is recommended that you run the install as a user without root privileges. ◆ Make sure the install directory is writable. The User Application is typically installed using the directory structure <code>novell/idm</code> in the user's home directory, but you can change this default.

System Component	System Requirements	Notes
Database Server and Service	<p>Local access means that the database is running on the same box as the application server. Remote access means the product accesses the database across the wire.</p> <p>Included in the User Application product:</p> <ul style="list-style-type: none"> ◆ JBoss Application Server Version 4.0.2 <p>Included in the User Application product and works in both local and remote access:</p> <ul style="list-style-type: none"> ◆ MySQL Version 4.1.12 <p>The following databases are not included, but can be used in remote access only:</p> <ul style="list-style-type: none"> ◆ Oracle 9i (9.2.0.4) ◆ Oracle 10g (10.2.0.1.0) ◆ MS SQL 2000 SP4 	<p>NOTE: If you want to implement clustering, you must download and install JBoss 4.0.3 SP1.</p> <p>You can use the JBoss Application server to host the User Application and MySQL, or you can use another supported database. The User Application uses a database for various tasks, such as storing User Application configuration data and storing data for any in-progress workflow activities.</p> <p>Both the secure logging service and the User Application and workflow provisioning require a database. You can set up one database to serve both applications, or you can set up independent databases for each one. The secure logging service does not include a specific database.</p> <p>For JBoss:</p> <ul style="list-style-type: none"> ◆ The minimum recommended RAM for JBoss when running the User Application is 512 MB. ◆ The computer where JBoss is installed should have port 8080 free. JBoss allows Tomcat to use port 8080 by default. You should install JBoss on a machine that has this port free. ◆ If the target machine also has an instance of iManager (or any other application that uses its own instance of Tomcat), you might end up with multiple Tomcat instances competing for the same port. You should either shut down other Tomcat instances or set the others to use a port other than 8080. <p>For MySQL:</p> <ul style="list-style-type: none"> ◆ The computer where MySQL is installed should have port 63306 free. The User Application installer installs MySQL at port number 63306 by default to avoid conflicts with any other MySQL server running on the machine.

System Component	System Requirements	Notes
<p>Workstations</p> <ul style="list-style-type: none"> ◆ Designer ◆ iManager Web access 	<p>Designer has been tested on the following platforms:</p> <p>Windows:</p> <ul style="list-style-type: none"> ◆ Windows 2000 Professional and Windows 2000 Server ◆ Windows XP Professional ◆ Windows Server 2003 R2 with the latest Service Pack (2003 64-bit is not supported) <p>Linux:</p> <ul style="list-style-type: none"> ◆ SUSE Linux Enterprise Server 9.2, 9.3, and 10 ◆ SUSE Linux Enterprise Server 9 SP1, SP2 ◆ SUSE Linux Enterprise Server 10 ◆ Red Hat Linux 9 ◆ Novell Linux Desktop ◆ GNOME, KDE, Red Hat Fedora 	<p>Designer uses Eclipse as its development platform. Refer to the Eclipse Web site (http://www.eclipse.org/) for platform-specific information.</p> <p>Designer minimum and recommended hardware requirements:</p> <ul style="list-style-type: none"> ◆ 1 GHz minimum; recommended 2 GHz or greater. ◆ 512 MB RAM minimum; recommended 1 GB RAM or greater. ◆ 1024 x 768 resolution minimum; recommended 1280 x 1024. <p>Prerequisite software:</p> <ul style="list-style-type: none"> ◆ Microsoft Internet Explorer 6.0 SP1 ◆ or Mozilla 1.7 ◆ or Mozilla Firefox 1.5.0.x
<p>Connected System Server (host on a separate server running Remote Loader)</p> <ul style="list-style-type: none"> ◆ Remote Loader ◆ Remote Loader configuration tool (Windows only) ◆ Novell Audit agent ◆ Driver shim for the connected system ◆ Tools for the connected system 	<p>Each driver requires that the connected system be available and the relevant APIs are provided.</p> <p>Refer to the Identity Manager Driver documentation (http://www.novell.com/documentation/idmdrivers) for operating system and connected system requirements that are specific to each system.</p>	<p>Each connected application requires individuals with application-specific knowledge and responsibility.</p> <p>Remote Loader System:</p> <ul style="list-style-type: none"> ◆ Windows NT 4.0, Windows 2000, or Windows 2003 ◆ Red Hat Linux AS 3.0 ◆ Linux Red Hat AS 4.0 for AMD 64/EM64T ◆ SUSE Linux Enterprise Server 8, 9, or 10 ◆ Solaris 8, 9, or 10 ◆ AIX 5L v5.2 <p>Java Remote Loader System:</p> <ul style="list-style-type: none"> ◆ HP-UX 11i ◆ OS/400 ◆ zOS ◆ Should be able to use on any system that has JVM 1.4.2 or higher

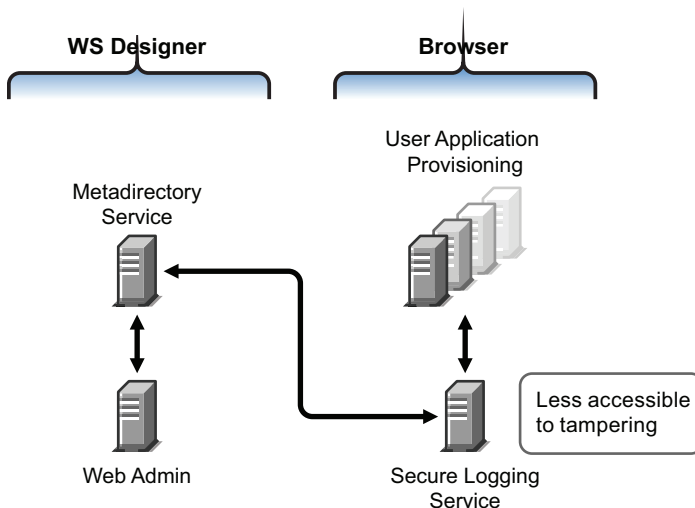
1.6 Recommended Deployment Strategies

As previously indicated, Identity Manager comes with seven services that you must install and configure. Although it's not recommended for a production environment, you can install and configure all seven services on a single server. Or you can deploy one service per server, or anything in between.

Workload is the main factor in designing Identity Manager deployments. The more traffic you can disperse, the better potential throughput your applications can have.

In Figure 1-3, we recommend one server for the Metadirectory service, one server for the Web-based administration service, one server for the secure logging service, and one server for user application and workflow-based provisioning service.

Figure 1-11 Recommended Approaches To Identity Manager Deployment



Metadirectory Service

How you deploy Identity Manager services depends on service workload. For instance, you can install Identity Manager's Metadirectory service on one server that communicates with the connected systems. You only need to install the Metadirectory engine on one server running eDirectory.

Because of potential heavy throughput with iManager, you might not want to install the Web-based administration service with the Metadirectory service. If you do install iManager on the same server as Identity Manager, install iManager first, then Identity Manager and its plug-ins.

Web-Based Administration Service

If you already have iManager 2.5 or 2.6 installed on a server, you only need to run the Identity Manager installation and install the Identity Manager plug-ins for iManager. If you are installing the User Application and workflow system service, you must also run the User Application installation and install only the User App plug-ins for iManager. You will need to do this for either the User Application or the User Application with Provisioning installations (they are two separate products).

User Application and Secure Logging Services

If you are performing a substantial amount of provisioning, we recommended that the User Application be installed on its own server. You can also set up clustering if needed. MySQL 4.1.12 is included with the User Application, and if it is deployed as part of the User Application install or as part of the User Application with workflow-based provisioning install, you do not need to set up another database service.

However, the secure logging service does not include a specific database, and both the secure logging service and the end-user application/workflow provisioning service require a database. You can set up one database to serve both applications, or you can set up independent databases for each service. This depends on how much provisioning you perform and on the logging service workload.

NOTE: If you want to setup Oracle 9i or 10g on a separate (remote) server, you will need to install Oracle, and configure the Application Server to provide a remote connection to the database.

Using the Remote Loader Configuration

You can use the *Connected System* option during the Identity Manager install if you don't want to install eDirectory services and the Metadirectory engine on a connected system server. The Remote Loader also provides a secure communication path between the Metadirectory engine and the driver using SSL technology. Keep this in mind when connecting systems to Identity Manager.

1.7 Where To Get Identity Manager and Its Services

- ◆ [Section 1.7.1, “Installing Identity Manager 3,” on page 36](#)
- ◆ [Section 1.7.2, “Activating Identity Manager 3 Products,” on page 36](#)

To download Identity Manager and its services, go to the [Novell Downloads Web site \(http://download.novell.com\)](http://download.novell.com).

1. In the *Product* or *Technology* menu, select *Novell Identity Manager*, then click *Search*.
2. On the Novell Identity Manager Downloads page, click the Download button next to a file you want.
3. Follow the on-screen prompts to download the file to a directory on your computer.
4. Repeat from Step 2 until you have downloaded all the files you need. Most installations require multiple ISO images.

The following Identity Manager components are available for download.

Table 1-4 *How the ISO Images Work*

Identity Manager Components	Platforms	ISO
<p><i>Identity Manager DVD</i></p> <p>The following Identity Manager components are available on one ISO image for DVD burning. These components are also available for individual download.</p> <ul style="list-style-type: none"> ◆ Identity Manager and Drivers ◆ Designer for Identity Manager 	<p>Identity Manager:</p> <p>Linux, NetWare, Windows, and UNIX</p> <p>Designer:</p> <p>Linux and Windows</p>	<p>Identity_Manager_3_0_1.iso</p>
<p><i>Identity Manager and Drivers</i></p>	<p>Linux, NetWare, and Windows</p>	<p>Identity_Manager_3_0_1_Linux_NW_Win.iso</p>
<p><i>Identity Manager and Drivers</i></p>	<p>UNIX</p>	<p>Identity_Manager_3_0_1_Unix.iso</p>
<p><i>User Application</i></p> <p>This is the standard version of the User Application that is included with your Identity Manager 3 purchase.</p>	<p>Linux and Windows</p>	<p>Identity_Manager_3_0_1_User_Application.iso</p>
<p><i>User Application with the Provisioning Module for Identity Manager</i></p> <p>This is the Provisioning version of the User Application, which is an add-on to Identity Manager and requires a separate purchase.</p>	<p>Linux and Windows</p>	<p>Identity_Manager_3_0_1_User_Application_Provisioning.iso</p>
<p><i>Designer for Identity Manager</i></p>	<p>Linux and Windows</p>	<p>Identity_Manager_3_0_1_Designer.iso</p>

Your Identity Manager purchase includes integration modules for several common customer systems that you might already have licenses for: Novell eDirectory, Microsoft Active Directory, Microsoft Windows NT, LDAP v3 Directories, Novell GroupWise, Microsoft Exchange, and Lotus Notes. All other Identity Manager Integration Modules must be purchased separately.

The User Application component comes on two ISO images: The User Application ISO image is a standard version and is included with your Identity Manager 3 purchase. The User Application with Provisioning Module for Identity Manager is an add-on product that integrates a powerful approval workflow. This Provisioning Module comes on a separate ISO image and is purchased separately.

Your Identity Manager purchase also includes Designer for Identity Manager, a powerful and flexible administration tool that dramatically simplifies configuration and deployment.

1.7.1 Installing Identity Manager 3

- ♦ To install Identity Manager 3 on Windows, NetWare, and Linux, see [Chapter 4, “Installing Identity Manager,”](#) on page 61
- ♦ To install the User Application or the User Application with Provisioning, see [Chapter 5, “Installing the User Application,”](#) on page 85
- ♦ To install Designer, see “[Installing Designer](#)” in *Designer for Identity Manager 3: Administration Guide*

NOTE: The Linux & UNIX (formerly NIS), Mainframe and Midrange driver installation programs are located in the `/platform/setup` directory. You must run these installs separately from the Identity Manager and User Application installation programs.

For a list of known issues, see the `Readme` file that comes with Identity Manager.

1.7.2 Activating Identity Manager 3 Products

Identity Manager products require activation (except Designer.) The following products can be used for a 90-day evaluation period before you need to either discontinue using them or purchase an activation.

- ♦ Identity Manager 3.0.1
- ♦ User Application with the Provisioning Module for Identity Manager
- ♦ Integration Modules

IMPORTANT: In order for the User Application to activate properly, you must download the correct ISO image. For example, if you purchase Identity Manager, but then download the User Application Provisioning Module without a separate purchase of the Provisioning Module, your User Application implementation stops working after 90 days.

For additional information on activation, see [Chapter 6, “Activating Novell Identity Manager Products,”](#) on page 111.

Planning

- ◆ Section 2.1, “Common Installation Scenarios,” on page 37
- ◆ Section 2.2, “Planning the Project Management Aspects of Identity Manager Implementation,” on page 45
- ◆ Section 2.3, “Planning the Technical Aspects of Identity Manager Implementation,” on page 51

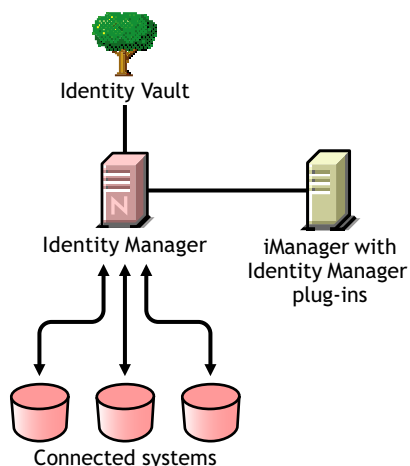
2.1 Common Installation Scenarios

The following scenarios are examples of the environment in which Identity Manager might be used. For each scenario, some guidelines are provided to help you with your implementation.

- ◆ Section 2.1.1, “New Installation of Identity Manager,” on page 37
- ◆ Section 2.1.2, “Using Identity Manager and DirXML 1.1a in the Same Environment,” on page 39
- ◆ Section 2.1.3, “Upgrading from the Starter Pack to Identity Manager,” on page 41
- ◆ Section 2.1.4, “Upgrading from Password Synchronization 1.0 to Identity Manager Password Synchronization,” on page 43

2.1.1 New Installation of Identity Manager

Figure 2-1 *New Installation*



Identity Manager is a data-sharing solution that leverages your Identity Vault to automatically synchronize, transform, and distribute information across applications, databases, and directories.

Your Identity Manager solution includes the following components:

- ◆ “Identity Vault with Identity Manager” on page 38
- ◆ “iManager Server with Identity Manager plug-ins” on page 38
- ◆ “Connected Systems” on page 38

- ♦ “Common Identity Manager Tasks” on page 38

Identity Vault with Identity Manager

The Identity Vault contains the user or object data you want to share or synchronize with other connected systems. We recommend that you install Identity Manager in its own eDirectory™ instance and use it as your Identity Vault.

iManager Server with Identity Manager plug-ins

You use Novell® iManager and the Identity Manager plug-ins to administer your Identity Manager solution.

Connected Systems

Connected systems might include other applications, directories, and databases that you want to share or synchronize data with the Identity Vault. To establish a connection from your Identity Vault to the connected system, install the appropriate driver for that connected system. Refer to the [driver implementation guides \(http://www.novell.com/documentation/dirxml/drivers/index.html\)](http://www.novell.com/documentation/dirxml/drivers/index.html) for specific instructions.

Common Identity Manager Tasks

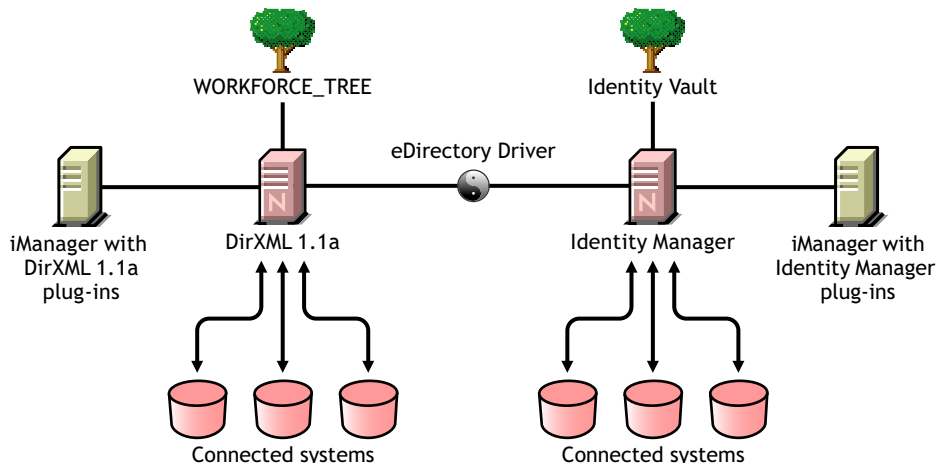
- ♦ **Install System Components:** Because your Identity Manager solution might be distributed across several computers, servers, or platforms, you should run the installation program and install the appropriate components per system. Refer to [Section 4.2, “Identity Manager Components and System Requirements,” on page 61](#) for more information.
- ♦ **Set Up Connected Systems:** Refer to [Section 4.2, “Identity Manager Components and System Requirements,” on page 61](#) and the [driver implementation guides \(http://www.novell.com/documentation/dirxml/drivers/index.html\)](http://www.novell.com/documentation/dirxml/drivers/index.html) for specific instructions.
- ♦ **Activate Your Solution:** Identity Manager products (professional, server editions, Integration Modules, and User Applications) require activation within 90 days of installation. See [Appendix 6, “Activating Novell Identity Manager Products,” on page 111](#).
- ♦ **Define Business Policies:** Business policies enable you to customize the flow of information into and out of the Identity Vault for a particular environment. Policies also create new objects, update attribute values, make schema transformations, define matching criteria, maintain Identity Manager associations, and many other things. A detailed guide to policies is contained in the *Policy Builder and Driver Customization Guide*.
- ♦ **Configure Password Management:** Using Password policies, you can increase security by setting rules for how users create their passwords. You can also decrease help desk costs by providing users with self-service options for forgotten passwords and for resetting passwords. For in-depth information on Password Management, refer to “Managing Passwords by Using Password Policies” in the Managing Passwords guide.
- ♦ **Configure Entitlements:** Entitlement definitions let you grant entitlements on connected systems to a defined group of users within the Identity Vault. Using Entitlement policies, you can streamline management of business policies and reduce the need to configure your Identity Manager drivers. For more information, see “[Creating and Using Entitlements](#)” in the *Novell Identity Manager 3.0.1 Administration Guide*.
- ♦ **Logging Events with Novell Audit:** Identity Manager is instrumented to use Novell Audit for auditing and reporting. Novell Audit is a collection of technologies providing monitoring,

logging, reporting and notification capabilities. Through integration with Novell Audit, Identity Manager provides detailed information about the current and historical status of driver and engine activity. This information is provided by a set of preconfigured reports, standard notification services, and user-defined logging. Refer to “[Logging and Reporting Using Novell Audit](#)” in the *Novell Identity Manager 3.0.1 Administration Guide*.

- ♦ **Workflow Approval and User Application:** The Novell Identity Manager User Application is a powerful web application (and supporting tools) designed to provide a rich, intuitive, highly configurable, highly administrable web-UI experience atop a sophisticated identity-services framework. When used in conjunction with the Provisioning Module for Identity Manager and Novell Audit, the Identity Manager User Application provides a complete, end-end provisioning solution that’s secure, scalable, and easy to manage. Refer to the [User Application Documentation \(http://www.novell.com/documentation/idm\)](http://www.novell.com/documentation/idm).

2.1.2 Using Identity Manager and DirXML 1.1a in the Same Environment

Figure 2-2 Installing Identity Manager in the Same Tree as DirXML 1.1a



If you are running both Identity Manager and DirXML[®] 1.1a in the same environment, keep in mind the following considerations.

- ♦ “[Creating an Identity Vault](#)” on page 39
- ♦ “[Management Tools](#)” on page 39
- ♦ “[Backward Compatibility](#)” on page 40
- ♦ “[Password Management](#)” on page 40

Creating an Identity Vault

- ♦ We recommend that you install Identity Manager in a separate eDirectory instance and use it as your Identity Vault.

Management Tools

- ♦ ConsoleOne[®] is supported for DirXML 1.1a, but not for Identity Manager.

- ◆ Two iManager servers are necessary, one for DirXML 1.1a plug-ins and one for Identity Manager plug-ins. This is because the plug-ins have been enhanced and because Identity Manager uses DirXML Script.
- ◆ iManager plug-ins for DirXML 1.1a can't read DirXML Script, which is used in the defined driver configurations for most Identity Manager drivers.

Backward Compatibility

- ◆ You can run DirXML 1.1a driver shims and configurations on an Identity Manager server, and you can view the drivers in iManager in the Identity Manager Overview for the driver set. But the Identity Manager plug-ins do not let you view or edit the driver configurations until you convert them to Identity Manager format.

In the Identity Manager plug-ins, if you click a driver that is in 1.1a format you are prompted to complete the conversion. This is a simple process done with a wizard, and it does not change the functionality of the driver configuration. As part of the process, a backup copy of the DirXML 1.1a version is saved.

- ◆ Activation for DirXML 1.1a drivers is still valid when running them with the Identity Manager engine. However, if you upgrade the driver shim to an Identity Manager version, you need to obtain a new activation credential. See [Appendix 6, “Activating Novell Identity Manager Products,” on page 111](#) for more detailed information.
- ◆ In most cases, an Identity Manager driver shim can run with a DirXML 1.1a configuration. See the individual [driver implementation guides \(http://www.novell.com/documentation/dirxml/drivers/index.html\)](http://www.novell.com/documentation/dirxml/drivers/index.html) for upgrade information.

A notable exception is that Password Synchronization 1.0 which does not run correctly for AD and NT after you upgrade the driver shim unless you add some additional driver policies. For instructions, see the sections about Password Synchronization in the [driver implementation guides \(http://www.novell.com/documentation/dirxml/drivers/index.html\)](http://www.novell.com/documentation/dirxml/drivers/index.html) for the Identity Manager Drivers for Active Directory and NT Domain.

- ◆ Running Identity Manager driver shims and driver configurations with the DirXML 1.1a engine is not supported.
- ◆ Running Identity Manager driver configurations with DirXML 1.1a driver shims is not supported.
- ◆ If you run the same Identity Manager driver configuration on more than one server, make sure the servers are running the same version of Identity Manager, and the same version of eDirectory.

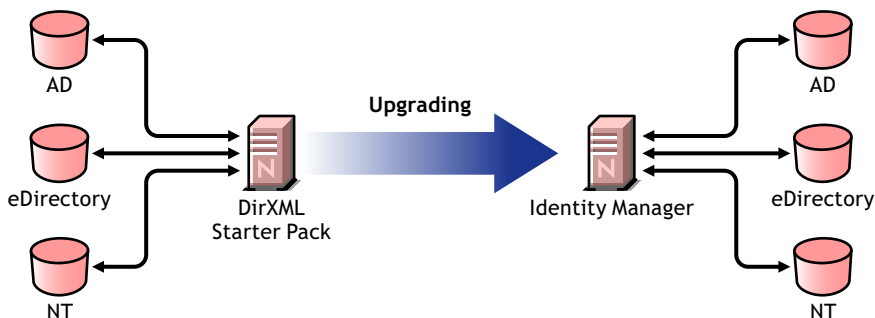
Password Management

- ◆ You can create Password policies that provide features such as Advanced Password Rules to require stronger passwords, and Forgotten Password Self-Service and Reset Password Self-Service for users. See the following section in the Password Management guide:
 - ◆ [“Managing Password Synchronization”](#)
- ◆ If you began using Universal Password with the initial release of NetWare 6.5[®], some upgrade steps are necessary before you can use the new password policy features. See “(NetWare 6.5 only) Re-Creating Universal Password Assignments” in the Password Management guide. The procedure is not necessary if you began using Universal Password with NetWare 6.5 SP2.
- ◆ Identity Manager Password Synchronization provides bidirectional password synchronization and supports more platforms than Password Synchronization 1.0.

- ♦ If you have been using Password Synchronization 1.0 with AD or NT, make sure you review the upgrade instructions before you install the new driver shims. See [Section 2.1.4, “Upgrading from Password Synchronization 1.0 to Identity Manager Password Synchronization,”](#) on page 43.
- ♦ Driver policy “overlays” are provided to help you add bidirectional Password Synchronization functionality to existing drivers. See [“Upgrading Existing Driver Configurations to Support Password Synchronization”](#) in the *Novell Identity Manager 3.0.1 Administration Guide*.

2.1.3 Upgrading from the Starter Pack to Identity Manager

Figure 2-3 *Upgrading from Starter Pack to Identity Manager*



The Identity Manager Starter Pack solutions included with other Novell products provide licensed synchronization of information held in NT Domains, Active Directory, and eDirectory. Additionally, evaluation drivers for several other systems including PeopleSoft*, GroupWise®, and Lotus Notes*, are included to allow you to explore data synchronization for your other systems.

This solution also offers you the ability to synchronize user passwords. With PasswordSync, a user is required to remember only a single password to log in to any of these systems. Administrators can manage passwords in the system of their choice. Any time a password is changed in one of these environments, it will be updated in all of them.

Identity Manager Starter Packs that shipped with NetWare 6.5 and Nenterprise™ Linux Services 1.0 were based on DirXML 1.1a technology. When upgrading from a Starter Pack to the latest version of Identity Manager, keep in mind the following considerations:

- ♦ [“Management Tools”](#) on page 41
- ♦ [“Backward Compatibility”](#) on page 41
- ♦ [“Password Management”](#) on page 42
- ♦ [“Activation”](#) on page 42

Management Tools

- ♦ ConsoleOne is supported for DirXML 1.1a, but not for Identity Manager.

Backward Compatibility

- ♦ You can run DirXML 1.1a driver shims and configurations on an Identity Manager server, and you can view the drivers in iManager in the Identity Manager Overview for the driver set. But the Identity Manager plug-ins do not let you view or edit the driver configurations until you convert them to Identity Manager format.

In the Identity Manager plug-ins, if you click a driver that is in 1.1a format, you are prompted to complete the conversion. This is a simple process done with a wizard, and it does not change the functionality of the driver configuration. As part of the process, a backup copy of the DirXML 1.1a version is saved.

- ◆ Activation for DirXML 1.1a drivers is still valid when running them with the Identity Manager engine. However, if you upgrade the driver shim to an Identity Manager version, you need new activation.
- ◆ In most cases, an Identity Manager driver shim can run with a DirXML 1.1a configuration. See the individual [driver implementation guides \(http://www.novell.com/documentation/dirxml/drivers/index.html\)](http://www.novell.com/documentation/dirxml/drivers/index.html) for upgrade information.

A notable exception Password Synchronization 1.0, which does not run correctly for AD and NT after you upgrade the driver shim unless you add some additional driver policies. For instructions, see the sections about Password Synchronization in the [driver implementation guides \(http://www.novell.com/documentation/dirxml/drivers/index.html\)](http://www.novell.com/documentation/dirxml/drivers/index.html) for the Identity Manager Drivers for Active Directory and NT Domain.

- ◆ Running Identity Manager driver shims and driver configurations with the DirXML 1.1a engine is not supported.
- ◆ Running Identity Manager driver configurations with DirXML 1.1a driver shims is not supported.
- ◆ If you run the same Identity Manager driver configuration on more than one server, make sure the servers are running the same version of Identity Manager, and the same version of eDirectory.

Password Management

- ◆ Password Synchronization 1.0, which shipped with Starter Packs (DirXML 1.1a), won't work correctly for AD and NT after you upgrade the driver shim unless you add some additional driver policies. For instructions, see the sections about Password Synchronization in the [driver implementation guides \(http://www.novell.com/documentation/dirxml/drivers/index.html\)](http://www.novell.com/documentation/dirxml/drivers/index.html) for the Identity Manager Drivers for Active Directory and NT Domain.
- ◆ Refer to [Section 2.1.4, "Upgrading from Password Synchronization 1.0 to Identity Manager Password Synchronization," on page 43](#) for specific instructions surrounding this upgrade process.

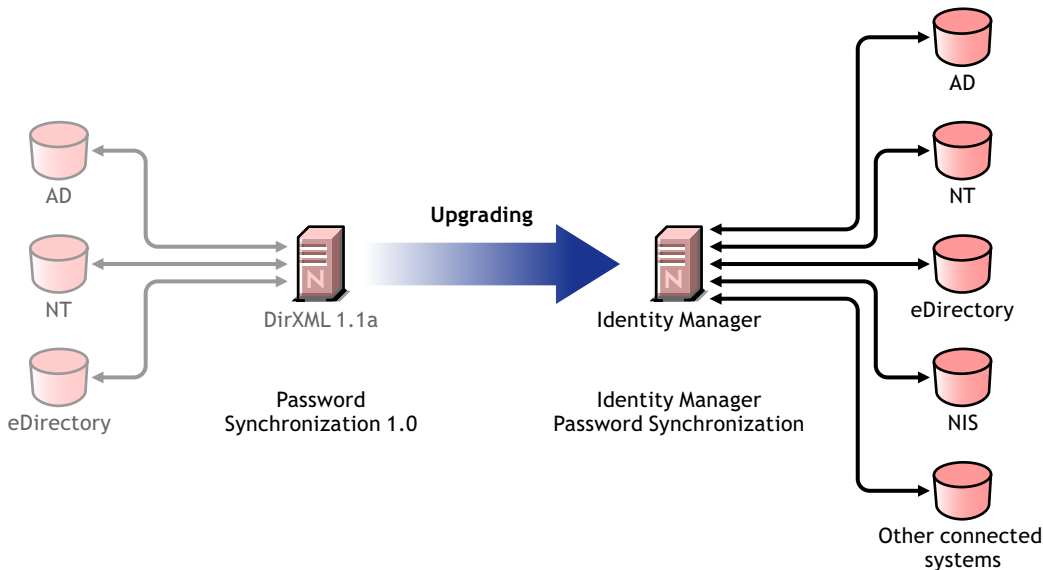
Activation

- ◆ All Identity Manager products must be activated within 90 days. When you purchased other Novell software, the DirXML Starter Pack included activations for the DirXML 1.1a engine and the NT, AD, and eDirectory drivers. When upgrading from the Identity Manager Starter Pack, you might need to re-apply your activation credentials for those drivers.

For more information on activation, refer to [Appendix 6, "Activating Novell Identity Manager Products," on page 111](#).

2.1.4 Upgrading from Password Synchronization 1.0 to Identity Manager Password Synchronization

Figure 2-4 Upgrading from Password Synchronization 1.0 to Identity Manager Password Synchronization



Identity Manager Password Synchronization offers many features, including bidirectional password synchronization, additional platforms, and e-mail notification when password synchronization fails.

If you are using Password Synchronization 1.0 with Active Directory or NT Domain, it's very important that you review the instructions for upgrading before you install the new driver shims.

If you are running Identity Manager 2.x with Password Synchronization 2.0, do you not need to follow these steps.

For information about Identity Manager Password Synchronization in general, see “[Password Synchronization across Connected Systems](#)” in the *Novell Identity Manager 3.0.1 Administration Guide*. That section contains conceptual information including a comparison of old and new features, prerequisites, a list of features supported for each connected system, instructions on adding support to existing drivers, and several scenarios showing how you could use the new features.

In this section:

- ◆ “[Upgrading Password Synchronization for AD or NT](#)” on page 43
- ◆ “[Upgrading Password Synchronization for eDirectory](#)” on page 44
- ◆ “[Upgrading Other Connected System Drivers](#)” on page 44
- ◆ “[Handling Sensitive Information](#)” on page 44

Upgrading Password Synchronization for AD or NT

The new Password Synchronization functionality is done by driver policies, not by a separate agent. This means that if you install the new driver shim without upgrading the driver configuration at the same time, Password Synchronization 1.0 continues to work only for existing users. New, moved, or renamed users do not participate in Password Synchronization until you complete the upgrade of the driver configuration.

Use the following general steps to upgrade:

1. Upgrade your environment so that it supports Universal Password, including upgrading the Novell Client™ if you are using it.
2. Install the Identity Manager 3.0.1 driver shim to replace the DirXML 1.1a driver shim for AD or NT.
3. Immediately create backward compatibility with Password Synchronization 1.0, by adding a new policy to the driver configuration.
This step allows Password Synchronization 1.0 to continue to function correctly until you make the switch to Identity Manager Password Synchronization.
4. Add support for the new Identity Manager Password Synchronization, using driver policies.
5. Install and configure new Password Synchronization filters.
6. Set up SSL, if necessary.
7. Turn on Universal Password using password policies, if necessary.
8. Set up the Identity Manager Password Synchronization scenario that you want to use.
See “**Implementing Password Synchronization**” in the *Novell Identity Manager 3.0.1 Administration Guide*.
9. Remove Password Synchronization 1.0.

For detailed instructions, see the [driver implementation guides \(http://www.novell.com/documentation/dirxml/drivers/index.html\)](http://www.novell.com/documentation/dirxml/drivers/index.html) for the Identity Manager Drivers for Active Directory and NT Domain.

Upgrading Password Synchronization for eDirectory

Upgrading for eDirectory is fairly simple, and the driver shim is intended to work with your existing DirXML 1.1a driver configuration with no changes, assuming that your driver shim and configuration have the latest patches. For instructions, see the *Identity Manager Driver for eDirectory: Implementation Guide*.

Upgrading Other Connected System Drivers

Identity Manager Password Synchronization supports more connected systems than Password Synchronization 1.0.

For a list of the features that are supported for other systems, see “**Connected System Support for Password Synchronization**” in the *Novell Identity Manager 3.0.1 Administration Guide*.

Driver policy “overlays” are provided to help you add bidirectional Password Synchronization functionality to existing drivers for connected systems that were not previously supported. See “**Upgrading Existing Driver Configurations to Support Password Synchronization**” in the *Novell Identity Manager 3.0.1 Administration Guide*.

Handling Sensitive Information

Universal Password is protected by four layers of encryption inside eDirectory, so it is very secure in that environment. If you choose to use bidirectional password synchronization, and you synchronize Universal Password with the Distribution Password, keep in mind that you are extracting the eDirectory password and sending it to other connected systems. You need to secure the transport of

the password, as well as the connected systems it is synchronized to. See “[Security: Best Practices](#)” in the *Novell Identity Manager 3.0.1 Administration Guide*.

2.2 Planning the Project Management Aspects of Identity Manager Implementation

This section outlines high-level political and project management aspects of implementing Identity Manager. (For the technical aspects, see [Section 2.3, “Planning the Technical Aspects of Identity Manager Implementation,”](#) on page 51.)

This planning material provides an overview of the type of activities that would normally be taken from the inception of an Identity Manager project to its full production deployment. Implementing an identity management strategy requires you to discover what the needs are and who the stakeholders are in your environment, 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.

We strongly recommend that an Identity Manager expert be engaged to assist in each phase of the solution deployment. 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.

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.

2.2.1 Novell Identity Manager Deployment

There are several activities suggested as best practices when deploying Identity Manager:

- ◆ “[Discovery](#)” on page 45
- ◆ “[Requirements and Design Analysis](#)” on page 46
- ◆ “[Proof of Concept](#)” on page 49
- ◆ “[Data Validation and Preparation](#)” on page 50
- ◆ “[Production Pilot](#)” on page 50
- ◆ “[Production Rollout Planning](#)” on page 50
- ◆ “[Production Deployment](#)” on page 51

Discovery

You might want to begin your Identity Manager implementation with a discovery process that can do the following:

- ◆ Identify the primary objectives in managing identity information
- ◆ Define or clarify the business issues being addressed
- ◆ Determine what initiatives are required to address outstanding issues
- ◆ Determine what it would take to carry out one or more of these initiatives
- ◆ Develop a high-level strategy or “solution roadmap” and an agreed execution path

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

- ◆ It can establish a base level understanding among all stakeholders
- ◆ It can capture key business and systems information from stakeholders
- ◆ It can enable a solution roadmap to be developed

The discovery also identifies immediate next steps, which might include the following:

- ◆ Identifying planning activities in preparation of a requirements and design phase
- ◆ Defining additional education for stakeholders

Key Deliverables

- ◆ Structured interviews with key business and technical stakeholders
- ◆ High-level summary report of the business and technical issues
- ◆ Recommendations for the next steps
- ◆ An executive presentation outlining the outcome of the discovery

Requirements and Design Analysis

This analysis phase captures both technical and business aspects of the project in detail and produces the data model and high-level Identity Manager architecture design. This activity is a crucial first step from which the solution is implemented.

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. Here is a sample of items that you might want to assess:

- ◆ What versions of system software are being used?
- ◆ Is the directory design appropriate?
- ◆ Is the directory being used to host the Identity Vault and Identity Manager or is it being used to extend other services?
- ◆ Is the quality of the data in all systems appropriate? (If the data is not of usable quality, business policy might not be implemented as desired.)
- ◆ Is data manipulation required for your environment?

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

The following tasks might be completed during the requirements assessment:

- ◆ [“Define the Business Requirements” on page 47](#)
- ◆ [“Analyze Your Business Processes” on page 47](#)
- ◆ [“Design an Enterprise Data Model” on page 48](#)

Define the Business Requirements

Gather your organization's business processes and the business requirements that define these business processes.

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 following tasks can guide you in defining the business requirements:

- ◆ Establish the process flows, process triggers, and data mapping relationships.

For example, if something is going to happen in a certain process, what will happen because of that process? What other processes are triggered?

- ◆ Map data flows between applications.
- ◆ Identify data transformations that need to take place from one format to another, such as 2/25/2006 to 25 Feb 2006.
- ◆ 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 roadmap.

It might be advantageous to divide the deployment into phases that will enable implementation of a portion of the deployment earlier and other portions of the deployment later. You can do a phased deployment approach as well. It should be 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 you are wanting to interface with Identity Manager.

- ◆ Identify authoritative data sources.

Learning early on which items of information 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.

Analyze Your Business Processes

The analysis of business processes often commences by interviewing 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 live (on what servers, in which departments)?
- ◆ What processes are not suitable for automated handling?

For example, questions that might be posed to an administrator for a PeopleSoft system in Human Resources may include

- ◆ What data are stored in the PeopleSoft database?
- ◆ What appears in the various panels for an employee account?
- ◆ What actions are required to 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.

Design an Enterprise Data Model

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

The model should illustrate where data originates, where it moves to, and where it can't move. It should also account for how critical events affect the data flow.

You might also wish 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.

Key Deliverables

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

Dependencies

- ◆ Staff familiar with all external systems (such as HR database administrator, network and messaging system administrator)
- ◆ Availability of system schemas and sample data
- ◆ Data model from the analysis and design phase
- ◆ Availability of basic information such as organizational chart, WAN and server infrastructure

Proof of Concept

The outcome of this activity is to have a sample implementation in a lab environment that reflects your company’s business policy and data flow. It 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.

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

Key Deliverables

- ◆ A functioning Identity Manager proof of concept with all system connections operational

Dependencies

- ◆ Hardware platform and Equipment
- ◆ Necessary software
- ◆ Analysis and design phase that identifies the required connections
- ◆ Availability and access to other systems for testing purposes
- ◆ Data model from the analysis and design phase

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.

Key Deliverables

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

Dependencies

- ◆ Data model from analysis and design phase (proposed record matching and data format strategy)
- ◆ Access to production data sets

Production Pilot

The purpose of this activity is to begin the migration into a production environment. During this phase, there might be additional customization that occurs. In this limited introduction, desired outcomes of the preceding activities can be confirmed and agreement obtained for production rollout.

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

Key Deliverables

- ◆ Pilot solution providing live proof of concept and validation for the data model and desired process outcomes

Dependencies

- ◆ All previous activities (analysis and design, Identity Manager technology platform).

Production Rollout Planning

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

- ◆ Confirm server platforms, software revisions, and service packs
- ◆ Confirm the general environment
- ◆ Confirm introduction of Identity Vault in a mixed coexistence
- ◆ Confirm partitioning and replication strategies
- ◆ Confirm Identity Manager implementation

- ♦ Plan the legacy process cutover
- ♦ Plan a rollback contingency strategy

Key Deliverables

- ♦ Production rollout plan
- ♦ Legacy process cutover plan
- ♦ Rollback contingency plan

Dependencies

- ♦ All previous activities

Production Deployment

This phase is where the pilot solution is expanded to affect all live data in the production environment. It typically follows agreement that the production pilot meets all the technical and business requirements.

Key Deliverables

- ♦ Production solution ready for transition

Dependencies

- ♦ All previous activities

2.3 Planning the Technical Aspects of Identity Manager Implementation

- ♦ [Section 2.3.1, “Using Designer,” on page 51](#)
- ♦ [Section 2.3.2, “Replicating the Objects that Identity Manager Needs on the Server,” on page 51](#)
- ♦ [Section 2.3.3, “Managing Users on Different Servers Using Scope Filtering,” on page 53](#)

2.3.1 Using Designer

Identity Manager 3.0.1 comes with a new tool called Designer. Designer allows you to design, test, and document the Identity Manager drivers. Designer allows you to see how password synchronization and data flows as well. For more information see the *Designer for Identity Manager 3: Administration Guide*.

2.3.2 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, then as part of your planning, you need to 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 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 creating 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, then 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 also is 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 to specify otherwise (rules for "scope filtering").

If you want a driver to synchronize all user objects, for example, 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 two 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 will 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 ["Managing Users on Different Servers Using Scope Filtering" on page 53](#).

- ◆ **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 will 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. But 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 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.

2.3.3 Managing Users on Different Servers Using Scope Filtering

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.

An Identity Manager driver by default 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.

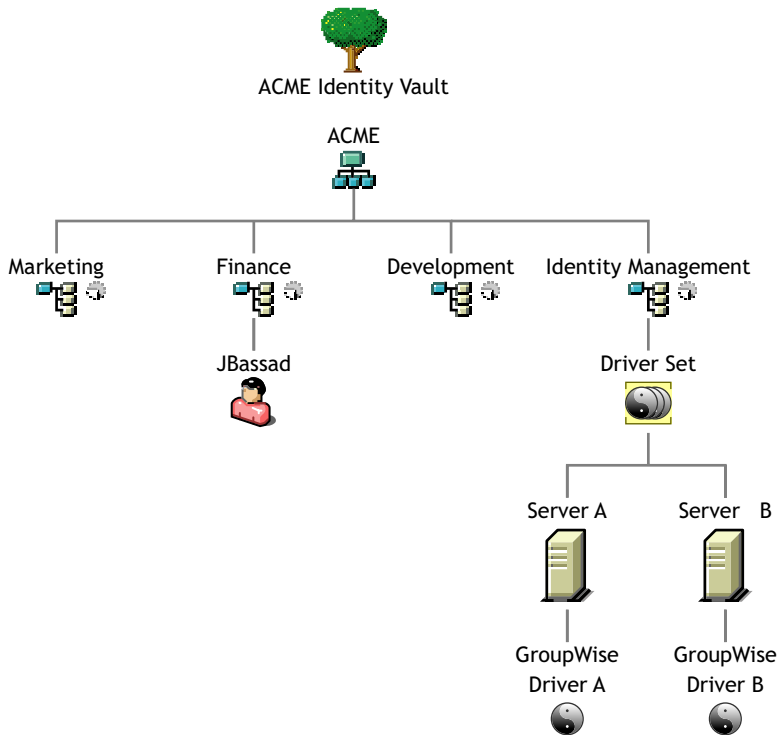
To synchronize all users without having them replicated on one single server, you need to determine which set of servers holds all the users, and then create an instance of the Identity Manager driver on each of those servers. To prevent two instances of the driver from trying to synchronize the same users, you will 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 Manager container that holds the driver sets. Each of these containers is a separate partition.

Figure 2-5 Example Tree for Scope Filtering



In this example, the Identity Manager administrator has two Identity Vault servers, Server A and Server B, shown in the next illustration. 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.

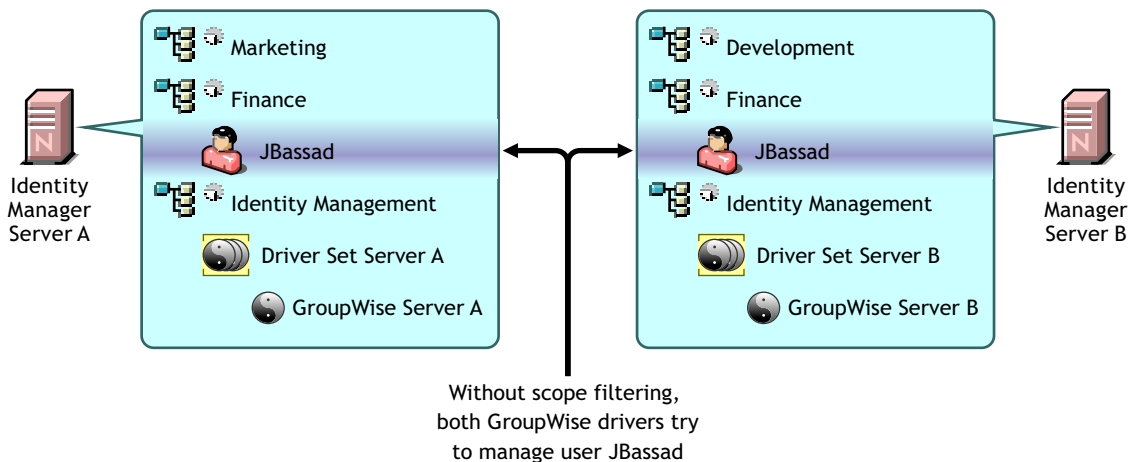
The administrator wants all the users in the tree to be synchronized by the GroupWise[®] driver, but does not want to aggregate replicas of the users onto a single server. He chooses instead to use two instances of the GroupWise driver, one on each server. He installs Identity Manager and sets up the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

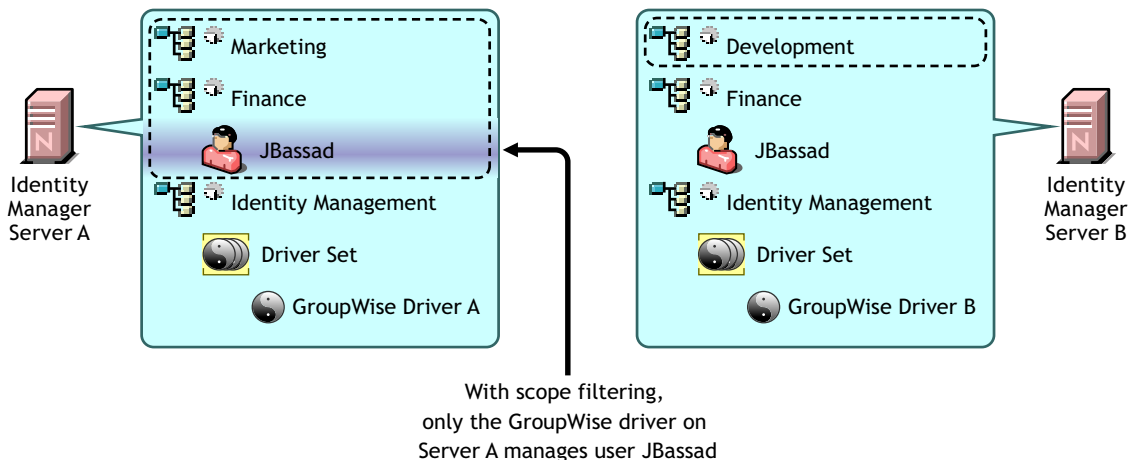
Because Server A and Server B both hold a replica of the Finance container, both servers hold the user JBassad, who is in the Finance container. Without scope filtering, both GroupWise Driver A and GroupWise Driver B would synchronize JBassad.

Figure 2-6 Two Servers with Overlapping Replicas, Without Scope Filtering



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

Figure 2-7 Scope Filtering Defines Which Drivers Synchronize Each Container



Identity Manager 3.0.1 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](#)” documented in the *Policy Builder and Driver Customization Guide*.

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.

Upgrading

Identity Manager has many different parts. To upgrade Identity Manager, you need to make sure you have considers all aspects of the product for the upgrade to be successful.

- ♦ [Section 3.1, “Upgrade Paths,” on page 57](#)
- ♦ [Section 3.2, “Upgrade Procedure,” on page 57](#)
- ♦ [Section 3.3, “Upgrading Password Synchronization,” on page 59](#)
- ♦ [Section 3.4, “Upgrading from RNS to Novell Audit,” on page 60](#)
- ♦ [Section 3.5, “Upgrading DirXML 1.1a Driver Configurations,” on page 60](#)
- ♦ [Section 3.6, “Activating Identity Manager,” on page 60](#)

Some upgrade scenarios are explained in [Section 2.1, “Common Installation Scenarios,” on page 37](#).

3.1 Upgrade Paths

The table contains the supported upgrade scenarios for the different versions of Identity Manager. Each scenario is listed as supported or not supported.

Table 3-1 *Upgrade Path Scenarios*

Installed Version	Current Version	Upgrade Supported?
DirXML® 1.1a	Identity Manager 3.0.1	Yes
Identity Manager 2.x	Identity Manager 3.0.1	Yes

3.2 Upgrade Procedure

For an upgrade to Identity Manager 3.0.1 to be successful, the following steps need to be completed.

- ♦ [Section 3.2.1, “Exporting Drivers,” on page 57](#)
- ♦ [Section 3.2.2, “Verifying Minimum Requirements,” on page 58](#)
- ♦ [Section 3.2.3, “Upgrading the Engine,” on page 58](#)
- ♦ [Section 3.2.4, “Upgrading the Remote Loader,” on page 59](#)

3.2.1 Exporting Drivers

Before an upgrade occurs, getting a backup of the current drivers and their configuration information is the most important step. To get a backup of the drivers, you need to export the drivers.

Exporting from ConsoleOne

- 1 In ConsoleOne, right-click on the Driver Set object, then select *Properties > DirXML > Drivers*.
- 2 Select the driver you want to create an export for, then click *Export*.

- 3 Specify a filename. Leave the default extension of .xml, then click *Save*.
- 4 Click *Export configuration*.

In iManager, you can export a driver or the entire driver set. If you export the driver set, there is a single configuration file created. If you export each driver, there is a configuration file created for each driver.

Exporting from iManager

- 1 In iManager select *DirXML Utilities > Export Driver*.
- 2 Browse to and select the Driver or Driver Set you want to export, then click *Next*.
- 3 Leave the prompting fields blank to create an exact copy of the driver, then click *Next*.
- 4 If you select the Driver Set object, you receive a prompting page for each driver. Leave the fields blank for each driver to create an exact copy.
- 5 Click *Save As*.
- 6 Click *Save* in the File Download window.
- 7 Browse to and specify a file location and name for the export, then click *Save*.

IMPORTANT: The file needs to have an .xml extension when it is saved.

After you have an export of the driver, test the export in a lab environment. Import the driver export and test the driver to make sure all of the parameters are correct and all of the functionality is there.

3.2.2 Verifying Minimum Requirements

In order to upgrade to Identity Manager 3.0.1, the servers running the Identity Manager services need to meet the minimum requirements. See [Section 4.2, “Identity Manager Components and System Requirements,” on page 61](#) for the list of minimum requirements for each platform.

If the supporting components need to be upgraded, do the upgrades in the following order:

1. Upgrade the OS to a supported version. For example, upgrade from NetWare® 6.0 to NetWare 6.5.
2. Upgrade eDirectory™ to eDirectory 8.73 with the latest patch, or upgrade to eDirectory 8.8.1.
3. Upgrade iManager to iManager 2.6 SP2 (includes upgrading Apache 2.0.52 or later and Tomcat 4.1.18 or later).
4. Upgrade Identity Manager.
5. Activate the Metadirectory engine and any upgraded driver.

3.2.3 Upgrading the Engine

After the supporting components have been upgraded, the DirXML or Identity Manager engine is upgraded.

- 1 Make sure you have a valid export of the drivers.
- 2 Stop the drivers.
 - 2a In iManager select *Identity Manager > Identity Manager Overview*.

- 2b** Browse to and select the Driver Set object, then click *Search*.
- 2c** Click in the upper-right corner of the driver icon, then select *Stop driver*.
- 3** Set the drivers to manual start.
 - 3a** In iManager select *Identity Manager > Identity Manager Overview*.
 - 3b** Browse to and select the Driver Set object, then click *Search*.
 - 3c** In the upper-right corner of the driver icon, click and select *Edit properties*.
 - 3d** On the Driver Configuration page, under Startup Options, select *Manual*.
- 4** Install Identity Manager 3.0.1. The steps to upgrade to Identity Manager 3.0.1 are the same as when you install Identity Manager 3.0. See **Chapter 4, “Installing Identity Manager,” on page 61** for the instructions on how to install Identity Manager.
- 5** Set the drivers startup options.
 - 5a** In iManager select *Identity Manager > Identity Manager Overview*.
 - 5b** Browse to and select the Driver Set object, then click *Search*.
 - 5c** In the upper-right corner of the driver icon, click and select *Edit properties*.
 - 5d** On the Driver Configuration page, under Startup Options, select *Auto start* or you preferred method of start up for the driver.
- 6** Look at the driver parameters and policies to make sure everything is set how you want it to be.
- 7** Start the driver.
 - 7a** In iManager select *Identity Manager > Identity Manager Overview*.
 - 7b** Browse to and select the Driver Set object, then click *Search*.
 - 7c** Click in the upper-right corner of the driver icon, then select *Start driver*.

3.2.4 Upgrading the Remote Loader

If you are running the Remote Loader, you need to upgrade the remote loader files as well.

- 1** Create a backup of the Remote Loader configuration files. The default location of the files:
 - ♦ Windows C:\Novell\RemoteLoader\remoteloadername-config.txt
 - ♦ Linux - You create your own configuration file in the path of rdxml.
- 2** Stop the Remote Loader service or daemon.
- 3** Run the installation programs for the remote loader. This updates the files and binaries to the current version. See “**Installing Remote Loaders**” in the *Novell Identity Manager 3.0.1 Administration Guide*.

3.3 Upgrading Password Synchronization

If you are upgrading from DirXML 1.1a to Identity Manager 3.0.1, Password Synchronization needs to be upgraded. See “**Upgrading Password Synchronization 1.0**” in the *Novell Identity Manager 3.0.1 Administration Guide*.

If you are upgrading from Identity Manager 2.x, Password Synchronization is the same and is not upgraded.

3.4 Upgrading from RNS to Novell Audit

Reporting and Notification Service (RNS) is deprecated, although the engine continues to process RNS functions if you are currently using RNS. You should plan to move to Novell® Audit, because Novell Audit expands the functionality provided by RNS, and RNS might not be supported in a future release of Identity Manager.

For more information, see “[Logging and Reporting Using Novell Audit](#)” in the *Novell Identity Manager 3.0.1 Administration Guide*.

3.5 Upgrading DirXML 1.1a Driver Configurations

When you upgrade from DirXML 1.1a to Identity Manager 3.0.1, the driver configuration is upgraded. Upgrading driver configurations has two aspects:

- ◆ Converting the rules to Identity Manager policies. This is done by a conversion tool, and it does not enhance the functionality of the driver. Legacy drivers run without this conversion, but doing the conversion allows you to view the existing driver configuration in the Identity Manager iManager plug-ins.
- ◆ Upgrading the driver policies to add new functionality. This is best handled by an Identity Manager expert.

See “[Upgrading a Driver Configuration from DirXML 1.1a to Identity Manager Format](#)” and “[Managing DirXML 1.1a Drivers in an Identity Manager Environment](#)” in the *Novell Identity Manager 3.0.1 Administration Guide*.

Another alternative is to begin with the Identity Manager driver configurations and customize them to do the same things your DirXML 1.1a configuration does.

3.6 Activating Identity Manager

After the upgrade has completed, you have 90 days to activate the Metadirectory engine and any drivers you have upgraded. If the engine and drivers are not activated, after 90 days they stop working. For instructions on how to activate Identity Manager, see [Chapter 6, “Activating Novell Identity Manager Products,”](#) on page 111.

Installing Identity Manager

4

This section contains requirements and instructions for installing Identity Manager and Identity Manager drivers.

- ♦ Section 4.1, “Before You Install,” on page 61
- ♦ Section 4.2, “Identity Manager Components and System Requirements,” on page 61
- ♦ Section 4.3, “Installing Identity Manager on NetWare,” on page 61
- ♦ Section 4.4, “Installing Identity Manager on Windows,” on page 68
- ♦ Section 4.5, “Installing the Connected System Option on Windows,” on page 73
- ♦ Section 4.6, “Installing Identity Manager on UNIX/Linux Platforms,” on page 76
- ♦ Section 4.7, “Installing the Connected System Option on UNIX/Linux,” on page 80
- ♦ Section 4.8, “Post-Installation Tasks,” on page 83
- ♦ Section 4.9, “Installing a Custom Driver,” on page 83

4.1 Before You Install

Before you install Identity Manager, refer to [Chapter 2, “Planning,”](#) on page 37.

4.2 Identity Manager Components and System Requirements

Novell Identity Manager contains components that can be installed within your environment on multiple systems and platforms. 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.

[Table 1-3, “Identity Manager System Components and Requirements,”](#) on page 27 lists the installation components of Identity Manager and requirements for each system.

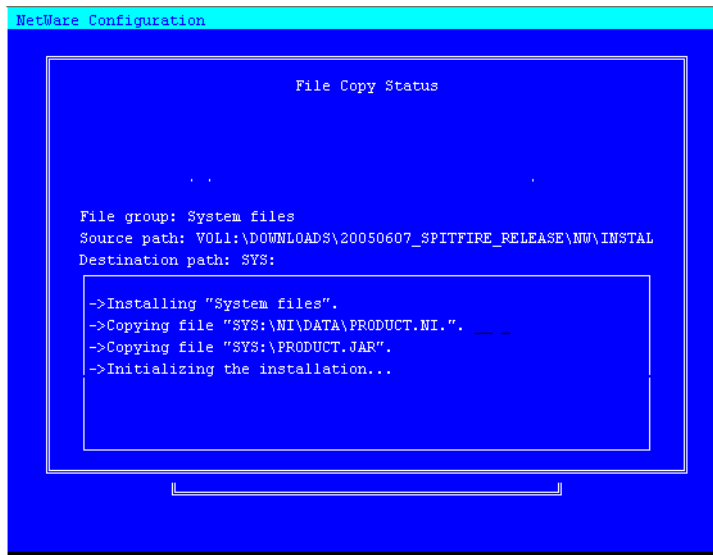
4.3 Installing Identity Manager on NetWare

This procedure covers the installation of the Metadirectory Server, Web Components, and Utilities for NetWare. Before you begin, make sure your system meets the requirements listed in [Section 4.2, “Identity Manager Components and System Requirements,”](#) on page 61.

- 1 Download and extract the Identity Manager installation file. You can download the Identity Manager installation file from [Novell's Download site \(http://download.novell.com\)](http://download.novell.com).
- 2 Once you extract the file, type `nwconfig` at the server console prompt.
- 3 Select Product Options > Install a Product Not Listed.
- 4 Press F3 (F4 if you're using RCONSOLE), then specify the path to the Identity Manager NetWare installation files in the \NW directory.

The graphical installation utility starts after a few moments.

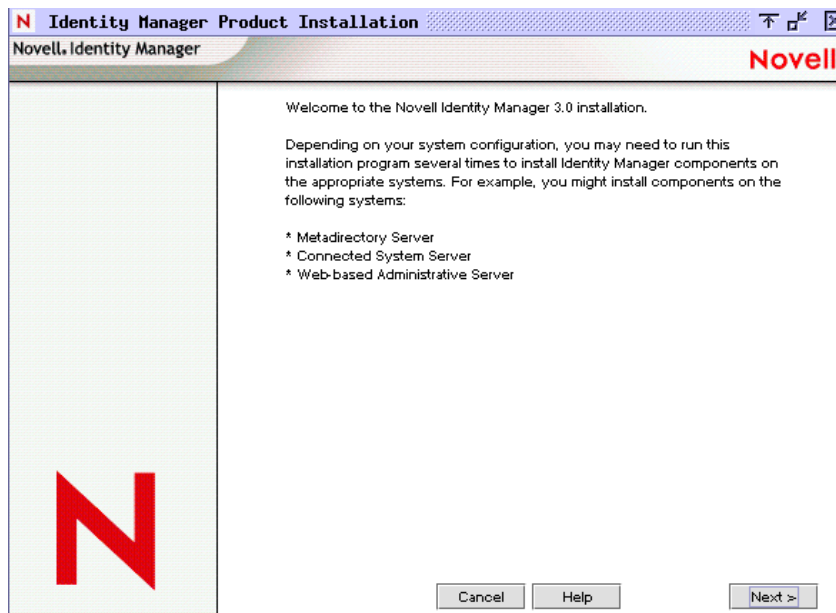
Figure 4-1 Initial Setup of the Identity Manager Installation Files



You can also begin the installation process by going directly to the server GUI and selecting Install from the Novell icon. In the Installed Products screen, select Add. Then in the Source Path screen, type the path leading to the products.ni file in the \NW directory. Click OK.

- 5 After the files have finished copying, the Identity Manager Product Installation page appears. Click Next to begin the installation.

Figure 4-2 The Initial Identity Manager Installation Page

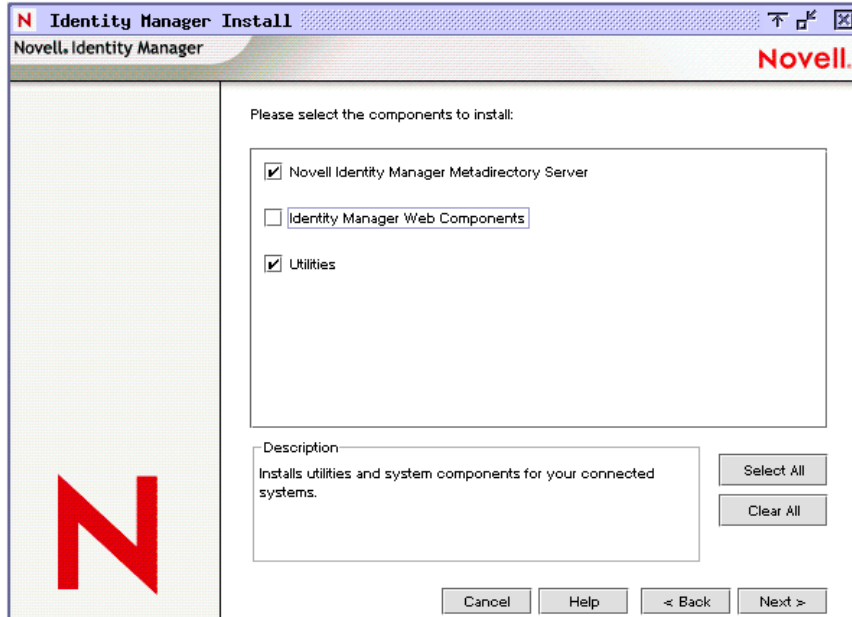


- 6 Read the license agreement, then click I Accept.
- 7 Review the Overview pages describing the system types, which include the Metadirectory Server, the Web Components, and the Utilities. Click Next to continue.

This information is also covered in the table under [Section 4.2, “Identity Manager Components and System Requirements,”](#) on page 61.

- 8 In the Identity Manager Install page, select the components you want to install:
See [Section 4.2, “Identity Manager Components and System Requirements,”](#) on page 61.

Figure 4-3 Identity Manager Installation Options



The following options are available. For most installations you will select all of the components.

- ♦ **Metadirectory Server:** Installs the Metadirectory engine and service drivers. On the NetWare platform, these include Identity Manager Drivers for eDirectory, LDAP, JDBC, GroupWise, Delimited Text, Composer, Avaya, SOAP, SIF, and the Novell Audit agent. Selecting this option also extends the eDirectory schema.

Novell eDirectory must be installed before you can install this option. Install the Metadirectory Server component where you want to run the Metadirectory engine for Identity Manager.

- ♦ **Connected System:** Installs the Remote Loader that allows you to establish a link between the connected system and a server running the Metadirectory engine. For NetWare, this option also installs the following drivers: LDAP, JDBC, GroupWise, Composer, Avaya, SOAP, SIF, and Delimited Text.

NOTE: For the NetWare installation of Identity Manager, this option is not available and you will not see it on the Install screen.

- ♦ **Identity Manager Web Components:** This option installs the Identity Manager plug-ins and driver configurations.

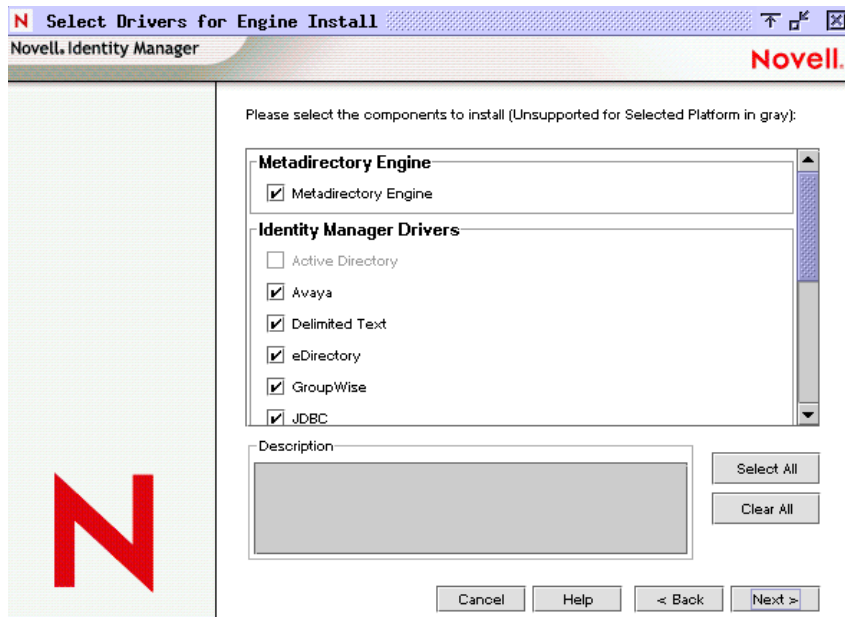
Novell iManager must be installed before you can install this option.

- ♦ **Utilities:** Installs additional scripts for the JDBC driver and utilities for other drivers. Most drivers don't have a utility connected to them.

- 9 Click Next.

10 Select the drivers you want to install, then click Next.

Figure 4-4 Selecting Drivers for the Metadirectory Engine



The Select Drivers for Engine Install page shows you which drivers can be installed on a corresponding platform. For example, on a NetWare server, you cannot install the Windows Active Directory driver.

By default, all available drivers for the option are selected. We recommend installing all of the selected driver files so you won't need to run the installation program later if you want another driver. The driver files are not used until a driver is configured through iManager or through Designer and then deployed.

NOTE: If you do not install all of the drivers at this time, you'll need to rerun this installation program to install the drivers. Or you can use Designer to create, modify, and deploy driver files.

11 When you see the informational message reminding you about product activation, click OK. You need to activate the drivers within 90 days of installation; otherwise, they will shut down.

12 On the Schema Extension page, specify the following:

Figure 4-5 The Schema Extension Page

The screenshot shows a window titled "Schema Extension" from Novell Identity Manager. The window contains the following elements:

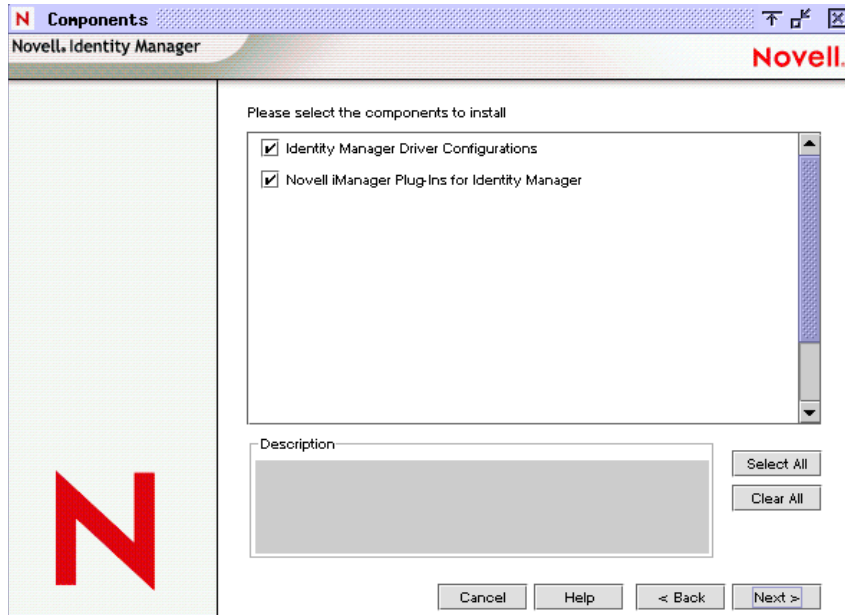
- A header bar with the Novell logo and the text "Novell Identity Manager".
- A large red "N" logo on the left side.
- Main text: "Identity Manager schema will be extended during the install. Please provide the following information."
- A section titled "Tree Information" with a "Tree name" field containing the text "IDMTREE".
- A section titled "User Login Information" with a "User name in LDAP Format (Example: CN=admin,O=novell)" field containing "CN=admin,O=novell" and a dropdown arrow.
- An "Enter the user password." field containing a series of asterisks "*****".
- Four buttons at the bottom: "Cancel", "Help", "< Back", and "Next >".

- ♦ **User Name:** Specify the username (in LDAP format, such as CN=admin,O=novell) of a user who has rights to extend the schema. In this screen, select a user (such as Admin) who has enough rights to extend the eDirectory schema.
- ♦ **User Password:** Specify the user's password.

13 Click Next. When the user information is validated, you see the first (of three) Components pages:

- 14 On the first Components page, select the driver configurations and the iManager plug-ins, then click Next.

Figure 4-6 First Components Page



- 15 On the second Components page, click Next.

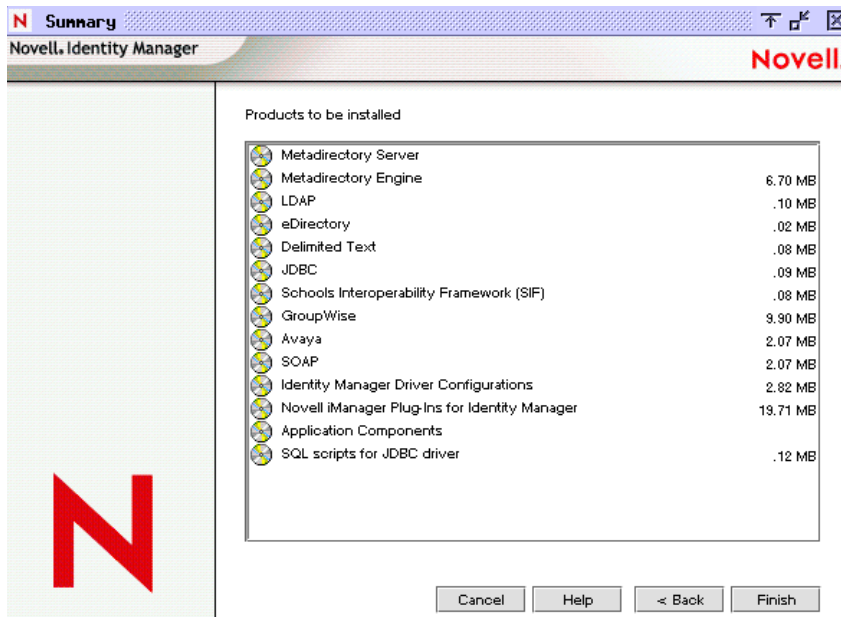
The Novell Audit System Components for Identity Manager is highlighted if you have the Novell Audit System installed on the server. Otherwise, it is not selected. The Application Components selection installs components for such application systems as JDBC and PeopleSoft.

- 16 The third Components page installs the utilities. Click Next.

Platform-specific utilities are dimmed if they are available for platforms other than the one you are installing on. For NetWare, the only selection available is SQL Scripts for JDBC Driver.

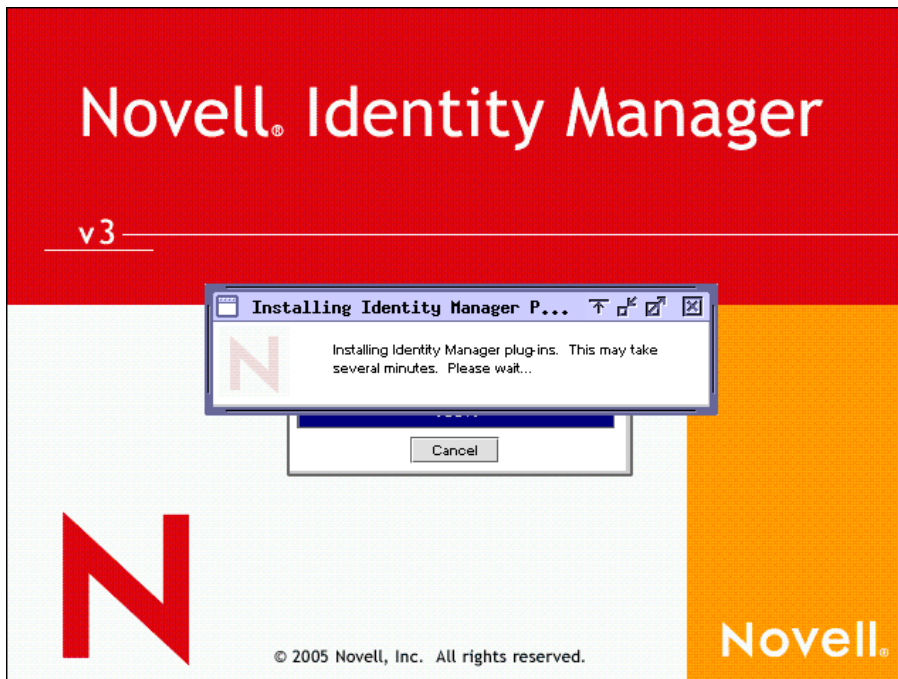
17 Read and verify your selections on the Summary page, then click Finish.

Figure 4-7 Summary Page Shows Products and Components To Be Installed



The Novell Identity Manager installation process shuts down eDirectory to extend the schema. The installation process commences installing the selected products and components.

Figure 4-8 The Installation Process on a NetWare Server



18 After the installation completes and displays the Installation Complete dialog box, click Close. Restart the server to complete the installation of the Metadirectory engine and restart Tomcat.

4.4 Installing Identity Manager on Windows

This procedure covers the installation of the Metadirectory Server, Web Components, and Utilities for Windows.

Before you begin, make sure your system meets the requirements listed in [Section 4.2, “Identity Manager Components and System Requirements,”](#) on page 61.

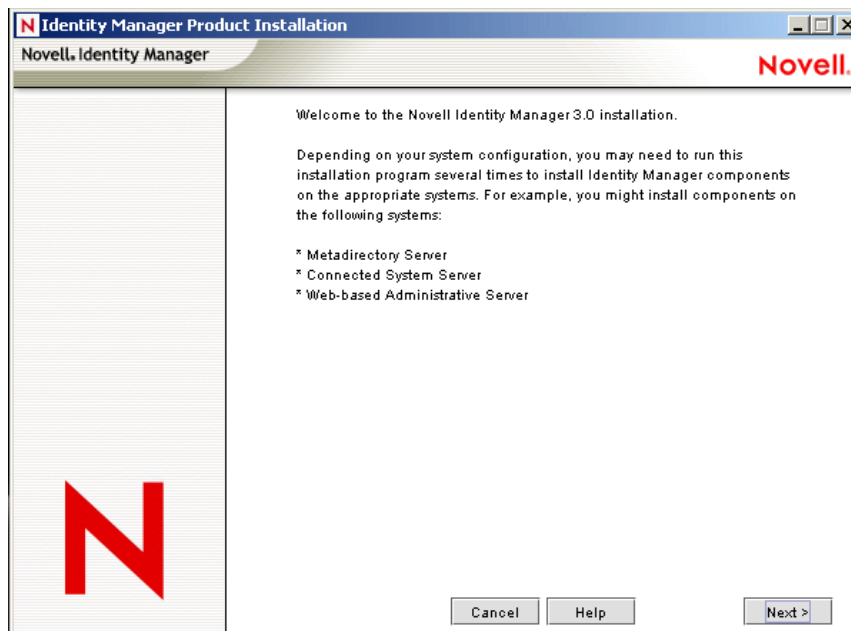
- 1 Download and extract the Identity Manager installation file.

You can download the Identity Manager installation file from [Novell's Download site \(http://download.novell.com\)](http://download.novell.com)

- 2 Once extracted, double-click the install.exe file found in the \NT directory.

After the files have finished copying, the Identity Manager Product Installation screen appears.

Figure 4-9 The Initial Identity Manager Installation Page

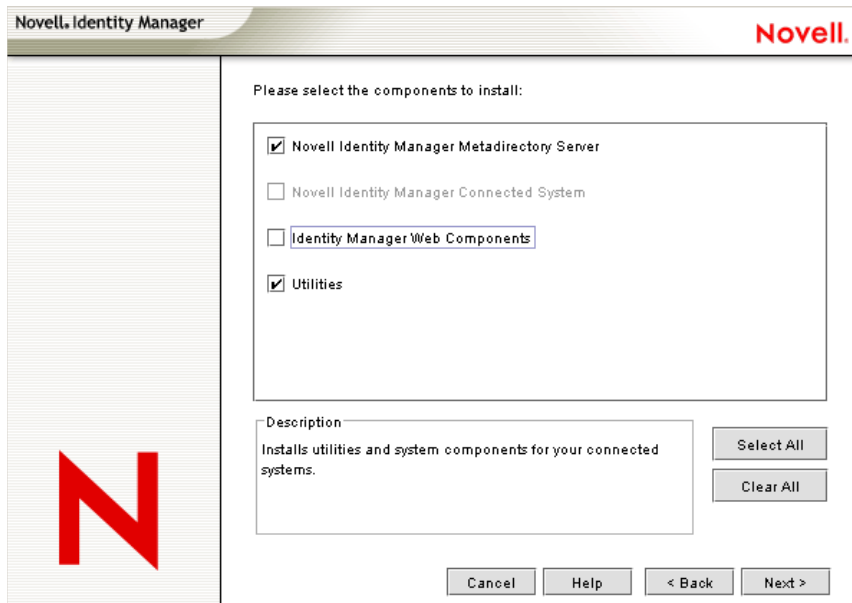


- 3 Click Next to begin the installation.
- 4 Read the license agreement, then click I Accept.
- 5 Review the Overview pages describing the system types, which include the Metadirectory Server, the Web Components, and the Utilities. Then click Next to continue.

This information is also covered in the table under [Section 4.2, “Identity Manager Components and System Requirements,”](#) on page 61.

6 On the Identity Manager Install page, select the components you want to install:

Figure 4-10 Identity Manager Installation Options



The following options are available:

- ♦ **Metadirectory Server:** Installs the Metadirectory engine and service drivers. These include Identity Manager Drivers for eDirectory, LDAP, JDBC, GroupWise, Delimited Text, Composer, Remedy, Avaya, SOAP, SIF, and the Novell Audit agent. Selecting this option also extends the eDirectory schema.

Novell eDirectory must be installed before you can install this option. Install the Metadirectory Server component where you want to run the Metadirectory engine for Identity Manager.

- ♦ **Connected System:** Installs the Remote Loader that allows you to establish a link between the connected system and a server running the Metadirectory engine. For Windows, this option installs the following drivers: Active Directory, Delimited Text, Exchange, GroupWise, JDBC, LDAP, Lotus Notes, NT Domain, PeopleSoft, Composer, Remedy, Avaya, SOAP, SAP, and SIF.

Install the Connected System to allow application connection from an application server to an eDirectory-based server running the Metadirectory engine. This procedure is covered under [Section 4.5, “Installing the Connected System Option on Windows,” on page 73](#).

- ♦ **Web Components:** This option installs driver configurations, iManager plug-ins, and application scripts and utilities.

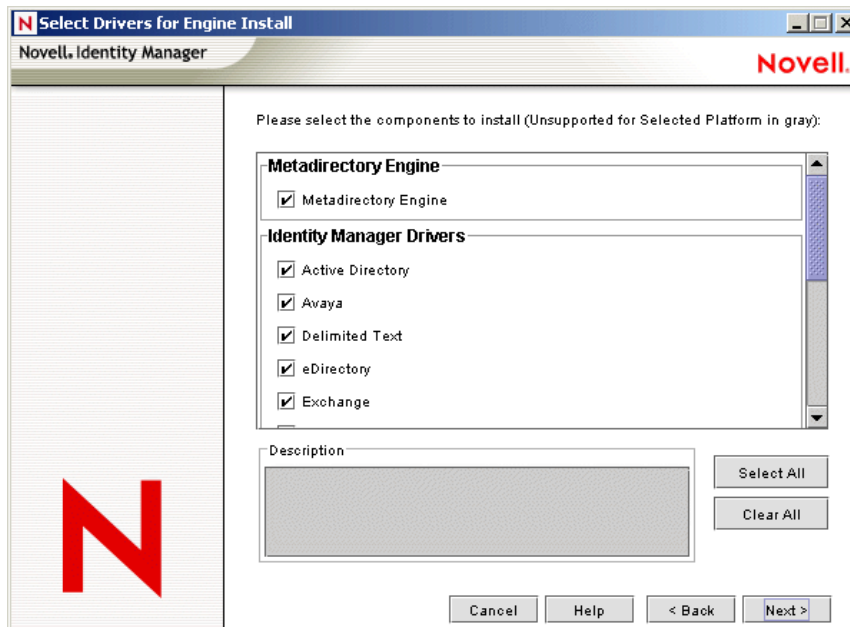
Novell iManager must be installed before you can install this option.

- ♦ **Utilities:** Installs additional scripts for the JDBC driver and utilities for other drivers. Most drivers don't have a utility connected to them.

7 Click Next.

- 8 Select the drivers you want to install, then click Next.

Figure 4-11 *Selecting Drivers for the Metadirectory Engine.*



The Select Drivers for Engine Install page shows you which drivers can be installed on a corresponding platform. By default, all available drivers are selected.

We recommend installing all of the driver files, so you won't need to run the installation program later if you want another driver. The driver files are not used until a driver is configured through iManager or through Designer.

- 9 When you see the informational message reminding you about product activation, click OK.
You need to activate the drivers within 90 days of installation; otherwise, they will shut down.
- 10 You will also see the Password Synchronization Upgrade Warning! message. Click OK.
This message is for Windows servers running Password Synchronization 1.0. If you want backward compatibility to 1.0, you must add additional policies to the driver configuration files. Without the policies, Password Synchronization 1.0 works for existing accounts, but not for new or renamed accounts

11 On the Schema Extension page, specify the following:

Figure 4-12 The Schema Extension Page

Schema Extension
Novell Identity Manager

Identity Manager schema will be extended during the install. Please provide the following information.

Tree Information

Tree name
2KS4TREE

User Login Information

User name in LDAP Format (Example: CN=admin,O=novell).
CN=admin,O=novell

Enter the user password.

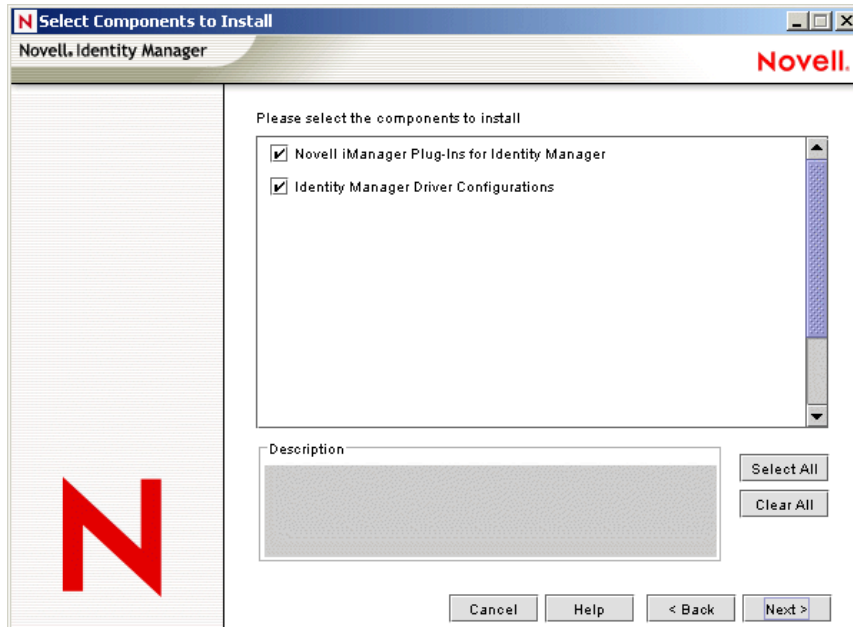
Cancel Help < Back Next >

- ♦ **User Name:** Specify the username (in LDAP format, such as CN=admin,O=novell) of a user (such as Admin) who has rights to extend the eDirectory schema.
- ♦ **User Password:** Specify the user's password.

12 Click Next. When the user information is validated, you see the first (of three) Components pages:

- 13 On the first Components page, select the driver configurations and the iManager plug-ins, then click Next.

Figure 4-13 First Components Page



You will see an additional screen that installs the Identity Manager plug-ins for iManager, using the SSL Port 443. Click Next.

- 14 On the second Components page, click Next.

The Novell Audit System Components for Identity Manager is highlighted if you have the Novell Audit System installed on the server. Otherwise, it is not selected. The Application Components selection installs components for such application systems as JDBC and PeopleSoft.

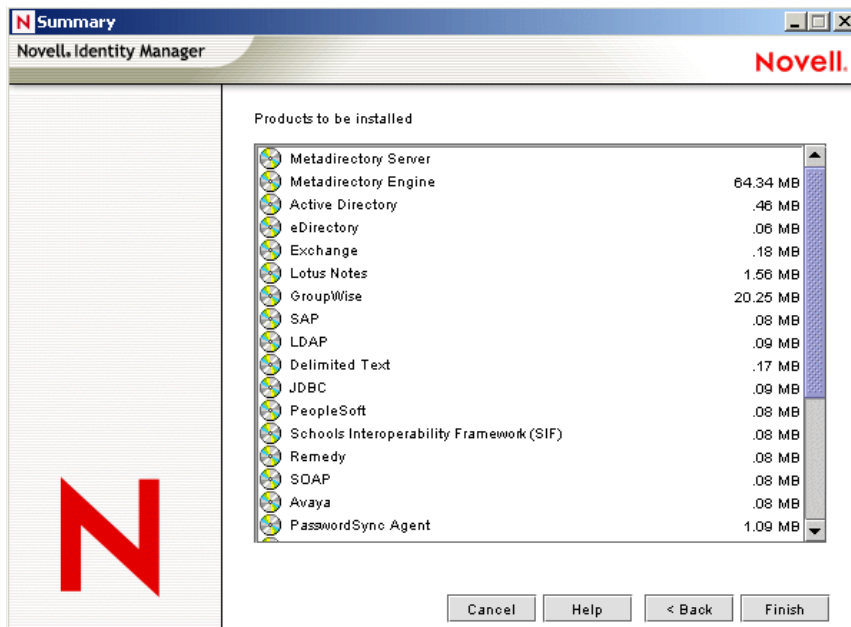
- 15 The third Components page installs the utilities. Click Next.

The Windows installation presents you with an additional screen showing the directory where the Application Components are placed. The default is C:\Novell\NDS\DirXMLUtilities. Click Next.

- 16 On the Select Components to Install page, platform-specific utilities are dimmed if they are available for platforms other than the one you are installing on. For Windows, all components are available, including SQL Scripts for JDBC Driver, PeopleSoft Components, License Auditing Tool, Active Directory Discovery Tool, Lotus Notes Discovery Tool, and SAP Utilities.

17 Read and verify your selections on the Summary page, then click Finish.

Figure 4-14 Summary Screen of the Products and Components



The Novell Identity Manager installation process shuts down eDirectory to extend the schema. The installation process commences installing the selected products and components.

18 After the installation completes and displays the Installation Complete dialog box, click Close. Restart the server to complete the installation of the Metadirectory engine and restart Tomcat.

4.5 Installing the Connected System Option on Windows

Section 4.4, “Installing Identity Manager on Windows,” on page 68 covered the installation of the Metadirectory Server, Web Components, and Utilities for Windows. Because Windows servers can use the Connected System option, installing the Connected System option is covered here.

Use the Connected System option when you don’t want to put the overhead of eDirectory services and the Metadirectory engine on an application server. The Remote Loader gives you desired synchronization through Identity Manager without the need to load applications that can be accessed elsewhere.

Before you begin, make sure your system meets the requirements listed in Section 4.2, “Identity Manager Components and System Requirements,” on page 61.

1 Download and extract the Identity Manager installation file.

You can download the Identity Manager installation file from [Novell's Download site \(http://download.novell.com\)](http://download.novell.com)

2 Run install.exe from the NT directory.

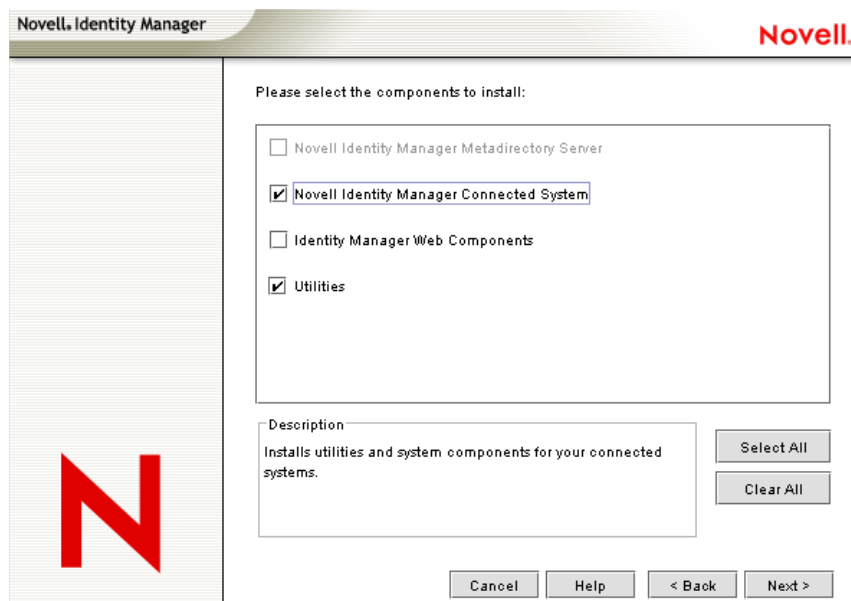
3 Read the Welcome information, then click Next.

4 Read the License Agreement, then click I Accept.

- 5 Review the Overview pages about the various systems and components, then click Next to begin the installation.
- 6 From the Identity Manager Install page, select the components Connected System and Utilities:
 - ♦ **Connected System:** Installs the Remote Loader that allows you to establish a link between a connected system and a server running the Metadirectory engine. This option can install the following drivers: Active Directory, Delimited Text, Exchange, GroupWise, JDBC, LDAP, Lotus Notes, NT Domain, PeopleSoft, Composer, Remedy, Avaya, Soap, SAP and SIF, or just the drivers you select.
 - ♦ **Utilities:** Installs additional scripts for the JDBC driver and other application utilities you select.

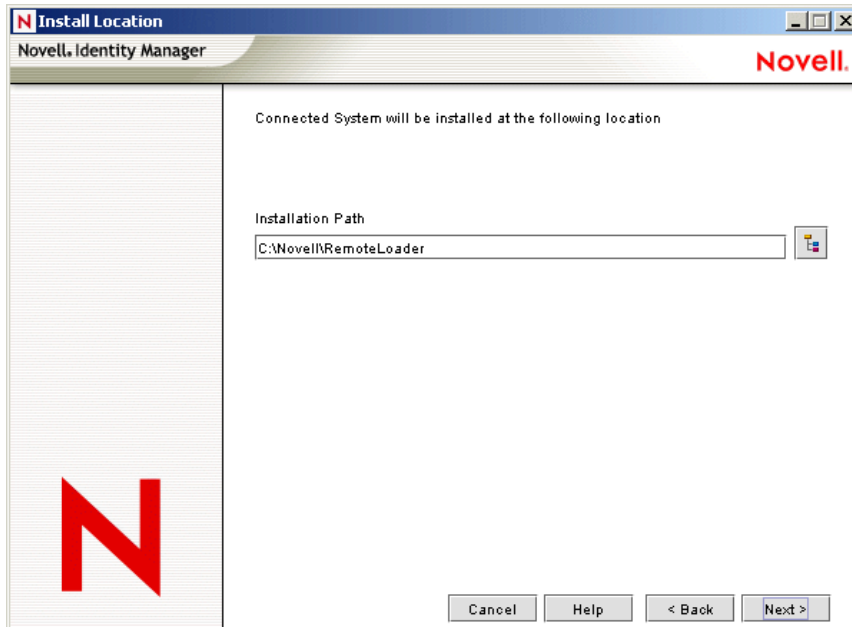
To select the Connected System option, first click Clear All, then select Connected System and Utilities. You should also select Web Components if you have the iManager utility installed on this server and you want Identity Manager plug-ins for Identity Manager and driver configurations added.

Figure 4-15 *The Connected System Option*



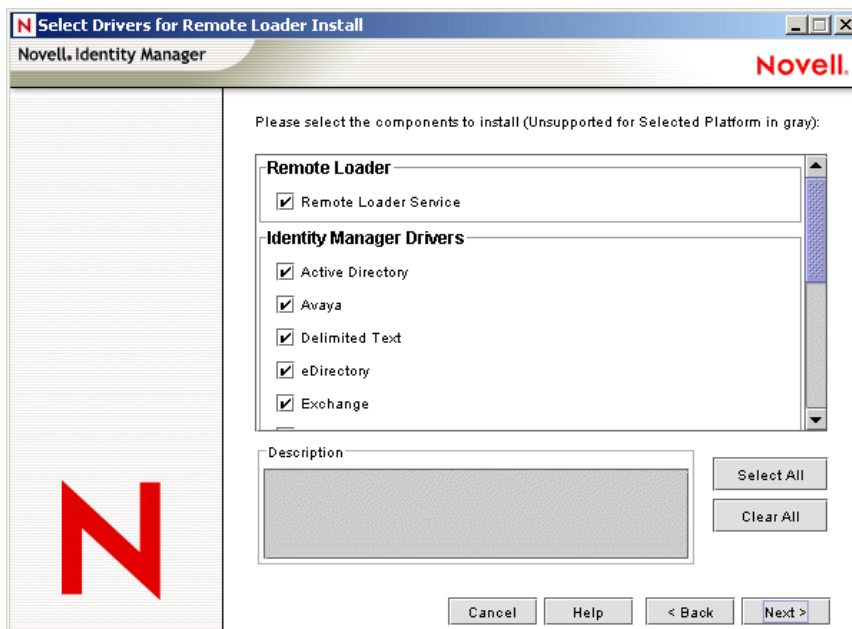
- 7 On the Install Location page, Click Next to accept the default directory path, which is C:\Novell\RemoteLoader.

Figure 4-16 *Selecting the Install Location.*



- 8 On the Select Drivers for Remote Loader Install page, select the Identity Manager drivers you want to load, then click Next. The selection includes Active Directory, Avaya, Delimited Text, eDirectory, Exchange, GroupWise, JDBC, LDAP, Lotus Notes, PeopleSoft, Remedy, SAP, SIF, and SOAP.

Figure 4-17 *Remote Loader and Identity Manager Drivers*



- 9 When you see the informational message reminding you about product activation, click OK.

You need to activate the drivers within 90 days of installation; otherwise, they will shut down.

- 10 You will also see the Password Synchronization Upgrade Warning! message. Click OK.

This message is for Windows servers running Password Synchronization 1.0. If you want backward compatibility to 1.0, you must add additional policies to the driver configuration files. Without the policies, Password Synchronization 1.0 works for existing accounts, but not for new or renamed accounts

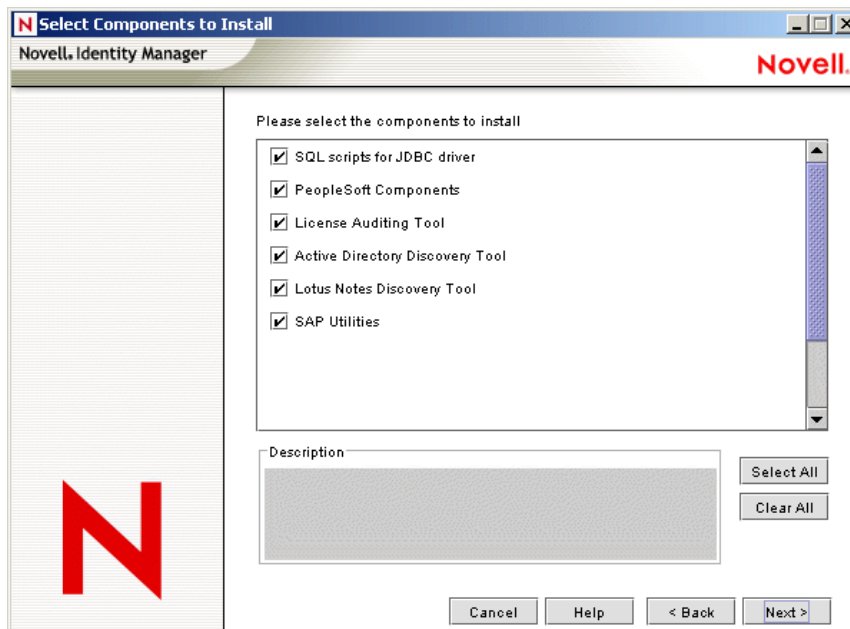
- 11 On the Components To Install page, click Next.

The Novell Audit System Components is highlighted if you have the Novell Audit System installed on the server. Otherwise, it is not selected. The Application Components selection installs components for such application systems as JDBC and PeopleSoft. Select the utilities you want to install.

- 12 Click Next to accept the default install path for Identity Manager utilities (C:\Novell\NDS\DirXMLUtilities).

- 13 Select the system components you want to install, then click Next.

Figure 4-18 System Components



- 14 Review the items listed in the Summary page. If you approve, click Finish to install the components.

- 15 Click Yes to add a shortcut to the Windows server's desktop.

- 16 Click Close to exit the installation program.

4.6 Installing Identity Manager on UNIX/Linux Platforms

Before you begin, make sure your system meets the requirements listed in [Section 4.2, "Identity Manager Components and System Requirements,"](#) on page 61.

- 1 Download and extract the tar file to a location of your choice.

You can download the Identity Manager installation file from [Novell's Download site \(http://download.novell.com\)](http://download.novell.com)

- 2 On the host computer, log in as root.
- 3 Execute the .bin file from the setup directory.

Change the current working directory to the setup directory, where the install is located. Then enter one of the following commands to run the install.

Platform	Example Path	Installation File
Linux	linux/setup/	dirxml_linux.bin
Solaris	solaris/setup/	dirxml_solaris.bin
AIX	aix/setup/	dirxml_aix.bin

These paths are relative to the root of the install image, which could be anywhere you expanded it or mounted the CD.

The installation program can't find the packages to install unless the current working directory is the directory where the installation program is located.

- 4 Review the Welcome information, the press Enter to continue the installation.

Figure 4-19 *The Welcome Screen*

```
=====
                                     (created with InstallAnywhere by Zero G)
=====

Introduction
-----

Welcome to the Novell Identity Manager 3.0 installation.

Depending on your system configuration, you may need to run this installation
program several times to install Identity Manager components on the appropriate
systems. These systems might include the following:

* Metadirectory Server
* Connected System Server
* Web-based Administrative Server

PRESS <ENTER> TO CONTINUE: █
```

- 5 Press Enter to progress through the license agreement, then enter Y if you agree to the usage terms. If you do not agree, enter N to exit the installation program.

Figure 4-20 *Choosing an Install Set*

```
DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N): y

=====
Choose Install Set
-----

Please choose the Install Set to be installed by this installer.

->1- Metadirectory Server
   2- Connected System Server
   3- Web-based Administrative Server

   4- Customize...

ENTER THE NUMBER FOR THE INSTALL SET, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
: █
```

- 6 Specify the appropriate number (1-4) for the install set you want to install. The install sets contain the following components:
- ♦ **Metadirectory Server:** Installs the Metadirectory engine and service drivers, Identity Manager drivers, Novell Audit agent, and extends the eDirectory schema.
Novell eDirectory must be installed before you can install this option.
 - ♦ **Connected System Server:** Installs the Remote Loader and the following drivers: LDAP, JDBC, eDirectory, SAP, Delimited Text, GroupWise, Composer, Remedy, Avaya, Soap, and Lotus Notes. You can choose the Connected System Server option when you don't want to put the overhead of eDirectory services and the Metadirectory engine on your application server.
 - ♦ **Web-based Administrative Server:** Installs the Identity Manager plug-ins and Identity Manager driver policies.
Novell iManager must be installed before you can install this option.
 - ♦ **Customize:** Installs the specific components you select from a list of all components.

Figure 4-21 Product Features

```
=====
Choose Product Features
=====

ENTER A COMMA SEPARATED LIST OF NUMBERS REPRESENTING THE FEATURES YOU WOULD
LIKE TO SELECT, OR DESELECT. TO VIEW A FEATURE'S DESCRIPTION, ENTER
'?<NUMBER>'. PRESS <RETURN> WHEN YOU ARE DONE:

  1- [X] Metadirectory Engine
  2- [ ] Remote Loader
  3- [X] eDirectory Driver
  4- [X] Delimited Text Driver
  5- [X] Groupwise Driver
  6- [X] JDBC Driver
  7- [X] LDAP Driver
  8- [X] Notes Driver
  9- [X] SAP Driver
 10- [X] AVAYA Driver
 11- [X] REMEDY Driver
 12- [X] SOAP Driver
 13- [ ] Identity Manager Plugins
 14- [ ] Identity Manager Policies

Please choose the Features to be installed by this installer.
: █
```

NOTE: Enter `prev` to return to previous menus and modify your installation options.

- 7** (Optional) Depending on the option you chose (such as the Metadirectory Server), you will be prompted to set the `LD_LIBRARY_PATH` environment variable. To do this, execute the `/opt/novell/eDirectory/bin/ndspath` script by typing `./opt/novell/eDirectory/bin/ndspath` and then re-run the installation.

If you select to install the Metadirectory Server, you are prompted for the LDAP user name and password (CN=admin,O=novell). Select a user (such as Admin) who has enough rights to extend the eDirectory schema.

Figure 4-22 Specifying User Name and Password in LDAP Format

```
=====
User Information
=====

Enter User Credentials to extend the Identity Manager Schema/iManager plug-ins:

User name in LDAP Format (Example: CN=admin,O=novell). (DEFAULT: )
: CN=admin,O=novell

=====

Enter User Password:
█
```

IMPORTANT: (Solaris installations only) If you are installing your Web-based Administration Server on the same server where eDirectory resides, when prompted for the Web Server Secure port, change the default value to some free port, such as 8443.

- 8 Verify that the information contained in the summary is correct and press Enter to start installing the packages.

Figure 4-23 *Installation Screen for Metadirectory Server*

```

=====
Installing...
-----

[=====|=====|=====|=====]
[-----]-----
Installing Manual Task Service Driver...
Installing Entitlement Service Driver...

Installing User Application Driver...
Installing Metadirectory Engine...
Installing Notes Driver...
Installing JDBC Driver...
Installing Delimited Text Driver...
Installing SAP Driver...
Installing LDAP Driver...
Installing eDirectory Driver...
Installing SOAP Driver...
Installing REMEDY Driver...
Installing AVAYA Driver...
Installing Groupwise Driver...
Starting eDirectory...
Installing Identity Manager Schema...
Extending Identity Manager Schema...
Installing NMAS 2.3 Objects...
---|-----]

=====
Installation Complete
-----

Congratulations. Novell Identity Manager 3.0 has been successfully installed
onto your system.

If you have installed Identity Manager Plugins, please restart your
Application server.

PRESS <ENTER> TO EXIT THE INSTALLER: █

```

eDirectory temporarily shuts down when installing the Metadirectory Engine and schema files. By default, all available drivers are installed so you won't need to run the installation program later if you want another driver. The driver files are not used until a driver is configured through iManager or through Designer and then deployed.

- 9 When you see the Installation Complete screen, press Enter to close the installation program.

4.7 Installing the Connected System Option on UNIX/Linux

Section 4.6, “Installing Identity Manager on UNIX/Linux Platforms,” on page 76 covered the installation of the Metadirectory Server, Web Components, and Utilities on UNIX platforms. Because UNIX or Linux servers can use the Connected System option, installing the Connected System option is covered here.

Use the Connected System option when you don't want to put the overhead of eDirectory services and the Metadirectory engine on an application server. The Remote Loader gives you desired synchronization through Identity Manager without the need to load applications that can be accessed elsewhere.

Before you begin, make sure your system meets the requirements listed in [Section 4.2, “Identity Manager Components and System Requirements,”](#) on page 61.

- 1 Download and extract the tar file to a location of your choice.

You can download the Identity Manager installation file from [Novell's Download site \(http://download.novell.com\)](http://download.novell.com)

- 2 On the host computer, log in as root.
- 3 Execute the .bin file from the setup directory.

Change the current working directory to the setup directory, where the install is located. Then enter one of the following commands to run the install.

Platform	Example Path	Installation File
Linux	linux/setup/	dirxml_linux.bin
Solaris	solaris/setup/	dirxml_solaris.bin
AIX	aix/setup/	dirxml_aix.bin

These paths are relative to the root of the install image, which could be anywhere you expanded it or mounted the CD.

The installation program can't find the packages to install unless the current working directory is the directory where the installation program is located.

- 4 Review the Welcome information, the press Enter to continue the installation.
- 5 Press Enter to progress through the license agreement, then enter Y if you agree to the usage terms. If you do not agree, enter N to exit the installation program.
- 6 Specify number 2 to install Connected System Server. The install set contains the following:
 - ♦ **Connected System Server:** Installs the Remote Loader and the following drivers: LDAP, SAP, JDBC, Delimited Text, GroupWise, Composer, Remedy, Avaya, Soap, and Lotus Notes. You can choose the Connected System Server option when you don't want to put the overhead of eDirectory services and the Metadirectory engine on your application server.

Figure 4-24 Pre-installation Summary

```
=====
Pre-Installation Summary
-----

Please Review the Following Before Continuing:

Product Name:
    Novell Identity Manager

Install Set
    Connected System Server

Product Components:
    LDAP Driver,
    SAP Driver,
    JDBC Driver,
    Delimited Text Driver,
    Notes Driver,
    Remote Loader,
    Groupwise Driver,
    AVAYA Driver,
    SOAP Driver,
    REMEDY Driver

PRESS <ENTER> TO CONTINUE: █
```

- 7 Review the items listed in the Pre-Installation Summary screen. Press Enter to install the components.

Figure 4-25 Installation Screen for Connected System Server

```
=====
Installing...
-----

[=====|=====|=====|=====]
[-----|-----|-----|-----]
Installing Manual Task Service Driver...
Installing Entitlement Service Driver...

Installing User Application Driver...
Installing Remote Loader...
Installing Notes Driver...
Installing JDBC Driver...
Installing Delimited Text Driver...
Installing SAP Driver...
Installing LDAP Driver...
Installing SOAP Driver...
Installing REMEDY Driver...
Installing AVAYA Driver...
Installing Groupwise Driver...
-----]

=====
Installation Complete
-----

Congratulations. Novell Identity Manager 3.0 has been successfully installed
onto your system.

If you have installed Identity Manager Plugins, please restart your
Application server.

PRESS <ENTER> TO EXIT THE INSTALLER: █
```

By default, all available drivers are installed so you won't need to run the installation program later if you want another driver. The driver files are not used until a driver is configured through iManager or through Designer and then deployed.

- 8 When you see the Installation Complete screen, press Enter to close the installation program.

4.8 Post-Installation Tasks

If one of the driver's parameters is set to Autostart and if the driver and eDirectory are running, the driver automatically launches the Identity Manager module. You do not need to manually load or unload Identity Manager. After Identity Manager installs, you should configure the drivers you installed to meet the policies and requirements defined by your business processes. Post-installation tasks typically include the following items:

- ◆ Configuring a Connected System. Refer to the [Identity Manager Driver Documentation \(http://www.novell.com/documentation/dirxml/drivers\)](http://www.novell.com/documentation/dirxml/drivers) for driver-specific configuration instructions.
- ◆ “Creating and Configuring a Driver ”
- ◆ “Defining Policies”
- ◆ “Starting, Stopping, or Restarting a Driver”
- ◆ “Activating Novell Identity Manager Products” on page 111

4.9 Installing a Custom Driver

A custom driver might consist of the following:

- ◆ A set of .jar or native (.dll, .nlm, or .so) files
- ◆ XML rules files for configuring the driver
- ◆ Documentation

For more information on creating a custom driver or installing one, see the [Novell Developer Kit \(http://developer.novell.com/ndk/dirxml-index.htm\)](http://developer.novell.com/ndk/dirxml-index.htm).

Installing the User Application

This section describes how to install the Identity Manager User Application. Topics include:

- ♦ [Section 5.1, “Prerequisites,” on page 85](#)
- ♦ [Section 5.2, “Installation and Configuration,” on page 86](#)
- ♦ [Section 5.3, “Creating the User Application Driver,” on page 87](#)
- ♦ [Section 5.4, “Installing the User Application,” on page 92](#)
- ♦ [Section 5.5, “Troubleshooting,” on page 108](#)

5.1 Prerequisites

Before you begin, verify that your environment supports the following:

Environment	Description
Identity Vault access	<p>The User Application requires credentials to log in to the Identity Vault. The credentials used to access the Identity Vault must:</p> <ul style="list-style-type: none"> ♦ Have full rights to the Identity Vault ♦ Must exist in the Identity Vault before you install the Identity Manager 3 User Application. <p>You are prompted for these credentials during installation. This user is referred to as the User Application Administrator.</p>
IDM User Application storage	<p>The computer where you will install the User Application must have 320 MB of storage available.</p>
JBoss	<p>RAM: The minimum recommended RAM for JBoss* when running the User Application is 512 MB.</p> <p>Port: The computer where JBoss is installed should have port 8080 free. JBoss allows Tomcat to use port 8080 by default. It is recommended that you install JBoss on a machine that has this port free.</p> <p>If the target machine also has an instance of iManager (or any other application that uses its own instance of Tomcat), you might end up with multiple Tomcat instances competing for the same port. You should either shut down other Tomcat instances or set the others to use a port other than 8080.</p>
MySQL	<p>The computer where MySQL is installed should have port 63306 free. The User Application installer installs MySQL at port number 63306 by default to avoid conflicts with any other MySQL server running on the machine.</p>

Environment	Description
Linux	<p>runlevel: The User Application installer needs XServer (XWindows), so your Linux runlevel must be set to 5 or higher.</p> <p>account: It is recommended that you run the install as a user without root privileges.</p> <p>install directory: Make sure it is writable. The User Application is typically installed using the directory structure <code>novell/idm</code> in the user's <code>home</code> directory but you can change this default.</p>

5.2 Installation and Configuration

Once you've installed all of the necessary prerequisite software and made sure your computer is properly set up, you can install the User Application. The order that you perform these tasks is important.

- ◆ The User Application expects certain artifacts to exist in the Identity Vault at runtime.
- ◆ The User Application relies on the User Application Driver for runtime communication with the Identity Manager 3 engine. (Conversely, if the User Application is not present, the User Application Driver might produce errors when it is turned on.)

1. Register the User Application driver with a given driver set. Do not turn it on yet. This step creates new objects in the Identity Vault with default data values (for some).

This step fails if you have not already installed Identity Manager. For more information, see [Section 5.3, “Creating the User Application Driver,” on page 87](#).

2. Run the User Application installation program. For more information, see [Section 5.4, “Installing the User Application,” on page 92](#).

3. Start your database. The default install leaves MySQL running.

If you chose the default install, the installer starts MySQL for you automatically. However, after a reboot, use the `start-mysql.sh` script (on Linux) or the `start-mysql.bat` (on Windows). It is located in `mysql` directory of your installation folder.

4. Start JBoss. When you use the User Application installer to install the JBoss application server, it provides a set of startup and shutdown scripts. They are located in the installation `/idm` directory. For example,

On Linux:

```
/idm/start-jboss.sh
```

On Windows:

```
\idm\start-jboss.bat
```

This is the recommended way to start JBoss.

- ◆ If you are using an existing JBoss application server then you cannot use these scripts and you need to do one of the following to avoid trusted certificate errors.
- ◆ Make sure that the `JAVA_HOME` points to the JRE installed by the User Application install program.

Or

- ♦ Change the keystore path value to point to the keystore for your existing JBoss install. The Identity Vault certificate will be downloaded to this location during the User Application install.
5. Turn on the User Application driver. This enables communication between the User Application and the driver. To turn on the User Application Driver:
 - a. Log into iManager.
 - b. In Roles and Tasks (left navigation frame), open the *Identity Manager* heading and select *Identity Manager Overview*.
 - c. In the content view that appears, specify the driver set that contains the User Application driver, then click *Search*.
 - d. A graphic appears, showing the driver set with its associated drivers. Click the minus sign in the red circular area at the upper right of the User Application Driver icon to turn the driver on.

NOTE: The driver, upon starting, attempts a handshake with the User Application. If JBoss isn't running or the WAR wasn't successfully deployed, the driver errors out.

6. Launch and log in to the User Application. Using your web browser, go to:

`http://hostname:port/ApplicationName`

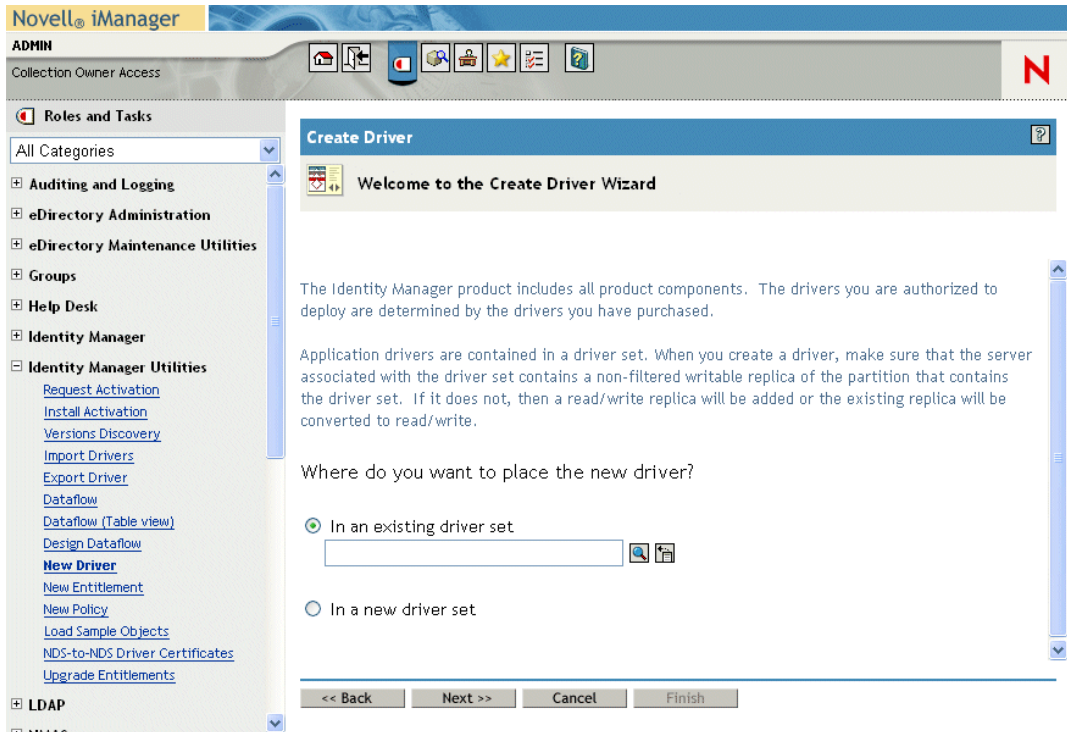
where *hostname:port* is the JBoss application server *ApplicationName* is IDM by default. You specified the application name during the install when providing JBoss configuration information. The Novell Identity Manager User Application home page should appear. In the upper right corner of that page, click *Login* to log in to the User Application.

5.3 Creating the User Application Driver

To create the User Application Driver and associate it with a driver set:

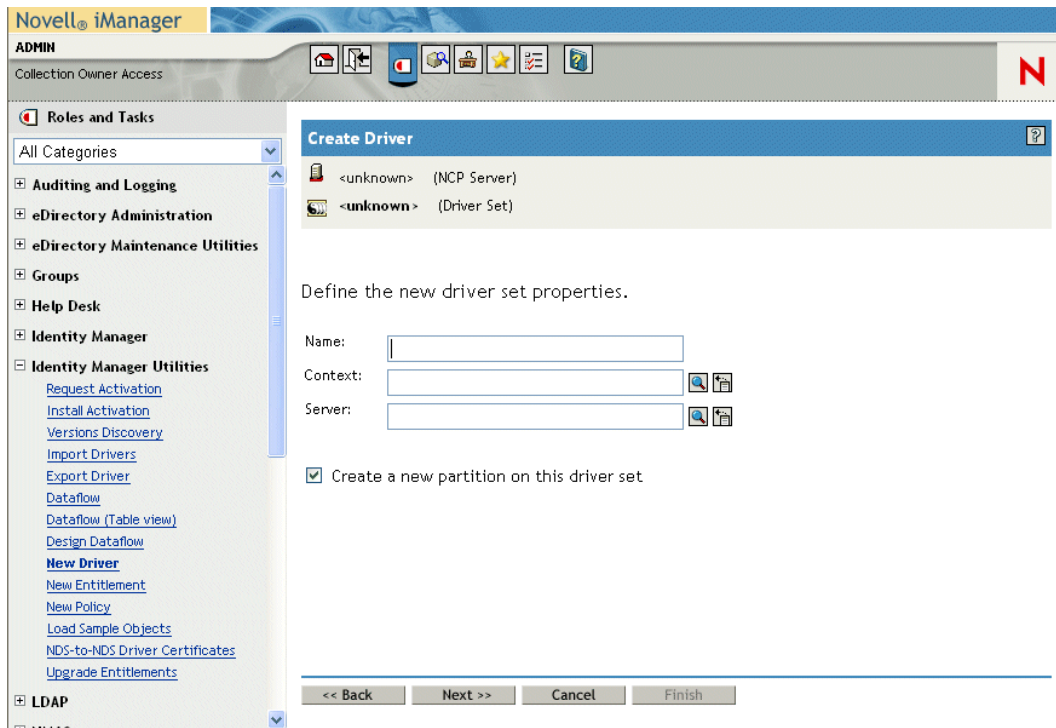
- 1 Log in to the Identity Vault with iManager (if you have not already done so).

- 2 Go to *Roles and Tasks > Utilities* and select *New Driver* to launch the Create Driver Wizard.



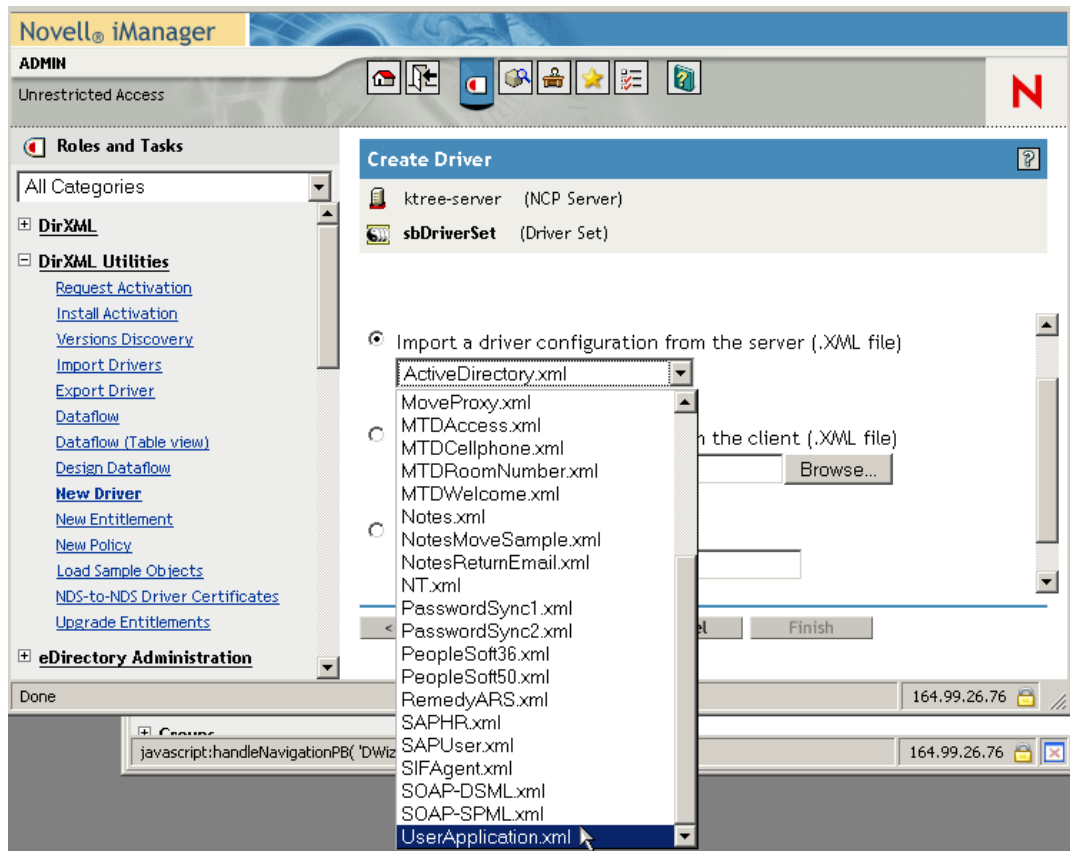
- 3 To create the driver in an existing driver set, click the Browse button locate the driver set. Then click *Next* and continue with **Step 4**.
Or to create the driver in a new driver set, select *In a new driver set* and click *Next*.

If you selected *In a new driver set*, you are prompted to define the new driver set properties.



3a Specify a name, a context, and a server for the driver set, then click *Next*. You are prompted for the driver XML file.

- Click *Import a driver configuration from the server (.XML file)*, then open the drop-down list of drivers.



- Select *UserApplication.xml*, then click *Next*.

NOTE: If *UserApplication.xml* is not listed in this drop-down list, you probably did not run the Web-Based Administration Server portion of the Identity Manager 3 install.

- Fill in the following fields:

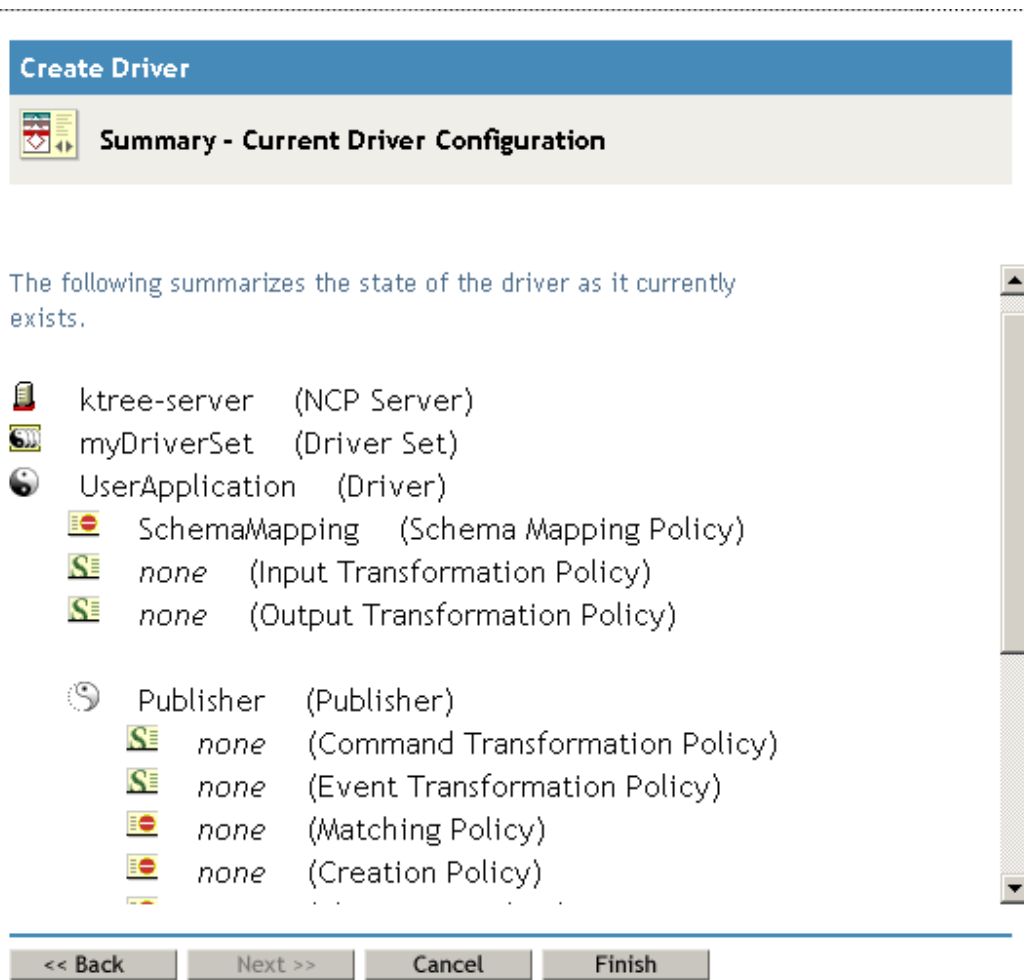
Field	Description
Driver Name	The name of the driver you are creating.
Authentication ID/Password	The Distinguished Name and associated password of the User Application Administrator. For example: <code>cn=admin,ou=orgunit,o=novell</code>
Application Context	The name of the User Application context (specified at install, for example, IDM.)
Host	The host name or IP address of the application server where the Identity Manager User Application is deployed. If the User Application is running in a cluster, type the dispatcher's host name or IP address.
Port	The port for the host (above).

- 7 Click *Next*.
- 8 Enter or edit the driver's configuration parameters, then click *Next*.
- 9 Click *Define Security Equivalences* to display the Security Equals window. Use the navigation widget to navigate to and select an administrator (or other Supervisor) object. Then click *Add* to make the driver equivalent to the object selected.

This step gives the driver the security permissions it needs. Details about the significance of this step can be found in your Identity Manager documentation.

- 10 (Optional, but recommended). Click *Exclude 'Administrative Roles'*. Click *Add*, select *Administrator*, click *OK*, click *OK*. Then click the *Next* button at the bottom. Close the popup window by clicking *OK*.

A summary screen displays.



- 11 Accept the information by clicking *Finish*. If a page appears with a *Finish with Overview* button, click that button.

You should now see the driver set and its attached drivers. The driver is turned off (the minus sign displays in the small red circle in the upper right corner of the driver graphic).

IMPORTANT: Leave the driver *off* until the User Application has been installed.

5.4 Installing the User Application

After you have created the User Application driver, you install the Identity Manager User Application.

5.4.1 About the Installation Program

The Novell Identity Manager User Application is a Java Web Application Archive (WAR) file that is deployed to the JBoss application server. It uses a database (MySQL by default) to store configuration information. Depending on the type of installation you choose, the User Application installation program does the following also:

- ◆ Installs JBoss or lets you specify an existing version of JBoss
- ◆ Installs MySQL or lets you specify an existing version of MySQL, Oracle or Microsoft SQL Server 2000.
- ◆ Configures the JRE's certificates file so that the User Application (running on JBoss) can securely communicate with the Identity Vault and the User Application Driver.
- ◆ Configures and deploys the WAR file to the JBoss application server.
- ◆ Enables Novell Audit logging.

Installation Scripts and Executables

To install the Novell Identity Manager User Application, you need the following files:

File	Description
Linux platforms:	Launches the installation program.
◆ IdmUserApp.bin	
Windows platforms:	
◆ IdmUserApp.exe	
User Application WAR	IDM.war: Includes the Identity Manager 3 User Application with Identity Self-Service features. IDMProv.war: Installs the Provisioning Module for Identity Manager 3.

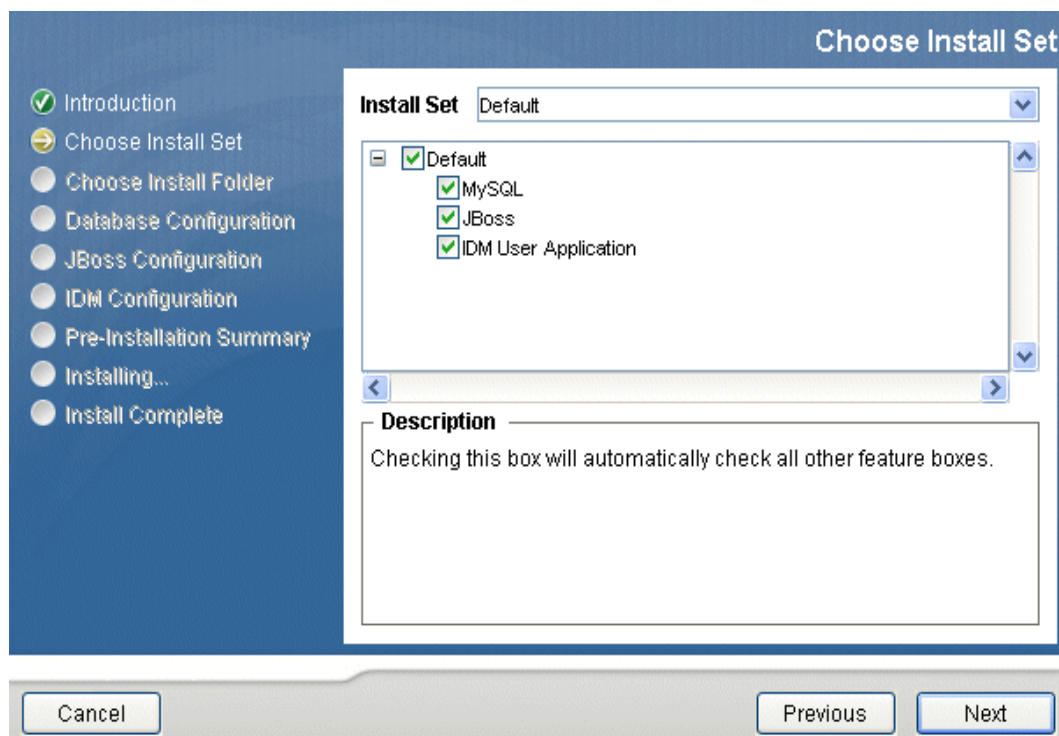
TIP: Make sure to stop any other versions of MySQL on the install machine. If you have other versions running during the install, the installer will not start a new MySQL server and will not create a new database.

To launch the installer:

- 1 Obtain the appropriate installation files described in [“Installation Scripts and Executables” on page 92](#).
- 2 Launch the program for your platform as described below:

Platform	Action
Linux	<p>1. Log in as a non-root account and open a terminal session.</p> <p>You must be logged into your Linux machine as a user other than root. If you are already logged in as root, log out and then log back in as another user. Do not simply “su” to another account in a terminal session, because the graphics state will not transfer to the other account. (We also do not recommend “sux.”)</p> <p>2. Execute the following command at the console:</p> <pre>./IdmUserApp.bin</pre> <p>The script unpacks a Java Runtime Environment (JRE) and launches a Zero-G installer application.</p>
Windows	<p>On Windows, double-click the <code>IdmUserApp.exe</code> file found in the <code>\NT</code> directory.</p>

- 3 Read the license agreement, then click *I accept the terms of the License Agreement*.
- 4 Click *Next* in the Introduction page of the install wizard.



- 5 Choose your install set, then click *Next*.

Install Option	What It Does
Default	<p>Installs and configures the following:</p> <ul style="list-style-type: none"> ◆ IDM user application WAR ◆ JBoss: Installs a JBoss application server or configures an existing one. For new application servers, it: <ul style="list-style-type: none"> ◆ Creates a server configuration whose name is the name you supply in the Application Name field (specified during the installation procedure). The configuration is based on the Default or All configuration. ◆ Creates scripts for starting and stopping the server. ◆ MySQL: Installs MySQL or configures an existing MySQL database. For new MySQL installations, it creates scripts for starting and stopping the database server.
Custom:	<p>IDM User Application</p> <ul style="list-style-type: none"> ◆ Installs the IDM User Application and allows you to specify an existing database and JBoss server. Supported database types are MySQL, Oracle9i, Oracle10g, and Microsoft SQL Server 2000. <p>JBoss</p> <ul style="list-style-type: none"> ◆ Install a JBoss application server or allows you to select an existing JBoss application server to use. When it installs a new application server, this option does two things: <ul style="list-style-type: none"> ◆ Creates a server configuration whose name is the name you supply in the Application Name field (specified during the installation procedure). The configuration is based on the Default or All configuration. ◆ Creates scripts for starting and stopping it. <p>MySQL</p> <ul style="list-style-type: none"> ◆ Installs MySQL. It does not create scripts for starting and stopping (unlike the default option.)

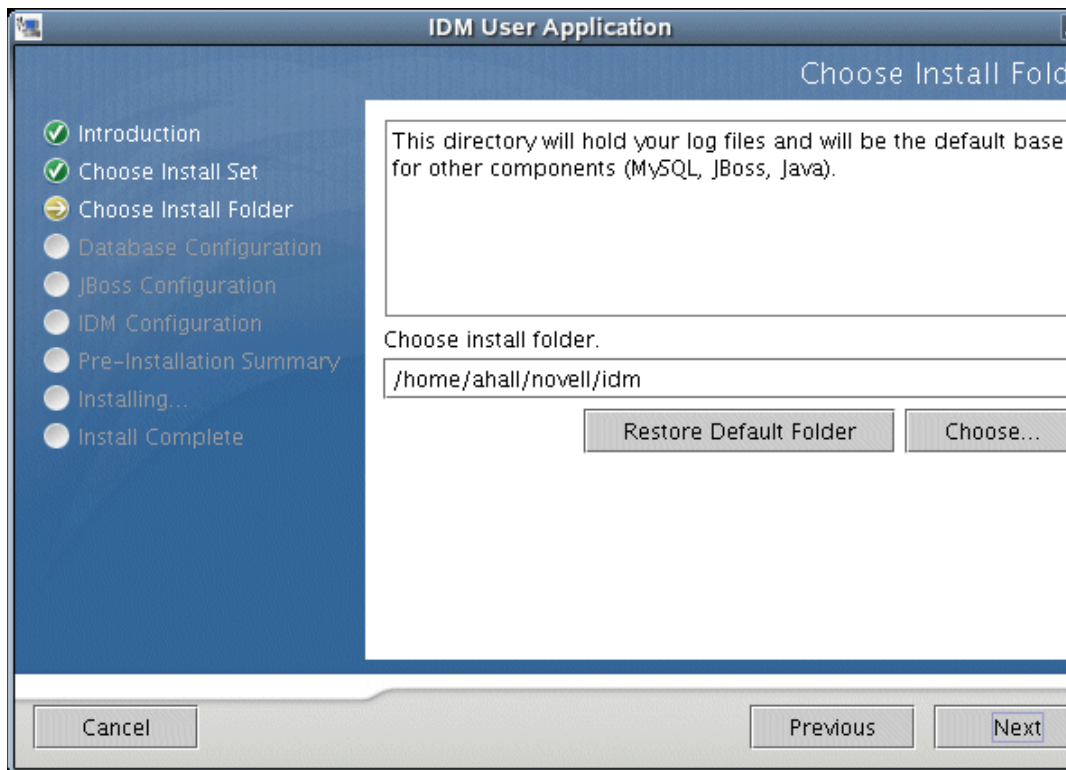
6 Follow the instructions for your installation type:

Installation Type	Action
Default install	<p>Go to:</p> <ul style="list-style-type: none"> ◆ Section 5.4.2, “Selecting an Install Folder,” on page 95 ◆ Section 5.4.3, “Specifying MySQL Details,” on page 96 ◆ Section 5.4.4, “Specifying the Database Host and Port,” on page 97 ◆ Section 5.4.5, “Specifying the JBoss Server Settings,” on page 98 ◆ Section 5.4.6, “Selecting the JBoss Server Configuration Type,” on page 99 ◆ Section 5.4.7, “Enabling Novell Audit Logging,” on page 99 ◆ Section 5.4.8, “Configuring the User Application,” on page 101

Installation Type	Action
Custom: JBoss	Go to: <ul style="list-style-type: none"> ◆ Section 5.4.5, “Specifying the JBoss Server Settings,” on page 98
Custom: MySQL	Go to: <ul style="list-style-type: none"> ◆ Section 5.4.3, “Specifying MySQL Details,” on page 96
Custom: IDM User Application	Go to: <ul style="list-style-type: none"> ◆ Section 5.4.2, “Selecting an Install Folder,” on page 95 ◆ Section 5.4.9, “Choosing a Database Platform,” on page 106 ◆ Section 5.4.4, “Specifying the Database Host and Port,” on page 97 ◆ Section 5.4.10, “Specifying the Database Name and Privileged User,” on page 107 ◆ Section 5.4.5, “Specifying the JBoss Server Settings,” on page 98 ◆ Section 5.4.6, “Selecting the JBoss Server Configuration Type,” on page 99 ◆ Section 5.4.7, “Enabling Novell Audit Logging,” on page 99 ◆ Section 5.4.8, “Configuring the User Application,” on page 101

5.4.2 Selecting an Install Folder

1 Complete selections on the following page:



NOTE: On Linux, if you see `/root` anywhere in the path, cancel the installation and log in again as a non-root user.

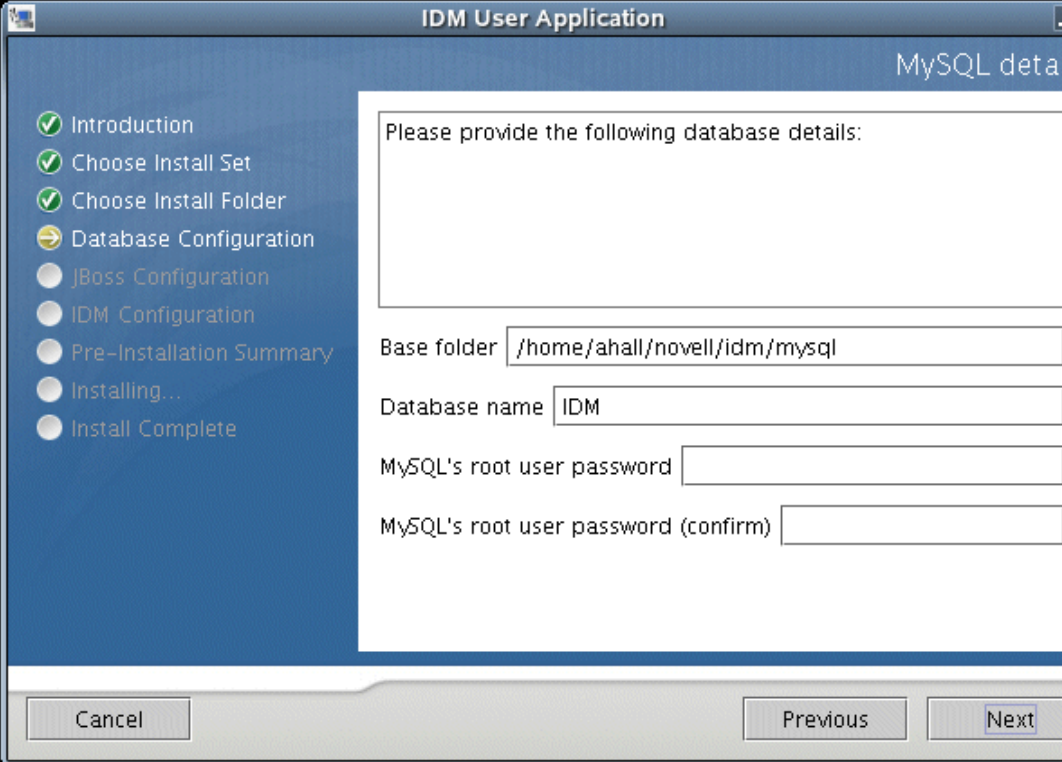
2 Click *Next*.

If you chose:

- ♦ *Default:* Go to [Section 5.4.3, “Specifying MySQL Details,”](#) on page 96.
- ♦ *Custom: IDM User Application:* Go to [Section 5.4.9, “Choosing a Database Platform,”](#) on page 106.

5.4.3 Specifying MySQL Details

1 Complete selections in the following page:



The screenshot shows a window titled "IDM User Application" with a sub-header "MySQL details". On the left is a navigation pane with the following items: Introduction (checked), Choose Install Set (checked), Choose Install Folder (checked), Database Configuration (highlighted with a yellow arrow), JBoss Configuration, IDM Configuration, Pre-Installation Summary, Installing..., and Install Complete. The main area contains the text "Please provide the following database details:" followed by four input fields: "Base folder" with the value "/home/ahall/novell/idm/mysql", "Database name" with the value "IDM", "MySQL's root user password", and "MySQL's root user password (confirm)". At the bottom are "Cancel", "Previous", and "Next" buttons.

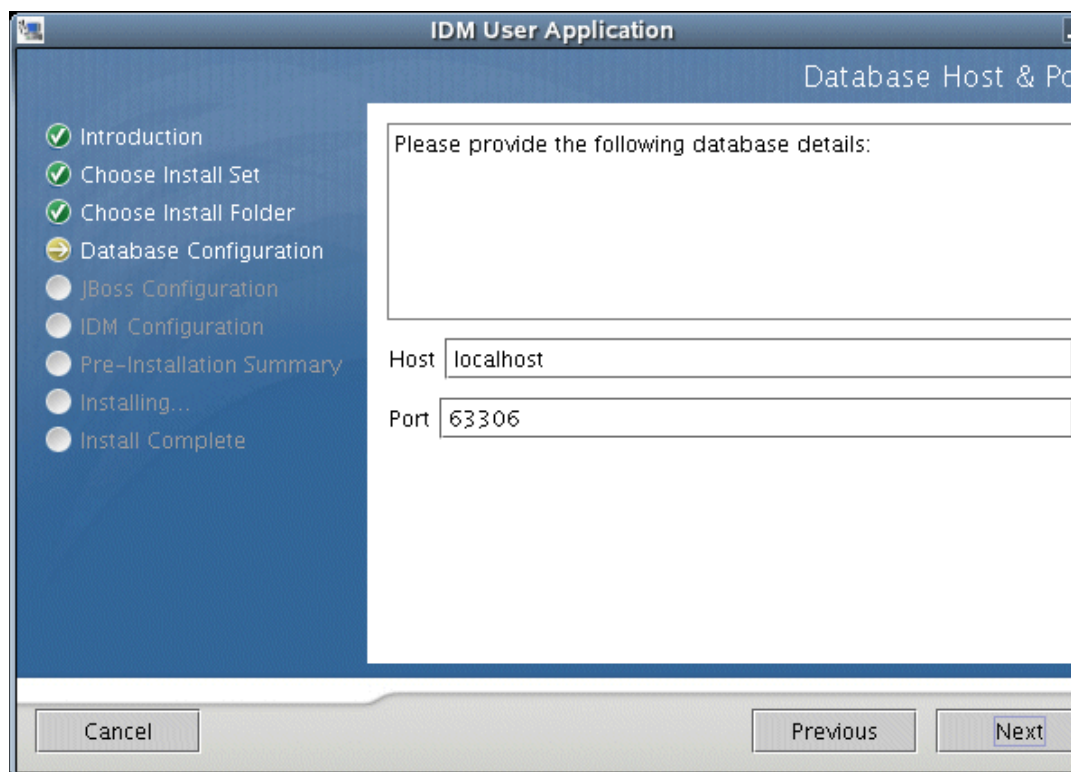
Field	Description
Base folder	Specify the location where you want the installer to create a new MySQL database.
Database name	Specify the name of the database you want the installer to create.

Field	Description
MySQL's root user password	<p>Enter the database password used for the MySQL database root user.</p> <p>This is not the same as your Linux root user account password. The IdmUserApp installer creates a new installation of MySQL on your machine, and in the process of doing that, it creates a database root account. You are specifying the password for the MySQL account.</p>

- 2 Click *Next* to access the page for [Section 5.4.4, “Specifying the Database Host and Port,”](#) on [page 97](#).

5.4.4 Specifying the Database Host and Port

- 1 Complete selections on the following page:



Field	Description
Host	Specify the database server's host name or IP address
Port	<p>Specify the database's listener port number.</p> <p>The default for MySQL is 63306.</p>

- 2 Click *Next*.

If you chose:

- ♦ *Custom: MySQL install:* You'll see the Pre-Install Summary. If everything is satisfactory, click *Install*.
- ♦ *Custom: IDM User Application:* Go to [Section 5.4.10, "Specifying the Database Name and Privileged User,"](#) on page 107.
- ♦ *Other install sets:* Go to [Section 5.4.5, "Specifying the JBoss Server Settings,"](#) on page 98.

5.4.5 Specifying the JBoss Server Settings

1 Complete selections on the following page:

The screenshot shows a window titled "IDM User Application" with a sub-header "JBoss Configuration". On the left is a vertical list of steps: Introduction, Choose Install Set, Choose Install Folder, Database Configuration, JBoss Configuration (highlighted with a yellow arrow), IDM Configuration, Pre-Installation Summary, Installing..., and Install Complete. The main content area contains a text box with the text: "Please provide details about JBoss. We will either configure JBoss for you using these values (if we are installing it), or use these values to configure your existing JBoss installation." Below this are three input fields: "Base folder" with the value "/home/ahall/novell/idm/jboss", "Host" with the value "localhost", and "Port" with the value "8080". At the bottom are three buttons: "Cancel", "Previous", and "Next".

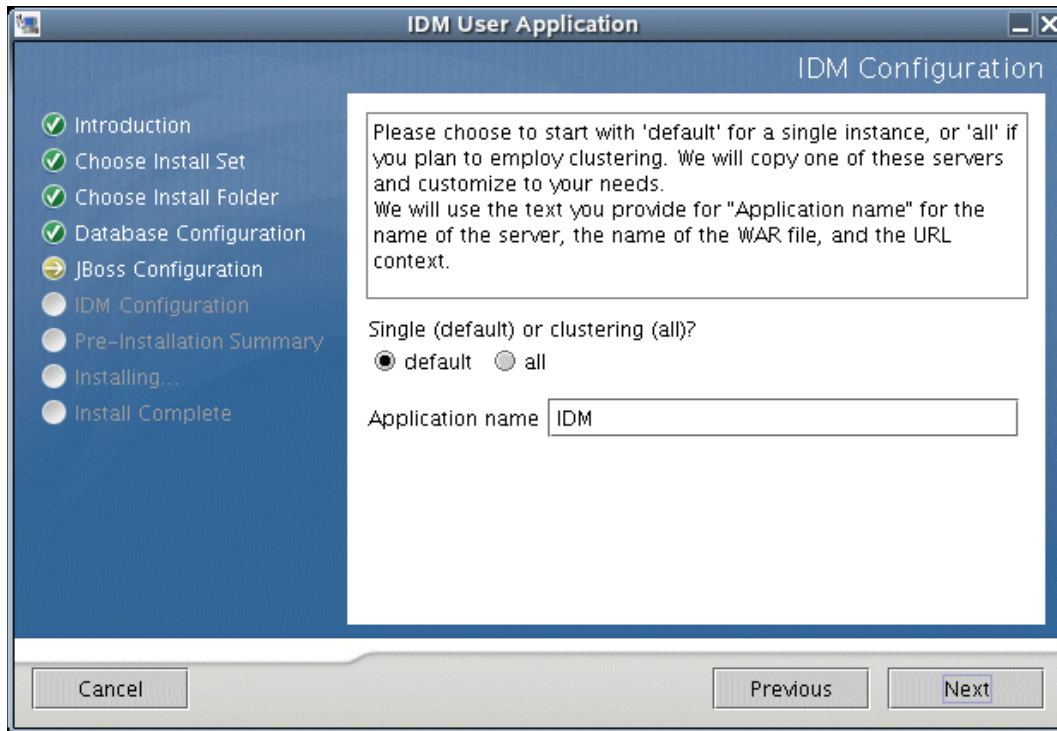
Field	Description
Base folder	Specify the location where you want the installer to create a new JBoss database.
Host	Specify the application server's host name or IP address.
Port	Specify the JBoss listener port number. The default is 8080.

2 Click *Next*. If you chose:

- ♦ *Custom: JBoss install:* You'll see the Pre-Install Summary. If everything is satisfactory, click *Install*.
- ♦ *Other install sets*—Go to [Section 5.4.6, "Selecting the JBoss Server Configuration Type,"](#) on page 99.

5.4.6 Selecting the JBoss Server Configuration Type

1 Complete selections on the following page:



Option	Description
Single (default) or clustering (all)	Choose the type of JBoss server configuration (All for clustering, Default otherwise) The installation script creates a server configuration based on the server base you select. The configuration name is the same name as the Application Name you specify next.
Application name	Specify the User Application context name. This name is part of the URL used to access the User Application.

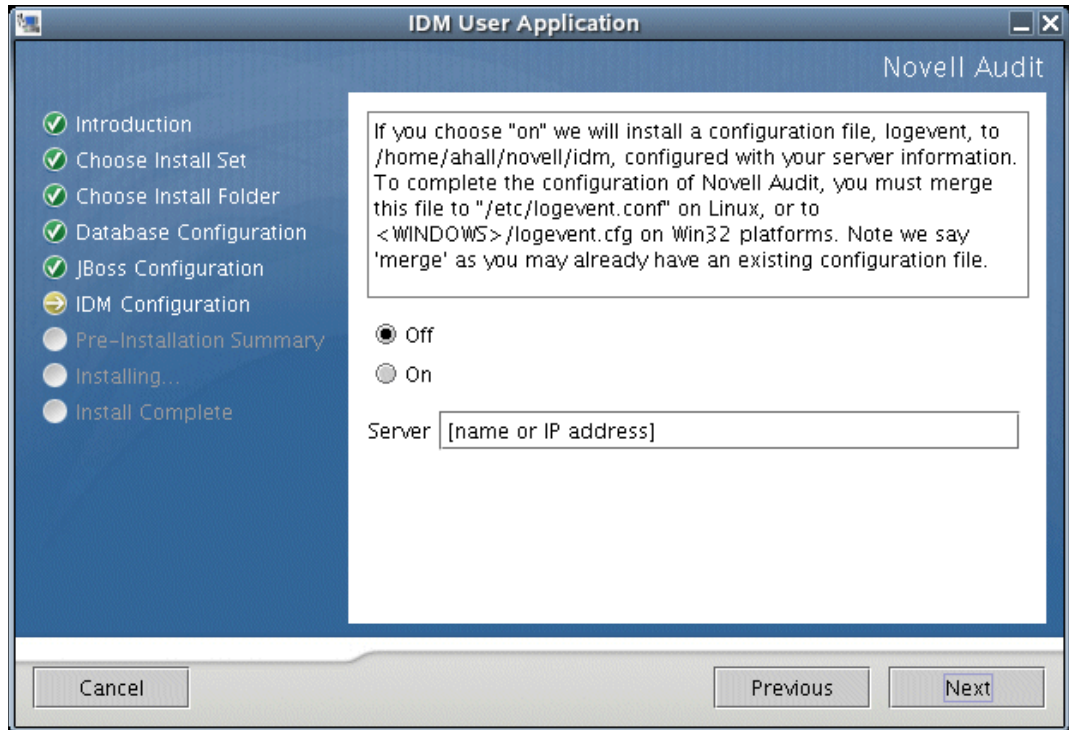
2 Click *Next*. If you chose:

- ♦ *Custom: JBoss install:* You'll see the Pre-Install Summary. If everything is satisfactory, click *Install*.
- ♦ *Other install sets:* Go to [Section 5.4.7, "Enabling Novell Audit Logging,"](#) on page 99.

5.4.7 Enabling Novell Audit Logging

To enable Novell Audit logging for the User Application:

- 1 Complete selections on the following page:



Field	Description
On	Enables Novell Audit Logging for the User Application. For more information on setting up Novell Audit logging, see the <i>Identity Manager User Application: Administration Guide</i> .
Off	Disables Novell Audit Logging for the User Application. You can enable it later using the Administration tab of the User Application. For more information on enabling Novell Audit logging, see the <i>Identity Manager User Application: Administration Guide</i> .
Server	Specify the host name or IP address for the Novell Audit server.

- 2 Click *Next*, then continue with [Section 5.4.8, “Configuring the User Application,”](#) on page 101.

5.4.8 Configuring the User Application

There are two pages for this configuration. One page lets you provide basic configuration information; the other is for advanced users and lets you configure additional parameters.

- 1 Complete selections on the following page:

The screenshot shows a window titled "User Application Configuration" with the following sections and fields:

- eDirectory Connection Settings**
 - LDAP Host: your_LDAP_host:secure_port
 - LDAP Administrator: cn=your_username,o=your_organization
 - LDAP Administrator Password: [Empty]
 - Confirm Password: [Empty]
- eDirectory DNs**
 - Root Container DN: [Empty] [Search]
 - Provisioning Driver DN: [Empty] [Search]
 - User Application Admin: [Empty] [Search]
 - User Container DN: [Empty] [Search]
 - Group Container DN: [Empty] [Search]
- eDirectory Certificates**
 - Keystore Path: /home/ahall/novell/idm/jre/lib/security/c ...
 - Keystore Password: [Empty]
 - Confirm Keystore Password: [Empty]
- Email**
 - Email Notify Host: [Empty]
 - Email Notify Port: [Empty]
 - Email Notify Secure Port: [Empty]

Buttons at the bottom: OK, Cancel, Show Advanced Options

Field	Description
LDAP Host	Required. Specify the host name or IP address for your LDAP server and its secure port. For example: myLDAPHost:636

Field	Description
LDAP Administrator and password	Required. Specify the credentials for the LDAP administrator. This user must already exist. The User Application uses this account to make an administrative connection to the Identity Vault.
Root Container DN	Required. Specify the LDAP distinguished name of the root container. This is used as the default entity definition search root when no search root is specified in the directory abstraction layer.
Provisioning Driver DN	Required. Specify the distinguished name of the User Application Driver that you created earlier in the section on Section 5.3, "Creating the User Application Driver," on page 87 . For example, if your driver is <code>UserApplicationDriver</code> and your driver set is called <code>myDriverSet</code> , and the driver set is in a context of <code>o=myCompany</code> , you would enter a value of: <code>cn=UserApplicationDriver,cn=myDriverSet,o=myCompany</code>
User Application Administrator	Required. An existing user in the Identity Vault that has the authority to perform any administrative task in the Identity Vault. This user can: <ul style="list-style-type: none"> ◆ Use the Administration tab of the User Application ◆ Use iManager to administer workflow tasks ◆ Create new provisioning requests
User Container DN	Required. Specify the LDAP distinguished name (DN) or fully qualified LDAP name of the user container. This defines the search scope for users and groups. Users in this container (and under) are allowed to log in to the User Application. IMPORTANT: Be sure the User Application Administrator specified during User Application Driver setup exists in this container if you want that user to be able to execute workflows.
Group Container DN	Required. Specify the LDAP distinguished name (DN) or fully qualified LDAP name of the group container. Used by entity definitions within the directory abstraction layer.
Keystore Path	Required. Specify the full path to your keystore (<code>cacerts</code>) file of the JRE that the JBoss application server is using to run or else click the small browser button and navigate to (and select) your <code>cacerts</code> file in the <code>/idm/jre/lib/security/</code> path). The utility must have permission to write to this file.

Field	Description
Keystore Password/Confirm Keystore Password	Required. Specify the cacerts password. The default is <i>changeit</i> .
Email Notify Host	Specify the JBoss server hosting the Identity Manager User Application. For example: <code>myJBossServer</code>
Email Notify Port	This value replaces the \$HOST\$ token in e-mail templates. The URL that gets constructed is the link to provisioning request tasks and approval notifications. Used to replace the \$PORT\$ token in e-mail templates used in provisioning request tasks and approval notifications.
Email Notify Secure Port	Used to replace the \$SECURE_PORT\$ token in e-mail templates used in provisioning request tasks and approval notifications.

2 (Optional) Click *Show Advanced Options*. Complete selections on the following page:

The screenshot shows a 'User Application Configuration' dialog box with the following fields and values:

- eDirectory Connection Settings:**
 - LDAP Host: your_LDAP_host:secure_port
 - LDAP Administrator: cn=your_username,o=your_organization
 - LDAP Administrator Password: (empty)
 - Confirm Password: (empty)
 - Connection Timeout (millis): 300000
 - Provider Referrals: ignore
 - Dereference Aliases: never
- eDirectory DNs:**
 - Root Container DN: (empty)
 - Provisioning Driver DN: (empty)
 - User Application Admin: (empty)
- Meta-Directory User Identity:**
 - User Container DN: (empty)
 - User Object Class: inetOrgPerson
 - Login Attribute: cn
 - User Membership Attribute: groupMembership
- Meta-Directory User Groups:**
 - Group Container DN: (empty)
 - Group Object Class: groupOfNames

Buttons at the bottom: OK, Cancel, Hide Advanced Options.

Field	Description
Connection Timeout (millis)	Time to wait (in milliseconds) for a user connection to the LDAP server before timing out.
Provider referrals	This property is sent from JNDI application to the LDAP server to indicate how to handle referrals. Valid values are Ignore, Follow, and Throw.
Dereference Aliases	This attribute contains entries returned from the LDAP operation whether they are dereferenced (true path) or not dereferenced (alias). Valid values are Never, Always, Finding, and Searching.
User Object class	The LDAP user object class (typically inetOrgPerson).

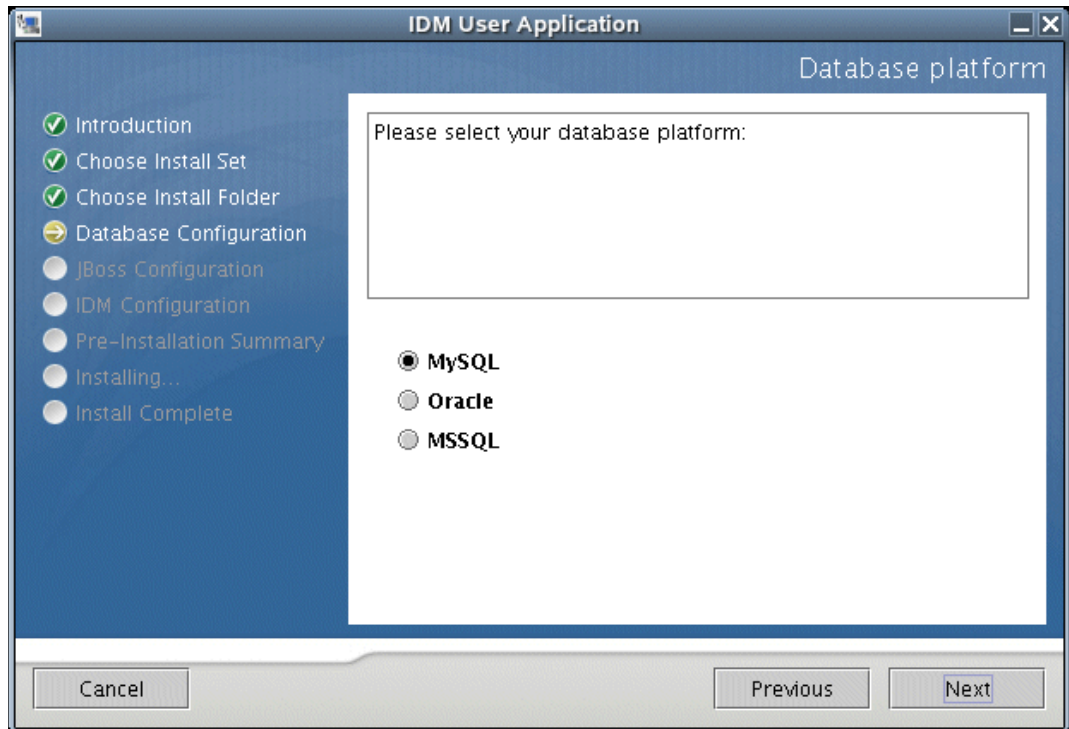
Field	Description
Login Attribute	The attribute (such as CN) that represents the user's login name.
User membership attribute	Optional. The attribute that represents the user's group membership. No spaces allowed.
Group Object Class	The LDAP group object class.
Group Membership Attribute	The attribute representing the user's group membership. Do not use spaces in this name.
Use Dynamic groups	Select this option if you want to use dynamic groups.
Dynamic Group Object Class	The LDAP dynamic group object class.
ICS Logout Enabled	If this option is selected, the application supports User Application and iChain [®] simultaneous logout.
ICS Logout Page	The URL to the iChain logout page.
Email Notify Protocol	Specify one of these values: <ul style="list-style-type: none"> ◆ HTTP ◆ HTTPS Used to replace the \$PROTOCOL\$ token in e-mail templates used in provisioning request tasks and approval notifications.
Email Notify Secure Protocol	Used to replace the \$SECURE_PROTOCOL\$ token in e-mail templates used in provisioning request tasks and approval notifications.
Session Timeout	Specify the number of minutes that user sessions can be inactive. By default, the user application times out of a session after 20 minutes.
DataSource	Specify the JNDI name of your connection pool. By default, the connection pool JNDI name is java:/IDM.
Add a New Container Object	Enter the LDAP name of an object class that can serve as a container.

NOTE: To modify these values after completing the install, run the `configupdate.sh` script (on Linux) or the `configupdate.bat` file (on Windows). These files are located in your installation subdirectory. The update utility can connect to eDirectory using SSL if you use the `-use_ssl` parameter at startup. Otherwise, it connects to eDirectory in non-SSL mode.

- 3 Click *OK*.
- 4 Review the Pre-Installation Summary page. If everything is correct, click *Install* to proceed with the installation.
- 5 Click *Done* when the installation completes.
- 6 Open the Readme file in the install directory.
- 7 Go to [Section 5.4.11, “Post-Install Tasks,”](#) on page 108.

5.4.9 Choosing a Database Platform

- 1 Complete selections on the following page:



- 2 Select the database platform. Depending on your choice, follow the configuration steps in the table below:

Database	Description and Configuration Details
MySQL	<p>For a remote MySQL environment, create a database of the name you specified in the Section 5.4.3, “Specifying MySQL Details,” on page 96.</p> <hr/> <p>TIP: The installer creates the JBoss data source file for you with the name of the User Application WAR file.</p>
Oracle	<p>To use Oracle databases with the User Application:</p> <ol style="list-style-type: none">1. Create a database on your Oracle instance (make sure the name is the same as the one you specify in Section 5.4.10, “Specifying the Database Name and Privileged User,” on page 107.)2. Download the <code>ojdbc14.jar</code> driver from Oracle’s download site and copy to <code>/idm/jboss/server/<server-name>/lib</code> <hr/> <p>TIP: The installer creates the JBoss data source file for you with the name of the User Application WAR file.</p>

Database	Description and Configuration Details
MS SQL	<p>To use MS SQL databases with the User Application:</p> <ol style="list-style-type: none"> 1. Create a database on your MS SQL instance (make sure the name is the same as the one you specify in Section 5.4.10, “Specifying the Database Name and Privileged User,” on page 107). 2. Download MS SQL JDBC drivers (<code>msbase.jar</code>, <code>mssqlserver.jar</code> and <code>msutil.jar</code>) from the Microsoft download site and copy them to <code>/idm/jboss/server/<server-name>/lib</code> 3. Create your JBoss data source file pointing to this database. <p>TIP: The installer creates the JBoss data source file for you with the name of the User Application WAR file.</p>

- 3 Click *Next*, then continue with [Section 5.4.4, “Specifying the Database Host and Port,”](#) on page 97.

5.4.10 Specifying the Database Name and Privileged User

- 1 Complete selections on the following page:

Field	Description
Database name (or sid)	Specify the name of the database you want to store the User Application configuration information.

Field	Description
Database user	Specify the database root user.
Database password/Confirm password	Specify the database root password.

- 2 Click *Next*, then continue with [Section 5.4.5, “Specifying the JBoss Server Settings,”](#) on page 98.

5.4.11 Post-Install Tasks

The Forgot Password and Workflow e-mail notifications capabilities require that you do the following post-installation tasks:

- 1 In iManager, select the *Passwords* Role.
- 2 Under *Passwords*, select *Email Server Options*.
- 3 Provide your SMTP server name in the *Host Name* field.
- 4 In the *From* field, specify an e-mail address (for example, `noreply@novell.com`), then click *OK*.

5.4.12 Testing the Install

To verify that the installation went correctly, complete the remaining steps outlined in the [Section 5.2, “Installation and Configuration,”](#) on page 86. If the Identity Manager User Application page does not appear in your browser after completing these steps, check the terminal console for error messages relating to MySQL, JBoss, and the User Application, and see [Section 5.5, “Troubleshooting,”](#) on page 108.

5.5 Troubleshooting

If you encounter problems with the installation process, try these troubleshooting steps. If they do not work, contact Novell Support. Your Novell representative will work through any setup and configuration problems you might have.

ISSUE	SUGGESTED ACTIONS
<p>You want to modify the User Application configuration settings made during installation. This includes configuration of such things as:</p> <ul style="list-style-type: none"> ♦ Identity Vault connections and certificates ♦ E-mail settings ♦ Metadirectory User Identity, User Groups ♦ iChain settings 	<p>You can run the configuration utility independent of the installer.</p> <p>On Linux , run this command from the installation directory (by default, <code>/home/user/novell/idm</code>): <code>configupdate.sh</code></p> <p>On Windows, run this command from the installation directory (by default, <code>c:\novell\idm</code>): <code>configupdate.bat</code></p>
<p>Exceptions thrown when JBoss starts up, with the log message “port 8080 already in use.”</p>	<p>Shut down any instances of Tomcat (or other server software) that might already be running. If you decide to reconfigure JBoss to use a port other than 8080, remember to edit the config settings for the User Application Driver in iManager.</p>

ISSUE	SUGGESTED ACTIONS
You see a message that no trusted certificates were found when JBoss starts.	Make sure you start JBoss using the JRE installed with the User Application.
Can't log into portal admin page.	Make sure the User Application administrator account exists. Don't confuse this with your iManager admin account. They are two different admin objects.
Can log into as admin, but can't create new users.	The User Application Administrator must be a trustee of the top container and needs to have Supervisor rights. As a stopgap, you can try setting the User Application's Administrator's rights equivalent to the LDAP administrator's rights (using iManager).
When starting JBoss, there are MySQL connection errors.	<p>Don't run as root.</p> <p>Make sure MySQL is running (and that the correct copy is running). Kill any other instances of MySQL. Run <code>/idm/mysql/start-mysql.sh</code>, then <code>/idm/start-jboss.sh</code>.</p> <p>Examine <code>/idm/mysql/setup-mysql.sh</code> in a text editor and correct any values that appear suspicious. Then run the script, and run <code>/idm/start-jboss.sh</code>.</p>
You encounter keystore errors when starting the JBoss application server	<p>Your JBoss application server is not using the JRE installed by the User Application installation program which uses the default path: <code>/idm/jre/lib/security/cacerts</code></p> <p>Use the <i>keytool</i> command to import the certificate file:</p> <pre>keytool -import -trustcacerts -alias <i>aliasName</i> -file <i>certFile</i> -keystore ..\lib\security\cacerts -storepass <i>changeit</i></pre> <ul style="list-style-type: none"> ◆ Replace <i>aliasName</i> with a unique name of your choice for this certificate. ◆ Replace <i>certFile</i> with the full path and name of your certificate file. ◆ The default keystore password is <i>changeit</i> (if you have a different password, specify it).

Activating Novell Identity Manager Products

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, otherwise they will shut down. At any time during the 90 days, or afterward, you can choose to activate Identity Manager products.

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

- ♦ [Purchasing an Identity Manager Product License](#)
- ♦ [Activating Identity Manager Products Using a Generic Credential](#)
- ♦ [Installing a Product Activation Credential](#)
- ♦ [Viewing Product Activations for Identity Manager and Drivers](#)

6.1 Purchasing an Identity Manager Product License

To purchase an Identity Manager product license, see the [Novell Identity Manager How to Buy Web page \(http://www.novell.com/products/nsureidentitymanager/howtobuy.html\)](http://www.novell.com/products/nsureidentitymanager/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 generic credential. If you do not remember or do not receive your Customer ID, please 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.)

6.2 Activating Identity Manager Products Using a Generic Credential

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

IMPORTANT: Only three differing e-mail addresses can be used to access the link where you can obtain the generic credential. If you try to access the link with more than three e-mail addresses, it is considered as a security risk and you are denied access. Additionally, only the e-mail address designated as the owner/contract for the Customer ID receives the e-mail containing the Order Detail section with the information on obtaining the generic license. If your response e-mail does not contain the Order Detail section, you need to contact the Customer ID person within your organization to obtain the generic credential.

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



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

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



- 3 Proceed to [Section 6.3, “Installing a Product Activation Credential,”](#) on page 113 for instructions on how to activate Identity Manager and drivers.

6.3 Installing a Product Activation Credential

You should install the Product Activation Credential via iManager. The following procedures explain how to install the Product Activation Credential.

- 1 Open the Novell e-mail that contains the Product Activation Credential.
- 2 Do one of these steps:
 - ♦ 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.
- 3 Open iManager.
- 4 Choose *Identity Manager Utilities > Install Activation*.
- 5 Select the driver set or browse to a driver set, then click *Next*.
- 6 If the driver set is not associated with a server or is associated with multiple servers, select a server to associate with a driver set, then click *Next*.
The installation dialog box appears.
- 7 Do one of these steps:
 - ♦ 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*.
- 8 Click *Finish*.

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

6.4 Viewing Product Activations for Identity Manager and Drivers

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

- 1 Open iManager.
- 2 Click *Identity Manager > Identity Manager Overview*.
- 3 Enter the driver set or the driver you want to view activation information for in the object name field.
or
Browse to the driver set or the driver you want to view activation information on.
- 4 Locate the driver set you want to view activation information for and click the driver set name.
- 5 Select the *Activation* tab.
You can view the text of the activation credential or, if an error is reported, you can remove an activation credential.

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.
