AUTHORIZED DOCUMENTATION

Installation Guide

Novell® Identity Manager

3.5.1

December 23, 2009

www.novell.com

Legal Notices

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

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

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

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

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

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

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide

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 the installation, administration, and configuration functions of Identity Manager.

Audience

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

Documentation Updates

For the most recent version of this document, see the Identity Manager Documentation Web site (http://www.novell.com/documentation/idm35/index.html).

Additional Documentation

For documentation on other Identity Manager drivers, see the Identity Manager Drivers Web site (http://www.novell.com/documentation/idm35drivers/index.html).

Documentation Conventions

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

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

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

Overview

1

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 data store—your Identity Vault—to synchronize, transform, and distribute information across applications, databases, and directories.

But Identity Manager is much more than that. Some of the features of Identity Manager include:

- Password synchronization
- Password self-service
- Logging and auditing services
- User management through the User Application
- Workflow provisioning
- E-mail notification
- Designing drivers and policies through the Designer utility

To see what’s new about these components in this version of Identity Manager, see Section 1.3, “What’s New in Identity Manager 3.5.1?,” on page 14. For a better view of the different components and services that make up Identity Manager, see Section 1.4, “Identity Manager Installation Programs and Services,” on page 19.

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 the data that 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 data store can choose to share User objects with a Human Resources data store, 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 other personnel without sharing the users' more personal information (such as 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 data store 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.
- 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.

Policies are the key to synchronizing data. A policy:

- 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 data store 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 allows Identity Manager to share data with any application.

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	With a single operation: Identity Manager immediately grants or removes access to resources for an employee. Identity Manager provides automated employee provisioning capability, to give a new employee access to network, e-mail, applications, resources, and so forth. Through workflow provisioning, this process can be set up to initiate an approval process. Identity Manager can also restrict or disable access upon termination or leave.
Track and Integrate Asset Inventory	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.
Automate White/Yellow Page Directories	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.
Enhance User Profiles	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.
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 recognizing customer needs to view data in one place instead of having it isolated in separate applications or areas.
Customize Service	Identity Manager provides users (employees, customers, partners, etc.) with profiles complete with synchronized information, including relationships, status, and service records. 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.

Activity	Identity Manager Solution
Password Management	Through the User Application, administrators can set up challenge/response questions, as well as allow users to set their own passwords. The Client Login Extension for Novell Identity Manager 3.5.1 facilitates password self-service by adding a link to the Novell and Microsoft GINA login clients. The clients allow access to the Identity Manager User Application Password Self-Service feature. If the Identity Manager driver supports password synchronization, passwords can be synchronized across connected systems.

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 3.5.1?

1.3.1 Identity Manager

Support for Open Enterprise Server 2

Open Enterprise Server 2 contains many prerequisite software components, including SUSE® Linux Enterprise Server 10 Support Pack 1, NetWare® 6.5 Support Pack 8, eDirectory 8.8 Support Pack 5, iManager 2.7, and Security Services 2.0.5. Identity Manager is supported on both the Linux and NetWare Open Enterprise Server 2 platforms.

iManager Plug-ins

The plug-ins for iManager in this version of Identity Manager are also compatible to Identity Manager 3.0. In addition to backward compatibility, Identity Manager 3.5.1 contains plug-ins that can report information from the driver cache file.

Additional Operating System Platform Support

Identity Manager provides support for all operating system platforms that the previous version of Identity Manager supports. In addition, certain components of Identity Manager will run on Microsoft Windows Vista*, AIX* 5.3, Red Hat* 5 AS/ES 64-bit, and Open Enterprise Server 2, which includes SUSE Linux Enterprise Server 10 SP1 and NetWare 6.5 SP8.

Additional Application Support

Identity Manager provides support for all applications that the previous version of Identity Manager supports. In addition, Identity Manager also supports eDirectory 8.8 SP5 and iManager 2.7 on the platforms where those applications run.

Non-root Installation

Identity Manager 3.5.1 includes information and scripts to install the Identity Manager Metadirectory engine into a non-root installation of eDirectory. For the steps to perform a non-root installation of Identity Manager, see Section 4.9, “Non-root Installation of Identity Manager,” on page 95.

Bundled Components

Identity Manager includes the Client Login Extension for Novell Identity Manager 3.5.1 and Designer 2.1.

A new component for Identity Manager, the Client Login Extension for Novell Identity Manager 3.5.1, facilitates password self-service by adding a link to the Novell and Microsoft GINA login clients. When users click the *Forgot Password* link in their login client, the Client Login Extension launches a restricted browser to access the Identity Manager User Application Password Self-Service feature. This feature assists in reducing help desk calls from people who forget their passwords.

For more information on Client Login Extension for Novell Identity Manager 3.5.1, see “Client Login Extension for Novell Identity Manager 3.5.1” in the *Novell Identity Manager 3.5.1 Administration Guide*. For more information on Designer 2.1, see Section 1.3.2, “Designer for Identity Manager,” on page 16.

1.3.2 Designer for Identity Manager

This section describes enhancements to Designer for Identity Manager. For a more detailed listing of all Designer 2.1 enhancements and changes, see What's New (http://www.novell.com/documentation/designer21/index.html).

Locale support

The Provisioning view of the Designer for Identity Manager now allows you to define:

- The user application's default locale. (This is the locale used to display content when a match for the user's locale cannot be found.)
- The locales supported by the User Application driver.

In addition, Designer can now import and export localization data for e-mail templates.

Provisioning Team Editor

Designer for Identity Manager now includes a Provisioning Team editor plug-in. This new editor allows you to define a set of users who can act as a team for the *Requests & Approvals* tab of the User Application. The team definition determines who can manage provisioning requests and approval tasks associated with this team.

The Provisioning Team editor provides an alternative to the iManager plug-in for team management.

Provisioning View usability enhancements

The Provisioning view has been enhanced so that you now have the ability to:

- Organize provisioning request definitions in categories. You can use the directory abstraction layer editor to define the categories.
- Assign multiple properties (such as trustee assignments) for more than one provisioning request definition at a time.

E-Mail Activity

The E-Mail activity provides a way to send an e-mail to interested parties outside of an Approval activity.

Approval Activity

The Approval activity now provides a way to create a new form from the Approval activity property page.

The Approval activity also provides the ability to set a Reply To address field in e-mail notifications that is different from the From address.

Log Activity

The Log activity now allows custom messages to be added to the Comment History of a workflow.

Form Enhancements

Forms now support the onload event.

ECMA Enhancements

The following field methods are now supported:

- getName()
- validate()
- hide()
- show()
- focus()
- select()
- activate()
- setRequired()

Enhancements for Provisioning Request Definition Display Names

The provisioning request definition's display name can now be defined as a static string or a localizable ECMA expression. By defining an expression, you can customize the approval task display name. This allows different instances of the same workflow to display unique entries in the task list in the User Application.

1.3.3 User Application

User Interface Enhancements

The display of Team Tasks has been enhanced to provide more flexibility in the interface and to optimize the user experience. The Team Tasks page displays dynamic content in two new presentation views, The Template view and the Exhibit view. Both formats use a table to display data to the user. In either format, the user can choose which columns to display, specify the order in which columns appear, and sort tasks by the values in a column.

The choice of display format is controlled by the administrator. Administrators can choose one view over the other because of presentation preferences or to take advantage of the following differentiating features:

- The Template view (the default) provides accessibility support for nonvisual users. In addition, it includes a customizable paging feature.
- The Exhibit view supports filtering and provides a data export facility.

Cross-Platform Changes

This release adds runtime support for the following application server platforms:

- JBoss* 4.2.0 on SUSE Linux Enterprise Server 10.1, SUSE Linux Enterprise Server 9 SP2, and Windows 2003 Server SP1
- WebSphere* 6.1 on Solaris* 10 and Windows 2003 SP1

  The Install program for the User Application installs the WAR for you. However, you need to deploy the WAR to WebSphere manually.

  The database support for WebSphere includes Oracle* 10g, MS SQL* 2005 SP1, and DB2.

  For a complete list of supported platforms, see "System Requirements for Identity Manager" on page 28.

This release also adds support for the following browser environments:

- Internet Explorer 7 on Windows 2000 Professional SP4, Windows XP SP2, and Windows Vista Enterprise Version 6
- Firefox* 2 on Red Hat Enterprise Linux WS 4.0, Novell Linux Desktop 9, SUSE Linux 10.1, and SUSE Linux Enterprise Desktop 10

Interoperability Changes

The following interoperability changes have been made in this release:

- The administrator can now use a configuration setting to specify whether the User Application should display the Hint on the Forgot Password screen.
- The administrator can now use a configuration setting to enable or disable the password autocomplete feature in the Login dialog. This controls whether the browser lets the user save their credentials.
- The login process now supports proxy smart card authentication through Access Manager. To make this possible, the User Application accepts SAML assertions injected into the HTTP header, and uses these assertions to make a SASL connection to the directory.

SOAP Endpoint Enhancements

The following enhancements have been made to the SOAP endpoints in this release:

- A new VDX service has been added to provide a SOAP endpoint for performing queries against the directory abstraction layer.
- A new Notification service has been added to provide a SOAP endpoint for sending e-mail notifications.
- A new method called getProcessesArray() has been added to the Provisioning service that includes an argument to allow you to limit the number of processes returned.
- A new method called startWithCorrelationId() has also been added to the Provisioning service to allow you to start a set of related workflows and track them using a correlation ID

The SOAP endpoints provide a way for developers to build their own applications. They are not exposed in the out-of-the-box user interface for the User Application.

Other Feature Enhancements

The User Application now lets you specify URL parameters to go directly to a provisioning request form.

1.4 Identity Manager Installation Programs and Services

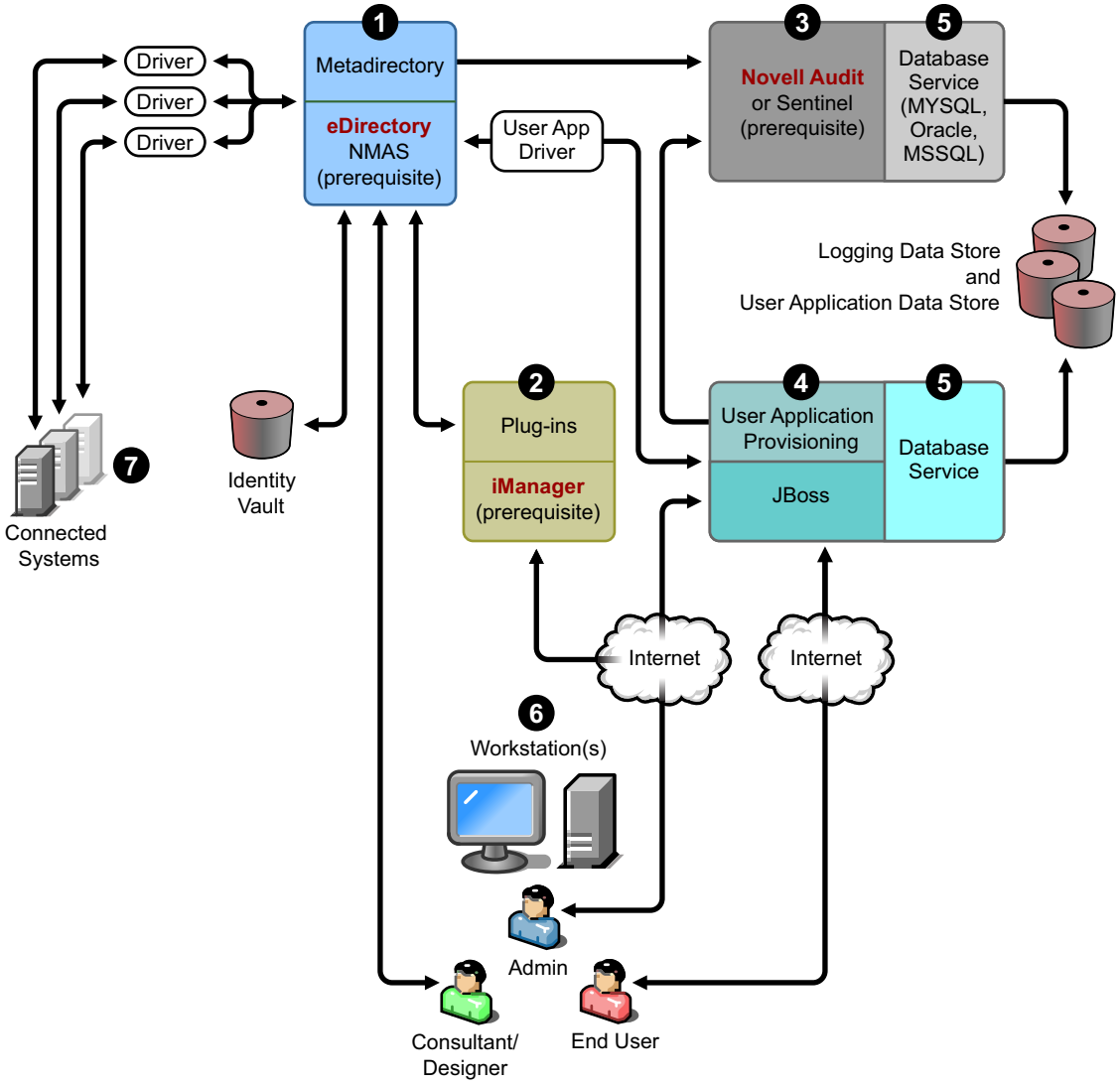
The following sections explain Identity Manager's Installation Programs and Services. This section points out the different services that make up a fully functioning Identity Manager.

- Section 1.4.1, "Installation Programs," on page 19
- Section 1.4.2, "Services," on page 21

1.4.1 Installation Programs

Identity Manager has three distinct installation programs with seven services to install and configure. The graphic below gives you an overview of all of the services necessary to make Identity Manager fully functional.

Figure 1-1 *Graphic Overview of the Seven Identity Manager Services*



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

- "Identity Manager Metadirectory System Installation" on page 21
- "User Application and Provisioning Module Installation" on page 21
- "Designer Installation" on page 21

NOTE: Before installing Identity Manager components, you need to first install prerequisite software including eDirectory 8.7.3.6 or later (for the services shown in numbers 1 and 3 in the graph above), Security Services 2.0.4 with NMAS™ 3.1.3 (for numbers 1 and 3), iManager 2.6 or later (for number 2), and Novell Audit 2.0.2 Starter Pack or Novell® Sentinel™ 5.1.3 (for number 3). You can get the prerequisite software from the Novell Download Web site (http://download.novell.com). For a detailed list of prerequisites and requirements, see Section 1.5, "System Requirements for Identity Manager," on page 28.

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 the Metadirectory system utilities and tools.

User Application and Provisioning Module Installation

The following services are installed on Linux* and Windows:

- JBoss and MySQL* (if selected).
- The WAR file required to run the User Application.

Designer Installation

There is an installer for Linux and one for Windows. They do the following tasks:

- Install the Eclipse* framework.
- Install the foundational plug-ins.
- Install the Metadirectory plug-ins.
- Install the directory abstraction layer plug-ins.
- Install the workflow editor plug-in.

1.4.2 Services

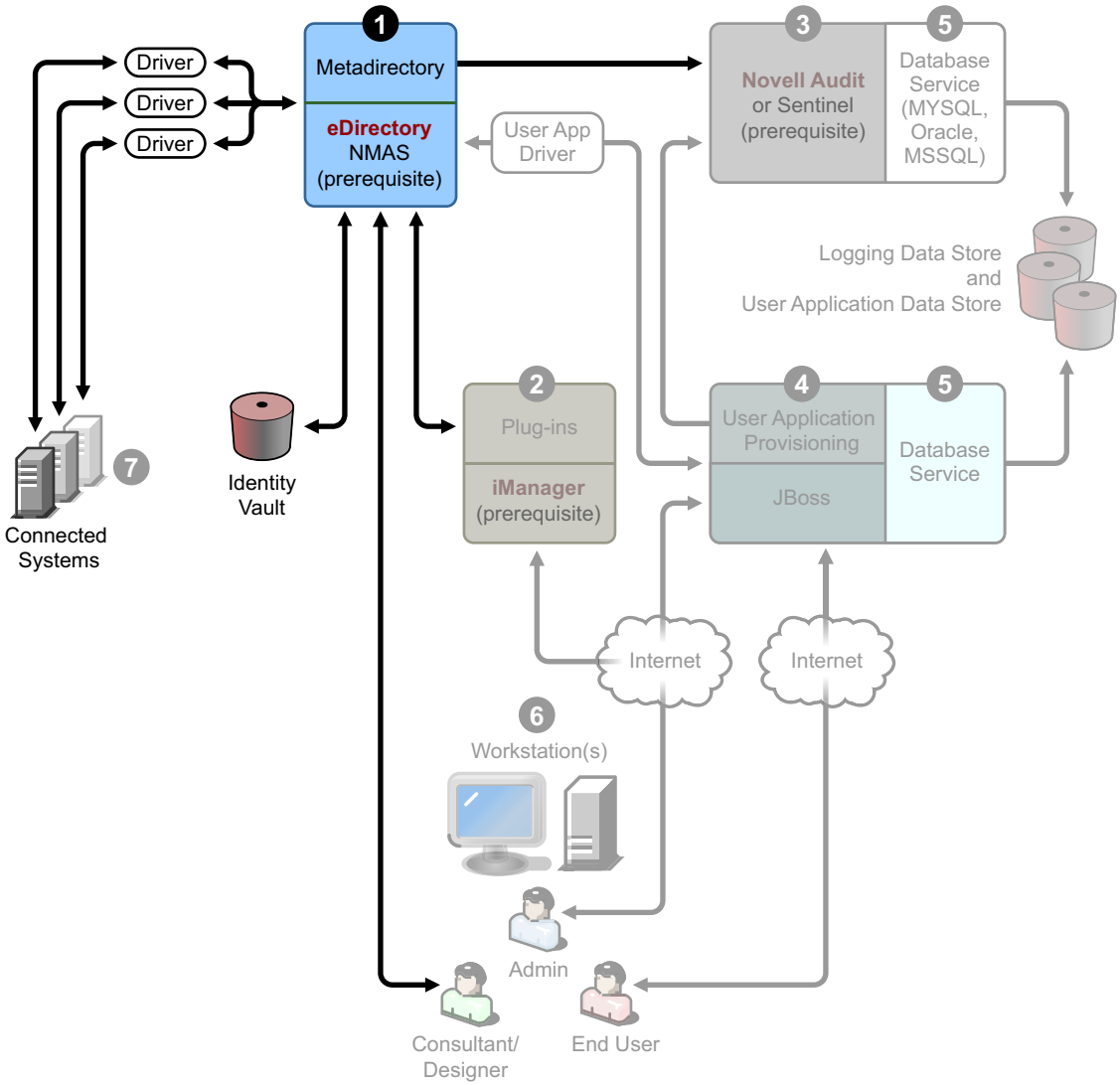
Identity Manager comes with seven services that you can install and configure. Although it's not recommended for a production environment, you can install and configure all seven services on a single computer. Or you can deploy one service per computer, or anything in between. The supported hardware and software prerequisites for each service are covered in Section 1.5, "System Requirements for Identity Manager," on page 28.

- "Metadirectory System Service" on page 22
- "Web-based Administration Services" on page 23
- "Secure Logging Services" on page 24
- "User Application and Provisioning Module" on page 25
- "Database Service" on page 25
- "Workstations" on page 27
- "Connected Systems" on page 27

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.

Figure 1-2 *Metadirectory System Service*



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).

To install Identity Manager and this service, see Chapter 4, "Installing Identity Manager," on page 69. To see any prerequisites before installing Identity Manager, see the system requirements for "Metadirectory System" on page 30.

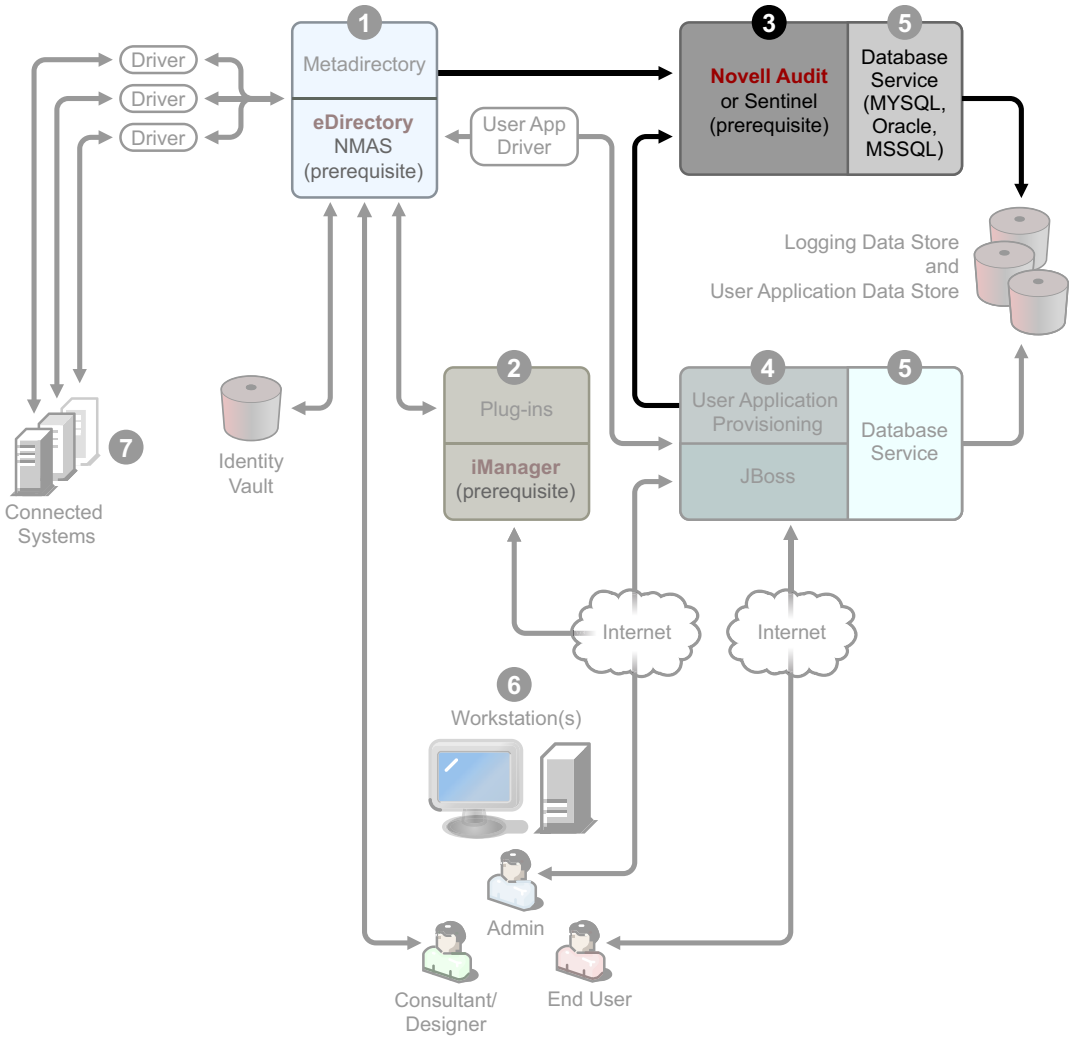
Web-based Administration Services

Figure 1-3 *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 69.

Secure Logging Services

Figure 1-4 *Secure Logging Service*

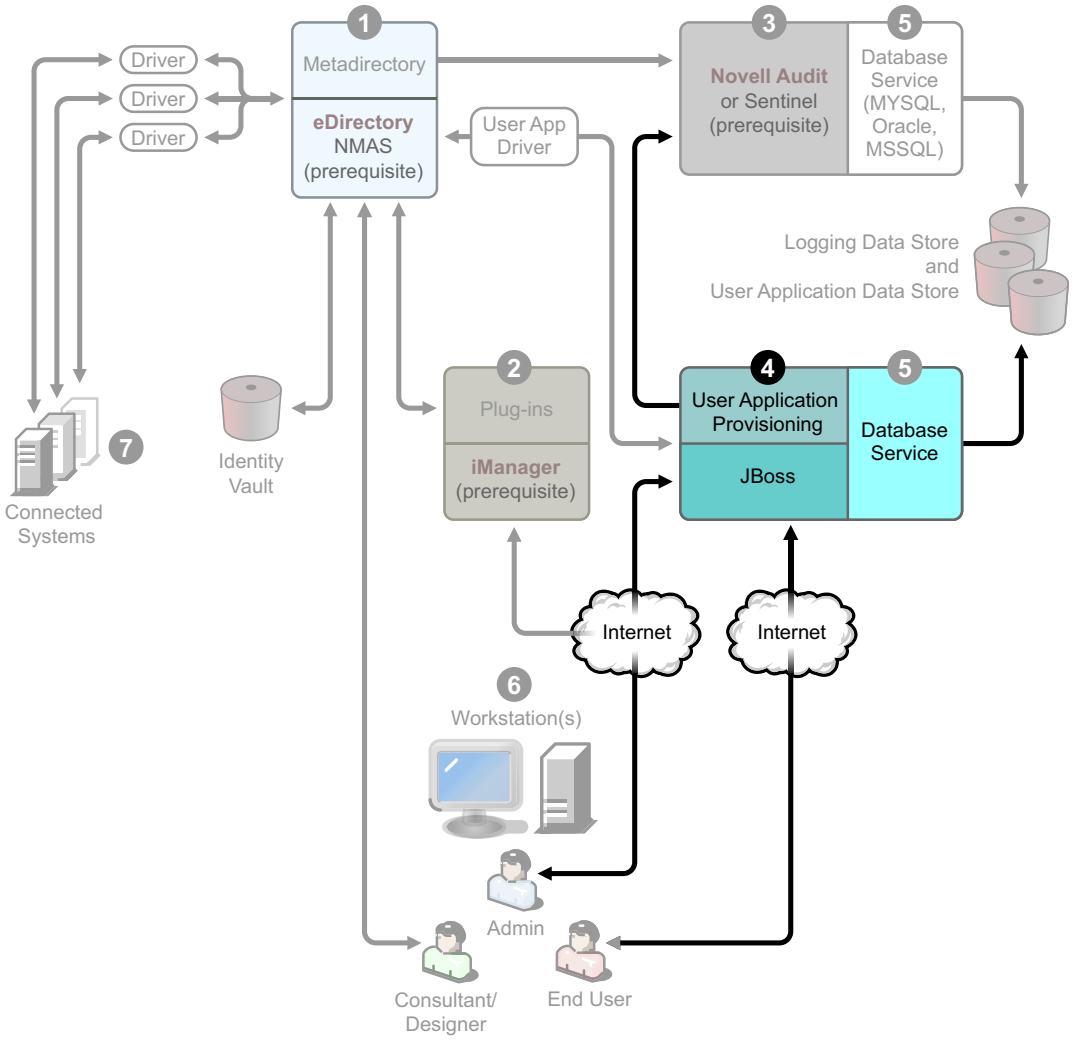


Repository for logging events (Identity Manager software is not installed on this server, but having a secure logging service is mandatory). This is a central service that is used by Identity Manager and the user application and workflow system services and is downloaded separately from the Novell Download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

From the *Product or Technology* pull-down menu on the Download Web site, select *Audit* and click *Search*. Click the *Audit 2.0.2 Starter Pack*. Follow the installation instructions included with the Starter Pack.

User Application and Provisioning Module

Figure 1-5 *User Application and Provisioning Module*

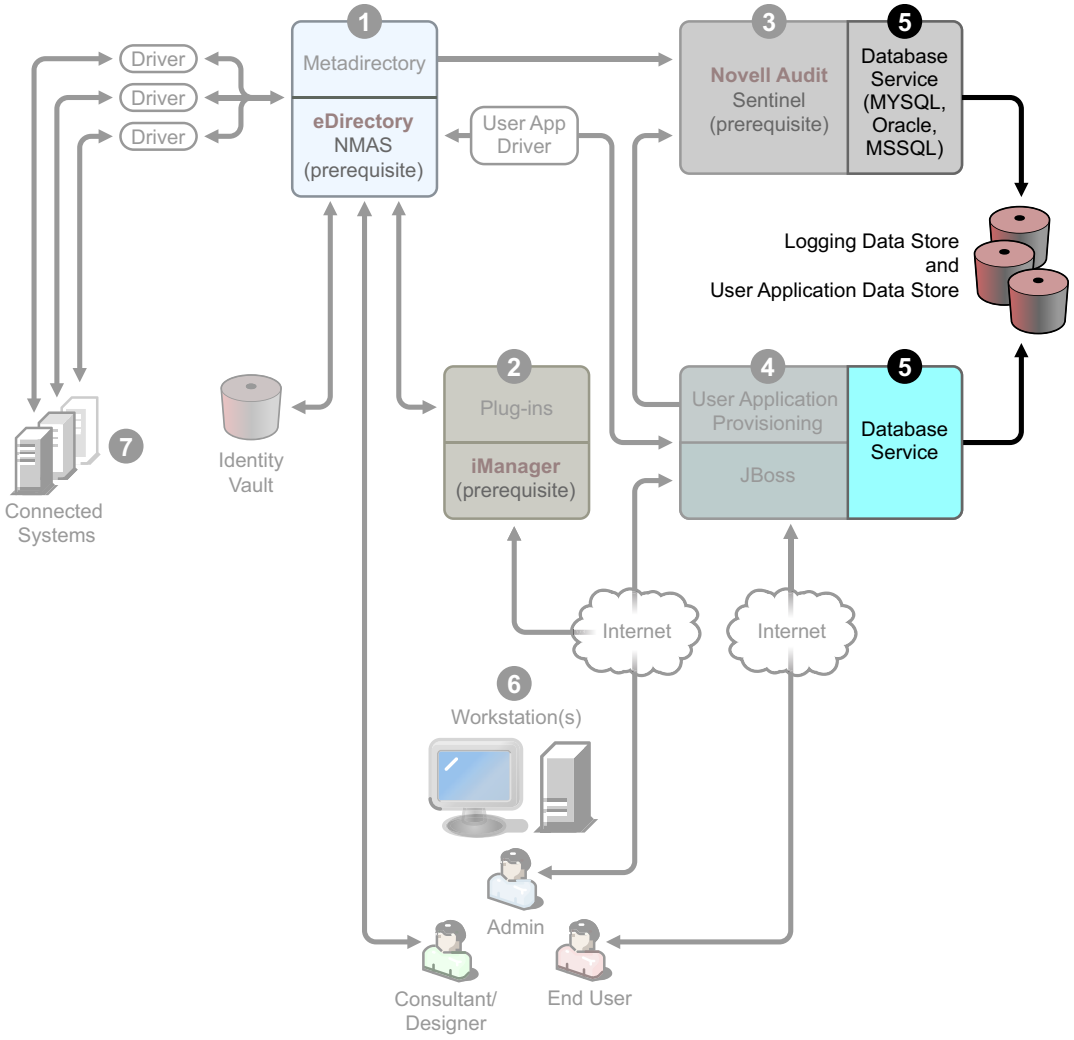


To install this service, see Chapter 5, “Installing the User Application,” on page 99. The supported hardware and software prerequisites for each service are covered in Section 5.2, “Prerequisites to Installation,” on page 99.

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.

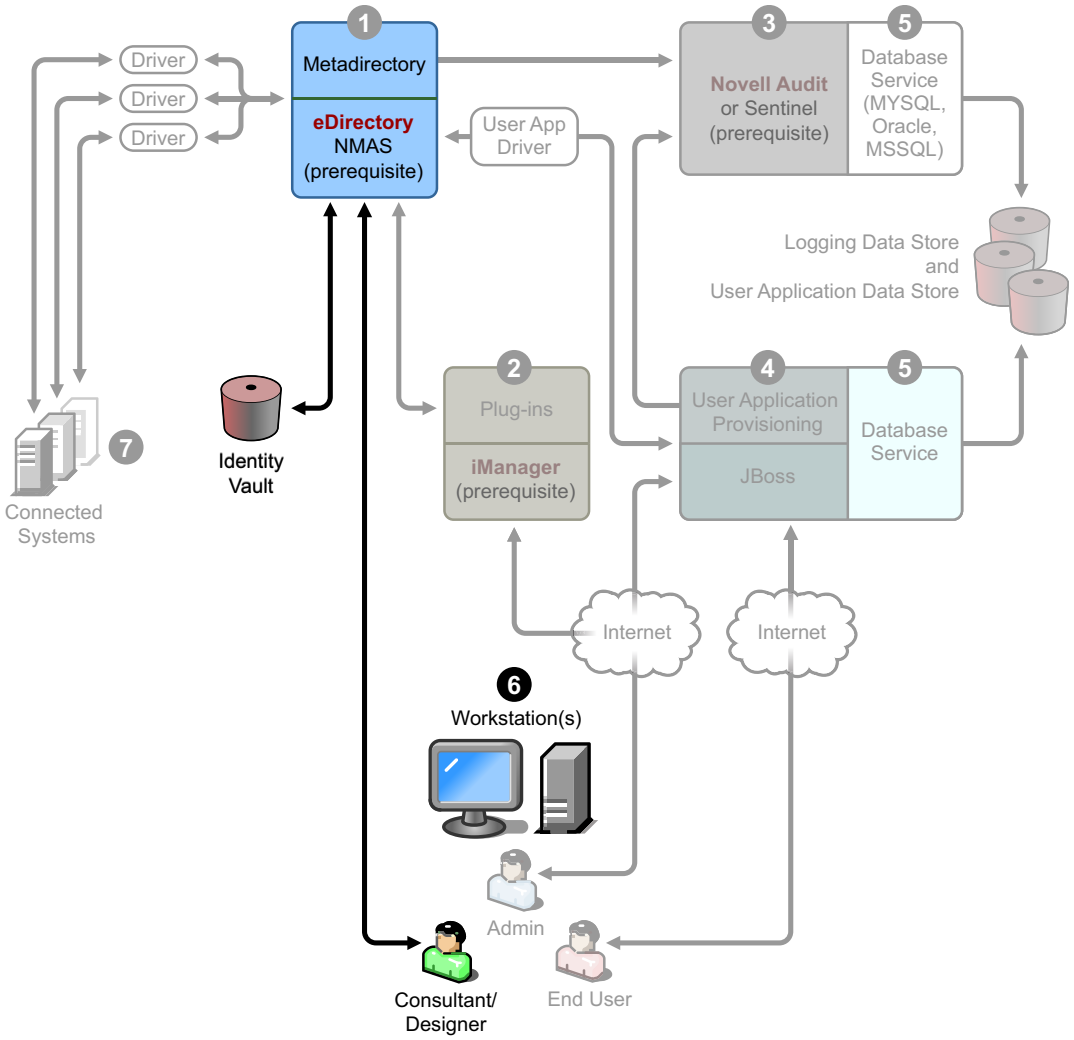
Figure 1-6 *Database Service*



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 4.2.0, and the User Application requires JRE* 1.5.0_10. To install this service, see Section 5.3, “Installation and Configuration Steps,” on page 107.

Workstations

Figure 1-7 *Workstation Services for Designer*

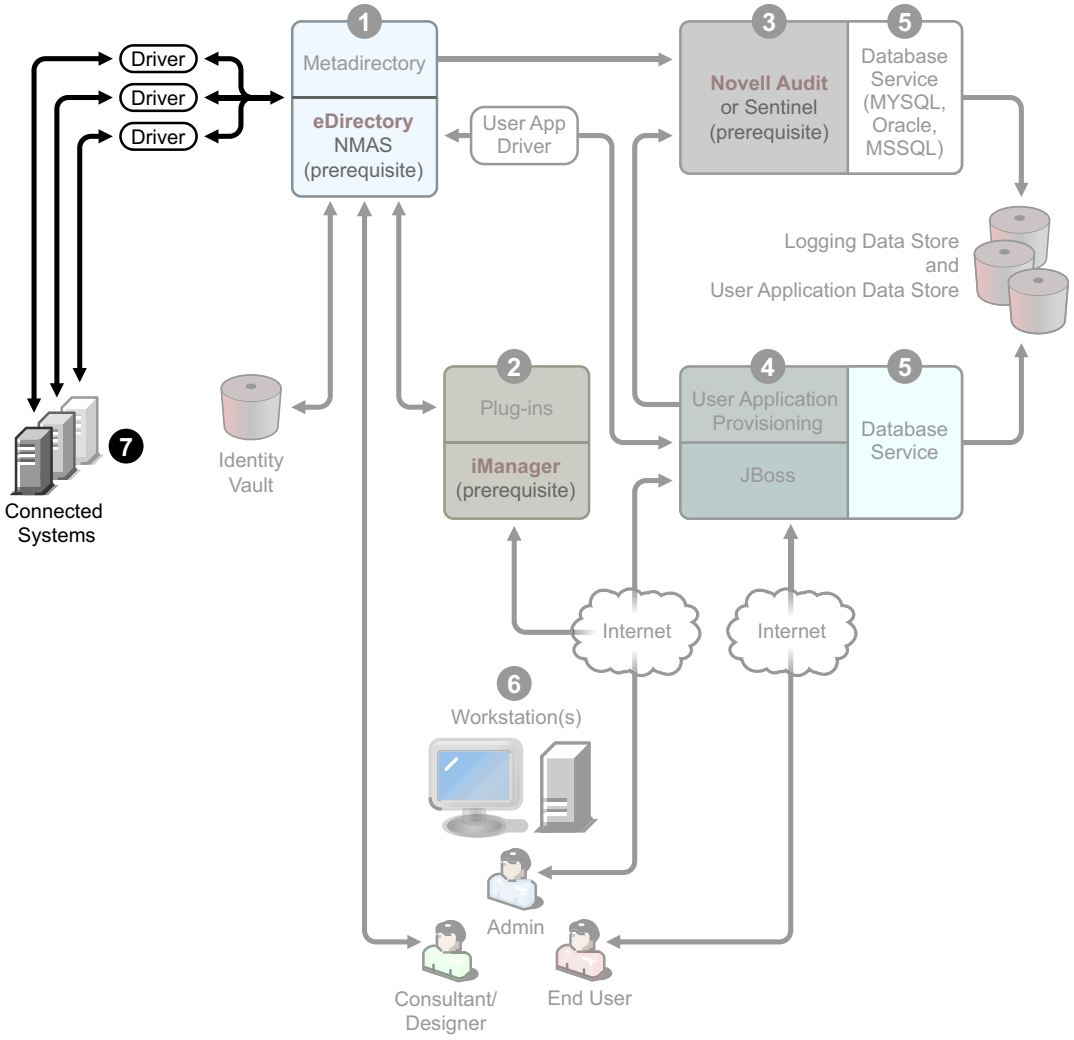


Used for Designer to design, deploy, and document the Identity Manager system and for utilities, reports, and tools included with the product. To install Designer on a workstation, see "Installing Designer" in the *Designer 2.1 for Identity Manager 3.5.1*.

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.

Figure 1-8 *Connected Systems*



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 69. To learn more about configuring drivers, read the driver-specific documentation on the Identity Manager Drivers Documentation Web site (http://www.novell.com/documentation/idm35drivers).

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 ◆ Metadirectory engine ◆ Novell Audit agent ◆ Service drivers ◆ Identity Manager Drivers ◆ Utilities (including Application Tools, and the Novell Audit Setup tool)	One of the following operating systems: ◆ NetWare 6.5 with the latest Support Pack ◆ Novell Open Enterprise Server (OES) 1.0 with the latest Support Pack ◆ Novell Open Enterprise Server (OES) 2.0 ◆ Novell Open Enterprise Server (OES) 2.0 SP1 (32-bit) ◆ Windows 2000 Server with the latest Service Pack (32-bit) ◆ Windows Server 2003 (32-bit) with Service Pack 1 (for eDirectory version < 8.8.3) or Service Pack 2 (for eDirectory 8.8.3 or later) ◆ Linux Red Hat 3.0, 4.0 and 5.0 ES and AS (both 32-bit and 64-bit are supported) ◆ SUSE Linux Enterprise Server 9 and 10 with the latest Support Pack (both 32-bit and 64-bit are supported) ◆ Solaris 9, or 10 ◆ AIX 5.2L, versions 5.2 and 5.3 One of the following versions of eDirectory: ◆ eDirectory 8.7.3 with at least Support Pack 9 (8.7.3.9) ◆ eDirectory 8.8 with at least Support Pack 1 (8.8.1) Security Services 2.0.5 (NMAS 3.2.0)	Using VMware* in your implementation is supported if you use a Metadirectory system platform. All Identity Manager software components in this release are 32-bit, even if they are running on a 64-bit processor or a 64-bit operating system. Unless specified otherwise, OES, NetWare, Windows, and Linux platforms (Red Hat and SUSE) support all of the following processors in 32-bit mode: ◆ Intel* x86-32 ◆ AMD x86-32 ◆ Intel EM64T ◆ AMD Athlon64* and Opteron* Identity Manager supports these features of eDirectory 8.8: ◆ Multiple instances of eDirectory on the same server ◆ Encrypted attributes eDirectory 8.8 supports 64-bit Red Hat Linux 4.0. A 64-bit version of Password Synchronization on Windows Server 2003 is available. Be sure to completely back up the eDirectory database before installing eDirectory 8.8. eDirectory 8.8 upgrades portions of the database structure and won't allow it to be rolled back after the upgrade process. Xen virtualization is now supported on SUSE Linux Enterprise Server 10/ Open Enterprise Server 2/Open Enterprise Server 2 SP1 when the Xen Virtual Machine (VM) is running SLES 10/OES 2/OES 2 SP1 as the guest operating system in paravirtualized mode. A 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%200%2020414606).

System Component	System Requirements	Notes
Web-based Administration Server ◆ Password synchronization plug-in ◆ iManager 2.6 and plug-ins ◆ iManager 2.7 and plug-ins ◆ Driver configurations	One of the following operating systems: ◆ Novell Open Enterprise Server (OES) 1.0 on NetWare with the latest Support Pack ◆ Novell Open Enterprise Server (OES) 2.0 ◆ NetWare 6.5 with the latest Support Pack ◆ Windows 2000 Server with the latest Service Pack (32-bit) ◆ Windows Server 2003 with the latest Service Pack (32-bit) ◆ Microsoft Windows Vista ◆ Linux Red Hat Linux 3.0, 4.0, and 5.0 ES and AS (both 32-bit and 64-bit are supported) ◆ Solaris 9 or 10 with latest support pack ◆ SUSE Linux Enterprise Server 9 and 10 with the latest Support Pack (both 32-bit and 64-bit are supported) Operating systems supported via iManager Workstation: ◆ Windows 2000 Professional with latest Service Pack ◆ Windows XP with SP2 ◆ SUSE Linux Enterprise Desktop 10 ◆ SUSE Linux 10.1 The following software. ◆ Novell iManager 2.6 and 2.7 with the latest support pack and plug-ins	All Identity Manager software components in this release are 32-bit, even if they are running on a 64-bit processor or a 64-bit operating system. Unless stated otherwise, OES, NetWare, Windows, and Linux platforms (Red Hat and SUSE) support all of the following processors in 32-bit mode: ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 and Opteron ◆ Browser support is determined by iManager 2.6. This list presently includes: ◆ Internet Explorer 6, SP1 and above ◆ Internet Explorer 7 ◆ Firefox* 2.0 and above ◆ You must go through the iManager Configuration Wizard or the Designer utility to install or deploy portal content into eDirectory. ◆ (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.

System Component	System Requirements	Notes
Secure Logging Service ◆ The Secure Logging Server ◆ The Platform Agent (client component) ◆ Novell Audit 2.0.2 or Novell Sentinel 5.1.3	For the Secure Logging Server, one of the following operating systems: ◆ Novell Open Enterprise Server (OES) 1.0 and 2.0 latest Support Pack ◆ NetWare 6.5 with the latest Support Pack ◆ Windows 2000 Server with the latest Service Pack (32-bit) ◆ WIndow 2003 Server with the latest Service Pack (32-bit) ◆ Red Hat Linux 3.0, 4.0, and 5.0 AS and ES (32-bit and 64-bit, although Novell Audit only runs in 32-bit mode) ◆ Solaris 9 or 10 with latest support pack ◆ SUSE Linux Enterprise Server 9 or 10 (32-bit and 64-bit, although Novell Audit only runs in 32-bit mode) ◆ Novell eDirectory 8.7.3.6 or 8.8 with latest support pack (must be installed on the Secure Logging Server) For the Platform Agent, one of the following operating systems: ◆ Novell Open Enterprise Server (OES) 1.0 SP1 or the latest Support Pack ◆ NetWare 6.5 with the latest Support Pack ◆ Windows 2000 or 2000 Server, XP, or Windows Server 2003 with the latest Service Pack (32-bit) ◆ Red Hat Linux 3 or 4 AS and ES (32-bit and 64-bit, although Novell Audit only runs in 32-bit mode) ◆ Solaris 8, 9, or 10 ◆ SUSE Linux Enterprise Server 9 or 10 (32-bit and 64-bit, although Novell Audit only runs in 32-bit mode) iManager 2.6 and 2.7 with the latest Support Pack and plug-ins	OES, NetWare, Windows, and Linux platforms (Red Hat and SUSE) support all of the following processors in 32-bit mode: ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 and Opteron Minimum Secure Server requirements include: ◆ A single processor, server-class PC with a Pentium* II 400 MHz ◆ A minimum of 40 MB disk space ◆ 512 MB RAM The eDirectory Instrumentation, which allows eDirectory events to be logged, supports the following versions of eDirectory: ◆ eDirectory 8.7.3 (NetWare, Windows, Linux, and Solaris) ◆ eDirectory 8.8 with latest support pack The NetWare Instrumentation, which allows NetWare events to be logged, supports the following versions of NetWare: ◆ 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	**Application server** The User Application runs on JBoss and WebSphere, as described below. JBoss 4.2.0 is supported on: ◆ Novell Open Enterprise Server (OES) 1.0 SP2 or the latest Support Pack -- Linux only ◆ SUSE Linux Enterprise Server 9 SP2 (included in OES 1.0 SP2) and 10.1.x (64-bit JVM*) ◆ Windows 2000 Server with SP4 (32-bit) ◆ Windows 2003 Server with SP1 (32-bit) ◆ Solaris 10 Support Pack dated 6/06 WebSphere 6.1 is supported on: ◆ Solaris 10 (64-bit mode) ◆ Windows 2003 SP1 The User Application requires JRE* 1.5.0_10 (See Section 5.2, “Prerequisites to Installation,” on page 99) **Browser** The User Application supports both Firefox and Internet Explorer, as described below. Firefox 2 is supported on: ◆ Windows 2000 Professional with SP4 ◆ Windows XP with SP2 ◆ Red Hat Enterprise Linux WS 4.0 ◆ Novell Linux Desktop 9 ◆ SUSE Linux 10.1 ◆ SUSE Linux Enterprise Desktop 10 Internet Explorer 7 is supported on: ◆ Windows 2000 Professional with SP4 ◆ Windows XP with SP2 ◆ Windows Vista Enterprise Version 6 Internet Explorer 6 is supported on: ◆ Windows 2000 Professional with SP4 ◆ Windows XP with SP2	SUSE Linux Enterprise Server supports the following processors in 32-bit mode: ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 and Opteron SUSE Linux Enterprise Server will run in 64-bit mode on the following processors: ◆ Intel EM64T ◆ AMD Athlon64 ◆ AMD Opteron ◆ Sun* SPARC* Xen* virtualization is now supported on SUSE Linux Enterprise Server 10/ Open Enterprise Server 2/Open Enterprise Server 2 SP1 when the Xen Virtual Machine (VM) is running SLES 10/OES 2/OES 2 SP1 as the guest operating system in paravirtualized mode. A 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%200%2020414606)).

System Component	System Requirements	Notes
Database Server for the User Application ◆ MySQL ◆ Oracle ◆ MS SQL ◆ DB2	The following databases are supported with JBoss: ◆ MySQL Version 5.0.27 ◆ Oracle 9i (9.2.0.1.0 and 9.2.0.5.0) ◆ Oracle 10g Release 2 (10.2.0.) ◆ MS SQL 2005 SP1 The following databases are supported with WebSphere: ◆ Oracle 10g Release 2 (10.2.0.) ◆ MS SQL 2005 SP1 ◆ DB2 DV2 v9.1.0.0	The User Application uses a database for various tasks, such as storing configuration data and storing data for any in-progress workflow activities. 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. Oracle is supported with both the thin client driver and the OCI client driver.
Workstations ◆ Designer ◆ iManager Web access	Designer has been tested on the following platforms: Windows: ◆ Windows 2000 Professional with the latest Service Pack ◆ Windows XP SP2 ◆ Windows Server 2003 with the latest Service Pack (32-bit) ◆ Microsoft Windows Vista Linux: ◆ SUSE Linux Enterprise Server 10 (for Designer only) ◆ SUSE Linux 10.1 ◆ SUSE Linux Enterprise Desktop 10 ◆ Red Hat Linux 4.0 (for Designer only) ◆ Red Hat Fedora* Core 5 (for Designer only) ◆ Novell Linux Desktop 9 ◆ GNOME*, KDE, Red Hat Fedora	Designer uses Eclipse as its development platform. Refer to the Eclipse Web site (http://www.eclipse.org/) for platform-specific information. Designer minimum and recommended hardware requirements: ◆ 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. Prerequisite software: ◆ Microsoft Internet Explorer 6.0 SP1 ◆ Microsoft Internet Explorer 7 ◆ or Mozilla* Firefox 2.0

System Component	System Requirements	Notes
Connected System Server (host on a separate server running Remote Loader) ◆ Remote Loader ◆ Remote Loader configuration tool (Windows only) ◆ Novell Audit agent ◆ Password Synchronization agent ◆ Driver shim for the connected system ◆ Tools for the connected system	Each driver requires that the connected system be available and the relevant APIs are provided. Refer to the Identity Manager Driver documentation (http://www.novell.com/documentation/idm35drivers) for operating system and connected system requirements that are specific to each system.	Each connected application requires individuals with application-specific knowledge and responsibility. The Remote Loader is 32-bit. It can be used on the following systems in 32-bit mode: ◆ Windows NT* 4.0, Windows 2000 Server, or Windows Server 2003 with latest Support Packs ◆ Windows Server 2003 (64-bit) with the latest Service Pack ◆ Red Hat Linux 3.0, 4.0, and 5.0 ES and AS ◆ SUSE Linux Enterprise Server 9, or 10 ◆ Solaris 9, or 10 ◆ AIX 5.2L, versions 5.2 and 5.3 The Java Remote Loader can be used on the following systems: ◆ HP-UX* 11i ◆ OS/400 ◆ zOS* ◆ You should be able to use it on any system that has JVM 1.4.2 or higher Both 32-bit and 64-bit versions of the Password Synchronization agent are included. The 64-bit version is supported on Windows Server 2003 (64-bit) only.

1.5.1 Supported Platforms for Identity Manager 3.5.1 with eDirectory 8.8 Support Pack 5 (8.8.5)

- Windows Server 2003 with the latest Service Pack (32-bit)
- Linux Red Hat AS 4.0 and AP 5.0 (both 32-bit and 64-bit are supported)
- SUSE Linux Enterprise Server 9 and 10 with the latest Support Pack (both 32-bit and 64-bit are supported)
- Solaris 9 and 10
- Novell Open Enterprise Server (OES) with the latest Support Pack
- NetWare 6.5 with the latest Support Pack
- AIX 5.3

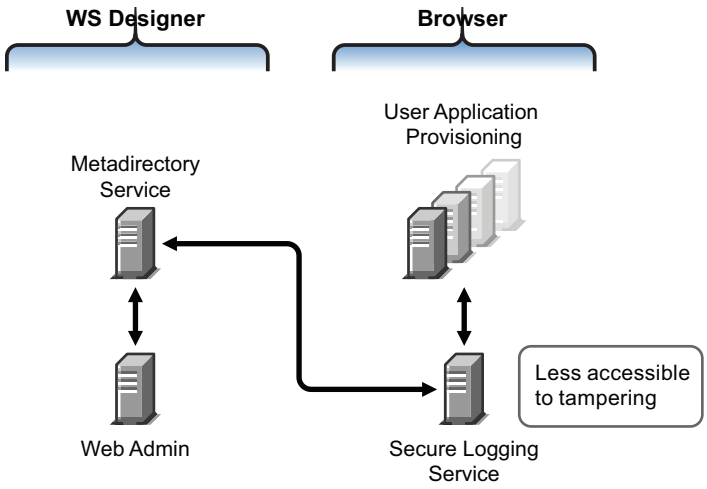
1.6 Recommended Deployment Strategies

As previously indicated, Identity Manager comes with a number of services that you must install and configure. Although it's not recommended for a production environment, you can install and configure all needed 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.

Figure 1-3 illustrates one possible deployment strategy, with 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 Provisioning services.

Figure 1-9 *Identity Manager Deployment Strategies*



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 2.6 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 Provisioning services, you must also run the User Application installation and install only the User Application plug-ins for iManager. You will need to do this for either the User Application or the User Application with Provisioning Module (they are two separate products).

User Application and Secure Logging Services

If you are doing 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 5.0.27-max 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 Provisioning Module 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 User Application/Provisioning services 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 set up Oracle 9i or 10g on a separate (remote) server, you 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 by using SSL technology. Keep this in mind when connecting systems to Identity Manager.

For more information on planning your Identity Manager system, see Chapter 2, "Planning," on page 41.

1.7 Where To Get Identity Manager and Its Services

To download Identity Manager and its services:

1. Go to the Novell Downloads Web site (http://download.novell.com).
2. In the *Product* or *Technology* menu, select *Novell Identity Manager*, then click *Search*.
3. On the Novell Identity Manager Downloads page, click the Download button next to a file you want.
4. Follow the on-screen prompts to download the file to a directory on your computer.
5. 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
Identity Manager DVD The following Identity Manager components are available on one ISO image for DVD burning. These components are also available for individual download. ◆ Identity Manager and Drivers ◆ Designer for Identity Manager	Identity Manager: Linux, NetWare, Windows, and UNIX* Designer: Linux and Windows	Identity_Manager_3_5_1_DVD.iso
Identity Manager and Drivers	NetWare, and Windows	Identity_Manager_3_5_1_NW_Win.iso
Identity Manager and Drivers	Linux	Identity_Manager_3_5_1_Linux.iso
Identity Manager and Drivers	UNIX	Identity_Manager_3_5_1_Unix.iso
User Application This is the standard version of the user application that is included with your Identity Manager 3 purchase.	Linux and Windows	Identity_Manager_3_5_1_User_Application.iso
User Application with the Provisioning Module for Identity Manager This is the Provisioning version of the user application, which is an add-on to Identity Manager and requires a separate purchase.	Linux and Windows	Identity_Manager_3_5_1_User_Application_Provisioning.iso
Designer for Identity Manager	Windows	Identity_Manager_3_5_1_Designer_Win.iso
Designer for Identity Manager	Linux	Identity_Manager_3_5_1_Designer_Linux.iso

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 3.5.1

- To install Identity Manager 3.5.1 on Windows, NetWare, UNIX, and Linux, see Chapter 4, "Installing Identity Manager," on page 69
- To install the User Application or the User Application with Provisioning Module, see Chapter 5, "Installing the User Application," on page 99
- To install Designer, see "Installing Designer" in the *Designer 2.1 for Identity Manager 3.5.1* 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 3.5.1 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 3.5.1
- 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 185.

Planning

2

2.1 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 56.)

This planning material provides an overview of the type of activities that are normally 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/). Novell Education also offers courses that address Identity Manager implementation.

We also strongly recommend setting up a test/development environment where you can test, analyze, and develop your solutions. After things are working the way you want, deploy the final product into your production environment.

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.

2.1.1 Novell Identity Manager Deployment

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

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 for 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 43
- "Analyze Your Business Processes" on page 44
- "Design an Enterprise Data Model" on page 44

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 2/25/2007 to 25 Feb 2007.
- 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 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 reside (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 might 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, and 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

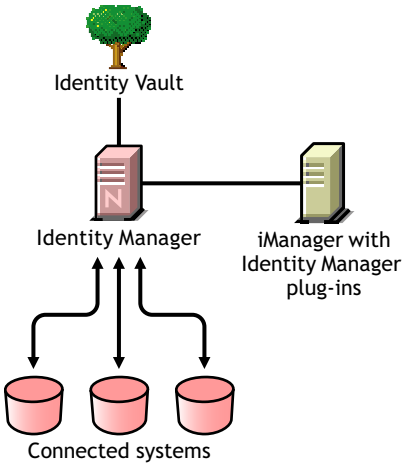
2.2 Planning for Common Installation Scenarios

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 2.2.1, “New Installation of Identity Manager,” on page 48
- Section 2.2.2, “Using Identity Manager and DirXML 1.1a in the Same Environment,” on page 50
- Section 2.2.3, “Upgrading from the Starter Pack to Identity Manager,” on page 52
- Section 2.2.4, “Upgrading from Password Synchronization 1.0 to Identity Manager Password Synchronization,” on page 54

2.2.1 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 48
- “iManager Server with Identity Manager plug-ins” on page 49
- “Connected Systems” on page 49
- “Common Identity Manager Tasks” on page 49

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/idm35drivers/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 1.4, "Identity Manager Installation Programs and Services," on page 19 for more information.
- **Set Up Connected Systems:** Refer to Section 1.4, "Identity Manager Installation Programs and Services," on page 19 and the driver implementation guides (http://www.novell.com/documentation/idm35drivers/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 Chapter 6, "Activating Novell Identity Manager Products," on page 185.
- **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 *Policies in iManager for Identity Manager 3.5.1*.
- **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" (http://www.novell.com/documentation/password_management31/index.html?page=/documentation/password_management31/pwm_administration/data/ampxjj0.html).
- **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 3.5.1 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 "Using Status Logs" in the *Identity Manager 3.5.1 Logging and Reporting*.

- **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, 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-to-end provisioning solution that's secure, scalable, and easy to manage. Refer to the User Application documentation (http://www.novell.com/documentation/idm35).

2.2.2 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 50
- "Management Tools" on page 50
- "Backward Compatibility" on page 51
- "Password Management" on page 51

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.
- Designer is a tool that allows you to design, test, update, and document the 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 185 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/idm35drivers/index.html) for upgrade information.

  A notable exception is that Password Synchronization 1.0 does not run correctly for Windows AD and Windows 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/idm35drivers/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.

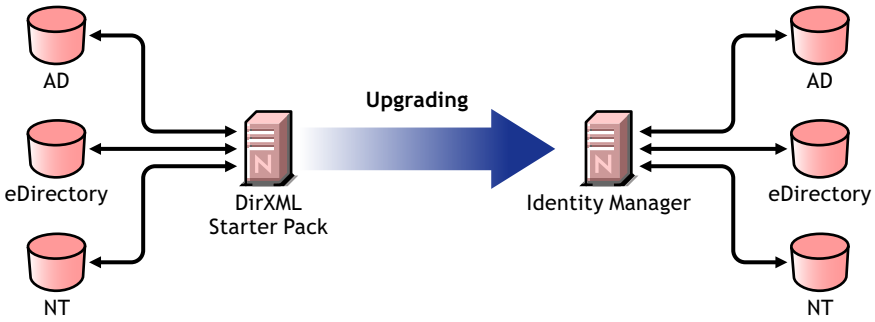
Password Management

- 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 "Managing Password Synchronization" section in the Password Management 3.1 Guide (http://www.novell.com/documentation/password_management31/index.html).
- 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) Deploying Universal Password" in the Password Management 3.1 Guide (http://www.novell.com/documentation/password_management31/index.html). The procedure is not necessary if you began using Universal Password with NetWare 6.5 SP8.

- 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 Windows AD or Windows NT, make sure you review the upgrade instructions before you install the new driver shims. See Section 2.2.4, "Upgrading from Password Synchronization 1.0 to Identity Manager Password Synchronization," on page 54.
- 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 3.5.1 Administration Guide*.

2.2.3 Upgrading from the Starter Pack to Identity Manager

Figure 2-3 *Upgrading from the 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 Nterprise™ 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:

- "Backward Compatibility" on page 53
- "Password Management" on page 53
- "Activation" on page 53

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/idm35drivers/index.html) for upgrade information.

  A notable exception is Password Synchronization 1.0, which does not run correctly for Windows AD and Windows 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/idm35drivers/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/idm35drivers/index.html) for the Identity Manager Drivers for Active Directory and NT Domain.
- Refer to Section 2.2.4, "Upgrading from Password Synchronization 1.0 to Identity Manager Password Synchronization," on page 54 for specific instructions surrounding this upgrade process.

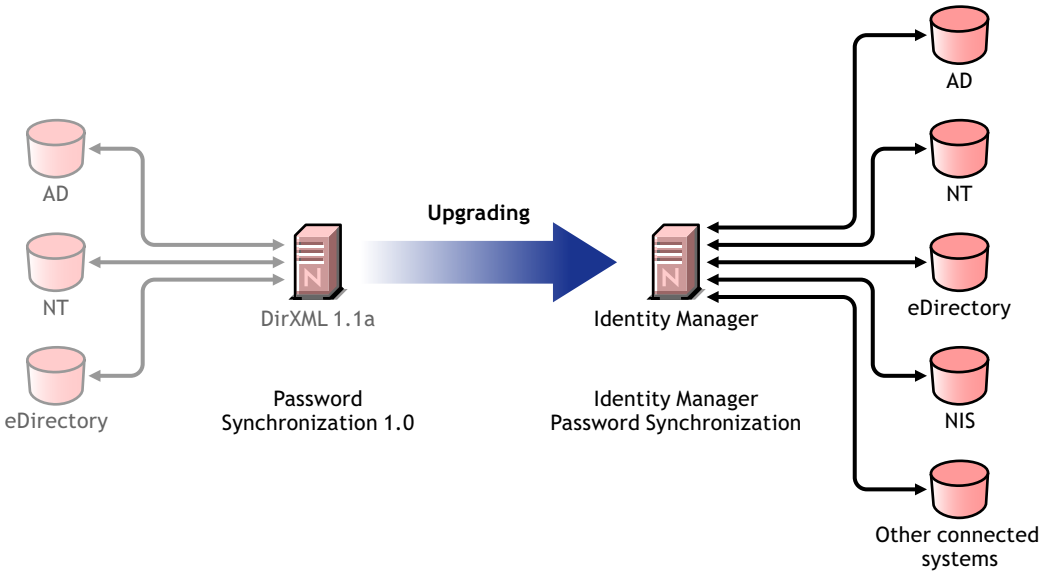
Activation

- 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 185.

2.2.4 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 3.5.1 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 can use the new features.

In this section:

- "Upgrading Password Synchronization for Active Directory or Windows NT" on page 54
- "Upgrading Password Synchronization for eDirectory" on page 55
- "Upgrading Other Connected System Drivers" on page 55
- "Handling Sensitive Information" on page 55

Upgrading Password Synchronization for Active Directory or Windows 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 3.5.1 driver shim to replace the DirXML 1.1a driver shim for Active Directory or Windows 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. Use driver policies to add support for the new Identity Manager Password Synchronization.
5. Install and configure new Password Synchronization filters.
6. Set up SSL, if necessary.
7. Turn on Universal Password by 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 3.5.1 Administration Guide*.
9. Remove Password Synchronization 1.0.

For detailed instructions, see the driver implementation guides (http://www.novell.com/documentation/idm35drivers/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 3.5.1 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 3.5.1 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 3.5.1 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.

Along with passwords, you can also use Novell SecretStore® and Novell SecureLogin to synchronize credentials. These allow you to provision the SecureLogin passphrase question and answer in environments where non-repudiation is desired. See "Security: Best Practices" in the *Novell Identity Manager 3.5.1 Administration Guide*.

2.3 Planning the Technical Aspects of Identity Manager Implementation

2.3.1 Using Designer

Identity Manager comes with a utility 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 2.1 for Identity Manager 3.5.1* 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 your plan should make sure that certain eDirectory objects are replicated on servers where you want to run these Identity Manager drivers.

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

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

An eDirectory server that is running an Identity Manager driver (or that the driver refers to, if you are using 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 is also important for Remote Loader authentication.

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

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

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

    To prevent separate instances of a driver from trying to synchronize the same users, you need to use scope filtering to define which users each instance of the driver should synchronize. Scope filtering means that you add rules to each driver to limit the scope of the driver's management to specific containers. See "Using Scope Filtering to Manage Users on Different Servers" on page 58.
  - **Use multiple instances of the driver on multiple servers, without scope filtering.** If you want to have multiple instances of a driver running on different servers without using filtered replicas, you need to define policies on the different driver instances that enable the driver to process different sets of objects within the same Identity Vault.
- The Template objects you want the driver to use when creating users, if you choose to use templates.

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

  For example, if you have created a container named Inactive Users to hold user accounts that have been disabled, you must have a master or read/write replica (preferably a master replica) of that container on the server where the driver is running.
- Any other objects that the driver needs to refer to (for example, work order objects for the Avaya* PBX driver).

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

2.3.3 Using Scope Filtering to Manage Users on Different Servers

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

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

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

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

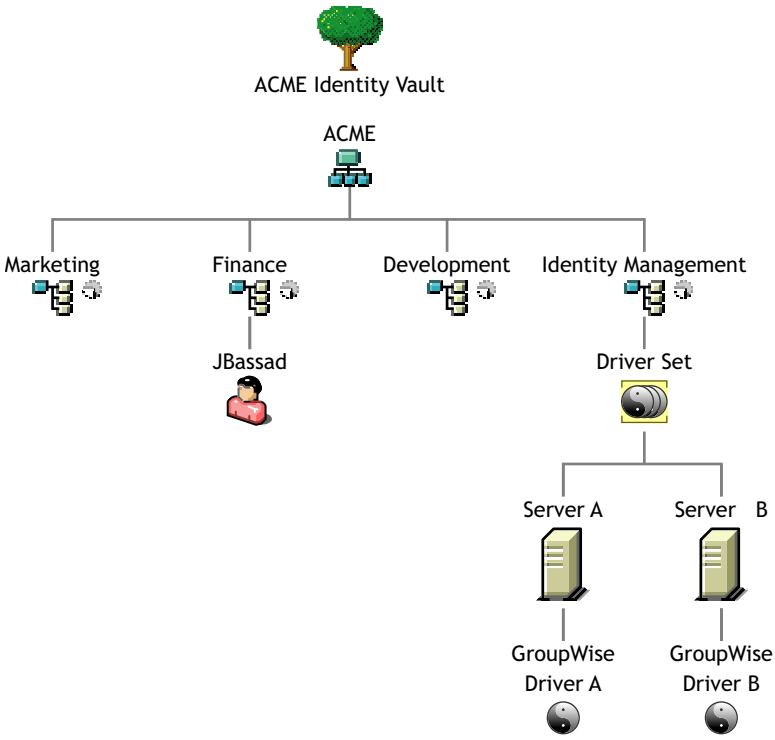
  To synchronize all users without having them replicated on one single server, you need to determine which set of servers holds all the users, and then create an instance of the Identity Manager driver on each of those servers. To prevent two instances of the driver from trying to synchronize the same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

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

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

The following illustration shows an Identity Vault with three containers that hold users: Marketing, Finance, and Development. It also shows an Identity 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 Figure 2-6 on page 60. 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.

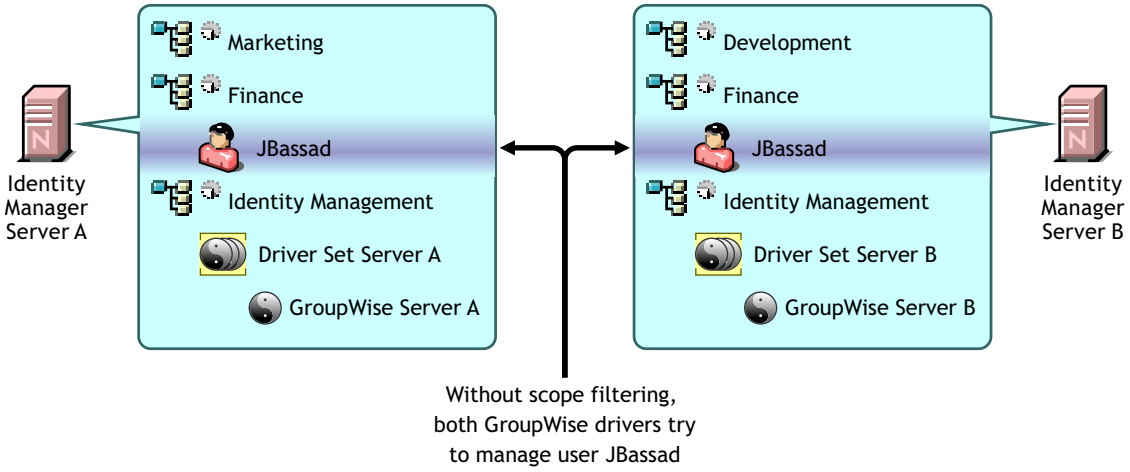
The administrator wants all the users in the tree to be synchronized by the GroupWise driver, but does not want to aggregate replicas of the users onto a single server. He chooses instead to use two instances of the GroupWise driver, one on each server. He installs Identity Manager and sets up the GroupWise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

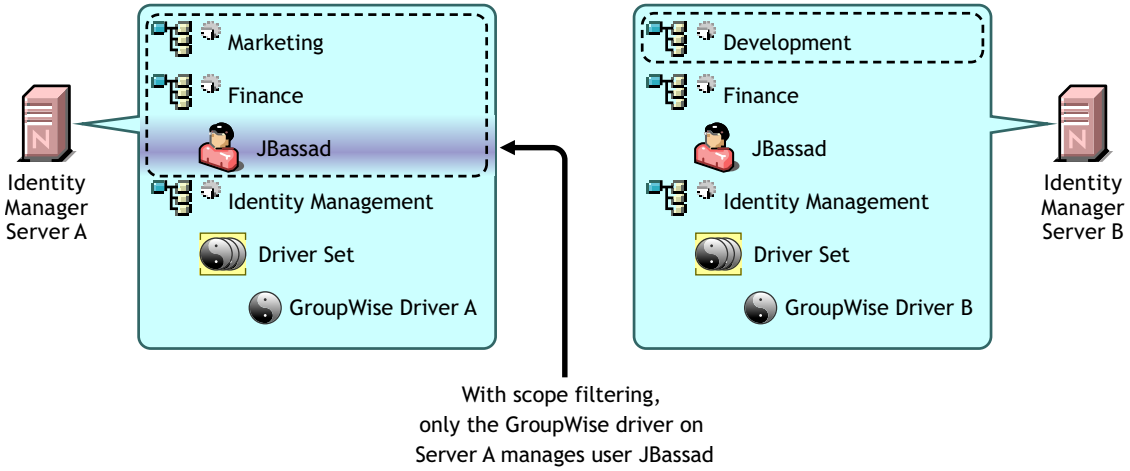
Because Server A and Server B both hold a replica of the Finance container, both servers hold the user JBassad, who is in the Finance container. Without scope filtering, both GroupWise Driver A and GroupWise Driver B would synchronize JBassad.

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 3.5.1 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 *Understanding Policies for Identity Manager 3.5.1*.

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

3

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

Some upgrade scenarios are explained in Section 2.2, “Planning for Common Installation Scenarios,” on page 48.

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 3.5.1	Yes
Identity Manager 2.x	Identity Manager 3.5.1	Yes
Identity Manager 3.0x	Identity Manager 3.5.1	Yes

3.2 Changes in Policy Architecture

Identity Manager 3.5 and 3.5.1 contain a new policy architecture, which affects how drivers reference policies. While the 3.5.1 driver architecture offers increased functionality in the Identity Manager 3.5.1 environment, the 3.0.x Metadirectory engine cannot run 3.5.1 driver configurations.

However, Identity Manager 3.5 and 3.5.1 can run 3.0x driver configurations. If you have 3.0.x driver configurations associated with both 3.0.x and 3.5.1 Metadirectory engines, do not upgrade the 3.0.x drivers. The 3.0.x driver configurations work in a 3.5.1 environment, but they don’t have the increased functionality that Identity Manager 3.5 and above affords. When 3.0.x driver configurations are only associated with a 3.5 or later Metadirectory engine, you should then upgrade the 3.0.x drivers to 3.5.1.

For more information on policy architecture and upgrading drivers to 3.5.1, see "Upgrading Identity Manager Policies" in *Understanding Policies for Identity Manager 3.5.1*.

3.3 Upgrade Procedure

For an upgrade to Identity Manager 3.5.1 to be successful, the following steps need to be completed.

3.3.1 Exporting Drivers

Before an upgrade occurs, backing up the current drivers and their configuration information is the most important step. To back up the drivers, you need to export them.

Exporting from ConsoleOne

1. In ConsoleOne®, right-click 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.

Exporting from Designer

1 From Designer, right-click the Driver or Driver Set object in the Modeler view and click *Export to Configuration File*.

2 In the Export Driver Configuration window, browse to and specify a file location and name for the export, then click *Save*.

3.3.2 Verifying Minimum Requirements

In order to upgrade to Identity Manager 3.5.1, the servers running the Identity Manager services need to meet the minimum requirements. See Table 1-3 on page 29 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 8.7.3.6 with the latest Support Pack, or upgrade to eDirectory 8.8 with the latest Support Pack.
3. You must have Security Services 2.0.5 with NMAS™ 3.2.0 for SSL support.
4. Upgrade iManager to iManager 2.6 or 2.7 with the latest Support Pack (includes upgrading to Apache 2.0.52 or later and Tomcat 4.1.18 or later).
5. For Identity Manager User Application and Provisioning, see Section 5.2, “Prerequisites to Installation,” on page 99.
6. Upgrade Identity Manager.
7. Activate the Metadirectory engine and any upgraded driver.

3.3.3 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 before upgrading. See Section 3.3.1, “Exporting Drivers,” on page 62.

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 *Edit properties*.
- **3d** On the Driver Configuration page, under *Startup Options*, select *Manual*.

4 Install Identity Manager 3.5.1.

The steps to upgrade to Identity Manager 3.5.1 are the same as the ones for installing Identity Manager 3.5. See Chapter 4, "Installing Identity Manager," on page 69 for the instructions on how to install Identity Manager.

Identity Manager 3.5.1 copies over previous versions of Identity Manager, updating the binaries. Both iManager and Designer update the drivers to the new functionality.

4a In iManager, click the drivers to begin the Driver Upgrade Wizard.

Designer automatically begins the Driver Upgrade Wizard when it detects older drivers.

5 Set the driver 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 *Edit properties*.

5d On the Driver Configuration page, under *Startup Options*, select *Auto start* or select your preferred method of starting 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 the upper right corner of the driver icon, then select *Start driver*.

3.3.4 Upgrading the Remote Loader

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

1 Create a backup of the Remote Loader configuration files. The default location of the files is as follows:

- Windows `C:\Novell\RemoteLoader\`*`remoteloadername`*`-config.txt`
- Linux: Create your own configuration file in the path of rdxml.

2 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 the Remote Loader" in the *Novell Identity Manager 3.5.1 Administration Guide*.

3.3.5 Upgrading in a UNIX/Linux Environment

Upgrading from Identity Manager 3.0.1 to Identity Manager 3.5.1 in either a UNIX or Linux environment creates two uninstall locations and doesn't completely remove packages. For example, if you start with a UNIX platform, such as SLES 9, and install Identity Manager 3.0.1, the Identity Manager uninstaller is in the `/root/dirXML` directory. Typing `rpm -qa | grep -i dxml` shows when the dxml packages were installed.

If you now upgrade this deployment to Identity Manager 3.5.1, it creates a new uninstall location at the `/root/idm` directory because of the naming change. Typing `rpm -qa` shows when the updated packages were installed.

Because of the directory change, if the administrator uninstalls Identity Manager 3.5.1, the uninstaller won't remove all of the packages, even though it states that all items were successfully removed. To remove the rest of the packages, use the DirXML uninstaller.

3.3.6 Migrating the User Application

If you are migrating to the latest version of the Identity Manager User Application, please refer to the *Identity Manager User Application: Migration Guide* (http://www.novell.com/documentation/idm35/pdfdoc/migration/migration.pdf) for directions.

3.4 Upgrading Password Synchronization

If you are upgrading from DirXML 1.1a to Identity Manager 3.5.1, Password Synchronization needs to be upgraded. See "Upgrading Password Synchronization 1.0" in the *Novell Identity Manager 3.5.1 Administration Guide*.

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

3.5 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 "Querying and Reporting" in *Identity Manager 3.5.1 Logging and Reporting*.

3.6 Upgrading DirXML 1.1a Driver Configurations

When you upgrade from DirXML 1.1a to Identity Manager 3.5.1, the driver configuration might be upgraded. Upgrading driver configurations has two aspects:

- Converting the DirXML 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.

  You need to thoroughly test to ensure that this step works. We also strongly recommend setting up a test/development environment where you can test, analyze, and develop your solutions. After things are working the way you want, deploy the final product into your production environment.
- Upgrading the driver policies to add new functionality. For instance, Identity Manager now uses DirXML script for the functionality that used to be in the style sheets. This level of functionality is best handled by an Identity Manager expert.

See "Upgrading a Driver Configuration from DirXML 1.1a to Identity Manager 3.5.1 Format" and "Managing DirXML 1.1a Drivers in an Identity Manager Environment" in the *Novell Identity Manager 3.5.1 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.

3.7 Activating Identity Manager

After the upgrade has completed, you have 90 days to active the Metadirectory engine and any drivers you have upgraded. If the engine and drivers are not activated, they stop working after 90 days. For instructions on how to activate Identity Manager, see Chapter 6, "Activating Novell Identity Manager Products," on page 185.

3.8 Upgrading from Open Enterprise Server 1 to Open Enterprise Server 2

When you upgrade from Open Enterprise Server (OES) 1 to OES 2 with Identity Manager 3.5.1 (IDM) installed on your OES server, you encounter package conflicts that must be resolved. A pop-up message appears immediately before the Installation Settings screen. The message informs you that the *Delete Unmaintained Packages* option is selected under *Update Options*. OES 2 considers IDM an "unmaintained package." This means that, by default, your IDM software will be deleted as part of the upgrade process. To prevent IDM from being deleted, follow the instructions below:

1. Read the pop-up warning carefully, then click *OK* to close it.

   NOTE: The pop-up describes three possible actions you can take to resolve the IDM status as an unmaintained package. This procedure steps you through the second of the three possible actions. This alternative works most efficiently for preserving your IDM installation.

2. On the Packages page, select *Search* in the *Filter* field.
3. Search for the IDM packages that are installed on the server by typing

   ```
   novell-DXML
   ```

   in the *Search* field. Click *Search.*

   Depending on what IDM packages are installed on the server, the search results include some or all of the following packages:

   ```
   novell-DXMLadeng
   novell-DXMLavpbx
   nobell-DXMLbase
   novell-DXMLcmpsr
   novell-DXMLdelim
   novell-DXMLdev
   novell-DXML-edir
   novell-DXML-engn
   novell-DXMLevent
   novell-DXMLgw
   novell-DXMLjdbc
   novell-DXML-jdbcu
   novell-DXMLjms
   novell-DXMLjms
   novell-DXMLldap
   novell-DXMLmtask
   novell-DXMLnotes
   novell-DXMLnxdrv
   novell-DXMLnxpam
   ```

```
novell-DXMLnxset
novell-DXMLpsoft
novell-DXMLracf
novell-DXMLsaphr
novell-DXMLsapum
novell-DXMLsch
novell-DXMLsoap
novell-DXMLssop
novell-DXMLsvUAD
novell-DXMLtlmnt
novell-DXMLtss
novell-DXMLwkodr
novell-NOVLjvml
```

4. Right-click on the first IDM package in the list, and select *All in this List > Keep.*

   This changes the status of each IDM package from *Delete* to *Keep*.

5. Select *Search* in the *Filter* field again and type

   ```
   novell-NOVLjvml
   ```

   NOTE: This package does not appear in the first search.

6. Right-click on this package and select *Keep*.
7. Click *Accept* on the Packages page.
8. If you are presented with a font License Agreement, click *Accept*.
9. Click *Continue* to return to the Installation Settings page.
10. Verify that the package conflict message is now gone from under the *Packages* link, then continue with the upgrade process.

Installing Identity Manager

4

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

4.1 Before You Install

Before you install Identity Manager, refer to Chapter 2, “Planning,” on page 41.

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 29 lists the installation components of Identity Manager and requirements for each system.

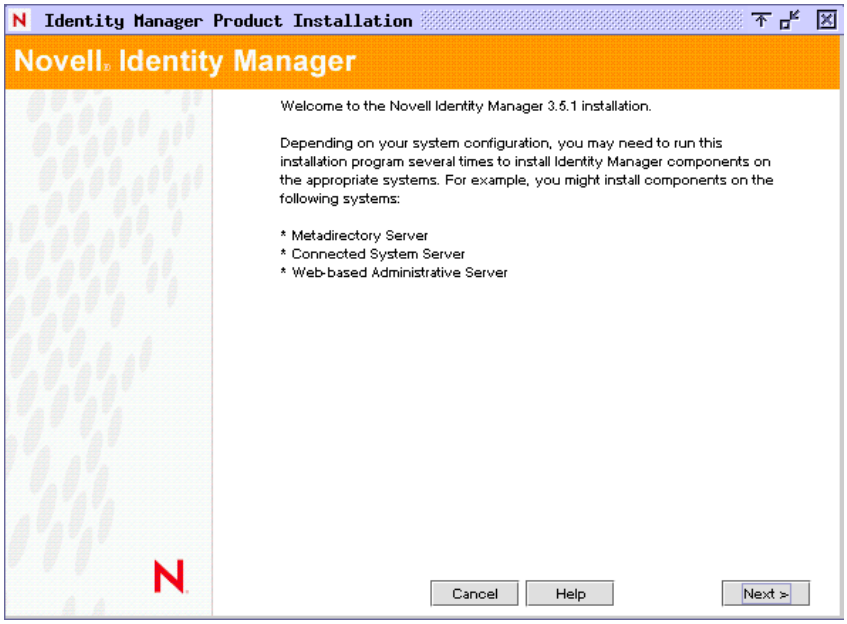
4.3 Installing Identity Manager on NetWare

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 69.

1 Download the Identity Manager `.iso` image file you need. You can download the Identity Manager `.iso` image files from the Novell Download site (http://download.novell.com).

The NetWare install of Identity Manager is located on the `Identity_Manager_3_5_1_NW_Win.iso` or on the `Identity_Manager_3_5_1_DVD.iso`.

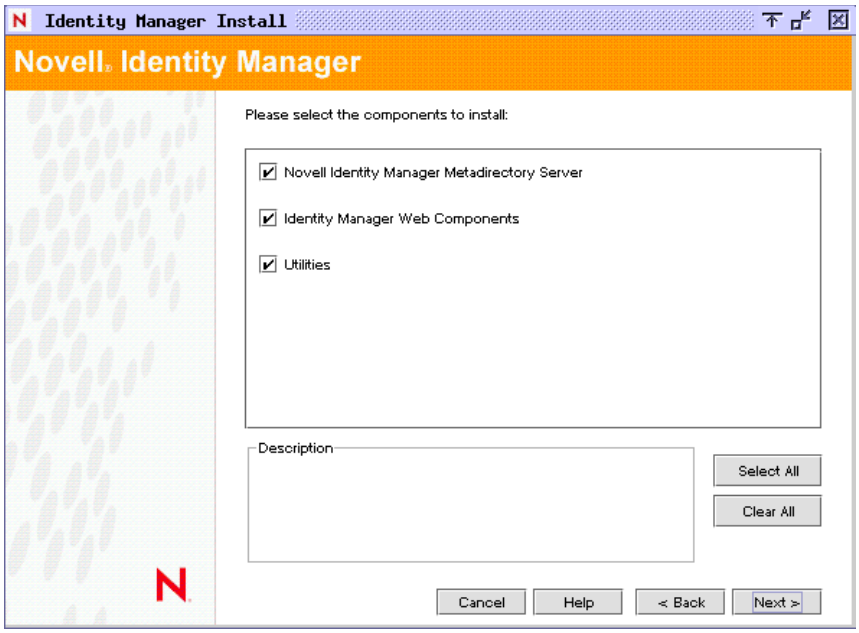
2. After you extract the file and place the image file on a disk, place the disk into the server's CD drive and allow the disk to be mounted as a volume.
3. Launch the NetWare GUI (enter `STARTX` at the server console prompt) and select *Novell* > *Install*.
4. In the Installed Products window, select *Add*, then specify the path to the Identity Manager `product.ini` file in the `\NW` directory. Click *OK*, then click *OK* again to begin loading the Identity Manager installation program.
5. After the files have finished copying, the Identity Manager Product Installation page appears. Click *Next* to begin the installation.



6. Select a language to view the license agreement or use the default (English).

   The Identity Manager installation program automatically runs in the language of the machine you are installing it on. If the installation program has not been translated to the language that your machine uses, it defaults to English.
7. Read the license agreement, then click *I Accept*.
8. 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 Table 1-3 on page 29.
9. On the Identity Manager Install page, select the components you want to install. See Table 1-3 on page 29.



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

- **Metadirectory Server:** Installs the Metadirectory engine and service drivers. On the NetWare platform, these include Identity Manager Drivers for Avaya, Delimited Text, eDirectory™, GroupWise®, JDBC*, JMS*, LDAP, Linux/UNIX Settings, RACF*, SOAP, SIF*, Top Secret, and Work Order. Selecting this option also extends the eDirectory schema.

  IMPORTANT: Novell eDirectory 8.7.3.6 or higher and Security Services 2.0.5 (NMAS™ 3.2.0) with current patches 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. If you do not have the correct version of NMAS, you receive a warning message and you lose Identity Manager functionality.

- **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 the NetWare installation of Identity Manager, this option is not available and you do 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. Driver utilities can include:

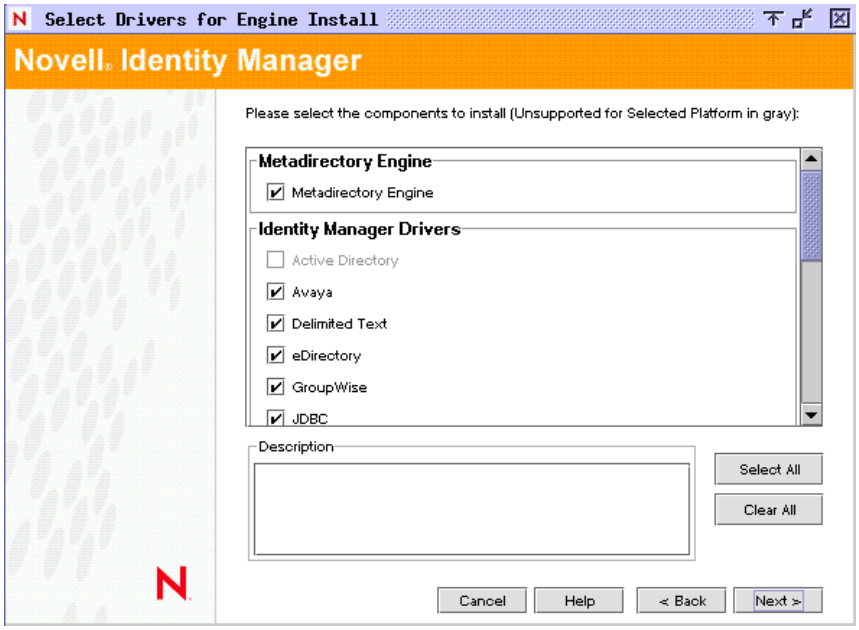
  - SQL scripts for the JDBC driver
  - JMS components
  - PeopleSoft components
  - License Auditing tool
  - Active Directory Discovery tool

- Lotus Notes Discovery tool
- SAP utilities

Another utility allows you to register the Novell Audit System components for Identity Manager (a valid eDirectory version and a Novell Audit logging server must be installed on the tree before this utility installs.)

10 Click *Next*.

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



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.

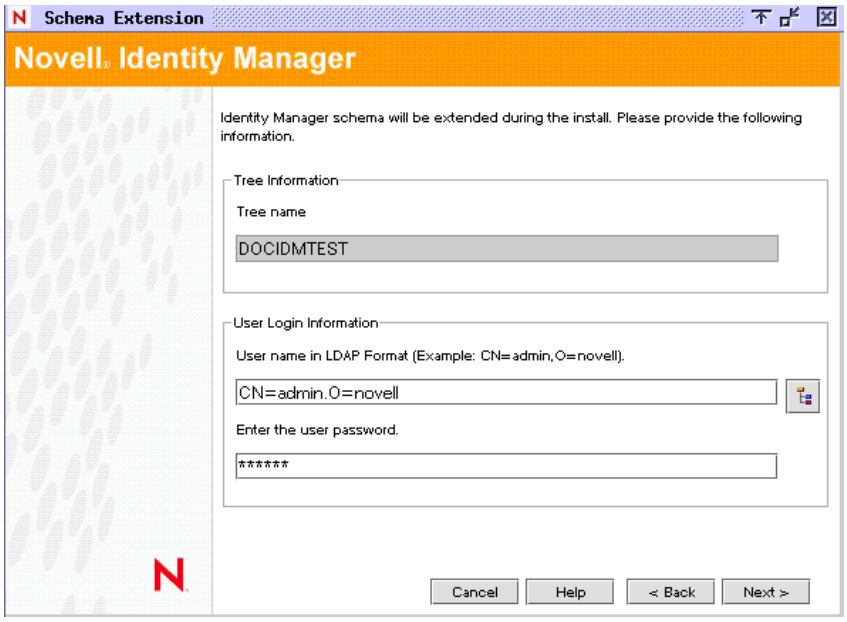
By default, all available drivers for the option are selected. We recommend installing all of the selected driver files so you won't need to run the installation program later if you want another driver. The driver files are not used until a driver is configured through iManager or through Designer and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

If you do not want to install all of the drivers, you can either click *Clear All* and then select the drivers you need, or click on the drivers you don't want to install to deselect them. If you need another driver in the future, you'll need to rerun this installation program to install any drivers you did not select. You can also use Designer to create, modify, and deploy driver files.

12 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.

13 On the Schema Extension page, specify the following:



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

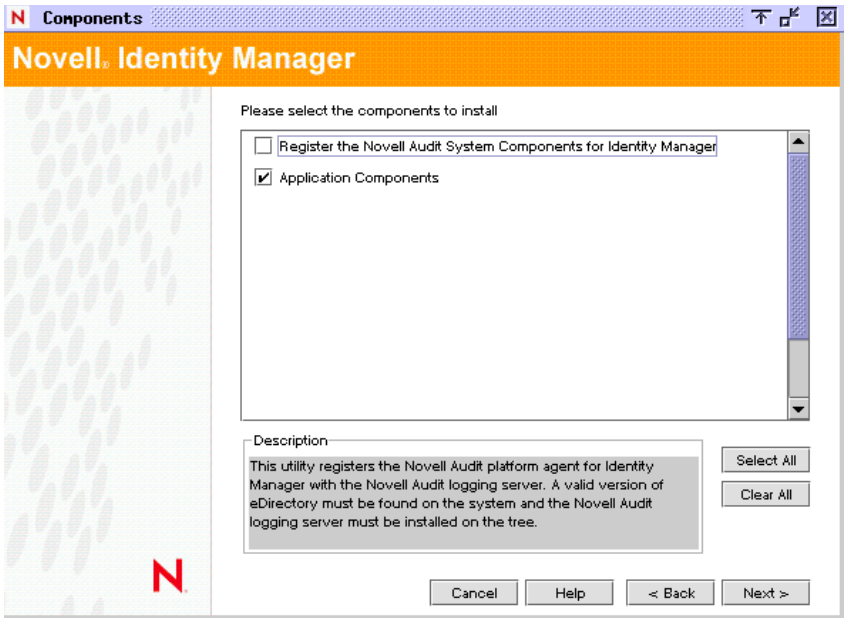
14 Click *Next*.

When the user information is validated, you see the first (of two) Components pages.

On the first Components page, *Novell Audit System Components for Identity Manager* is selected 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.

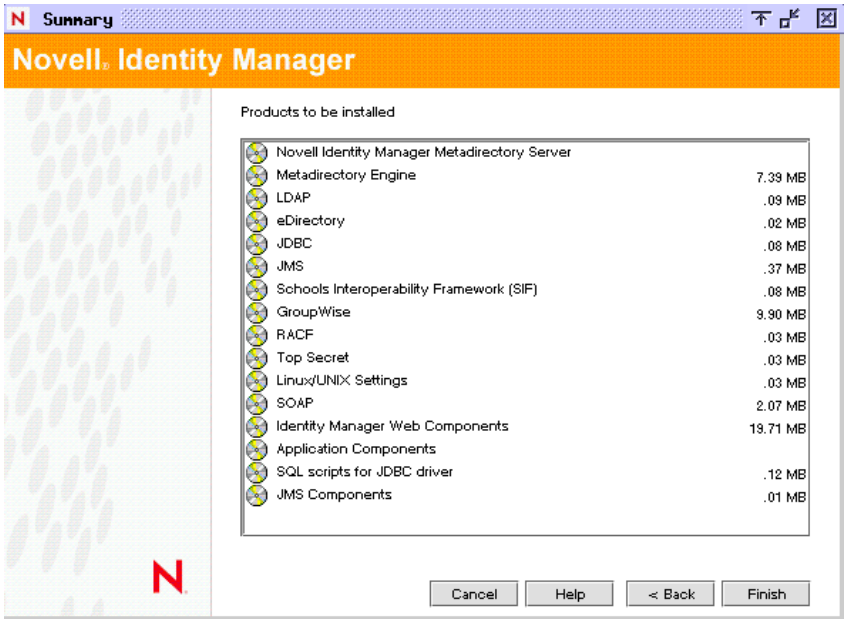
If the installer detects existing driver configuration files, it moves them to a backup path.

15 Click *Next*.

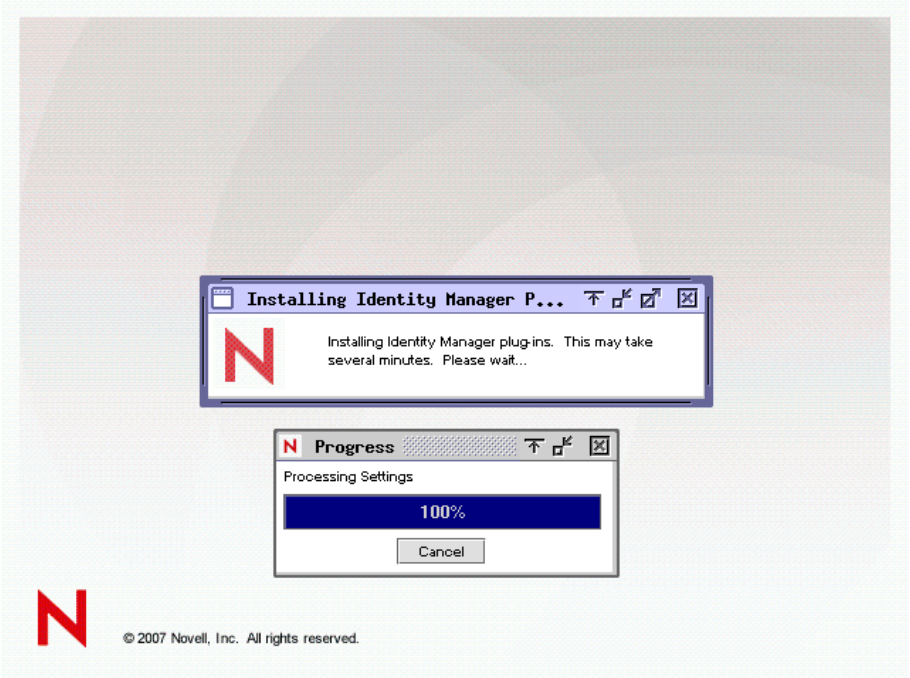


16 The second Components page installs the utilities. Platform-specific utilities are dimmed if they are available for platforms other than the one you are installing on. For NetWare, the only selections available are SQL Scripts for JDBC Driver and JMS components. Select the components you need, then click *Next*.

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



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*.

19 In order for iManager to recognize the plug-ins you installed, restart your Web services now and restart Tomcat.

If you have installed Identity Manager drivers, use the Identity Manager Configuration Wizard in iManager 2.6 or later, or you can use Designer to configure the drivers.

4.4 Installing Identity Manager on Windows

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

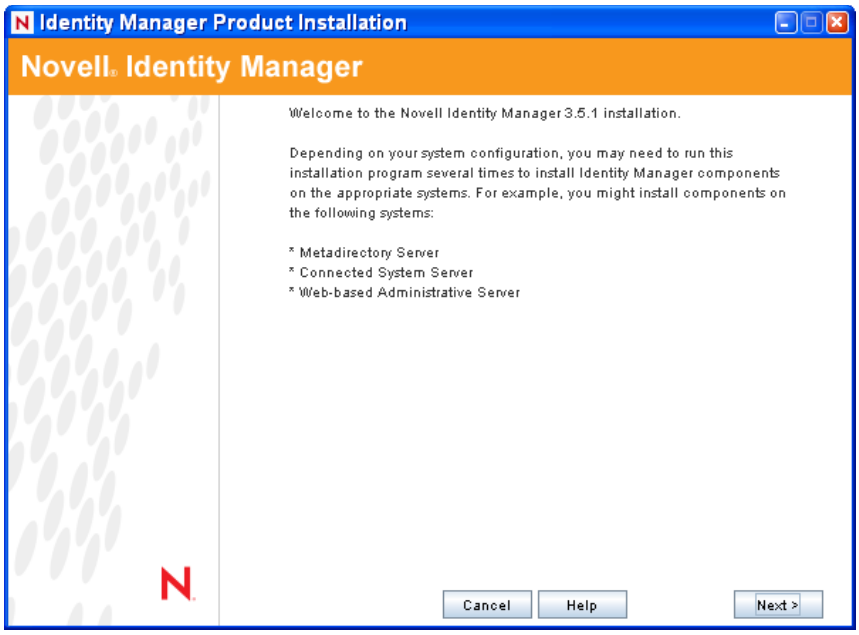
Before you begin, make sure your system meets the requirements listed in Table 1-3 on page 29.

1 Download the Identity Manager `.iso` image file you need. You can download the Identity Manager `.iso` image files from the Novell Download site (http://download.novell.com).

The Windows installation of Identity Manager is located on the `Identity_Manager_3_5_1_NW_Win.iso` or on the `Identity_Manager_3_5_1_DVD.iso`.

2 After you extract the file, double-click the `install.exe` file found in the `\NT` directory.

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



3 Click *Next* to begin the installation.

4 Select a language to view the license agreement or use the default (English).

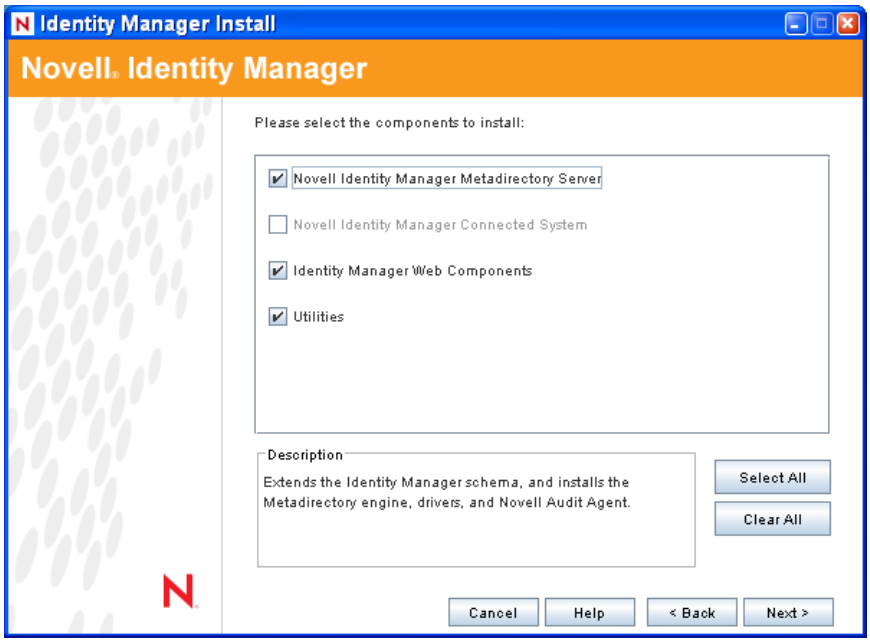
The Identity Manager installation program automatically runs in the language of the machine that you are installing it on. If the installation program has not been translated to the language that your machine uses, it defaults to English.

5 Read the license agreement, then click *I Accept*.

6 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 Table 1-3 on page 29.

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



The following options are available:

- **Metadirectory Server:** Installs the Metadirectory engine and service drivers. These include Identity Manager Drivers for Active Directory, Avaya, Delimited Text, eDirectory, Exchange, GroupWise, JDBC, JMS, LDAP, Linux/UNIX Settings, Lotus Notes, PeopleSoft, RACF, Remedy, SOAP, SAP, SIF, and Top Secret. Selecting this option also extends the eDirectory schema.

  IMPORTANT: Novell eDirectory 8.7.3.6 or 8.8 and Security Services 2.0.5 (NMAS 3.2.0) with current patches 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. If you do not have the correct version of NMAS, you receive a warning message and you lose Identity Manager functionality.

- **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, Avaya, Delimited Text, eDirectory, Exchange, GroupWise, JDBC, JMS, LDAP, Linux/UNIX Settings, Lotus Notes, PeopleSoft, RACF, Remedy, SOAP, SAP, SIF, and Top Secret.

  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 81.

- **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. Driver utilities can include:

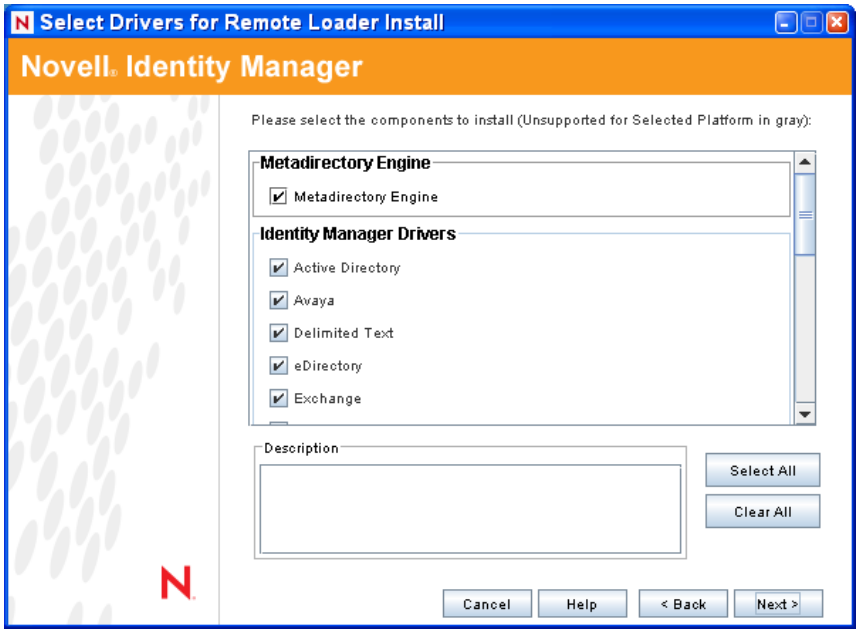
  - SQL scripts for JDBC driver
  - JMS components

- PeopleSoft components
- License Auditing tool
- Active Directory Discovery tool
- Lotus Notes Discovery tool
- SAP utilities
- Scripting Driver Installer and Configuration Tool

Another utility allows you to register the Novell Audit System components for Identity Manager (a valid eDirectory version and a Novell Audit logging server must be installed on the tree before this utility installs.)

8 Click *Next*.

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



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.

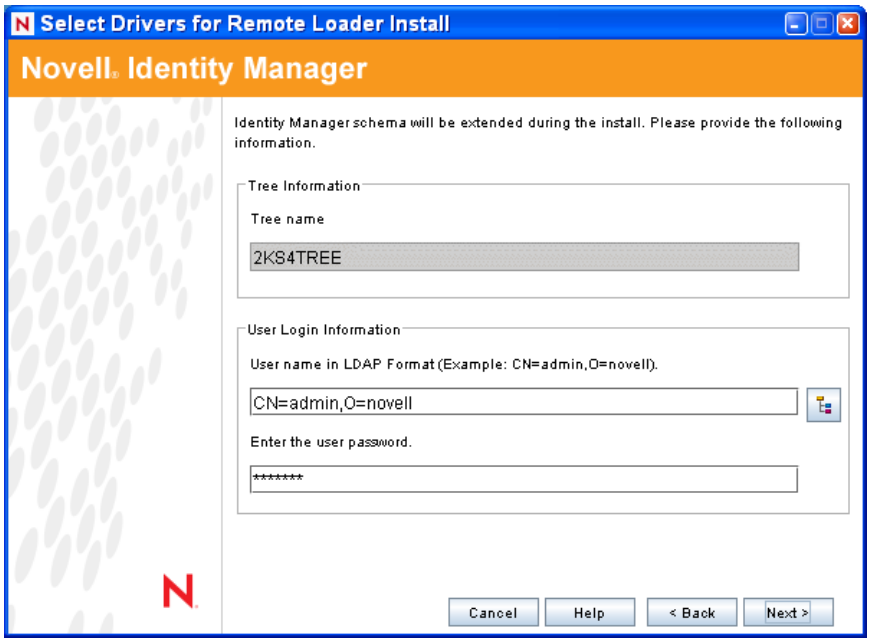
10 When you see the informational message reminding you about product activation, click *OK*.

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

11 When you 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

12 On the Schema Extension page, specify the following:



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

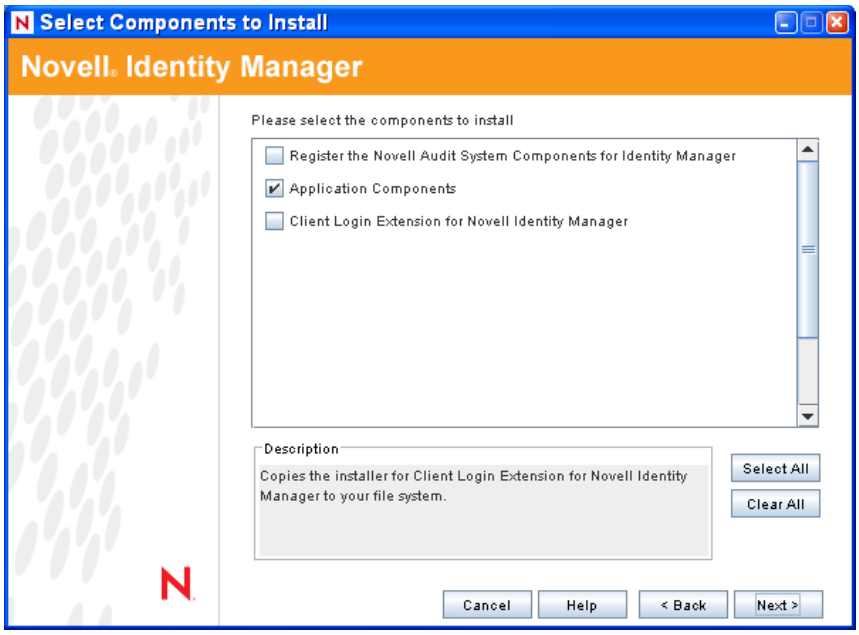
13 Click *Next*. When the user information is validated, you see the first of two Components pages:

On the Select Components To Install page, *Register the Novell Audit System Components for Identity Manager* is selected if you have a valid version of eDirectory and the Novell Audit logging server installed on the tree. Otherwise, it is not selected. The *Application Components* selection installs components for such application systems as JDBC and PeopleSoft.

If the installer detects existing driver configuration files, it moves them to a backup path.

The *Client Login Extension for Novell Identity Manager* selection copies the installer for the Client Login Extension to your file system. For more information on the Client Login Extension for Novell Identity Manager, see "Client Login Extension for Novell Identity Manager 3.5.1" in the *Novell Identity Manager 3.5.1 Administration Guide*.

14 Select the components you want to install, then click *Next*.



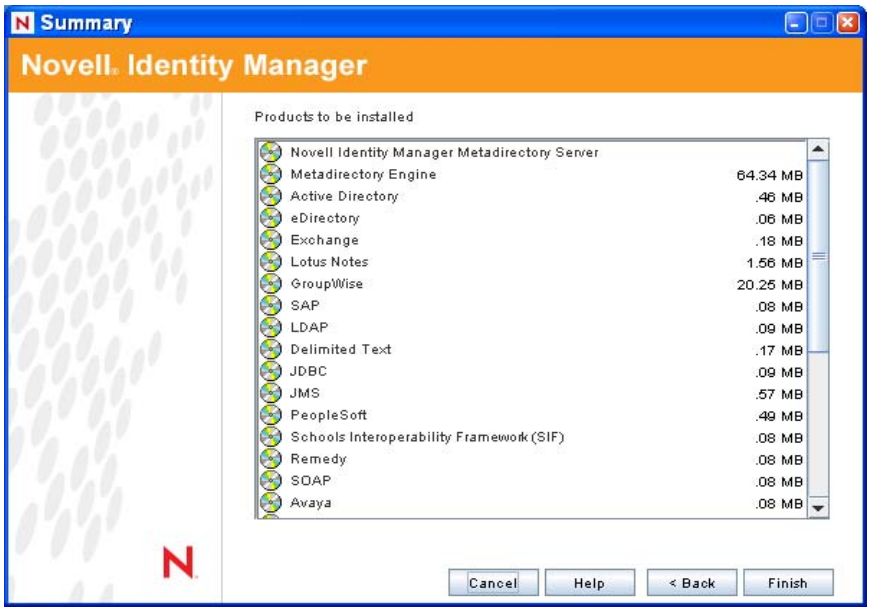
15 An additional page displays to install the Identity Manager plug-ins for iManager, using the SSL Port 443. Click *Next*.

16 The second Components page installs the utilities. The Windows installation presents you with an additional page showing the directory where the Application Components are placed. The default is `C:\Novell\NDS\DirXMLUtilities`. Click *Next*.

17 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, JMS Components, PeopleSoft Components, License Auditing Tool, Active Directory Discovery Tool, Lotus Notes Discovery Tool, SAP Utilities and Scripting Driver Installer and Configuration Tool. Select the components you need and click *Next*.

18 If you selected to copy the installer of the Client Login Extension for Novell Identity Manager to your file system, select an installation path or use the default path of `C:\Novell\NDS\DirXMLUtilities\cle`. Click *Next*.

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



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

20 After the installation completes and displays the Installation Complete dialog box, click *Close*.

21 In order for iManager to recognize the plug-ins you installed, restart your Web services now and restart Tomcat.

If you have installed Identity Manager drivers, use the Identity Manager Configuration Wizard in iManager 2.6 or later, or you can use Designer to configure the drivers.

4.5 Installing the Connected System Option on Windows

Section 4.4, “Installing Identity Manager on Windows,” on page 75 covered the installation of the Metadirectory Server, Web Components, and Utilities for Windows. In addition, Windows servers can also use the Connected System option.

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 Table 1-3 on page 29.

1 Download the Identity Manager `.iso` image file you need. You can download the Identity Manager `.iso` image files from the Novell Download site (http://download.novell.com).

The Windows installation of Identity Manager is located on the `Identity_Manager_3_5_1_NW_Win.iso` or on the `Identity_Manager_3_5_1_DVD.iso`.

2 Run `install.exe` from the `\NT` directory.

3 Read the Welcome information, then click *Next*.

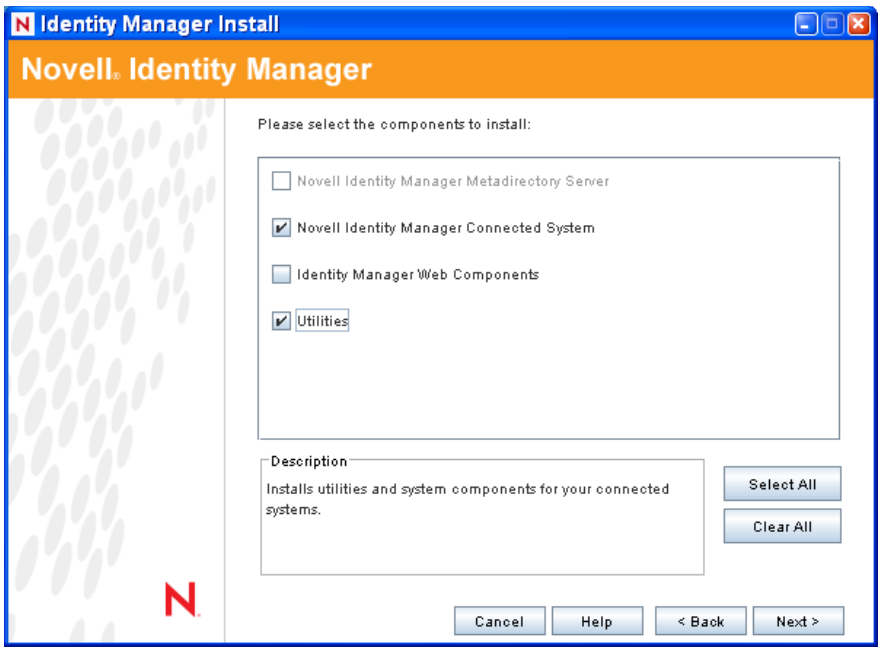
4 Select a language to view the license agreement or use the default (English).

The Identity Manager installation program automatically runs in the language of the machine you are installing it on. If the installation program has not been translated to the language that your machine uses, it defaults to English.

5 Read the License Agreement, then click *I Accept*.

6 Review the Overview pages about the various systems and components, then click *Next* to begin the installation.

7 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.



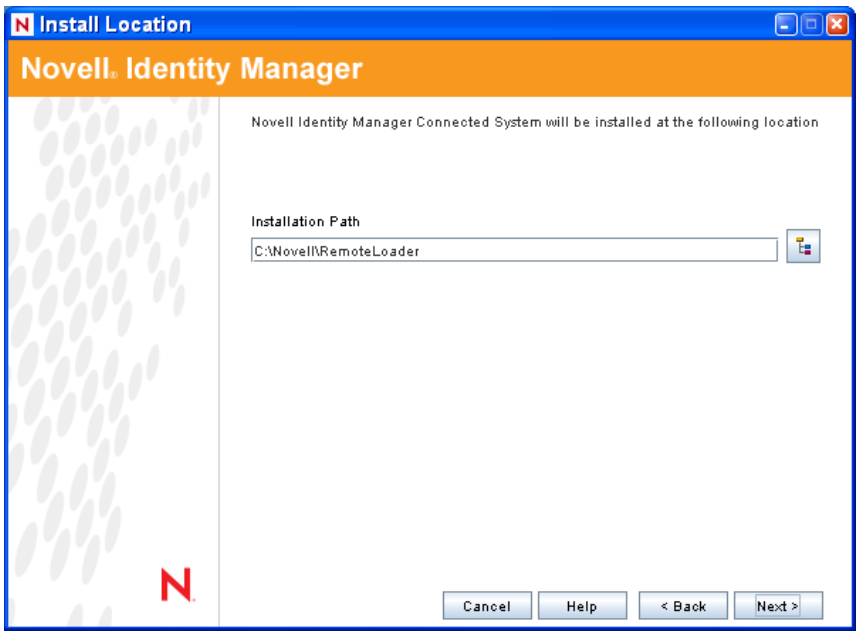
- **Connected System:** Installs the Remote Loader that allows you to establish a link between the connected system and a server running the Metadirectory engine. For Windows, this option installs the following drivers: Active Directory, Avaya, Delimited Text, eDirectory, Exchange, GroupWise, JDBC, JMS, LDAP, Linux/UNIX Settings, Lotus Notes, PeopleSoft, RACF, Remedy, SOAP, SAP, SIF, and Top Secret.
- **Utilities:** Installs additional scripts for the JDBC driver and utilities for other drivers. Most drivers don't have a utility connected to them. Driver utilities can include:
  - SQL scripts for JDBC driver
  - JMS components
  - PeopleSoft components
  - License Auditing tool
  - Active Directory Discovery tool
  - Lotus Notes Discovery tool

- SAP utilities
- Scripting Driver Installer and Configuration Tool

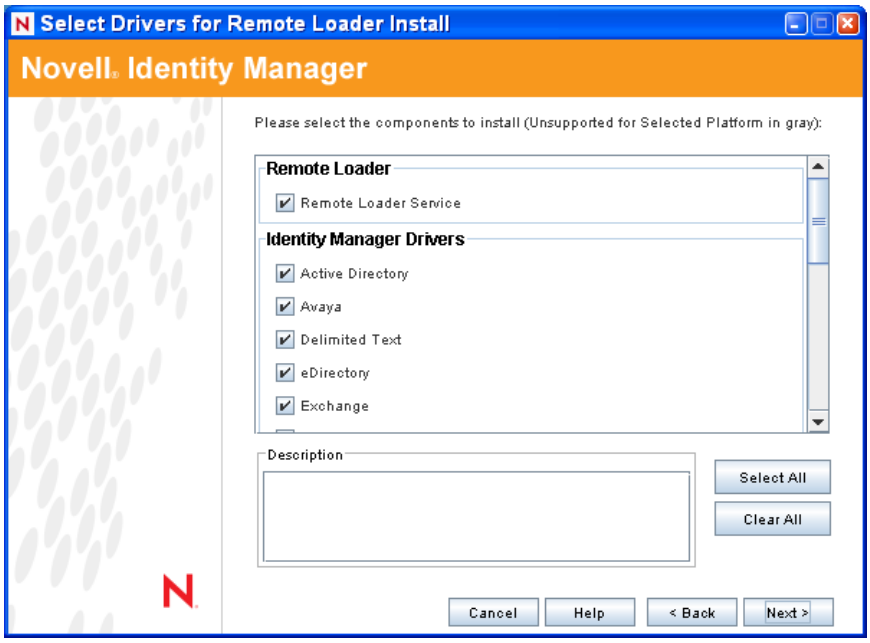
Another utility allows you to register the Novell Audit System components for Identity Manager (a valid eDirectory version and a Novell Audit logging server must be installed on the tree before this utility installs.)

8 Click *Next*.

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



10 On the Select Drivers for Remote Loader Install page, select the Identity Manager drivers you want to load, then click *Next*.



The driver selection includes Active Directory, Avaya, Delimited Text, eDirectory, Exchange, GroupWise, JDBC, JMS, LDAP, Linux/UNIX Settings, Lotus Notes, PeopleSoft, RACF, Remedy, SOAP, SAP, SIF, and Top Secret.

If you do not want to install all of the drivers, you can either click *Clear All* and then select the drivers you need, or click on the drivers you don't want to install to deselect them. If you need another driver in the future, you'll need to rerun this installation program to install any drivers you did not select. You can also 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 When you 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.

13 Click *Yes* to create a shortcut on the desktop for the Remote Loader Console. If you do not want a shortcut, click *No*.

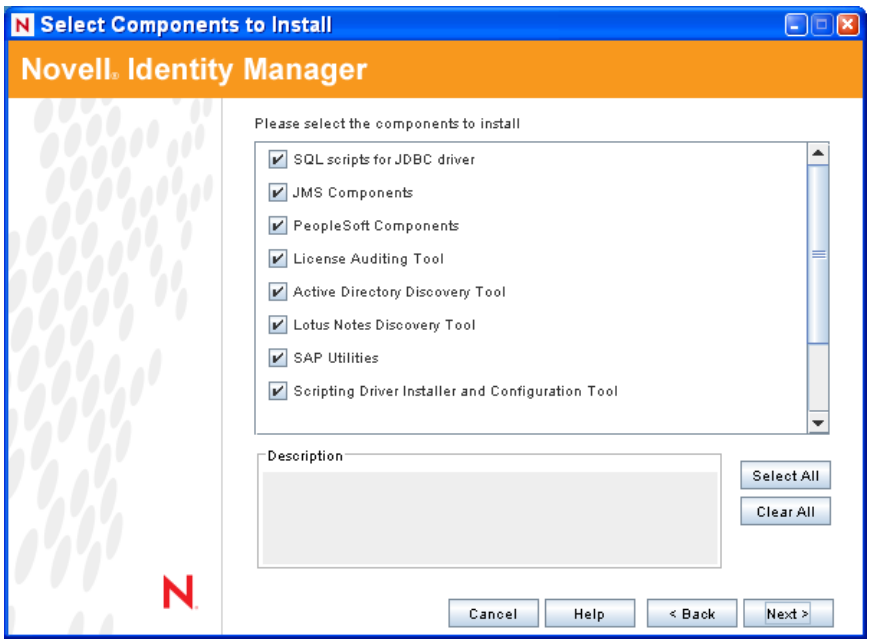
On the Select Components To Install page, the *Register the Novell Audit System Components for Identity Manager* is selected if you have a valid version of eDirectory and the Novell Audit logging server installed on the tree. Otherwise, it is not selected. The *Application Components* selection installs components for such application systems as JDBC and PeopleSoft.

The *Client Login Extension for Novell Identity Manager* selection copies the installer for the Client Login Extension to your file system. For more information on the Client Login Extension for Novell Identity Manager, see "Client Login Extension for Novell Identity Manager 3.5.1" in the *Novell Identity Manager 3.5.1 Administration Guide*.

14 Select the components you want to install, then click *Next*.

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

16 Select the driver components and utilities you want to install, then click *Next*.



17 If you selected to copy the installer of the Client Login Extension for Novell Identity Manager to your file system, select an installation path or use the default path of `C:\Novell\NDS\DirXMLUtilities\cle`. Click *Next*.

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

19 Click *Close* to exit the installation program.

4.6 Installing Identity Manager through the GUI Interface 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 69.

1 Download the Identity Manager `.iso` image file you need. You can download the Identity Manager `.iso` image files from the Novell Download site (http://download.novell.com).

The Linux install for Identity Manager is located on the `Identity_Manager_3_5_1_Linux.iso` or on the `Identity_Manager_3_5_1_DVD.iso`, while AIX and Solaris are located on the `Identity_Manager_3_5_1_Unix.iso` or the `Identity_Manager_3_5_1_DVD.iso`.

2 On the host computer, log in as `root`.

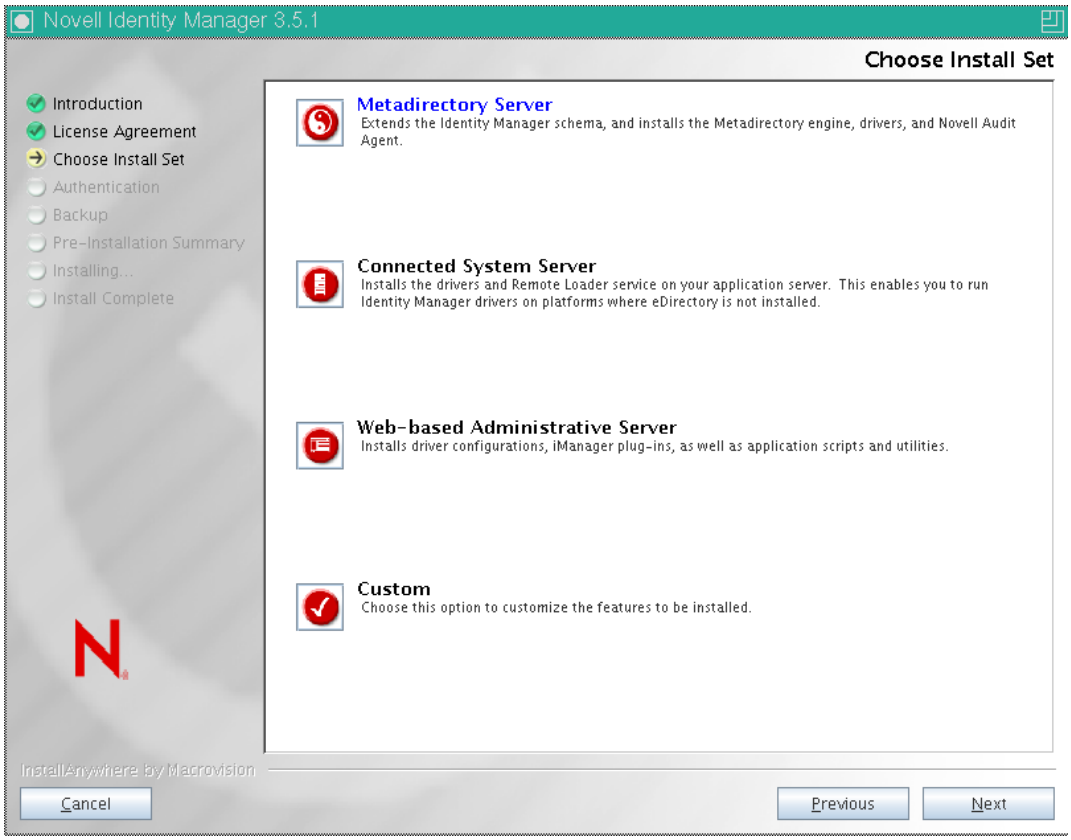
3 To run the GUI install on Linux, click the `install.bin` file in the root directory. You are asked if you want to run the install file in terminal mode or in display mode. Select *Terminal*. The `install.bin` file checks to see if Xwindows is present, and if it is, it brings up Identity Manager’s GUI install program for Linux.

NOTE: If clicking the `install.bin` fails to launch the GUI install program, open a terminal window and run `install.bin` manually. If you have a Solaris server running eDirectory 8.8.x, run the Identity Manager install program without the GUI. See Section 4.7, "Using the Console To Install Identity Manager on UNIX/Linux Platforms," on page 89.

4 Select the language that you want to run the installation program in, or use the default (English). Click *OK*.

5 Review the Welcome information, then click *Next* to continue the installation.

6 Read the License Agreement, select *I accept the terms of the License Agreement*, then click *Next*.



7 Specify 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 8.7.3.6 or higher and Security Services 2.0.5 (NMAS 3.2.0) with the latest Support Packs must be installed before you can install this option. The Identity Manager installation process stops if these are not installed.

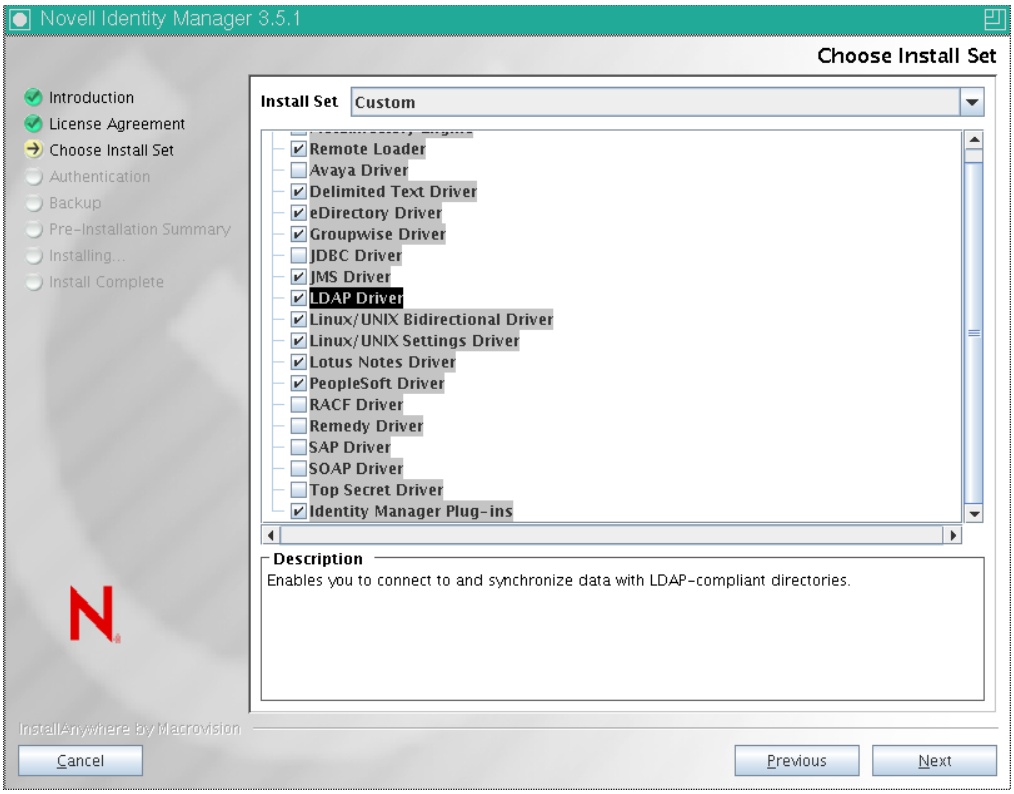
- **Connected System Server:** Installs the Remote Loader and the following drivers: Avaya, Delimited Text, GroupWise, JDBC, JMS, LDAP, Linux/UNIX Settings, Linux/UNIX Bidirectional, Lotus Notes, PeopleSoft, RACF, Remedy, SAP, SIF, Top Secret, and Work Order. Choose the Connected System Server option 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.

  By default, Identity Manager driver utilities are not installed on Linux/UNIX installations. You must manually copy the utilities from the Identity Manager installation CD to the Identity Manager server. All utilities are found under the *platform's* `\setup\utilities` directory.

- **Customize:** Installs the specific components you select from a list of all components.



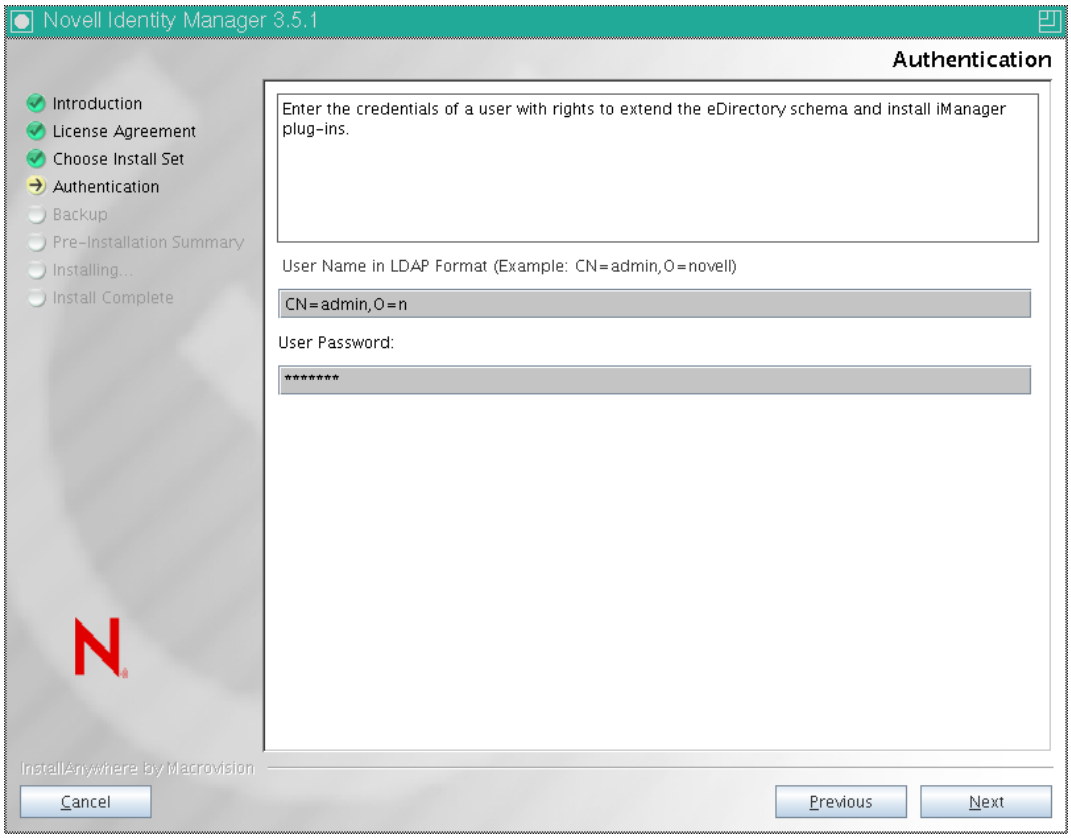
You can select *Previous* to return to previous menus and modify your installation options.

8 (Optional) Depending on the option you chose (such as the Metadirectory Server) and whether you are running eDirectory v8.8, you are prompted to set the LD_LIBRARY_PATH environment variable. To do this, execute the `/opt/novell/eDirectory/bin/ndspath` script by entering `. /opt/novell/eDirectory/bin/ndspath`, and then re-run the installation.

NOTE: After the `ndspath` command is executed, use the same window to start the installer.

---

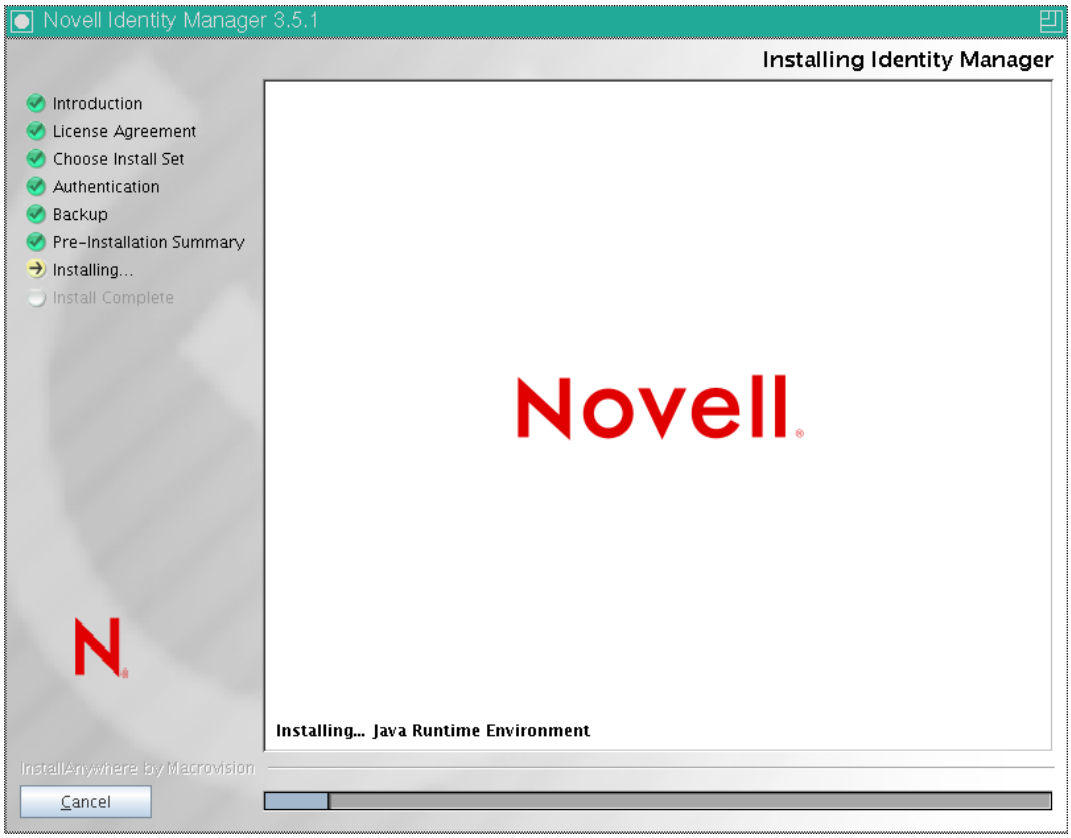
9 If you select to install the Metadirectory Server, you are prompted for the LDAP username (CN=admin,O=novell) and password. Select a user who has enough rights to extend the eDirectory schema (someone who has Supervisor rights to the root of the tree, such as Admin).



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

---

10 Verify that the information contained in the Pre-Installation Summary page is correct, then click *Install* to start installing the packages.



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.

11 When you see the Installation Complete page, click *Done* to close the installation program.

4.7 Using the Console To Install Identity Manager on UNIX/Linux Platforms

Before you begin, make sure your system meets the requirements listed in Table 1-3 on page 29.

1 Download the Identity Manager `.iso` image file you need. You can download the Identity Manager `.iso` image files from the Novell Download site (http://download.novell.com).

The Linux install for Identity Manager is located on the `Identity_Manager_3_5_1_Linux.iso` or on the `Identity_Manager_3_5_1_DVD.iso`, while AIX and Solaris are located on the `Identity_Manager_3_5_1_Unix.iso` or the `Identity_Manager_3_5_1_DVD.iso`.

2 On the host computer, log in as `root`.

3 Execute the `.bin` file from the setup directory.

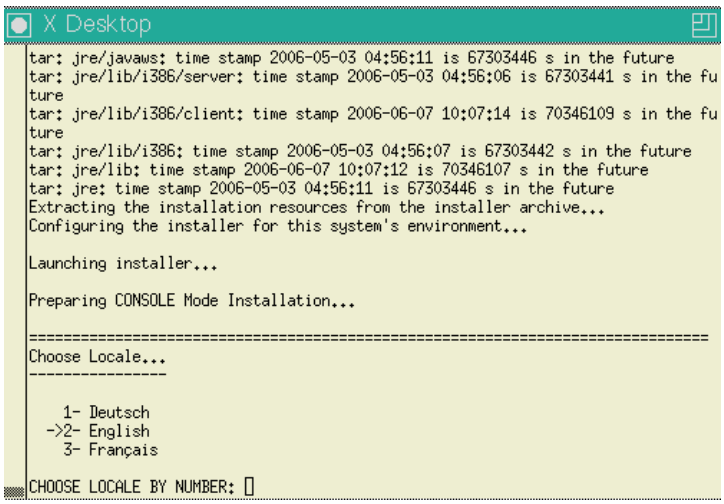
Change the current working directory to the setup directory, where the install is located. Then enter one of the following commands to run the install.

Platform	Example Path	Installation File
Linux	`linux/setup/`	`idm_linux.bin`
Solaris	`solaris/setup/`	`idm_solaris.bin`
AIX	`aix/setup/`	`idm_aix.bin`

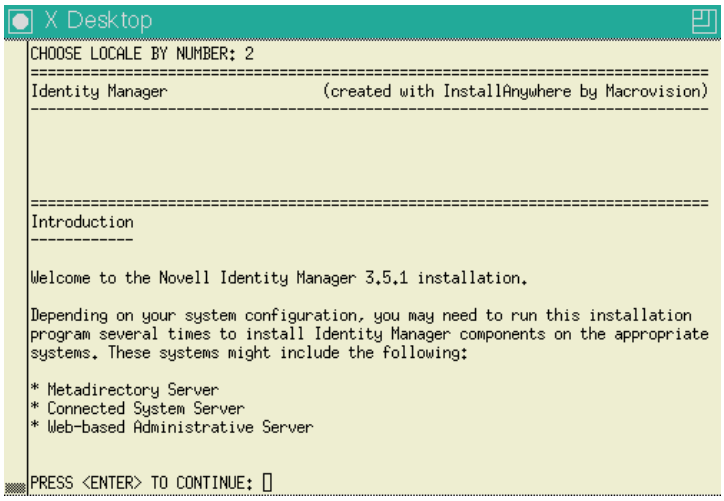
These paths are relative to the root of the install image, which could be anywhere you expanded it or mounted the CD. It also depends on the ISO image you downloaded. For example, Linux is located on the `Identity_Manager_3_5_1_Linux.iso` or on the `Identity_Manager_3_5_1_DVD.iso`, while AIX and Solaris are located on the `Identity_Manager_3_5_1_Unix.iso` or the `Identity_Manager_3_5_1_DVD.iso`.

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

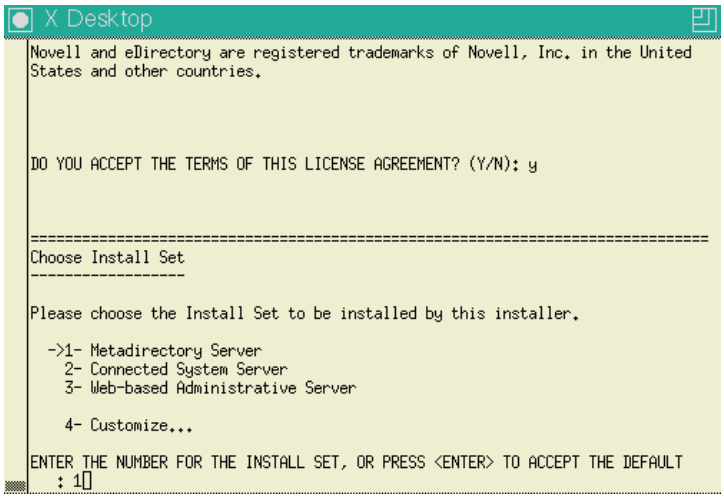
4 Select the language that you want to run the installation program in, or use the default (English). Type a number and press Enter.



5 Review the Welcome information, the press Enter to continue the installation.



6 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.



7 Specify the appropriate number (1-4) for the install set you want to install. The install sets contain the following components:

- **1- Metadirectory Server:** Installs the Metadirectory engine and service drivers, Identity Manager drivers, Novell Audit agent, and extends the eDirectory schema.

  Novell eDirectory 8.7.3.6 or 8.8 and Security Services 2.0.5 (NMAS 3.2.0) with the latest Support Packs must be installed before you can install this option. The Identity Manager installation process will stop if these are not installed.

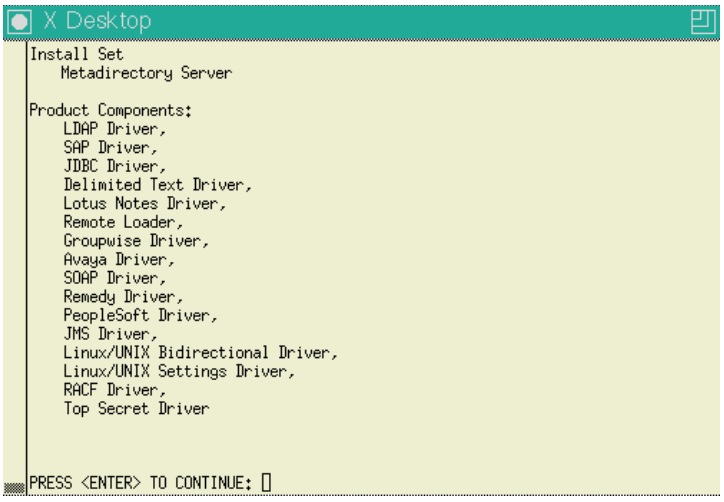
- **2- Connected System Server:** Installs the Remote Loader and the following drivers: Avaya, Delimited Text, GroupWise, JDBC, JMS, LDAP, Linux/UNIX Settings, Linux/UNIX Bidirectional, Lotus Notes, PeopleSoft, RACF, Remedy, SAP, SIF, Top Secret, and Work Order. You can choose the *Connected System Server* option when you don't want to put the overhead of eDirectory services and the Metadirectory engine on your application server.

- **3- 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.

  By default, Identity Manager driver utilities are not installed on Linux/UNIX installations. You must manually copy the utilities from the Identity Manager installation CD to the Identity Manager server. All utilities are found under the *platform's* `\setup\utilities` directory.

- **4- Customize:** Installs the specific components you select from a list of all components.



You can enter `prev` to return to previous menus and modify your installation options.

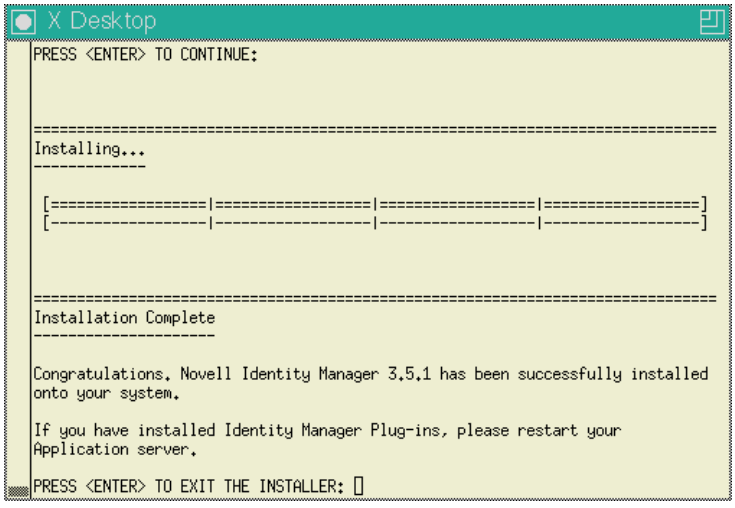
8 (Optional) Depending on the option you chose (such as the Metadirectory Server) and whether you are running eDirectory v8.8, you are prompted to set the LD_LIBRARY_PATH environment variable. To do this, execute the `/opt/novell/eDirectory/bin/ndspath` script by entering `. /opt/novell/eDirectory/bin/ndspath`, then re-run the installation.

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

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

---

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



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.

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

4.8 Using the Console To Install the Connected System Option on UNIX/Linux

Section 4.7, "Using the Console To Install Identity Manager on UNIX/Linux Platforms," on page 89 covered the installation of the Metadirectory Server, Web Components, and Utilities on UNIX platforms. In addition, UNIX or Linux servers can use the Connected System option.

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 Table 1-3 on page 29.

1 Download the Identity Manager `.iso` image file you need. You can download the Identity Manager `.iso` image files from the Novell Download site (http://download.novell.com).

The Linux install for Identity Manager is located on the `Identity_Manager_3_5_1_Linux.iso` or on the `Identity_Manager_3_5_1_DVD.iso`, while AIX and Solaris are located on the `Identity_Manager_3_5_1_Unix.iso` or the `Identity_Manager_3_5_1_DVD.iso`.

2 On the host computer, log in as `root`.

3 Execute the `.bin` file from the setup directory.

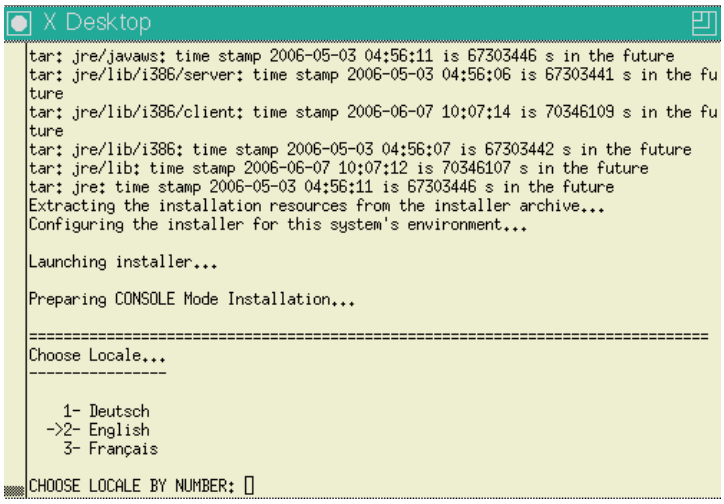
Change the current working directory to the setup directory, where the install is located. Then enter one of the following commands to run the install:

Platform	Example Path	Installation File
Linux	`linux/setup/`	`idm_linux.bin`
Solaris	`solaris/setup/`	`idm_solaris.bin`
AIX	`aix/setup/`	`idm_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 Select the language that you want to run the installation program in, or use the default (English). Type a number and press Enter.

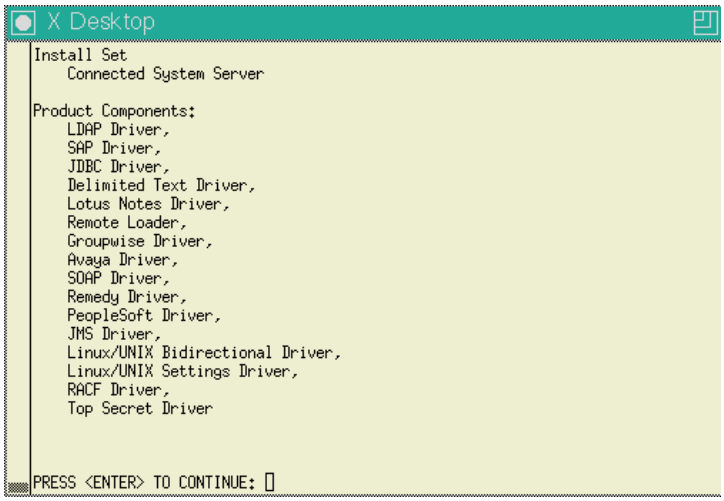


5 Review the Welcome information, the press Enter to continue the installation.

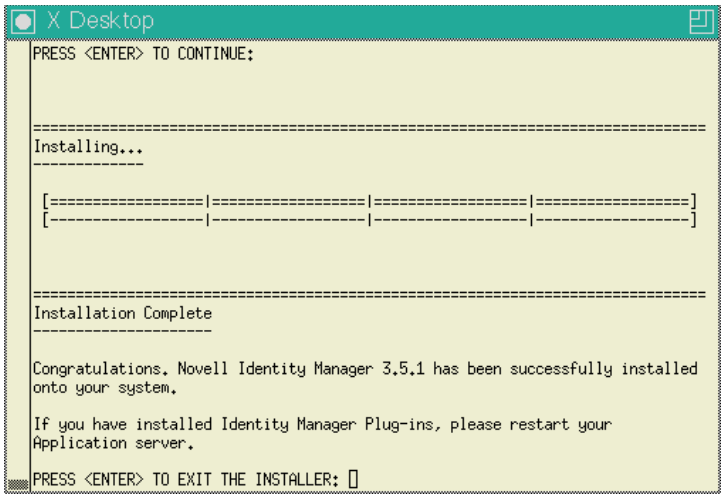
6 Press Enter to progress through the license agreement, then enter `Y` if you agree to the usage terms. If you do not agree, enter `N` to exit the installation program.

7 Specify number 2 to install Connected System Server.

The install set contains the Remote Loader and the following drivers: Avaya, Delimited Text, GroupWise, JDBC, JMS, LDAP, Linux/UNIX Settings, Linux/UNIX Bidirectional, Lotus Notes, PeopleSoft, RACF, Remedy, SAP, SIF, Top Secret, and Work Order.



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



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.

By default, Identity Manager driver utilities are not installed on Linux/Unix installations. You must manually copy the utilities from the Identity Manager installation CD to the Identity Manager server. All utilities are found under the *platform's* `\setup\utilities` directory.

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

4.9 Non-root Installation of Identity Manager

This release of Identity Manager allows you to install the Identity Manager Metadirectory engine into a non-root installation of eDirectory.

Novell Security Services 2.0.4 (NMAS 3.1.3) and non-root eDirectory 8.8 with current patches must be installed before you can install this option. For information on installing NICI as a non-root user, see the *"Installing NICI*" subsection under the "*3.0 Installing or Upgrading Novell eDirectory on Linux*" heading in the Novell eDirectory 8.8 Installation Guide (http://www.novell.com/documentation/edir88/index.html).

After NICI is installed, follow the installation instructions for non-root eDirectory 8.8 found in the *"Nonroot User Installing eDirectory 8.8"* subsection under the "*3.0 Installing or Upgrading Novell eDirectory on Linux*" heading in the Novell eDirectory 8.8 Installation Guide (http://www.novell.com/documentation/edir88/index.html).

1 Download the Identity Manager `.iso` image file you need. You can download the Identity Manager `.iso` file from the Novell Download site (http://download.novell.com).

Linux is located on the `Identity_Manager_3_5_1_Linux.iso` or on the `Identity_Manager_3_5_1_DVD.iso`, while AIX and Solaris are located on the `Identity_Manager_3_5_1_Unix.iso` or the `Identity_Manager_3_5_1_DVD.iso`. The non-root install program is included in the `.iso` image.

2 On the host computer, log in as someone who has write rights to the directory you have installed non-root eDirectory.

3 Execute the `idm-nonroot-install` file from the `/setup/` directory. To do this, change the current working directory to the `setup` directory, then enter the following command to run the non-root install:

```
./idm-nonroot-install
```

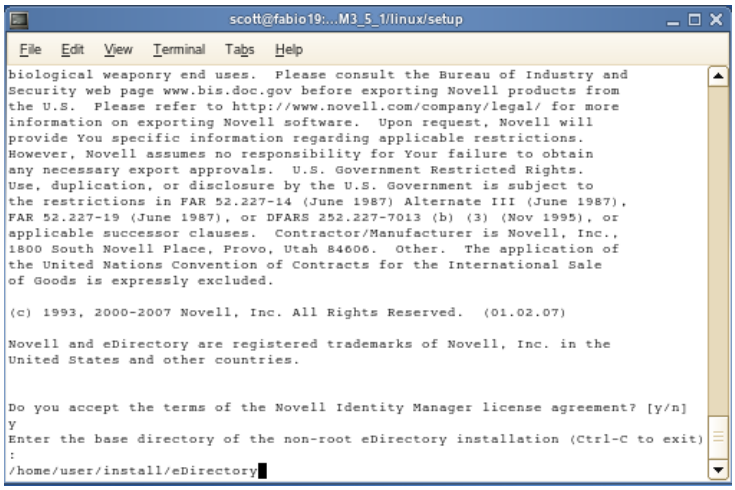
Platform	Example Path	Installation File
Linux	`linux/setup/`	`idm-nonroot-install`
Solaris	`solaris/setup/`	`idm-nonroot-install`
AIX	`aix/setup/`	`idm-nonroot-install`

These paths are relative to the root of the `iso` image, and 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 Press Enter to bring up the end user license agreement, then press the spacebar to scroll through the agreement. Enter `Y` if you agree to the usage terms. If you do not agree, enter `N` to exit the installation program.

5 Enter the path that points to where the non-root eDirectory resides. For example:

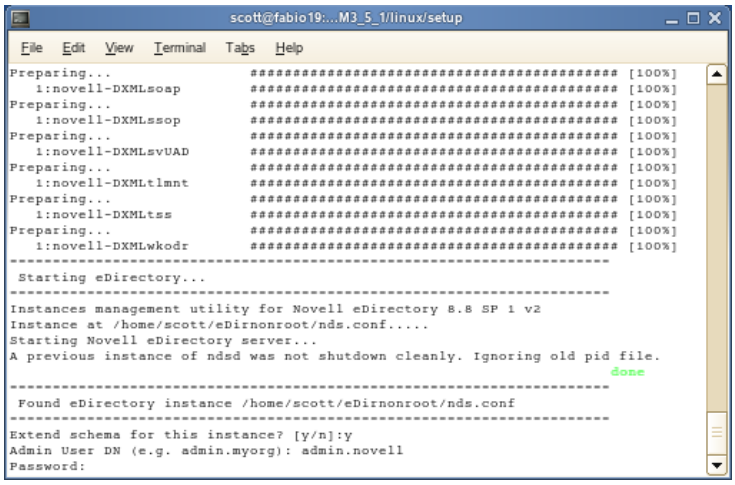
```
/home/user/installed/eDirectory
```



The installation script then installs Identity Manager with the following drivers: Avaya, Delimited Text, GroupWise, JDBC, JMS, LDAP, Linux/UNIX Settings, Linux/UNIX Bidirectional, Lotus Notes, PeopleSoft, RACF, Remedy, SAP, SIF, Top Secret, and Work Order.

6 You are next asked to extend the schema for each eDirectory instance that is owned by the logged-in user. For each instance, enter `Y` to extend the schema for that instance, or `N` if you don't want to extend the schema for that instance.

7 If you select to extend the schema, type the distinguished name (DN) of the person who has rights to extend the schema (such as admin.novell). Select a user who has enough rights to extend the eDirectory schema (someone who has Supervisor rights to the root of the tree, such as Admin).



8 Type in the password and press Enter. You need to perform Steps 7 and 8 for each eDirectory instance that you extend.

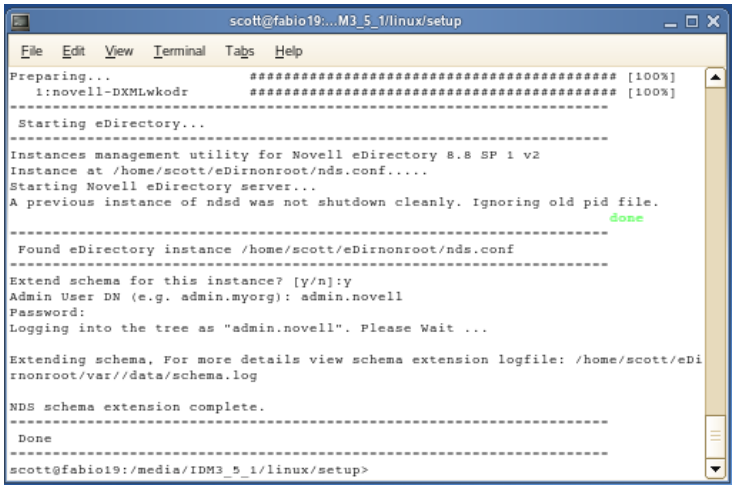
If you want to extend the schema for other eDirectory instances at a later time, run the `idm-nonroot-install` script in the `opt/novell/eDirectory/bin` subdirectory of the non-root eDirectory installation. Run the script while logged in as the owner of the eDirectory instance you want to extend.

The install script logs into the eDirectory tree and extends the schema. If you want more details on the schema extension process, go to the `/home/user/eDirnonroot/var/data/schema.log` file.

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.

By default, Identity Manager driver utilities are not installed on Linux/UNIX installations. You must manually copy the utilities from the Identity Manager installation CD to the Identity Manager server. All utilities are found under the *platform's* `\setup\utilities` directory.

9 When the schema extension in completes, Identity Manager is installed.



4.10 Post-Installation Tasks

You do not need to manually load or unload Identity Manager, because the Identity Manager module loads when an Identity Manager driver starts. 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. If one of the driver's parameters is set to Manual, the Identity Manager module loads when you start an Identity Manager driver.

After you install Identity Manager, you need to configure the drivers you installed to implement the policies and requirements that you define as business processes. Post-installation tasks typically include the following items:

- Configure a connected system. Refer to the Identity Manager driver documentation (http://www.novell.com/documentation/idm35drivers/index.html) for driver-specific configuration instructions.
- Create and configure a driver. Use iManager or the Designer utility to create a driver or to configure an existing driver. See "Importing a Driver Configuration File" in the *Designer 2.1 for Identity Manager 3.5.1* guide.
- Define policies. Use iManager or the Designer utility to define policies for drivers to meet your business needs. See "Creating a Policy" in the *Policies in Designer 2.1* guide, or see the *Understanding Policies for Identity Manager 3.5.1* guide.
- Start, stop, or restart a driver. Use iManager or the Designer utility to manage a driver's activities. See "Importing a Driver Configuration File" in the *Designer 2.1 for Identity Manager 3.5.1* guide.
- Activate Identity Manager. See Chapter 6, "Activating Novell Identity Manager Products," on page 185.

4.11 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). See also "Editing Driver Configuration Files" in the *Novell Identity Manager 3.5.1 Administration Guide*.

Installing the User Application

5

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

5.1 Migrating the User Application

If you are migrating to the latest version of the Identity Manager User Application, please refer to the *Identity Manager User Application: Migration Guide* (http://www.novell.com/documentation/idm35/pdfdoc/migration/migration.pdf) for directions.

5.2 Prerequisites to Installation

Before you install the Identity Manager User Application, verify that the following requirements are met:

Table 5-1 *Installation Prerequisites*

Environment Requirements	Description

Java* Development Kit	On JBoss Application Servers, download and install the following Sun JDK: Java 2 Platform Standard Edition Development Kit 5.0. Use JRE version 1.5.0_10. Do not use the IBM JDK that comes with SLES.
	
	On WebSphere* Application Servers, use the IBM JDK that comes with WebSphere Application Server 6.1.0.9 and apply the unrestricted policy files. Apply the WAS JDK fixpack for 6.1.0.9.
	
	Set the JAVA_HOME environment variable to point to the JDK* to use with the User Application. Or, manually specify the path during the User Application install to override JAVA_HOME.
	
	◆ At the Linux or Solaris command prompt, enter `echo $JAVA_HOME`. To create or change JAVA_HOME, create or edit `~/.profile` (in SUSE Linux):
	
	`# Java Home`
	
	`export JAVA_HOME=/usr/java/jdk1.5.0_10`
	
	`#JRE HOME`
	
	`export JRE_HOME=$JAVA_HOME/jre`
	
	◆ In Windows, see *Control Panel* > *System* > *Advanced* > *Environment Variables* > *System Variables*.

JBoss Application Server	If you are using JBoss*, download and install the JBoss 4.2.0 Application Server. (Start this server after you install the User Application. See Section 5.10, “Post-Install Tasks,” on page 178). **RAM.** The minimum recommended RAM for the JBoss application server when running the User Application is 512 MB. **Port.** Make a note of the port that your application server uses. (The default for the application server is 8080.) **SSL.** If you plan to use external password management, enable SSL in the JBoss servers on which you deploy the User Application and the `IDMPwdMgt.war` file. See your JBoss documentation for directions. Also, make sure the SSL port is open on your firewall. For more information on the `IDMPwdMgt.war file`, see Section 5.10.4, “Accessing the External Password WAR,” on page 179 and also see the *IDM 3.5.1 User Application: Administration Guide* (http://www.novell.com/documentation/idm35/index.html).
WebSphere Application Server	If you are using WebSphere*, download and install the WebSphere 6.1.0.9 Application Server. Apply the WAS JDK fixpack for 6.1.0.9.
Enable iChain Logout	Enable ICS Logout in the Identity Manager User Application by turning on the Cookie Forward option in Novell Access Manager™ or iChain®.

Environment Requirements	Description
Database	Install your database and database driver and create a database or a database instance. Note the host and port; you will use it in Section 5.6.7, “Specifying the Database Host and Port,” on page 121. Note the database name, username, and user password; you will use it in Section 5.6.8, “Specifying the Database Name and Privileged User,” on page 122. A datasource file must point to the database. This is handled differently according to your application server. For JBoss, the User Application install program creates an application server datasource file pointing to the database and names the file based on the User Application WAR file. For WebSphere, configure the datasource manually prior to the install. Databases must be enabled for UTF-8. Whether you install MySQL* through the IDM User Application utility or install MySQL on your own, read Section 5.2.3, “Configuring Your MySQL Database,” on page 106. **NOTE:** If you plan to migrate a database, start that database before you select the migration option in the installation program. If you are not migrating a database, the database does not need to be running during installation of the User Application. Just start it before you start the application server.
If installing IDM 3.5.1 User Application on Linux or Solaris	The default install location is `/opt/novell/idm`. You can select another default installation directory during the installation procedure. Make sure the directory exists and is writable by a non-`root` user.
If installing IDM 3.5.1 User Application on Windows	**Install directory.** The default install location is `C:\Novell\IDM`. Make sure this directory exists and is writable. You can select another default installation directory during the installation procedure.
Identity Manager 3.5.1	The Identity Manager 3.5.1 metadirectory server must be installed before you can create a User Application driver and install the User Application.
User Application driver	The User Application driver must already exist (but not be turned on) before you install the User Application.
Identity Vault access	The User Application requires a user with administrator access to the context where the User Application users will reside.
IDM User Application storage	The computer where you install the User Application must have at least 320 MB of storage available.

After you verify all prerequisites, follow the installation instructions in the following sections:

- Section 5.2.1, “Installing the JBoss Application Server and the MySQL Database,” on page 102
- Section 5.2.2, “Installing the JBoss Application Server as a Service,” on page 105
- Section 5.2.3, “Configuring Your MySQL Database,” on page 106

5.2.1 Installing the JBoss Application Server and the MySQL Database

Use the JbossMysql utility to install a JBoss Application Server and MySQL on your system.

This utility does not install the JBoss Application Server as a Windows service. To install the JBoss Application Server as a service on a Windows system, see Section 5.2.2, “Installing the JBoss Application Server as a Service,” on page 105.

1. Locate and execute `JbossMysql.bin` or `JbossMysql.exe`. You can find this utility bundled with the User Application installer in

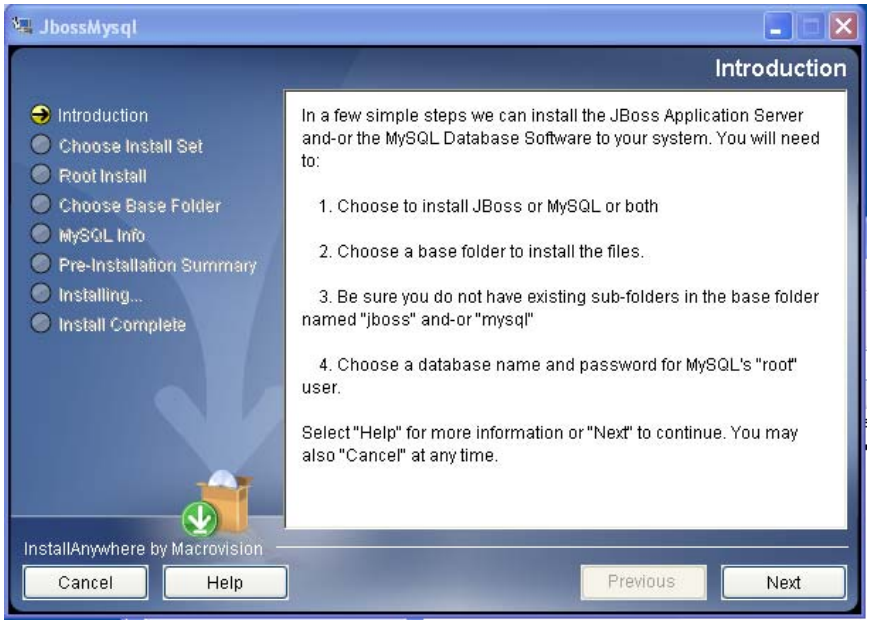
   `/linux/user_application` (for Linux)

   `/nt/user_application` (for Windows)

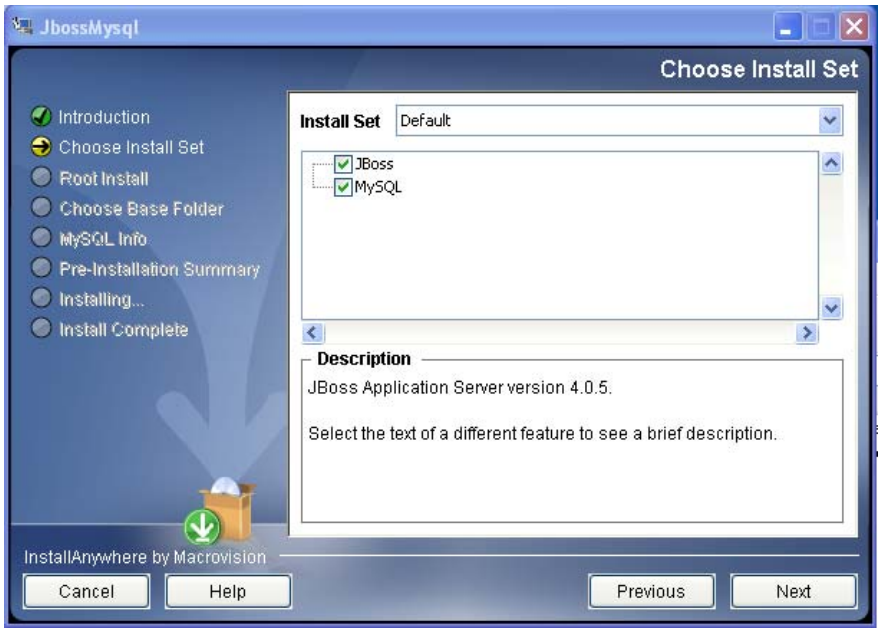
   The utility is not available for Solaris.

2. Select your locale.

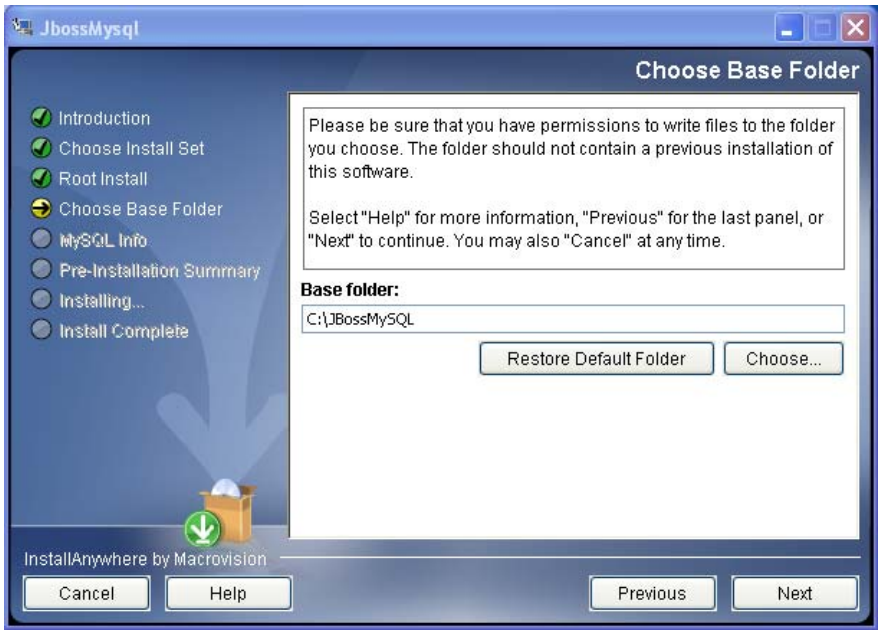
3. Read the introductory page, then click *Next*.



4. Select the products you want to install, then click *Next*.

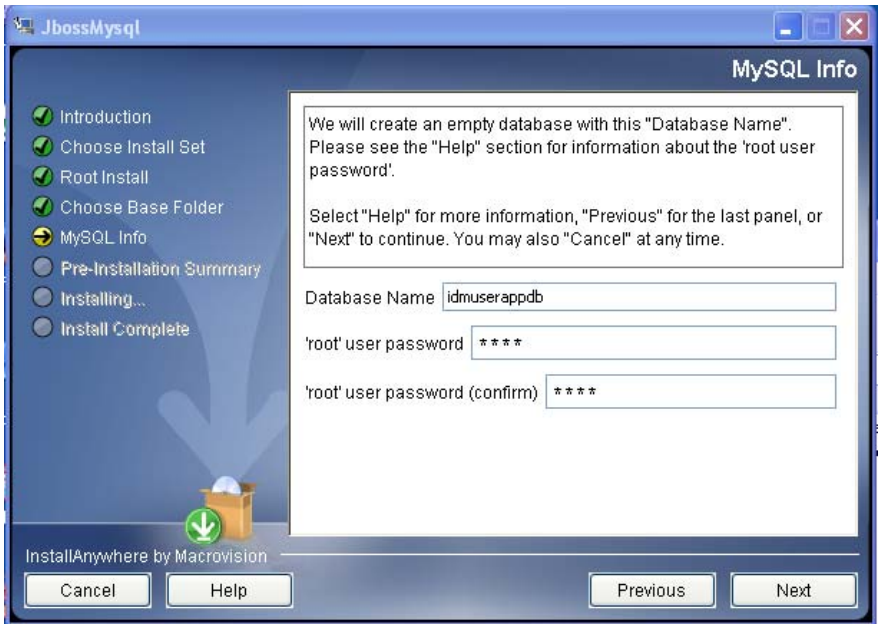


5 Click *Choose* to select the base folder in which to install the selected products, then click *Next*.



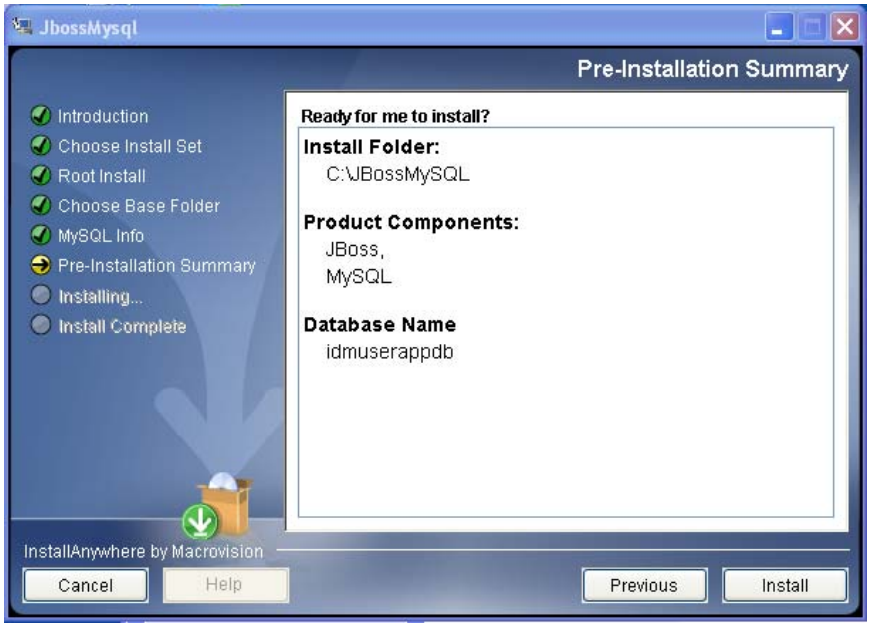
6 Specify a name for your database. The User Application installation requires this name.

7 Specify the database `root` user password.



8 Click *Next*.

9 Review your specifications in the Pre-Installation Summary, then click *Install*.



The utility displays a successful-completion message after it installs the products that you selected. If you installed the MySQL database, continue to Section 5.2.3, “Configuring Your MySQL Database,” on page 106.

5.2.2 Installing the JBoss Application Server as a Service

To run the JBoss Application Server as a service, use a Java Service Wrapper or a third-party utility. See directions from JBoss at http://wiki.jboss.org/wiki/Wiki.jsp?page=RunJBossAsAServiceOnWindows (http://wiki.jboss.org/wiki/Wiki.jsp?page=RunJBossAsAServiceOnWindows).

Using a Java Service Wrapper

You can use a Java Service Wrapper to install, start, and stop the JBoss Application Server as a Windows service or Linux or UNIX daemon process. Please check the Internet for available utilities and download sites.

One such wrapper is at http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html (http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html): manage it by JMX (see http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss (http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss)). Some sample configuration files include:

```
wrapper.conf :
wrapper.java.command=%JAVA_HOME%/bin/java
wrapper.java.mainclass=org.tanukisoftware.wrapper.WrapperSimpleApp
wrapper.java.classpath.1=%JBOSS_HOME%/server/default/lib/wrapper.jar
wrapper.java.classpath.2=%JAVA_HOME%/lib/tools.jar
  wrapper.java.classpath.3=./run.jar
wrapper.java.library.path.1=%JBOSS_HOME%/server/default/lib
  wrapper.java.additional.1=-server wrapper.app.parameter.1=org.jboss.Main
  wrapper.logfile=%JBOSS_HOME%/server/default/log/wrapper.log
  wrapper.ntservice.name=JBoss wrapper.ntservice.displayname=JBoss Server
```

WARNING: You must set your JBOSS_HOME environment variable correctly. The wrapper does not set this for itself.

```
java-service-wrapper-service.xml : <Xxml version="1.0" encoding="UTF-
8"?><!DOCTYPE server><server> <mbean
code="org.tanukisoftware.wrapper.jmx.WrapperManager"
name="JavaServiceWrapper:service=WrapperManager"/> <mbean
code="org.tanukisoftware.wrapper.jmx.WrapperManagerTesting"
name="JavaServiceWrapper:service=WrapperManagerTesting"/></server
```

Using a Third-Party Utility

For previous versions, you could use a third-party utility such as JavaService to install, start, and stop the JBoss Application Server as a Windows service.

WARNING: JBoss no longer recommends using JavaService. For details, see http://wiki.jboss.org/wiki/Wiki.jsp?page=JavaService (http://wiki.jboss.org/wiki/Wiki.jsp?page=JavaService).

5.2.3 Configuring Your MySQL Database

Your MySQL configuration settings must be set so that MySQL and Identity Manager 3.5.1 work together. If you install MySQL yourself, you must set the settings yourself. If you install MySQL using the JbossMysql utility, the utility sets the correct values for you, but you need to know the values to maintain for the following:

- "Character Set" on page 106
- "INNODB Storage Engine and Table Types" on page 106
- "Case Sensitivity" on page 106

Character Set

Specify UTF8 as the character set for the whole server or just for a database.

Specify UTF8 on a server-wide basis by including the following option in `my.cnf` (Linux or Solaris) or `my.ini` (Windows):

```
character-set-server=utf8
```

or,

Specify the character set for a database at database creation time, using the following command:

```
create database databasename character set utf8 collate utf8_bin;
```

If you set the character set for the database, you must also specify the character set in the JDBC URL in the `IDM-ds.xml` file, as in:

```
<connection-url>jdbc:mysql://localhost:3306/
databasename?useUnicode=true&amp;characterEncoding
```

INNODB Storage Engine and Table Types

The User Application uses the INNODB storage engine, which enables you to choose INNODB table types for MySQL. If you create a MySQL table without specifying its table type, the table receives the MyISAM table type by default. If you choose to install MySQL from the Identity Manager installation procedure, the MySQL issued with that procedure comes with the INNODB table type specified.

To ensure that your MySQL server is using INNODB, verify that `my.cnf` (Linux or Solaris) or `my.ini` (Windows) contains the following option:

```
default-table-type=innodb
```

It should not contain the `skip-innodb` option.

Case Sensitivity

Ensure that case sensitivity is consistent across servers or platforms if you plan to back up and restore data across servers or platforms. To ensure consistency, specify the same value (either 0 or 1) for `lower_case_table_names` in all your `my.cnf` (Linux or Solaris) or `my.ini` (Windows) files, instead of accepting the default (Windows defaults to 0 and Linux defaults to 1.) Specify this value before you create the database to hold the Identity Manager tables. For example, you would specify

```
lower_case_table_names=1
```

in the `my.cnf` and `my.ini` files for all platforms on which you plan to back up and restore a database.

5.3 Installation and Configuration Steps

This section outlines the installation and configuration steps:

1. Create the User Application driver and leave it turned off.

   This step creates new objects in the Identity Vault. Some will have default data values. For more information see Section 5.4, "Creating the User Application Driver," on page 107.

2. Run the User Application installation program.

   For more information, see Section 5.6, "Installing the User Application on a JBoss Application Server from the Install GUI," on page 114 or Section 5.7, "Installing the User Application on a WebSphere Application Server," on page 143.

3. WebSphere users must manually deploy the WAR file.

IMPORTANT: The Identity Manager User Application installation requires that the User Application driver already exist prior to installing the application. However, start the driver *after* you install the Identity Manager User Application, or the User Application driver might return errors.

5.4 Creating the User Application Driver

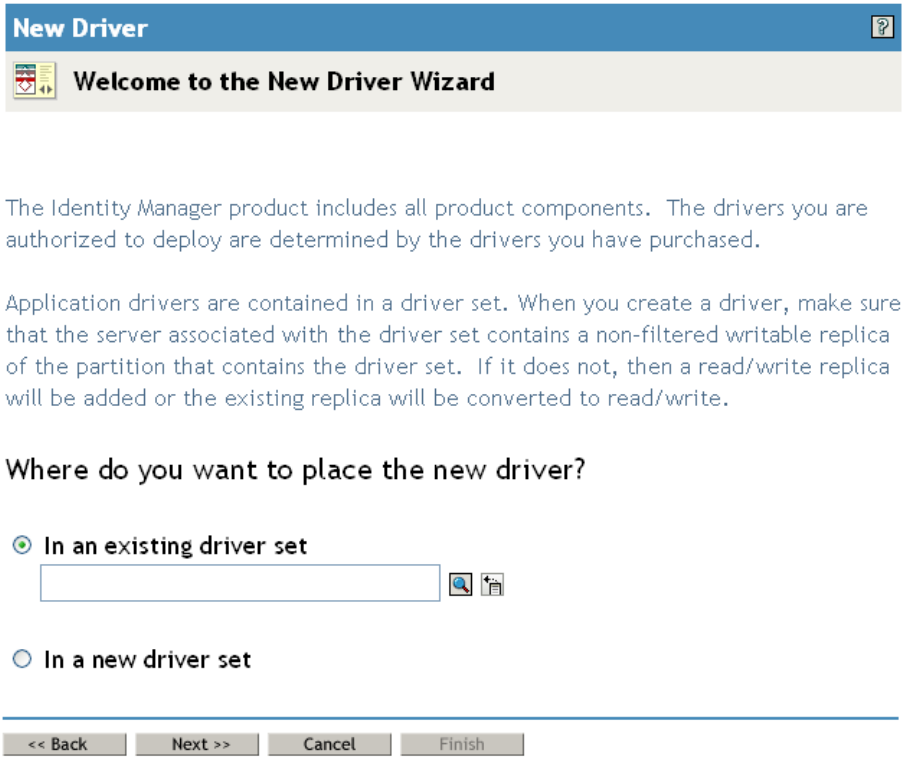
You must create a separate User Application driver for each User Application, except for User Applications on a cluster. User applications that are part of the same cluster must share a single User Application driver. For information on running the User Application in a cluster, see the *Identity Manager 3.5.1 User Application Administration Guide* (http://www.novell.com/documentation/idm35/index.html).

The User Application stores application-specific data in the driver to control and configure the application environment. This includes the application server cluster information and the workflow engine configuration.

IMPORTANT: Configuring a set of non-cluster User Applications to share a single driver creates ambiguity and misconfiguration for one or more of the components running inside the User Application. The source of the resulting problems is difficult to detect.

To create a 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* > *Identity Manager Utilities* and select *New Driver* to launch the Create Driver Wizard.

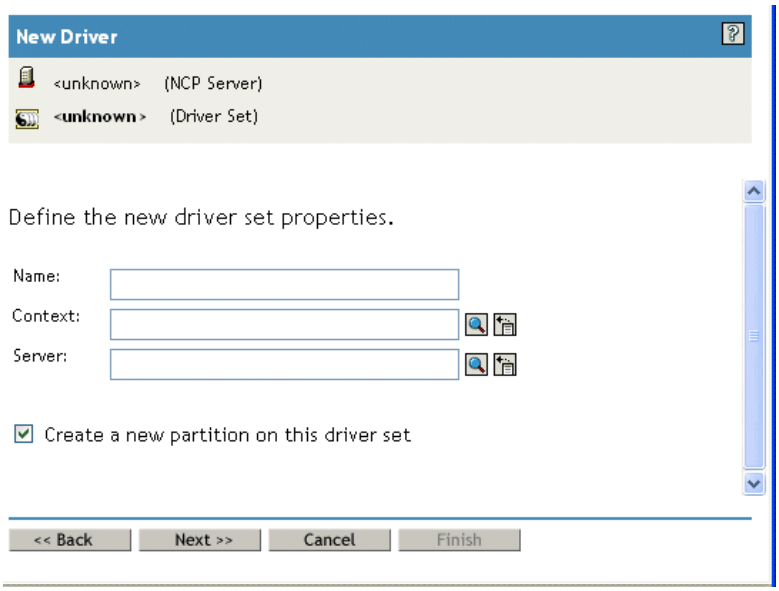


3 To create the driver in an existing driver set, select *In an existing driver set*, click the object selector icon, select a driver set object, click *Next,* and continue with Step 4.

or

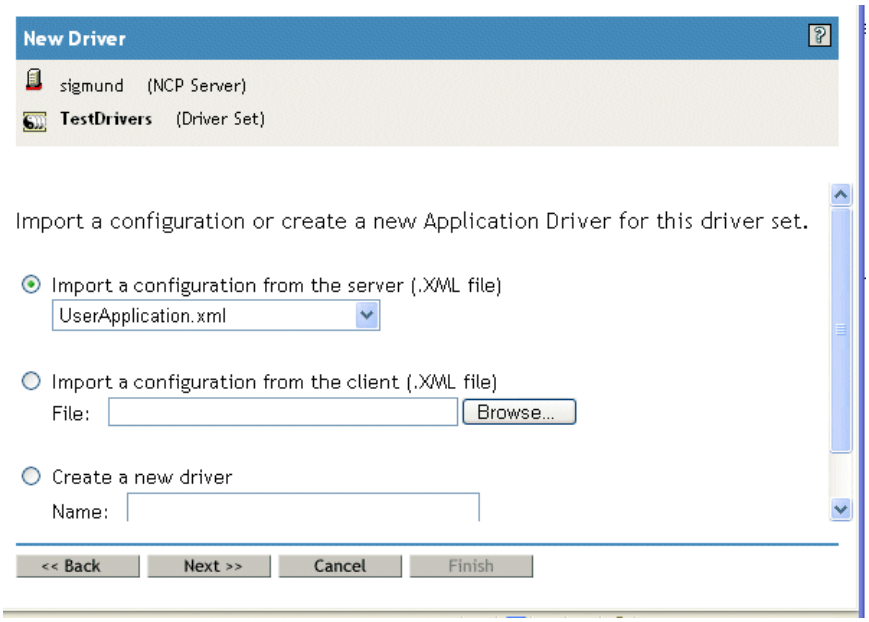
If you need to create a new driver set (for example, if you are placing the User Application driver on a different server from your other drivers), select *In a new driver set*, click *Next*, then define the new driver set properties.

3a Specify a name, a context, and a server for the new driver set.



3b Click *Next*.

4 Click *Import a driver configuration from the server (.XML file)*.



5 Select *UserApplication.xml* from the drop-down list.

This is the configuration file for your new driver.

6 Click *Next*.

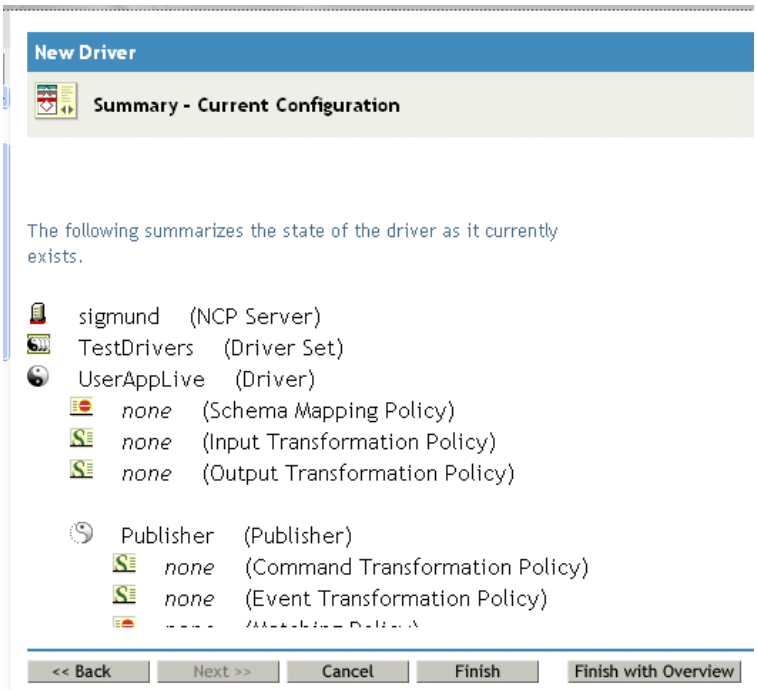
If *UserApplication.xml* is not in this drop-down list, you probably did not run the Web-Based Administration Server portion of the Identity Manager 3.5.1 install.

7 You are prompted for parameters for your driver. (Scroll to view all.) Make a note of the parameters; you need these when you install the User Application.

Field	Description
Driver Name	The name of the driver you are creating.
Authentication ID	The distinguished name of the User Application Administrator. This is a User Application Administrator to whom you are giving rights to administer the User Application portal. Use the eDirectory™ format, for example admin.orgunit.novell, or browse to find the user. This is a required field.
Password	Password of the User Application Administrator specified in the Authentication ID.
Application Context	The User Application context. This is the context portion of the URL for the User Application WAR file. The default is:IDM.
Host	The hostname or IP address of the application server where the Identity Manager User Application is deployed. If running in a cluster, type the dispatcher's hostname or IP address.
Port	The port for the host you listed above.
Allow Override Initiator: (values are No/Yes)	Select Yes to allow the Provisioning Administrator to start workflows in the name of the person for whom the Provisioning Administrator is designated as proxy.

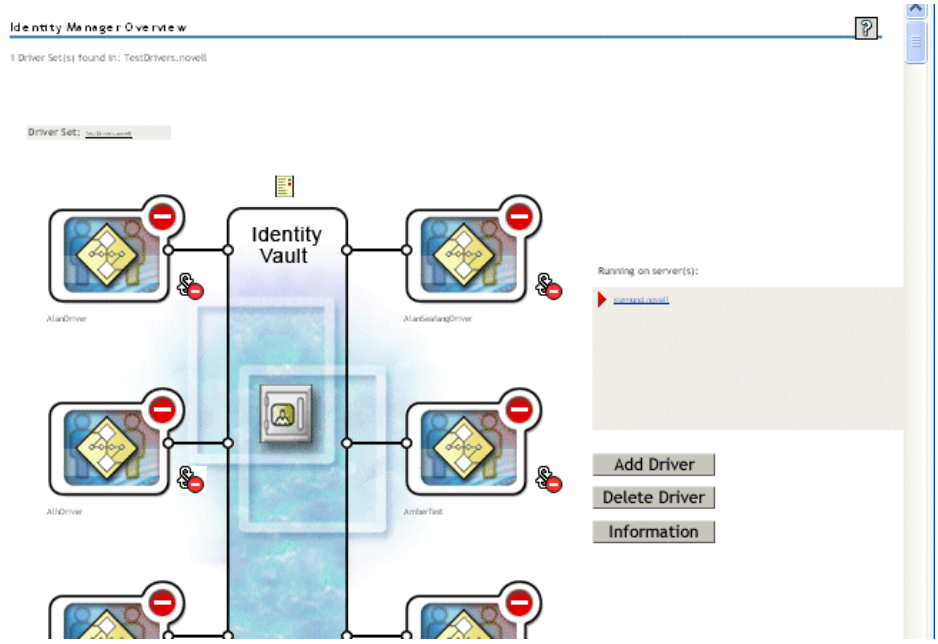
8. Click *Next*.
9. Click *Define Security Equivalences* to open the Security Equals window. Browse to and select an administrator or other Supervisor object, then click *Add*.

   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*.
11. Click *Add*, select users you want to exclude for driver actions (such as administrative roles). Click *OK* twice, then click *Next*.
12. Click *OK* to close the Security Equals window and display the summary page.



13 If the information is correct, click *Finish* or *Finish with Overview.*

IMPORTANT: The driver is off by default. Leave the driver off until the User Application has been installed.



5.5 About the Installation Program

The User Application installation program does the following:

- Designates an existing version of an application server to use.
- Designates an existing version of a database to use, for example MySQL, Oracle*, or Microsoft SQL Server. The database stores User Application data and User Application configuration information.
- Configures the JDK's certificates file so that the User Application (running on the application server) can communicate with the Identity Vault and the User Application driver securely.
- Configures and deploys the Java Web Application Archive (WAR) file for the Novell Identity Manager User Application to the JBoss Application Server.
- Enables Novell Audit logging if you select to do so.
- Enables you to import an existing master key to restore a specific User Application installation and to support clusters.

You can launch the installation program in one of three modes:

- Graphical user interface. See Section 5.6, "Installing the User Application on a JBoss Application Server from the Install GUI," on page 114)
- Console (command line) interface. See Section 5.8, "Installing the User Application from a Console Interface," on page 171)
- Silent install. See Section 5.9, "Installing the User Application with a Single Command," on page 172.

5.5.1 Installation Scripts and Executables

Obtain the Identity Manager 3.5.1 installation files by one of the following methods:

- Download the correct User Application `.iso` image or `.zip` file for your system: `Identity_Manager_3_5_1_User_Application.iso` or `Identity_Manager_3_5_1_User_Application_Provisioning.iso`. Downloads are available from Novell Downloads (http://download.novell.com/index.jsp). See Activating Novell Identity Manager Products (http://www.novell.com/documentation/idm35/install/data/afbx4oc.html) for more information.
- Download the product DVD, `Identity_Manager_3_5_1_DVD.iso`, from Novell, Inc.

Table 5-2 lists the files and scripts you need to install the Identity Manager 3.5.1 User Application.

Table 5-2 *Files and Scripts Required for Installing the Identity Manager 3.5.1 User Application*

File	Description
User Application WAR	Choose one: **IDM.war.** Includes the Identity Manager 3.5.1 User Application with Identity Self-Service features. **IDMProv.war.** Includes the Identity Manager 3.5.1 User Application with Identity Self-Service features and the Provisioning Module.

The WAR files for your system, as well as the `IdmUserApp.jar` and `silent.properties` files, are initially available in the following delivery CD directory appropriate for your system:

`/linux/user_application` (for Linux)
`/nt/user_application` (for Windows)
`/solaris/user_application` (for Solaris)

5.5.2 Values Required at Installation

Table 5-3 is a worksheet for noting the installation parameter values you plan to use at installation on JBoss. User Application configuration parameters can also be set at installation; see Section 5.6.14, “Configuring the User Application,” on page 129.

Table 5-3 *Installation Parameters Worksheet for JBoss*

Parameter	Sample Value	Your Value
Install folder	C:\IDM\IDMinstallIocation	
Database platform	MySQL	
Database host	localhost	
Database port	3306	
Database name or sid	IDM	
Database user	`root`	
Database user password		
Java root folder	C:\Java\jdk1.5.0_10\	
(JBoss) Base folder	C:\jboss	
JBoss host	localhost	
JBoss port	8080	
Workflow Engine ID (For cluster installs. Must be unique for each cluster member.)		
Application name (URL context)	IDM	

Parameter	Sample Value	Your Value
Novell Audit Server	[name or IP address]	
Encrypted master key. See Section 5.6.13, “Specifying a Master Key,” on page 128.	_+FEJEefMAglH0A= =:3VRmp04lub21Y3GpdaXCY)LG qS1nBaL/	

5.6 Installing the User Application on a JBoss Application Server from the Install GUI

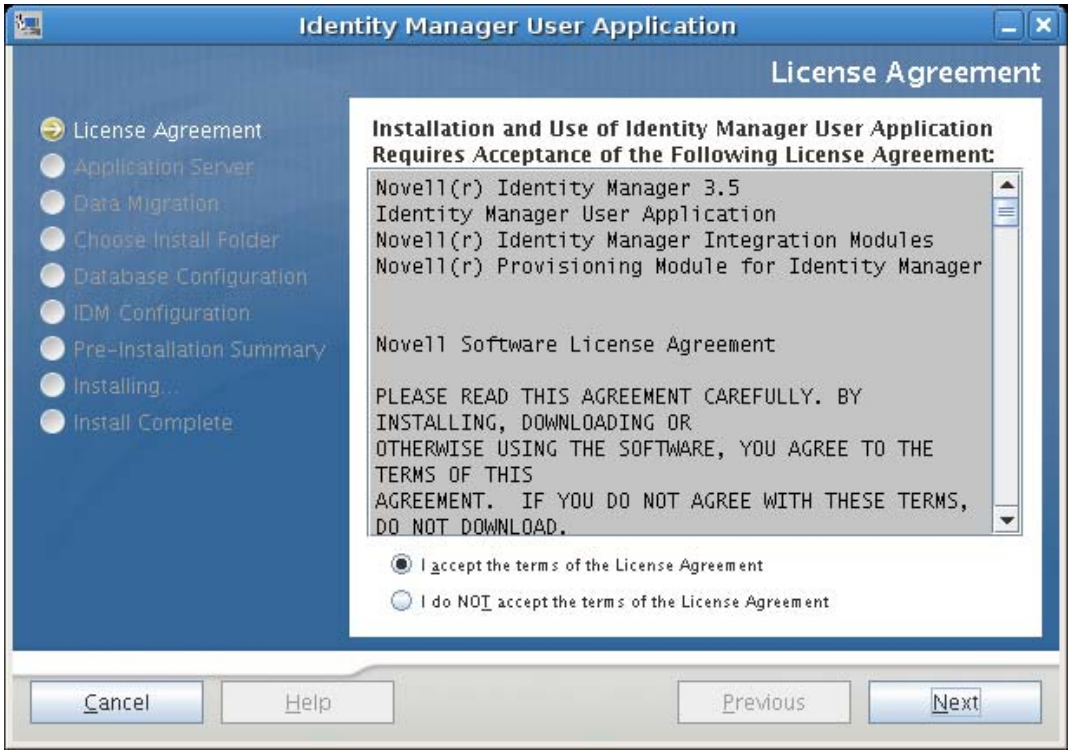
This section describes how to install the Identity Manager User Application on a JBoss Application Server by using the graphical user interface version of the installer.

5.6.1 Launching the Installer GUI

1. Navigate to the directory containing your installation files, described in Table 5-2 on page 113.
2. Launch the installer for your platform from the command line:

   ```
   java -jar IdmUserApp.jar
   ```
3. Select a language from the drop-down menu, then click *OK*.

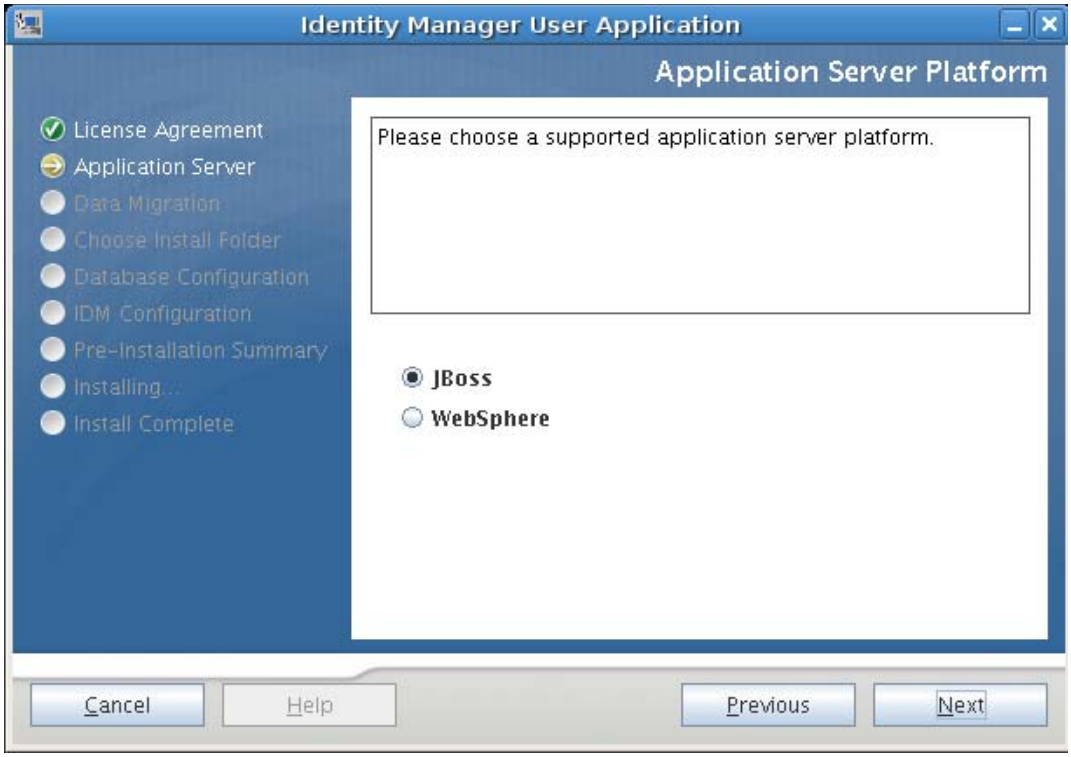
4 Read the license agreement, click *I accept the terms of the License Agreement,* then click *Next*.



5 Read the Introduction page of the install wizard, then click *Next*.

5.6.2 Choosing an Application Server Platform

1 Choose the JBoss application server platform and click *Next*.



5.6.3 Migrating Your Database

If you do not want to migrate a database, click *Next* and continue to Section 5.6.4, “Specifying the Location of the WAR,” on page 118.

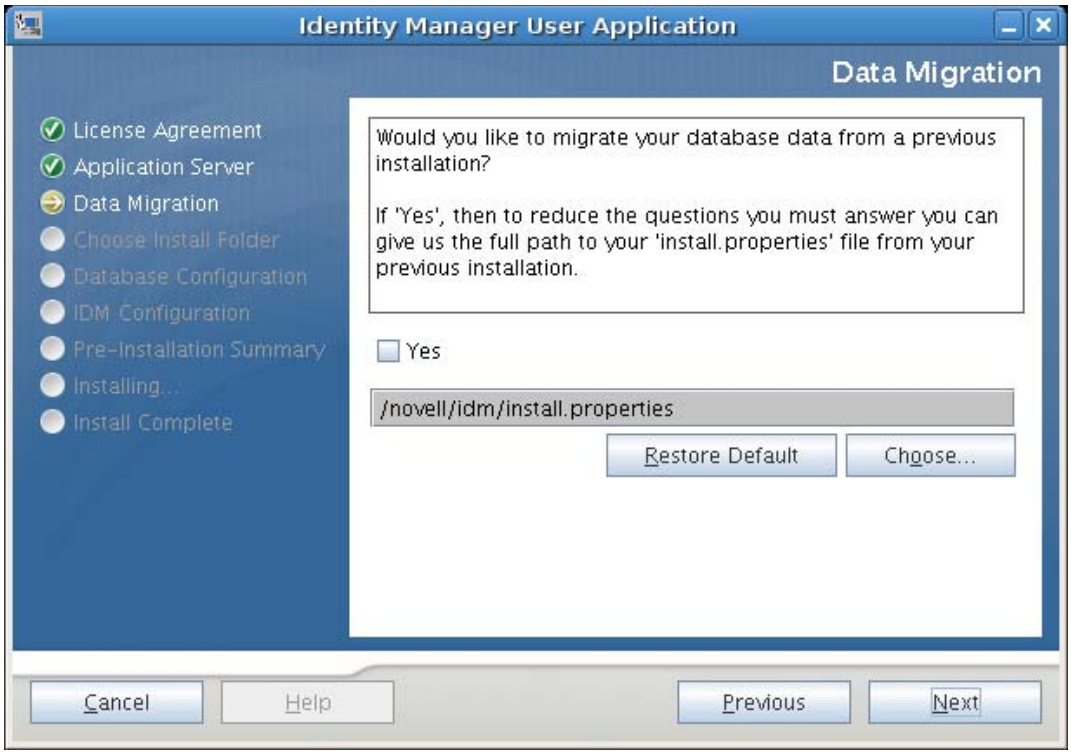
If you want to use an existing database from your Version 3.0 or Version 3.01 User Application, you must migrate the database.

1 Verify that you started the database that you want to migrate.

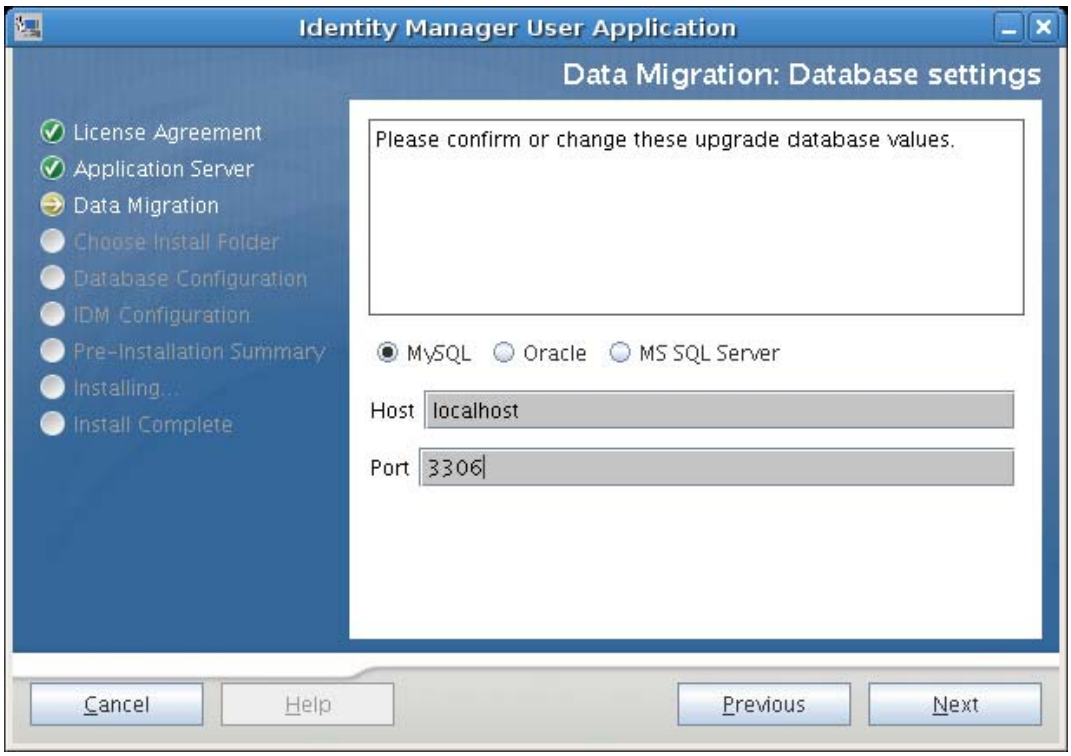
2 Click *Yes* in the Data Migration page of the installation program.

3 Click *Choose* to navigate to the `install.properties` file in the Identity Manager 3.0 or 3.01 User Application installation directory.

Specifying the location of the `install.properties` file from your previous installation reduces the number of items that you have to specify in the following pages.



4 You are asked to confirm the database type, hostname, and port. Do so, and click *Next*.



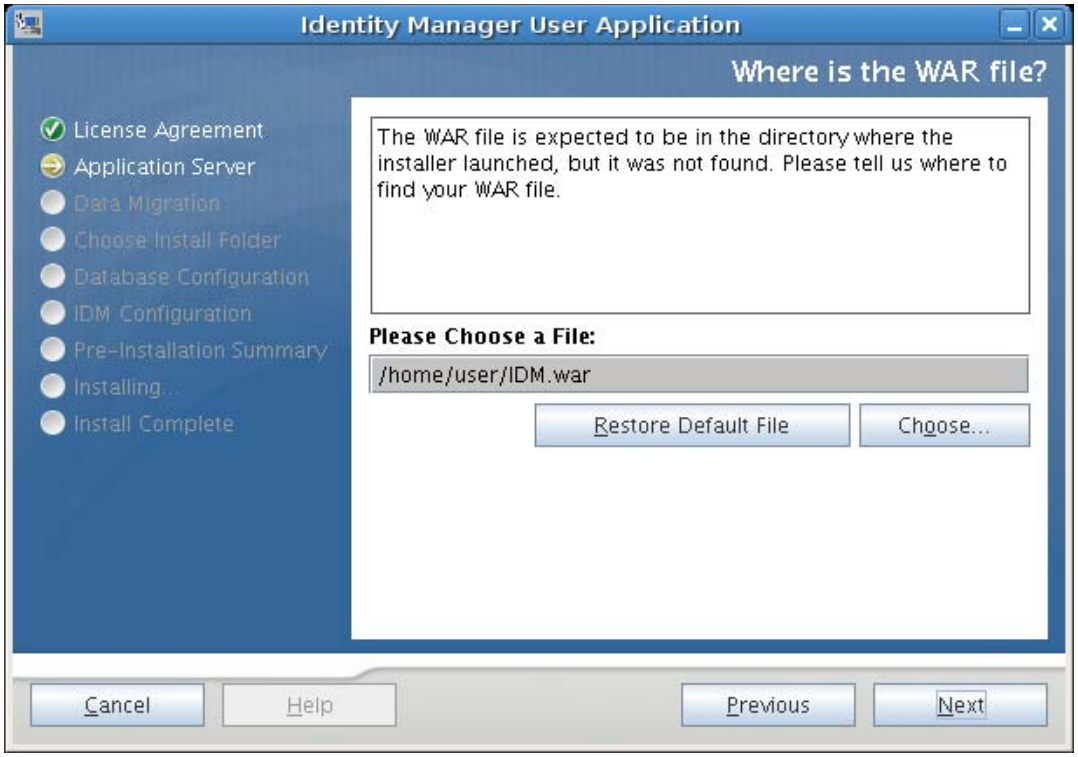
5 Click *Next* and continue to Section 5.6.4, “Specifying the Location of the WAR,” on page 118 or Section 5.6.5, “Choosing an Install Folder,” on page 118.

The User Application installer upgrades your User Application and migrates data from the Version 3.0 or 3.0.1 database to the database used for Version 3.5.1. For information on and additional steps for migrating your database, see the *Identity Manager User Application: Migration Guide* (http://www.novell.com/documentation/idm35/index.html).

5.6.4 Specifying the Location of the WAR

If the Identity Manager User Application WAR file is in a different directory from the installer, the installer prompts for the path to the WAR.

1. If the WAR is in the default location, click *Restore Default Folder*. Or, to specify the location of the WAR file, click *Choose* and select a location.
2. Click *Next*, then continue with Section 5.6.5, "Choosing an Install Folder," on page 118.



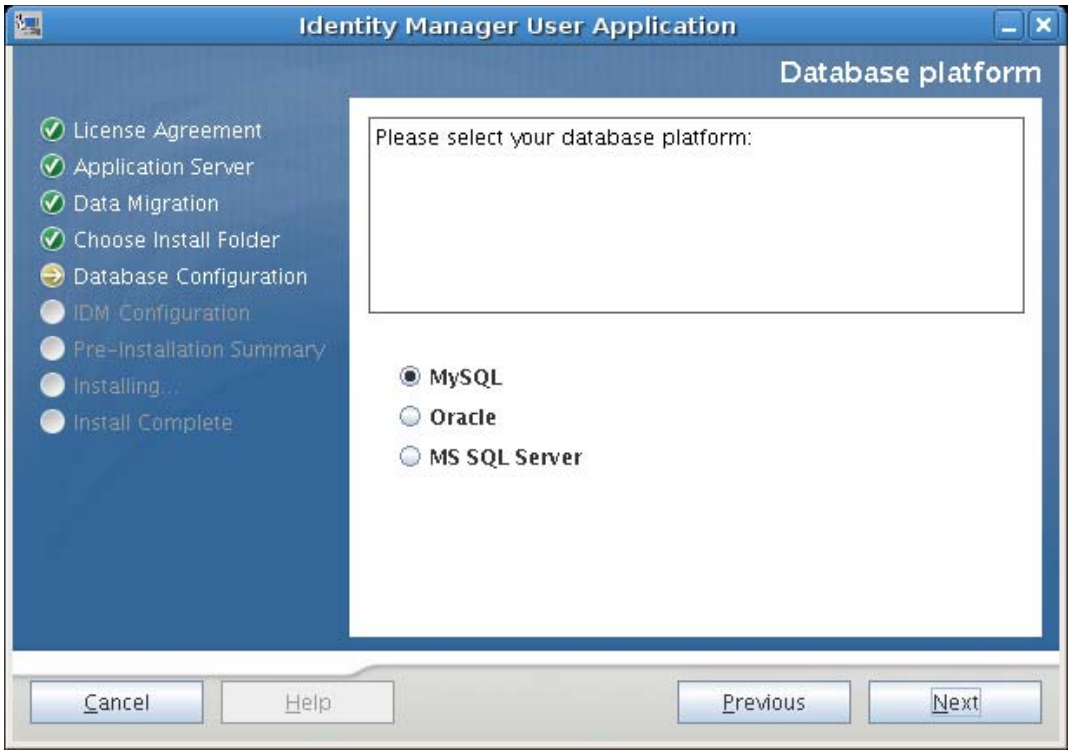
5.6.5 Choosing an Install Folder

1. On the Choose Install Folder page, select where to install the User Application. If you need to remember and use the default location, click *Restore Default Folder*, or if you want to choose another location for the installation files, click *Choose* and browse to a location.

2 Click *Next*, then continue with Section 5.6.6, “Choosing a Database Platform,” on page 119.

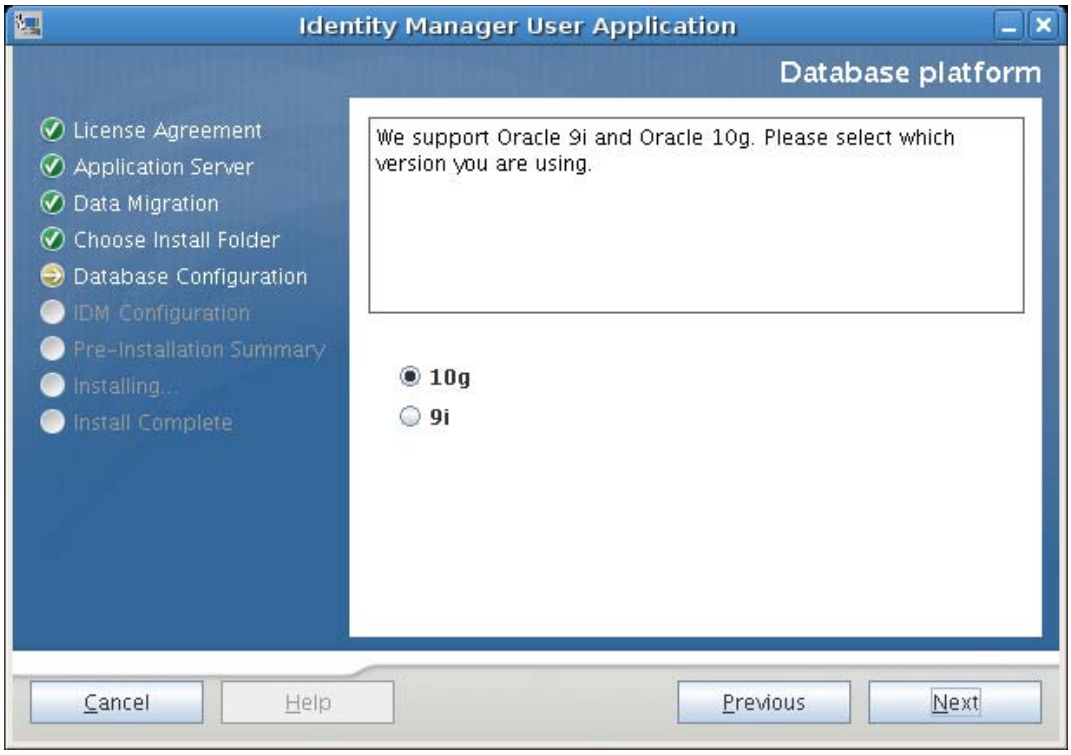
5.6.6 Choosing a Database Platform

1 Select the database platform to use.



2 If you are using an Oracle database, continue with Step 3. Otherwise, skip to Step 4.

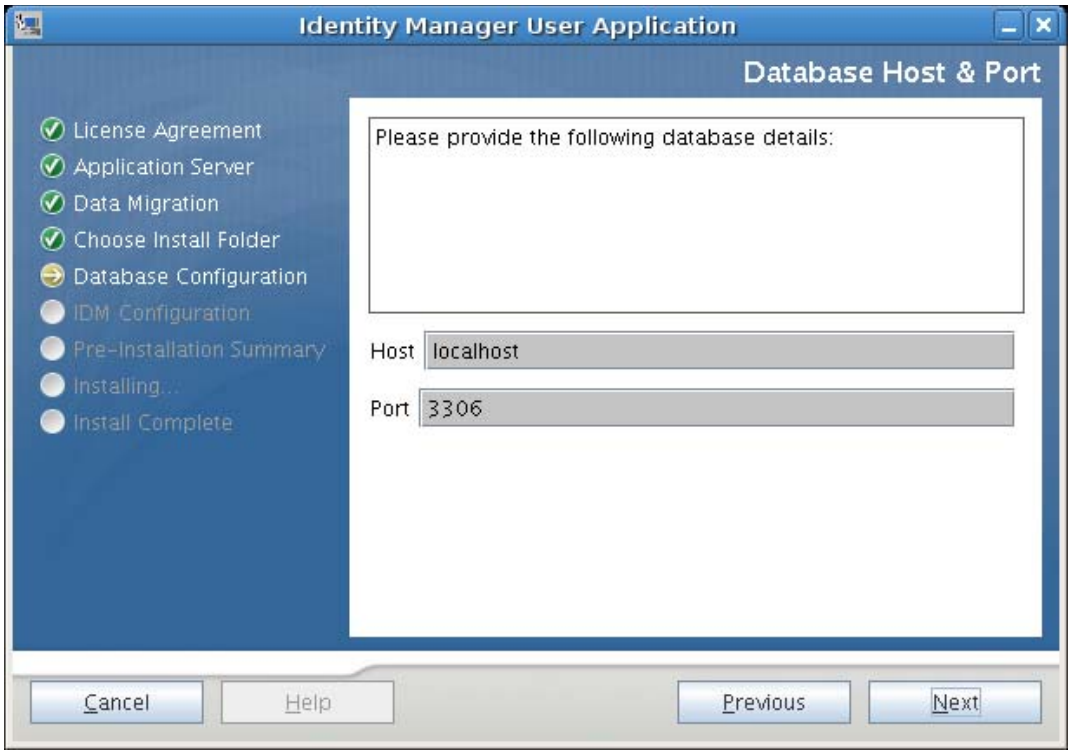
3 If you are using an Oracle database, the installer asks you which version you are using. Choose your version.



4 Click *Next,* then continue with Section 5.6.7, “Specifying the Database Host and Port,” on page 121.

5.6.7 Specifying the Database Host and Port

1 Fill in the following fields:

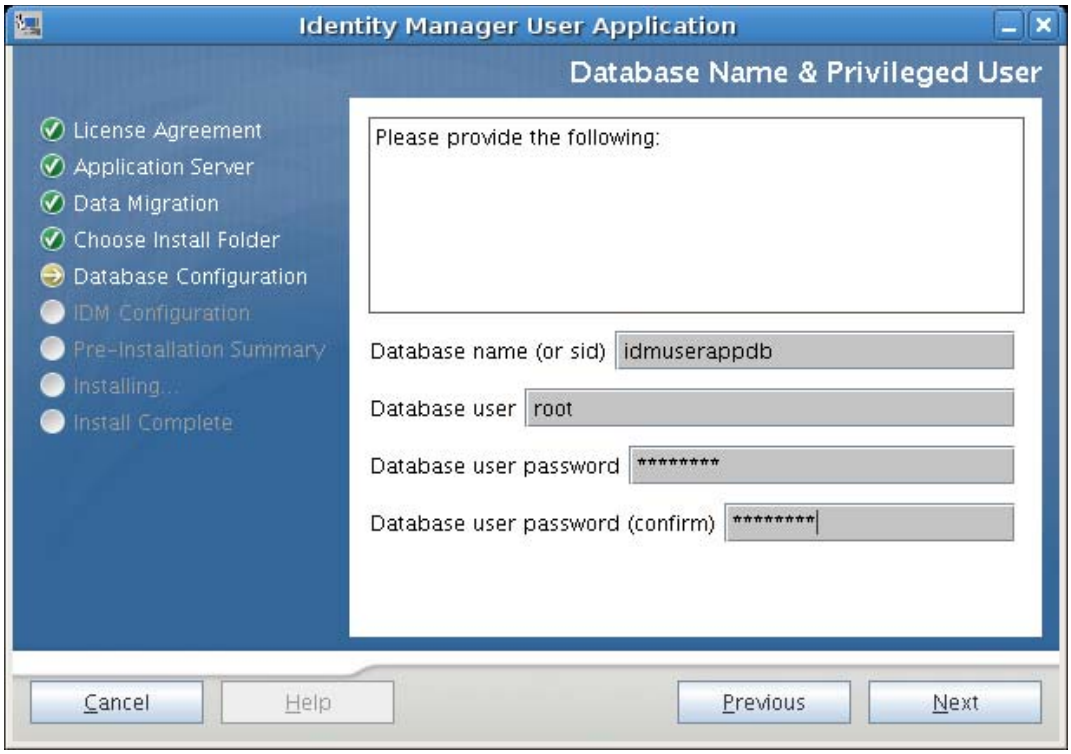


Field	Description
Host	Specify the database server's hostname or IP address. For a cluster, specify the same hostname or IP address for each member of the cluster.
Port	Specify the database's listener port number. For a cluster, specify the same port for each member of the cluster.

2 Click *Next*, then continue with Section 5.6.8, "Specifying the Database Name and Privileged User," on page 122.

5.6.8 Specifying the Database Name and Privileged User

1 Fill in the following fields:

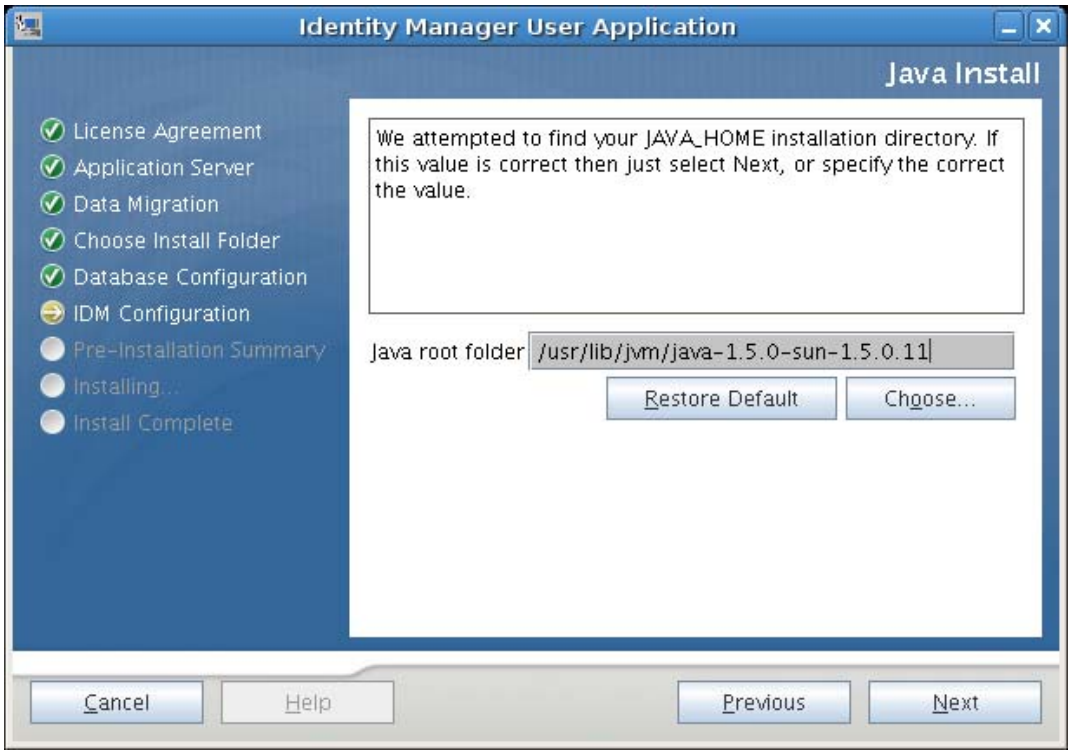


Field	Description
Database name (or sid)	For MySQL or MS SQL Server, provide the name of your preconfigured database. For Oracle, provide the Oracle System Identifier (SID) that you previously created. For a cluster, specify the same database name or SID for each member of the cluster.
Database user	Specify the database user. For a cluster, specify the same database user for each member of the cluster. **NOTE:** Use the root account created for the MySQL server account. Creation of a regular user account is not part of this installation.
Database password/Confirm password	Specify the database password. For a cluster, specify the same database password for each member of the cluster.

2 Click *Next,* then continue with Section 5.6.9, “Specifying the Java Root Directory,” on page 124.

5.6.9 Specifying the Java Root Directory

1 Click *Choose* to browse for your Java root folder. To use the default location, click *Restore Default*.



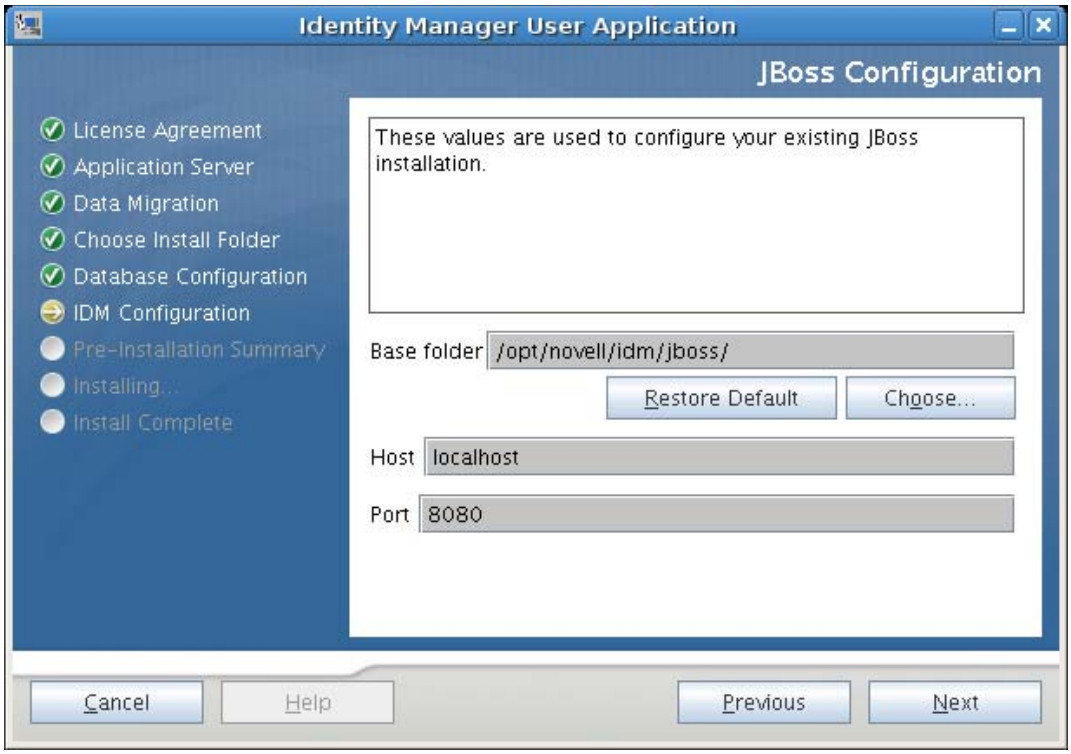
2 Click *Next*, then continue with Section 5.6.10, “Specifying the JBoss Application Server Settings,” on page 124.

5.6.10 Specifying the JBoss Application Server Settings

On this page, tell the User Application where to find the JBoss Application Server.

This installation procedure does not install the JBoss Application Server: for directions on installing the JBoss Application Server, see Section 5.2.1, “Installing the JBoss Application Server and the MySQL Database,” on page 102.

1 Supply the base folder, host, and port:

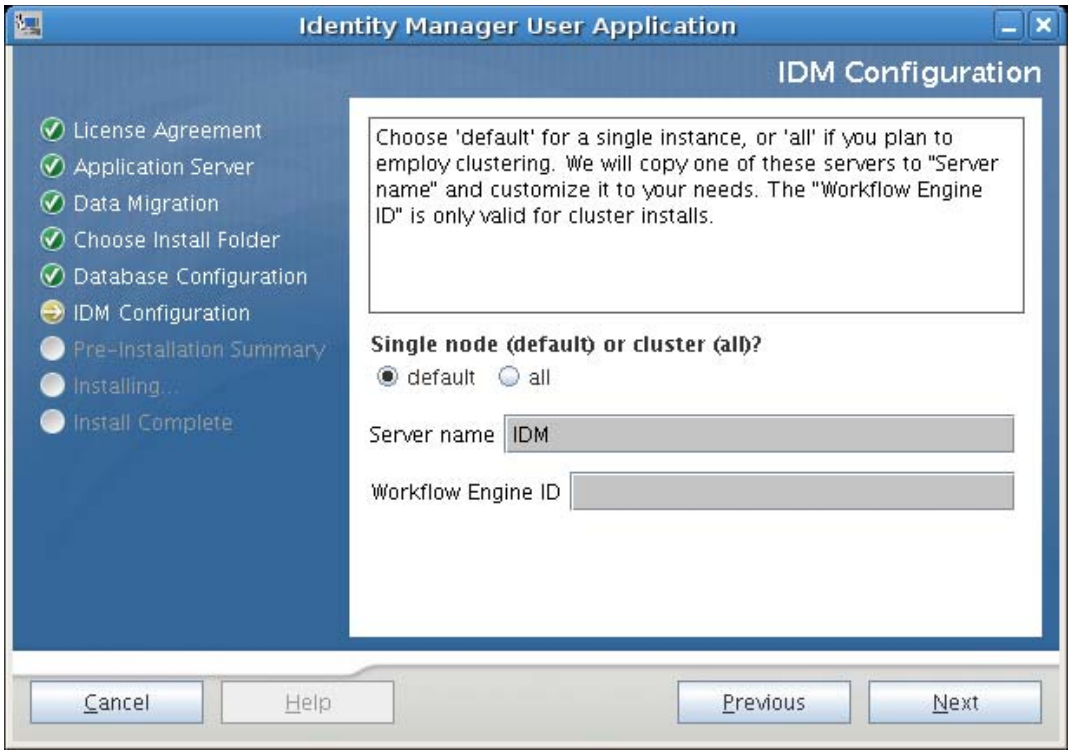


Field	Description
Base folder	Specify the location of the application server.
Host	Specify the application server's hostname or IP address
Port	Specify the application server's listener port number. The JBoss default port is 8080.
	NOTE: You can change this port value by using the JBoss sources.

2 Click *Next*, then continue with Section 5.6.11, "Choosing the Application Server Configuration Type," on page 125.

5.6.11 Choosing the Application Server Configuration Type

1 Fill in the following fields:



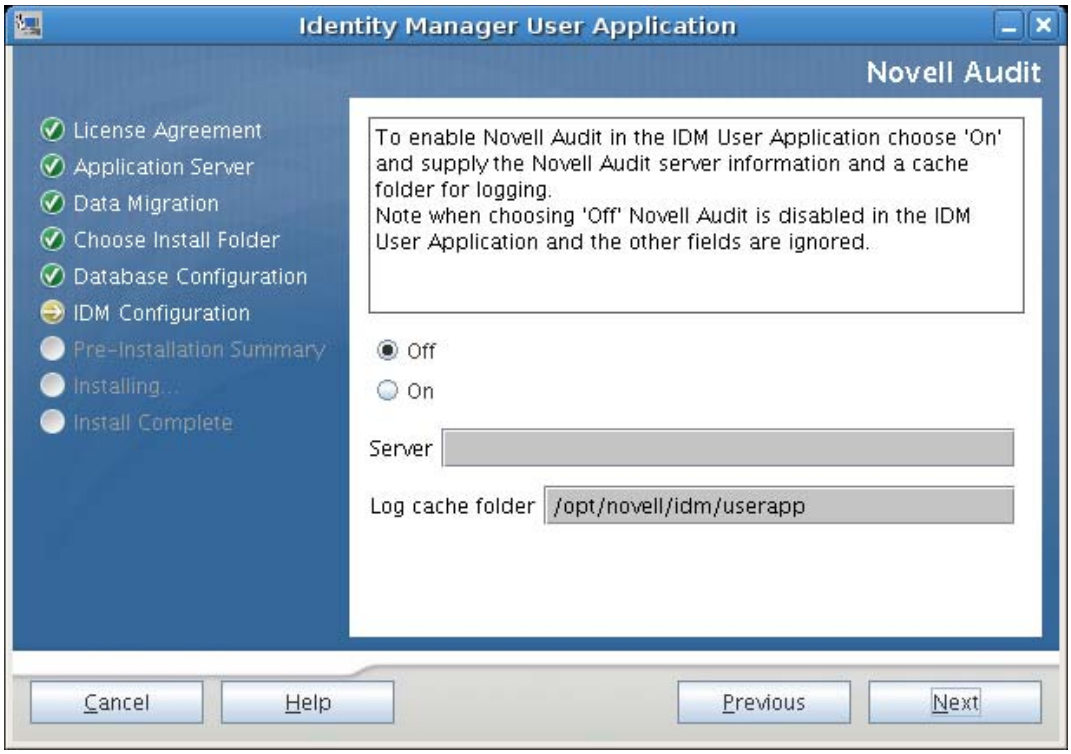
Option	Description
Single (default) or *clustering* (all)	Select the type of application server configuration: ◆ Select *all* if this installation is part of a cluster ◆ Select *default* if this installation is on a single node that is not part of a cluster
Server name	Specify the server name. The server name is the name of the application server configuration, the name of the application WAR file, and the name of the URL context. The installation script creates a server configuration and by default names the configuration based on *Application name*. Note the application name and include it in the URL when you start the Identity Manager User Application from a browser.
Workflow Engine ID	Each server in a cluster must have a unique Workflow Engine ID. Workflow Engine IDs are described in the *Identity Manager User Application: Administration Guide* in Section 3.5.4, Configuring Workflows for Clustering.

2 Click *Next*, then continue with Section 5.6.12, “Enabling Novell Audit Logging,” on page 127.

5.6.12 Enabling Novell Audit Logging

(Optional) To enable Novell Audit logging for the User Application:

1 Fill in the following fields:



Option	Description
On	Enables Novell Audit Logging for the User Application. For more information on setting up Novell Audit logging, see the *Identity Manager User Application: Administration Guide*.
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 *Identity Manager User Application: Administration Guide.*
Server	If you turn Novell Audit logging on, specify the hostname or IP address for the Novell Audit server. If you turn logging off, this value is ignored.

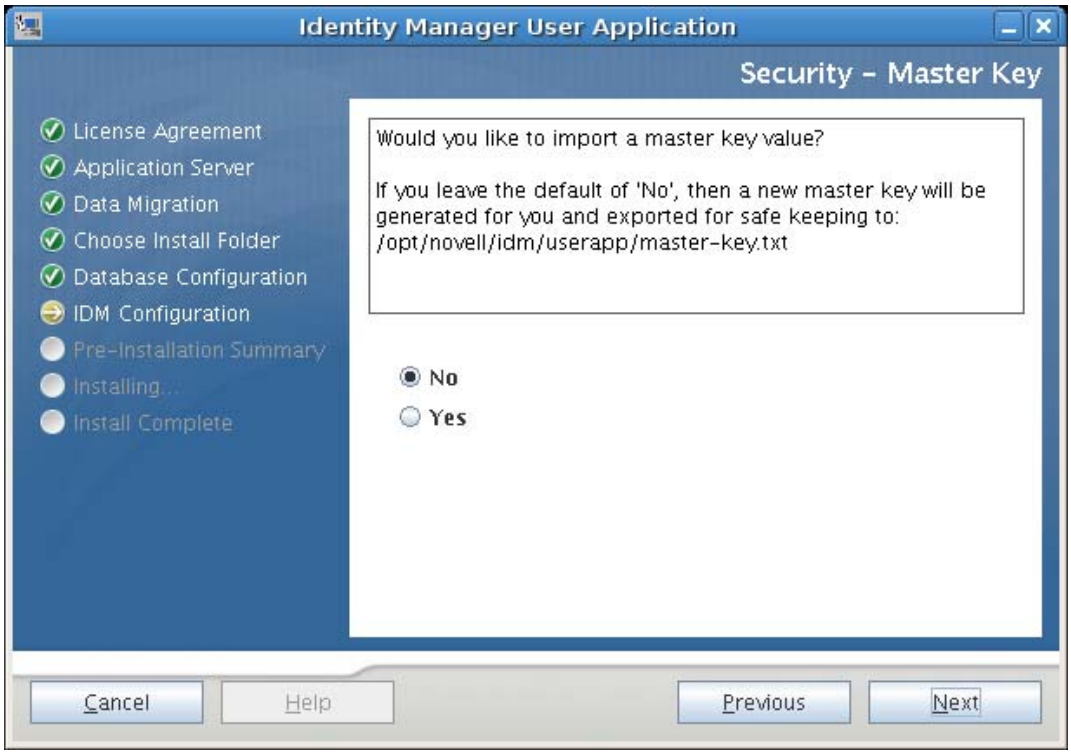
2 Click *Next*, then continue with Section 5.6.14, “Configuring the User Application,” on page 129.

5.6.13 Specifying a Master Key

Specify whether to import an existing master key or create a new one. Examples of reasons to import an existing master key include:

- You are moving your installation from a staging system to a production system and want to keep access to the database you used with the staging system.
- You installed the User Application on the first member of a JBoss cluster and are now installing on subsequent members of the cluster (they require the same master key).
- Because of a failed disk, you need to restore your User Application. You must reinstall the User Application and specify the same encrypted master key that the previous installation used. This gives you access to the previously stored encrypted data.

1 Click *Yes* to import an existing master key, or click *No* to create a new one.



2 Click *Next*.

The installation procedure writes the encrypted master key to the `master-key.txt` file in the installation directory.

If you chose *No*, skip to Section 5.6.14, “Configuring the User Application,” on page 129. After you finish the installation, you must manually record the master key as described in Section 5.10.1, “Recording the Master Key,” on page 178.

If you chose *Yes*, continue with Step 3.

3 If you choose to import an existing encrypted master key, cut and paste the key into the install procedure window.

4 Click *Next*.

5.6.14 Configuring the User Application

The User Application install enables you to set User Application configuration parameters. Most of these parameters are also editable with `configupdate.sh` or `configupdate.bat` after installation; exceptions are noted in the parameter descriptions.

For a cluster, specify identical User Application configuration parameters for each member of the cluster.

1 Set the basic User Application configuration parameters described in Table 5-4, then continue with Step 2.

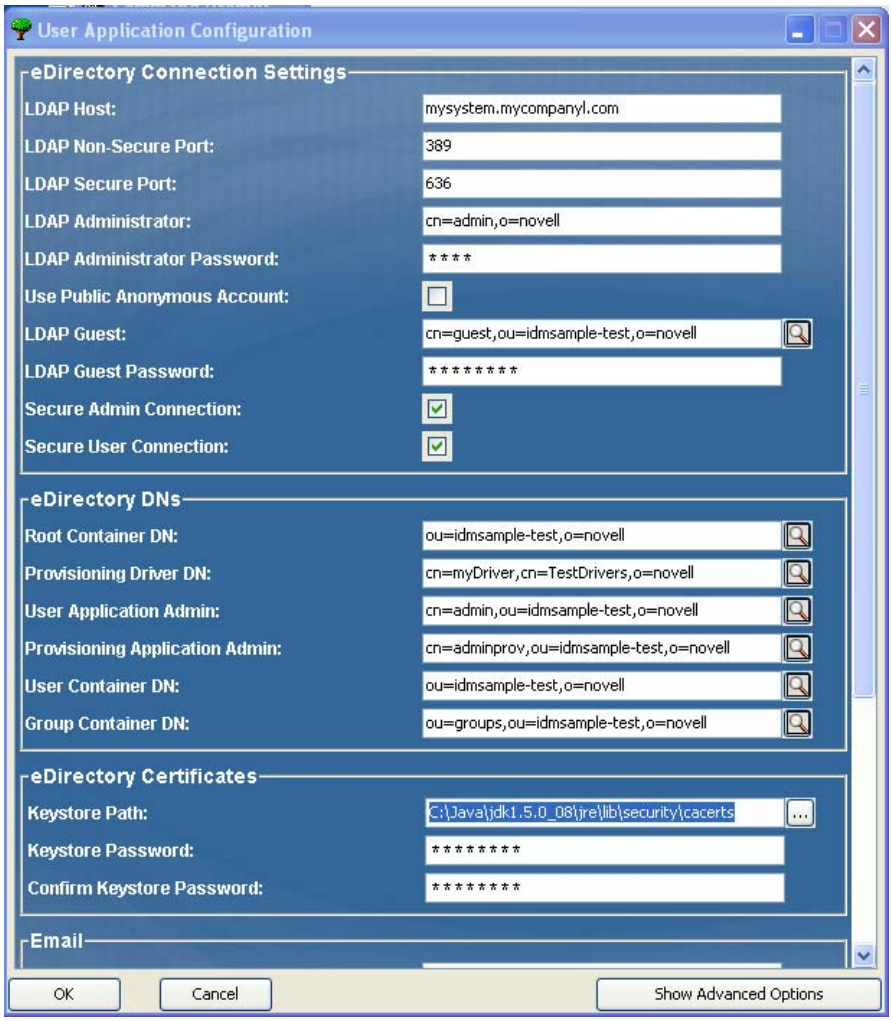

User Application Configuration
eDirectory Connection Settings
LDAP Host:
mysystem.mycompanyl.com
LDAP Non-Secure Port:
389
LDAP Secure Port:
636
LDAP Administrator:
cn=admin,o=novell
LDAP Administrator Password:
****
Use Public Anonymous Account:
LDAP Guest:
cn=guest,ou=idmsample-test,o=novell
LDAP Guest Password:
****
Secure Admin Connection:
Secure User Connection:
eDirectory DNs
Root Container DN:
ou=idmsample-test,o=novell
Provisioning Driver DN:
cn=myDriver,cn=TestDrivers,o=novell
User Application Admin:
cn=admin,ou=idmsample-test,o=novell
Provisioning Application Admin:
cn=adminprov,ou=idmsample-test,o=novell
User Container DN:
ou=idmsample-test,o=novell
Group Container DN:
ou=groups,ou=idmsample-test,o=novell
eDirectory Certificates
Keystore Path:
C:\Java\jdk1.5.0_08\jre\lib\security\cacerts
Keystore Password:
****
Confirm Keystore Password:
****
Email
OK
Cancel
Show Advanced Options

Table 5-4 *User Application Configuration: Basic Parameters*

Type of Setting	Field	Description
eDirectory Connection Settings	*LDAP Host*	Required. Specify the hostname or IP address for your LDAP server and its secure port. For example: `myLDAPhost` This is same server that is actively running the IDM engine.
	LDAP Non-Secure Port	Specify the non-secure port for your LDAP server. For example: 389.
	LDAP Secure Port	Specify the secure port for your LDAP server. For example: 636.
	LDAP Administrator	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. This value is encrypted, based on the master key.
	LDAP Administrator Password	Required. Specify the LDAP Administrator password. This password is encrypted, based on the master key.
	Use Public Anonymous Account	Allows users who are not logged in to access the LDAP Public Anonymous Account.
	LDAP Guest	Allows users who are not logged in to access permitted portlets. This user account must already exist in the Identity Vault. To enable LDAP Guest, you must deselect *Use Public Anonymous Account*. To disable Guest User, select *Use Public Anonymous Account*.
	LDAP Guest Password	Specify the LDAP Guest password.
	Secure Admin Connection	Select this option to require that all communication using the admin account be done using a secure socket (this option can have adverse performance implications). This setting allows other operations that don't require SSL to operate without SSL.
	Secure User Connection	Select this option to require that all communication using the logged-in user’s account be done using a secure socket (this option can have adverse performance implications). This setting allows other operations that don't require SSL to operate without SSL.

Type of Setting	Field	Description
eDirectory DNs	*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 Section 5.4, “Creating the User Application Driver,” on page 107. For example, if your driver is UserApplicationDriver and your driver set is called myDriverSet, and the driver set is in a context of o=myCompany, you would type a value of: `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	User Application Admin	Required. An existing user in the Identity Vault who has the rights to perform administrative tasks for the User Application user container specified. This user can use the *Administration* tab of the User Application to administer the portal. If the User Application Administrator participates in workflow administration tasks exposed in iManager, Novell Designer for Identity Manager, or the User Application (*Requests & Approvals* tab), you must grant this administrator appropriate trustee rights to object instances contained in the User Application driver. Refer to the *IDM User Application: Administration Guide* for details. To change this assignment after you deploy the User Application, you must use the *Administration* > *Security* pages in the User Application.
	Provisioning Application Admin	This role is available in the provisioning version of Identity Manager 3.5.1. The Provisioning Application Administrator uses the *Provisioning* tab (under the *Administration* tab) to manage the Provisioning Workflow functions. These functions are available to users through the *Requests and Approvals* tab of the User Application. This user must exist in the Identity Vault prior to being designated the Provisioning Application Administrator. To change this assignment after you deploy the User Application, you must use the *Administration* > *Security* pages in the User Application.

Type of Setting	Field	Description
eDirectory DNs (continued)	*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 below) 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.
eDirectory Certificates	*Keystore Path*	Required. Specify the full path to your keystore (`cacerts`) file of the JDK that the application server application server is using to run, or click the small browser button and navigate to the `cacerts` file. On Linux or Solaris, the user must have permission to write to this file.
	Keystore Password/Confirm Keystore Password	Required. Specify the `cacerts` password. The default is `changeit`.
Email	*Notify Template Host Token*	Specify the application server hosting the Identity Manager User Application. For example: `myapplication serverServer` This value replaces the $HOST$ token in e-mail templates. The URL that is constructed is the link to provisioning request tasks and approval notifications.
	Notify Template Port Token	Used to replace the $PORT$ token in e-mail templates used in provisioning request tasks and approval notifications.
	NotifyTemplate Secure Port Token	Used to replace the $SECURE_PORT$ token in e-mail templates used in provisioning request tasks and approval notifications.
	Notification SMTP Email From:	Specify e-mail to come from a user in provisioning e-mail.
	Notification SMTP Email Host:	Specify the SMTP e-mail host that provisioning e-mail is using. This can be an IP address or a DNS name.

Type of Setting	Field	Description
Password Management	*Use External Password WAR*	This feature enables you to specify a Forgot Password page residing in an external Forgot Password WAR and a URL that the external Forgot Password WAR uses to call back the User Application through a Web service. If you check *Use External Password WAR*, you must supply values for *Forgot Password Link* and *Forgot Password Return Link*. If you do not select *Use External Password WAR,* IDM uses the default internal Password Management functionality, `./jsps/pwdmgt/ForgotPassword.jsf` (without the http(s) protocol at the beginning). This redirects the user to the Forgot Password functionality built into the User Application, rather than to an external WAR.
	Forgot Password Link	This URL points to the Forgot Password functionality page. Specify a `ForgotPassword.jsf` file in an external or internal password management WAR. For details, see "Using Password WARs" on page 141.
	Forgot Password Return Link	If you are using an external password management WAR, supply the path that the external Password Management WAR uses to call back the User Application through Web Services, for example `https://idmhost:sslport/idm`.

2 If you want to set additional User Application configuration parameters, click *Show Advanced Options*. (Scroll to view the whole panel.) Table 5-5 describes the Advanced Options parameters.

If you do not want to set additional parameters described in this step, skip to Step 3.

Table 5-5 *User Application Configuration: All Parameters*

Type of Setting	Field	Description
eDirectory Connection Settings	*LDAP Host*	Required. Specify the hostname or IP address for your LDAP server. For example: myLDAPhost
	LDAP Non-Secure Port	Specify the non-secure port for your LDAP server. For example: 389.
	LDAP Secure Port	Specify the secure port for your LDAP server. For example: 636.
	LDAP Administrator	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. This value is encrypted, based on the master key.
	LDAP Administrator Password	Required. Specify the LDAP Administrator password. This password is encrypted, based on the master key.
	Use Public Anonymous Account	Allows users who are not logged in to access the LDAP Public Anonymous Account.
	LDAP Guest	Allows users who are not logged in to access permitted portlets. This user account must already exist in the Identity Vault. To enable LDAP Guest, you must deselect *Use Public Anonymous Account*. To disable Guest User, select *Use Public Anonymous Account*.
	LDAP Guest Password	Specify the LDAP Guest password.
	Secure Admin Connection	Select this option to require that all communication using the admin account be done using a secure socket (this option can have adverse performance implications). This setting allows other operations that don't require SSL to operate without SSL.
	Secure User Connection	Select this option to require that all communication done on the logged-in user's account be done using a secure socket (this option can have severe adverse performance implications). This setting allows other operations that don't require SSL to operate without SSL.

Type of Setting	Field	Description
eDirectory DNs	*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 Section 5.4, “Creating the User Application Driver,” on page 107. For example, if your driver is UserApplicationDriver and your driver set is called myDriverSet, and the driver set is in a context of o=myCompany, you type a value of: `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	User Application Admin	Required. An existing user in the Identity Vault who has the rights to perform administrative tasks for the User Application user container specified. This user can use the *Administration* tab of the User Application to administer the portal. If the User Application Administrator participates in workflow administration tasks exposed in iManager, Novell Designer for Identity Manager, or the User Application (*Requests & Approvals* tab), you must grant this administrator appropriate trustee rights to object instances contained in the User Application driver. Refer to the *IDM User Application: Administration Guide* for details. To change this assignment after you deploy the User Application, you must use the *Administration* > *Security* pages in the User Application.
	Provisioning Application Admin	This role is available in the provisioning version of Identity Manager 3.5.1. The Provisioning Application Administrator manages Provisioning Workflow functions available through the *Requests and Approvals* tab of the User Application. This user must exist in the Identity Vault prior to being designated the Provisioning Application Administrator. To change this assignment after you deploy the User Application, you must use the *Administration* > *Security* pages in the User Application.

Type of Setting	Field	Description
Meta-Directory User Identity	*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 below) 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.
	User Object Class	The LDAP user object class (typically inetOrgPerson).
	Login Attribute	The LDAP attribute (for example, CN) that represents the user's login name.
	Naming Attribute	The LDAP attribute used as the identifier when looking up users or groups. This is not the same as the login attribute, which is used only during login, and not during user/group searches.
	User Membership Attribute	Optional. The LDAP attribute that represents the user's group membership. Do not use spaces in this name.
Meta-Directory User Groups	*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.
	Group Object Class	The LDAP group object class (typically groupofNames).
	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 (typically dynamicGroup).

Type of Setting	Field	Description
eDirectory Certificates	*Keystore Path*	Required. Specify the full path to your keystore (`cacerts`) file of the JRE that the application server application server is using to run, or else click the small browser button and navigate to the `cacerts` file. The User Application installation modifies the keystore file. On Linux or Solaris, the user must have permission to write to this file.
	Keystore Password *Confirm Keystore Password*	Required. Specify the `cacerts` password. The default is `changeit`.
Private Key Store	*Private Keystore Path*	The private keystore contains the User Application's private key and certificates. Reserved. If you leave this empty, this path is `/jre/lib/security/cacerts` by default.
	Private Keystore Password	This password is `changeit` unless you specify otherwise. This password is encrypted, based on the master key.
	Private Key Alias	This alias is `novellIDMUserApp` unless you specify otherwise.
	Private Key Password	This password is `novellIDM` unless you specify otherwise. This password is encrypted, based on the master key.
Trusted Key Store	*Trusted Store Path*	The Trusted Key Store contains all trusted signers' certificates used to validate digital signatures. If this path is empty, the User Application gets the path from System property `javax.net.ssl.trustStore`. If the path isn't there, it is assumed to be `jre/lib/security/cacerts`.
	Trusted Store Password	If this field is empty, the User Application gets the password from System property `javax.net.ssl.trustStorePassword`. If the value is not there, `changeit` is used. This password is encrypted, based on the master key.
Novell Audit Digital Signature and Certificate Key		Contains the Novell Audit digital signature key and certificate.
	Novell Audit Digital Signature Certificate	Displays the digital signature certificate.
	Novell Audit Digital Signature Private Key	Displays the digital signature private key. This key is encrypted, based on the master key.

Type of Setting	Field	Description
iChain Settings	*ICS Logout Enabled*	If this option is selected, the User Application supports simultaneous logout of the User Application and either iChain or Novell Access Manager. The User Application checks for an iChain or Novell Access Manager cookie on logout and, if the cookie is present, reroutes the user to the ICS logout page.
	ICS Logout Page	The URL to the iChain or Novell Access Manager logout page, where the URL is a hostname that iChain or Novell Access Manager expects. If ICS logging is enabled and a user logs out of the User Application, the user is rerouted to this page.
Email	*Notify Template Host Token*	Specify the application server hosting the Identity Manager User Application. For example: `myapplication serverServer` This value replaces the $HOST$ token in e-mail templates. The URL that is constructed is the link to provisioning request tasks and approval notifications.
	Notify Template Port Token	Used to replace the $PORT$ token in e-mail templates used in provisioning request tasks and approval notifications.
	Notify Template Secure Port Token	Used to replace the $SECURE_PORT$ token in e-mail templates used in provisioning request tasks and approval notifications.
	Notify Template PROTOCOL token	Refers to a non-secure protocol, HTTP. Used to replace the $PROTOCOL$ token in e-mail templates used in provisioning request tasks and approval notifications.
	Notify Template SECURE PROTOCOL token	Refers to a secure protocol, HTTPS. Used to replace the $SECURE_PROTOCOL$ token in e-mail templates used in provisioning request tasks and approval notifications.
	Notification SMTP Email From:	Specify e-mail from a user in provisioning e-mail.
	Notification SMTP Email Host:	Specify the SMTP e-mail host that provisioning e-mail is using. This can be an IP address or a DNS name.

Type of Setting	Field	Description
Password Management		
	Use External Password WAR	This feature enables you to specify a Forgot Password page residing in an external Forgot Password WAR and a URL that the external Forgot Password WAR uses to call back the User Application through a Web service. If you select *Use External Password WAR*, you must supply values for *Forgot Password Link* and *Forgot Password Return Link*. If you do not select *Use External Password WAR,* IDM uses the default internal Password Management functionality, `./jsps/pwdmgt/ForgotPassword.jsf` (without the http(s) protocol at the beginning). This redirects the user to the Forgot Password functionality built into the User Application, rather than to an external WAR.
	Forgot Password Link	This URL points to the Forgot Password functionality page. Specify a `ForgotPassword.jsf` file in an external or internal password management WAR. For details, see "Using Password WARs" on page 141.
	Forgot Password Return Link	If you are using an external password management WAR, supply the path that the external Password Management WAR uses to call back the User Application through Web Services, for example `https://idmhost:sslport/idm`.
Miscellaneous	*Session Timeout*	The application session timeout.
	OCSP URI	If the client installation uses the On-Line Certificate Status Protocol (OCSP), supply a Uniform Resource Identifier (URI). For example, the format is http://host:port/ocspLocal. The OCSP URI updates the status of trusted certificates online.
	Authorization Config Path	Fully qualified name of the authorization configuration file.

Type of Setting	Field	Description
Container Object	*Selected*	Select each Container Object Type to use.
	Container Object Type	Select from the following standard containers: locality, country, organizationalUnit, organization, and domain. You can also define your own containers in iManager and add them under *Add a new Container Object*.
	Container Attribute Name	Lists the Attribute Type name associated with the Container Object Type.
	Add a New Container Object: Container Object Type	Specify the LDAP name of an objectclass from the Identity Vault that can serve as a container. For information on containers, see the *Novell iManager 2.6 Administration Guide (http://www.novell.com/documentation/imanager26/pdfdoc/imanager_admin_26/imanager_admin_26.pdf)* .
	Add a New Container Object: Container Attribute Name	Supply the attribute name of the container object.

NOTE: You can edit most of the settings in this file after installation. To do so, run the `configupdate.sh` script or the Windows `configupdate.bat` file located in your installation subdirectory. Remember that in a cluster, the settings in this file must be identical for all members of the cluster.

3 After you finish configuring the settings, click *OK*, then continue with Section 5.6.15, "Verify Choices and Install," on page 142

Using Password WARs

Use the *Forgot Password Link* configuration parameter to specify the location of a WAR containing Forgot Password functionality. You can specify a WAR that is external or internal to the User Application.

Specifying an External Password Management WAR

1 Use either the install procedure or the configupdate utility.

2 In the User Application configuration parameters, select the *Use External Password WAR* configuration parameter check box.

3 For the *Forgot Password Link* configuration parameter, specify the location for the external password WAR.

Include the host and port, for example `http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf`. An external password WAR can be outside the firewall protecting the User Application.

4 For the *Forgot Password Return Link*, supply the path that the external Password Management WAR uses to call back the User Application through Web Services, for example `https://idmhost:sslport/idm`.

The return link must use SSL to ensure secure Web Service communication to the User Application. See also Section 5.10.3, “Configuring SSL Communication Between JBoss Servers,” on page 179.

5 If you are using the installer, read the information in this step and proceed to Step 6 on page 142.

If you are using the configupdate utility to update the external password WAR in the installation root directory, read this step and manually rename the WAR to the first directory you specified in *Forgot Password Link*. Then, proceed to Step 6 on page 142.

Before the installation ends, the installer renames `IDMPwdMgt.war` (bundled with the installer) to the name of the first directory that you specify. The renamed `IDMPwdMgt.war` becomes your external password WAR. For example, if you specify `http://www.idmpwdmgthost.com/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf`, the installer renames `IDMPwdMgt.war` to `ExternalPwd.war`. The installer moves the renamed WAR into the installation root directory.

6 Manually copy `ExternalPwd.war` to the remote JBoss server deploy directory that runs the external password WAR functionality.

Specifying an Internal Password Management WAR

1 Do not select *Use External Password WAR*.

2 Accept the default location for the *Forgot Password Link*, or supply a URL for another password WAR.

3 Accept the default value for *Forgot Password Return Link*.

5.6.15 Verify Choices and Install

1 Read the Pre-Install Summary page to verify your choices for the installation parameters.

2 If necessary, use *Back* to return to earlier installation pages to change installation parameters.

The User Application configuration page does not save values, so after you re-specify earlier pages in the installation, you must re-enter the User Application configuration values.

3 When you are satisfied with your installation and configuration parameters, return to the Pre-Install Summary page and click *Install*.

5.6.16 View Log Files

1 If your installation completed without error, go to Section 5.10, “Post-Install Tasks,” on page 178.

2 If the installation issued errors or warnings, review the log files to determine the problems:

- `Identity_Manager_User_Application_InstallLog.log` holds results of the basic installation tasks
- `Novell-Custom-Install.log` holds information about the User Application configuration done during installation

For help solving problems, see Section 5.12, “Troubleshooting,” on page 181.

5.7 Installing the User Application on a WebSphere Application Server

This section describes how to install the IDM User Application on a WebSphere Application Server with the graphical user interface version of the installer.

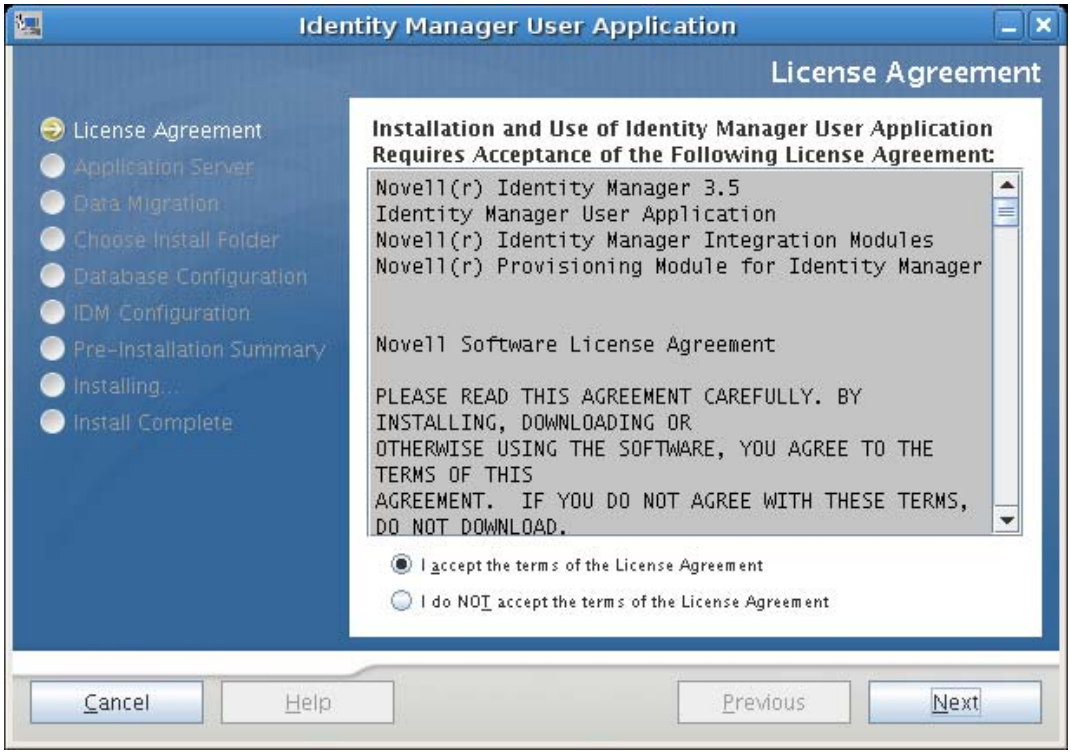
5.7.1 Launching the Installer GUI

1. Navigate to the directory containing your installation files.
2. Launch the installer:

   ```
   java -jar IdmUserApp.jar
   ```

3. Select a language from the drop-down menu, then click OK.

4 Read the license agreement, click *I accept the terms of the License Agreement*, then click *Next*.

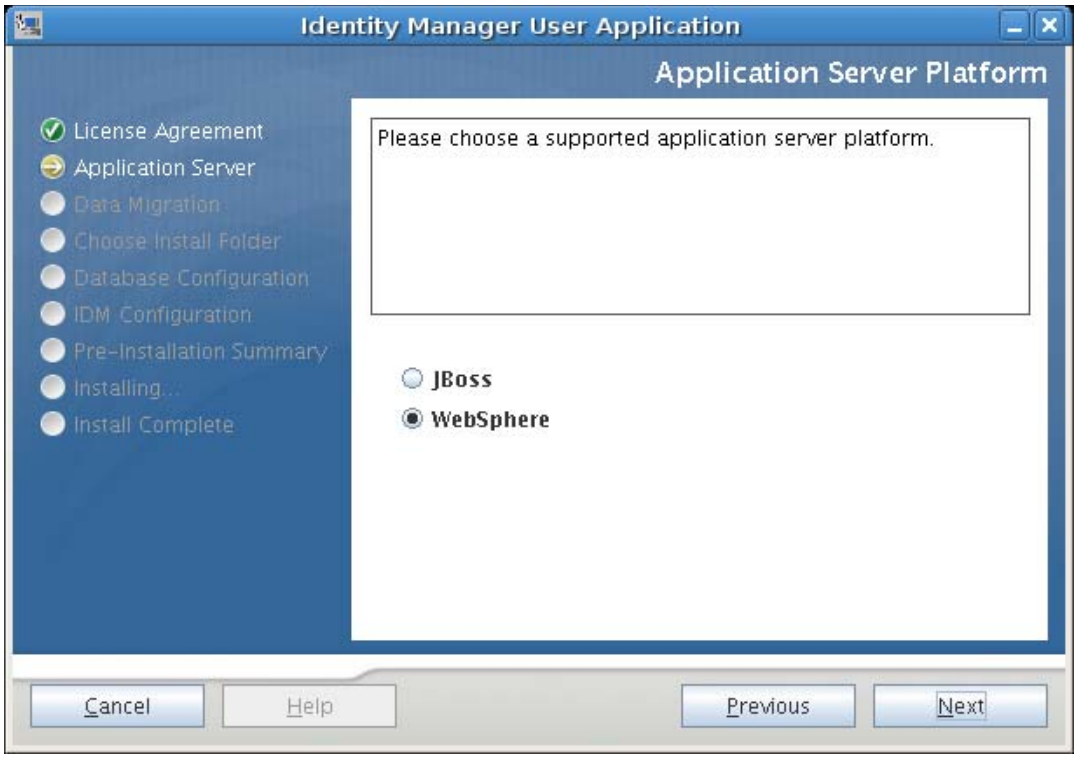


5 Read the Introduction page of the install wizard, then click *Next*.

5.7.2 Choosing an Application Server Platform

1 In the Application Server Platform window, select the WebSphere application server platform.

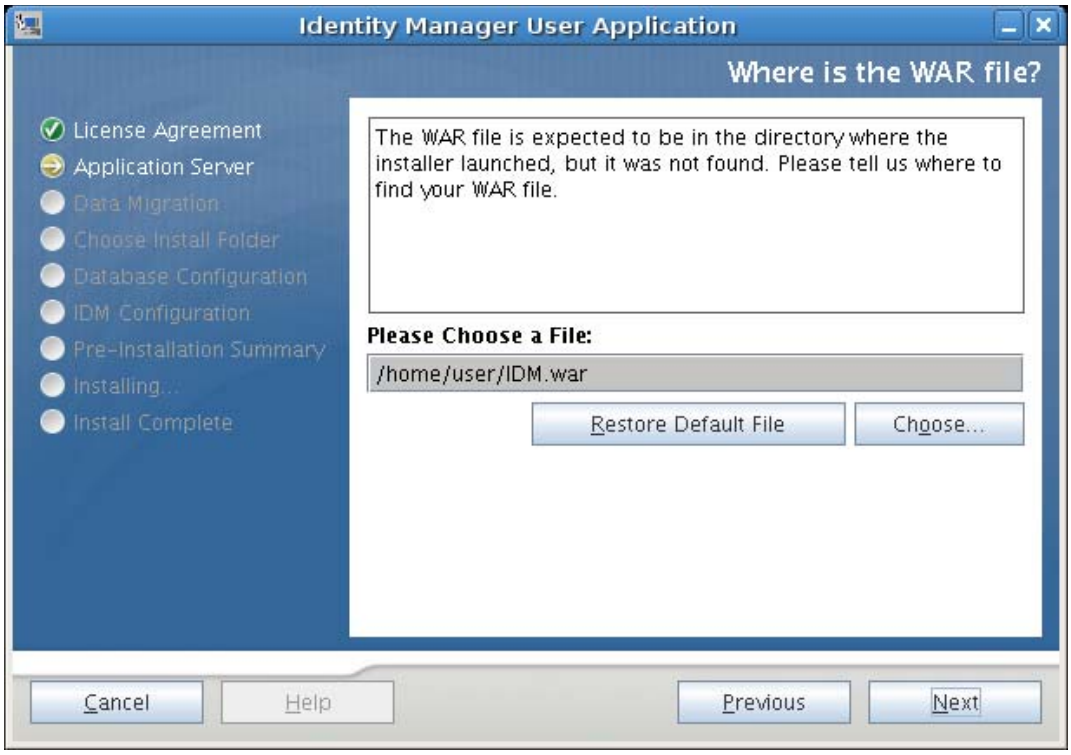
2 Select *Next*. Then continue with Section 5.7.3, “Specifying the Location of the WAR,” on page 145.



5.7.3 Specifying the Location of the WAR

If the Identity Manager User Application WAR file is in a different directory from the installer, the installer prompts for the path to the WAR.

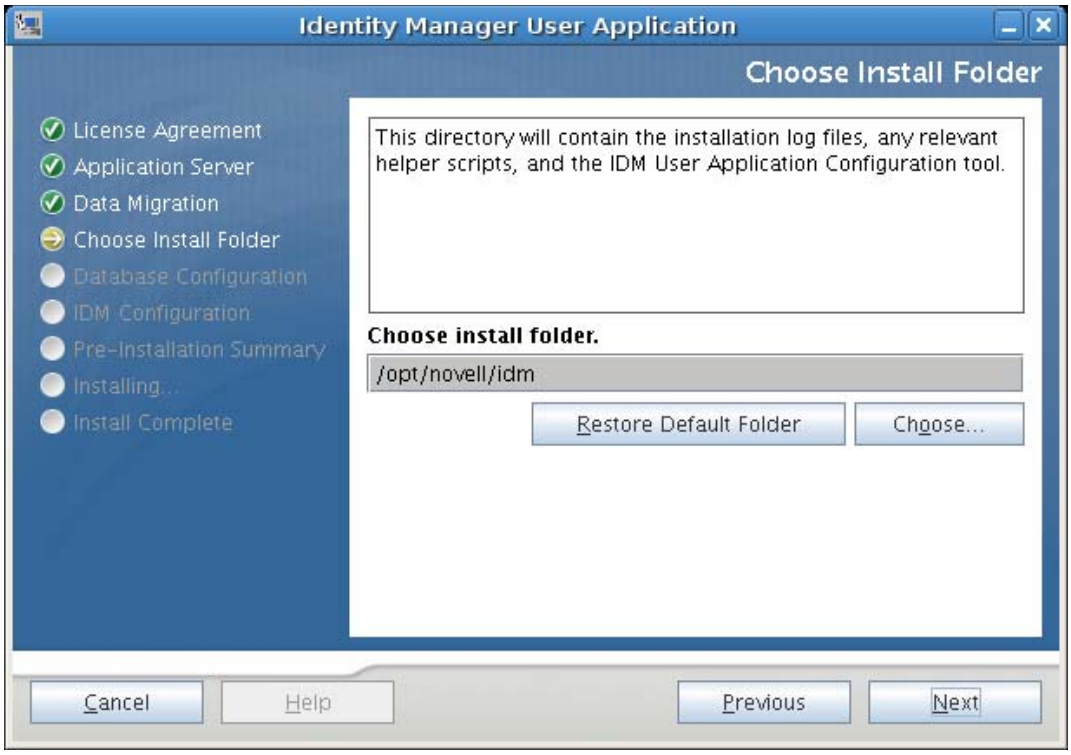
1 If the WAR is in the default location, you can click *Restore Default Folder*. Or, to specify the location of the WAR file, click *Choose* and select a location.



2 Click *Next*, then continue with Section 5.7.4, “Choosing an Install Folder,” on page 146.

5.7.4 Choosing an Install Folder

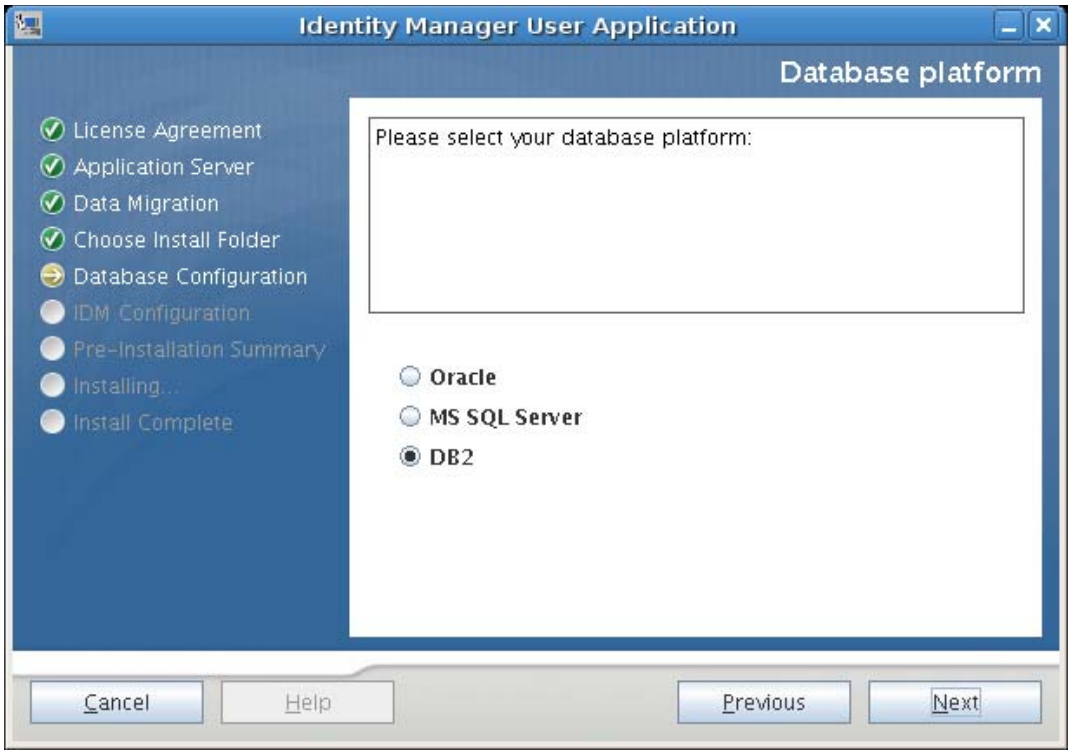
1 On the Choose Install Folder page, select where to install the User Application. If you want to to use the default location, click *Restore Default Folder*, or if you want to choose another location for the installation files, click *Choose* and browse to a location.



2 Click *Next*, then continue with Section 5.7.5, “Choosing a Database Platform,” on page 147.

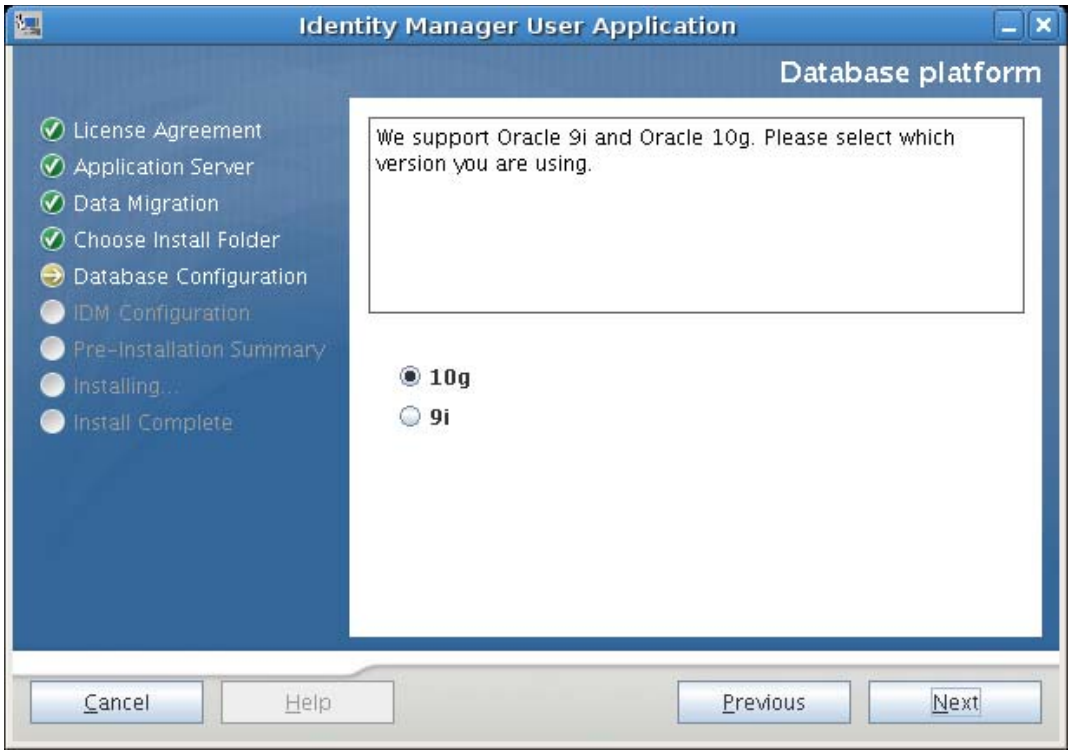
5.7.5 Choosing a Database Platform

1 Select the database platform to use.



2 If you are using an Oracle database, continue with Step 3. Otherwise, skip to Step 4.

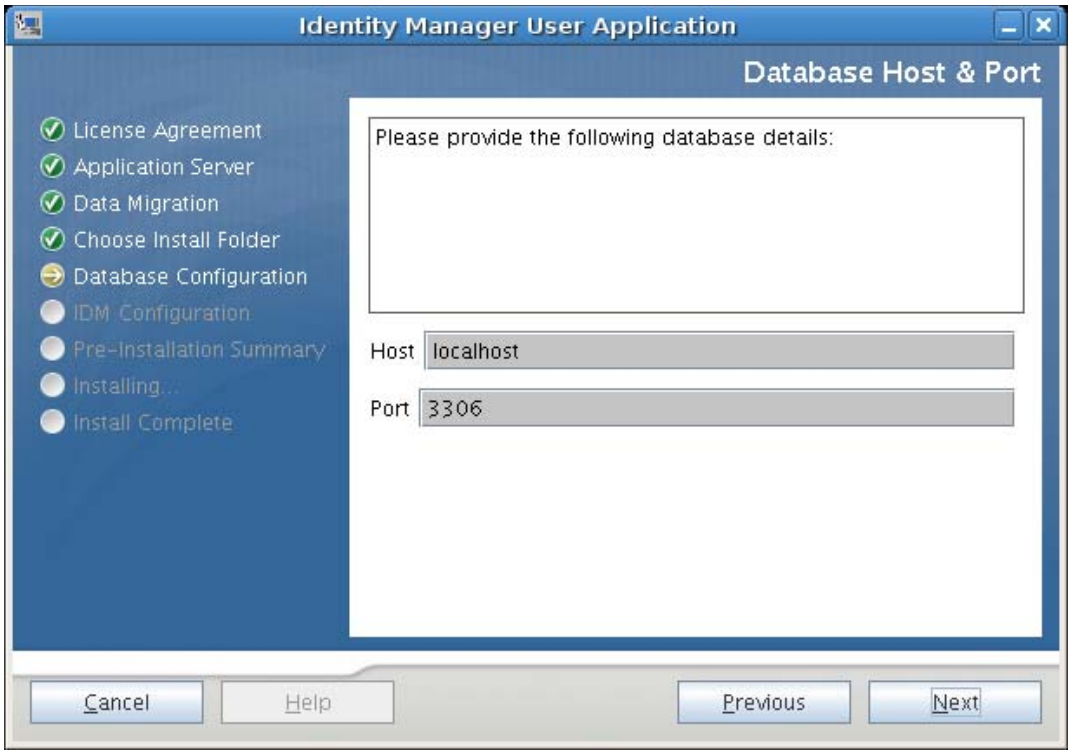
3 If you are using an Oracle database, the installer asks you which version you are using. Choose your version.



4 Click *Next*, then continue with Section 5.7.6, “Specifying the Database Host and Port,” on page 149.

5.7.6 Specifying the Database Host and Port

1 Fill in the following fields:



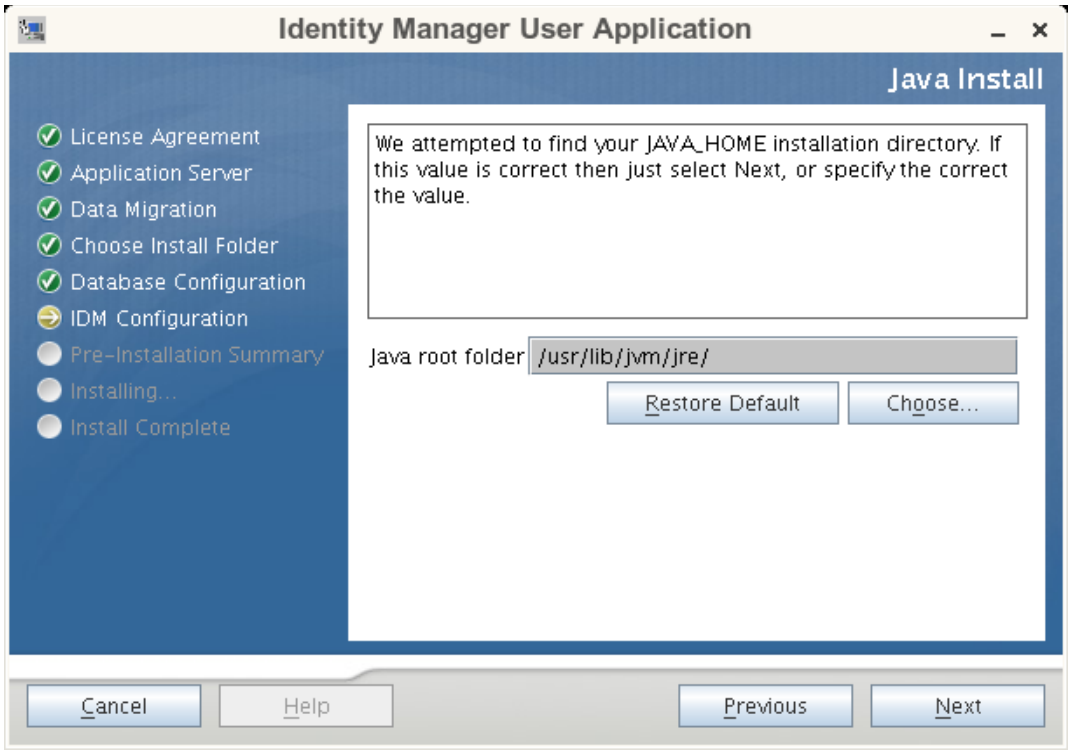
Field	Description
Host	Specify the database server's hostname or IP address. For a cluster, specify the same hostname or IP address for each member of the cluster.
Port	Specify the database's listener port number. For a cluster, specify the same port for each member of the cluster.

2 Click *Next*, then continue with Section 5.7.7, "Specifying the Java Root Directory," on page 150.

5.7.7 Specifying the Java Root Directory

NOTE: With WebSphere, you must use the IBM JDK that has the unrestricted policy files applied.

1 Click *Choose* to browse for your Java root folder. Or, to use the default location, click *Restore Default*.

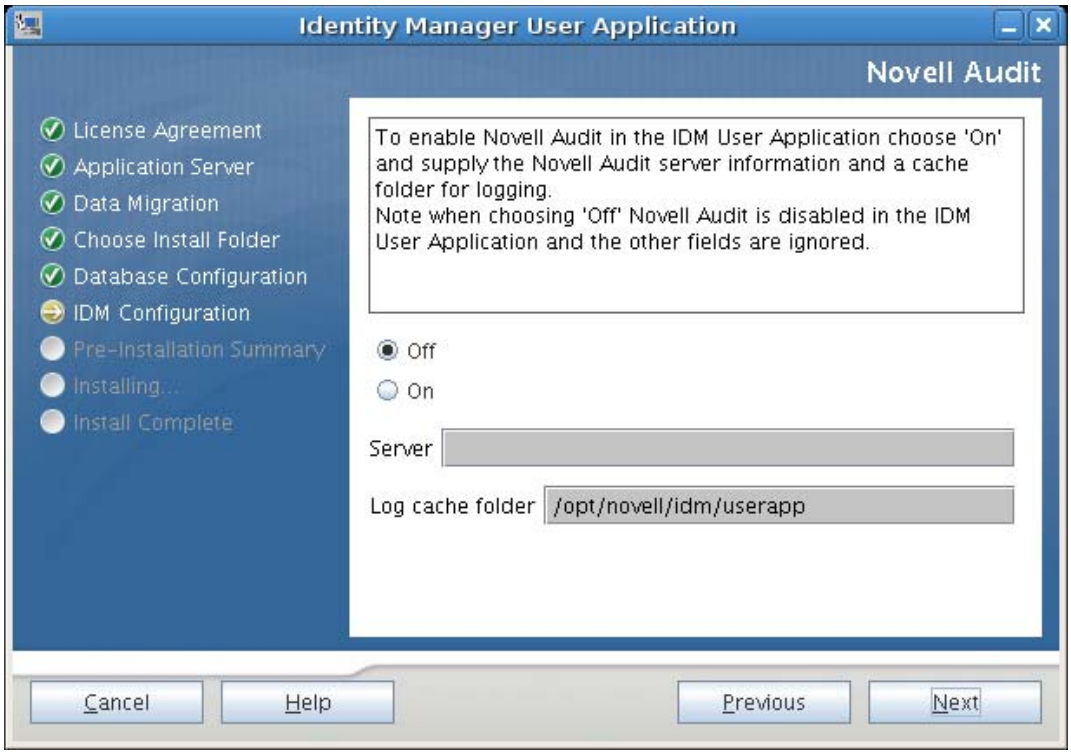


2 Click *Next*, then continue with Section 5.7.8, "Enabling Novell Audit Logging," on page 151.

5.7.8 Enabling Novell Audit Logging

To enable Novell Audit logging (optional) for the User Application:

1 Fill in the following fields:



Option	Description
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 *Identity Manager User Application: Administration Guide*.
On	Enables Novell Audit Logging for the User Application. For more information on setting up Novell Audit logging, see the *Identity Manager User Application: Administration Guide*.
Server	If you turn Novell Audit logging on, specify the hostname or IP address for the Novell Audit server. If you turn logging off, this value is ignored.
Log Cache Folder	Specify the directory for the logging cache.

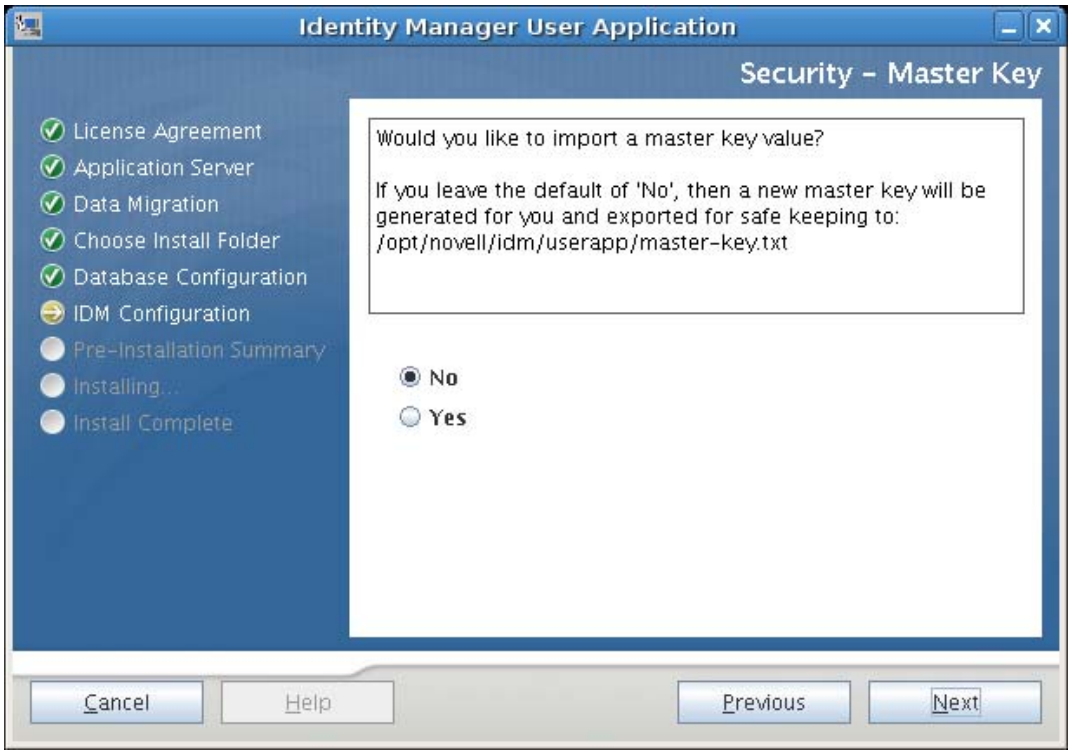
2 Click *Next* and continue with Section 5.7.9, “Specifying a Master Key,” on page 153.

5.7.9 Specifying a Master Key

Specify whether to import an existing master key or create a new one. Examples of reasons to import an existing master key include:

- You are moving your installation from a staging system to a production system and want to keep access to the database you used with the staging system.
- You installed the User Application on the first member of a cluster and are now installing on subsequent members of the cluster (they require the same master key).
- Because of a failed disk, you need to restore your User Application. You must reinstall the User Application and specify the same encrypted master key that the previous installation used. This gives you access to the previously stored encrypted data.

1 Click *Yes* to import an existing master key, or click *No* to create a new one.



2 Click *Next*.

The installation procedure writes the encrypted master key to the `master-key.txt` file in the installation directory.

If you chose *No*, skip to Section 5.7.10, “Configuring the User Application,” on page 154. After you finish the installation, you must manually record the master key.

If you chose *Yes*, continue with Step 3 on page 153.

3 If you choose to import an existing encrypted master key, cut and paste the key into the install procedure window.

4 Click *Next* and continue with Section 5.7.10, "Configuring the User Application," on page 154.

5.7.10 Configuring the User Application

The User Application install enables you to set User Application configuration parameters. Most of these parameters are also editable with `configupdate.sh` or `configupdate.bat` after installation; exceptions are noted in the parameter descriptions. For a cluster, specify identical User Application configuration parameters for each member of the cluster.

1 Click *Next* through the first User Application Configuration page.

2 Set the basic User Application configuration parameters described in Table Table 5-6 on page 157, then continue with Step 3.

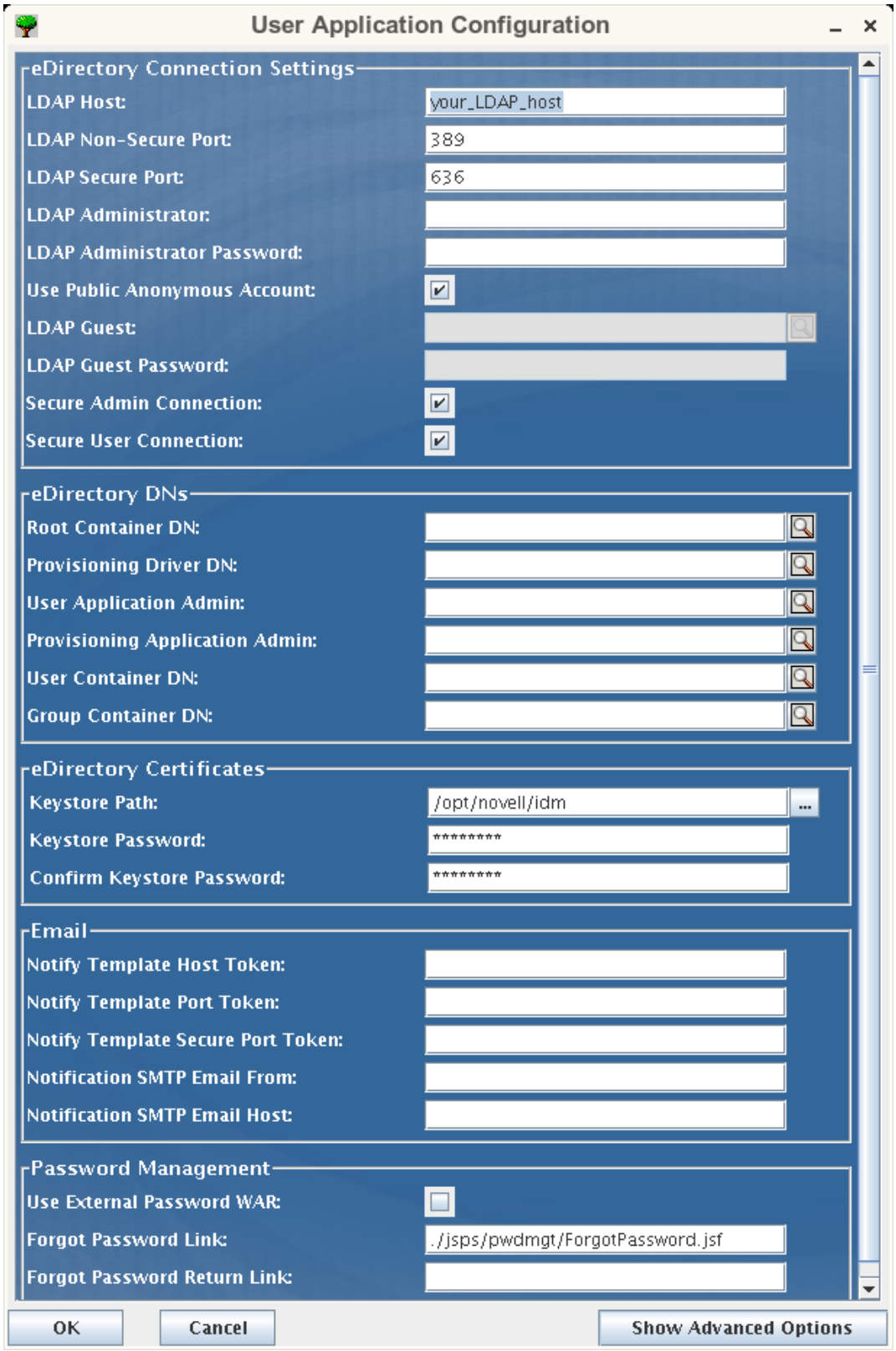

User Application Configuration
eDirectory Connection Settings
LDAP Host:
your_LDAP_host
LDAP Non-Secure Port:
389
LDAP Secure Port:
636
LDAP Administrator:
LDAP Administrator Password:
Use Public Anonymous Account:
LDAP Guest:
LDAP Guest Password:
Secure Admin Connection:
Secure User Connection:
eDirectory DNs
Root Container DN:
Provisioning Driver DN:
User Application Admin:
Provisioning Application Admin:
User Container DN:
Group Container DN:
eDirectory Certificates
Keystore Path:
/opt/novell/idm
Keystore Password:
Confirm Keystore Password:
Email
Notify Template Host Token:
Notify Template Port Token:
Notify Template Secure Port Token:
Notification SMTP Email From:
Notification SMTP Email Host:
Password Management
Use External Password WAR:
Forgot Password Link:
./jsps/pwdmgt/ForgotPassword.jsf
Forgot Password Return Link:
OK
Cancel
Show Advanced Options

Table 5-6 *User Application Configuration: Basic Parameters*

Type of Setting	Field	Description
eDirectory Connection Settings	*LDAP Host*	Required. Specify the hostname or IP address for your LDAP server and its secure port. For example: `myLDAPhost`
	LDAP Non-Secure Port	Specify the non-secure port for your LDAP server. For example: 389.
	LDAP Secure Port	Specify the secure port for your LDAP server. For example: 636.
	LDAP Administrator	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. This value is encrypted, based on the master key.
	LDAP Administrator Password	Required. Specify the LDAP Administrator password. This password is encrypted, based on the master key.
	Use Public Anonymous Account	Allows users who are not logged in to access the LDAP Public Anonymous Account.
	LDAP Guest	Allows users who are not logged in to access permitted portlets. This user account must already exist in the Identity Vault. To enable LDAP Guest, you must deselect *Use Public Anonymous Account*. To disable Guest User, select *Use Public Anonymous Account*.
	LDAP Guest Password	Specify the LDAP Guest password.
	Secure Admin Connection	Select this option to require that all communication using the admin account be done using a secure socket (this option can have adverse performance implications). This setting allows other operations that don't require SSL to operate without SSL.
	Secure User Connection	Select this option to require that all communication using the logged-in user’s account be done using a secure socket (this option can have adverse performance implications). This setting allows other operations that don't require SSL to operate without SSL.

Type of Setting	Field	Description
eDirectory DNs	*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. For example, if your driver is UserApplicationDriver and your driver set is called myDriverSet, and the driver set is in a context of o=myCompany, you would type a value of: `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	User Application Admin	Required. An existing user in the Identity Vault who has the rights to perform administrative tasks for the User Application user container specified. This user can use the *Administration* tab of the User Application to administer the portal. If the User Application Administrator participates in workflow administration tasks exposed in iManager, Novell Designer for Identity Manager, or the User Application (*Requests & Approvals* tab), you must grant this administrator appropriate trustee rights to object instances contained in the User Application driver. Refer to the *IDM User Application: Administration Guide* for details. To change this assignment after you deploy the User Application, you must use the *Administration* > *Security* pages in the User Application.
	Provisioning Application Admin	This role is available in the provisioning version of Identity Manager 3.5.1. The Provisioning Application Administrator uses the *Provisioning* tab (under the *Administration* tab) to manage the Provisioning Workflow functions. These functions are available to users through the *Requests and Approvals* tab of the User Application. This user must exist in the Identity Vault prior to being designated the Provisioning Application Administrator. To change this assignment after you deploy the User Application, you must use the *Administration* > *Security* pages in the User Application.

Type of Setting	Field	Description
eDirectory DNs (continued)	*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 below) 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.
eDirectory Certificates	*Keystore Path*	Required. Specify the full path to your keystore (`cacerts`) file of the JDK that the application server application server is using to run, or click the small browser button and navigate to the `cacerts` file. On Linux or Solaris, the user must have permission to write to this file.
	Keystore Password/Confirm Keystore Password	Required. Specify the `cacerts` password. The default is `changeit`.
Email	*Notifiy Template Host Token*	Specify the application server hosting the Identity Manager User Application. For example: `myapplication serverServer` This value replaces the $HOST$ token in e-mail templates. The URL that is constructed is the link to provisioning request tasks and approval notifications.
	Notify Template Port Token	Used to replace the $PORT$ token in e-mail templates used in provisioning request tasks and approval notifications.
	Notify Template Secure Port token	Used to replace the $SECURE_PORT$ token in e-mail templates used in provisioning request tasks and approval notifications.
	Notification SMTP Email From:	Specify e-mail to come from a user in provisioning e-mail.
	Notification SMTP Email Host:	Specify the SMTP e-mail host that provisioning e-mail is using. This can be an IP address or a DNS name.

Type of Setting	Field	Description
Password Management	*Use External Password WAR*	This feature enables you to specify a Forgot Password page residing in an external Forgot Password WAR and a URL that the external Forgot Password WAR uses to call back the User Application through a Web service. If you select *Use External Password WAR*, you must supply values for *Forgot Password Link* and *Forgot Password Return Link*. If you do not select *Use External Password WAR,* IDM uses the default internal Password Management functionality, `./jsps/pwdmgt/ForgotPassword.jsf` (without the http(s) protocol at the beginning). This redirects the user to the Forgot Password functionality built into the User Application, rather than to an external WAR.
	Forgot Password Link	This URL points to the Forgot Password functionality page. Specify a `ForgotPassword.jsf` file in an external or internal password management WAR.
	Forgot Password Return Link	If you are using an external password management WAR, supply the path that the external Password Management WAR uses to call back the User Application through Web Services, for example `https://idmhost:sslport/idm`.

3 If you want to set additional User Application configuration parameters, click *Show Advanced Options*. (Scroll to view the whole panel.) Table Table 5-7 on page 161 describes the Advanced Options parameters. If you do not want to set additional parameters described in this step, skip to Step 4.

Table 5-7 *User Application Configuration: All Parameters*

Type of Setting	Field	Description
eDirectory Connection Settings	*LDAP Host*	Required. Specify the hostname or IP address for your LDAP server. For example: myLDAPhost
	LDAP Non-Secure Port	Specify the non-secure port for your LDAP server. For example: 389.
	LDAP Secure Port	Specify the secure port for your LDAP server. For example: 636.
	LDAP Administrator	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. This value is encrypted, based on the master key.
	LDAP Administrator Password	Required. Specify the LDAP Administrator password. This password is encrypted, based on the master key.
	Use Public Anonymous Account	Allows users who are not logged in to access the LDAP Public Anonymous Account.
	LDAP Guest	Allows users who are not logged in to access permitted portlets. This user account must already exist in the Identity Vault. To enable LDAP Guest, you must deselect *Use Public Anonymous Account*. To disable Guest User, select *Use Public Anonymous Account*.
	LDAP Guest Password	Specify the LDAP Guest password.
	Secure Admin Connection	Select this option to require that all communication using the admin account be done using a secure socket (this option can have adverse performance implications). This setting allows other operations that don't require SSL to operate without SSL.
	Secure User Connection	Select this option to require that all communication done on the logged-in user's account be done using a secure socket (this option can have severe adverse performance implications). This setting allows other operations that don't require SSL to operate without SSL.

Type of Setting	Field	Description
eDirectory DNs	*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. For example, if your driver is UserApplicationDriver and your driver set is called myDriverSet, and the driver set is in a context of o=myCompany, you type a value of: `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	User Application Admin	Required. An existing user in the Identity Vault who has the rights to perform administrative tasks for the User Application user container specified. This user can use the *Administration* tab of the User Application to administer the portal. If the User Application Administrator participates in workflow administration tasks exposed in iManager, Novell Designer for Identity Manager, or the User Application (*Requests & Approvals* tab), you must grant this administrator appropriate trustee rights to object instances contained in the User Application driver. Refer to the *IDM User Application: Administration Guide* for details. To change this assignment after you deploy the User Application, you must use the *Administration* > *Security* pages in the User Application.
	Provisioning Application Admin	This role is available in the provisioning version of Identity Manager 3.5.1. The Provisioning Application Administrator manages Provisioning Workflow functions available through the *Requests and Approvals* tab of the User Application. This user must exist in the Identity Vault prior to being designated the Provisioning Application Administrator. To change this assignment after you deploy the User Application, you must use the *Administration* > *Security* pages in the User Application.

Type of Setting	Field	Description
Meta-Directory User Identity	*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 below) 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.
	User Object Class	The LDAP user object class (typically inetOrgPerson).
	Login Attribute	The LDAP attribute (for example, CN) that represents the user's login name.
	Naming Attribute	The LDAP attribute used as the identifier when looking up users or groups. This is not the same as the login attribute, which is used only during login, and not during user/group searches.
	User Membership Attribute	Optional. The LDAP attribute that represents the user's group membership. Do not use spaces in this name.
Meta-Directory User Groups	*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.
	Group Object Class	The LDAP group object class (typically groupofNames).
	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 (typically dynamicGroup).

Type of Setting	Field	Description
eDirectory Certificates	*Keystore Path*	Required. Specify the full path to your keystore (`cacerts`) file of the JRE that the application server application server is using to run, or else click the small browser button and navigate to the `cacerts` file. The User Application installation modifies the keystore file. On Linux or Solaris, the user must have permission to write to this file.
	Keystore Password *Confirm Keystore Password*	Required. Specify the `cacerts` password. The default is `changeit`.
Private Key Store	*Private Keystore Path*	The private keystore contains the User Application's private key and certificates. Reserved. If you leave this empty, this path is `/jre/lib/security/cacerts` by default.
	Private Keystore Password	This password is `changeit` unless you specify otherwise. This password is encrypted, based on the master key.
	Private Key Alias	This alias is `novellIDMUserApp` unless you specify otherwise.
	Private Key Password	This password is `novellIDM` unless you specify otherwise. This password is encrypted, based on the master key.
Trusted Key Store	*Trusted Store Path*	The Trusted Key Store contains all trusted signers' certificates used to validate digital signatures. If this path is empty, the User Application gets the path from System property `javax.net.ssl.trustStore`. If the path isn't there, it is assumed to be `jre/lib/security/cacerts`.
	Trusted Store Password	If this field is empty, the User Application gets the password from System property `javax.net.ssl.trustStorePassword`. If the value is not there, `changeit` is used. This password is encrypted, based on the master key.
Novell Audit Digital Signature and Certificate Key		Contains the Novell Audit digital signature key and certificate.
	Novell Audit Digital Signature Certificate	Displays the digital signature certificate.
	Novell Audit Digital Signature Private Key	Displays the digital signature private key. This key is encrypted, based on the master key.

Type of Setting	Field	Description
iChain Settings	*ICS Logout Enabled*	If this option is selected, the User Application supports simultaneous logout of the User Application and either iChain or Novell Access Manager. The User Application checks for an iChain or Novell Access Manager cookie on logout and, if the cookie is present, reroutes the user to the ICS logout page.
	ICS Logout Page	The URL to the iChain or Novell Access Manager logout page, where the URL is a hostname that iChain or Novell Access Manager expects. If ICS logging is enabled and a user logs out of the User Application, the user is rerouted to this page.
Email	*Notify Template HOST token*	Specify the application server hosting the Identity Manager User Application. For example: `myapplication serverServer` This value replaces the $HOST$ token in e-mail templates. The URL that is constructed is the link to provisioning request tasks and approval notifications.
	Notify Template PORT token	Used to replace the $PORT$ token in e-mail templates used in provisioning request tasks and approval notifications.
	Notify Template SECURE PORT token	Used to replace the $SECURE_PORT$ token in e-mail templates used in provisioning request tasks and approval notifications.
	Notify Template PROTOCOL token	Refers to a non-secure protocol, HTTP. Used to replace the $PROTOCOL$ token in e-mail templates used in provisioning request tasks and approval notifications.
	Notify Template SECURE PROTOCOL token	Refers to a secure protocol, HTTPS. Used to replace the $SECURE_PROTOCOL$ token in e-mail templates used in provisioning request tasks and approval notifications.
	Notification SMTP Email From:	Specify e-mail from a user in provisioning e-mail.
	Notification SMTP Email Host:	Specify the SMTP e-mail host that provisioning e-mail is using. This can be an IP address or a DNS name.

Type of Setting	Field	Description
Password Management		
	Use External Password WAR	This feature enables you to specify a Forgot Password page residing in an external Forgot Password WAR and a URL that the external Forgot Password WAR uses to call back the User Application through a Web service. If you select *Use External Password WAR*, you must supply values for *Forgot Password Link* and *Forgot Password Return Link*. If you do not select *Use External Password WAR,* IDM uses the default internal Password Management functionality, `./jsps/pwdmgt/ForgotPassword.jsf` (without the http(s) protocol at the beginning). This redirects the user to the Forgot Password functionality built into the User Application, rather than to an external WAR.
	Forgot Password Link	This URL points to the Forgot Password functionality page. Specify a `ForgotPassword.jsf` file in an external or internal password management WAR.
	Forgot Password Return Link	If you are using an external password management WAR, supply the path that the external Password Management WAR uses to call back the User Application through Web Services, for example `https://idmhost:sslport/idm`.
Miscellaneous	*Session Timeout*	The application session timeout.
	OCSP URI	If the client installation uses the On-Line Certificate Status Protocol (OCSP), supply a Uniform Resource Identifier (URI). For example, the format is http://host:port/ocspLocal. The OCSP URI updates the status of trusted certificates online.
	Authorization Config Path	Fully qualified name of the authorization configuration file.
	Create eDirectory Index	
	Server DN	

Type of Setting	Field	Description
Container Object	*Selected*	Select each Container Object Type to use.
	Container Object Type	Select from the following standard containers: locality, country, organizationalUnit, organization, and domain. You can also define your own containers in iManager and add them under *Add a new Container Object*.
	Container Attribute Name	Lists the Attribute Type name associated with the Container Object Type.
	Add a New Container Object: Container Object Type	Specify the LDAP name of an objectclass from the Identity Vault that can serve as a container. For information on containers, see the *Novell iManager 2.6 Administration Guide (http://www.novell.com/documentation/imanager26/pdfdoc/imanager_admin_26/imanager_admin_26.pdf)* .
	Add a New Container Object: Container Attribute Name	Supply the attribute name of the container object.

4 After you finish configuring the settings, click *OK*, then continue with Section 5.7.11, “Verify Choices, and Install,” on page 167.

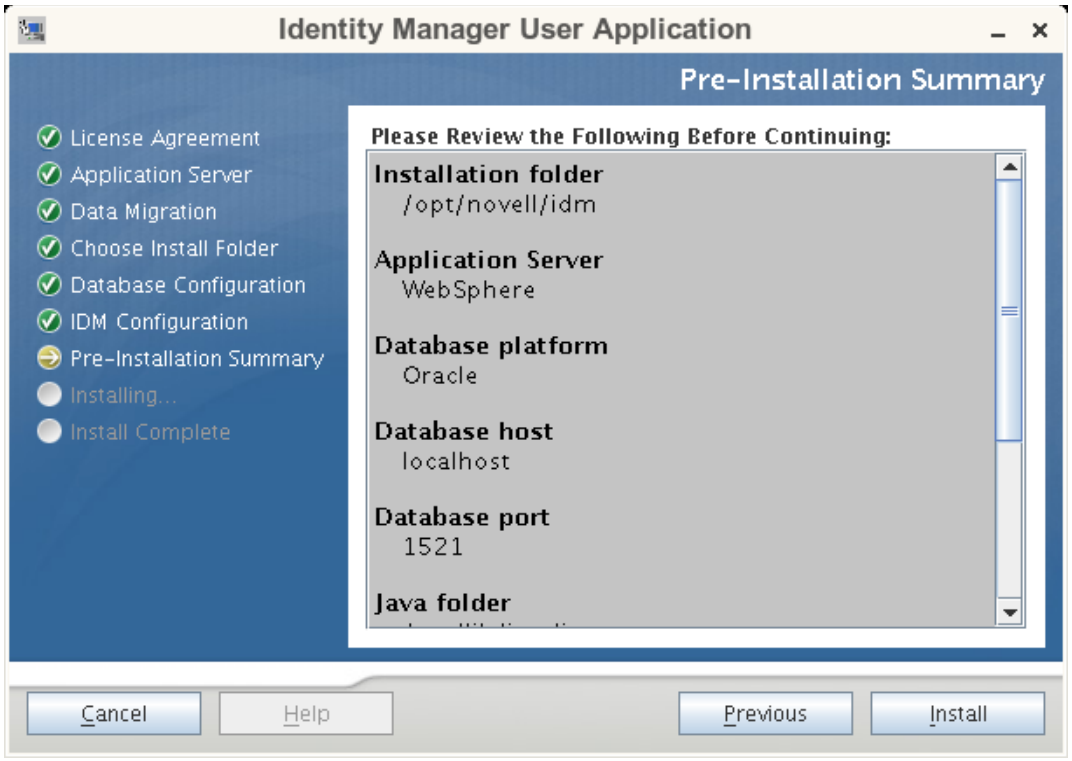
5.7.11 Verify Choices, and Install

Read the Pre-Install Summary page to verify your choices for the installation parameters.

If necessary, use *Back* to return to earlier installation pages to change installation parameters.

The User Application configuration page does not save values, so after you re-specify earlier pages in the installation, you must re-enter the User Application configuration values.

When you are satisfied with your installation and configuration parameters, return to the Pre-Install Summary page and click *Install*. Continue with Section 5.7.12, “View Log Files,” on page 168.



5.7.12 View Log Files

If your installation completed without error, continue with Section 5.7.13, “Add User Application configuration files and JVM system properties,” on page 168.

If the installation issued errors or warnings, review the log files to determine the problems:

- `Identity_Manager_User_Application_InstallLog.log` holds results of the basic installation tasks.
- `Novell-Custom-Install.log` holds information about the User Application configuration done during installation.

5.7.13 Add User Application configuration files and JVM system properties

1. Copy the `sys-configuration-xmldata.xml` file from the User Application install directory to a directory on the machine hosting the WebSphere server, for example `/UserAppConfigFiles`. The User Application install directory is the directory in which you installed the User Application.
2. Set the path to the `sys-configuration-xmldata.xml` file in the JVM system properties. Log in to the WebSphere admin console as an admin user to do this.
3. From the left panel, go to *Servers* > *Application Servers*
4. Click on the server name in the server list, for example server1.
5. In the list of settings on the right, go to *Java and Process Management* under *Server Infrastructure*.

6 Expand the link and select *Process Definition*.

7 Under the list of *Additional Properties*, select *Java Virtual Machine*.

8 Select *Custom Properties* under the *Additional Properties* heading for the JVM page.

9 Click *New* to add a new JVM system property.

9a For the *Name*, enter `extend.local.config.dir`.

9b For the *Value*, enter the name of the install folder (directory) that you specified during installation. (The installer wrote the `sys-configuration-xmldata.xml` file to this folder.).

9c For the *Description*, enter a description for the property, for example `path to sys-configuration-xmldata.xml`.

9d Click *OK* to save the property.

10 Click *New* to add another new JVM system property.

10a For the *Name*, enter `idmuserapp.logging.config.dir`

10b For the *Value*, enter the name of the install folder (directory) that you specified during installation.

10c For the *Description*, enter a description for the property, for example `path to idmuserapp_logging.xml`.

10d Click *OK* to save the property.

NOTE: The `idmuserapp-logging.xml` file does not exist until you persist the changes through *User Application* > *Administration* > *Application Configuration* > *Logging*.

5.7.14 Import the eDirectory Trusted Root to the WebSphere keystore

1 The User Application installation procedure exports the eDirectory trusted root certificates to the directory in which you install the User Application. Copy these certificates to the machine hosting the WebSphere server.

2 Import the certificates into the WebSphere keystore. You can do this using the WebSphere admininstrator's console ("Importing Certificates with the WebSphere Administrator's Console" on page 169) or through the command line ("Importing certificates with the command line" on page 170).

3 After you import certificates, proceed to Section 5.7.15, "Deploy the IDM WAR file," on page 170.

Importing Certificates with the WebSphere Administrator's Console

1 Log in to the WebSphere administration console as an admin user.

2 From the left panel, go to *Security* > *SSL Certificate and Key Management*.

3 In the list of settings on the right, go to *Key stores and certificates* under *Additional Properties*.

4 Select *NodeDefaultTrustStore* (or the truststore you are using).

5 Under *Additional Properties* on the right, select *Signer Certificates*.

6 Click *Add*.

7 Type in the Alias name and full path to the certificate file.

8 Change the Data type in the dropdown to *Binary DER data*.

9 Click *OK*. You should now see the certificate in the list of signer certificates.

Importing certificates with the command line

From the command line on the machine hosting the WebSphere server, run the keytool to import the certificate into the WebSphere keystore.

NOTE: You need to use the WebSphere keytool or this does not work. Also, be sure the store type is PKCS12.

The WebSphere keytool can be found at `/IBM/WebSphere/AppServer/java/bin`.

Sample Keytool Command

```
keytool -import -trustcacerts -file servercert.der -alias myserveralias -
keystore trust.p12 -storetype PKCS12
```

If you have more than one `trust.p12` file on your system, you might need to specify the full path to the file.

5.7.15 Deploy the IDM WAR file

1 Log in to the WebSphere administration console as an admin user.

2 From the left panel, go to *Applications* > *Install New Application*

3 Browse to the file location of the IDM War. (The IDM WAR file is configured during the installation of the User Application. It is in the the User Application installation directory that you specified during installation of the User Application.)

4 Type in the Context root for the application, for example `IDMProv`. This will be the URL path.

5 Keep the radio button selected for *Prompt me only when additional information is required.* Then, click *Next* to move to the *Select installation options* page.

6 Accept the defaults for this screen and click *Next* to move to the *Map modules to servers* screen.

7 Leave everything as the defaults for this page and click *Next* to move to the *Map resource references to resources* page.

8 For the authentication method, select the *User default method* check box. Then for the *Authentication data entry* drop-down, select the alias you created earlier, for example `MyServerNode01/MyAlias`.

9 In the table below the authentication settings, find the module you are deploying. Under the column titled `Target Resource JNDI Name` click the browse button to specify a JNDI name. This should bring up a list of resources. Select the datasource that you created earlier and click the *Apply* button to get back to the `Map resource references to resources` page, for example `MyDataSource`.

10 Select *Next* to go to the *Map virtual hosts for Web modules*.

11 Leave everything as the defaults for this page and select *Next* to go to the *Summary* page.

12 Select *Finish* to complete the deployment.

13 After the deployment is finished, click *Save* to save the changes.

14 Continue with Section 5.7.16, “Start the Application,” on page 171.

5.7.16 Start the Application

1 Log in to the WebSphere administrator’s console as an admin user.

2 From the left navigation panel go to *Applications* > *Enterprise Applications*.

3 Select the check box next to the application you want to start. Then, click *Start*.

After starting, the *Application status* column shows a green arrow.

5.7.17 Access the User Application portal

1 Access the portal using the context you specified during deployment. The default port for the Web container on WebSphere is 9080, or 9443 for the secure port. The format for the URL is:

```
http://<server>:9080/IDMProv
```

5.8 Installing the User Application from a Console Interface

This section describes how to install the Identity Manager User Application using the console (command line) version of the installer.

1 Obtain the appropriate installation files described in Table 5-2 on page 113.

2 Log in and open a terminal session.

3 Launch the installer for your platform with Java as described below:

```
java -jar IdmUserApp.jar -i console
```

4 Follow the same steps described for the graphical user interface under Section 5.6, “Installing the User Application on a JBoss Application Server from the Install GUI,” on page 114, reading the prompts at the command line and entering responses at the command line, through the steps on importing or creating the master key.

5 To set the User Application configuration parameters, you must manually launch the configupdate utility. At a command line, enter `configupdate.sh` (Linux or Solaris) or `configupdate.bat` (Windows), and fill in values as described in Section 5.6.14, “Configuring the User Application,” on page 129.

6 If you are using an external password management war, manually copy it to the install directory and to the remote JBoss server deploy directory that runs the external password WAR functionality.

7 Continue with Section 5.10, “Post-Install Tasks,” on page 178.

5.9 Installing the User Application with a Single Command

This section describes how to do a silent install. A silent install requires no interaction during the installation and can save you time, especially when you install on more than one system. Silent install is supported for Linux and Solaris.

1. Obtain the appropriate installation files listed in Table 5-2 on page 113.
2. Log in and open a terminal session.
3. Locate the IDM properties file, `silent.properties`, which is bundled with the installation files. If you are working from a CD, make a local copy of this file.
4. Edit `silent.properties` to supply your installation parameters and User Application configuration parameters.

   See the `silent.properties` file for an example of each installation parameter. The installation parameters correspond to the installation parameters you set in the GUI or Console installation procedures.

   See Table 5-8 on page 172 for a description of each User Application configuration parameter. The User Application configuration parameters are the same ones you can set in the GUI or Console installation procedures or with the configupdate utility.
5. Launch the silent install as follows:

   ```
   java -jar IdmUserApp.jar -i silent -f /yourdirectorypath/silent.properties
   ```

   Type the full path to `silent.properties` if that file is in a different directory from the installer script. The script unpacks the necessary files to a temporary directory and launches the silent install.

Table 5-8 *User Application Configuration Parameters for Silent Install*

User Application Parameter Name in silent.properties	Equivalent Parameter Name in the User Application Configuration Parameters File, and Description
NOVL_CONFIG_LDAPHOST=	eDirectory Connection Settings: LDAP Host. Required. Specify the hostname or IP address for your LDAP server.
NOVL_CONFIG_LDAPADMIN=	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. This value is encrypted, based on the master key.
NOVL_CONFIG_LDAPADMINPASS=	eDirectory Connection Settings: LDAP Administrator Password. Required. Specify the LDAP Administrator password. This password is encrypted, based on the master key.
NOVL_CONFIG_ROOTCONTAINERNAME=	eDirectory DNs: 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.

User Application Parameter Name in silent.properties	Equivalent Parameter Name in the User Application Configuration Parameters File, and Description
NOVL_CONFIG_PROVISIONROOT=	eDirectory DNs: Provisioning Driver DN. Required. Specify the distinguished name of the User Application driver that you created earlier in Section 5.4, “Creating the User Application Driver,” on page 107. For example, if your driver is UserApplicationDriver and your driver set is called myDriverSet, and the driver set is in a context of o=myCompany, you type a value of: `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
NOVL_CONFIG_LOCKSMITH=	eDirectory DNs: User Application Admin. Required. An existing user in the Identity Vault who has the rights to perform administrative tasks for the User Application user container specified. This user can use the *Administration* tab of the User Application to administer the portal. If the User Application Administrator participates in workflow administration tasks exposed in iManager, Novell Designer for Identity Manager, or the User Application (*Requests & Approvals* tab), you must grant this administrator appropriate trustee rights to object instances contained in the User Application driver. Refer to the *IDM User Application: Administration Guide* for details. To change this assignment after you deploy the User Application, you must use the *Administration* > *Security* pages in the User Application.
NOVL_CONFIG_PROVLOCKSMITH=	eDirectory DNs: Provisioning Application Admin. This role is available in the provisioning version of Identity Manager 3.5.1. The Provisioning Application Administrator uses the *Provisioning* tab (under the *Administration* tab) to manage the Provisioning Workflow functions. These functions are available to users through the *Requests and Approvals* tab of the User Application. This user must exist in the Identity Vault prior to being designated the Provisioning Application Administrator. To change this assignment after you deploy the User Application, you must use the *Administration* > *Security* pages in the User Application.

User Application Parameter Name in silent.properties	Equivalent Parameter Name in the User Application Configuration Parameters File, and Description
NOVL_CONFIG_USERCONTAINERDN=	Meta-Directory User Identity: 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 below) 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.
NOVL_CONFIG_GROUPCONTAINERDN=	Meta-Directory User Groups: 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.
NOVL_CONFIG_KEYSTOREPATH=	eDirectory Certificates: Keystore Path. Required. Specify the full path to your keystore (`cacerts`) file of the JRE that the application server application server is using. The User Application installation modifies the keystore file. On Linux or Solaris, the user must have permission to write to this file.
NOVL_CONFIG_KEYSTOREPASSWORD=	eDirectory Certificates: Keystore Password. Required. Specify the `cacerts` password. The default is `changeit`.
NOVL_CONFIG_SECUREADMINCONNECTION=	eDirectory Connection Settings: Secure Admin Connection. Specify True to require that all communication using the admin account be done using a secure socket (this option can have adverse performance implications). This setting allows other operations that don't require SSL to operate without SSL. Specify False if the admin account does not use secure socket communication.
NOVL_CONFIG_SECUREUSERCONNECTION=	eDirectory Connection Settings: Secure User Connection. Specify True to require that all communication done on the logged-in user's account be done using a secure socket (this option can have severe adverse performance implications). This setting allows other operations that don't require SSL to operate without SSL. Specify False if the user’s account does not use secure socket communication.
NOVL_CONFIG_SESSIONTIMEOUT=	Miscellaneous: Session Timeout. Specify an application session timeout interval.

User Application Parameter Name in silent.properties	Equivalent Parameter Name in the User Application Configuration Parameters File, and Description
NOVL_CONFIG_LDAPPLAINPORT=	eDirectory Connection Settings: LDAP Non-Secure Port. Specify the non-secure port for your LDAP server, for example 389.
NOVL_CONFIG_LDAPSECUREPORT=	eDirectory Connection Settings: LDAP Secure Port. Specify the secure port for your LDAP server, for example 636.
NOVL_CONFIG_ANONYMOUS=	eDirectory Connection Settings: Use Public Anonymous Account. Specify True to allow users who are not logged in to access the LDAP Public Anonymous Account. Specify False to enable NOVL_CONFIG_GUEST instead.
NOVL_CONFIG_GUEST=	eDirectory Connection Settings: LDAP Guest. Allows users who are not logged in to access permitted portlets. You must also deselect *Use Public Anonymous Account*. The Guest user account must already exist in the Identity Vault. To disable the Guest user, select *Use Public Anonymous Account*.
NOVL_CONFIG_GUESTPASS=	eDirectory Connection Settings: LDAP Guest Password.
NOVL_CONFIG_EMAILNOTIFYHOST=	Email: Notify Template HOST token. Specify the application server hosting the Identity Manager User Application. For example: `myapplication serverServer` This value replaces the $HOST$ token in e-mail templates. The URL that is constructed is the link to provisioning request tasks and approval notifications.
NOVL_CONFIG_EMAILNOTIFYPORT=	Email: Notify Template Port token. Used to replace the $PORT$ token in e-mail templates used in provisioning request tasks and approval notifications.
NOVL_CONFIG_EMAILNOTIFYSECUREPORT=	Email: Notify Template Secure Port token. Used to replace the $SECURE_PORT$ token in e-mail templates used in provisioning request tasks and approval notifications
NOVL_CONFIG_NOTFSMTPEMAILFROM=	Email: Notification SMTP Email From. Specify e-mail From a user in provisioning e-mail.
NOVL_CONFIG_NOTFSMTPEMAILHOST=	Email: Notification SMTP Email Host. Specify the SMTP e-mail host that provisioninig e-mail is using. This can be an IP address or a DNS name.

User Application Parameter Name in silent.properties	Equivalent Parameter Name in the User Application Configuration Parameters File, and Description
NOVL_CONFIG_USEEXTPWDWAR=	Password Management: Use External Password WAR. Specify True if you are using an external password management WAR. If you specify True, you must also supply values for *NOVL_CONFIG_EXTPWDWARPTH* and *NOVL_CONFIG_EXTPWDWARRTNPATH*. Specify False to use the default internal Password Management functionality, `./jsps/pwdmgt/ForgotPassword.jsf` (without the http(s) protocol at the beginning). This redirects the user to the Forgot Password functionality built into the User Application, rather than to an external WAR.
NOVL_CONFIG_EXTPWDWARPATH=	Password Management: Forgot Password Link. Specify the URL for the Forgot Password functionality page, `ForgotPassword.jsf`, in an external or internal password management WAR. Or, accept the default internal password managment WAR. For details, see "Using Password WARs" on page 141
NOVL_CONFIG_EXTPWDWARRTNPATH=	Password Management: Forgot Password Return Link. If you are using an external password management WAR, supply the path that the external Password Management WAR uses to call back the User Application through Web Services, for example `https://idmhost:sslport/idm`.
NOVL_CONFIG_USEROBJECTATTRIBUTE=	Meta-Directory User Identity: User Object Class. The LDAP user object class (typically inetOrgPerson).
NOVL_CONFIG_LOGINATTRIBUTE=	Meta-Directory User Identity: Login Attribute. The LDAP attribute (for example, CN) that represents the user's login name.
NOVL_CONFIG_NAMINGATTRIBUTE=	Meta-Directory User Identity: Naming Attribute. The LDAP attribute used as the identifier when looking up users or groups. This is not the same as the login attribute, which is used only during login, and not during user/group searches.
NOVL_CONFIG_USERMEMBERSHIPATTRIBUTE=	Meta-Directory User Identity: User Membership Attribute. Optional. The LDAP attribute that represents the user's group membership. Do not use spaces in this name.
NOVL_CONFIG_GROUPOBJECTATTRIBUTE=	Meta-Directory User Groups: Group Object Class. The LDAP group object class (typically groupofNames).
NOVL_CONFIG_GROUPMEMBERSHIPATTRIBUTE=	Meta-Directory User Groups: Group Membership Attribute. Specify the attribute representing the user's group membership. Do not use spaces in this name.

User Application Parameter Name in silent.properties	Equivalent Parameter Name in the User Application Configuration Parameters File, and Description
NOVL_CONFIG_USEDYNAMICGROUPS=	Meta-Directory User Groups: Use Dynamic Groups. Specify True to use dynamic groups. Otherwise, specify False.
NOVL_CONFIG_DYNAMICGROUPOBJECTCLASS=	Meta-Directory User Groups: Dynamic Group Object Class. Specify the LDAP dynamic group object class (typically dynamicGroup).
NOVL_CONFIG_PRIVATESTOREPATH=	Private Key Store: Private Keystore Path. Specify the path to the private keystore that contains the User Application's private key and certificates. Reserved. If you leave this empty, this path is `/jre/lib/security/cacerts` by default.
NOVL_CONFIG_PRIVATESTOREPASSWORD=	Private Key Store: Private Keystore Password.
NOVL_CONFIG_PRIVATEKEYALIAS=	Private Key Store: Private Key Alias. This alias is `novellIDMUserApp` unless you specify otherwise.
NOVL_CONFIG_PRIVATEKEYPASSWORD=	Private Key Store: Private Key Password.
NOVL_CONFIG_TRUSTEDSTOREPATH=	Trusted Key Store: Trusted Store Path. The Trusted Key Store contains all trusted signers' certificates used to validate digital signatures. If this path is empty, the User Application gets the path from System property `javax.net.ssl.trustStore`. If the path isn't there, it is assumed to be `jre/lib/security/cacerts`.
NOVL_CONFIG_TRUSTEDSTOREPASSWORD=	Trusted Key Store: Trusted Store Password.
NOVL_CONFIG_AUDITCERT=	Novell Audit Digital Signature Certificate
NOVL_CONFIG_AUDITKEYFILEPATH=	Novell Audit Digital Signature Private Key File path.
NOVL_CONFIG_ICSLOGOUTENABLED=	iChain Settings: ICS Logout Enabled. Specify True to enable simultaneous logout of the User Application and either iChain or Novell Access Manager. The User Application checks for an iChain or Novell Access Manager cookie on logout and, if the cookie is present, reroutes the user to the ICS logout page. Specify False to disable simultaneous logout.
NOVL_CONFIG_ICSLOGOUTPAGE=	iChain Settings: ICS Logout Page. Specify the URL to the iChain or Novell Access Manager logout page, where the URL is a hostname that iChain or Novell Access Manager expects. If ICS logging is enabled and a user logs out of the User Application, the user is rerouted to this page.
NOVL_CONFIG_EMAILNOTIFYPROTOCOL=	Email: Notify Template PROTOCOL token. Refers to a non-secure protocol, HTTP. Used to replace the $PROTOCOL$ token in e-mail templates used in provisioning request tasks and approval notifications.

User Application Parameter Name in silent.properties	Equivalent Parameter Name in the User Application Configuration Parameters File, and Description
NOVL_CONFIG_EMAILNOTIFYSECUREPROTOCOL=	Email: Notify Template Secure Port token.
NOVL_CONFIG_OCSPURI=	Miscellaneous: OCSP URI. If the client installation uses the On-Line Certificate Status Protocol (OCSP), supply a Uniform Resource Identifier (URI). For example, the format is http://hstport/ocspLocal. The OCSP URI updates the status of trusted certificates online.
NOVL_CONFIG_AUTHCONFIGPATH=	Miscellaneous: Authorization Config Path. The fully qualified name of the authorization configuration file.

5.10 Post-Install Tasks

After you install and configure the User Application, take care of the post-installation tasks.

5.10.1 Recording the Master Key

Immediately after installation, copy the encrypted master key and record it in a safe place.

1. Open the `master-key.txt` file in the installation directory.
2. Copy the encrypted master key to a safe place that is accessible in event of system failure.

WARNING: Always keep a copy of the encrypted master key. You need the encrypted master key to regain access to encrypted data if the master key is lost, for example because of equipment failure.

If this installation is on the first member of a cluster, use this encrypted master key when installing the User Application on other members of the cluster.

For more information on the master key, see the *Identity Manager User Application: Administration Guide* (http://www.novell.com/documentation/idm35/index.html) sections on *Encryption of Sensitive User Application Data* and *Clustering JBoss*.

5.10.2 Checking Your Cluster Installations

Check your cluster installations. Ensure that each JBoss server in a JBoss cluster has

- A unique partition name (partition name)
- A unique partition UDP (partition.udpGroup)
- A unique Workflow Engine ID
- The same (identical) WAR file. The WAR is written by the installation to the `jboss\server\IDM\deploy` directory by default.

Ensure that each server in a WebSphere cluster has a unique Workflow Engine ID.

For more information, see the section on Clustering in Chapter 4 of the *Identity Manager User Application: Administration Guide* (http://www.novell.com/documentation/idm35/index.html)

5.10.3 Configuring SSL Communication Between JBoss Servers

If you select *Use External Password WAR* in the User Application configuration file during installation, you must configure SSL communication between the JBoss servers on which you are deploying the User Application WAR and the `IDMPwdMgt.war` file. Refer to your JBoss documentation for directions.

5.10.4 Accessing the External Password WAR

If you have an external password WAR and want to test the Forgot Password functionality by accessing it, you can access it:

- Directly, in a browser. Go to the Forgot Password page in the external password WAR, for example `http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf`.
- Or, at the User Application login page, click the *Forgot Password* link.

5.10.5 Updating Forgot Password Settings

You can change the values of *Forgot Password Link* and *Forgot Password Return Link* after installation. Use either the configupdate utility or the User Application.

To use the configupdate utility. At a command line, change directories to the install directory and enter `configupdate.sh` (Linux or Solaris) or `configupdate.bat` (Windows). If you are creating or editing an external password management WAR, you must then manually rename that WAR before you copy it to the remote JBoss server.

To use the User Application. Log in as the User Application Administrator and go to *Administration* > *Application Configuration* > *Password Module Setup* > *Login*. Modify these fields:

- *Forgot Password Link* (for example: `http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf`)
- *Forgot Password Return Link* (for example: `https://idmhost:sslport/idm`)

5.10.6 Setting Up E-Mail Notification

To implement Forgot Password and Workflow e-mail notification capabilities:

1. In iManager, under Roles and Tasks, select Workflow Administration, then select *Email Server Options*.
2. Specify your SMTP server name under *Host Name*.
3. Next to *From*, specify an e-mail address (for example, *noreply@novell.com*), then click *OK*.

5.10.7 Testing the Installation on the JBoss Application Server

1. Start your database. Refer to your database documentation for directions.
2. Start the User Application server (JBoss). At the command line, make the installation directory your working directory and execute the following script (provided by the User Application installation):

   `start-jboss.sh` (Linux and Solaris)

   `start-jboss.bat` (Windows)

   If you need to stop the application server, use `stop-jboss.sh` or `stop-jboss.bat`, or close the window in which `start-jboss.sh` or `start-jboss.bat` is running.
3. Start the User Application driver. This enables communication to the User Application driver.
   - **3a** Log into iManager.
   - **3b** In the Roles and Tasks display in the left navigation frame, select *Identity Manager Overview* under *Identity Manager*.
   - **3c** In the content view that appears, specify the driver set that contains the User Application driver, then click *Search*. A graphic appears, showing the driver set with its associated drivers.
   - **3d** Click the red and white icon on the driver.
   - **3e** Select *Start Driver*. The driver status changes to the yin-yang symbol, indicating that the driver is now started.

     The driver, upon starting, attempts a "handshake" with the User Application. If your application server isn't running or if the WAR wasn't successfully deployed, the driver returns an error.
4. To launch and log in to the User Application, use your Web browser to go to

   http://*hostname*:*port*/*ApplicationName*

   Where *hostname*:*port* is the application server hostname (for example, myserver.domain.com) and the port is your application server's port (for example, 8080 by default on JBoss). *ApplicationName* is IDM by default. You specified the application name during the install when you provided application server configuration information.

   The Novell Identity Manager User Application landing page should appear.
5. In the upper right corner of that page, click *Login* to log in to the User Application.

If the Identity Manager User Application page does not appear in your browser after completing these steps, check the terminal console for error messages and refer to Section 5.12, "Troubleshooting," on page 181.

5.10.8 Setting Up Your Provisioning Team and Requests

Set up your Provisioning Team and Provisioning Team Requests to enable workflow tasks. For directions, see the *Identity Manager 3.5.1 User Application: Administration Guide* (http://www.novell.com/documentation/idm35/index.html).

5.10.9 Creating Indexes in eDirectory

For improved performance of the IDM User Application, the eDirectory Administrator must create indexes for the manager, ismanager and srvprvUUID attributes. Without indexes on these attributes, User Application users can experience impeded performance of the User Application, particularly in a clustered environment. Refer to the *Novell eDirectory Administration Guide* (http://www.novell.com/documentation) for directions on using Index Manager to create indexes.

5.11 Reconfiguring the IDM WAR file after installation

To update your IDM WAR file:

1. Run the ConfigUpdate utility in the User Application install directory by executing `configupdate.sh` or `configupdate.bat`. This allows you to update the WAR file in the install directory.

   For information on ConfigUpdate utility parameters, see Section 5.6.14, "Configuring the User Application," on page 129 or Section 5.7.10, "Configuring the User Application," on page 154.
2. Deploy the new WAR file to your application server.

5.12 Troubleshooting

Your Novell representative will work through any setup and configuration problems with you. In the meantime, here are a few things to try if you encounter problems.

Issue	Suggested Actions

You want to modify the User Application configuration settings made during installation. This includes configuration of such things as:
◆ Identity Vault connections and certificates
◆ E-mail settings
◆ Metadirectory User Identity, User Groups
◆ iChain settings
	You can run the configuration utility independent of the installer.
	On Linux and Solaris, run the following command from the installation directory (by default, `/opt/novell/idm`):
	`configupdate.sh`
	On Windows, run the following command from the installation directory (by default, `c:\opt\novell\idm`):
	`configupdate.bat`

Issue	Suggested Actions
Exceptions are thrown when application server starts up, with a log message `port 8080 already in use`.	Shut down any instances of Tomcat (or other server software) that might already be running. If you decide to reconfigure the application server to use a port other than 8080, remember to edit the `config` settings for the User Application driver in iManager.
When the application server starts, you see a message that no trusted certificates were found.	Make sure that you start application server using the JDK specified in the installation of the User Application.
You can't log into the portal admin page.	Make sure that the User Application Administrator account exists. Don't confuse this with your iManager admin account. They are two different admin objects (or should be).
You can log in as admin, but you 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 Administrator's rights equivalent to the LDAP Administrator's rights (using iManager).
When starting the application server, there are MySQL connection errors.	Don't run as `root`. (This issue is unlikely, however, if you are running the version of MySQL supplied with IDM.) Make sure MySQL is running (and that the correct copy is running). Kill any other instances of MySQL. Run `/idm/mysql/start-mysql.sh`, then `/idm/start-jboss.sh`. Examine `/idm/mysql/setup-mysql.sh` in a text editor and correct any values that appear suspicious. Then run the script, and run `/idm/start-jboss.sh`.
You encounter keystore errors when starting the application server.	Your application server is not using the JDK specified at the installation of the User Application. Use the `keytool` command to import the certificate file: `keytool -import -trustcacerts -alias` *`aliasName`* `-file` *`certFile`* `-keystore ..\lib\security\cacerts -storepass changeit` ◆ Replace *aliasName* with a unique name of your choice for this certificate. ◆ Replace *certFile* with the full path and name of your certificate file. ◆ The default keystore password is `changeit` (if you have a different password, specify it).

Issue	Suggested Actions

E-mail notification was not sent.	Run the configupdate utility to check whether you supplied values for the following User Application configuration parameters: E-Mail From and E-Mail Host.
	
	On Linux or Solaris, run this command from the installation directory (by default, `/opt/novell/idm`):
	
	`configupdate.sh`
	
	On Windows, run this command from the installation directory (by default, `c:\opt\novell\idm`):
	
	`configupdate.bat`

Activating Novell Identity Manager Products

6

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

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

- Purchasing an Identity Manager Product License
- Activating Identity Manager Products by Using a Credential
- Installing a Product Activation Credential
- Viewing Product Activations for Identity Manager and for 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/identitymanager//howtobuy.html)

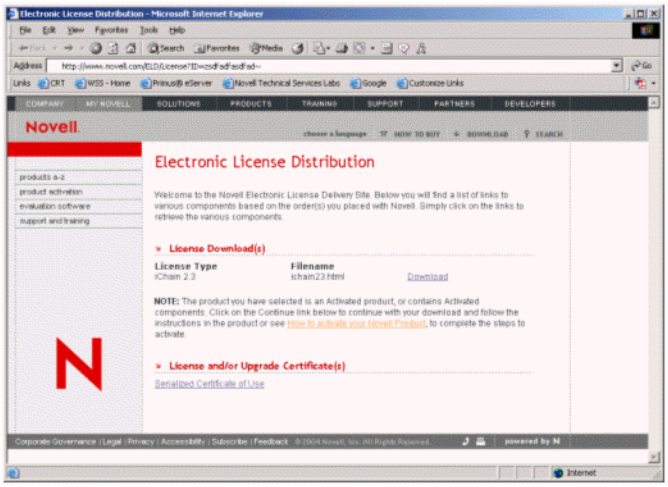
After you purchase a product license, Novell sends you a Customer ID via e-mail. The e-mail also contains a URL to the Novell site where you can obtain a credential. If you do not remember or do not receive your Customer ID, call the Novell Activation Center at 1-800-418-8373 in the U.S. In all other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

6.2 Activating Identity Manager Products by Using a Credential

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

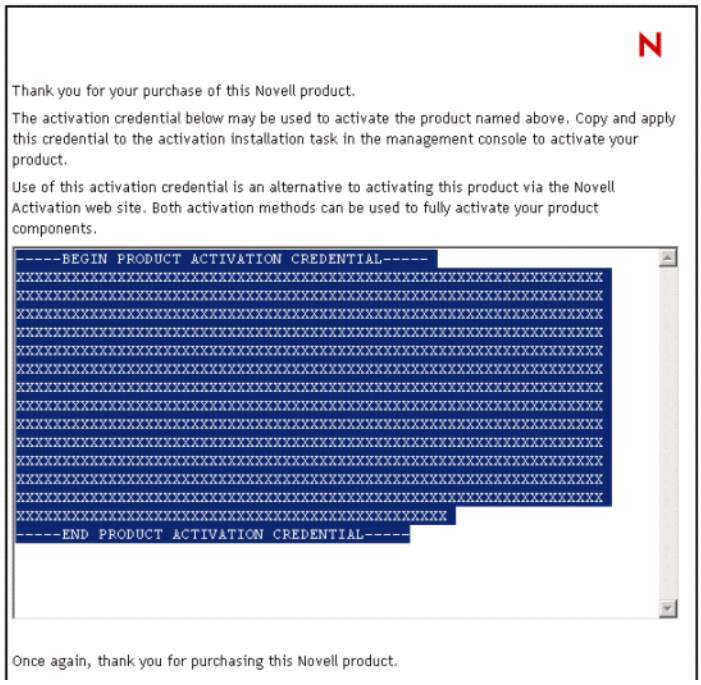
IMPORTANT: The e-mail is not required to activate the product. If the e-mail was sent to someone else within your company, contact the Novell Activation Center for more information.

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



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

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



3 Proceed to Section 6.3, “Installing a Product Activation Credential,” on page 186 for instructions on how to activate Identity Manager components.

6.3 Installing a Product Activation Credential

You should install the Product Activation Credential via iManager.

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

2 Do one of the following:

- Save the Product Activation Credential file.

  or

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

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

3 Open iManager.

4 Choose *Identity Manager > Identity Manager Overview*.

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

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

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

8 Do one of the following:

- Specify where you saved the Identity Manager Activation Credential, then click *Next*.

  or

- Paste the contents of the Identity Manager Activation Credential into the text area, then click *Next*.

9 Click *Finish*.

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

6.4 Viewing Product Activations for Identity Manager and for 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 In the object name field, specify the name of the driver set or the driver you want to view activation information.

  or

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

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.

Documentation Updates

A

The documentation was updated on the following dates:

- Section A.1, “September 15, 2008,” on page 189

A.1 September 15, 2008

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

A.1.1 System Requirements for Identity Manager

Location	Change
Section 1.5.1, “Supported Platforms for Identity Manager 3.5.1 with eDirectory 8.8 Support Pack 5 (8.8.5),” on page 35	Added this section which lists the supported platforms for Identity Manager 3.5.1 with eDirectory 8.8 Support Pack 5 (8.8.5).