

Novell Identity Manager Roles Based Provisioning Module

3.6

www.novell.com

February 22, 2008

USER APPLICATION: INSTALLATION
GUIDE



Novell®

Legal Notices

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

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

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

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

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

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

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

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide	7
1 Overview	9
1.1 Overview of the Installation	9
1.2 About the Installer Program	10
1.3 System Requirements	10
2 Prerequisites to Installation	19
2.1 The Java Development Kit	19
2.2 Installing the Identity Manager Metadirectory	20
2.3 Installing the JBoss Application Server	20
2.3.1 Installing the JBoss Application Server and the MySQL Database	20
2.3.2 Installing the JBoss Application Server as a Service or a Daemon	23
2.4 Installing the WebSphere Application Server	24
2.5 Databases	24
2.5.1 Installing MySQL	24
2.5.2 Configuring Your MySQL Database	24
2.6 Downloading the Product	26
2.7 Installing the Contents of the prerequisitefiles.zip File	27
2.7.1 Extending the eDirectory Schema for Roles Based Provisioning Module Version 3.627	
2.7.2 Copying the JAR File for the Role Service Driver	28
2.7.3 Copying the Role Service Driver Configuration File	29
2.7.4 Copying the User Application Driver Configuration File	29
2.7.5 Copying the dirxml.lsc File	30
2.8 Installing the iManager Icons for Roles	30
3 Creating Drivers	31
3.1 Creating the User Application Driver in iManager	31
3.2 Creating the Role Service Driver in iManager	35
4 Installing on JBoss Using a GUI	37
4.1 Launching the Installer GUI	37
4.2 Choosing an Application Server Platform	38
4.3 Migrating Your Database	39
4.4 Specifying the Location of the WAR	41
4.5 Choosing an Install Folder	42
4.6 Choosing a Database Platform	44
4.7 Specifying the Database Host and Port	46
4.8 Specifying the Database Name and Privileged User	47
4.9 Specifying the Java Root Directory	48
4.10 Specifying the JBoss Application Server Settings	48
4.11 Choosing the Application Server Configuration Type	50
4.12 Enabling Novell Audit Logging	51
4.13 Specifying a Master Key	52
4.14 Configuring the User Application	53

4.15	Using Password WARs	66
4.15.1	Specifying an External Password Management WAR	66
4.15.2	Specifying an Internal Password WAR	67
4.16	Verify Choices and Install	67
4.17	View Log Files	67
5	Installing from the Console or With a Single Command	69
5.1	Installing the User Application from the Console	69
5.2	Installing the User Application with a Single Command	69
6	Installing on a WebSphere Application Server	79
6.1	Launching the Installer GUI	79
6.2	Choosing an Application Server Platform	80
6.3	Specifying the Location of the WAR	81
6.4	Choosing an Install Folder	83
6.5	Choosing a Database Platform	84
6.6	Specifying the Java Root Directory	86
6.7	Enabling Novell Audit Logging	87
6.8	Specifying a Master Key	88
6.9	Configuring the User Application	89
6.10	Verify Choices and Install	103
6.11	View Log Files	104
6.12	Adding User Application Configuration Files and JVM System Properties	104
6.13	Import the eDirectory Trusted Root to the WebSphere Keystore	105
6.13.1	Importing Certificates with the WebSphere Administrator's Console	105
6.13.2	Importing Certificates with the Command Line	106
6.14	Deploying the IDM WAR File	106
6.15	Starting the Application	107
6.16	Accessing the User Application Portal	107
7	Post-Installation Tasks	109
7.1	Recording the Master Key	109
7.2	Post-Installation Configuration	109
7.3	Checking Your Cluster Installations	109
7.4	Configuring SSL Communication between JBoss Servers	110
7.5	Accessing the External Password WAR	110
7.6	Updating Forgot Password Settings	110
7.7	Setting Up E-Mail Notification	111
7.8	Testing the Installation on the JBoss Application Server	111
7.9	Setting Up Your Provisioning Team and Requests	112
7.10	Creating Indexes in eDirectory	112
7.11	Reconfiguring the IDM WAR File after Installation	112
7.12	Troubleshooting	112

About This Guide

The Novell® Identity Manager Roles Based Provisioning Module 3.6 comprises an Identity Manager User Application with roles-based provisioning. This guide describes how to install the Novell Identity Manager Roles Based Provisioning Module 3.6. Sections include:

- ♦ Chapter 1, “Overview,” on page 9
- ♦ Chapter 2, “Prerequisites to Installation,” on page 19
- ♦ Chapter 3, “Creating Drivers,” on page 31
- ♦ Chapter 4, “Installing on JBoss Using a GUI,” on page 37
- ♦ Chapter 5, “Installing from the Console or With a Single Command,” on page 69
- ♦ Chapter 6, “Installing on a WebSphere Application Server,” on page 79
- ♦ Chapter 7, “Post-Installation Tasks,” on page 109

Audience

This guide is intended for administrators and consultants who will plan and implement the Identity Manager Roles Based Provisioning Module.

Feedback

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

Additional Documentation

For additional documentation on the Identity Manager Roles Based Provisioning Module, see the [Identity Manager Documentation Web site \(http://www.novell.com/documentation/lg/dirxml/drivers/index.html\)](http://www.novell.com/documentation/lg/dirxml/drivers/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.

This section outlines the installation and describes system requirements. Topics include:

- ♦ [Section 1.1, “Overview of the Installation,” on page 9](#)
- ♦ [Section 1.2, “About the Installer Program,” on page 10](#)
- ♦ [Section 1.3, “System Requirements,” on page 10](#)

1.1 Overview of the Installation

The installation procedure for the Novell® Identity Manager Roles Based Provisioning Module 3.6 installs both a User Application that supports roles and the Roles Based Provisioning Module. Installation includes the following steps:

- 1 If you are migrating to the Identity Manager Roles Based Provisioning Module, please refer to the *Identity Manager User Application: Migration Guide* (<http://www.novell.com/documentation/idmrpbm36/pdfdoc/migration/migration.pdf>).
- 2 Ensure that you are meeting system requirements. See [Section 1.3, “System Requirements,” on page 10](#).
- 3 Install the Identity Manager metadirectory. For directions, refer to the *Identity Manager 3.5.1 Installation Guide* (<http://www.novell.com/documentation/idm35/pdfdoc/install/install.pdf>). The Identity Manager metadirectory server must be installed before you can create the required drivers and install the User Application and Roles Based Provisioning Module.
- 4 Satisfy the prerequisites to installation. See [Chapter 2, “Prerequisites to Installation,” on page 19](#).
- 5 In your download directory, find and unzip the `prerequisitefiles.zip` file. Manually install or apply the unzipped files.
- 6 If you will use Designer to create and configure drivers, install Designer 2.1.1. See [“Installing Designer.”](#) (http://www.novell.com/documentation/designer21/admin_guide/index.html?page=/documentation/designer21/admin_guide/data/ginstall.html).
- 7 Create the User Application Driver in iManager or Designer 2.1.1. Directions for creating the driver in iManager are in [Section 3.1, “Creating the User Application Driver in iManager,” on page 31](#).
The User Application driver must already exist (but not be turned on) before you install the Novell Identity Manager User Application and Roles Based Provisioning Module.
- 8 Create the Role Service Driver in iManager or Designer 2.1.1. Directions for creating the driver in iManager are at [Section 3.2, “Creating the Role Service Driver in iManager,” on page 35](#).
The Role Service Driver must already exist (but not be turned on) before you install the Novell Identity Manager User Application and Roles Based Provisioning Module.
- 9 Install and configure the Novell Identity Manager User Application and Roles Based Provisioning Module. See:
 - ♦ [Chapter 4, “Installing on JBoss Using a GUI,” on page 37](#)
 - ♦ [Chapter 5, “Installing from the Console or With a Single Command,” on page 69](#)
 - ♦ [Chapter 6, “Installing on a WebSphere Application Server,” on page 79](#)

NOTE: If you are using WebSphere*, you must manually deploy the WAR file.

10 Carry out post-installation tasks.

1.2 About the Installer 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*, DB2*, 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 Application Server. On WebSphere, you must manually deploy the WAR.
- ◆ Enables Novell Audit logging if you select to do so.
- ◆ Enables you to import an existing master key to restore a specific Roles Based Provisioning Module installation and to support clusters.

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

- ◆ Graphical user interface. See [Chapter 4, "Installing on JBoss Using a GUI," on page 37](#) or [Chapter 6, "Installing on a WebSphere Application Server," on page 79](#).
- ◆ Console (command line) interface. See [Section 5.1, "Installing the User Application from the Console," on page 69](#).
- ◆ Silent install. See [Section 5.2, "Installing the User Application with a Single Command," on page 69](#).

1.3 System Requirements

To use the Novell Identity Manager Roles Based Provisioning Module 3.6, you must have one of each of the required components listed in [Table 1-1](#).

Table 1-1 System Requirements

Required System Component	System Requirements	Notes
Metadirectory System (Identity Manager 3.5.1)	One of the following operating systems:	Using VMware* in your implementation is supported if you use a Metadirectory system platform.
<ul style="list-style-type: none"> ◆ Metadirectory engine ◆ Novell Audit agent ◆ Service drivers ◆ Identity Manager drivers ◆ Utilities (including Application Tools, and the Novell Audit Setup tool) 	<ul style="list-style-type: none"> ◆ Netware® 6.5 SP6 ◆ Novell Open Enterprise Server (OES) 1.0 with the latest Support Pack ◆ Novell Open Enterprise Server (OES) 2.0 ◆ Windows* 2000 Server with the latest Service Pack (32-bit) ◆ Windows Server 2003 with the latest Service Pack (32-bit) ◆ Linux Red Hat 3.0, 4.0, or 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 or 5.3 	<p>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:</p> <ul style="list-style-type: none"> ◆ Intel* x86-32 ◆ AMD* x86-32 ◆ Intel EM64T ◆ AMD Athlon64* and Opteron*
	One of the following versions of eDirectory™:	Identity Manager supports these features of eDirectory 8.8:
	<ul style="list-style-type: none"> ◆ eDirectory 8.7.3.10 ◆ eDirectory 8.8.1 or 8.8.2 	<ul style="list-style-type: none"> ◆ Multiple instances of eDirectory on the same server ◆ Encrypted attributes
	Security Services 2.0.5 (NMASTM 3.1.3)	<p>eDirectory 8.8 supports 64-bit Red Hat Linux 4.0.</p> <p>A 64-bit version of Password Synchronization on Windows Server 2003 is available.</p> <p>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.</p> <p>Xen* virtualization is now supported on SUSE Linux Enterprise Server 10 when the Xen Virtual Machine (VM) is running SLES 10 as the guest operating system in paravirtualized mode. 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=52670386&stated=1%20%204926187)).</p>

Required System Component	System Requirements	Notes
<p>Web-based Administration Server</p> <ul style="list-style-type: none"> ◆ Password synch ◆ iManager 2.6 and plug-ins ◆ iManager 2.7 and plug-ins ◆ Driver configurations 	<p>One of the following operating systems:</p> <ul style="list-style-type: none"> ◆ 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, or 5.0 ES or AS (both 32-bit and 64-bit are supported) ◆ Solaris* 9 or 10 with latest support pack ◆ SUSE Linux Enterprise Server 9 or 10 with the latest Support Pack (both 32-bit and 64-bit are supported) <p>Operating systems supported via iManager Workstation:</p> <ul style="list-style-type: none"> ◆ Windows 2000 Professional with latest Service Pack ◆ Windows XP with SP2 ◆ SUSE Linux Enterprise Desktop 10 ◆ SUSE Linux 10.1 <p>The following software:</p> <ul style="list-style-type: none"> ◆ Novell iManager 2.6 or 2.7 with the latest support pack and plug-ins 	<p>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:</p> <ul style="list-style-type: none"> ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 and Opteron ◆ Browser support is determined by iManager 2.6. This list presently includes: <ul style="list-style-type: none"> ◆ 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. ◆ Only the Password Synchronization agent is supported on 64-bit Windows 2003.

Required System Component	System Requirements	Notes
<p>Secure Logging Service</p> <ul style="list-style-type: none"> ◆ The Secure Logging Server ◆ The Platform Agent (client component) ◆ Novell Audit 2.0.2 or Sentinel™ 5.1.3 	<p>For the Secure Logging Server, one of the following operating systems:</p> <ul style="list-style-type: none"> ◆ Novell Open Enterprise Server (OES) 1.0 or 2.0 with the latest Support Pack ◆ NetWare 6.5 with the latest Support Pack ◆ Windows 2000 Server with the latest Service Pack (32-bit) ◆ Windows Server 2003 with the latest Service Pack (32-bit) ◆ Linux Red Hat Linux 3.0, 4.0, or 5.0 ES or AS (32-bit or 64-bit, although Novell Audit runs only in 32-bit mode) ◆ Solaris 9 or 10 with latest support pack ◆ SUSE Linux Enterprise Server 9 or 10 with the latest Support Pack (32-bit and 64-bit, although Novell Audit runs only 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) <p>For the Platform Agent, one of the following operating systems:</p> <ul style="list-style-type: none"> ◆ 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 or ES (32-bit or 64-bit, although Novell Audit runs only in 32-bit mode) ◆ Solaris 8, 9, or 10 ◆ SUSE Linux Enterprise Server 9 or 10 (32-bit and 64-bit, although Novell Audit runs only in 32-bit mode) <p>iManager 2.6 or 2.7 with the latest Support Pack and plug-ins</p>	<p>OES, NetWare, Windows, and Linux platforms (Red Hat and SUSE) support all of the following processors in 32-bit mode:</p> <ul style="list-style-type: none"> ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 and Opteron <p>Minimum Secure Server requirements include:</p> <ul style="list-style-type: none"> ◆ A single processor, server-class PC with a Pentium II 400 MHz ◆ A minimum of 40 MB disk space ◆ 512 MB RAM <p>The eDirectory Instrumentation, which allows eDirectory events to be logged, supports the following versions of eDirectory:</p> <ul style="list-style-type: none"> ◆ eDirectory 8.7.3 (NetWare, Windows, Linux, and Solaris) ◆ eDirectory 8.8 with latest support pack <p>The NetWare Instrumentation, which allows NetWare events to be logged, supports the following versions of NetWare:</p> <ul style="list-style-type: none"> ◆ NetWare 5.1 with the latest Support Pack ◆ NetWare 6.0 with the latest Support Pack ◆ NetWare 6.5 or NetWare 6.5 with the latest Support Pack ◆ Novell Open Enterprise Server (OES) with the latest Support Pack

Required System Component	System Requirements	Notes
User Application Application Server	<p>The User Application runs on JBoss* and WebSphere, as described below.</p> <p>The User Application with JBoss 4.2.0 GA requires JRE* 1.5.0_14 and is supported on:</p> <ul style="list-style-type: none"> ◆ 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) or 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 <p>The User Application on WebSphere 6.1 requires the IBM JDK and is supported on these platforms:</p> <ul style="list-style-type: none"> ◆ Solaris 10 (64-bit) ◆ Windows 2003 SP1 	<p>SUSE Linux Enterprise Server supports the following processors in 32-bit mode:</p> <ul style="list-style-type: none"> ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 and Opteron <p>SUSE Linux Enterprise Server will run in 64-bit mode on the following processors:</p> <ul style="list-style-type: none"> ◆ Intel EM64T ◆ AMD Athlon64 ◆ AMD Opteron ◆ Sun* SPARC* <p>Xen* virtualization is now supported on SUSE Linux Enterprise Server 10 when the Xen Virtual Machine (VM) is running SLES 10 as the guest operating system in paravirtualized mode. A Xen patch for SLES 10 is needed (see TID # (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3915180&sliceId=SAL_Public&dialogID=52670386&stated=1%20%204926187)).</p>

Required System Component	System Requirements	Notes
User Application Browser	<p>The User Application supports both Firefox and Internet Explorer, as described below.</p> <p>Firefox 2 is supported on:</p> <ul style="list-style-type: none"> ◆ 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 <p>Internet Explorer 7 is supported on:</p> <ul style="list-style-type: none"> ◆ Windows 2000 Professional with SP4 ◆ Windows XP with SP2 ◆ Windows Vista Enterprise Version 6 <p>Internet Explorer 6 SP1 is supported on:</p> <ul style="list-style-type: none"> ◆ Windows 2000 Professional with SP4 ◆ Windows XP with SP2 	
Database Server for the User Application <ul style="list-style-type: none"> ◆ MySQL ◆ Oracle ◆ MS SQL ◆ DB2 	<p>The following databases are supported with JBoss:</p> <ul style="list-style-type: none"> ◆ MySQL Version 5.0.27 ◆ Oracle 9i (9.2.0.1.4) ◆ Oracle 10g Release 2 (10.2.0.1.0) ◆ MS SQL 2005 SP1 <p>The following databases are supported with WebSphere:</p> <ul style="list-style-type: none"> ◆ Oracle 10g Release 2 (10.2.0) ◆ MS SQL 2005 SP1 ◆ DB2 DV2 v9.1.0.0 	<p>The User Application uses a database for various tasks such as storing configuration data and storing data for any in-progress workflow activities.</p> <p>Both the secure logging service and the User Application and workflow provisioning require a database. You can set up one database to serve both applications, or you can set up independent databases for each one. The Secure logging service does not include a specific database.</p> <p>Oracle is supported with both the thin client driver and the OCI client driver.</p>

Required System Component	System Requirements	Notes
Workstations	Designer has been tested on the following platforms:	Designer uses Eclipse as its development platform. Refer to the Eclipse Web site (http://www.eclipse.org) for platform-specific information.
<ul style="list-style-type: none"> ◆ Designer 2.1.1 for Identity Manager 3.5.1 	Windows:	Designer minimum and recommended hardware requirements:
<ul style="list-style-type: none"> ◆ iManager Web access 	<ul style="list-style-type: none"> ◆ Windows 2000 Professional with the latest Service Pack ◆ Windows XP SP2 ◆ Microsoft Windows Vista 	<ul style="list-style-type: none"> ◆ 1 GHz minimum; recommended 2 GHz or greater ◆ 512 MB RAM minimum; recommended 1 GB RAM or greater ◆ 1024 x 768 resolution minimum; recommended 1280 x 1024
	Linux:	Prerequisite software:
	<ul style="list-style-type: none"> ◆ SUSE Linux Enterprise Server 10 (for Designer only) ◆ SUSE Linux 10.1 ◆ SUSE Linux Enterprise Desktop 10 ◆ Red Hat Enterprise LinuxWS 4.0 (for Designer only), Gnome* default ◆ Red Hat Fedora Core 5 (for Designer only), Gnome default ◆ Novell Linux Desktop 9, KDE default 	<ul style="list-style-type: none"> ◆ Microsoft Internet Explorer 6.0 SP1 ◆ Microsoft Internet Explorer 7 ◆ or Mozilla* Firefox 2.0

Required System Component	System Requirements	Notes
<p>Connected System Server (host on a separate server running Remote Loader)</p> <ul style="list-style-type: none"> ◆ Remote Loader ◆ Remote Loader configuration tool (Windows only) ◆ Novell Audit agent ◆ Password Synchronization agent ◆ Driver shim for the connected system ◆ Tools for the connected system 	<p>Each driver requires that the connected system be available and the relevant APIs are provided.</p> <p>Refer to the Identity Manager Driver documentation (http://www.novell.com/documentation/idm35drivers) for operating system and connected system requirements that are specific to each system.</p>	<p>Each connected application requires individuals with application-specific knowledge and responsibility.</p> <p>Remote Loader System:</p> <ul style="list-style-type: none"> ◆ Windows NT* 4.0, Windows 2000 Server, or Windows Server 2003 with latest Support Packs ◆ Windows Server* 2003 (64-bit) with the latest Service Pack ◆ Password Synchronization agent is supported on Windows Server 2003 (64-bit) ◆ Red Hat Linux 3.0, 4.0, or 5.0 ES or AS ◆ SUSE Linux Enterprise Server9 or 10 ◆ AIX 5.2L, version 5.2 or 5.3 <p>Java Remote Loader System:</p> <ul style="list-style-type: none"> ◆ HP-UX* 11i ◆ OS/400 ◆ xOS* ◆ You should be able to use it on any system that has JVM 1.4.2 or higher
Audit	Novell Audit 2.0.2	
User Application SSO integration	Requires Novell Access Manager 3.0.1.	Includes a version of saslsaml.jar built with JDK*1.5.

Prerequisites to Installation

This section describes prerequisites to installing the Identity Manager Roles Based Provisioning Module. Topics include:

- ♦ [Section 2.1, “The Java Development Kit,” on page 19](#)
- ♦ [Section 2.2, “Installing the Identity Manager Metadirectory,” on page 20](#)
- ♦ [Section 2.3, “Installing the JBoss Application Server,” on page 20](#)
- ♦ [Section 2.4, “Installing the WebSphere Application Server,” on page 24](#)
- ♦ [Section 2.5, “Databases,” on page 24](#)
- ♦ [Section 2.6, “Downloading the Product,” on page 26](#)
- ♦ [Section 2.7, “Installing the Contents of the prerequisitefiles.zip File,” on page 27](#)
- ♦ [Section 2.8, “Installing the iManager Icons for Roles,” on page 30](#)

2.1 The Java Development Kit

JBoss, WebSphere, and the Identity Vault have individual Java Development Kit requirements.

JBoss Application Servers: On JBoss Application Servers, use the Java 2 Platform Standard Edition Development Kit version 1.5.0_14.

Use this version of the Sun JDK to start the Roles Based Provisioning Module installer as follows:

Linux/Solaris:

```
$ /opt/jdk1.5.0_14/bin/java -jar IdmUserApp.jar
```

Windows:

```
C:\Novell\InstallFiles\> "C:\Program  
Files\Java\jdk1.5.0_14\bin\java.exe" -jar IdmUserApp.jar
```

When the installation procedure asks for the full path of your Java installation, provide the root path of the Sun JDK. For example, the root path on Linux could be

```
/opt/jdk1.5.0_14
```

NOTE: SLES users: Do not use the IBM JDK that comes with SLES. This version is incompatible with some aspects of the installation.

WebSphere Application Servers: On WebSphere* Application Servers, use the IBM JDK that comes with the WebSphere Application Server 6.1. Apply the unrestricted policy files. The minimum fixpack level required is 6.1.0.9.

Identity Vault (Metadirectory) installer: The Identity Vault (Metadirectory) installer installs its own copy of the JVM on all platforms except NetWare®. On NetWare, the Identity Vault uses whatever version of Java is installed on the system.

2.2 Installing the Identity Manager Metadirectory

Install the Identity Manager 3.5.1 metadirectory. Directions are in the *Novell Identity Manager 3.5.1 Installation Guide* (<http://www.novell.com/documentation/idm35/pdfdoc/install/install.pdf>).

Give access to the Identity Vault to an Identity Manager Roles Based Provisioning Module administrator. To do so, in iManager assign Administrator access to the context where the Identity Manager Roles Based Provisioning Module users will reside.

2.3 Installing the JBoss Application Server

If you plan to use the JBoss* Application Server, do either of the following:

- ♦ Download and install the JBoss 4.2.0 Application Server according to manufacturer's instructions
- ♦ Use the JbossMysql utility provided with the Roles Based Provisioning Module download to install a JBoss Application Server (and optionally MySQL). For directions, see [Section 2.3.1, "Installing the JBoss Application Server and the MySQL Database,"](#) on page 20.

Wait until after you install the Identity Manager Roles Based Provisioning Module to start the JBoss server. Starting the JBoss server is a post-installation task.

RAM: The minimum recommended RAM for the JBoss Application Server when running the Identity Manager Roles Based Provisioning Module is 512 MB.

Port: Record the port that your application server uses; the Roles Based Provisioning Module installer asks for this port. (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 Identity Manager Roles Based Provisioning Module and the `IDMPwdMgt.war` file. See your JBoss documentation for directions on enabling SSL. Also, make sure the SSL port is open on your firewall. For information on the `IDMPwdMgt.war` file, see [Section 7.5, "Accessing the External Password WAR,"](#) on page 110 and also see the *IDM User Application: Administration Guide* (<http://www.novell.com/documentation/idmrbpm36/index.html>).

2.3.1 Installing the JBoss Application Server and the MySQL Database

You can use the JbossMysql utility to install a JBoss Application Server and MySQL on your system.

NOTE: 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 2.3.2, "Installing the JBoss Application Server as a Service or a Daemon,"](#) on page 23.

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



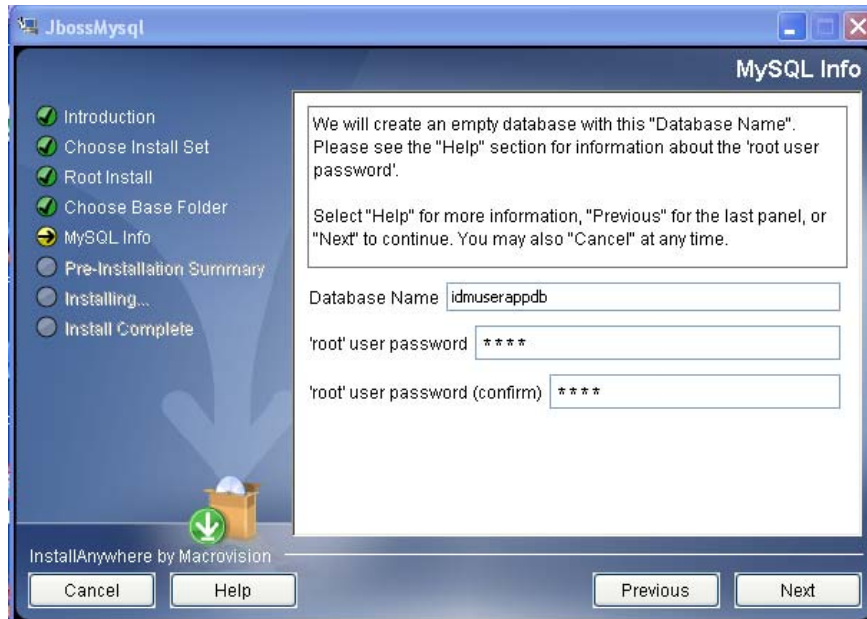
3 Select the products you want to install, then click *Next*.

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



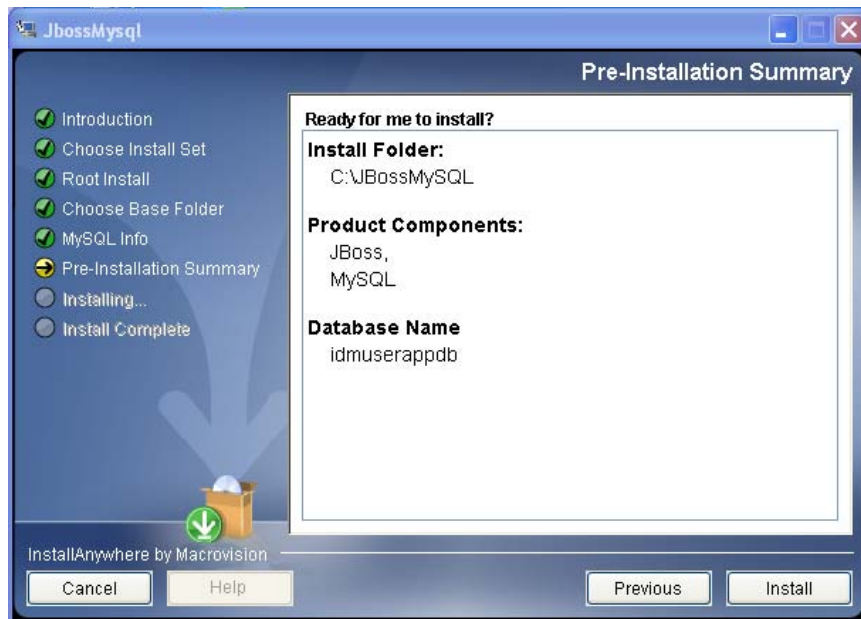
5 Specify a name for your database. The User Application installation requires this name.

6 Specify the database root user password.



7 Click *Next*.

8 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 2.5.2, “Configuring Your MySQL Database,”](#) on page 24.

2.3.2 Installing the JBoss Application Server as a Service or a Daemon

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>).

To start JBoss Application as a daemon, see the instructions from JBoss (<http://wiki.jboss.org/wiki/Wiki.jsp?page=StartJBossOnBootWithLinux>).

This section includes these topics:

- ♦ “Using a Java Service Wrapper” on page 23
- ♦ “Using a Third-Party Utility” on page 24

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
```

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

```
java-service-wrapper-service.xml: <Xml 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.

IMPORTANT: 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>).

2.4 Installing the WebSphere Application Server

If you plan to use the WebSphere Application Server 6.1, download and install WebSphere Application Server 6.1. The minimum fixpack level needed is 6.1.0.9.

2.5 Databases

Install your database and database driver and create a database or a database instance. Record the following database parameters for use in the installation procedure for the Identity Manager Roles Based Provisioning Module:

- ♦ host and port
- ♦ database name, username, and user password

A datasource file must point to the database. The method varies according to your application server. For JBoss, the Identity Manager Roles Based Provisioning Module install program creates an application server datasource file pointing to the database and names the file based on the name of the Identity Manager Roles Based Provisioning Module WAR file. For WebSphere, configure the datasource manually prior to the install.

Databases must be enabled for UTF-8.

- ♦ [Section 2.5.1, “Installing MySQL,” on page 24](#)
- ♦ [Section 2.5.2, “Configuring Your MySQL Database,” on page 24](#)

2.5.1 Installing MySQL

Whether you install MySQL* through the IDM User Application utility or install MySQL on your own, read [Section 2.5.2, “Configuring Your MySQL Database,” on page 24](#).

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 Identity Manager Roles Based Provisioning Module. Just start the database before you start the application server.

2.5.2 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:

- ♦ “[INNODB Storage Engine and Table Types](#)” on page 25
- ♦ “[Character Set](#)” on page 25
- ♦ “[Case Sensitivity](#)” on page 25

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.

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
```

You can also 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&characterEncoding
```

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.

2.6 Downloading the Product

Obtain the Identity Manager Roles Based Provisioning Module 3.6 product from [Novell Downloads](http://download.novell.com/index.jsp) (<http://download.novell.com/index.jsp>).

Download the correct User Application .iso image file for your system:

Identity_Manager_3_6_0_User_Application_Provisioning.iso

The .iso file contains the following delivery directories:

```
/linux/user_application (for Linux)
/nt/user_application (for Windows)
/solaris/user_application (for Solaris)
/36MetaDirSupport (includes the files needed to update the IDM 3.5.1 metadirectory to
support the IDM 3.6 User Application)
```

Table 2-1 lists the files and scripts you need to install the Identity Manager Roles Based Provisioning Module 3.6.

Table 2-1 Files and Scripts Required for Installing the Identity Manager 3.6 User Application

File	Description
IDMProv.war	This is the Roles Based Provisioning Module WAR. It includes the Identity Manager 3.6 User Application with Identity Self-Service features and the Roles Based Provisioning Module.
IDMUserApp.jar	This is the Roles Based Provisioning Module installation program.
silent.properties	This file contains the installation parameters required for a silent install. These parameters correspond to the installation parameters you set in the GUI or Console installation procedures.
prerequisitefiles.zip	This ZIP file contains other files that require manual installation.
UserApplication_3_6_0- IDM3_5_1-V1.xml	This is the configuration file for the User Application driver.
iManager_icons_for_roles.zip	This contains the iManager icons for roles objects in the eDirectory.

TIP: You can find the `iManager_icons_for_roles.zip` and `prerequisites.zip` in the `/36MetaDirSupport` directory. The other files are located in the `<operating_system>/user_application` directories.

The system on which you install the Identity Manager Roles Based Provisioning Module must have at least 320 MB of available storage.

The default installation location is:

- ◆ Linux or Solaris: `/opt/novell/idm`

- ◆ Windows: C:\Novell\IDM

You can select another default installation directory during the installation, but it must exist prior to starting the installation and be writable (and in the case of Linux or Solaris, be writable by non-root users).

2.7 Installing the Contents of the prerequisitefiles.zip File

In your downloaded .iso image, locate the `prerequisitefiles.zip` file and unzip it. It contains files that you must manually install, as listed in [Table 2-2](#):

Table 2-2 Files Requiring Manual Installation

Filename	Description	Directions
<code>nrf-extensions.sch</code>	eDirectory™ schema file	Section 2.7.1, “Extending the eDirectory Schema for Roles Based Provisioning Module Version 3.6,” on page 27
<code>nrfdriver.jar</code>	Role Service Driver JAR	Section 2.7.2, “Copying the JAR File for the Role Service Driver,” on page 28
<code>RoleService-IDM3_5_1-V1.xml</code>	Role Service Driver configuration file	Section 2.7.3, “Copying the Role Service Driver Configuration File,” on page 29
<code>UserApplicationn_3_6_0-IDM3_5_1-V1.xml</code>	User Application Driver configuration file that supports the Roles Based Provisioning Module	Section 2.7.4, “Copying the User Application Driver Configuration File,” on page 29
<code>dirxml.lsc</code>	Logging application log schema file	Section 2.7.5, “Copying the dirxml.lsc File,” on page 30

- ◆ [Section 2.7.1, “Extending the eDirectory Schema for Roles Based Provisioning Module Version 3.6,” on page 27](#)
- ◆ [Section 2.7.2, “Copying the JAR File for the Role Service Driver,” on page 28](#)
- ◆ [Section 2.7.3, “Copying the Role Service Driver Configuration File,” on page 29](#)
- ◆ [Section 2.7.4, “Copying the User Application Driver Configuration File,” on page 29](#)
- ◆ [Section 2.7.5, “Copying the dirxml.lsc File,” on page 30](#)

2.7.1 Extending the eDirectory Schema for Roles Based Provisioning Module Version 3.6

Extend the eDirectory schema for the Roles Based Provisioning Module as described in the following sections:

- ◆ [“Extending the Schema on Windows” on page 28](#)
- ◆ [“Extending the Schema on UNIX/Linux” on page 28](#)
- ◆ [“Extending the Schema on NetWare” on page 28](#)

Extending the Schema on Windows

Use `NDSCons.exe` to extend the schema on Windows servers. Schema files (*.sch) that come with eDirectory are installed by default into the `C:\Novell\NDS` directory.

- 1 Click *Start > Settings > Control Panel > Novell eDirectory Services*.
- 2 Click *install.dlm*, then click *Start*.
- 3 Click *Install Additional Schema Files*, then click *Next*.
- 4 Log in as a user with administrative rights, then click *OK*.
- 5 Specify the schema file path and name (for example, `c:\Novell\NDS\nrf-extensions.sch`).
- 6 Click *Finish*.

Extending the Schema on UNIX/Linux

To extend eDirectory schema for the Roles Based Provisioning Module on a UNIX/Linux platform, perform the following steps:

- 1 Add the Roles Based Provisioning Module schema file, `nrf-extensions.sch`. To do this, use the `ndssch` command from the command line:

```
ndssch [-h hostname[:port]] [-t tree_name] admin-FDN
schemafilename.sch
```

Extending the Schema on NetWare

Use `NWConfig.nlm` to extend the schema on NetWare servers. Schema files (*.sch) that come with eDirectory are installed into the `sys:\system\schema` directory.

- 1 At the server console, enter `nwconfig`.
- 2 Select *Directory Options > Extend Schema*.
- 3 Log in as a user with administrative rights.
- 4 Press F3 to specify a different path, then type `sys:\system\schema` (or the path for your *.sch file) and the `nrf-extensions.sch` schema file.
- 5 Press `Enter`.

2.7.2 Copying the JAR File for the Role Service Driver

Manually install the Role Service Driver on the metadirectory server. To do so, copy the executable Role Service JAR file, `nrfdriver.jar`, from the unzipped `prerequisitefiles.zip` archive to the correct directory for your system:

Table 2-3 Location for the Role Service Driver JAR file

Operating System	Directory
UNIX (eDirectory 8.7.x)	<code>/usr/lib/dirxml/classes</code>
UNIX (eDirector 8.8.x)	<code>/opt/novell/eDirectory/lib/dirxml/classes</code>

Operating System	Directory
Windows	<drive>:\novell\nds\lib
NetWare	SYS:SYSTEM\LIB

2.7.3 Copying the Role Service Driver Configuration File

Manually install the Role Service Driver configuration file, `RoleService_IDM3_5_1-V1.xml`, to the correct directory for your system:

Table 2-4 Location for the Role Service Driver Configuration File

Operating System	Directory
Linux (eDirectory 8.7.x)	/usr/lib/dirxml/classes
Linux (eDirectory 8.8)	/var/opt/novell/iManager/nps/DirXML.Drivers
Windows	C:\Program Files\Novell\tomcat\webapps\nps\Dirxml.Drivers
NetWare	SYS:\tomcat\4\webapps\nps\Dirxml.Drivers

If you want iManager's Create Driver wizard to display in any of the supported languages (besides English), you must also copy the `RoleService-IDM3_5_1.xlf` files from the `prerequisitefiles.zip` archive to the same directory as the `RoleService_IDM3_5_1-V1.xml`. There is an XLF file for each of the supported languages. The file name includes the two character language code that indicate the contents of the file.

2.7.4 Copying the User Application Driver Configuration File

Manually install the User Application Driver configuration file, `UserApplication_3_6_0-IDM3_5_1-V1.xml`, to the correct directory for your system:

Table 2-5 Location for the User Application Driver Configuration File

Operating System	Directory
Linux (eDir 8.7.x)	/usr/lib/dirxml/classes
Linux (eDir 8.8)	/var/opt/novell/iManager/nps/DirXML.Drivers
Windows	C:\Program Files\Novell\tomcat\webapps\nps\Dirxml.Drivers
NetWare	SYS:\tomcat\4\webapps\nps\Dirxml.Drivers

If you want iManager's Create Driver wizard to display in any of the supported languages (besides English), you must also copy the `UserApplication_3_6_0-IDM3_5_1-V1.xlf` files from the `prerequisitefiles.zip` archive to the same directory as the `UserApplication_3_6_0-IDM3_5_1-V1.xlf`. There is an XLF file for each of the

supported languages. The file name includes the two character language code that indicate the contents of the file.

2.7.5 Copying the dirxml.lsc File

Copy the `dirxml.lsc` file to the Audit server according to the directions in the section titled “Setting Up Logging” in the [Identity Manager User Application: Administration Guide \(http://www.novell.com/documentation/idmrbpm36/pdfdoc/agpro/agpro.pdf\)](http://www.novell.com/documentation/idmrbpm36/pdfdoc/agpro/agpro.pdf).

2.8 Installing the iManager Icons for Roles

In your downloaded .iso image, locate the `iManager_icons_for_roles.zip` file and unzip it. Copy the extracted icons files to the `nps/portal/modules/dev/images/dir` directory. Restart iManager so it uses the new icons.

Creating Drivers

This section describes how to create the drivers necessary for using the Roles Based Provisioning Module. Topics include:

- ♦ [Section 3.1, “Creating the User Application Driver in iManager,” on page 31](#)
- ♦ [Section 3.2, “Creating the Role Service Driver in iManager,” on page 35](#)

IMPORTANT: You need to create the User Application driver before creating the Role Service driver. The User Application driver needs to be created first because the Role Service driver references the role vault container (RoleConfig.AppConfig) in the User Application driver.

The allowed driver configuration is:

- ♦ You can add one Role Service driver per driver set in iManager.
- ♦ You can associate one User Application driver with a Role Service driver.
- ♦ You can associate one User Application with a User Application driver.

3.1 Creating the User Application Driver in iManager

You must create a separate User Application driver for each Identity Manager Roles Based Provisioning Module, except for Roles Based Provisioning Modules that are members of a cluster. Roles Based Provisioning Modules that are part of the same cluster must share a single User Application driver. For information on running the Roles Based Provisioning Module in a cluster, see the *Identity Manager User Application: Administration Guide* (<http://www.novell.com/documentation/idmrpbpm36/index.html>).

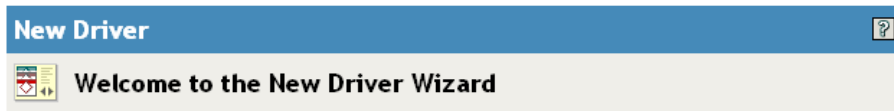
The Roles Based Provisioning Module stores application-specific data in the User Application driver to control and configure the application environment. This includes the application server cluster information and the workflow engine configuration.

IMPORTANT: Configuring a set of non-cluster Roles Based Provisioning Modules to share a single driver creates ambiguity for one or more of the components running inside the Roles Based Provisioning Module. The source of the resulting problems is difficult to detect.

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

- 1 Open iManager 2.6 or later in a Web browser.

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





The Identity Manager product includes all product components. The drivers you are authorized to deploy are determined by the drivers you have purchased.

Application drivers are contained in a driver set. When you create a driver, make sure that the server associated with the driver set contains a non-filtered writable replica of the partition that contains the driver set. If it does not, then a read/write replica will be added or the existing replica will be converted to read/write.

Where do you want to place the new driver?

In an existing driver set

In a new driver set

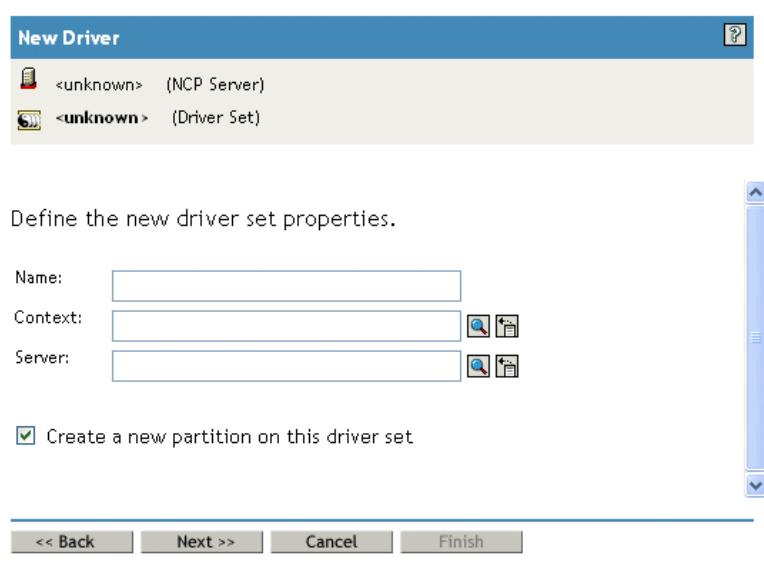


- 3 To create the driver in an existing driver set, select *In an existing driver set*, click the object selector icon, select a driver set object, click *Next*, and continue with **Step 4**.

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. The context is the eDirectory™ context where the server object is located.



- 3b** Click *Next*.

- 4** Click *Import a driver configuration from the server (.XML file)*.
- 5** Select *UserApplication_3_6_0-IDM3_5_1-VI.xml* from the drop-down list. This is the User Application Driver configuration file that supports the Roles Based Provisioning Module.

If *UserApplication_3_6_0-IDM3_5_1-VI.xml* is not in this drop-down list, you did not copy this file to the correct location. Please refer to [Section 2.7.4, “Copying the User Application Driver Configuration File,”](#) on page 29.

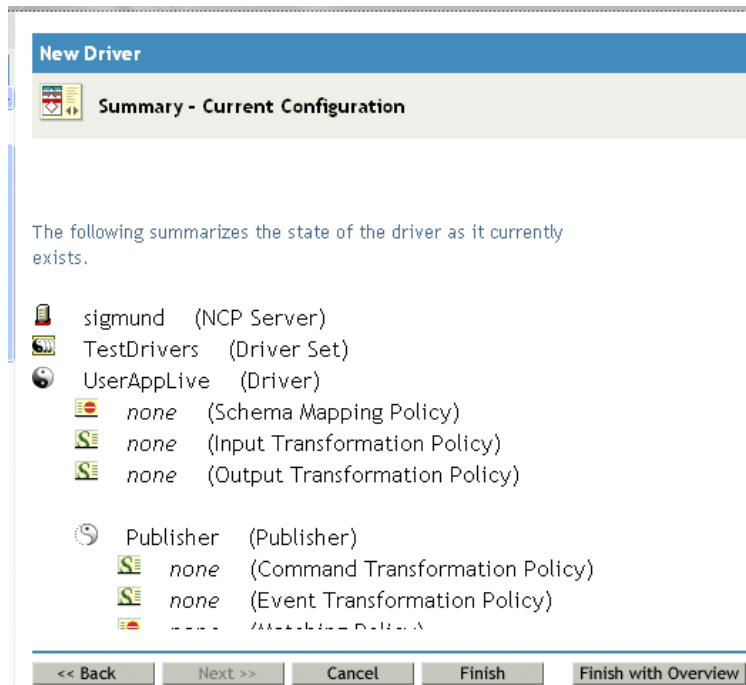
- 6** Click *Next*.
- 7** You are prompted for parameters for your driver. (Scroll to view all.) Make a note of the parameters; you need these when you install the Roles Based Provisioning Module.

Field	Description
<i>Driver Name</i>	The name of the driver you are creating.
<i>Authentication ID</i>	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.
<i>Password</i>	Password of the User Application Administrator specified in the Authentication ID.
<i>Application Context</i>	The User Application context. This is the context portion of the URL for the User Application WAR file. The default is IDM.

Field	Description
<i>Host</i>	The hostname or IP address of the application server where the Identity Manager User Application is deployed. If the User Application is running in a cluster, type the dispatcher's hostname or IP address.
<i>Port</i>	The port for the host you listed above.
<i>Allow Override Initiator:</i> (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.

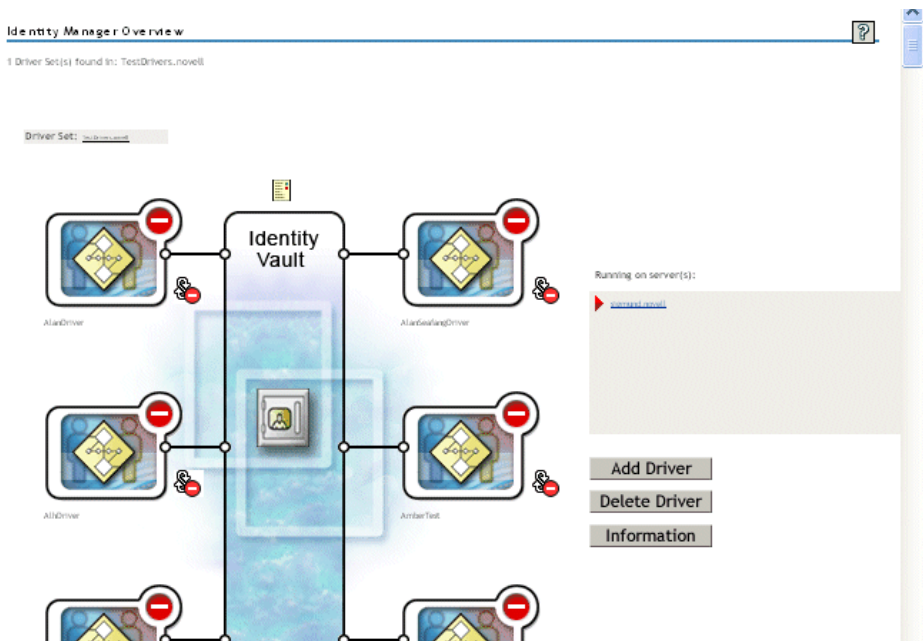
- 8 Click *Next*.
- 9 Click *Define Security Equivalences* to open the Security Equals window. Browse to and select an administrator or other Supervisor object, then click *Add*.

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, then click *Next* to display the summary page.



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

IMPORTANT: The driver is turned off by default. Leave the driver off until the Roles Based Provisioning Module has been installed.



3.2 Creating the Role Service Driver in iManager

To create and configure the Role Service driver in iManager.

- 1 Open iManager 2.6 or later in a Web browser.
- 2 Under *Identity Manager > Identity Manager Overview*, select the Driver Set where you want to install the Role Service driver.

Install the User Application driver before installing the Role Service driver. Use Version 3.6 of the User Application driver (`UserApplication_3_6_0-IDM3_5_1-V1.xml`) with the Role Service driver. If you use a different version of the User Application driver, the Roles Catalog will not be available.

You can only have one Role Service driver per driver set.

- 3 Click *Add Driver*.
- 4 In the New Driver Wizard, keep the default of *In an existing driver set*. Click *Next*.
- 5 Select `RoleService-IDM3_5_1-V1.xml` from the drop-down list. This is the Role Service driver configuration file that supports the Roles Based Provisioning Module.

If `RoleService-IDM3_5_1-V1.xml` is not in this drop-down list, you did not copy this file to the correct location. Please refer to [Section 2.7.3, “Copying the Role Service Driver Configuration File,”](#) on page 29.

Click *Next*.

You might see the following error when trying to create the driver:

```
The following 'Namespace Exception' occurred while trying to access the directory. (CLASS_NOT_DEFINED)
```

If so, the iManager application might not have picked up your new Roles schema yet. The new schema is necessary for the Role Service driver. Try restarting your iManager session (close all browsers and log into the iManager again). Or, try restarting the server.

- 6 Fill out the requested information in the Import Information Requested page. The following table describes the requested information.

Option	Description
<i>Driver Name</i>	Specify the driver name or keep the default name, <code>Role Service</code> , of the Role Service driver. If you install a new driver with the same name as an existing driver, the new driver overwrites the existing driver's configuration. Use the <i>Browse</i> button to see the existing drivers on the selected driver set. This is a required field.
<i>User Application Driver DN</i>	The distinguished name of the User Application driver object that is hosting the role system. Use the eDirectory format, such as <code>UserApplication.driverset.org</code> , or browse to find the driver object. This is a required field.
<i>User Application URL</i>	The URL used to connect to the User Application in order to start Approval Workflows. The example URL given is <code>http://host:port/IDM</code> . This is a required field.
<i>User Application Identity</i>	The distinguished name of the object used to authenticate to the User Application in order to start Approval Workflows. This can be a User Application Administrator to whom you are giving rights to administer the User Application portal. Use the eDirectory format, such as <code>admin.department.org</code> , or browse to find the user. This is a required field.
<i>User Application Password</i>	Password of the User Application Administrator specified in the Authentication ID. The password is used to authenticate to the User Application in order to start Approval Workflows. This is a required field.
<i>Reenter the Password</i>	Re-enter the password of the User Application Administrator.

- 7 After the information is filled in, click *Next*.
- 8 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.
- 9 (Optional, but recommended) Click *Exclude Administrative Roles*.
- 10 Click *Add*, select users you want to exclude for driver actions (such as administrative roles), click *OK* twice, then click *Next*.
- 11 Click *OK* to close the Security Equals window, then click *Next* to display the summary page.
- 12 If the information is correct, click *Finish*.

Installing on JBoss Using a GUI

4

This section describes how to install the Identity Manager Roles Based Provisioning Module on a JBoss Application Server by using the graphical user interface version of the installer. If you would rather install the module on JBoss from the console or by using a single command, see [Chapter 5, “Installing from the Console or With a Single Command,”](#) on page 69.

- ◆ [Section 4.1, “Launching the Installer GUI,”](#) on page 37
- ◆ [Section 4.2, “Choosing an Application Server Platform,”](#) on page 38
- ◆ [Section 4.3, “Migrating Your Database,”](#) on page 39
- ◆ [Section 4.4, “Specifying the Location of the WAR,”](#) on page 41
- ◆ [Section 4.5, “Choosing an Install Folder,”](#) on page 42
- ◆ [Section 4.6, “Choosing a Database Platform,”](#) on page 44
- ◆ [Section 4.7, “Specifying the Database Host and Port,”](#) on page 46
- ◆ [Section 4.8, “Specifying the Database Name and Privileged User,”](#) on page 47
- ◆ [Section 4.9, “Specifying the Java Root Directory,”](#) on page 48
- ◆ [Section 4.10, “Specifying the JBoss Application Server Settings,”](#) on page 48
- ◆ [Section 4.11, “Choosing the Application Server Configuration Type,”](#) on page 50
- ◆ [Section 4.12, “Enabling Novell Audit Logging,”](#) on page 51
- ◆ [Section 4.13, “Specifying a Master Key,”](#) on page 52
- ◆ [Section 4.14, “Configuring the User Application,”](#) on page 53
- ◆ [Section 4.15, “Using Password WARs,”](#) on page 66
- ◆ [Section 4.16, “Verify Choices and Install,”](#) on page 67
- ◆ [Section 4.17, “View Log Files,”](#) on page 67

If you prefer to use the command line for installation, see [Chapter 5, “Installing from the Console or With a Single Command,”](#) on page 69.

4.1 Launching the Installer GUI

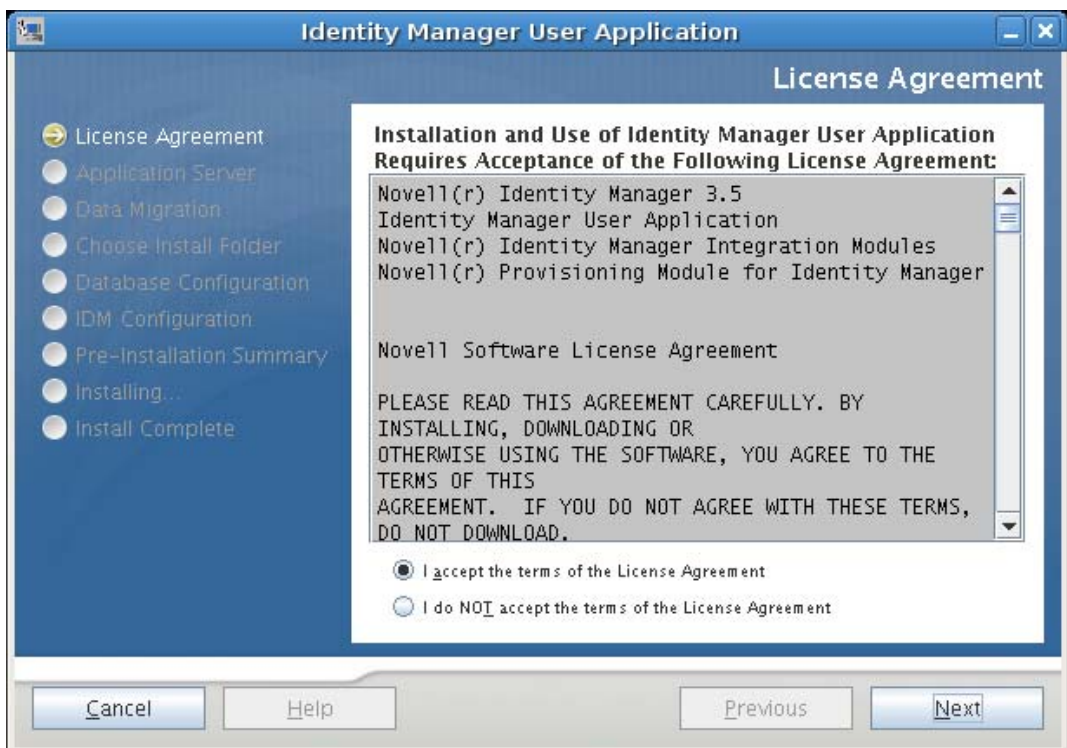
- 1 Navigate to the directory containing your installation files, described in [Table 2-1 on page 26](#).
- 2 Launch the installer for your platform from the command line:

```
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*.

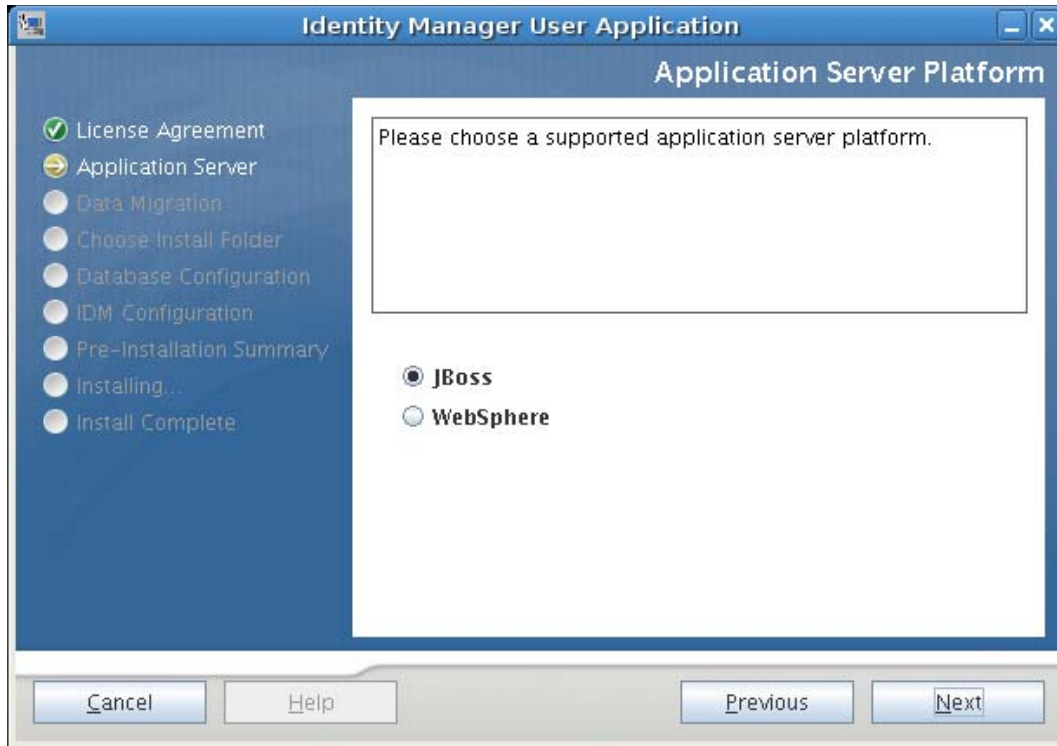


- 5 Read the Introduction page of the install wizard, then click *Next*.
- 6 Continue with [Section 4.2, "Choosing an Application Server Platform,"](#) on page 38.

4.2 Choosing an Application Server Platform

Complete the procedure in [Section 4.1, "Launching the Installer GUI,"](#) on page 37, then continue with the steps below:

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



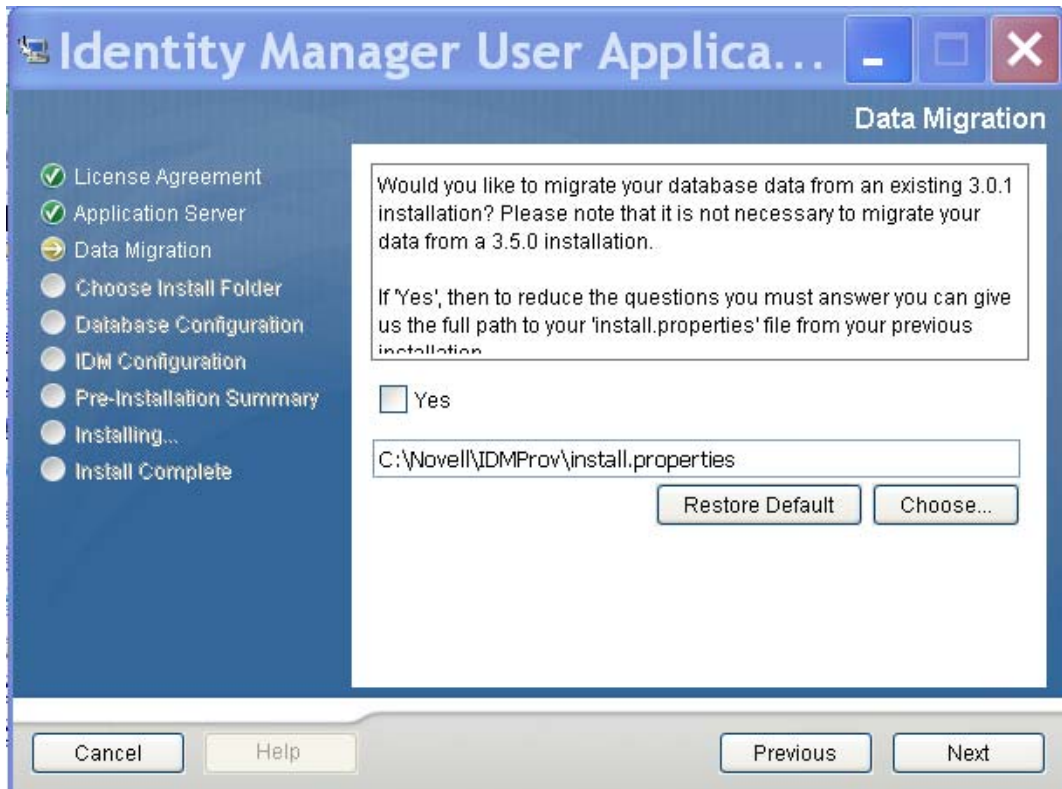
4.3 Migrating Your Database

- 1 If you do not want to migrate a database, click *Next* and continue to [Section 4.4, “Specifying the Location of the WAR,”](#) on page 41.

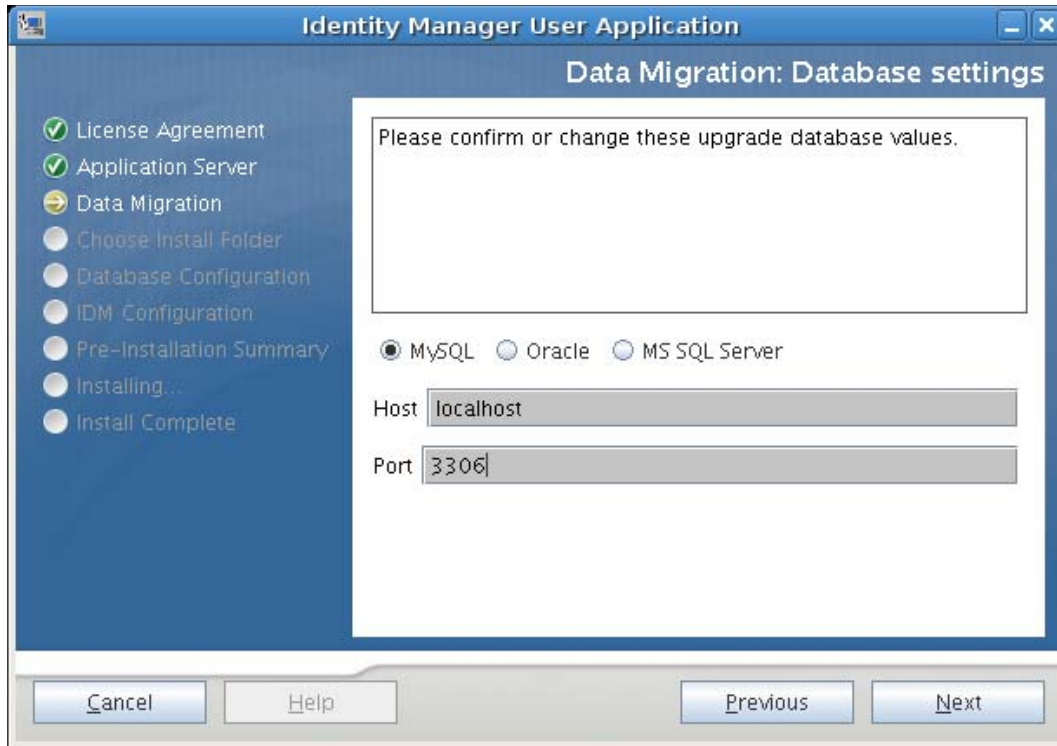
To use an existing database from a Version 3.0 or Version 3.01 User Application, you must migrate it to the updated format.

- 2 Verify that you started the database that you want to migrate.
- 3 Click *Yes* in the Data Migration page of the installation program.
- 4 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 must specify in the following pages.



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



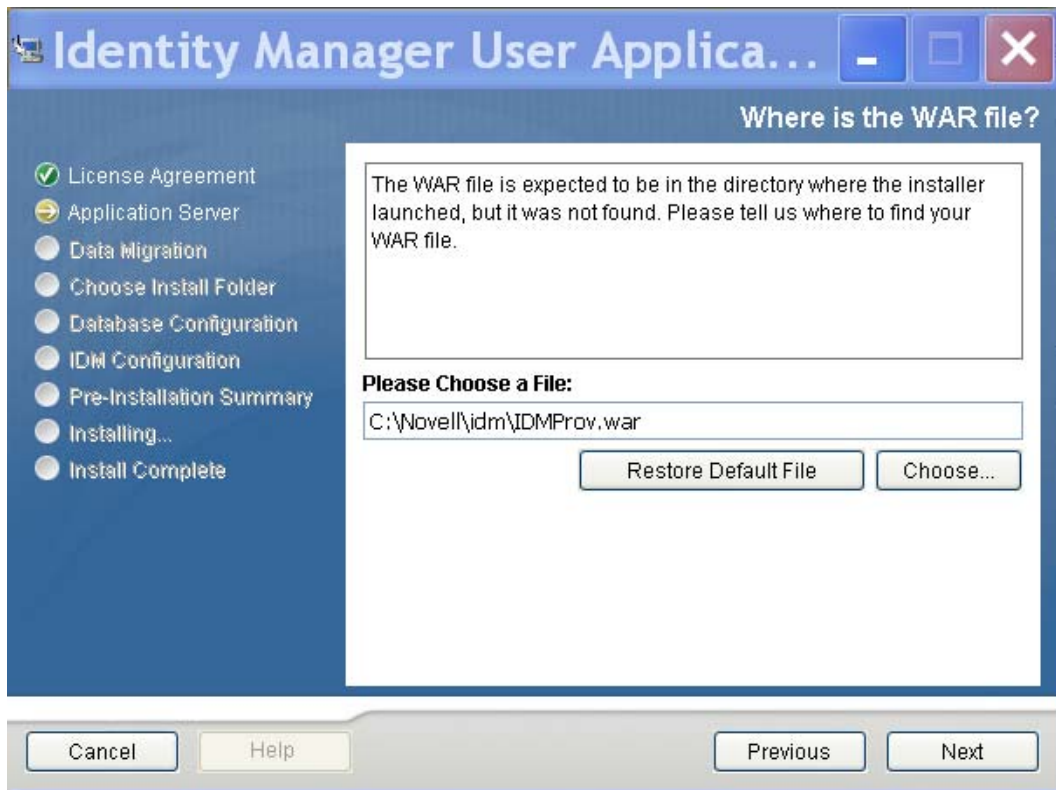
- 6 Click *Next* and continue to [Section 4.4, “Specifying the Location of the WAR,” on page 41](#) or [Section 4.5, “Choosing an Install Folder,” on page 42](#).

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 migrating a Version 3.5.1 User Application to Version 3.6, see the *Identity Manager User Application: Migration Guide* (<http://www.novell.com/documentation/idmrbpm36/index.html>).

4.4 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.

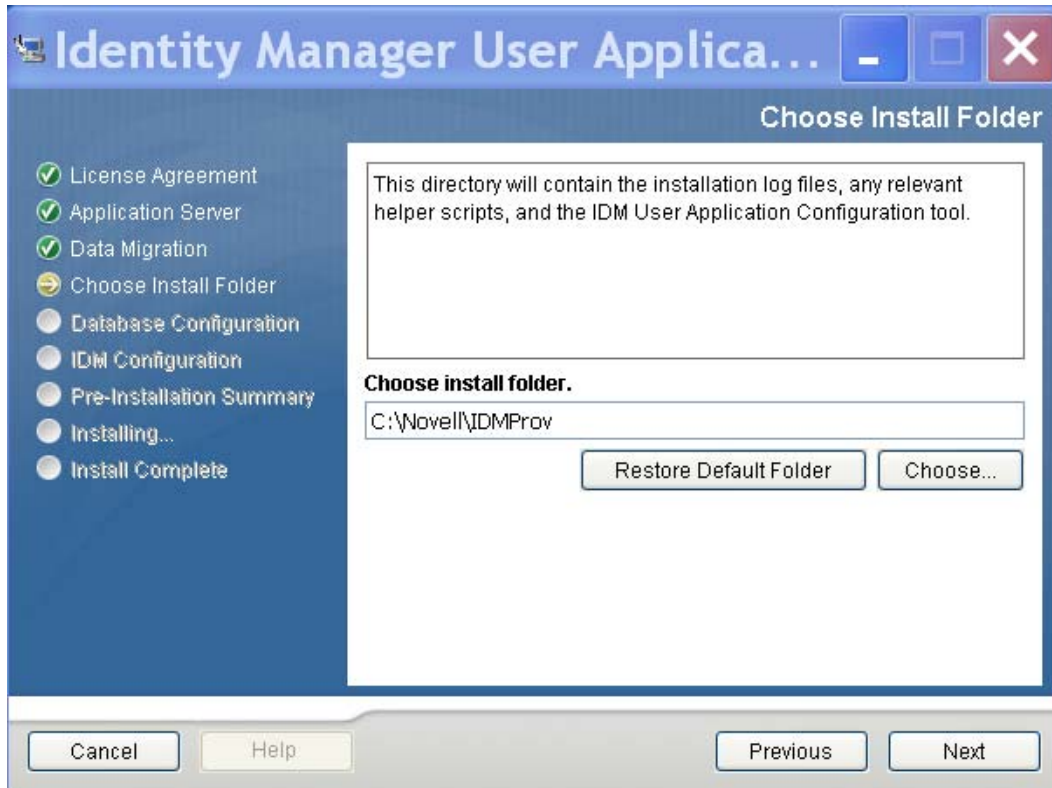
- 1 If the WAR is in the default location, click *Restore Default Folder*. Or, to specify the location of the WAR file, click *Choose* and select a location.
- 2 Click *Next*, then continue with [Section 4.5, “Choosing an Install Folder,” on page 42](#).



4.5 Choosing an Install Folder

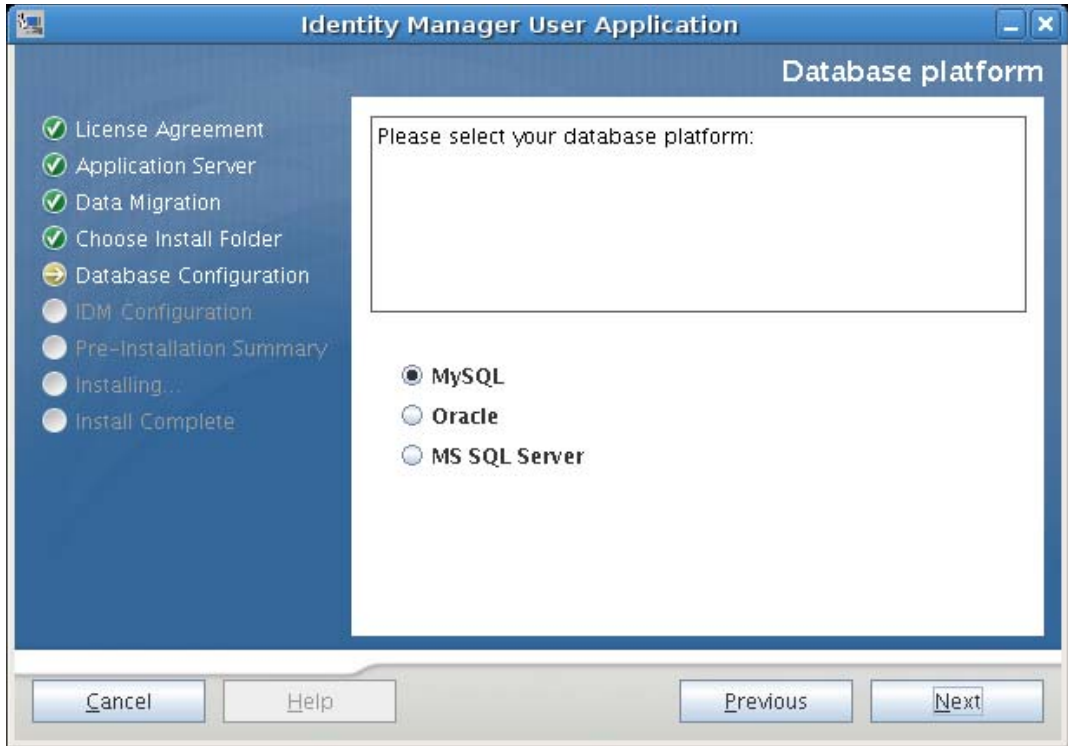
- 1 On the Choose Install Folder page, select where to install the User Application. If you need to remember and use the default location, click *Restore Default Folder*, or if you want to choose another location for the installation files, click *Choose* and browse to a location.

2 Click *Next*, then continue with [Section 4.6, “Choosing a Database Platform,”](#) on page 44.



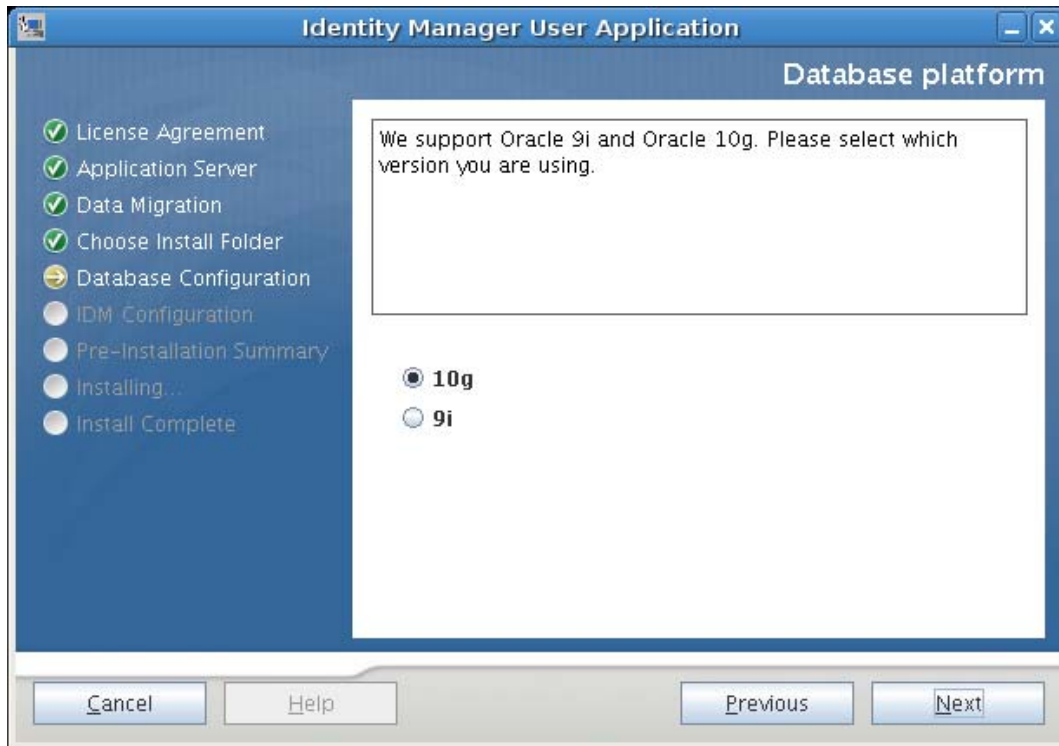
4.6 Choosing a Database Platform

- 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 4.7, “Specifying the Database Host and Port,”](#) on [page 46](#).

4.7 Specifying the Database Host and Port

- 1 Fill in the following fields:

Identity Manager User Application

Database Host & Port

Please provide the following database details:

Host localhost

Port 3306

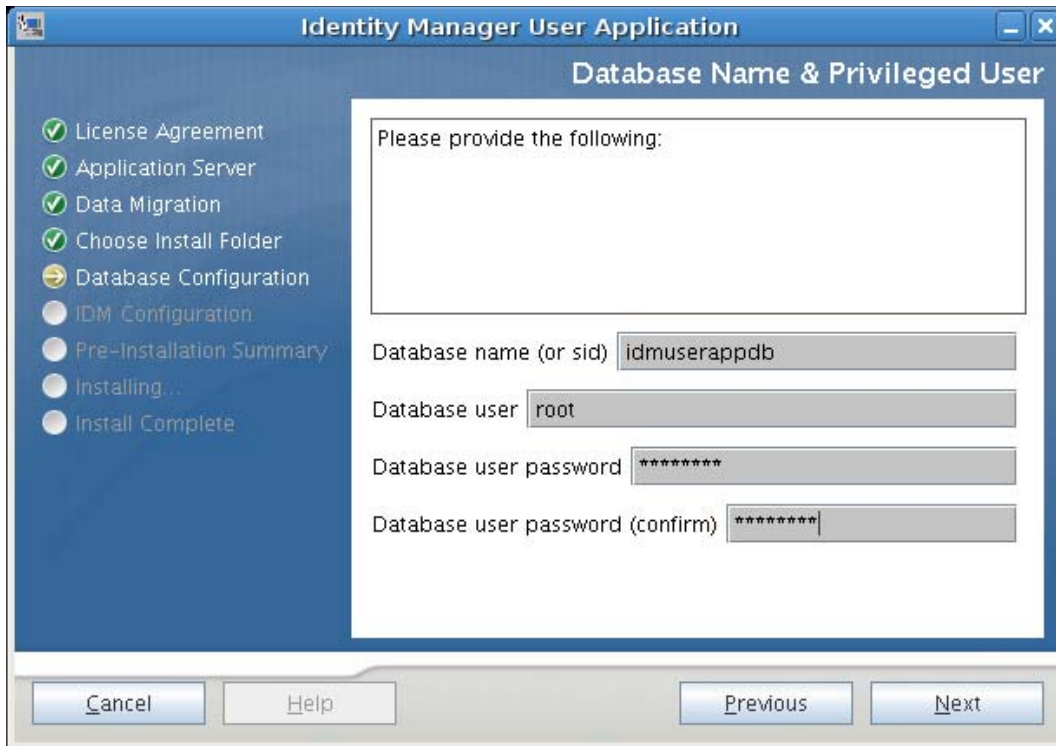
Cancel Help Previous Next

Field	Description
<i>Host</i>	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.
<i>Port</i>	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 4.8, “Specifying the Database Name and Privileged User,”](#) on page 47.

4.8 Specifying the Database Name and Privileged User

- 1 Fill in the following fields:

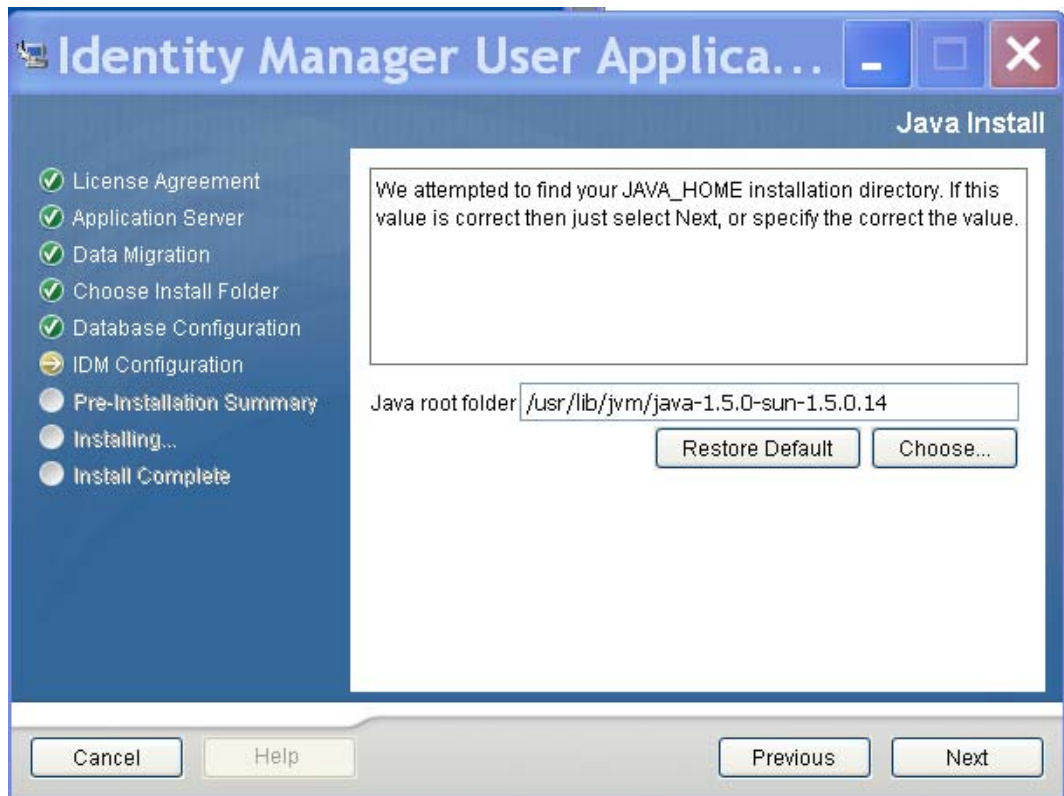


Field	Description
<i>Database name (or sid)</i>	For MySQL or MS SQL Server, provide the name of your preconfigured database. For Oracle, provide the Oracle System Identifier (SID) that you previously created. For a cluster, specify the same database name or SID for each member of the cluster.
<i>Database user</i>	Specify the database user. For a cluster, specify the same database user for each member of the cluster.
<i>Database password/Confirm password</i>	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 4.9, “Specifying the Java Root Directory,”](#) on page 48.

4.9 Specifying the Java Root Directory

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



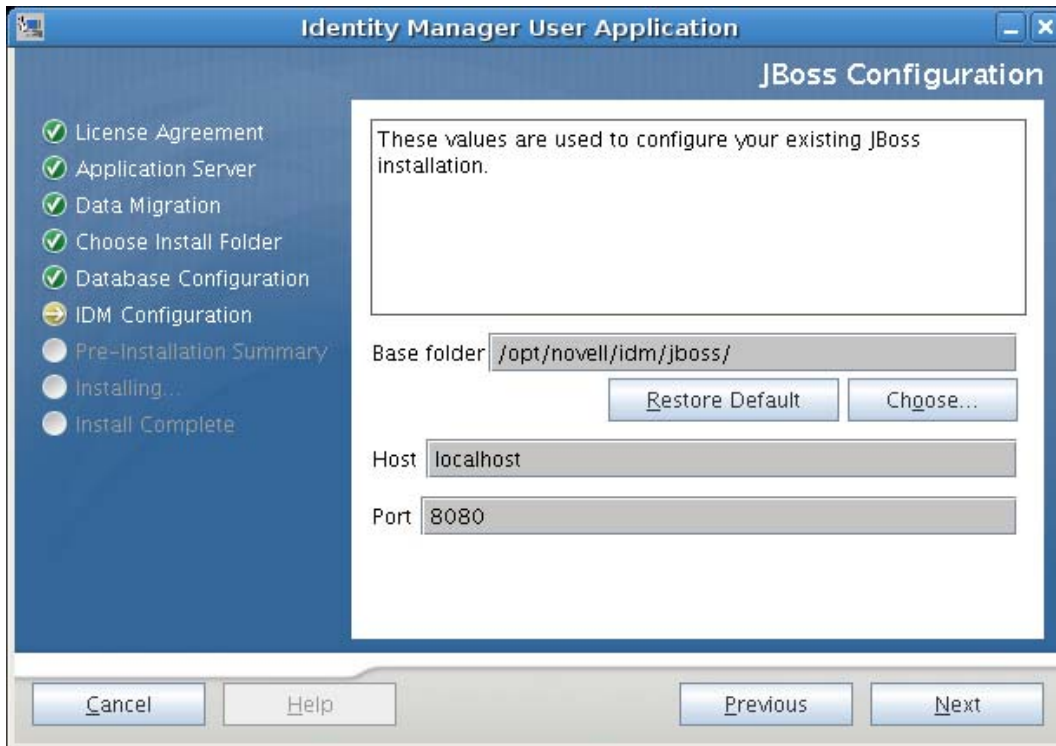
- 2 Click *Next*, then continue with [Section 4.10, “Specifying the JBoss Application Server Settings,”](#) on page 48.

4.10 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 2.3.1, “Installing the JBoss Application Server and the MySQL Database,”](#) on page 20.

- 1 Supply the base folder, host, and port:

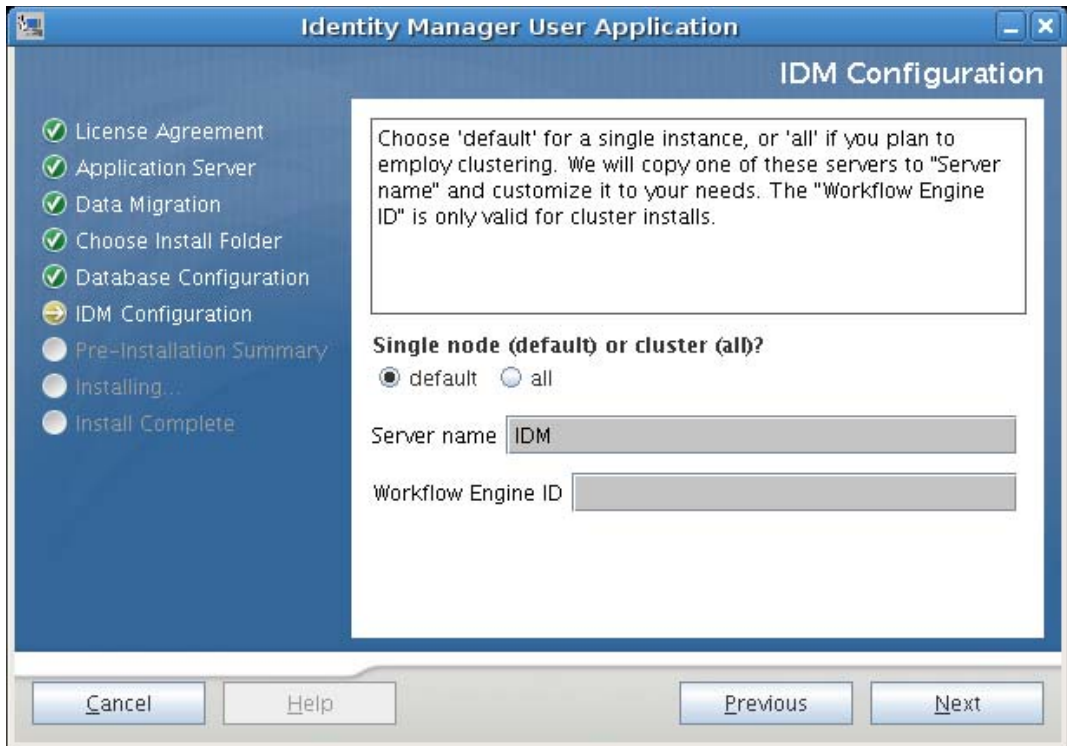


Field	Description
<i>Base folder</i>	Specify the location of the application server.
<i>Host</i>	Specify the application server's hostname or IP address
<i>Port</i>	Specify the application server's listener port number. The JBoss default port is 8080.

- 2 Click *Next*, then continue with [Section 4.11, “Choosing the Application Server Configuration Type,”](#) on page 50.

4.11 Choosing the Application Server Configuration Type

- 1 Fill in the following fields:



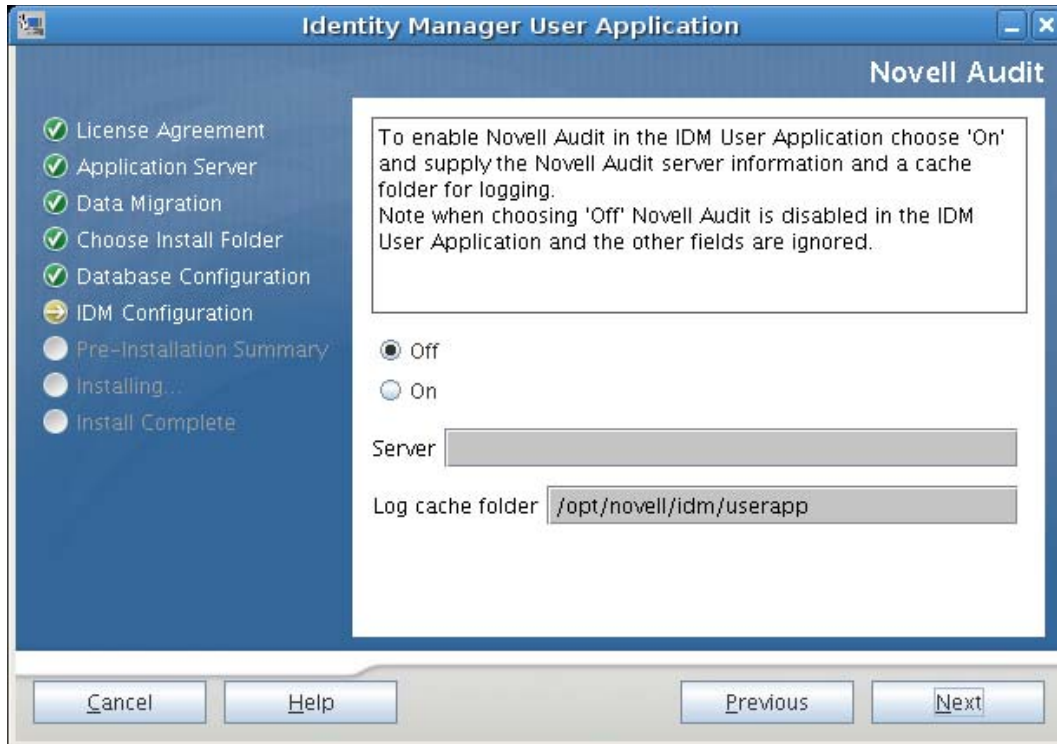
Option	Description
<i>Single (default) or clustering (all)</i>	Select the type of application server configuration: <ul style="list-style-type: none"> ◆ Select <i>all</i> if this installation is part of a cluster ◆ Select <i>default</i> if this installation is on a single node that is not part of a cluster
<i>Server name</i>	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 <i>Application name</i> . Note the application name and include it in the URL when you start the Identity Manager User Application from a browser.
<i>Workflow Engine ID</i>	Each server in a cluster must have a unique Workflow Engine ID. Workflow Engine IDs are described in the <i>Identity Manager User Application: Administration Guide</i> in Section 3.5.4, Configuring Workflows for Clustering.

2 Click *Next*, then continue with [Section 4.12, “Enabling Novell Audit Logging,”](#) on page 51.

4.12 Enabling Novell Audit Logging

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

1 Fill in the following fields:



Option	Description
<i>On</i>	Enables Novell Audit Logging for the User Application. For more information on setting up Novell Audit logging, see the <i>Identity Manager User Application: Administration Guide</i> .
<i>Off</i>	Disables Novell Audit Logging for the User Application. You can enable it later using the <i>Administration</i> tab of the User Application. For more information on enabling Novell Audit logging, see the <i>Identity Manager User Application: Administration Guide</i> .
<i>Server</i>	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.
<i>Log cache folder</i>	Specify the directory for the logging cache.

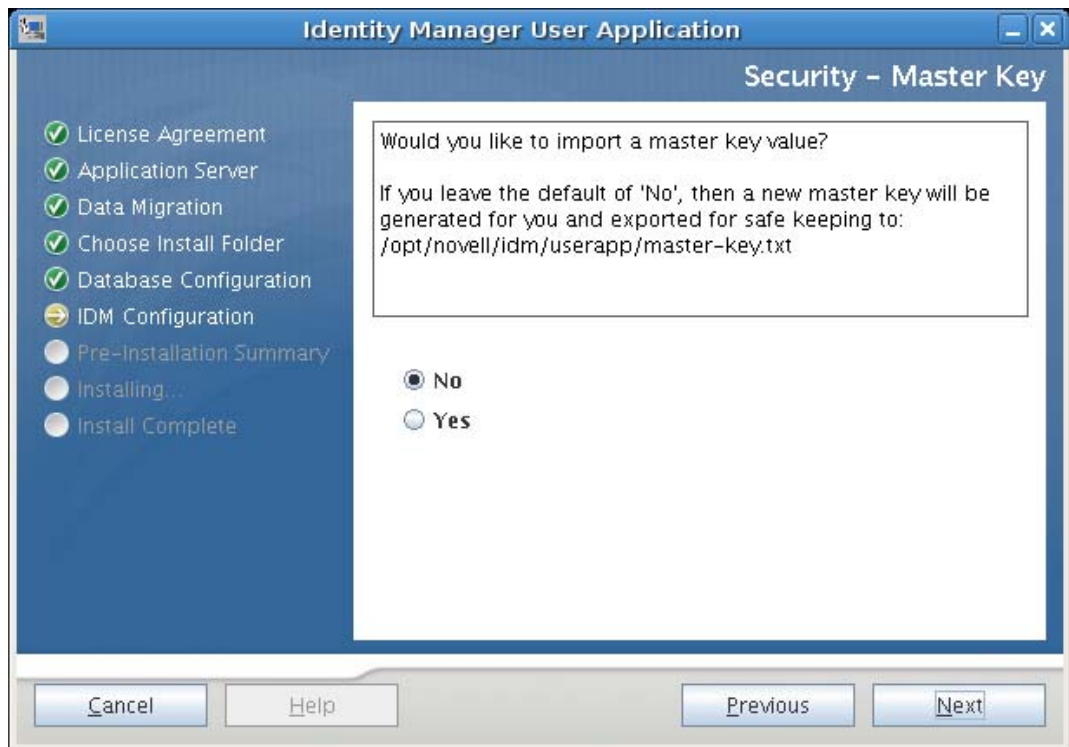
2 Click *Next*, then continue with [Section 4.13, “Specifying a Master Key,”](#) on page 52.

4.13 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.



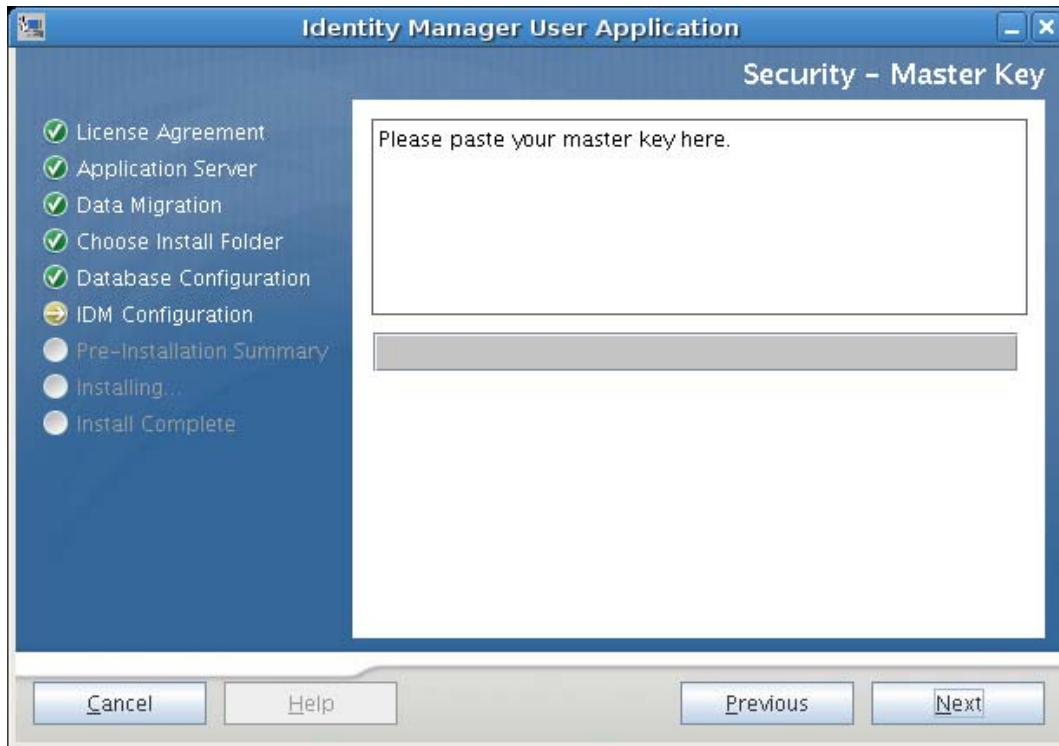
- 2 Click *Next*.

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 4.14, “Configuring the User Application,” on page 53](#). After you finish the installation, you must manually record the master key as described in [Section 7.1, “Recording the Master Key,” on page 109](#).

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*.

4.14 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 4-1](#), then continue with [Step 2](#).

User Application Configuration

eDirectory Connection Settings

LDAP Host:

LDAP Non-Secure Port:

LDAP Secure Port:

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:

Roles Administrator:

User Container DN:

Group Container DN:

eDirectory Certificates

Keystore Path:

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:

Forgot Password Return Link:

OK Cancel Show Advanced Options

Table 4-1 *User Application Configuration: Basic Parameters*

Type of Setting	Field	Description
eDirectory Connection Settings	<i>LDAP Host</i>	Required. Specify the hostname or IP address for your LDAP server and its secure port. For example: <code>myLDAPHost</code>
	<i>LDAP Non-Secure Port</i>	Specify the non-secure port for your LDAP server. For example: 389.
	<i>LDAP Secure Port</i>	Specify the secure port for your LDAP server. For example: 636.
	<i>LDAP Administrator</i>	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.
	<i>LDAP Administrator Password</i>	Required. Specify the LDAP Administrator password. This password is encrypted, based on the master key.
	<i>Use Public Anonymous Account</i>	Allows users who are not logged in to access the LDAP Public Anonymous Account.
	<i>LDAP Guest</i>	Allows users who are not logged in to access permitted portlets. This user account must already exist in the Identity Vault. To enable the LDAP Guest, you must deselect <i>Use Public Anonymous Account</i> . To disable the Guest User, select <i>Use Public Anonymous Account</i> .
	<i>LDAP Guest Password</i>	Specify the LDAP Guest password.
	<i>Secure Admin Connection</i>	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.
	<i>Secure User Connection</i>	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	<i>Root Container DN</i>	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.
	<i>Provisioning Driver DN</i>	Required. Specify the distinguished name of the User Application driver that you created earlier in Section 3.1, “Creating the User Application Driver in iManager,” on page 31 . For example, if your driver is <code>UserApplicationDriver</code> and your driver set is called <code>myDriverSet</code> , and the driver set is in a context of <code>o=myCompany</code> , you would type a value of: <code>cn=UserApplicationDriver,cn=myDriverSet,o=myCompany</code>
	<i>User Application Admin</i>	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 <i>Administration</i> 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 (<i>Requests & Approvals</i> tab), you must grant this administrator appropriate trustee rights to object instances contained in the User Application driver. Refer to the <i>IDM User Application: Administration Guide</i> for details. To change this assignment after you deploy the User Application, you must use the <i>Administration > Security</i> pages in the User Application.
	<i>Provisioning Application Admin</i>	The Provisioning Application Administrator uses the <i>Provisioning</i> tab (under the <i>Administration</i> tab) to manage the Provisioning Workflow functions. These functions are available to users through the <i>Requests and Approvals</i> 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 <i>Administration > Security</i> pages in the User Application.

Type of Setting	Field	Description
eDirectory DNs (continued)	<i>Roles Administrator</i>	<p>This role is available in the Novell Identity Manager Roles Based Provisioning Module. This role allows members to create, remove, or modify all roles, and grant or revoke any role assignment to any user, group, or container. It also allows its role members to run any report for any user. By default, the User Application Admin is assigned this role.</p> <p>To change this assignment after you deploy the User Application, use the <i>Roles > Role Assignment</i> page in the User Application.</p>
	<i>User Container DN</i>	<p>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.</p> <hr/> <p>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.</p>
	<i>Group Container DN</i>	<p>Required. Specify the LDAP distinguished name (DN) or fully qualified LDAP name of the group container.</p> <p>Used by entity definitions within the directory abstraction layer.</p>
eDirectory Certificates	<i>Keystore Path</i>	<p>Required. Specify the full path to your keystore (<code>cacerts</code>) file of the JDK that the application server application server is using to run, or click the small browser button and navigate to the <code>cacerts</code> file.</p> <p>On Linux or Solaris, the user must have permission to write to this file.</p>
	<i>Keystore Password/Confirm Keystore Password</i>	<p>Required. Specify the <code>cacerts</code> password. The default is <code>changeit</code>.</p>

Type of Setting	Field	Description
Email	<i>Notify Template Host Token</i>	Specify the application server hosting the Identity Manager User Application. For example: <code>myapplication serverServer</code> 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.
	<i>Notify Template Port Token</i>	Used to replace the \$PORT\$ token in e-mail templates used in provisioning request tasks and approval notifications.
	<i>Notify Template Secure Port Token</i>	Used to replace the \$SECURE_PORT\$ token in e-mail templates used in provisioning request tasks and approval notifications.
	<i>Notification SMTP Email From:</i>	Specify e-mail to come from a user in provisioning e-mail.
	<i>Notification SMTP Email Host:</i>	Specify the SMTP e-mail host that provisioning e-mail is using. This can be an IP address or a DNS name.
Password Management	<i>Use External Password WAR</i>	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 <i>Use External Password WAR</i> , you must supply values for <i>Forgot Password Link</i> and <i>Forgot Password Return Link</i> . If you do not select <i>Use External Password WAR</i> , IDM uses the default internal Password Management functionality, <code>./jsps/pwdmgt/ForgotPassword.jsf</code> (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.
	<i>Forgot Password Link</i>	This URL points to the Forgot Password functionality page. Specify a <code>ForgotPassword.jsf</code> file in an external or internal password management WAR. For details, see “Using Password WARs” on page 66 .
	<i>Forgot Password Return Link</i>	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 <code>https://idmhost:sslport/idm</code> .

2 If you want to set additional User Application configuration parameters, click *Show Advanced Options*. (Scroll to view the whole panel.) **Table 4-2** describes the Advanced Options parameters.

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

Table 4-2 *User Application Configuration: All Parameters*

Type of Setting	Field	Description
eDirectory Connection Settings	<i>LDAP Host</i>	Required. Specify the hostname or IP address for your LDAP server. For example: myLDAPhost
	<i>LDAP Non-Secure Port</i>	Specify the non-secure port for your LDAP server. For example: 389.
	<i>LDAP Secure Port</i>	Specify the secure port for your LDAP server. For example: 636.
	<i>LDAP Administrator</i>	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.
	<i>LDAP Administrator Password</i>	Required. Specify the LDAP Administrator password. This password is encrypted, based on the master key.
	<i>Use Public Anonymous Account</i>	Allows users who are not logged in to access the LDAP Public Anonymous Account.
	<i>LDAP Guest</i>	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 <i>Use Public Anonymous Account</i> . To disable Guest User, select <i>Use Public Anonymous Account</i> .
	<i>LDAP Guest Password</i>	Specify the LDAP Guest password.
	<i>Secure Admin Connection</i>	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.
	<i>Secure User Connection</i>	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	<i>Root Container DN</i>	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.
	<i>Provisioning Driver DN</i>	Required. Specify the distinguished name of the User Application driver that you created earlier in Section 3.1, "Creating the User Application Driver in iManager," on page 31 . For example, if your driver is <code>UserApplicationDriver</code> and your driver set is called <code>myDriverSet</code> , and the driver set is in a context of <code>o=myCompany</code> , you type a value of: <code>cn=UserApplicationDriver,cn=myDriverSet,o=myCompany</code>
	<i>User Application Admin</i>	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 <i>Administration</i> 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 (<i>Requests & Approvals</i> tab), you must grant this administrator appropriate trustee rights to object instances contained in the User Application driver. Refer to the <i>IDM User Application: Administration Guide</i> for details. To change this assignment after you deploy the User Application, you must use the <i>Administration > Security</i> pages in the User Application.
	<i>Provisioning Application Admin</i>	The Provisioning Application Administrator manages Provisioning Workflow functions available through the <i>Requests and Approvals</i> 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 <i>Administration > Security</i> pages in the User Application.

Type of Setting	Field	Description
Meta-Directory User Identity	<i>User Container DN</i>	<p>Required. Specify the LDAP distinguished name (DN) or fully qualified LDAP name of the user container.</p> <p>This defines the search scope for users and groups.</p> <p>Users in this container (and below) are allowed to log in to the User Application.</p> <hr/> <p>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.</p> <hr/>
	<i>User Object Class</i>	The LDAP user object class (typically inetOrgPerson).
	<i>Login Attribute</i>	The LDAP attribute (for example, CN) that represents the user's login name.
	<i>Naming Attribute</i>	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.
	<i>User Membership Attribute</i>	Optional. The LDAP attribute that represents the user's group membership. Do not use spaces in this name.
	<i>Roles Administrator</i>	<p>This role is available in the Novell Identity Manager Roles Based Provisioning Module. This role allows members to create, remove, or modify all roles, and grant or revoke any role assignment to any user, group, or container. It also allows its role members to run any report for any user. By default, the User Application Admin is assigned this role.</p> <p>To change this assignment after you deploy the User Application, use the <i>Roles > Role Assignment</i> page in the User Application.</p>

Type of Setting	Field	Description
Meta-Directory User Groups	<i>Group Container DN</i>	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.
	<i>Group Object Class</i>	The LDAP group object class (typically groupofNames).
	<i>Group Membership Attribute</i>	The attribute representing the user's group membership. Do not use spaces in this name.
	<i>Use Dynamic Groups</i>	Select this option if you want to use dynamic groups.
	<i>Dynamic Group Object Class</i>	The LDAP dynamic group object class (typically dynamicGroup).
eDirectory Certificates	<i>Keystore Path</i>	Required. Specify the full path to your keystore (<code>cacerts</code>) 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 <code>cacerts</code> file. The User Application installation modifies the keystore file. On Linux or Solaris, the user must have permission to write to this file.
	<i>Keystore Password</i>	Required. Specify the <code>cacerts</code> password. The default is <code>changeit</code> .
	<i>Confirm Keystore Password</i>	
Private Key Store	<i>Private Keystore Path</i>	The private keystore contains the User Application's private key and certificates. Reserved. If you leave this empty, this path is <code>/jre/lib/security/cacerts</code> by default.
	<i>Private Keystore Password</i>	This password is <code>changeit</code> unless you specify otherwise. This password is encrypted, based on the master key.
	<i>Private Key Alias</i>	This alias is <code>novellIDMUserApp</code> unless you specify otherwise.
	<i>Private Key Password</i>	This password is <code>novellIDM</code> unless you specify otherwise. This password is encrypted, based on the master key.

Type of Setting	Field	Description
Trusted Key Store	<i>Trusted Store Path</i>	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 <code>javax.net.ssl.trustStore</code> . If the path isn't there, it is assumed to be <code>jre/lib/security/cacerts</code> .
	<i>Trusted Store Password</i>	If this field is empty, the User Application gets the password from System property <code>javax.net.ssl.trustStorePassword</code> . If the value is not there, <code>changeit</code> 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.
	<i>Novell Audit Digital Signature Certificate</i>	Displays the digital signature certificate.
	<i>Novell Audit Digital Signature Private Key</i>	Displays the digital signature private key. This key is encrypted, based on the master key.
Access Manager & iChain Settings	<i>Simultaneous Logout Enabled</i>	If this option is selected, the User Application supports simultaneous logout of the User Application and either Novell Access Manager or iChain. The User Application checks for a Novell Access Manager™ or iChain® cookie on logout and, if the cookie is present, reroutes the user to the simultaneous logout page.
	<i>Simultaneous Logout Page</i>	The URL to the Novell Access Manager or iChain logout page, where the URL is a hostname that Novell Access Manager or iChain expects. If Simultaneous Logout is enabled and a user logs out of the User Application, the user is rerouted to this page. One of the two following URLs should direct the simultaneous logout feature to the correct page, depending on your environment: Access Manager: <code>https://yourAccessGatewayServer/AGLogout</code> iChain: <code>https://youriChainServer/cmd/ICSLogout</code>

Type of Setting	Field	Description
Email	<i>Notify Template Host Token</i>	Specify the application server hosting the Identity Manager User Application. For example: <code>myapplication serverServer</code> 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.
	<i>Notify Template Port Token</i>	Used to replace the \$PORT\$ token in e-mail templates used in provisioning request tasks and approval notifications.
	<i>Notify Template Secure Port Token</i>	Used to replace the \$SECURE_PORT\$ token in e-mail templates used in provisioning request tasks and approval notifications.
	<i>Notify Template PROTOCOL token</i>	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.
	<i>Notify Template SECURE PROTOCOL token</i>	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.
	<i>Notification SMTP Email From:</i>	Specify e-mail from a user in provisioning e-mail.
	<i>Notification SMTP Email Host:</i>	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	<i>Use External Password WAR</i>	<p>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.</p> <p>If you select <i>Use External Password WAR</i>, you must supply values for <i>Forgot Password Link</i> and <i>Forgot Password Return Link</i>.</p> <p>If you do not select <i>Use External Password WAR</i>, IDM uses the default internal Password Management functionality, <code>./jssps/pwdmgt/ForgotPassword.jsf</code> (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.</p>
	<i>Forgot Password Link</i>	<p>This URL points to the Forgot Password functionality page. Specify a <code>ForgotPassword.jsf</code> file in an external or internal password management WAR. For details, see “Using Password WARs” on page 66.</p>
	<i>Forgot Password Return Link</i>	<p>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 <code>https://idmhost:sslport/idm</code>.</p>
Miscellaneous	<i>Session Timeout</i>	The application session timeout.
	<i>OCSP URI</i>	<p>If the client installation uses the On-Line Certificate Status Protocol (OCSP), supply a Uniform Resource Identifier (URI). For example, the format is <code>http://host:port/ocspLocal</code>. The OCSP URI updates the status of trusted certificates online.</p>
	<i>Authorization Config Path</i>	Fully qualified name of the authorization configuration file.

Type of Setting	Field	Description
Container Object	<i>Selected</i>	Select each Container Object Type to use.
	<i>Container Object Type</i>	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 <i>Add a new Container Object</i> .
	<i>Container Attribute Name</i>	Lists the Attribute Type name associated with the Container Object Type.
	<i>Add a New Container Object: Container Object Type</i>	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) .
	<i>Add a New Container Object: Container Attribute Name</i>	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 4.16, “Verify Choices and Install,”](#) on page 67

4.15 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.

- [Section 4.15.1, “Specifying an External Password Management WAR,”](#) on page 66
- [Section 4.15.2, “Specifying an Internal Password WAR,”](#) on page 67

4.15.1 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/jsp/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 7.4, “Configuring SSL Communication between JBoss Servers,” on page 110](#).

- 5 Do one of the following:

- ♦ If you are using the installer, read the information in this step and proceed to [Step 6 on page 67](#).
- ♦ 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 67](#).

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/jsp/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.

4.15.2 Specifying an Internal Password WAR

- 1 In the User Application configuration parameters, 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*.

4.16 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*.

4.17 View Log Files

- 1 If your installation completed without error, go to [Chapter 7, “Post-Installation Tasks,” on page 109](#).
- 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 in solving problems, see [Section 7.12, “Troubleshooting,”](#) on page 112.

Installing from the Console or With a Single Command

This section describes installation methods you can use instead of installing with a graphical user interface, which was described in [Chapter 4, “Installing on JBoss Using a GUI,” on page 37](#). Topics include:

- [Section 5.1, “Installing the User Application from the Console,” on page 69](#)
- [Section 5.2, “Installing the User Application with a Single Command,” on page 69](#)

5.1 Installing the User Application from the Console

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

- 1 Obtain the appropriate installation files described in [Table 2-1 on page 26](#).
- 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 [Chapter 4, “Installing on JBoss Using a GUI,” on page 37](#), 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, 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 4.14, “Configuring the User Application,” on page 53](#).
- 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 [Chapter 7, “Post-Installation Tasks,” on page 109](#).

5.2 Installing the User Application with a Single Command

This procedure 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 2-1 on page 26](#).
- 2 Log in and open a terminal session.
- 3 Locate the Identity Manager 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 5-1](#) 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 5-1 *User Application Configuration Parameters for a Silent Install*

User Application Parameter Name in <code>silent.properties</code>	Equivalent Parameter Name in the User Application Configuration Parameters File
NOVL_CONFIG_LDAPHOST=	eDirectory Connection Settings: LDAP Host. Specify the hostname or IP address for your LDAP server.
NOVL_CONFIG_LDAPADMIN=	eDirectory Connection Settings: LDAP Administrator. 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. Specify the LDAP Administrator password. This password is encrypted, based on the master key.
NOVL_CONFIG_ROOTCONTAINERNAME=	eDirectory DNs: Root Container DN. 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
NOVL_CONFIG_PROVISIONROOT=	<p>eDirectory DNs: Provisioning Driver DN.</p> <p>Specify the distinguished name of the User Application driver that you created earlier in Section 3.1, “Creating the User Application Driver in iManager,” on page 31. 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: <code>cn=UserApplicationDriver,cn=myDriverSet,o=myCompany</code></p>
NOVL_CONFIG_LOCKSMITH=	<p>eDirectory DNs: User Application Admin.</p> <p>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 <i>Administration</i> tab of the User Application to administer the portal.</p> <p>If the User Application Administrator participates in workflow administration tasks exposed in iManager, Novell Designer for Identity Manager, or the User Application (<i>Requests & Approvals</i> tab), you must grant this administrator appropriate trustee rights to object instances contained in the User Application driver. Refer to the <i>IDM User Application: Administration Guide</i> for details.</p> <p>To change this assignment after you deploy the User Application, you must use the <i>Administration > Security</i> pages in the User Application.</p>
NOVL_CONFIG_PROVLOCKSMITH=	<p>eDirectory DNs: Provisioning Application Admin.</p> <p>This role is available in the provisioning version of Identity Manager. The Provisioning Application Administrator uses the <i>Provisioning</i> tab (under the <i>Administration</i> tab) to manage the Provisioning Workflow functions. These functions are available to users through the <i>Requests and Approvals</i> tab of the User Application. This user must exist in the Identity Vault prior to being designated the Provisioning Application Administrator.</p> <p>To change this assignment after you deploy the User Application, you must use the <i>Administration > Security</i> pages in the User Application.</p>

User Application Parameter Name in silent.properties	Equivalent Parameter Name in the User Application Configuration Parameters File
NOVL_CONFIG_ROLECONTAINERDN=	<p>This role is available in the Novell Identity Manager Roles Based Provisioning Module. This role allows members to create, remove, or modify all roles, and grant or revoke any role assignment to any user, group, or container. It also allows its role members to run any report for any user. By default, the User Application Admin is assigned this role.</p> <p>To change this assignment after you deploy the User Application, use the <i>Roles > Role Assignment</i> page in the User Application.</p>
NOVL_CONFIG_USERCONTAINERDN=	<p>Meta-Directory User Identity: User Container DN.</p> <p>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.</p> <hr/> <p>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.</p>
NOVL_CONFIG_GROUPCONTAINERDN=	<p>Meta-Directory User Groups: Group Container DN.</p> <p>Specify the LDAP distinguished name (DN) or fully qualified LDAP name of the group container. Used by entity definitions within the directory abstraction layer.</p>
NOVL_CONFIG_KEYSTOREPATH=	<p>eDirectory Certificates: Keystore Path. Required.</p> <p>Specify the full path to your keystore (<i>cacerts</i>) 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.</p>
NOVL_CONFIG_KEYSTOREPASSWORD=	<p>eDirectory Certificates: Keystore Password.</p> <p>Specify the <i>cacerts</i> password. The default is <i>changeit</i>.</p>
NOVL_CONFIG_SECUREADMINCONNECTION=	<p>eDirectory Connection Settings: Secure Admin Connection.</p> <p>Required. Specify <i>True</i> 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.</p> <p>Specify <i>False</i> if the admin account does not use secure socket communication.</p>

User Application Parameter Name in silent.properties	Equivalent Parameter Name in the User Application Configuration Parameters File
NOVL_CONFIG_SECUREUSERCONNECTION=	<p>eDirectory Connection Settings: Secure User Connection.</p> <p>Required. Specify <i>True</i> 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.</p> <p>Specify <i>False</i> if the user's account does not use secure socket communication.</p>
NOVL_CONFIG_SESSIONTIMEOUT=	<p>Miscellaneous: Session Timeout.</p> <p>Required. Specify an application session timeout interval.</p>
NOVL_CONFIG_LDAPPLAINPORT=	<p>eDirectory Connection Settings: LDAP Non-Secure Port.</p> <p>Required. Specify the non-secure port for your LDAP server, for example 389.</p>
NOVL_CONFIG_LDAPSECUREPORT=	<p>eDirectory Connection Settings: LDAP Secure Port.</p> <p>Required. Specify the secure port for your LDAP server, for example 636.</p>
NOVL_CONFIG_ANONYMOUS=	<p>eDirectory Connection Settings: Use Public Anonymous Account.</p> <p>Required. Specify <i>True</i> to allow users who are not logged in to access the LDAP Public Anonymous Account.</p> <p>Specify <i>False</i> to enable NOVL_CONFIG_GUEST instead.</p>
NOVL_CONFIG_GUEST=	<p>eDirectory Connection Settings: LDAP Guest.</p> <p>Allows users who are not logged in to access permitted portlets. You must also deselect <i>Use Public Anonymous Account</i>. The Guest user account must already exist in the Identity Vault. To disable the Guest user, select <i>Use Public Anonymous Account</i>.</p>
NOVL_CONFIG_GUESTPASS=	<p>eDirectory Connection Settings: LDAP Guest Password.</p>

User Application Parameter Name in silent.properties	Equivalent Parameter Name in the User Application Configuration Parameters File
NOVL_CONFIG_EMAILNOTIFYHOST=	<p>Email: Notify Template HOST token.</p> <p>Specify the application server hosting the Identity Manager User Application. For example: <code>myapplication serverServer</code></p> <p>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.</p>
NOVL_CONFIG_EMAILNOTIFYPORT=	<p>Email: Notify Template Port token.</p> <p>Used to replace the \$PORT\$ token in e-mail templates used in provisioning request tasks and approval notifications.</p>
NOVL_CONFIG_EMAILNOTIFYSECUREPORT=	<p>Email: Notify Template Secure Port token.</p> <p>Used to replace the \$SECURE_PORT\$ token in e-mail templates used in provisioning request tasks and approval notifications</p>
NOVL_CONFIG_NOTFSMTPEMAILFROM=	<p>Email: Notification SMTP Email From.</p> <p>Required. Specify e-mail From a user in provisioning e-mail.</p>
NOVL_CONFIG_NOTFSMTPEMAILHOST=	<p>Email: Notification SMTP Email Host.</p> <p>Required. Specify the SMTP e-mail host that provisioning e-mail is using. This can be an IP address or a DNS name.</p>
NOVL_CONFIG_USEEXTPWDWAR=	<p>Password Management: Use External Password WAR.</p> <p>Specify <i>True</i> if you are using an external password management WAR. If you specify <i>True</i>, you must also supply values for <code>NOVL_CONFIG_EXTPWDWARPTH</code> and <code>NOVL_CONFIG_EXTPWDWARRTPATH</code>.</p> <p>Specify <i>False</i> to use the default internal Password Management functionality, <code>./jsps/pwdmgt/ForgotPassword.jsf</code> (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.</p>
NOVL_CONFIG_EXTPWDWARPATH=	<p>Password Management: Forgot Password Link.</p> <p>Specify the URL for the Forgot Password functionality page, <code>ForgotPassword.jsf</code>, in an external or internal password management WAR. Or, accept the default internal password management WAR. For details, see “Using Password WARs” on page 66</p>

User Application Parameter Name in silent.properties	Equivalent Parameter Name in the User Application Configuration Parameters File
NOVL_CONFIG_EXTPWDWARRTPATH=	<p>Password Management: Forgot Password Return Link.</p> <p>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 <code>https://idmhost:sslport/idm</code>.</p>
NOVL_CONFIG_USEROBJECTATTRIBUTE=	<p>Meta-Directory User Identity: User Object Class.</p> <p>Required. The LDAP user object class (typically <code>inetOrgPerson</code>).</p>
NOVL_CONFIG_LOGINATTRIBUTE=	<p>Meta-Directory User Identity: Login Attribute.</p> <p>Required. The LDAP attribute (for example, <code>CN</code>) that represents the user's login name.</p>
NOVL_CONFIG_NAMINGATTRIBUTE=	<p>Meta-Directory User Identity: Naming Attribute.</p> <p>Required. 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.</p>
NOVL_CONFIG_USERMEMBERSHIPATTRIBUTE=	<p>Meta-Directory User Identity: User Membership Attribute. Optional.</p> <p>Required. The LDAP attribute that represents the user's group membership. Do not use spaces in this name.</p>
NOVL_CONFIG_GROUPOBJECTATTRIBUTE=	<p>Meta-Directory User Groups: Group Object Class.</p> <p>Required. The LDAP group object class (typically <code>groupofNames</code>).</p>
NOVL_CONFIG_GROUPMEMBERSHIPATTRIBUTE=	<p>Meta-Directory User Groups: Group Membership Attribute.</p> <p>Required. Specify the attribute representing the user's group membership. Do not use spaces in this name.</p>
NOVL_CONFIG_USEDYNAMICGROUPS=	<p>Meta-Directory User Groups: Use Dynamic Groups.</p> <p>Required. Specify <i>True</i> to use dynamic groups. Otherwise, specify <i>False</i>.</p>
NOVL_CONFIG_DYNAMICGROUPOBJECTCLASS=	<p>Meta-Directory User Groups: Dynamic Group Object Class.</p> <p>Required. Specify the LDAP dynamic group object class (typically <code>dynamicGroup</code>).</p>

User Application Parameter Name in silent.properties	Equivalent Parameter Name in the User Application Configuration Parameters File
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 <code>/jre/lib/security/cacerts</code> by default.
NOVL_CONFIG_PRIVATESTOREPASSWORD=	Private Key Store: Private Keystore Password.
NOVL_CONFIG_PRIVATEKEYALIAS=	Private Key Store: Private Key Alias. This alias is <code>novellIDMUserApp</code> 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 <code>javax.net.ssl.trustStore</code> . If the path isn't there, it is assumed to be <code>jre/lib/security/cacerts</code> .
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=	Access Manager and iChain Settings: Simultaneous Logout Enabled. Specify <i>True</i> to enable simultaneous logout of the User Application and either Novell Access Manager™ or iChain®. The User Application checks for a Novell Access Manager or iChain cookie on logout and, if the cookie is present, reroutes the user to the ICS logout page. Specify <i>False</i> to disable simultaneous logout.
NOVL_CONFIG_ICSLOGOUTPAGE=	Access Manager and iChain Settings: Simultaneous Logout Page. Specify the URL to the Novell Access Manager or iChain logout page, where the URL is a hostname that Novell Access Manager or iChain expects. If ICS logging is enabled and a user logs out of the User Application, the user is rerouted to this page.

User Application Parameter Name in silent.properties	Equivalent Parameter Name in the User Application Configuration Parameters File
NOVL_CONFIG_EMAILNOTIFYPROTOCOL=	<p>Email: Notify Template PROTOCOL token.</p> <p>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.</p>
NOVL_CONFIG_EMAILNOTIFYSECUREPROTOCOL=	Email: Notify Template Secure Port token.
NOVL_CONFIG_OCSPURI=	<p>Miscellaneous: OCSP URI.</p> <p>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.</p>
NOVL_CONFIG_AUTHCONFIGPATH=	<p>Miscellaneous: Authorization Config Path.</p> <p>The fully qualified name of the authorization configuration file.</p>

Installing on a WebSphere Application Server

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

- ◆ [Section 6.1, “Launching the Installer GUI,” on page 79](#)
- ◆ [Section 6.2, “Choosing an Application Server Platform,” on page 80](#)
- ◆ [Section 6.3, “Specifying the Location of the WAR,” on page 81](#)
- ◆ [Section 6.4, “Choosing an Install Folder,” on page 83](#)
- ◆ [Section 6.5, “Choosing a Database Platform,” on page 84](#)
- ◆ [Section 6.6, “Specifying the Java Root Directory,” on page 86](#)
- ◆ [Section 6.7, “Enabling Novell Audit Logging,” on page 87](#)
- ◆ [Section 6.8, “Specifying a Master Key,” on page 88](#)
- ◆ [Section 6.9, “Configuring the User Application,” on page 89](#)
- ◆ [Section 6.10, “Verify Choices and Install,” on page 103](#)
- ◆ [Section 6.11, “View Log Files,” on page 104](#)
- ◆ [Section 6.12, “Adding User Application Configuration Files and JVM System Properties,” on page 104](#)
- ◆ [Section 6.13, “Import the eDirectory Trusted Root to the WebSphere Keystore,” on page 105](#)
- ◆ [Section 6.14, “Deploying the IDM WAR File,” on page 106](#)
- ◆ [Section 6.15, “Starting the Application,” on page 107](#)
- ◆ [Section 6.16, “Accessing the User Application Portal,” on page 107](#)

6.1 Launching the Installer GUI

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

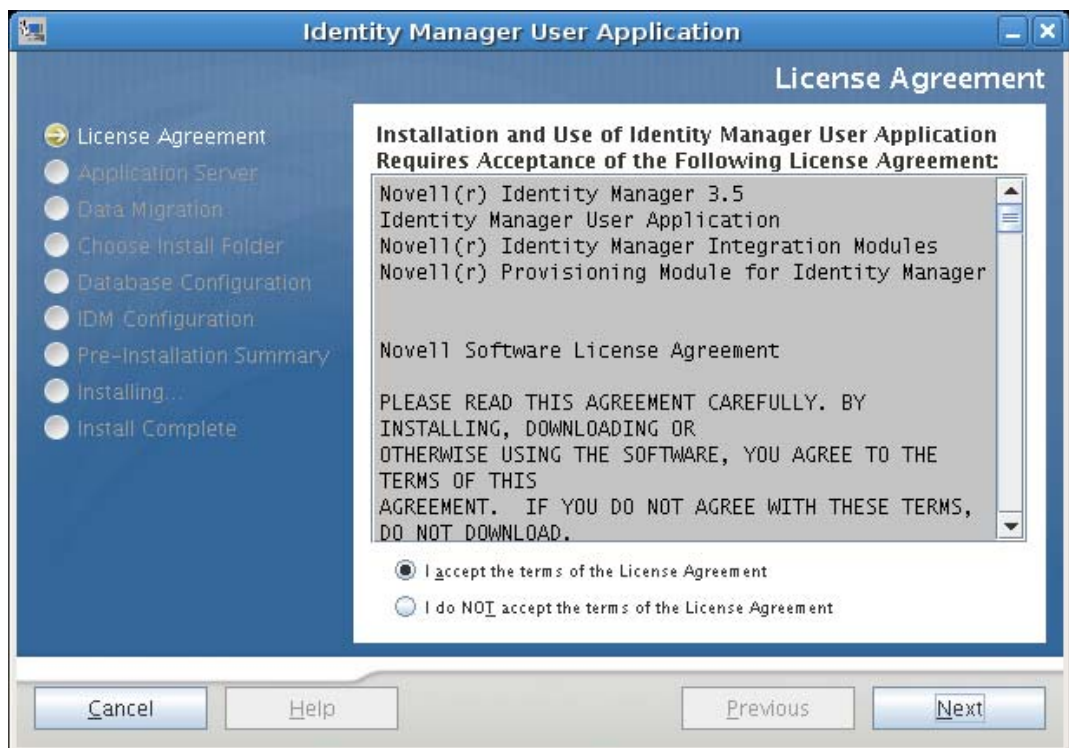
```
java -jar IdmUserApp.jar
```

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

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



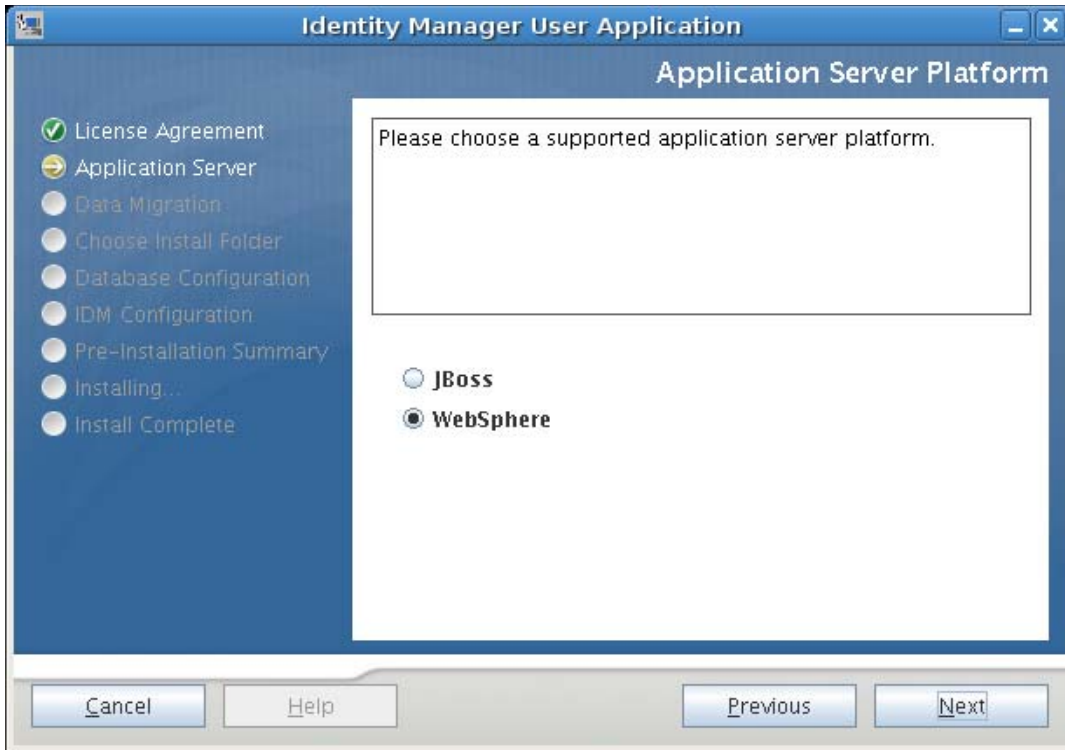
- 4 Read the license agreement, click *I accept the terms of the License Agreement*, then click *Next*.



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

6.2 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 6.3, “Specifying the Location of the WAR,” on page 81](#).

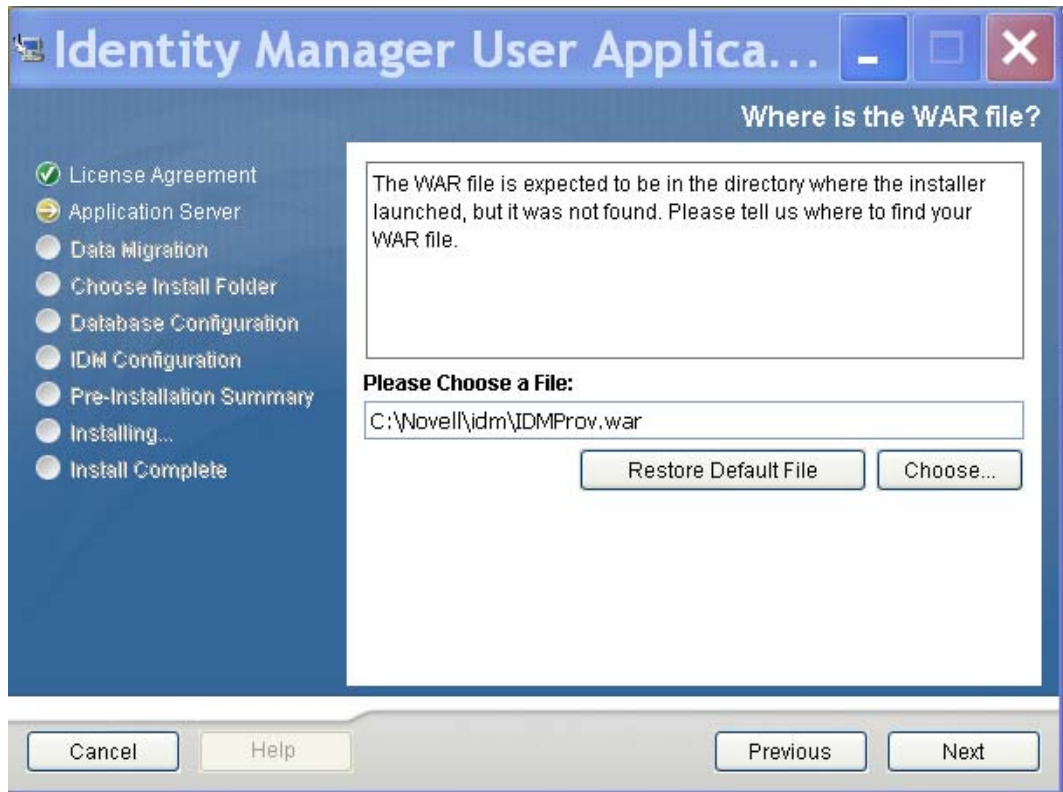


6.3 Specifying the Location of the WAR

Complete the procedure in [Section 6.1, “Launching the Installer GUI,”](#) on page 79, then continue with the steps below:

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.

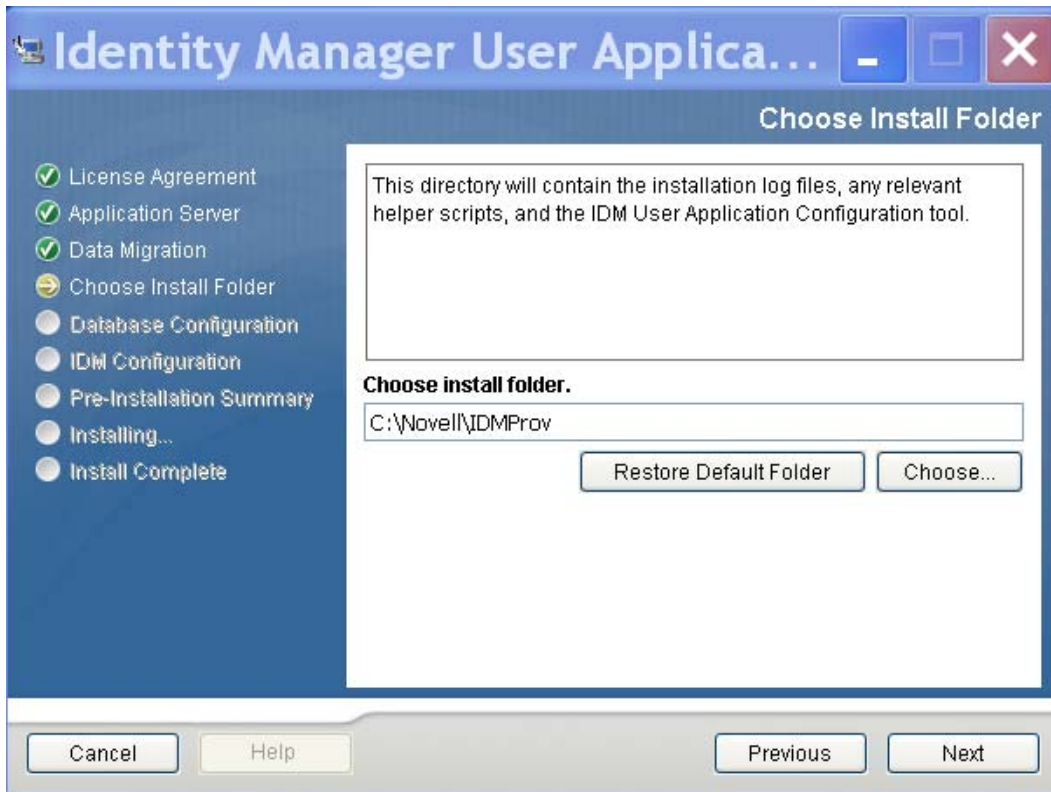
- 1 If the WAR is in the default location, you can click *Restore Default Folder*. Or, to specify the location of the WAR file, click *Choose* and select a location.



- 2 Click *Next*, then continue with [Section 6.4, "Choosing an Install Folder,"](#) on page 83.

6.4 Choosing an Install Folder

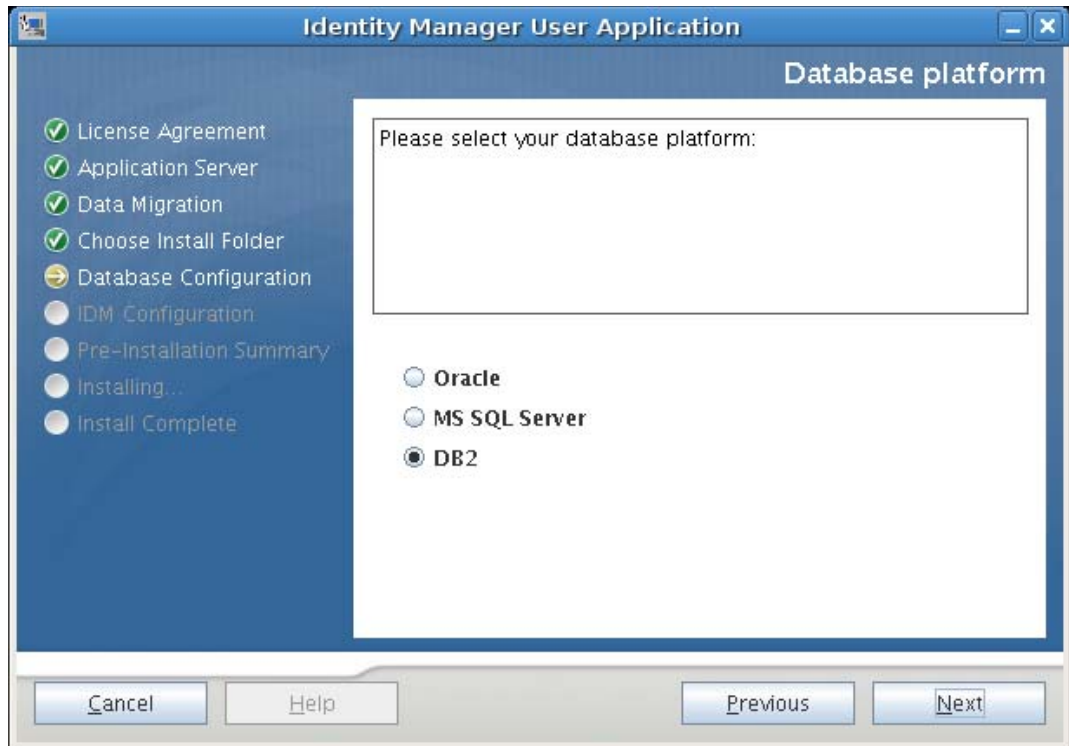
- 1 On the Choose Install Folder page, select where to install the User Application. If you want to use the default location, click *Restore Default Folder*, or if you want to choose another location for the installation files, click *Choose* and browse to a location.



- 2 Click *Next*, then continue with [Section 6.5, “Choosing a Database Platform,”](#) on page 84.

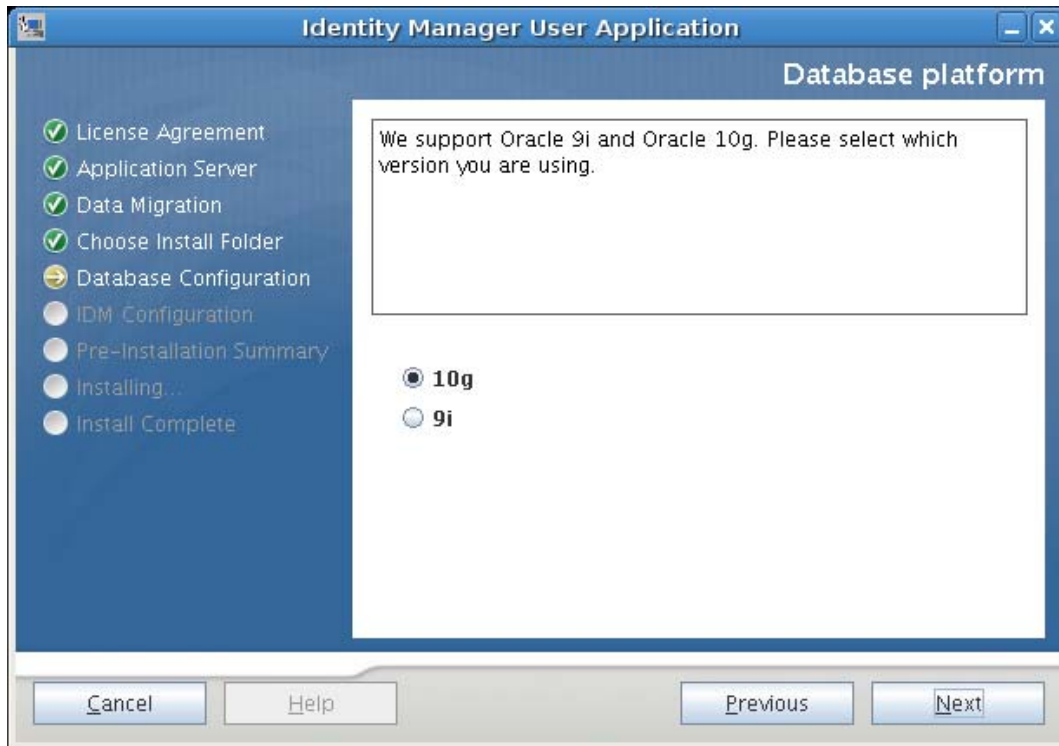
6.5 Choosing a Database Platform

- 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.

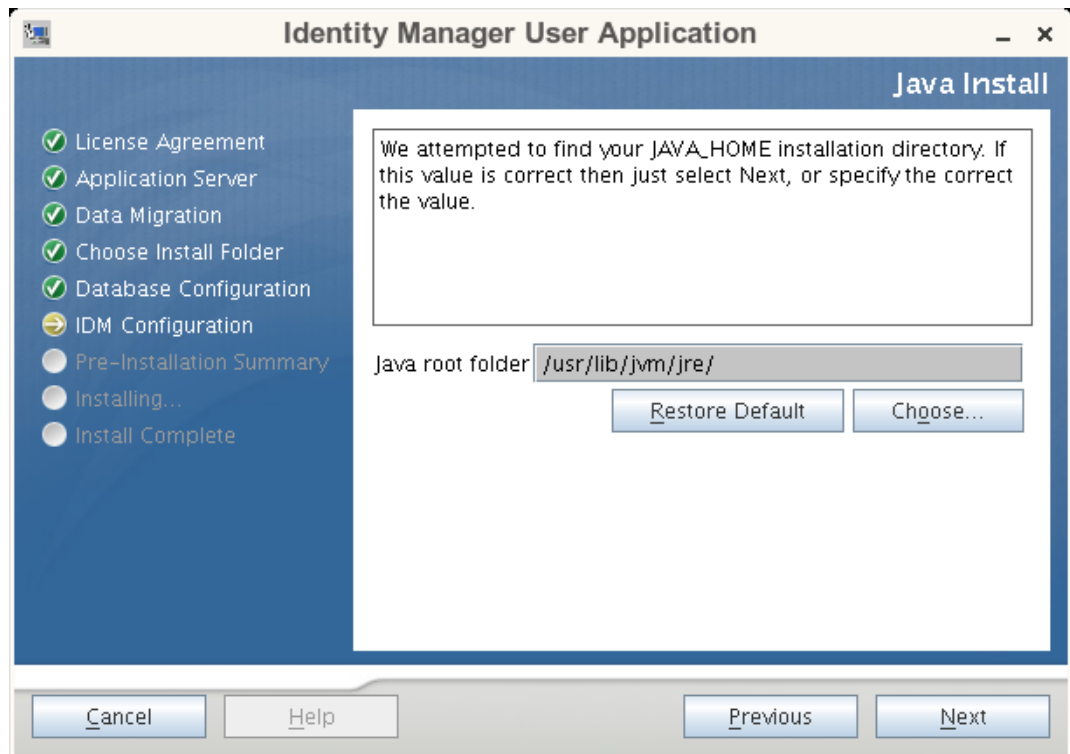


- 4 Click *Next*, then continue with [Section 6.6, “Specifying the Java Root Directory,”](#) on page 86.

6.6 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*.

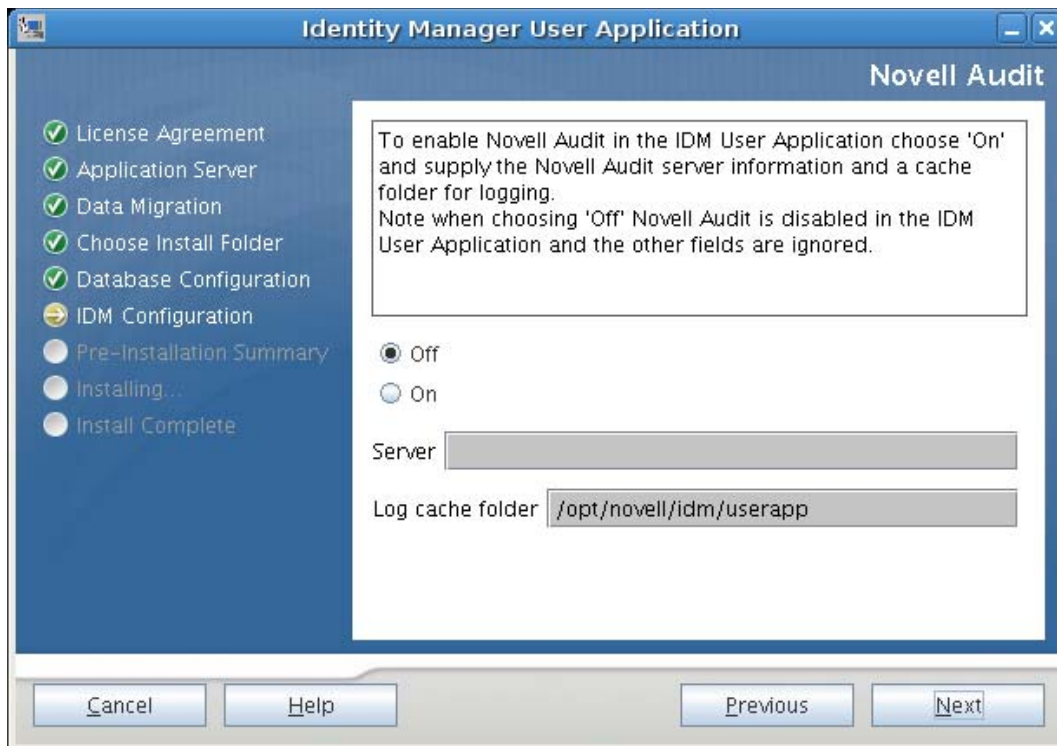


- 2 Click *Next*, then continue with [Section 6.7, “Enabling Novell Audit Logging,”](#) on page 87.

6.7 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 by using the <i>Administration</i> tab of the User Application. For more information on enabling Novell Audit logging, see the <i>Identity Manager User Application: Administration Guide</i> .
On	Enables Novell Audit Logging for the User Application. For more information on setting up Novell Audit logging, see the <i>Identity Manager User Application: Administration Guide</i> .
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.

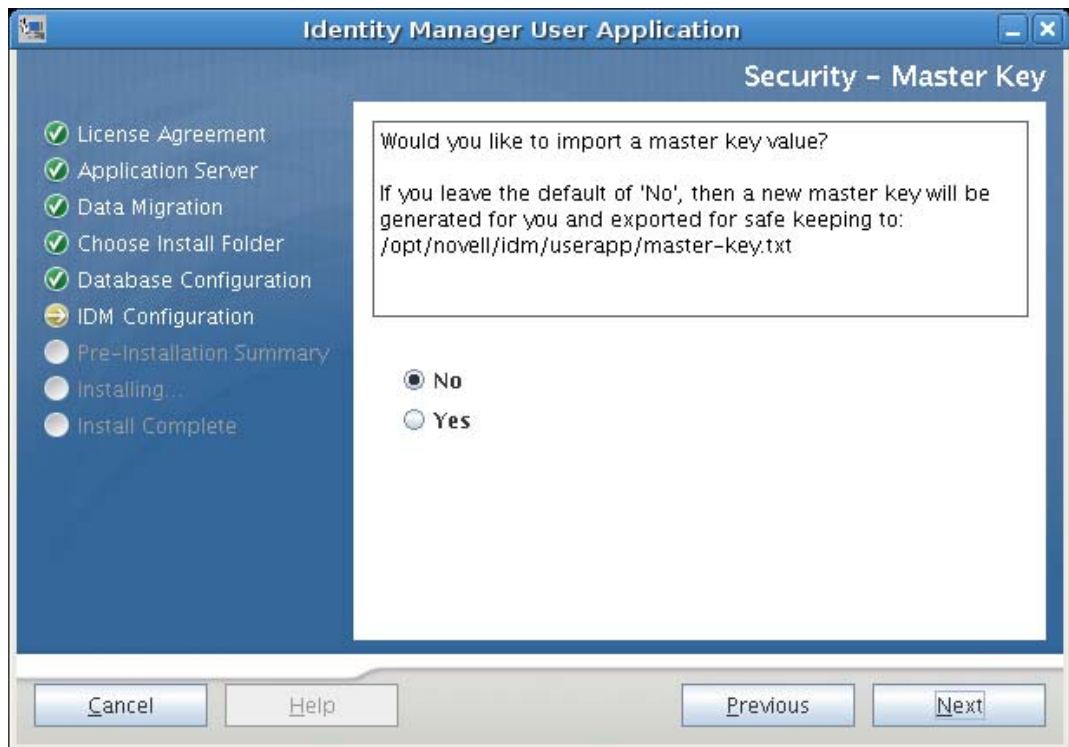
- 2 Click *Next* and continue with [Section 6.8, “Specifying a Master Key,” on page 88](#).

6.8 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 6.9, “Configuring the User Application,” on page 89](#). After you finish the installation, you must manually record the master key.

If you chose *Yes*, continue with [Step 3 on page 89](#).

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



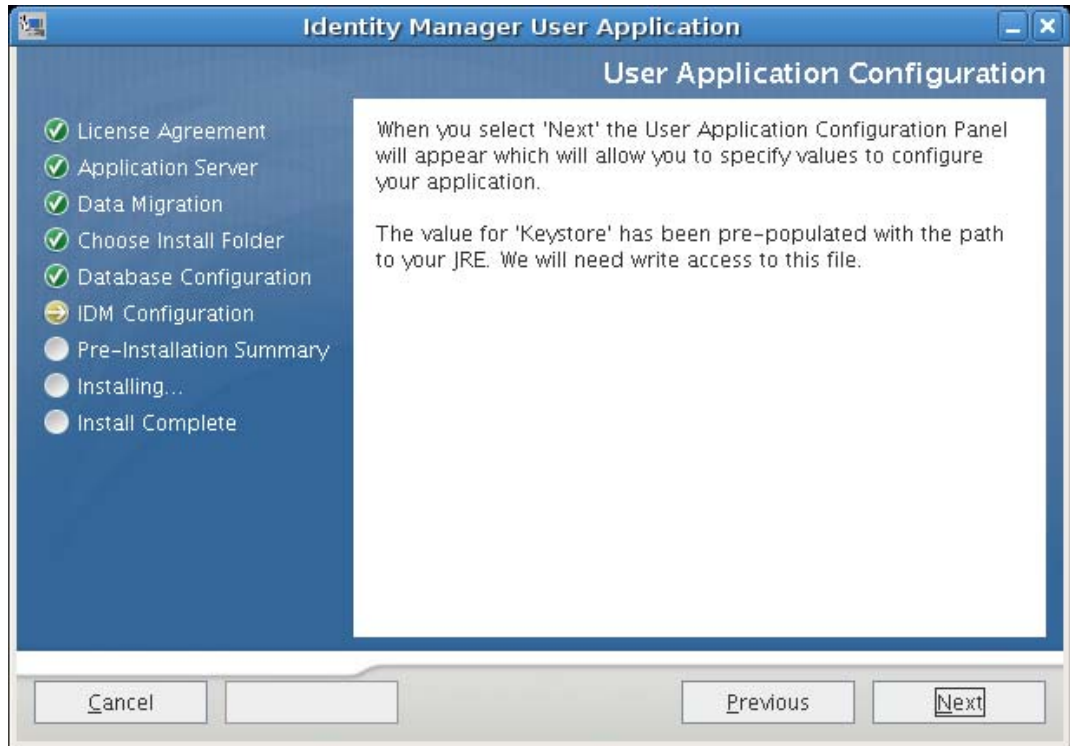
- 4 Click *Next* and continue with [Section 6.9, “Configuring the User Application,”](#) on page 89.

6.9 Configuring the User Application

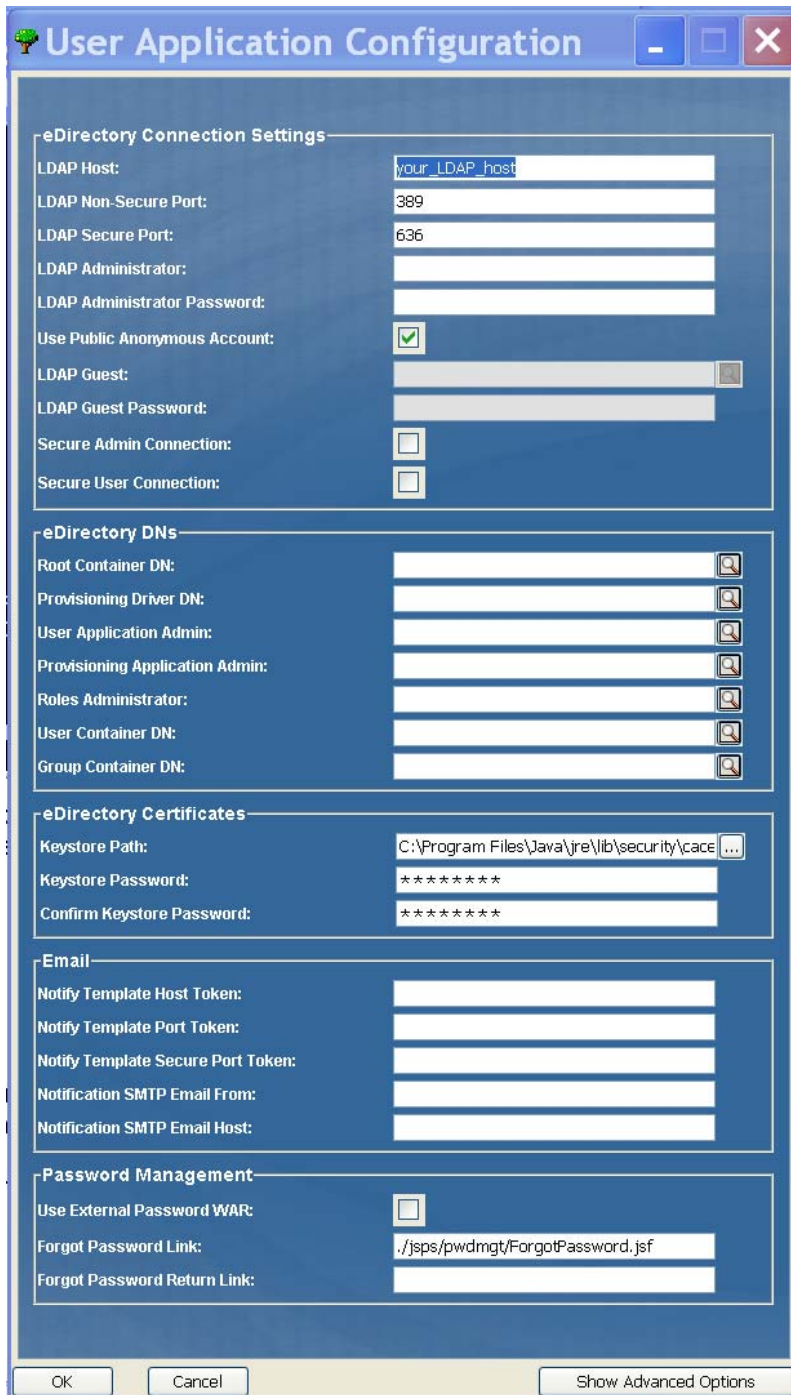
The User Application install enables you to set User Application configuration parameters. Most of these parameters are also editable with `configupdate.sh` or `configupdate.bat` after

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 6-1 on page 92, then continue with Step 3.



The image shows a 'User Application Configuration' dialog box with several sections for setting LDAP and application parameters.

eDirectory Connection Settings

- LDAP Host: your_LDAP_host
- LDAP Non-Secure Port: 389
- LDAP Secure Port: 636
- LDAP Administrator: [empty]
- LDAP Administrator Password: [empty]
- Use Public Anonymous Account:
- LDAP Guest: [empty]
- LDAP Guest Password: [empty]
- Secure Admin Connection:
- Secure User Connection:

eDirectory DNs

- Root Container DN: [empty]
- Provisioning Driver DN: [empty]
- User Application Admin: [empty]
- Provisioning Application Admin: [empty]
- Roles Administrator: [empty]
- User Container DN: [empty]
- Group Container DN: [empty]

eDirectory Certificates

- Keystore Path: C:\Program Files\Java\jre\lib\security\cacerts
- Keystore Password: *****
- Confirm Keystore Password: *****

Email

- Notify Template Host Token: [empty]
- Notify Template Port Token: [empty]
- Notify Template Secure Port Token: [empty]
- Notification SMTP Email From: [empty]
- Notification SMTP Email Host: [empty]

Password Management

- Use External Password WAR:
- Forgot Password Link: ./jsps/pwdmgt/ForgotPassword.jsf
- Forgot Password Return Link: [empty]

Buttons: OK, Cancel, Show Advanced Options

Table 6-1 *User Application Configuration: Basic Parameters*

Type of Setting	Field	Description
eDirectory Connection Settings	<i>LDAP Host</i>	Required. Specify the hostname or IP address for your LDAP server and its secure port. For example: <code>myLDAPhost</code>
	<i>LDAP Non-Secure Port</i>	Specify the non-secure port for your LDAP server. For example: 389.
	<i>LDAP Secure Port</i>	Specify the secure port for your LDAP server. For example: 636.
	<i>LDAP Administrator</i>	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.
	<i>LDAP Administrator Password</i>	Required. Specify the LDAP Administrator password. This password is encrypted, based on the master key.
	<i>Use Public Anonymous Account</i>	Allows users who are not logged in to access the LDAP Public Anonymous Account.
	<i>LDAP Guest</i>	Allows users who are not logged in to access permitted portlets. This user account must already exist in the Identity Vault. To enable the LDAP Guest, you must deselect <i>Use Public Anonymous Account</i> . To disable the Guest User, select <i>Use Public Anonymous Account</i> .
	<i>LDAP Guest Password</i>	Specify the LDAP Guest password.
	<i>Secure Admin Connection</i>	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.
	<i>Secure User Connection</i>	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	<i>Root Container DN</i>	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.
	<i>Provisioning Driver DN</i>	Required. Specify the distinguished name of the User Application driver. For example, if your driver is <code>UserApplicationDriver</code> and your driver set is called <code>myDriverSet</code> , and the driver set is in a context of <code>o=myCompany</code> , you would type a value of: <code>cn=UserApplicationDriver, cn=myDriverSet, o=myCompany</code>
	<i>User Application Admin</i>	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 <i>Administration</i> 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 (<i>Requests & Approvals</i> tab), you must grant this administrator appropriate trustee rights to object instances contained in the User Application driver. Refer to the <i>IDM User Application: Administration Guide</i> for details. To change this assignment after you deploy the User Application, you must use the <i>Administration > Security</i> pages in the User Application.
	<i>Provisioning Application Admin</i>	The Provisioning Application Administrator uses the <i>Provisioning</i> tab (under the <i>Administration</i> tab) to manage the Provisioning Workflow functions. These functions are available to users through the <i>Requests and Approvals</i> 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 <i>Administration > Security</i> pages in the User Application.

Type of Setting	Field	Description
eDirectory DNs (continued)	<i>Roles Administrator</i>	<p>This role is available in the Novell Identity Manager Roles Based Provisioning Module. This role allows members to create, remove, or modify all roles, and grant or revoke any role assignment to any user, group, or container. It also allows its role members to run any report for any user. By default, the User Application Admin is assigned this role.</p> <p>To change this assignment after you deploy the User Application, use the <i>Roles > Role Assignment</i> page in the User Application.</p>
	<i>User Container DN</i>	<p>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.</p> <hr/> <p>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.</p>
	<i>Group Container DN</i>	<p>Required. Specify the LDAP distinguished name (DN) or fully qualified LDAP name of the group container.</p> <p>Used by entity definitions within the directory abstraction layer.</p>
eDirectory Certificates	<i>Keystore Path</i>	<p>Required. Specify the full path to your keystore (<code>cacerts</code>) file of the JDK that the application server application server is using to run, or click the small browser button and navigate to the <code>cacerts</code> file.</p> <p>On Linux or Solaris, the user must have permission to write to this file.</p>
	<i>Keystore Password/Confirm Keystore Password</i>	<p>Required. Specify the <code>cacerts</code> password. The default is <code>changeit</code>.</p>

Type of Setting	Field	Description
Email	<i>Notify Template Host Token</i>	Specify the application server hosting the Identity Manager User Application. For example: <code>myapplication serverServer</code> 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.
	<i>Notify Template Port Token</i>	Used to replace the \$PORT\$ token in e-mail templates used in provisioning request tasks and approval notifications.
	<i>Notify Template Secure Port token</i>	Used to replace the \$SECURE_PORT\$ token in e-mail templates used in provisioning request tasks and approval notifications.
	<i>Notification SMTP Email From:</i>	Specify e-mail to come from a user in provisioning e-mail.
	<i>Notification SMTP Email Host:</i>	Specify the SMTP e-mail host that provisioning e-mail is using. This can be an IP address or a DNS name.
Password Management	<i>Use External Password WAR</i>	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 <i>Use External Password WAR</i> , you must supply values for <i>Forgot Password Link</i> and <i>Forgot Password Return Link</i> . If you do not select <i>Use External Password WAR</i> , IDM uses the default internal Password Management functionality, <code>./jsps/pwdmgt/ForgotPassword.jsf</code> (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.
	<i>Forgot Password Link</i>	This URL points to the Forgot Password functionality page. Specify a <code>ForgotPassword.jsf</code> file in an external or internal password management WAR.
	<i>Forgot Password Return Link</i>	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 <code>https://idmhost:sslport/idm</code> .

- 3** If you want to set additional User Application configuration parameters, click *Show Advanced Options*. (Scroll to view the whole panel.) Table [Table 6-2 on page 96](#) describes the Advanced

Options parameters. If you do not want to set additional parameters described in this step, skip to [Step 4](#).

Table 6-2 *User Application Configuration: All Parameters*

Type of Setting	Field	Description
eDirectory Connection Settings	<i>LDAP Host</i>	Required. Specify the hostname or IP address for your LDAP server. For example: myLDAPhost
	<i>LDAP Non-Secure Port</i>	Specify the non-secure port for your LDAP server. For example: 389.
	<i>LDAP Secure Port</i>	Specify the secure port for your LDAP server. For example: 636.
	<i>LDAP Administrator</i>	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.
	<i>LDAP Administrator Password</i>	Required. Specify the LDAP Administrator password. This password is encrypted, based on the master key.
	<i>Use Public Anonymous Account</i>	Allows users who are not logged in to access the LDAP Public Anonymous Account.
	<i>LDAP Guest</i>	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 <i>Use Public Anonymous Account</i> . To disable Guest User, select <i>Use Public Anonymous Account</i> .
	<i>LDAP Guest Password</i>	Specify the LDAP Guest password.
	<i>Secure Admin Connection</i>	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.
<i>Secure User Connection</i>	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	<i>Root Container DN</i>	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.
	<i>Provisioning Driver DN</i>	Required. Specify the distinguished name of the User Application driver. For example, if your driver is <code>UserApplicationDriver</code> and your driver set is called <code>myDriverSet</code> , and the driver set is in a context of <code>o=myCompany</code> , you type a value of: <code>cn=UserApplicationDriver,cn=myDriverSet,o=myCompany</code>
	<i>User Application Admin</i>	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 <i>Administration</i> 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 (<i>Requests & Approvals</i> tab), you must grant this administrator appropriate trustee rights to object instances contained in the User Application driver. Refer to the <i>IDM User Application: Administration Guide</i> for details. To change this assignment after you deploy the User Application, you must use the <i>Administration > Security</i> pages in the User Application.
	<i>Provisioning Application Admin</i>	The Provisioning Application Administrator manages Provisioning Workflow functions available through the <i>Requests and Approvals</i> 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 <i>Administration > Security</i> pages in the User Application.

Type of Setting	Field	Description
Meta-Directory User Identity	<i>User Container DN</i>	<p>Required. Specify the LDAP distinguished name (DN) or fully qualified LDAP name of the user container.</p> <p>This defines the search scope for users and groups.</p> <p>Users in this container (and below) are allowed to log in to the User Application.</p> <hr/> <p>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.</p> <hr/>
	<i>User Object Class</i>	The LDAP user object class (typically inetOrgPerson).
	<i>Login Attribute</i>	The LDAP attribute (for example, CN) that represents the user's login name.
	<i>Naming Attribute</i>	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.
	<i>User Membership Attribute</i>	Optional. The LDAP attribute that represents the user's group membership. Do not use spaces in this name.
	<i>Roles Administrator</i>	<p>This role is available in the Novell Identity Manager Roles Based Provisioning Module. This role allows members to create, remove, or modify all roles, and grant or revoke any role assignment to any user, group, or container. It also allows its role members to run any report for any user. By default, the User Application Admin is assigned this role.</p> <p>To change this assignment after you deploy the User Application, use the <i>Roles > Role Assignment</i> page in the User Application.</p>

Type of Setting	Field	Description
Meta-Directory User Groups	<i>Group Container DN</i>	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.
	<i>Group Object Class</i>	The LDAP group object class (typically <code>groupofNames</code>).
	<i>Group Membership Attribute</i>	The attribute representing the user's group membership. Do not use spaces in this name.
	<i>Use Dynamic Groups</i>	Select this option if you want to use dynamic groups.
	<i>Dynamic Group Object Class</i>	The LDAP dynamic group object class (typically <code>dynamicGroup</code>).
eDirectory Certificates	<i>Keystore Path</i>	Required. Specify the full path to your keystore (<code>cacerts</code>) 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 <code>cacerts</code> file. The User Application installation modifies the keystore file. On Linux or Solaris, the user must have permission to write to this file.
	<i>Keystore Password</i>	Required. Specify the <code>cacerts</code> password. The default is <code>changeit</code> .
	<i>Confirm Keystore Password</i>	
Private Key Store	<i>Private Keystore Path</i>	The private keystore contains the User Application's private key and certificates. Reserved. If you leave this empty, this path is <code>/jre/lib/security/cacerts</code> by default.
	<i>Private Keystore Password</i>	This password is <code>changeit</code> unless you specify otherwise. This password is encrypted, based on the master key.
	<i>Private Key Alias</i>	This alias is <code>novellIDMUserApp</code> unless you specify otherwise.
	<i>Private Key Password</i>	This password is <code>novellIDM</code> unless you specify otherwise. This password is encrypted, based on the master key.

Type of Setting	Field	Description
Trusted Key Store	<i>Trusted Store Path</i>	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 <code>javax.net.ssl.trustStore</code> . If the path isn't there, it is assumed to be <code>jre/lib/security/cacerts</code> .
	<i>Trusted Store Password</i>	If this field is empty, the User Application gets the password from System property <code>javax.net.ssl.trustStorePassword</code> . If the value is not there, <code>changeit</code> 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.
	<i>Novell Audit Digital Signature Certificate</i>	Displays the digital signature certificate.
	<i>Novell Audit Digital Signature Private Key</i>	Displays the digital signature private key. This key is encrypted, based on the master key.
Access Manager and iChain Settings	<i>Simultaneous Logout Enabled</i>	If this option is selected, the User Application supports simultaneous logout of the User Application and either Novell Access Manager or iChain. The User Application checks for a Novell Access Manager or iChain cookie on logout and, if the cookie is present, reroutes the user to the ICS logout page.
	<i>Simultaneous Logout Page</i>	The URL to the Novell Access Manager or iChain logout page, where the URL is a hostname that Novell Access Manager or iChain expects. If ICS logging is enabled and a user logs out of the User Application, the user is rerouted to this page.

Type of Setting	Field	Description
Email	<i>Notify Template HOST token</i>	Specify the application server hosting the Identity Manager User Application. For example: <code>myapplication serverServer</code> 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.
	<i>Notify Template PORT token</i>	Used to replace the \$PORT\$ token in e-mail templates used in provisioning request tasks and approval notifications.
	<i>Notify Template SECURE PORT token</i>	Used to replace the \$SECURE_PORT\$ token in e-mail templates used in provisioning request tasks and approval notifications.
	<i>Notify Template PROTOCOL token</i>	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.
	<i>Notify Template SECURE PROTOCOL token</i>	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.
	<i>Notification SMTP Email From:</i>	Specify e-mail from a user in provisioning e-mail.
	<i>Notification SMTP Email Host:</i>	Specify the SMTP e-mail host that provisioning e-mail is using. This can be an IP address or a DNS name.

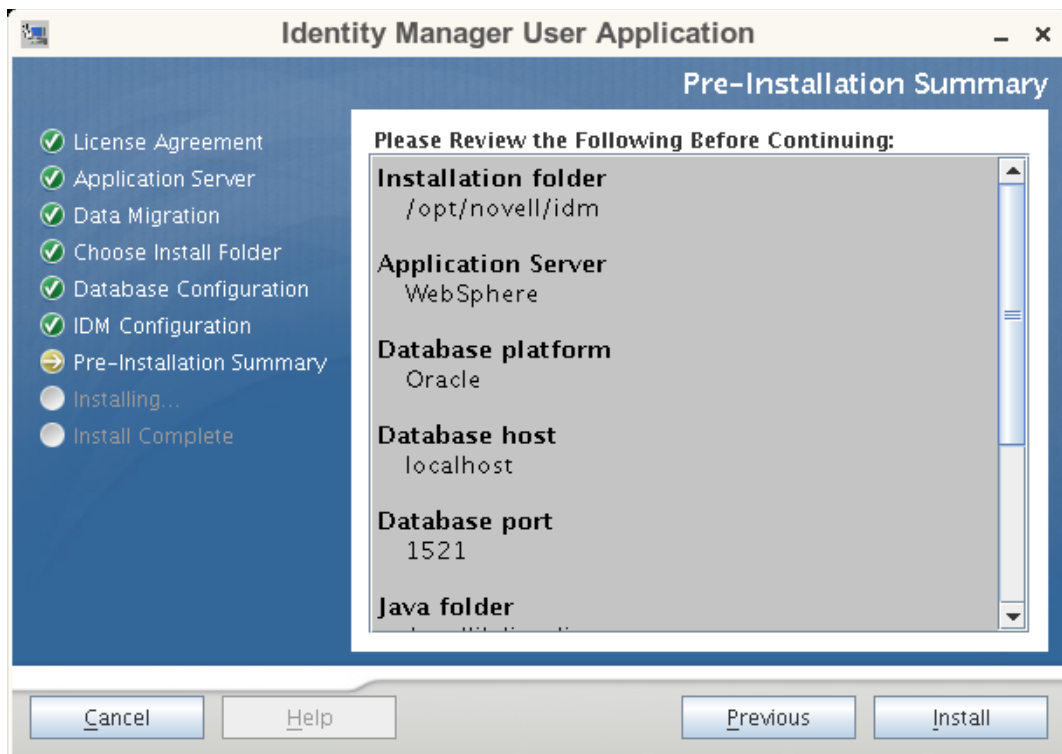
Type of Setting	Field	Description
Password Management	<i>Use External Password WAR</i>	<p>This feature enables you to specify a Forgot Password page residing in an external Forgot Password WAR and a URL that the external Forgot Password WAR uses to call back the User Application through a Web service.</p> <p>If you select <i>Use External Password WAR</i>, you must supply values for <i>Forgot Password Link</i> and <i>Forgot Password Return Link</i>.</p> <p>If you do not select <i>Use External Password WAR</i>, IDM uses the default internal Password Management functionality, <code>./jssps/pwdmgt/ForgotPassword.jsf</code> (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.</p>
	<i>Forgot Password Link</i>	This URL points to the Forgot Password functionality page. Specify a <code>ForgotPassword.jsf</code> file in an external or internal password management WAR.
	<i>Forgot Password Return Link</i>	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 <code>https://idmhost:sslport/idm</code> .
	Miscellaneous	<p><i>Session Timeout</i></p> <p>The application session timeout.</p> <p><i>OCSP URI</i></p> <p>If the client installation uses the On-Line Certificate Status Protocol (OCSP), supply a Uniform Resource Identifier (URI). For example, the format is <code>http://host:port/ocspLocal</code>. The OCSP URI updates the status of trusted certificates online.</p> <p><i>Authorization Config Path</i></p> <p>Fully qualified name of the authorization configuration file.</p> <p><i>Create eDirectory Index</i></p> <p><i>Server DN</i></p>

Type of Setting	Field	Description
Container Object	<i>Selected</i>	Select each Container Object Type to use.
	<i>Container Object Type</i>	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 <i>Add a new Container Object</i> .
	<i>Container Attribute Name</i>	Lists the Attribute Type name associated with the Container Object Type.
	<i>Add a New Container Object: Container Object Type</i>	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) .
	<i>Add a New Container Object: Container Attribute Name</i>	Supply the attribute name of the container object.

- 4 After you finish configuring the settings, click *OK*, then continue with [Section 6.10, “Verify Choices and Install,”](#) on page 103.

6.10 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*.



6.11 View Log Files

If your installation completed without error, continue with [Section 6.12, “Adding User Application Configuration Files and JVM System Properties,”](#) on page 104.

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.

6.12 Adding User Application Configuration Files and JVM System Properties

The following steps are required for a successful WebSphere installation:

- 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 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*, specify `extend.local.config.dir`.
 - 9b For the *Value*, specify 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*, specify 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*, specify `idmuserapp.logging.config.dir`
 - 10b For the *Value*, specify the name of the install folder (directory) that you specified during installation.
 - 10c For the *Description*, specify 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*.

6.13 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 by using the WebSphere administrator's console ("[Importing Certificates with the WebSphere Administrator's Console](#)" on page 105) or through the command line ("[Importing Certificates with the Command Line](#)" on page 106).
- 3 After you import certificates, proceed to [Section 6.14, "Deploying the IDM WAR File,"](#) on page 106.

6.13.1 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 trust store you are using).
- 5 Under *Additional Properties* on the right, select *Signer Certificates*.
- 6 Click *Add*.
- 7 Type the Alias name and full path to the certificate file.
- 8 Change the Data type in the drop-down list to *Binary DER data*.
- 9 Click *OK*. You should now see the certificate in the list of signer certificates.

6.13.2 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`.

The following is a 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.

6.14 Deploying the IDM WAR File

- 1 Log in to the WebSphere administration console as an admin user.
- 2 In 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 User Application installation directory that you specified during installation of the User Application.
- 4 Type the Context root for the application, for example `IDMPROV`. This is 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 all the defaults for this page, then click *Next* to move to the Map modules to servers page.
- 7 Accept all the defaults for this page, then click *Next* to move to the Map resource references to resources page.
- 8 For the authentication method, select the *Use default method* check box. Then, in 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 *Map virtual hosts for Web modules*.
- 11 Accept all the defaults for this page, then 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 6.15, “Starting the Application,” on page 107](#).

6.15 Starting 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.

6.16 Accessing 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
```


Post-Installation Tasks

This section describes post-installation tasks. Topics include:

- ◆ [Section 7.1, “Recording the Master Key,” on page 109](#)
- ◆ [Section 7.2, “Post-Installation Configuration,” on page 109](#)
- ◆ [Section 7.3, “Checking Your Cluster Installations,” on page 109](#)
- ◆ [Section 7.4, “Configuring SSL Communication between JBoss Servers,” on page 110](#)
- ◆ [Section 7.5, “Accessing the External Password WAR,” on page 110](#)
- ◆ [Section 7.6, “Updating Forgot Password Settings,” on page 110](#)
- ◆ [Section 7.7, “Setting Up E-Mail Notification,” on page 111](#)
- ◆ [Section 7.8, “Testing the Installation on the JBoss Application Server,” on page 111](#)
- ◆ [Section 7.9, “Setting Up Your Provisioning Team and Requests,” on page 112](#)
- ◆ [Section 7.10, “Creating Indexes in eDirectory,” on page 112](#)
- ◆ [Section 7.11, “Reconfiguring the IDM WAR File after Installation,” on page 112](#)
- ◆ [Section 7.12, “Troubleshooting,” on page 112](#)

7.1 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.

7.2 Post-Installation Configuration

For post-installation directions on configuring the Identity Manager User Application and Roles Subsystem, refer to the following:

- ◆ In the *Novell IDM Roles Based Provisioning Module 3.6 Administration Guide*, the section entitled “Configuring the User Application Environment.”
- ◆ The *Novell IDM Roles Based Provisioning Module 3.6 Design Guide*

7.3 Checking Your Cluster Installations

In JBoss clusters, ensure that each application server in the cluster has the following:

- ◆ 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.

In WebSphere clusters, ensure that each application server in the 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/idmrbpm36/index.html>)

7.4 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.

7.5 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 in the following locations:

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

7.6 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.

Using 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.

Using 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/jsp/pwdmgt/ForgotPassword.jsf`)
- ♦ *Forgot Password Return Link* (for example: `https://idmhost:sslport/idm`)

7.7 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*.

7.8 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.

If you are not running on an X11 Window System, you need to include the `-Djava.awt.headless=true` flag in your server startup script. This is necessary for running reports. For example, you might include this line in your script:

```
JAVA_OPTS="-Djava.awt.headless=true -server -Xms256M -Xmx256M  
-XX:MaxPermSize=256m"
```

- 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 the following URL:

```
http://hostname:port/ApplicationName
```

In this URL, *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 7.12, “Troubleshooting,” on page 112](#).

7.9 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 User Application: Administration Guide* (<http://www.novell.com/documentation/idmrpbpm36/index.html>).

7.10 Creating Indexes in eDirectory

For improved performance of the IDM User Application, the eDirectory Administrator must create indexes for the manager, ismanager and srvrprvUUID 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.

7.11 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 [Table 4-2 on page 59](#), [Table 5-1 on page 70](#), or [Table 6-2 on page 96](#).
- 2 Deploy the new WAR file to your application server.

7.12 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
<p>You want to modify the User Application configuration settings made during installation. This includes configuration of such things as:</p> <ul style="list-style-type: none"> ◆ Identity Vault connections and certificates ◆ E-mail settings ◆ Metadirectory User Identity, User Groups ◆ Access Manager or iChain® settings 	<p>Run the configuration utility independent of the installer.</p> <p>On Linux and Solaris, run the following command from the installation directory (by default, <code>/opt/novell/idm</code>):</p> <pre>configupdate.sh</pre> <p>On Windows, run the following command from the installation directory (by default, <code>c:\opt\novell\idm</code>):</p> <pre>configupdate.bat</pre>
<p>Exceptions are thrown when application server starts up, with a log message <code>port 8080 already in use</code>.</p>	<p>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 <code>config</code> settings for the User Application driver in iManager.</p>
<p>When the application server starts, you see a message that no trusted certificates were found.</p>	<p>Make sure that you start application server using the JDK specified in the installation of the User Application.</p>
<p>You can't log into the portal admin page.</p>	<p>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).</p>
<p>You can log in as admin, but you can't create new users.</p>	<p>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).</p>
<p>When starting the application server, there are MySQL connection errors.</p>	<p>Don't run as <code>root</code>. (This issue is unlikely, however, if you are running the version of MySQL supplied with Identity Manager.)</p> <p>Make sure MySQL is running (and that the correct copy is running). Kill any other instances of MySQL. Run <code>/idm/mysql/start-mysql.sh</code>, then <code>/idm/start-jboss.sh</code>.</p> <p>Examine <code>/idm/mysql/setup-mysql.sh</code> in a text editor and correct any values that appear suspicious. Then run the script, and run <code>/idm/start-jboss.sh</code>.</p>

Issue	Suggested Actions
You encounter keystore errors when starting the application server.	<p>Your application server is not using the JDK specified at the installation of the User Application.</p> <p>Use the <code>keytool</code> command to import the certificate file:</p> <pre>keytool -import -trustcacerts - alias <i>aliasName</i> -file <i>certFile</i> - keystore ..\lib\security\cacerts - storepass changeit</pre> <ul style="list-style-type: none"> ◆ Replace <i>aliasName</i> with a unique name of your choice for this certificate. ◆ Replace <i>certFile</i> with the full path and name of your certificate file. ◆ The default keystore password is <code>changeit</code> (if you have a different password, specify it).
E-mail notification was not sent.	<p>Run the <code>configupdate</code> utility to check whether you supplied values for the following User Application configuration parameters: E-Mail From and E-Mail Host.</p> <p>On Linux or Solaris, run this command from the installation directory (by default, <code>/opt/novell/idm</code>):</p> <pre>configupdate.sh</pre> <p>On Windows, run this command from the installation directory (by default, <code>c:\opt\novell\idm</code>):</p> <pre>configupdate.bat</pre>