www.novell.com/documentation

User Application: Installation Guide

Identity Manager Roles Based Provisioning Module 4.0.2

January 2014

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/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
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.netiq.com/documentation).

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide

This guide describes how to install the Novell Identity Manager Roles Based Provisioning Module 4.0.2. Sections include:

Audience

This guide is intended for administrators and consultants who 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 4.0.2, see the Identity Manager Documentation Web site (http://www.netiq.com/documentation/idm402/index.html).

1 Roles Based Provisioning Module Installation Overview

This section provides an overview of the steps for installing the Roles Based Provisioning Module. Topics include:

- Section 1.1, "Installation Checklist," on page 9
- Section 1.2, "About the Installer Program," on page 10
- Section 1.3, "System Requirements," on page 10
- Section 1.4, "Design Constraints," on page 13
- Section 1.5, "Installing the Roles Based Provisioning Module in a Clustered Environment," on page 14

If you are migrating from an earlier version of the User Application or Roles Based Provisioning Module, refer to the *RBPM and Reporting Migration Guide* (http://www.netiq.com/documentation/idm402/index.html)

1.1 Installation Checklist

To install the Novell Identity Manager Roles Based Provisioning Module, you must perform the following tasks:

- ❐ Verify that your software meets the system requirements. See Section 1.3, "System Requirements," on page 10.
- ❐ Download Identity Manager 4.0.2 Advanced Edition. See Section 2.2, "Downloading Identity Manager 4.0.2 Advanced Edition," on page 15.
- ❐ Set up the following supporting components:
  - ❐ Make sure you have a supported Identity Manager metadirectory installed. See Section 2.1, "Installing the Identity Manager Metadirectory," on page 15.
  - ❐ Install and configure an application server. See Section 2.3, "Installing an Application Server," on page 17.
  - ❐ Install and configure a database. See Section 2.4, "Installing a Database," on page 21.
- ❐ Install the Roles Based Provisioning Module Metadirectory components. See Chapter 3, "Installing the Roles Based Provisioning Module," on page 29.
- ❐ Create the User Application driver. See Chapter 4, "Creating the Drivers," on page 47.
- ❐ Create the Role and Resource Service driver. See Chapter 4, "Creating the Drivers," on page 47
- ❐ Install and configure the Novell Identity Manager User Application. (You must have the correct JDK installed before you start the installation program. See Section 2.5, "Installing the Java Development Kit," on page 27.)

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

- Graphical user interface. See one of the following:
  - Chapter 5, "Installing the User Application on JBoss," on page 53.
  - Chapter 6, "Installing the User Application on WebSphere," on page 67.
  - Chapter 7, "Installing the User Application on WebLogic," on page 89.
- Console (command line) interface. See Section 8.1, "Installing the User Application from the Console," on page 101.
- Silent install. See Section 8.2, "Installing the User Application with a Single Command," on page 102.

❒ Carry out the post-installation tasks described in Chapter 9, "Post-Installation Tasks," on page 115.

IMPORTANT: This book does not provide instructions on setting up the security environment. For details on security, see *User Application: Administration Guide* (http://www.netiq.com/documentation/idm402/index.html).

1.2 About the Installer Program

The User Application installation program does the following:

- Determines whether your licensing is for Identity Manager 4.0.2 Advanced Edition or Standard Edition. It then displays appropriate screens for the licensed edition.
- Designates an existing version of an application server to use.
- Designates an existing version of a database to use, for example PostgreSQL, Oracle, DB2, Microsoft SQL Server, or MySQL. 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 and WebLogic, you must manually deploy the WAR.
- Enables logging through Novell or OpenXDAS auditing clients 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.

1.3 System Requirements

To use the Novell Identity Manager Roles Based Provisioning Module 4.0.2, you must have one of each of the required components listed in Table 1-1. Certified platforms have been fully tested. Supported platforms are expected to be functional, but have not been fully tested.

Table 1-1 *System Requirements*

Required System Component	System Requirements
Metadirectory	eDirectory 8.8.7 with Identity Manager 4.0.2 For the list of certified operating systems, see the Identity Manager and eDirectory documentation.
Application Server	The User Application runs on JBoss, WebSphere, and WebLogic. The User Application with JBoss Enterprise Application Platform 5.1.2 (or JBoss Community Edition 5.1.0) requires JRE 1.6.0_31 from Sun (Oracle) and is certified on: ◆ Windows Server 2003 SP2 (32-bit only) ◆ Windows Server 2008 R2 SP1 (64-bit only) ◆ Windows Server 2008 SP2 (32-bit and 64-bit) ◆ Open Enterprise Server 2 SP3 (32-bit and 64-bit) ◆ Open Enterprise Server 11 (64-bit only) ◆ SUSE Linux Enterprise Server 10 SP4 (32-bit and 64-bit) ◆ SUSE Linux Enterprise Server 11 SP1 and SP2 (32-bit and 64-bit) ◆ Red Hat Linux 5.7 (32-bit and 64-bit) ◆ Red Hat Enterprise Linux 6.2 (32-bit and 64-bit) The User Application on WebSphere 7.0 requires the IBM J9 VM (build 2.4, J2RE 1.6.0) and Fix Pack 7 or higher. The User Application with WebSphere 7.0 is certified on these platforms: ◆ Windows Server 2003 SP2 (32-bit only) ◆ Windows Server 2008 R2 SP1 (64-bit only) ◆ Windows Server 2008 SP2 (32-bit and 64-bit) ◆ SUSE Linux Enterprise Server 10 SP4 (32-bit and 64-bit) ◆ SUSE Linux Enterprise Server 11 SP1 and SP2 (32-bit and 64-bit) ◆ Red Hat Linux 5.7 (32-bit and 64-bit) ◆ Red Hat Enterprise Linux 6.2 (32-bit and 64-bit) The User Application on WebLogic 10.3.5 (11gR1) requires JRockit JVM 1.6.0_17 and is certified on these platforms. ◆ Windows Server 2003 SP2 (32-bit only) ◆ Windows Server 2008 R2 SP1 (64-bit only) ◆ Windows Server 2008 SP2 (32-bit and 64-bit) ◆ SUSE Linux Enterprise Server 10 SP4 (32-bit and 64-bit) ◆ SUSE Linux Enterprise Server 11 SP1 and SP2 (32-bit and 64-bit) ◆ Red Hat Linux 5.7 (32-bit and 64-bit) ◆ Red Hat Enterprise Linux 6.2 (32-bit and 64-bit)

Required System Component	System Requirements
Virtualization	The User Application supports virtualization on the following platforms as long as the guest operating system is one that is certified by the User Application: ◆ Red Hat Enterprise Linux Virtualization ◆ Xen ◆ VMWare ESX/ESXi ◆ Windows Server 2008 R2 Virtualization with Hyper-V
Browser	The User Application is certified with both Firefox and Internet Explorer, as described below. FireFox 9 is certified on: ◆ Windows XP with SP3 ◆ Windows 7 ◆ SUSE Linux Enterprise Desktop 11 ◆ SUSE Linux Enterprise Server 11 ◆ Novell OpenSUSE 11.2 ◆ Apple Mac Internet Explorer 8 is certified on: ◆ Windows XP with SP3 Internet Explorer 9 is certified on: ◆ Windows 7 **NOTE:** For Internet Explorer browsers, the XML DOM (ActiveX control) from Microsoft Corporation is required for the Identity Manager Roles Based Provisioning Module 4.01 to work correctly. The version number of the XML DOM depends on the version of Internet Explorer being used.

Required System Component	System Requirements
Database Server	The following databases are certified with JBoss 5.1.2 Enterprise Application Platform (or JBoss Community Edition 5.1.0): ◆ MS SQL 2008 and MS SQL 2008 R2 ◆ MySQL Version 5.1 ◆ Oracle 11gR2 ◆ PostgreSQL 8.4.3 and 9.0 The following databases are certified with WebSphere 7.0: ◆ DB2 9.5b ◆ MS SQL 2008 ◆ Oracle 11gR2 ◆ PostgreSQL 8.4.3 and 9.0 The following databases are certified with WebLogic 10.3.5: ◆ MS SQL 2008 and MS SQL 2008 R2 ◆ Oracle 11gR2 ◆ PostgreSQL 8.4.3 and 9.0
Designer	Designer 4.0.2
OpenXDAS	OpenXDAS version 0.8.345 The following OpenXDAS versions are needed for SLES10: ◆ openxdas-0.8.351-1.1.i586.rpm ◆ openxdas-0.8.351-1.1.x86_64.rpm
Domain Services	OES 2 SP1 Domain Services for Windows
Password Management Challenge Response	NMAS Challenge Response Login Method Version: 2770 Build: 20080603 or higher is needed for Password Management Challenge Response functionality.

1.4 Design Constraints

Before you set up a production environment, you need to be aware of some important design constraints that determine which configurations are possible and which should not be used. For more information, see the discussion on “Design Constraints” in the *User Application: Administration Guide*.

1.5 Installing the Roles Based Provisioning Module in a Clustered Environment

Database clustering is a feature of each respective database server. We do not officially test with any clustered database configuration, because clustering is independent of the product functionality.

Therefore, we support clustered database servers with the following caveats:

- We have not officially tested the Roles Based Provisioning Module with any clustered database servers.
- There may be some features or aspects of your clustered database server that will need to be disabled. For example, Transactional Replication must be disabled on certain tables due to constraint violations when trying to insert a duplicate key.
- We do not provide assistance on the installation, configuration, or optimization of the clustered database server, including installation of our products into a clustered database server.
- We exert our best effort to resolve any issues that may arise with the use of our products in a clustered database environment. Troubleshooting methods in a complex environment often require cooperative work to resolve issues. NetIQ provides expertise to analyze, plan and troubleshoot the NetIQ products. The customer must provide expertise to analyze, plan and troubleshoot any third-party products. We ask customers to reproduce issues or analyze behavior of their components in a non-clustered environment to help isolate potential cluster setup issues from NetIQ product issues.

2 Prerequisites

This section describes the software components you must install or configure before you can install the Identity Manager Roles Based Provisioning Module (RBPM). Topics include:

- Section 2.1, “Installing the Identity Manager Metadirectory,” on page 15
- Section 2.2, “Downloading Identity Manager 4.0.2 Advanced Edition,” on page 15
- Section 2.3, “Installing an Application Server,” on page 17
- Section 2.4, “Installing a Database,” on page 21
- Section 2.5, “Installing the Java Development Kit,” on page 27

2.1 Installing the Identity Manager Metadirectory

The Roles Based Provisioning Module 4.0.2 must be used with Identity Manager 4.0.2.

For instructions on installing Identity Manager 4.0.2, see the Identity Manager Documentation Web site (http://www.netiq.com/documentation/idm402/index.html).

2.2 Downloading Identity Manager 4.0.2 Advanced Edition

To obtain the Identity Manager Roles Based Provisioning Module, download the `.iso` image file for Identity Manager 4.0.2 Advanced Edition from Novell Downloads (http://download.novell.com/index.jsp). Choose the correct `.iso` image file for your operating system environment (for example, `Identity_Manager_4.0.2_Linux_Advanced.iso`).

Table 2-1 describes the installation files delivered for the User Application and Roles Based Provisioning Module. You can find these files in the products/RBPM directory within the `.iso` file.

Table 2-1 *Files and Scripts Delivered*

File	Description
`IDMProv.war`	The Roles Based Provisioning Module WAR. It includes the Identity Manager User Application with Identity Self-Service and Roles Based Provisioning Module features.
`IDMUserApp.jar`	The User Application installation program.
`silent.properties`	A files that contains the parameters required for a silent install. These parameters correspond to the installation parameters you set in the GUI or Console installation procedures. You should copy this file, then modify the contents to suit your installation environment.

File	Description
`JBossPostgreSQL.bin` or `JBossPostgreSQL.exe`	A convenience utility to install the JBoss application server and PostgreSQL database. Novell provides the JBossPostgreSQL utility as a convenience. If your company does not already provide an application server and a database server, you can use the JBossPostgreSQL utility to install an Open Source version of these components. By running this utility, you can install these components without having to download them separately. If you need support, go to the third party provider of the component. Novell does not provide updates for these components, or administration, configuration, or tuning information for these components, beyond what it is outlined in the Roles Based Provisioning Module documentation. This utility provides the Community Edition of the JBoss Application Server, which JBoss only supports via their User Forums. We recommend that an enterprise application server be used for staging and production environments, and this utility be used for creating development environments. The enterprise application servers that we support are: ◆ IBM WebSphere ◆ JBoss Enterprise Application Platform ◆ Oracle WebLogic
`nmassaml.zip`	Contains an eDirectory method to support SAML. Only needed if you are not using Access Manager.
`rbpm_driver_install.exe`	Windows install program for the Metadirectory components of the Roles Based Provisioning Module (Role and Resource Service Driver, User Application Driver, and eDirectory schema).
`rbpm_driver_install_linux.bin`	Linux install program for the Metadirectory components of the Roles Based Provisioning Module (Role and Resource Service Driver, User Application Driver, and eDirectory schema).
`rbpm_driver_install_solaris.bin`	Solaris install program for the Metadirectory components of the Roles Based Provisioning Module (Role and Resource Service Driver, User Application Driver, and eDirectory schema).

The system where you install the Identity Manager Roles Based Provisioning Module must have at least 320 MB of available storage plus space for the supporting applications (database, application server, and so on). The system will require additional space, over time, to accommodate growth of other data, such as database or application server logs.

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).

2.3 Installing an Application Server

- Section 2.3.1, “Installing the JBoss Application Server,” on page 17
- Section 2.3.2, “Installing the WebLogic Application Server,” on page 21
- Section 2.3.3, “Installing the WebSphere Application Server,” on page 21

2.3.1 Installing the JBoss Application Server

If you plan to use the JBoss Application Server, you can either:

- Download and install the JBoss Application Server according to manufacturer’s instructions. See Section 1.3, “System Requirements,” on page 10 for the supported version.
- Use the JBossPostgreSQL utility provided with the Roles Based Provisioning Module download to install a JBoss Application Server (and optionally PostgreSQL). For directions, see “Installing the JBoss Application Server and the PostgreSQL Database” on page 17.

Do not start the JBoss server until after you install the Identity Manager Roles Based Provisioning Module. Starting the JBoss server is a post-installation task.

Table 2-2 *JBoss Application Server Minimum Recommended Requirements*

Component	Recommendation
RAM	512 MB is the minimum recommended RAM for the JBoss Application Server when running the Identity Manager Roles Based Provisioning Module.
Port	8180 is the default for the application server. Record the port that your application server uses.
SSL	Enable SSL if you plan to use external password management: ◆ Enable SSL for the JBoss servers on which you deploy the Identity Manager Roles Based Provisioning Module and `IDMPwdMgt.war` file. ◆ Ensure that the SSL port is open on your firewall. For information on enabling SSL, see your JBoss documentation. For information on the `IDMPwdMgt.war file`, see Section 9.5, “Configuring External Forgot Password Management,” on page 118 and also see the *User Application: Administration Guide* (http://www.netiq.com/documentation/idm402/index.html).

Installing the JBoss Application Server and the PostgreSQL Database

The JBossPostgreSQL utility installs the JBoss Application Server and PostgreSQL on your system.

Novell provides the JBossPostgreSQL utility as a convenience. If your company does not already provide an application server and a database server, you can use the JBossPostgreSQL utility to install an Open Source version of these components. By running this utility, you can install these components without having to download them separately. If you need support, go to the third party provider of the component. Novell does not provide updates for these components, or administration, configuration, or tuning information for these components, beyond what it is outlined in the Roles Based Provisioning Module documentation.

This utility provides the Community Edition of the JBoss Application Server, which JBoss only supports via their User Forums. We recommend that an enterprise application server be used for staging and production environments, and this utility be used for creating development environments. The enterprise application servers that we support are:

- IBM WebSphere
- JBoss Enterprise Application Platform
- Oracle WebLogic

NOTE: Before running the RBPM JBossPostgreSQL installer on Windows 2008, you need to check with your Windows Administrator to see what the password policy is for your system. The Windows 2008 server password policy requires a password to conform to a certain set of rules. For example, the policy might require that a password contain a non-alphabetic characters, as well as upper or lowercase characters, or be at least 8 characters in length. The policy can be modified or disabled by the Windows Administrator.

Run the installer as root You need to run the installer as the root user.

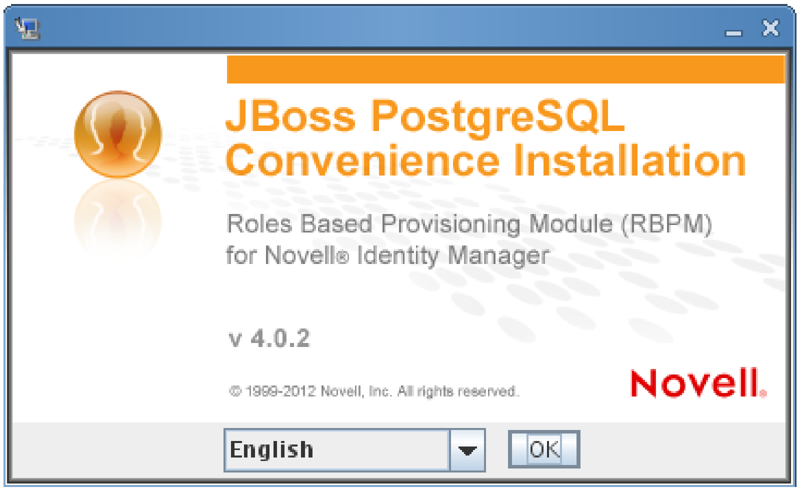
To run the JBossPostgreSQL utility:

1 Locate and execute `JBossPostgreSQL.bin` or `JBossPostgreSQL.exe`.

`/products/RBPM/JBossPostgreSQL.bin` (for Linux)
`/products/RBPM/JBossPostgreSQL.exe` (for Windows)

The utility is not available for Solaris.

The JBossPostgreSQLJBossPostgreSQL utility displays its splash screen:



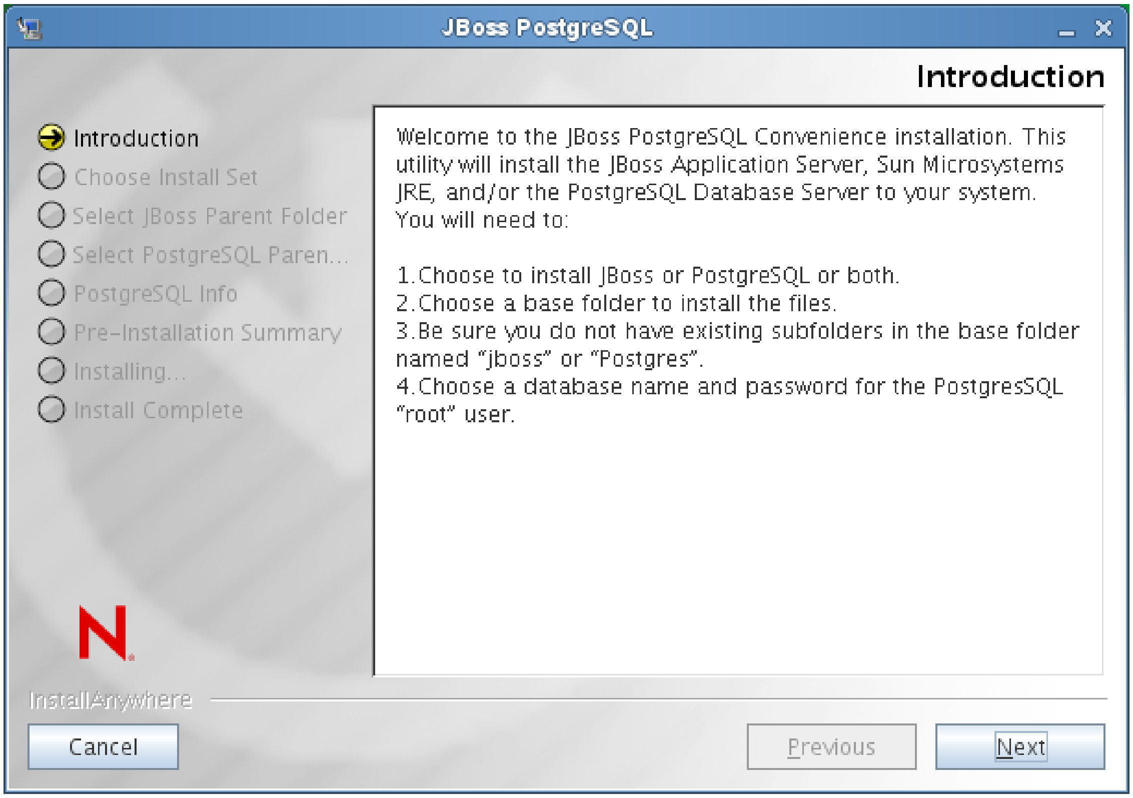
JBoss PostgreSQL
Convenience Installation

Roles Based Provisioning Module (RBPM)
for Novell® Identity Manager

v 4.0.2

© 1999-2012 Novell, Inc. All rights reserved.

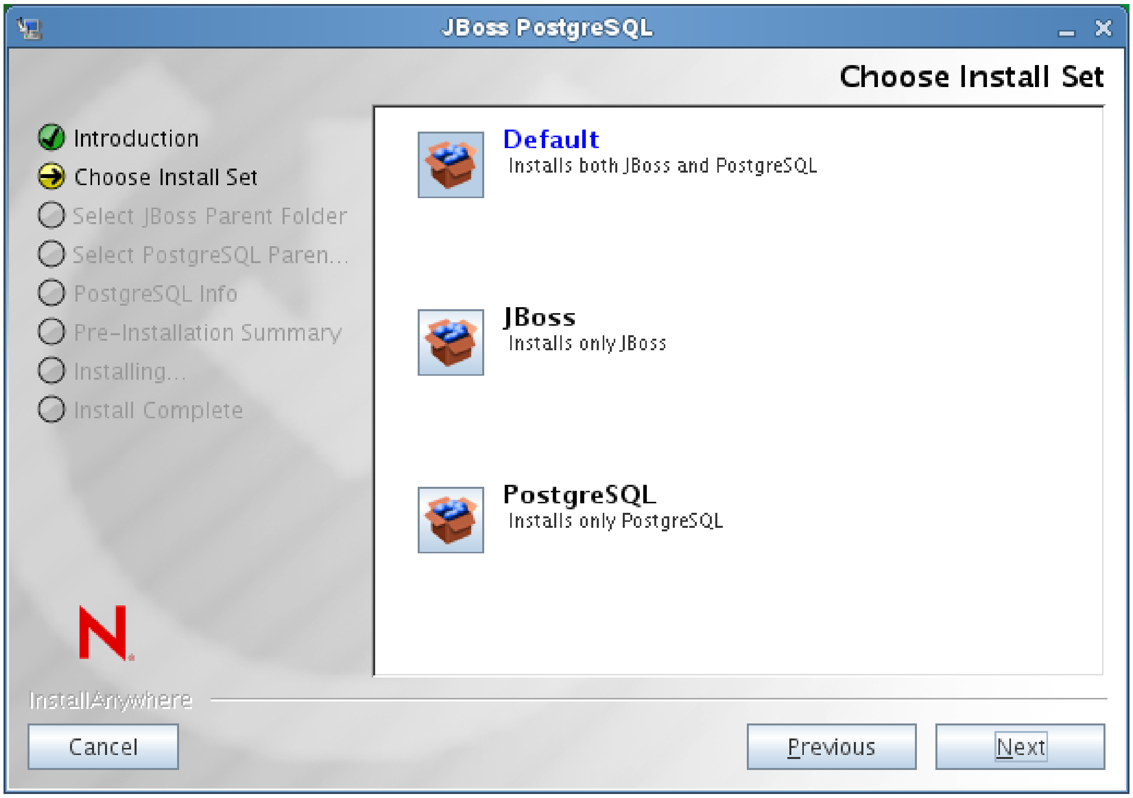
Then the utility displays the Introduction screen:



Welcome to the JBoss PostgreSQL Convenience installation. This utility will install the JBoss Application Server, Sun Microsystems JRE, and/or the PostgreSQL Database Server to your system. You will need to:

1. Choose to install JBoss or PostgreSQL or both.
2. Choose a base folder to install the files.
3. Be sure you do not have existing subfolders in the base folder named “jboss” or “Postgres”.
4. Choose a database name and password for the PostgresSQL “root” user.

When you click Next, the utility displays the *Choose Install Set* screen:



Default
Installs both JBoss and PostgreSQL

JBoss
Installs only JBoss

PostgreSQL
Installs only PostgreSQL

2 Follow the on-screen instructions for navigating the utility. Refer to the following table for additional information.

Installation Screen	Description
Choose Install Set	Choose which products to install. ◆ *Default:* installs both JBoss and PostgreSQL in the directory you specify along with scripts to start and stop it. ◆ *JBoss*: Installs the JBoss Application server in the directory you specify along with scripts to start and stop it. **NOTE:** This utility does not install the JBoss Application Server as a Windows service. For directions, see "Installing the JBoss Application Server as a Service or a Daemon" on page 21. ◆ *PostgreSQL*: Installs PostgreSQL and creates a PostgreSQL database in the directory you specify along with scripts to start and stop it.
Choose JBoss parent folder	Click *Choose* to select an installation folder other than the default.
Choose PostgreSQL parent folder	Click *Choose* to select an installation folder other than the default.
PostgreSQL Info	Specify the following: ◆ *Database Name*: Specify the name of the database for the installer to create. You are prompted for this name by the User Application installation utility, so you should make a note of the name and location. The default database is `idmuserappdb`. ◆ *Database Admin*: The user will be the administrator for the database. The default administrator is `idmadmin`. ◆ *Password for Admin User*: The password for the database administrator. ◆ *Confirm Password Admin User*: Confirmation of the password. ◆ *PostgreSQL Port*: The port on which the PostgreSQL database server will listen.
PreInstallation Summary	Review the Summary page. If the specifications are correct, click *Install.*
Install Complete	The utility displays a successful-completion message after it installs the products you selected: `The Installer has completed successfully.  Thank you for choosing Novell` **Installer creates the novlua user** The installer creates a new user with the name novlua. The jboss_init script runs JBoss as this user and the permissions defined in the JBoss files are set to this user. **IMPORTANT:** You need to be aware that the JBossPostgreSQL utility does not secure the JMX Console or the JBoss Web Console. This leaves the JBoss environment wide open. You need to lock down the environment as soon as you complete your installation to eliminate security risks. For details on how to secure the JMX Console and JBoss Web Console, see (http://community.jboss.org/wiki/SecureTheJmxConsole).

Installing the JBoss Application Server as a Service or a Daemon

On Linux, JBoss starts as a service by default. A script called /etc/init.d/jboss_init start/stop is installed to start JBoss at system reboot.

Using a JavaServiceWrapper You can use a JavaServiceWrapper to install, start, and stop the JBoss Application Server as a Windows service or Linux or UNIX daemon process. See directions from JBoss at http://www.jboss.org/community/wiki/RunJBossAsAServiceOnWindows (http://www.jboss.org/community/wiki/RunJBossAsAServiceOnWindows). 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)).

IMPORTANT: 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, but JBoss no longer recommends using JavaService. For details, see http://www.jboss.org/wiki/JavaService (http://www.jboss.org/community/wiki/JavaService).

2.3.2 Installing the WebLogic Application Server

If you plan to use the WebLogic Application Server, download and install it. See Section 1.3, "System Requirements," on page 10 for information about the supported versions.

2.3.3 Installing the WebSphere Application Server

If you plan to use the WebSphere Application Server, download and install it. See Section 1.3, "System Requirements," on page 10 for information about the supported versions.

For notes on DB2 configuration, see "Notes on Configuring a DB2 Database" on page 25.

2.4 Installing a Database

The User Application uses a database for various tasks such as storing configuration data and storing data for any workflow activities. Before you can install the Roles Based Provisioning Module and User Application, you must have one of the supported databases for your platform installed and configured. You need to perform these steps:

❐ Install your database and database driver.

  When you install the User Application, you need to specify a driver JAR file that has been provided by the database vendor for the particular database you are using. Driver JAR files provided by third-party vendors are not supported.

❐ Create a database or a database instance.

❐ Record the following database parameters for use in the installation procedure for the User Application:

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

❐ Create a datasource file that points to the database.

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

- ❒ Enable the database for Unicode encoding.

  The User Application requires that the database character set use Unicode encoding. For example, UTF-8 is an example of a character set that uses Unicode encoding, but Latin1 does not use Unicode encoding. Before installing the User Application, verify that your database is configured with a character set that has Unicode encoding.

- ❒ Be sure not to use case-insensitive collation.

  Case-insensitive collation is not supported. If you use case-insensitive collation, you might encounter duplicate key errors during migration. If a duplicate key error is encountered, check the collation and correct it, then re-install the User Application.

NOTE: If you are migrating to a new version of the Roles Based Provisioning Module, you must use the same User Application database that you used for the previous installation (that is, the installation from which you are migrating.)

2.4.1 Notes on Configuring a MySQL Database

The User Application requires certain configuration options for MySQL, as described below:

- "INNODB Storage Engine and Table Types" on page 22
- "Character Set" on page 22
- "Case Sensitivity" on page 23
- "Ansi Setting" on page 23
- "User Account Requirements" on page 23

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.

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.

As an alternative to setting the `default-table-type=innodb` option, you can append the `ENGINE=InnoDB` option to the Create Table statements in the SQL script for your database.

Character Set

Specify UTF-8 as the character set for the whole server or just for a database.

Specify UTF-8 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 the following example:

```
<connection-url>jdbc:mysql://localhost:3306/
databasename?useUnicode=true&amp;characterEncoding=utf8&amp;connectionCollation=ut
f8_bin</connection-url>
```

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.

Ansi Setting

You need to add the `ansi` entry to your my.cnf (on Linux) or my.ini file (on Windows). If you do not add this entry, the RBPM tables will be created, but the initial data load of the tables will not be performed, and you may see a “Guest Container Page definition not found” error message.

Here’s what the my.cnf (or my.ini) file should look like after you’ve added the `ansi` entry:

```
# These variables are required for IDM User Application
character_set_server=utf8
default-table-type=innodb

# Put the server in ANSI SQL mode.
#See http://www.mysql.com/doc/en/ANSI_mode.html
ansi
```

To confirm the change to use ansi mode has taken effect, you can execute the following SQL on your MySQL server:

```
mysql> select @@global.sql_mode;
+-------------------------------------------------------------+
| @@global.sql_mode                                           |
+-------------------------------------------------------------+
| REAL_AS_FLOAT,PIPES_AS_CONCAT,ANSI_QUOTES,IGNORE_SPACE,ANSI |
+-------------------------------------------------------------+
1 row in set (0.00 sec)
```

User Account Requirements

The user account that is used during the install process must have full access to (be the owner of) the database that will be used by the User Application. In addition, this account will need access to the tables in the system. The tables may vary, depending on your environment.

Create a user to log into the MySQL server and grant privileges to the user, for example:

```
GRANT ALL PRIVILEGES ON <dbname.>* TO <username>@<host> IDENTIFIED BY ‘password’
```

The minimum set of privileges is CREATE, INDEX, INSERT, UPDATE, DELETE, and LOCK TABLES. For documentation on the GRANT command, see http://www.mysql.org/doc/refman/5.0/en/grant.html (http://www.mysql.org/doc/refman/5.0/en/grant.html).

IMPORTANT: The user account must also have select rights to the mysql.user table. Here is the SQL syntax needed to give the proper rights:

```
USE mysql;
GRANT SELECT ON mysql.user TO <username>@<host>;
```

2.4.2 Notes on Configuring an Oracle Database

When you create your Oracle database, you need to be sure to use AL32UTF8 to specify a Unicode-encoded character set. For more information on choosing a character set, see "Choosing an Oracle Database Character Set" (http://docs.oracle.com/cd/B28359_01/server.111/b28298/ch2charset.htm).

When you create a user for your Oracle database, you need to issue the following statements using the SQL Plus utility. These statements create the user and set the user's privileges. Grant the user CONNECT and RESOURCE privileges, for example:

```
CREATE USER idmuser IDENTIFIED BY password
```

```
GRANT CONNECT, RESOURCE to idmuser
```

UTF-8 on Oracle 11g On Oracle 11g, you can issue the following command to confirm that you are enabled for UTF-8:

```
select * from nls_database_parameters;
```

If you are not setup for UTF-8, you will see this data returned:

```
NLS_CHARACTERSET
WE8MSWIN1252
```

If you are setup for UTF-8, you will see this data returned:

```
NLS_CHARACTERSET
AL32UTF8
```

The User Application requires the specific version of the Oracle JDBC Driver that is included with the installation package for the supported version of the Oracle database.

2.4.3 Notes on Configuring an MS SQL Server Database

Set up your MS SQL Server database as follows:

1. Install the MS SQL server.
2. Connect to the server and open an application for creating the database and database user (typically the SQL Server Management Studio application).
3. Create a database. SQL Server does not allow users to select the character set for databases. The User Application stores SQL Server character data in a NCHAR column type, which supports UTF-8.
4. Create a login.
5. Add the login as a user of the database.
6. Grant these privileges to the login: CREATE TABLE, CREATE INDEX, SELECT, INSERT, UPDATE, and DELETE.

The User Application requires version 3.0 of the Microsoft SQL Server 2008 JDBC Driver. The User Application has been tested specifically with version 3.0.119.0 of the Microsoft SQL Server 2008 JDBC Driver.

NOTE: Only the Sun Solaris, Red Hat Linux, and Windows 2000 operating systems are officially certified with the JDBC driver.

2.4.4 Notes on Configuring a DB2 Database

This section provides notes on DB2 configuration.

Providing the Database Driver JARs

The Database Driver JAR files need to be selected during the installation process on the *Database Username and Password* screen. However, the browse button for the *Database Driver JAR File* field only allows you to select one (1) jar. For DB2, you must provide two (2) jars:

- db2jcc.jar
- db2jcc_license_cu.jar

Therefore, if you are running the install program against WebSphere (the only Application Server supported with DB2), you can select one jar, but you will have to manually enter the second one using the correct file separator for the operating system that the install program is running on. Alternatively, you can manually enter both entries.

For example, on Windows:

```
c:\db2jars\db2jcc.jar;c:\db2jars\db2jcc_license_cu.jar
```

For example, on Solaris and Linux:

```
/home/lab/db2jars/db2jcc.jar:/home/lab/db2jcc_license_cu.jar
```

Tuning DB2 Databases to Prevent Deadlocks and Timeouts

When using DB2, if you see an error indicating that the current transaction has been rolled back because of a deadlock or timeout, the problem may be caused by a high level of user and database concurrency.

DB2 provides many techniques for resolving lock conflicts including tuning of the cost-based optimizer. The *Performance Guide* included in the DB2 Administration documentation is an excellent source that contains much information on the topic of tuning.

There are no prescribed tuning values that can be used for all installations since the level of concurrency and size of data varies. However, here are some DB2 tuning tips that may be relevant for your installation:

- The `reorgchk update statistics` command will update the statistics used by the optimizer. Periodic updates of these statistics may be enough to alleviate the problem.
- Use of the DB2 registry parameter DB2_RR_TO_RS can improve concurrency by not locking the next key of the row that was inserted or updated.
- Increase the MAXLOCKS and LOCKLIST parameters on the database.
- Increase the currentLockTimeout property on the database connection pool.
- Use the Database Configuration Advisor and optimize for faster transactions.

- Alter all the User Application tables to be VOLATILE to indicate to the optimizer that cardinality of the table will vary significantly. For example, to make the AFACTIVITY table VOLATILE, you might issue the command: `ALTER TABLE AFACTIVITY VOLATILE`

  The ALTER TABLE commands need to be run after the User Application has been started once and the database tables have been created. Refer to the ALTER TABLE documentation for more information on this statement. Here are the SQL statements for all the User Application tables:

```
ALTER TABLE AFACTIVITY VOLATILE
ALTER TABLE AFACTIVITYTIMERTASKS VOLATILE
ALTER TABLE AFBRANCH VOLATILE
ALTER TABLE AFCOMMENT VOLATILE
ALTER TABLE AFDOCUMENT VOLATILE
ALTER TABLE AFENGINE VOLATILE
ALTER TABLE AFENGINESTATE VOLATILE
ALTER TABLE AFMODEL VOLATILE
ALTER TABLE AFPROCESS VOLATILE
ALTER TABLE AFPROVISIONINGSTATUS VOLATILE
ALTER TABLE AFQUORUM VOLATILE
ALTER TABLE AFRESOURCEREQUESTINFO VOLATILE
ALTER TABLE AFWORKTASK VOLATILE
ALTER TABLE AF_ROLE_REQUEST_STATUS VOLATILE
ALTER TABLE ATTESTATION_ATTESTER VOLATILE
ALTER TABLE ATTESTATION_ATTRIBUTE VOLATILE
ALTER TABLE ATTESTATION_QUESTION VOLATILE
ALTER TABLE ATTESTATION_REPORT VOLATILE
ALTER TABLE ATTESTATION_REQUEST VOLATILE
ALTER TABLE ATTESTATION_RESPONSE VOLATILE
ALTER TABLE ATTESTATION_SURVEY_QUESTION VOLATILE
ALTER TABLE ATTESTATION_TARGET VOLATILE
ALTER TABLE AUTHPROPS VOLATILE
ALTER TABLE DATABASECHANGELOG VOLATILE
ALTER TABLE DATABASECHANGELOGLOCK VOLATILE
ALTER TABLE DSS_APPLET_BROWSER_TYPES VOLATILE
ALTER TABLE DSS_APPLET_CFG VOLATILE
ALTER TABLE DSS_APPLET_CFG_MAP VOLATILE
ALTER TABLE DSS_BROWSER_TYPE VOLATILE
ALTER TABLE DSS_CONFIG VOLATILE
ALTER TABLE DSS_EXT_KEY_USAGE_RESTRICTION VOLATILE
ALTER TABLE DSS_USR_POLICY_SET VOLATILE
ALTER TABLE JBM_COUNTER VOLATILE
ALTER TABLE JBM_DUAL VOLATILE
ALTER TABLE JBM_ID_CACHE VOLATILE
ALTER TABLE JBM_MSG VOLATILE
ALTER TABLE JBM_MSG_REF VOLATILE
ALTER TABLE JBM_POSTOFFICE VOLATILE
ALTER TABLE JBM_ROLE VOLATILE
ALTER TABLE JBM_TX VOLATILE
ALTER TABLE JBM_USER VOLATILE
ALTER TABLE PORTALCATEGORY VOLATILE
ALTER TABLE PORTALPORTLETHANDLES VOLATILE
ALTER TABLE PORTALPORTLETSETTINGS VOLATILE
ALTER TABLE PORTALPRODUCERREGISTRY VOLATILE
ALTER TABLE PORTALPRODUCERS VOLATILE
ALTER TABLE PORTALREGISTRY VOLATILE
ALTER TABLE PROFILEGROUPPREFERENCES VOLATILE
ALTER TABLE PROFILEUSERPREFERENCES VOLATILE
ALTER TABLE PROVISIONING_CODE_MAP VOLATILE
ALTER TABLE PROVISIONING_CODE_MAP_LABEL VOLATILE
ALTER TABLE PROVISIONING_VIEW_VALUE VOLATILE
ALTER TABLE PROVISIONING_VIEW_VALUE_LABEL VOLATILE
ALTER TABLE SECURITYACCESSRIGHTS VOLATILE
ALTER TABLE SECURITYPERMISSIONMETA VOLATILE
ALTER TABLE SECURITYPERMISSIONS VOLATILE
ALTER TABLE SEC_DELPROXY_CFG VOLATILE
ALTER TABLE SEC_DELPROXY_SRV_CFG VOLATILE
ALTER TABLE SEC_SYNC_CLEANUP_QUEUE VOLATILE
```

2.5 Installing the Java Development Kit

The User Application installation program requires that you use the correct version of the Java environment for your application server, as described below:

- For JBoss 5.1.0, you need to use Java 2 Platform Standard Edition Development version 1.6 or later (JDK or JRE) from Sun (Oracle).

  NOTE: If you use JBoss and want to be able to receive updates to the JDK or JRE from Oracle, you must upgrade your environment to use the Java 2 Platform Standard Edition Development version 1.7 or later.

- For WebSphere 7.0, you need to use the 1.6 or later JDK from IBM.
- For WebLogic 10.3, you need to use the 1.6 or later JDK from JRockit.

NOTE: The current certified version of the JDK or JRE is 1.6.34. If you upgrade to the latest version and encounter problems, revert to the certified version.

Set the JAVA_HOME environment variable to point to the JDK to use with the User Application. Or, manually specify the path during the User Application install to override JAVA_HOME.

IMPORTANT: SUSE Linux Enterprise Server (SLES) users, do not use the IBM JDK that comes with SLES. This version is incompatible with some aspects of the installation.

3 Installing the Roles Based Provisioning Module

This section describes how to install the runtime components for the Roles Based Provisioning Module (RBPM) into Identity Manager by using the Roles Based Provisioning Module install program. Topics include:

- Section 3.1, "About the Roles Based Provisioning Module Installation," on page 29
- Section 3.2, "Running the NrfCaseUpdate Utility," on page 30
- Section 3.3, "Running the RBPM Install Program," on page 35
- Section 3.4, "Extending the Schema Manually," on page 42
- Section 3.5, "Extending the Schema Manually with a Non-GUI Install," on page 44

IMPORTANT: In this release, you can no longer create the User Application Driver and the Role and Resource Service Driver through iManager. This method of creating the drivers is no longer supported. To create these drivers, you now need to use the new package management features provided in Designer, as described in Chapter 4, "Creating the Drivers," on page 47.

3.1 About the Roles Based Provisioning Module Installation

Identity Manager 4.0.2 will install the core runtime components of RBPM for you automatically. However, you can also invoke the installation program for the Roles Based Provisioning Module separately.

The RBPM installation program needs to be executed on the machine where your Identity Manager Metadirectory environment has been installed. The installation will fail if eDirectory is not installed in the default location or default dib location.

The User Application expects the eDirectory server be set to require the use of NMAS Login first during login, so that Universal Password (UP) functionality may be enforced. In version 4.0.2, the IDM integrated installer automatically handles this by modifying the `pre_ndsd_start` script (for Linux) or the "HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\Environment" registry key (for Windows):

- In Linux, the `/opt/novell/eDirectory/sbin/pre_ndsd_start` script will be modified by the IDM integrated installer to add the following commands:

  ```
  NDSD_TRY_NMASLOGIN_FIRST=true
  export NDSD_TRY_NMASLOGIN_FIRST
  ```

- In Windows, the registry key "HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\Environment" will be modified to add the key "NDSD_TRY_NMASLOGIN_FIRST" with the string value "true".

  For more information, see the *Identity Manager 4.0.2 Integrated Installation Guide* *(http://www.netiq.com/documentation/idm402/idm_integrated_install/data/front.html)*.

NOTE: The RBPM installation program will fail to execute properly if eDirectory is not running on the default LDAP ports of 389 and 636. If you are not running on the default LDAP ports, you will always be told that the schema is not valid and that you have to run the NrfCaseUpdate utility. To fix this problem, you need to extend the schema manually, as described in Section 3.4, "Extending the Schema Manually," on page 42.

Once these items have been installed into Identity Manager, you need to follow the steps described in Chapter 4, "Creating the Drivers," on page 47 to create the drivers needed to run the User Application.

IMPORTANT: If you have a User Application Driver in your eDirectory tree that was created with 3.6.1 or an earlier release of the RBPM, you need to run the NrfCaseUpdate utility before you run the Roles Based Provisioning Module installation program. If you do not, your installation will fail. This step is not required if you are doing a new installation of version 4.0.2 or are upgrading from 3.7.

3.2 Running the NrfCaseUpdate Utility

This section provides details about the NrfCaseUpdate utility. Topics include:

- Section 3.2.1, "Overview of NrfCaseUpdate," on page 30
- Section 3.2.2, "Installation Overview," on page 30
- Section 3.2.3, "How NrfCaseUpdate Affects the Schema," on page 31
- Section 3.2.4, "Creating a Backup of the User Application Drivers," on page 31
- Section 3.2.5, "Using NrfCaseUpdate," on page 31
- Section 3.2.6, "Verification of the NrfCaseUpdate Process," on page 33
- Section 3.2.7, "Enabling the JRE for SSL Connections," on page 34
- Section 3.2.8, "Restoring Invalidated User Application Drivers," on page 34

3.2.1 Overview of NrfCaseUpdate

The NrfCaseUpdate procedure is necessary to provide support for mixed-case searching on roles and resources. This procedure updates the schema by modifying the nrfLocalizedDescrs and nrfLocalizedNames attributes, which are used by User Application drivers. The procedure is required before installing RBPM 4.0.2 and before migrating existing drivers in Designer 4.0.2, if your eDirectory tree was created with 3.6.1 or an earlier release of the RBPM. This step is not required if you are doing a new installation of version 4.0.2 or are upgrading from 3.7.

3.2.2 Installation Overview

This section provides an overview of the steps for upgrading and migrating your existing RBPM environment. This overview emphasizes use of Designer 4.0.2 to create backups of User Application drivers before proceeding with any upgrade.

1. Install Designer 4.0.2.
2. Run a health check of the Identity Vault to make sure the schema extends properly. Use TID 3564075 to complete the health check.
3. Import existing User Application drivers into Designer 4.0.2.
4. Archive the Designer project. It represents the pre-RBPM 4.0.2 state of the driver.

5. Run the NrfCaseUpdate process.
6. Create a new Designer 4.0.2 project and import the User Application driver to prepare for migration.
7. Install RBPM 4.0.2.
8. Migrate the driver using Designer 4.0.2.
9. Deploy the migrated driver.

3.2.3 How NrfCaseUpdate Affects the Schema

When the NrfCaseUpdate utility updates existing attributes in the eDirectory schema, any existing instances of those attributes are effectively deleted. User Application drivers use these attributes and thus will be affected by this schema update, specifically roles and separation of duties names and descriptions, custom attestation requests, and reports.

The NrfCaseUpdate procedure updates existing User Application drivers by providing a utility for exporting existing User Application drivers to an LDIF file before running the schema update. Importing the LDIF files after the schema update effectively recreates any objects deleted during the schema update.

As always, it is important that you back up any existing User Application drivers as a precaution. Remember that schema updates will affect all Identity Manager partitions, so it is very important to use NrfCaseUpdate to export any User Application drivers in the tree.

3.2.4 Creating a Backup of the User Application Drivers

It is recommended that you use Designer to create a backup of your User Application drivers. Before running the NrfCaseUpdate procedure, you should follow this procedure to back up your existing User Application drivers:

1. Install Designer 4.0.2, which ships with RBPM 4.0.2.
2. Create an Identity Vault and map it to your Identity Manager server containing your User Application drivers.
3. Use the *Live->Import* command to import your Driver Set and User Application drivers.
4. Save and archive this Designer project.

3.2.5 Using NrfCaseUpdate

NrfCaseUpdate will prompt you to export each driver and then will perform the schema update. If you are unsure about the existence or location of any existing User Application drivers, you should not proceed, as the schema update may invalidate any existing User Application drivers.

The JRE provided under the Identity Manager installation directory, typically `/root/idm/jre`, can be used to run NrfCaseUpdate. If you require SSL connections to eDirectory, you will need to enable your JRE for SSL connections by following the instructions in Section 3.2.7, “Enabling the JRE for SSL Connections,” on page 34.

Alternatively, you may run the NrfCaseUpdate utility remotely from a host with a JRE that contains the eDirectory certificate, such as the User Application server host. In this case, you will need to exit the NrfCaseUpdate utility using CTRL-C after exporting all drivers to LDIF and before the schema update. Then, you can manually update the schema on the eDirectory host using the ndssch command, as shown below:

```
ndssch -h hostname adminDN update-nrf-case.sch
```

NOTE: NrfCaseUpdate can accept several arguments to the command line. Pass `-help` or `-?` for more information.

Follow these steps to run NrfCaseUpdate:

1 Verify that you have completed a health check of the Identity Vault before running the NrfCaseUpdate utility. Use TID 3564075 to complete the health check.

2 Identify all the DNs of any existing User Application drivers before you start the utility. You will need authentication credentials to export these drivers to LDIF.

3 Run the NrfCaseUpdate utility. You may optionally pass the `-v` option to obtain more verbose output:

```
/root/idm/jre/bin/java -jar NrfCaseUpdate.jar -v
```

4 You will be asked if you have an existing User Application driver. Answer true if you have an existing User Application driver. Otherwise, answer false and skip to Step 15 on page 33.

```
Do you currently have a User Application Driver configured [DEFAULT true] :
```

5 Next, the utility asks if you have more than one User Application driver. Answer true if you have more than one User Application driver:

```
Do you currently have more than one (1) User Application Driver configured
[DEFAULT false] :
```

6 Specify the DN of the administrator with proper credentials for exporting the User Application driver:

```
Specify the DN of the Identity Vault administrator user.
This user must have inherited supervisor rights to the user application driver
specified above.
(e.g. cn=admin,o=acme):
```

7 Enter the password for this administrator:

```
Specify the Identity Vault administrator password:
```

8 Enter the host name or IP address of the Identity Manager server hosting the User Application driver:

```
Specify the DNS address of the Identity Vault (e.g acme.com):
```

9 Specify the port to be used for the connection:

```
Specify the Identity Vault port [DEFAULT 389]:
```

10 The next question asks if you will use SSL for the connection. If you want to use SSL, the JRE requires the eDirectory certificate to be in the trusted store. To persist the certificate, follow the instructions in Section 3.2.7, “Enabling the JRE for SSL Connections,” on page 34.

```
Use SSL to connect to Identity Vault: [DEFAULT false] :
```

11 Specify the fully qualified distinguished name of the User Application driver that will be exported:

```
Specify the fully qualified LDAP DN of the User Application driver located in
the Identity Vault
(e.g. cn=UserApplication,cn=driverset,o=acme):
```

If the DN includes a space, it has to be included in single quotes, as shown below:

```
'cn=UserApplication driver,cn=driverset,o=acme'
```

12 Specify a name for the LDIF file where the User Application will be exported:

```
Specify the LDIF file name where the restore data will be written (enter
defaults to nrf-case-restore-data.ldif):
```

13 The utility will post information about the objects saved to the LDIF.

14 If you indicated you have multiple drivers, you will see the following prompt:

```
You indicated you have more than one (1) User Application Driver to configure.
Do you have another driver to export? [DEFAULT false] :

If you have another driver to export then specify true. The utility will repeat
Steps 5 through 12 for each driver.

If you do not have another driver to export then specify false. Ensure that you
have exported all existing drivers before proceeding as the utility will
proceed with the schema update.
```

15 You will be prompted for the location of your `ndssch` utility, along with the typical locations. The `ndssch` utility is used for updating the schema.

```
Please enter the path to the schema utility:
For Unix/Linux typically /opt/novell/eDirectory/bin/ndssch
For Windows C:\Novell\NDS\schemaStart.bat:
```

16 The utility will post the status message for the schema update:

```
Schema has successfully been updated for mixed case compliance!
```

NOTE: Be sure to give eDirectory enough time to synchronize the schema changes. If you don't allow enough time, the import of the LDIF file fail.

17 Run another health check on the Identity Vault to verify that the schema was extended properly before importing the LDIF file. Use TID 3564075 to complete the health check.

18 After all drivers have been exported and the schema update has been applied successfully, you need to import each LDIF file. You should indicate to allow forward references in your `ice` command. A suggested command line is shown below:

```
ice -l [mylogfile.log] -v -SLDIF -f [your_created_ldif] -c -DLDAP -s [hostname]
-p [389/636] -d [cn=myadmin,o=mycompany] -w [MYPASSWORD] -F -B
```

19 After all drivers have been re-imported, verify that the NrfCaseUpdate process was successful. See Section 3.2.6, "Verification of the NrfCaseUpdate Process," on page 33 for more information.

20 After you have verified that the NrfCaseUpdate process was successful, you may continue with the RBPM 4.0.2 installation.

3.2.6 Verification of the NrfCaseUpdate Process

After all drivers have been re-imported, verify that the restoration was successful by reviewing the following items in the User Application:

- Role names and descriptions
- Separation of duties names and descriptions
- Attestation requests, including custom requests
- Reporting

After you complete the verification, you can continue with installation and upgrade to RBPM 4.0.2.

3.2.7 Enabling the JRE for SSL Connections

This section explains how to configure the JRE to use an SSL connection.

First, export a self-signed certificate from the certificate authority in the Identity Vault:

1. From iManager, in the *Roles and Tasks* view, click *Directory Administration* > *Modify Object*.
2. Select the certificate authority object for the Identity Vault, then click *OK*. It is usually found in the Security container and named as *TREENAME* CA.Security.
3. Click *Certificate* > *Self Signed Certificate*.
4. Click *Export*.
5. When you are asked if you want to export the private key with the certificate, click *No*, then click *Next*.
6. Select binary DER format.
7. Click the link *Save the exported certificate*.
8. Browse to a location on your computer where you want to save the file, then click *Save*.
9. Click *Close*.

Next, import the self-signed certificate into the JRE's trusted store.

1. Use the keytool utility that is included in the JRE.
2. Import the certificate into the Role Mapping Administrator's trust store by entering the following command at a command prompt:

   ```
   keytool -import -file name_of_cert_file -trustcacerts -noprompt -keystore
   filename -storepass password
   ```

   For example:

   ```
   keytool -import -file tree_ca_root.b64 -trustcacerts -noprompt -keystore
   cacerts -storepass changeit
   ```

3.2.8 Restoring Invalidated User Application Drivers

If the schema update is applied to an existing User Application driver before that driver has been processed using NrfCaseUpdate, it will be invalidated and you will need to restore that driver using a backup.

IMPORTANT: It is essential that you do *not* delete or rename the invalidated User Application driver, since doing so will also invalidate all the driver's associations. Additionally, if the Role and Resource Service driver is running, and you delete the User Application driver, the Role and Resource Service driver will detect the role deletions and remove the roles from the assigned users.

Additionally, it is not sufficient to redeploy the backed up driver to Identity Manager as the schema change cannot be reconciled in this manner. The following procedure performs the restoration by deploying a renamed copy of the driver in order to generate the data to be restored.

The following procedure outlines the process for restoring the User Application driver backup using Designer 4.0.2:

1. Restart the eDirectory server to ensure that the schema modification has taken effect.
2. Open a copy of the Designer 4.0.2 project containing the backup of the User Application driver, UserAppDriver. Since this procedure modifies the driver name so it is important to use a copy of the project.

3 Select the connector between the User Application driver and the Identity Vault, right-click and choose *Properties*.

4 Specify a new name such as `UserAppDriver_restore`. Select *Apply* and *OK*.

5 Click *Save* to save the project.

6 Synchronize the ID Vault schema by selecting the ID Vault and choosing *Live->Schema->Compare* and choose to *Update Designer for the Reconcile Action*.

7 Save the project.

8 Deploy the renamed driver by selecting the driver and choosing *Driver->Deploy*.

9 Run NrfCaseUpdate and export the newly named driver to an LDIF file.

10 Make a copy of the LDIF file for editing.

11 Edit the LDIF file and rename all the driver references to reflect the User Application driver that you are restoring. For example, if your original User Application driver is `cn=UserAppDriver` then you would rename `cn=UserAppDriver_restore` to `cn=UserAppDriver`. This step effectively builds an LDIF file reflecting the real User Application driver.

12 Import the modified LDIF file using ice:

```
ice -l[mylogfile.log] -v -SLDIF -f[your_created_ldif] -c -DLDAP -s[hostname] -
p[389/636] -d[cn=myadmin,o=mycompany] -w[MYPASSWORD] -F -B
```

13 Note the status of the import using ice to ensure it was successful.

14 Follow the instructions under Section 3.2.6, "Verification of the NrfCaseUpdate Process," on page 33 to verify the restoration of the driver.

15 Delete the renamed driver from the Driver Set.

3.3 Running the RBPM Install Program

1 Launch the installer for your platform:

Linux

```
rbpm_driver_install_linux.bin
```

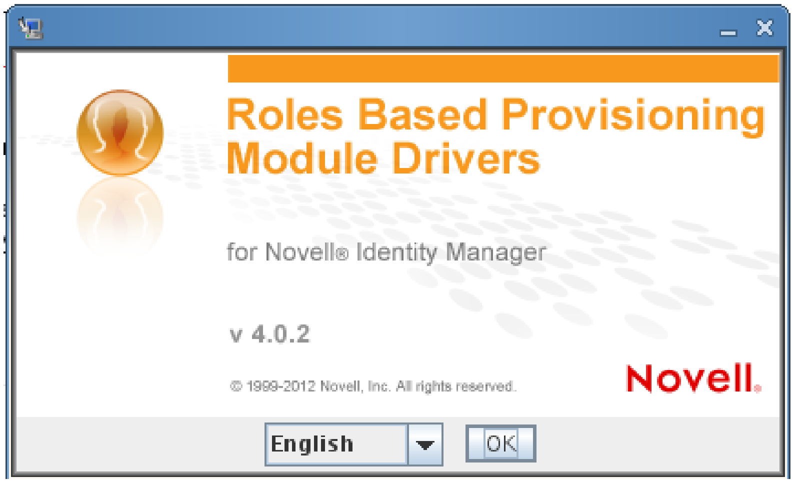
Solaris

```
rbpm_driver_install_solaris.bin
```

Windows

```
rbpm_driver_install.exe
```

When the installation program launches, you are prompted for the language:


Roles Based Provisioning Module Drivers

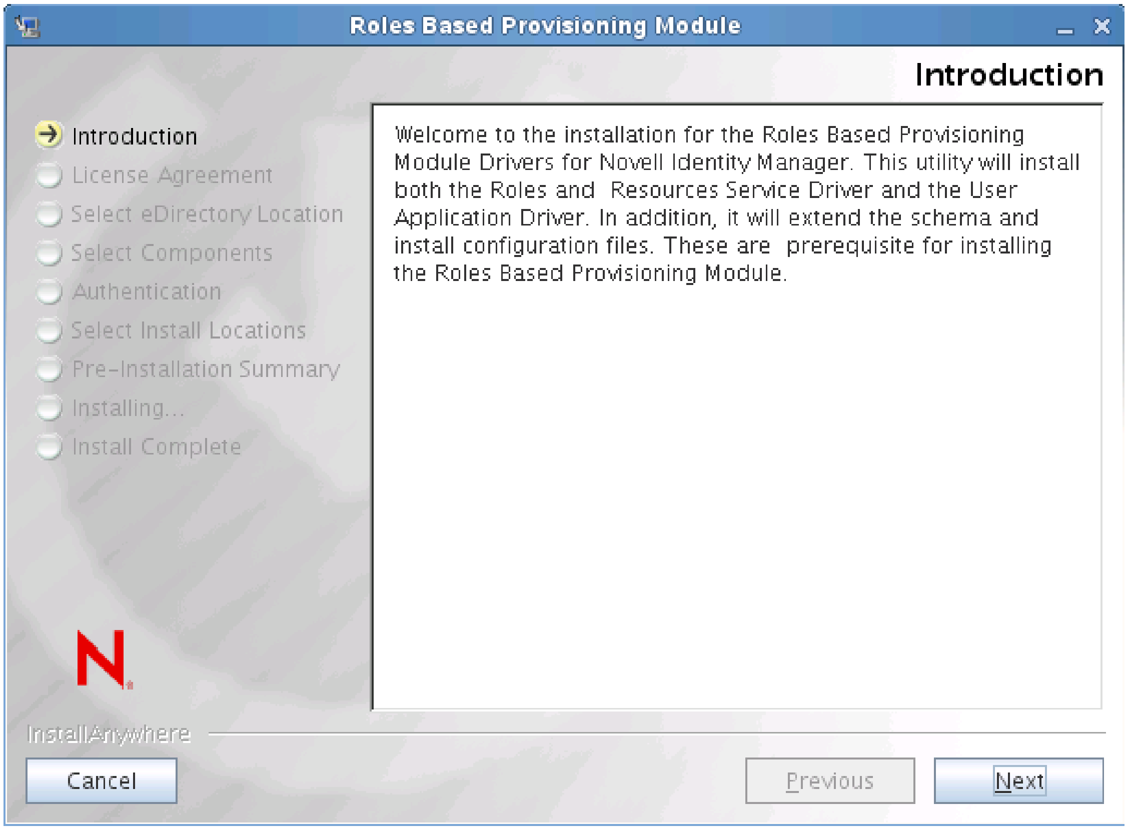
for Novell® Identity Manager

v 4.0.2

© 1999-2012 Novell, Inc. All rights reserved.

2 Choose the language for your installation and click OK.

The installer displays the Introduction screen.

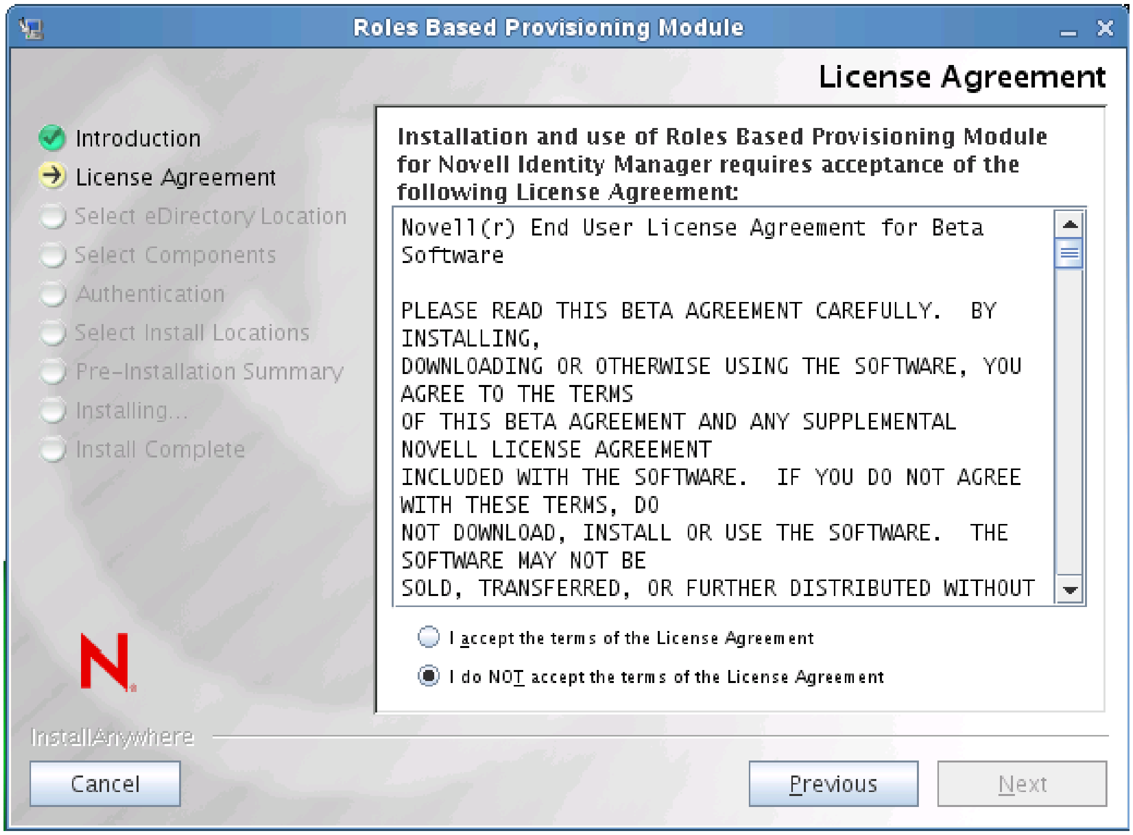

Roles Based Provisioning Module

Introduction

Welcome to the installation for the Roles Based Provisioning Module Drivers for Novell Identity Manager. This utility will install both the Roles and Resources Service Driver and the User Application Driver. In addition, it will extend the schema and install configuration files. These are prerequisite for installing the Roles Based Provisioning Module.

3 Click *Next*.

The installer displays the License Agreement screen.



Installation and use of Roles Based Provisioning Module for Novell Identity Manager requires acceptance of the following License Agreement:

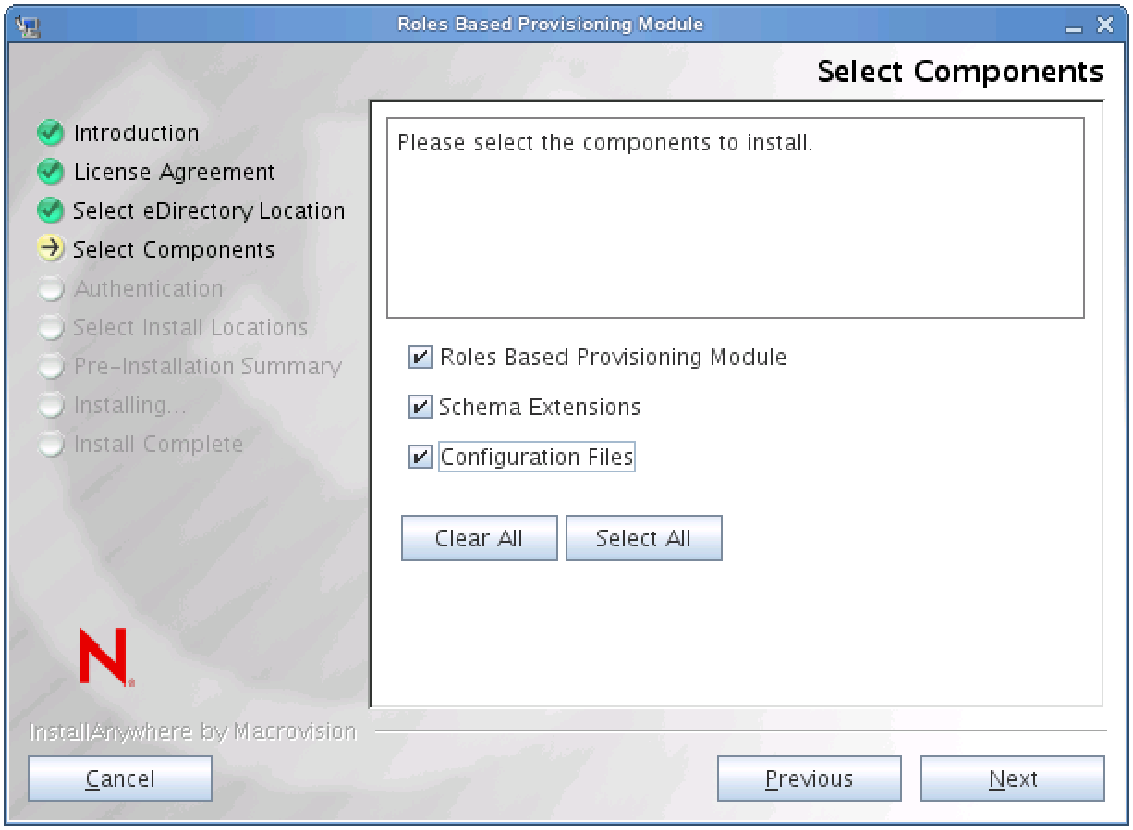
```
Novell(r) End User License Agreement for Beta
Software

PLEASE READ THIS BETA AGREEMENT CAREFULLY.  BY
INSTALLING,
DOWNLOADING OR OTHERWISE USING THE SOFTWARE, YOU
AGREE TO THE TERMS
OF THIS BETA AGREEMENT AND ANY SUPPLEMENTAL
NOVELL LICENSE AGREEMENT
INCLUDED WITH THE SOFTWARE.  IF YOU DO NOT AGREE
WITH THESE TERMS, DO
NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE.  THE
SOFTWARE MAY NOT BE
SOLD, TRANSFERRED, OR FURTHER DISTRIBUTED WITHOUT
```

○ I accept the terms of the License Agreement

● I do NOT accept the terms of the License Agreement

4 Confirm the license agreement and click *Next*.

The installer displays the Select Components screen, which lists the Metadirectory components required for the RBPM User Application to run:



Please select the components to install.

☑ Roles Based Provisioning Module

☑ Schema Extensions

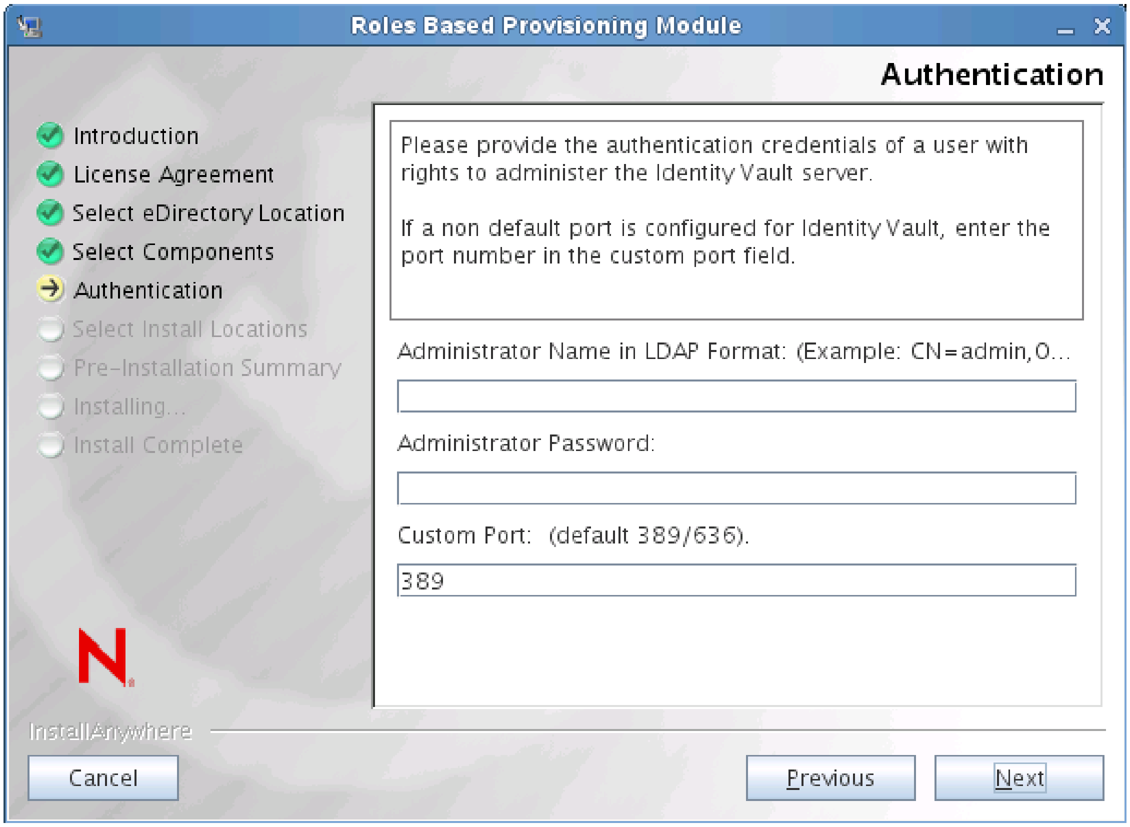
☑ Configuration Files

The components are described below:

Component	Description
Roles Based Provisioning Module	Installs the User Application Driver and the Role and Resource Driver.
Schema Extensions	Installs the eDirectory schema extensions.
Configuration Files	Installs driver configuration files.

5 Select the components you want to install, and click *Next*. Typically, you will want to install all of the components.

The installer displays the Authentication screen:



Authentication

Please provide the authentication credentials of a user with rights to administer the Identity Vault server.

If a non default port is configured for Identity Vault, enter the port number in the custom port field.

Administrator Name in LDAP Format: (Example: CN=admin,O...

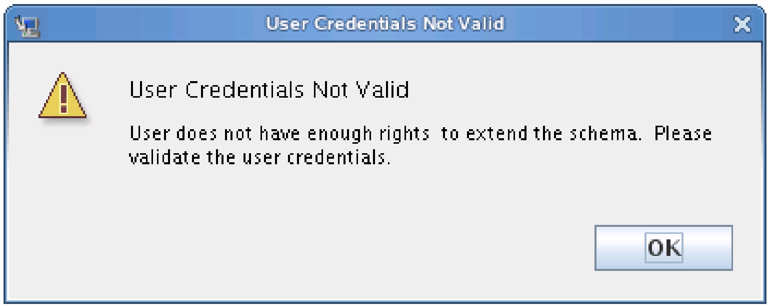
Administrator Password:

Custom Port: (default 389/636).

389

6 Provide the name of the administrator in LDAP format and type the password. Also, specify the port for the LDAP server.

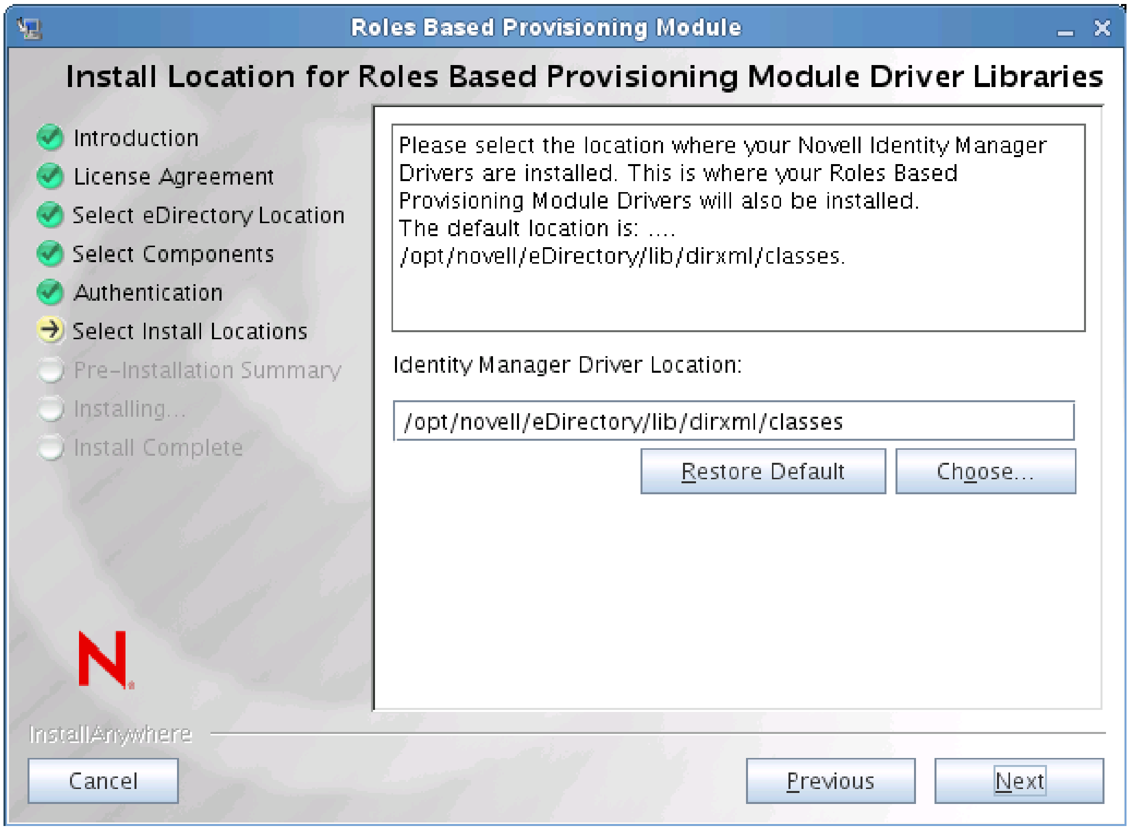
If the user credentials are not valid, or if the user does not have the necessary rights, the installer displays an error screen:



User Credentials Not Valid

User does not have enough rights to extend the schema. Please validate the user credentials.

If the user credentials are valid and the user has the proper rights, the installer displays the Install Location for Roles Based Provisioning Module Driver Libraries screen:



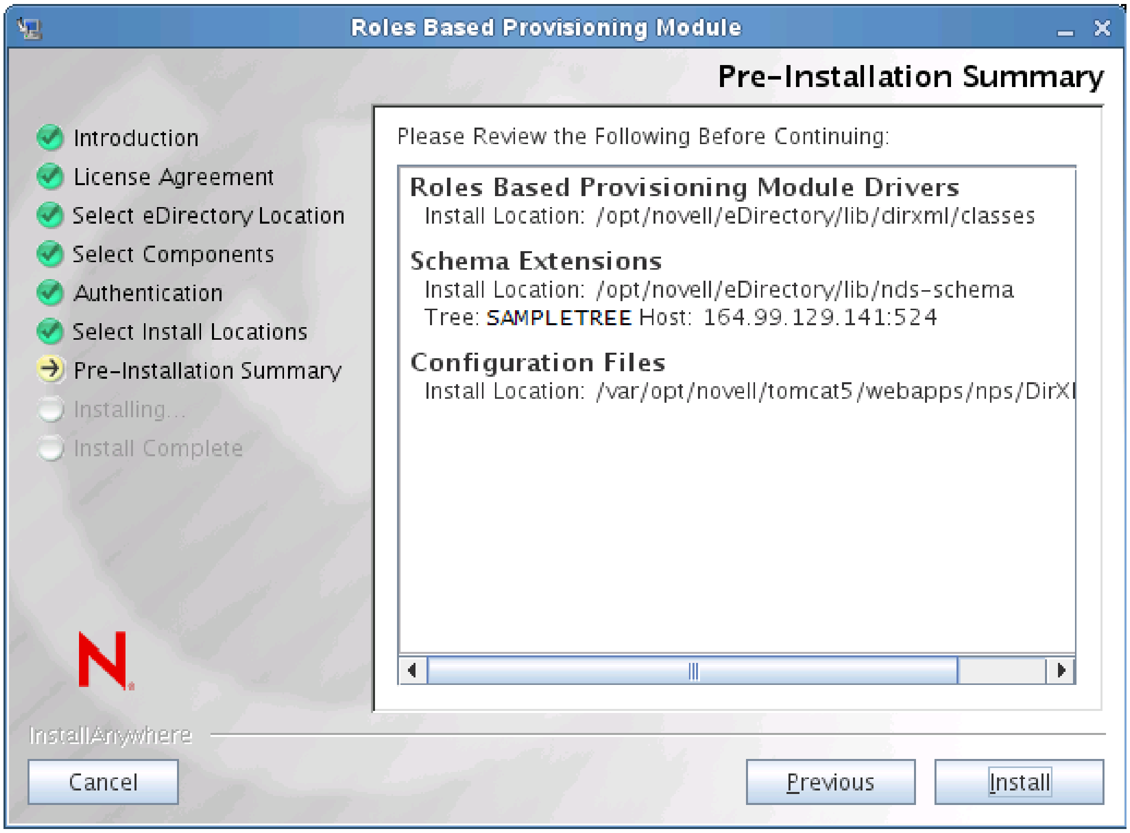
Please select the location where your Novell Identity Manager Drivers are installed. This is where your Roles Based Provisioning Module Drivers will also be installed.
The default location is: ....
/opt/novell/eDirectory/lib/dirxml/classes.

Identity Manager Driver Location:

/opt/novell/eDirectory/lib/dirxml/classes

7 Specify the target location on disk where you want the driver libraries to be stored and click *Next*.

The installer displays the Pre-Installation Summary screen:



Please Review the Following Before Continuing:

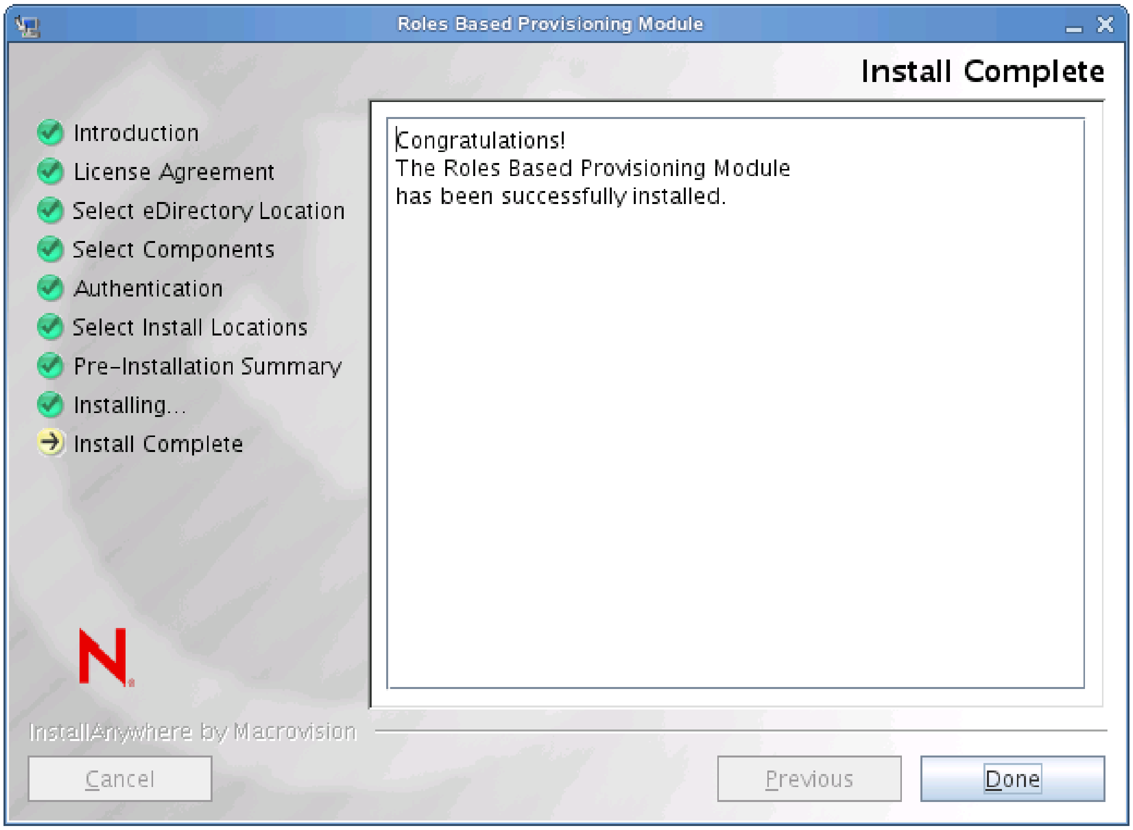
Roles Based Provisioning Module Drivers
Install Location: /opt/novell/eDirectory/lib/dirxml/classes

Schema Extensions
Install Location: /opt/novell/eDirectory/lib/nds-schema
Tree: SAMPLETREE Host: 164.99.129.141:524

Configuration Files
Install Location: /var/opt/novell/tomcat5/webapps/nps/DirXI

8 If the summary information appears to be correct, click *Install* to begin the installation process.

When the installation process is finished, the installer displays the Installation Complete screen:



Congratulations!
The Roles Based Provisioning Module
has been successfully installed.

NOTE: If you need to uninstall the runtime components associated with RBPM, the uninstall program will automatically reboot your server machine, unless you are running the uninstall program in silent mode on Windows. In this case, you need to reboot your Windows machine manually. In addition, if you want to uninstall Identity Manager outside of the Integrated Installer, you need to stop the nds service before launching the uninstall program.

3.4 Extending the Schema Manually

This section provides instructions for extending the schema manually. These steps are only required to fix a problem that occurs if eDirectory is not installed in the default location.

To extend the schema manually (Windows):

1 After installing Identity Manager, stop eDirectory.

2 Run the following command to extend the schemas listed in `sch_nt.cfg`, which is located in the eDirectory installation location.

```
<eDirLocation>\schemaStart.bat <eDirLocation> yes <admin name
with tree> <password> yes 6 " " " <schemafileName>"
"<serverName>" <dibPathLocation>
```

NOTE: The <*dibPathLocation*> must contain the DIBFiles folder.

Here is a sample command:

```
C:\eDir\NDS\schemaStart.bat "C:\eDir\NDS" yes
".cn=admin.o=n.T=IDM-INSTALLISSUE." "n" yes 6 " "
"C:\eDir\NDS\ vrschema.sch" ".CN=WIN2008-64-NDS.O=n.T=IDMINSTALLISSUE."
"C:\DIB\NDS\DIBFiles"
```

NOTE: The above command does not use sch_nt.cfg to extend all the schema files, but instead extends each and every schema file mentioned in sch_nt.cfg manually.

3 Install the Role and Resource Driver (as described under Section 3.3, "Running the RBPM Install Program," on page 35), unchecking the *Schema Extensions* option in the *Select Components* window. Complete the installation.

NOTE: If you are not able to use the GUI installer, you need to perform some additional steps manually. These steps are covered under Section 3.5, "Extending the Schema Manually with a Non-GUI Install," on page 44. The additional manual steps are required if you are installing RBPM on top of a non-root install of eDirectory and Identity Manager.

4 After installing the Role and Resource Driver, extend the role-based schema files `srvprv.sch` and `nrf-extensions.sch` by executing the command listed in Step 2 on page 42.

NOTE: This procedure extends the needed schema files using `schemaStart.bat`.

5 Extend the NrfCaseupdate schema (`update-nrf-case.sch`) using the command listed in Step 2 on page 42.

6 Start eDirectory.

To extend the schema manually (SUSE):

1 Install the Role and Resource Driver (as described under Section 3.3, "Running the RBPM Install Program," on page 35), with the *Schema Extensions* option unchecked in the *Select Components* window. Click *Next*.

NOTE: If you are not able to use the GUI installer, you need to perform some additional steps manually. These steps are covered under Section 3.5, "Extending the Schema Manually with a Non-GUI Install," on page 44. The additional manual steps are required if you are installing RBPM on top of a non-root install of eDirectory and Identity Manager.

2 Choose an appropriate install location for the Driver and click *Next*.

3 Choose an appropriate install location for the Driver configuration files and click *Next*. Complete the installation.

Steps 1 through 3 copy the Driver and Driver Configuration files in the Non-default location of eDirectory.

4 Run the `ndssch` command to extend the schema (i.e. `srvprv.sch`, `nrf-extensions.sch`).

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

For example:

```
ndssch -h 172.16.1.137:524 -t TESTTREE -p 'PASSWORD'
.cn=admin.o=novell.T=TESTTREE.
/opt/novell/eDirectory/lib/nds-schema/srvprv.sch'
```

5 Repeat Step 4 to extend `nrf-extensions.sch`.

3.5 Extending the Schema Manually with a Non-GUI Install

If you are not able to use the GUI installer to extend your schema manually, you need to perform some additional steps. This is the case if you are installing RBPM on top of a non-root install of eDirectory and Identity Manager.

These steps are presented below.

- Section 3.5.1, "Extending the eDirectory Schema for Roles Based Provisioning Module," on page 44
- Section 3.5.2, "Copying Additional JAR files," on page 45
- Section 3.5.3, "Copying the dirxml.lsc File," on page 45

For these steps, you need several additional files, `nrf-extensions.sch`, `nrfdriver.jar`, `srvprvUAD.jar`, `xcd-all.jar`, and `dirxml.lsc`. These files can be found in the `prerequisites.zip` file.

You can find the `nrf-extensions.sch` file in the `./schema` folder within the `prerequisitefiles.zip` archive within the .iso image for Identity Manager Advanced Edition. You can find the additional JAR files in the `./lib` folder within the `prerequisitefiles.zip` archive. You can find the `dirxml.lsc` file in the top-most folder within the `prerequisitefiles.zip` archive.

3.5.1 Extending the eDirectory Schema for Roles Based Provisioning Module

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

- "Extending the Schema on Windows" on page 44
- "Extending the Schema on UNIX/Linux" on page 44

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`).

   NOTE: You can copy this file from the `./schema` folder within the `prerequisitefiles.zip` archive within the .iso image for Identity Manager Advanced Edition.

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, use the `ndssch` command from the command line:

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

3.5.2 Copying Additional JAR files

Manually install the following additional JAR files on the metadirectory server:

- `nrfdriver.jar`
- `srvprvUAD.jar`
- `xcd-all.jar`

You can find these files in the `./lib` folder within the `prerequisitefiles.zip` archive within the .iso image for Identity Manager Advanced Edition. You must add all of the JAR files and the `tmp` folder that is located under `./lib` in the `prerequisitefiles.zip` archive.

Copy these files to the correct directory for your system:

Table 3-1 *Location for the Role Service Driver JAR file*

Operating System	Directory
UNIX/Linux (eDirector 8.8.x)	`/opt/novell/eDirectory/lib/dirxml/classes`
Windows	`<drive>:\novell\nds\lib`

3.5.3 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.netiq.com/documentation/idm402/pdfdoc/agpro/agpro.pdf).

You can find this file in the top-most directory in the `prerequisitefiles.zip` archive within the .iso image for Identity Manager Advanced Edition.

4 Creating the Drivers

This section describes how to use Designer to create the drivers for using the Roles Based Provisioning Module (RBPM). Topics include:

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

The driver configuration support allows you to do the following:

- Associate one User Application driver with a Role and Resource Service driver.
- Associate one User Application with a User Application driver.

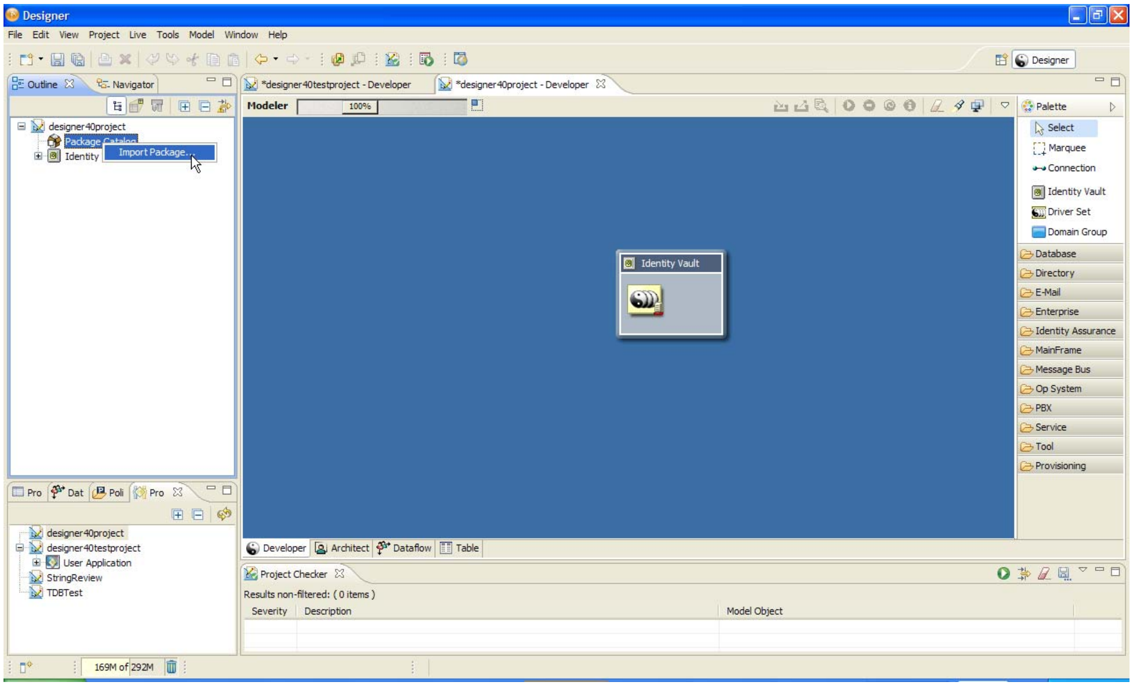
IMPORTANT: In this release, you can no longer create the User Application Driver and the Role and Resource Service Driver through iManager. This method of creating the drivers is no longer supported. To create these drivers, you now need to use the new package management features provided in Designer, as described below.

4.1 Installing the Packages

Before you attempt to configure the drivers, you need to be sure you have all of the necessary packages in the Package Catalog. When you create a new Identity Manager project, the user interface automatically prompts you to import several packages into the new project. If you choose not to import the packages at the time you create your project, you need to install them later, as described below.

To install the packages after creating a new Identity Manager project:

1. Once you’ve create a new Identity Manager project in Designer, select the *Package Catalog* and click *Import Package*.



Designer displays the *Select Package* dialog box.

2 Click *Select All*, then click *OK*.

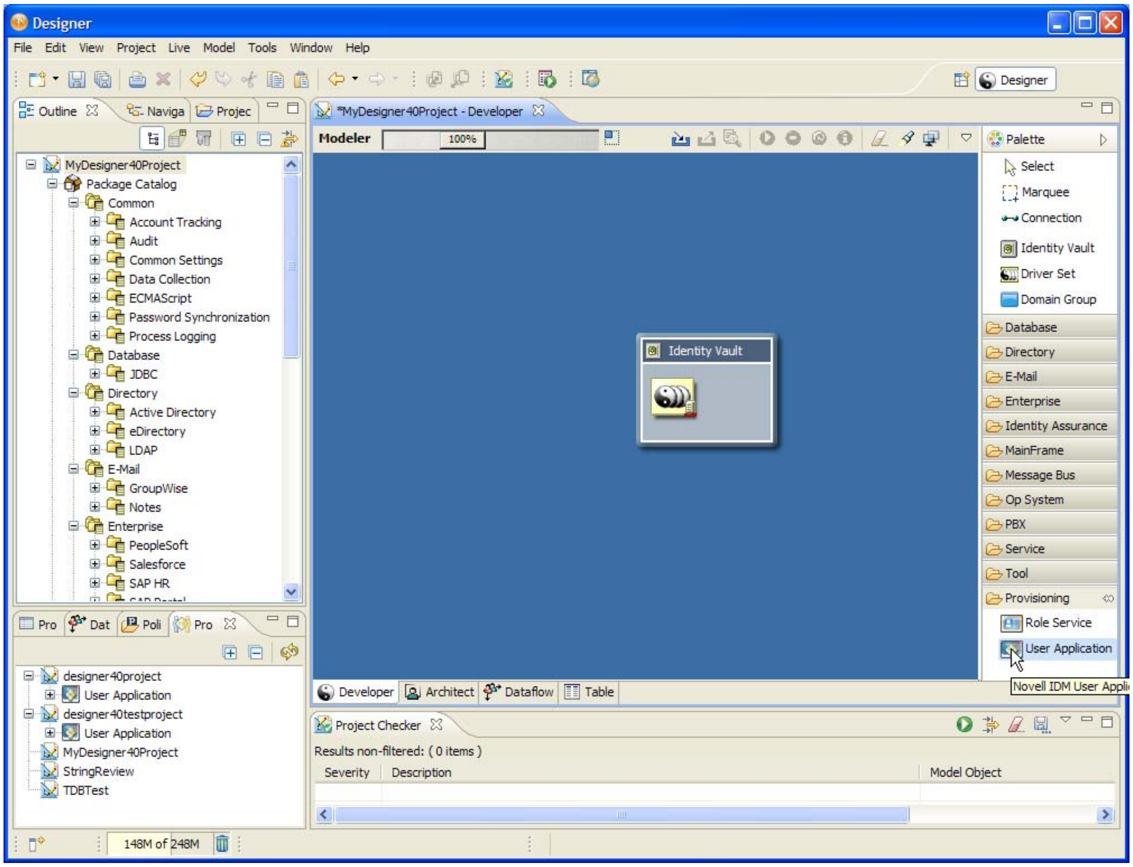
Designer adds several new package folders under the *Package Catalog*. These package folders correspond to the objects in the palette on the right side of the *Modeler* view in Designer.

3 Click *Save* to save your project.

4.2 Creating the User Application Driver

To create the User Application Driver in Designer:

1 Select *User Application* in the palette in the *Modeler* view:



2 Drag the icon for *User Application* onto the *Modeler* view.

Designer displays the *Driver Configuration Wizard*.

3 Select *User Application Base* and click *Next*.

NOTE: For the 4.0.2 release, you need to have version 2.2.0.20120516011608 of the User Application Base package.

The interface displays a dialog to inform you that need several additional packages.

4 Click *OK* to install the required packages.

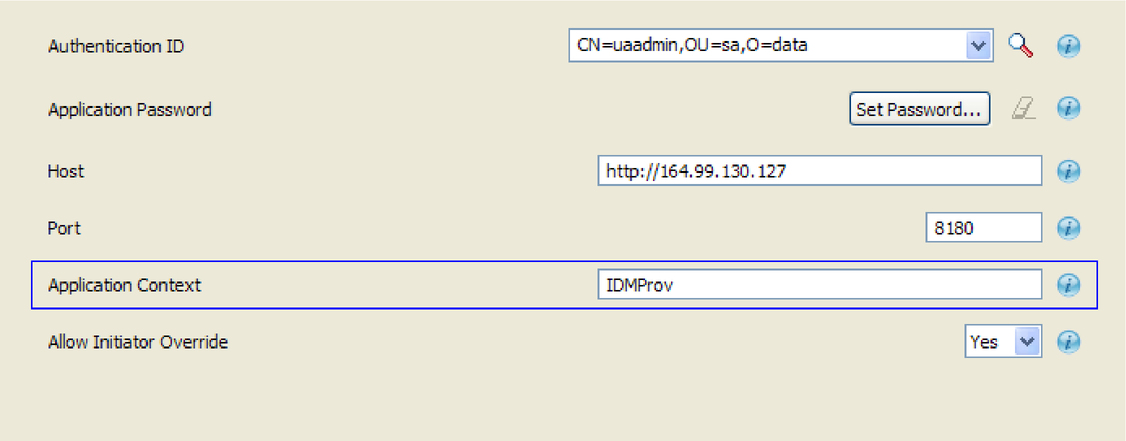
At this point, the wizard displays a screen that allows you to name the driver.

5 You can accept the default driver name, or change it if you like.

Press *Next*.

The wizard now displays a screen that allows you to specify the connection parameters for the driver.

6 Specify the ID and password for the User Application Administrator, as well as the host, port, and application context for the User Application server. If you want to allow the Provisioning Administrator to start workflows in the name of another person for whom the Provisioning Administrator is designated as proxy, select *Yes* for *Allow Initiator Override*:



Authentication ID: CN=uaadmin,OU=sa,O=data

Application Password: Set Password...

Host: http://164.99.130.127

Port: 8180

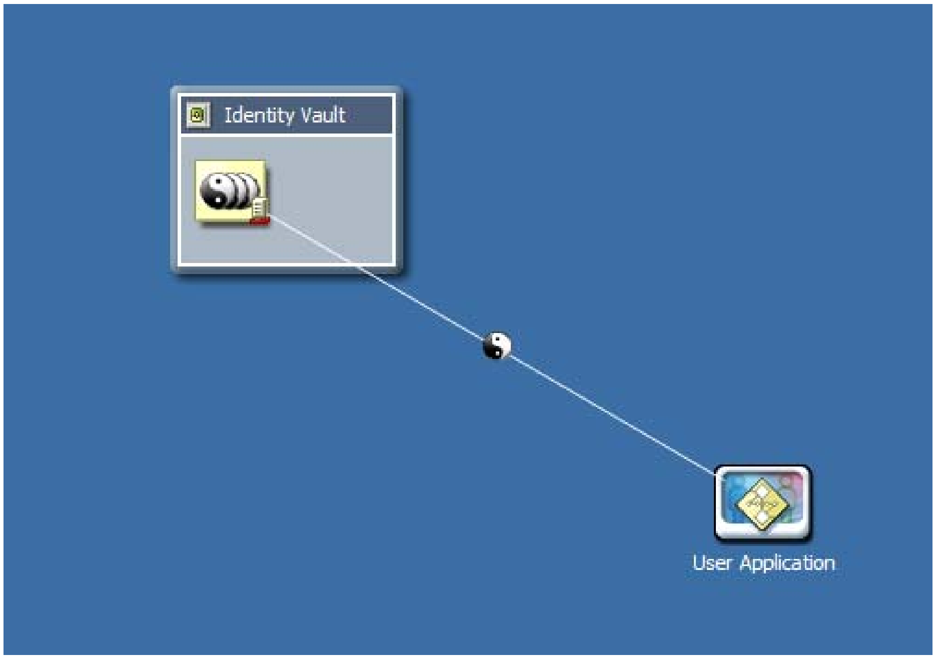
Application Context: IDMProv

Allow Initiator Override: Yes

The wizard then displays the *Confirm Installation Tasks* screen.

7 If everything looks correct, click *Finish*.

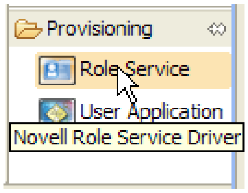
Designer adds the *User Application* driver to the *Modeler* view:



4.3 Creating the Role and Resource Service Driver

To create the Role and Resource Service Driver in Designer:

1 Select *Role Service* in the palette in the *Modeler* view:



2 Drag the icon for *Role Service* onto the *Modeler* view.

Designer displays the *Driver Configuration Wizard*.

3 Select *Role and Resource Service Base* and click *Next*.

NOTE: For the 4.0.2 release, you need to have version 2.0.0.20120509191258 of the Role and Resource Service Base package.

The wizard displays a screen that allows you to specify a name for the driver.

4 You can accept the default driver name, or change it if you like.

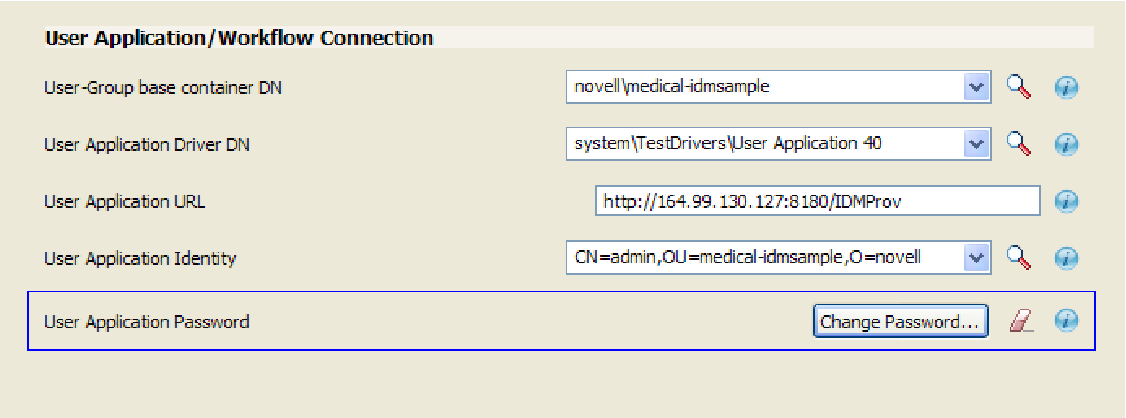
Press *Next*.

The wizard now displays a screen that allows you to specify the connection parameters for the driver.

NOTE: Because the Role and Resource Service Driver uses jClient, Identity Manager does not support using the Role and Resource Service Driver with the Remote Loader.

5 Specify the DN for the base container and the User Application Driver you just created. Since the driver has not yet been deployed, the browse function will not show the User Application Driver you just configured, so you may need to type the DN for the driver.

Also, provide the URL for the User Application, along with the ID and password for the User Application Administrator:



User Application/Workflow Connection

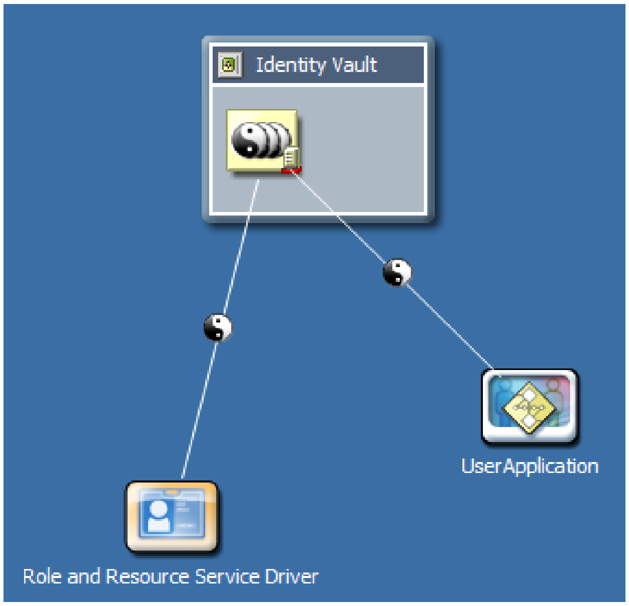
User-Group base container DN	novell\medical-idmsample
User Application Driver DN	system\TestDrivers\User Application 40
User Application URL	http://164.99.130.127:8180/IDMProv
User Application Identity	CN=admin,OU=medical-idmsample,O=novell
User Application Password	

Click *Next*.

The wizard now displays the *Confirm Installation Tasks* screen.

6 If everything looks correct, click *Finish*.

Designer adds the *Role Service* driver to the *Modeler* view:



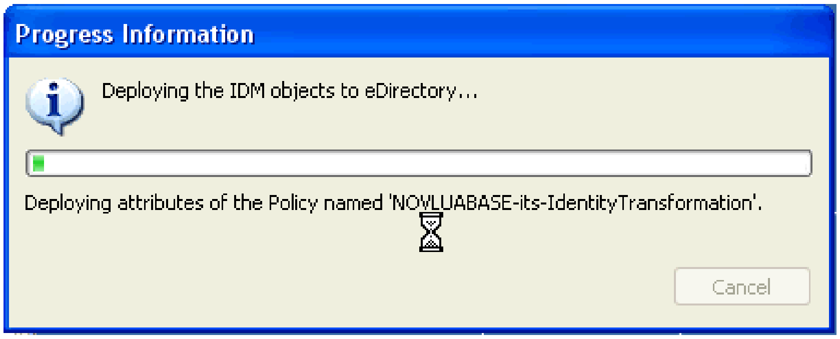
4.4 Deploying the Drivers

To deploy the drivers you've just configured:

1 Select the Driver Set (either in the *Modeler* view or in the *Outline* view).

2 Choose *Live>Deploy*.

Designer displays a progress window that shows which objects are being deployed:



Deploying the IDM objects to eDirectory...

Deploying attributes of the Policy named 'NOVLUABASE-its-IdentityTransformation'.

NOTE: When replicating an eDirectory environment, you must ensure that the replicas contain the NCP Server object for Identity Manager. Identity Manager is constrained to the local replicas of a server. For this reason, the Role and Resource Service Driver may not start properly if a secondary server does not include the server object.

5 Installing the User Application on JBoss

This section describes how to install the User Application for the Roles Based Provisioning Module on a JBoss Application Server by using the graphical user interface version of the installer. It includes these topics:

- Section 5.1, “Installing and Configuring the User Application WAR,” on page 53
- Section 5.2, “Deploying RBPM on JBoss EAP,” on page 61
- Section 5.3, “Testing the Installation,” on page 65

If you prefer to use the command line for installation, see Chapter 8, “Installing from the Console or with a Single Command,” on page 101.

Run the installer as root You need to run the installer as the root user.

Data Migration For information on migrating, see the *RBPM and Reporting Migration Guide* (http://www.netiq.com/documentation/idm402/index.html).

5.1 Installing and Configuring the User Application WAR

NOTE: For JBoss 5.1.0, the installation program requires the Java 2 Platform Standard Edition Development Kit version 1.6 (JRE or JDK) from Sun (Oracle). If you use a different version, the installation procedure does not successfully configure the User Application WAR file. The installation appears to succeed, but you encounter errors when trying to start the User Application.

1. Launch the installer for your platform from the command line.

   To launch the installer, you need to start the `IdmUserApp.jar` file with the JRE. The installer JAR file can be found in `products/RBPM/user_app_install` within the `.iso` image file for Identity Manager 4.0.2.

   Be sure to use the correct version of the Sun JRE (as outlined in the Section 1.3, “System Requirements,” on page 10) to start the User Application installer.

   Depending on where the JRE is installed, the command you use to launch the installer would be one of the following:

   Linux/Solaris

   ```
   $ /opt/novell/jre/bin/java -jar IdmUserApp.jar
   ```

   or

   ```
   $ /opt/novell/idm/jre/bin/java -jar IdmUserApp.jar
   ```

   Windows

   ```
   C:\Novell\InstallFiles\> "C:\Program Files\Java\jdk1.6.0_31\bin\java.exe" -jar
   IdmUserApp.jar
   ```

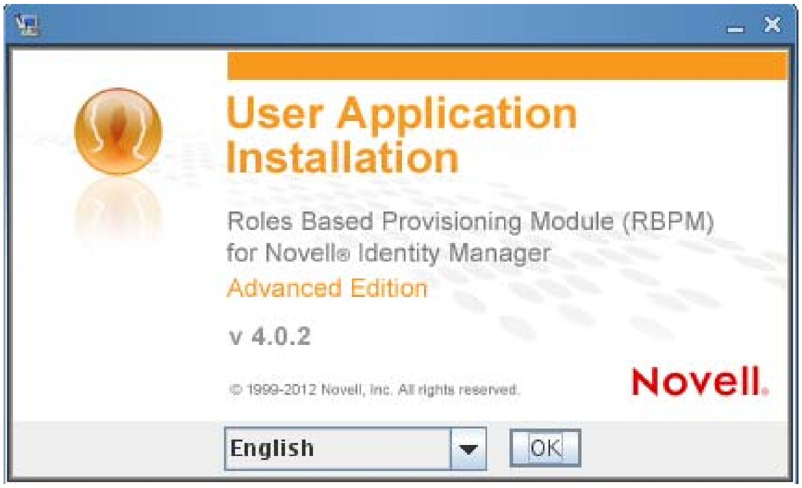
The commands shown above are examples. You may need to adjust the path to the JRE. For example, if you installed into `/opt/novell/idm` on Linux, then the command would be:

```
/opt/novell/idm/jre/bin/java -jar IdmUserApp.jar
```

If you used the JBossPostgreSQL utility provided with the Roles Based Provisioning Module to install JBoss, you can use the JRE that it provided to launch the User Application installer.

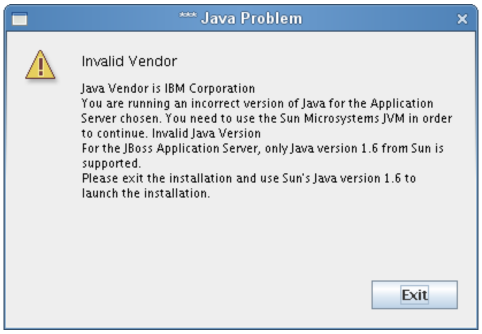
NOTE: SLES users: Do not use the IBM* JDK that comes with SLES. This version is incompatible with some aspects of the installation and can cause master key corruption errors.

When the installation program launches, you are prompted for the language:


User Application Installation
Roles Based Provisioning Module (RBPM)
for Novell® Identity Manager
Advanced Edition
v 4.0.2
© 1999-2012 Novell, Inc. All rights reserved.
Novell.
English
OK

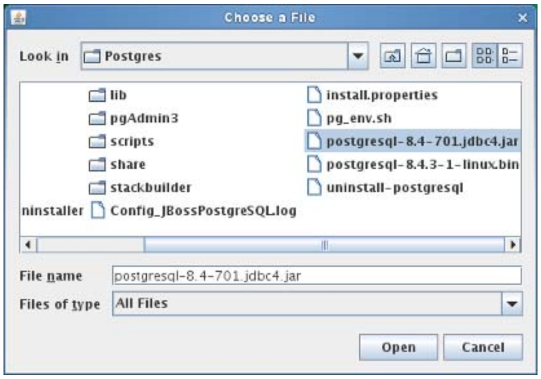
2 Use the following information to choose the language, confirm the license agreement, and select the Application Server platform:

Installation Screen	Description
User Application Installation	Select the language for the Installation program. The default is English.
License Agreement	Read the License Agreement, then select *I accept the terms of the License Agreement*.

Installation Screen	Description
Application Server Platform	Select *JBoss*. When you’re installing on JBoss, you need to launch the installation program by using Sun’s Java environment. If you select JBoss as the application server, and do not use Sun’s Java to launch the installation, you will see a pop-up error message, and the installation will terminate:  Invalid Vendor Java Vendor is IBM Corporation You are running an incorrect version of Java for the Application Server chosen. You need to use the Sun Microsystems JVM in order to continue. Invalid Java Version For the JBoss Application Server, only Java version 1.6 from Sun is supported. Please exit the installation and use Sun's Java version 1.6 to launch the installation.

3 Use the following information to choose an install folder and configure the database:

Installation Screen	Description
Choose Install Folder	Specify where you want the installer to put the files.
Database Platform	Select the database platform. The database and JDBC driver must already be installed. For JBoss, the options include the following: ◆ MySQL ◆ Microsoft SQL Server ◆ Oracle ◆ PostgreSQL
Database Host and Port	*Host*: Specify the database server’s hostname or IP address. For a cluster, specify the same hostname or IP address for each member of the cluster. *Port*: Specify the database’s listener port number. For a cluster, specify the same port for each member of the cluster.

Installation Screen	Description
Database Username and Password	*Database Name* (or SID): For PostgreSQL, MySQL, or MS SQL Server, provide the name of your 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. The default database name is `idmuserappdb`. *Database Username*: Specify the database user. For a cluster, specify the same database user for each member of the cluster. *Database Password*: Specify the database password. For a cluster, specify the same database password for each member of the cluster. *Database Driver JAR file*: Provide the Thin Client JAR for the Database Server. This is required. You need to specify a driver JAR file that has been provided by the database vendor for the particular database you are using. Driver JAR files provided by third-party vendors are not supported. For PostgreSQL, choose the postgresql-8.4-701.jdbc4.jar file:  Look in: Postgres File name: postgresql-8.4-701.jdbc4.jar Files of type: All Files Choose a File lib pgAdmin3 scripts share stackbuilder ninstaller Config_JBossPostgreSQL.log install.properties pg_env.sh postgresql-8.4-701.jdbc4.jar postgresql-8.4.3-1-linux.bin uninstall-postgresql Open Cancel
Database Administrator	This screen is pre-populated with the same username and password from the Database Username and Password page. If the database user that was specified earlier does not have enough permissions to create tables in the Database Server, then a different user ID that has the necessary rights needs to be entered.
Create Database Tables	Specify when the database tables should be created. The Create Database Tables screen gives you the option to create tables at installation time or at application startup. Alternatively, you can create a schema file at installation time, which the Database Administrator would use to create the tables later. If you want to generate a schema file, select *Write SQL to File* and provide a name for the file in the *Schema Output File* field.
New Database or Existing Database	If the database that will be used is new or empty, then select the *New Database* button. If the database is an existing one from a previous installation, select the *Existing Database* button.

Installation Screen	Description
Test Database Connection	To confirm that the information provided in the previous screens was correct, you can test the database connection by selecting *Test Database Connection*. The installer needs to connect to the database both for creating tables directly and for creating the .SQL file. If you test the database connection and it fails, you may still continue with installation. In this case, you will need to create the tables after installation, as described in the *User Application: Administration Guide* (http://www.netiq.com/documentation/idm402/agpro/?page=/documentation/idm402/agpro/data/bncf7rj.html).

4 Use the following information to configure Java, the JBoss installation, and Identity Manager, as well as audit settings and security.

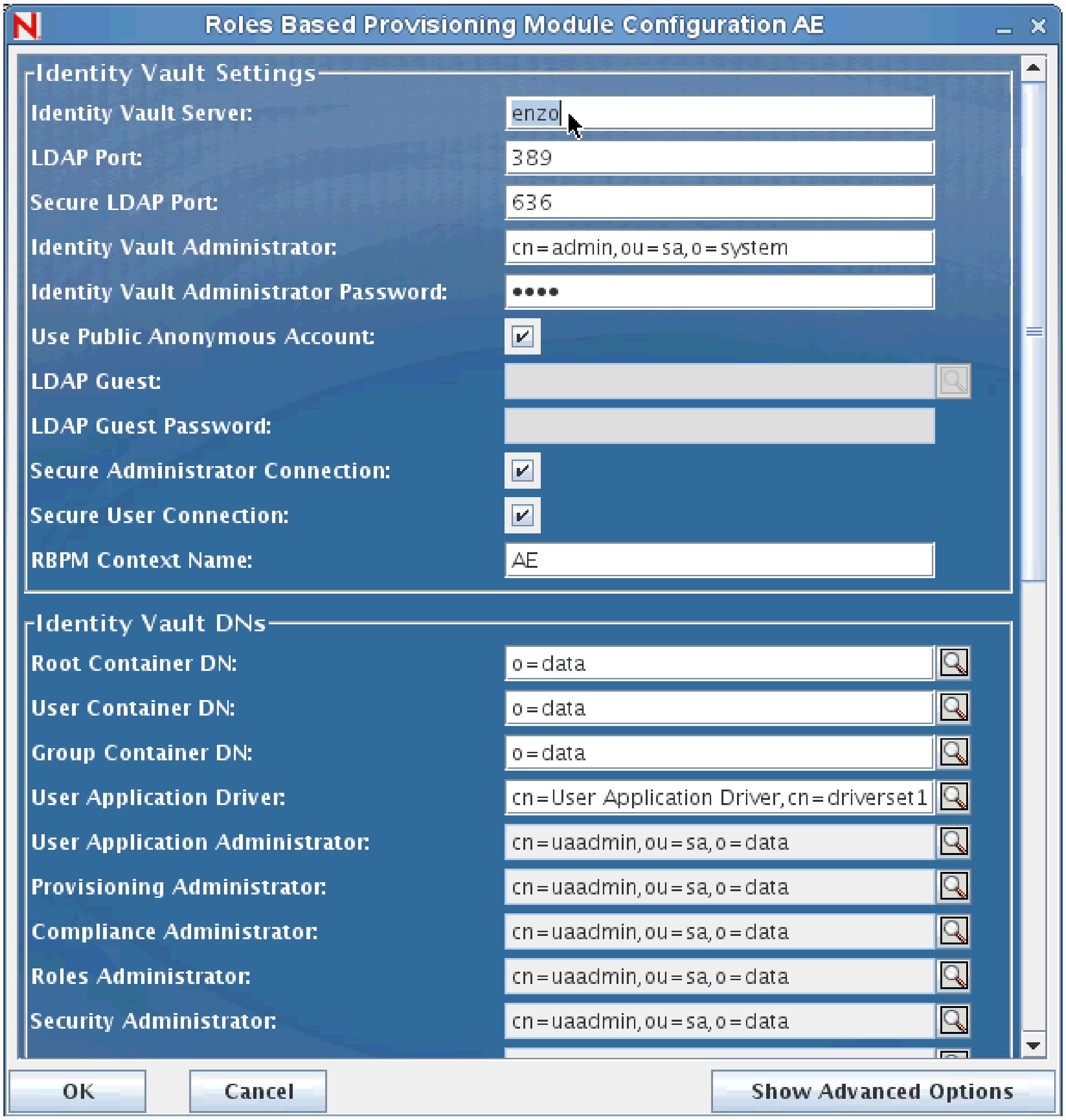
Installation Screen	Description
Java Install	Specify the Java root install folder. The Java Install provides the path to Java based on your JAVA_HOME environment variable and gives you the option to correct it. At this point, the Installation program also validates that the Java selected is the correct one for the Application Server selected. In addition, it validates that it can write to the cacerts in the JRE that was specified. You are then prompted for information about where your JBoss application server is installed.
JBoss Configuration	Tells 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 “Installing the JBoss Application Server and the PostgreSQL Database” on page 17. *JBoss Parent Folder*: Specify the location of the JBoss application server.
IDM Configuration	Select the type of application server configuration: ◆ Select *default* if this installation is on a single node that is not part of a cluster If you select *default* and decide you need a cluster later, then you must reinstall the User Application. ◆ Select *all* if this installation is part of a cluster *Application Context*: The name of the application server configuration, the name of the application WAR file, and the name of the URL context. The installation script creates a server configuration and by default names the configuration based on *Application name*. Make a note of the application name and include it in the URL when you start the User Application from a browser. *Workflow Engine ID*: Each server in a cluster must have a unique Workflow Engine ID. The Workflow Engine ID is only valid for cluster installs, and only if you are installing the provisioning WAR. The engine ID cannot exceed 32 characters. Workflow Engine IDs are described in the *User Application: Administration Guide* in the section on configuring workflows for clustering.

Installation Screen	Description
Select Audit Logging Type	To enable logging, click *Yes*. To disable logging, click *No*. The next panel prompts you to specify the type of logging. Choose from the following options: ◆ *Novell Identity Audit or Novell Sentinel*: Enables logging through a Novell client for the User Application. ◆ *OpenXDAS*: Events are logged to your OpenXDAS logging server. For more information on setting up logging, see the *User Application: Administration Guide*.
Novell Identity Audit or Novell Sentinel	*Server*: If you enable logging, specify the hostname or IP address for the server. If you turn logging off, this value is ignored. *Log Cache Folder*: Specify the directory for the logging cache.
Security - Master Key	*Yes*: Allows you to Import an existing master key. If you choose to import an existing encrypted master key, cut and paste the key into the install procedure window. *No*: Creates a new master key. After you finish the installation, you must manually record the master key as described in Section 9.1, "Recording the Master Key," on page 115. The installation procedure writes the encrypted master key to the `master-key.txt` file in the installation directory. **NOTE:** If you install the User Application from the console, the installation program does not automatically create the `master-key.txt` file. Instead, you must manually copy the master key from the `/opt/novell/idm/jboss/server/IDMProv/conf/sys-configuration-xmldata.xml` file. 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.

5 If you would like to configure RBPM now, select *Configure Now* and click *Next*.

(If you are not prompted for this information, you might not have completed the steps outlined in Section 2.5, "Installing the Java Development Kit," on page 27.)

The default view of the Roles Based Provisioning Module Configuration panel shows these fields:



Roles Based Provisioning Module Configuration AE

Identity Vault Settings

Identity Vault Server: enzo

LDAP Port: 389

Secure LDAP Port: 636

Identity Vault Administrator: cn=admin,ou=sa,o=system

Identity Vault Administrator Password: ••••

Use Public Anonymous Account: ☑

LDAP Guest:

LDAP Guest Password:

Secure Administrator Connection: ☑

Secure User Connection: ☑

RBPM Context Name: AE

Identity Vault DNs

Root Container DN: o=data

User Container DN: o=data

Group Container DN: o=data

User Application Driver: cn=User Application Driver,cn=driverset1

User Application Administrator: cn=uaadmin,ou=sa,o=data

Provisioning Administrator: cn=uaadmin,ou=sa,o=data

Compliance Administrator: cn=uaadmin,ou=sa,o=data

Roles Administrator: cn=uaadmin,ou=sa,o=data

Security Administrator: cn=uaadmin,ou=sa,o=data

The Installation program will take the value from the Root Container DN and apply it to the following values:

- User Container DN
- Group Container DN

The Installation program will take the value from the User Application Administrator fields and apply it to the following values:

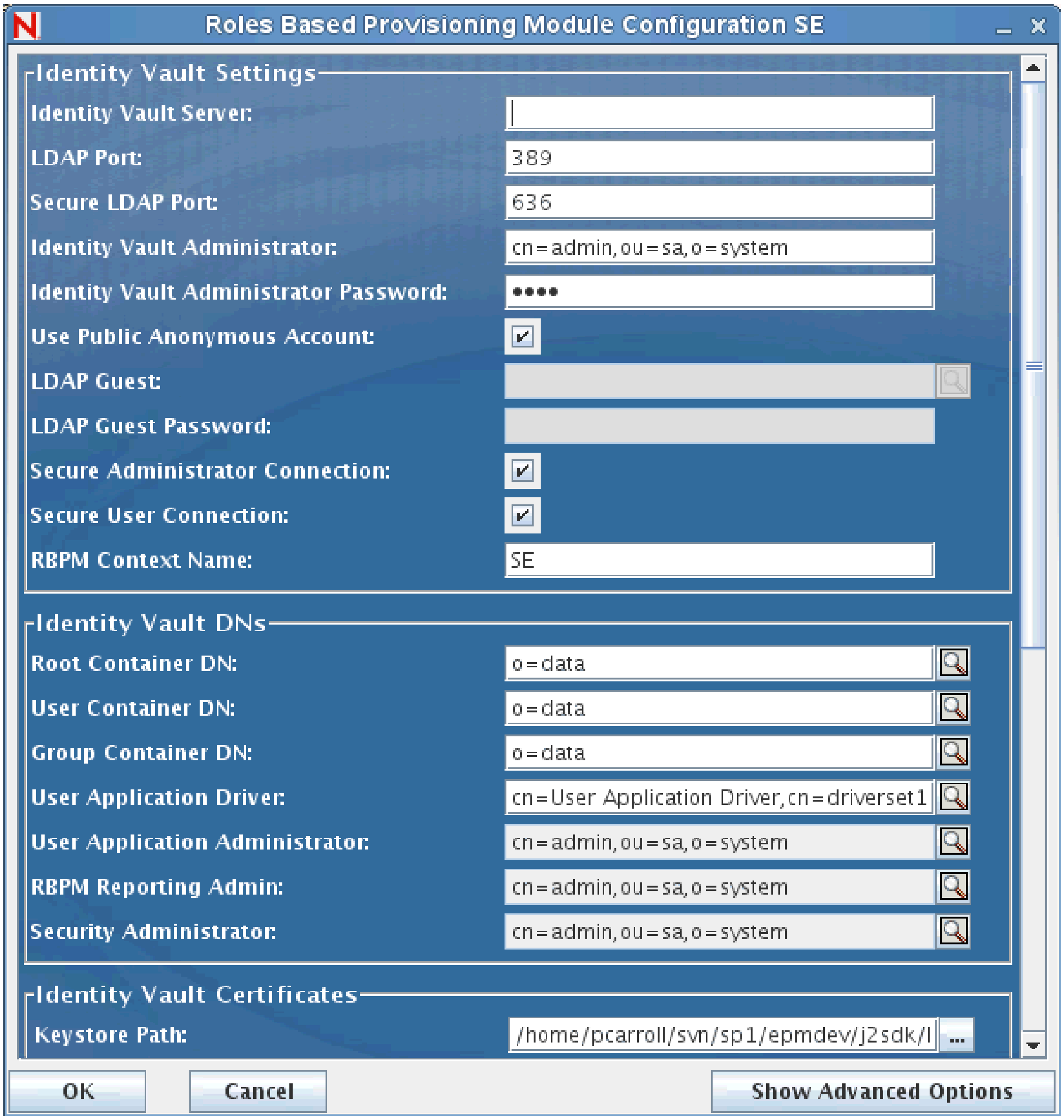
- Provisioning Administrator
- Compliance Administrator
- Roles Administrator
- Security Administrator
- Resources Administrator
- RBPM Configuration Administrator

If you want to be able to specify these values explicitly, you can click the *Show Advanced Options* button and change them.

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.

See Appendix A, "User Application Configuration Reference," on page 123 for a description of each option.

The default view for Standard Edition shows a subset of the security fields, as shown below:



Roles Based Provisioning Module Configuration SE

Identity Vault Settings

Identity Vault Server:	
LDAP Port:	389
Secure LDAP Port:	636
Identity Vault Administrator:	cn=admin,ou=sa,o=system
Identity Vault Administrator Password:	••••
Use Public Anonymous Account:	☑
LDAP Guest:	
LDAP Guest Password:	
Secure Administrator Connection:	☑
Secure User Connection:	☑
RBPM Context Name:	SE

Identity Vault DNs

Root Container DN:	o=data
User Container DN:	o=data
Group Container DN:	o=data
User Application Driver:	cn=User Application Driver,cn=driverset1
User Application Administrator:	cn=admin,ou=sa,o=system
RBPM Reporting Admin:	cn=admin,ou=sa,o=system
Security Administrator:	cn=admin,ou=sa,o=system

Identity Vault Certificates

Keystore Path:	/home/pcarroll/svn/sp1/epmdev/j2sdk/l

In Identity Manager 4.0.2 Standard Edition, only the following administrators need to be assigned:

- User Application Administrator
- RBPM Reporting Administrator
- Security Administrator

NOTE: For testing purposes, Novell does not lock down the security model in Standard Edition. Therefore, the Security Administrator is able to assign all domain administrators, delegated administrators, and also other Security Administrators. However, the use of these advanced features is not supported in production. In production environments, all administrator assignments are restricted by licensing. Novell collects monitoring data in the audit database to ensure that production environments comply. Furthermore, Novell recommends that only one user be given the permissions of the Security Administrator.

6 Use the following information to complete the installation.

Installation Screen	Description
Pre-Installation Summary	Read the Pre-Installation Summary page to verify your choices for the installation parameters. If necessary, use *Back* to return to earlier installation pages to change installation parameters. The User Application configuration page does not save values, so after you re-specify earlier pages in the installation, you must re-enter the User Application configuration values. When you are satisfied with your installation and configuration parameters, return to the Pre-Install Summary page and click *Install*.
Install Complete	Indicates that the installation is finished.

Installer creates the novlua user The installer creates a new user with the name novlua. The jboss_init script runs JBoss as this user and the permissions defined in the JBoss files are set to this user.

5.1.1 Viewing Installation and Log Files

If your installation completed without error, continue with Testing the Installation. If the installation issued errors or warnings, review the log files to determine the problems:

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

5.2 Deploying RBPM on JBoss EAP

To deploy the Roles Based Provisioning Module on JBoss 5.1.2 Enterprise Application Platform (EAP), you need to perform several manual setup steps. The setup process is outlined below:

1. Install JBoss 5.1.2 EAP.
2. Copy the `jbosssx.jar` file from the `%jboss-root%/lib` directory to the `%jboss-root%/common/lib` directory before launching the RBPM User Application installer.
3. Install the RBPM User Application.
4. Replace the `messaging-jboss-beans.xml` file you have with a modified XML file.

   If you deploy RBPM on JBoss 5.1.2 EAP without replacing the `messaging-jboss-beans.xml` file, you might see multiple warrnings and errors in the startup log.

The problem is that the RBPM installer uses the community version of the `messaging-jboss-beans.xml` file as a template to generate its own version of the file. Unfortunately, the EAP version is very different in many aspects, including the definitions of QueueMODefinition and TopicMODefinition.

The workaround for this issue is to replace the the `messaging-jboss-beans.xml` file you have with the modified XML file shown below. The file needs to be in the `IDMProv/deploy/messaging` folder.

```
<?xml version="1.0" encoding="UTF-8"?>

<!--
 =========================================================================

 Copyright (c) 2009 Novell, Inc. All Rights Reserved.

 THIS WORK IS SUBJECT TO U.S. AND INTERNATIONAL COPYRIGHT LAWS AND TREATIES
 NO PART OF THIS WORK MAY BE USED, PRACTICED, PERFORMED COPIED, DISTRIBUTED,
 REVISED, MODIFIED, TRANSLATED, ABRIDGED, CONDENSED, EXPANDED, COLLECTED,
 COMPILED, LINKED, RECAST, TRANSFORMED OR ADAPTED WITHOUT THE PRIOR WRITTEN
 CONSENT OF NOVELL, INC. ANY USE OR EXPLOITATION OF THIS WORK WITHOUT
 AUTHORIZATION COULD SUBJECT THE PERPETRATOR TO CRIMINAL AND CIVIL
 LIABILITY.

 =========================================================================
-->

<!--
    Messaging beans
    $Id: messaging-jboss-beans.xml 88672 2009-05-11 20:49:47Z
anil.saldhana@jboss.com $
-->
<deployment xmlns="urn:jboss:bean-deployer:2.0">

   <!-- messaging application-policy definition -->
   <application-policy xmlns="urn:jboss:security-beans:1.0" name="messaging">
      <authentication>
         <login-module
code="org.jboss.security.auth.spi.DatabaseServerLoginModule" flag="required">
            <module-option name="unauthenticatedIdentity">guest</module-option>
            <module-option name="dsJndiName">java:/IDMUADataSource</module-
option>
            <module-option name="principalsQuery">SELECT PASSWD FROM JBM_USER
WHERE USER_ID=?</module-option>
            <module-option name="rolesQuery">SELECT ROLE_ID, 'Roles' FROM
JBM_ROLE WHERE USER_ID=?</module-option>
         </login-module>
      </authentication>
   </application-policy>

   <bean name="SecurityStore"
class="org.jboss.jms.server.jbosssx.JBossASSecurityMetadataStore">
      <!-- default security configuration -->
      <property name="defaultSecurityConfig">
         <![CDATA[
            <security>
               <role name="guest" read="true" write="true" create="true"/>
            </security>
         ]]>
      </property>
      <property name="suckerPassword">changeit</property>
      <property name="securityDomain">messaging</property>
      <property name="securityManagement"><inject
bean="JNDIBasedSecurityManagement"/></property>
      <!-- @JMX annotation to export the management view of this bean -->

<annotation>@org.jboss.aop.microcontainer.aspects.jmx.JMX(name="jboss.messagin
g:service=SecurityStore",exposedInterface=org.jboss.jms.server.jbosssx.JBossAS
SecurityMetadataStoreMBean.class)</annotation>
      <!-- Password Annotation to inject the password from the common password
utility

<annotation>@org.jboss.security.integration.password.Password(securityDomain="
messaging",methodName="setSuckerPassword")</annotation>
       -->
   </bean>

   <bean name="MessagingDeploymentTemplateInfoFactory"
     class="org.jboss.managed.plugins.factory.DeploymentTemplateInfoFactory"/>

   <bean name="QueueTemplate"
class="org.jboss.profileservice.management.templates.JmsDestinationTemplate">
      <property name="info"><inject bean="QueueTemplateInfo"/></property>
   </bean>
   <bean name="QueueTemplateInfo"

class="org.jboss.profileservice.management.templates.JmsDestinationTemplateInf
o">
      <constructor factoryMethod="createTemplateInfo">
         <factory bean="DSDeploymentTemplateInfoFactory"/>
         <parameter
class="java.lang.Class">org.jboss.profileservice.management.templates.JmsDesti
nationTemplateInfo</parameter>
         <parameter
class="java.lang.Class">org.jboss.jms.server.destination.QueueServiceMO</
parameter>
         <parameter class="java.lang.String">QueueTemplate</parameter>
         <parameter class="java.lang.String">A template for JMS queue *-
service.xml deployments</parameter>
      </constructor>
      <property name="destinationType">QueueTemplate</property>
   </bean>

   <bean name="TopicTemplate"
class="org.jboss.profileservice.management.templates.JmsDestinationTemplate">
      <property name="info"><inject bean="TopicTemplateInfo"/></property>
   </bean>
   <bean name="TopicTemplateInfo"

class="org.jboss.profileservice.management.templates.JmsDestinationTemplateInf
o">
      <constructor factoryMethod="createTemplateInfo">
         <factory bean="DSDeploymentTemplateInfoFactory"/>
         <parameter
class="java.lang.Class">org.jboss.profileservice.management.templates.JmsDesti
nationTemplateInfo</parameter>
         <parameter
class="java.lang.Class">org.jboss.jms.server.destination.TopicServiceMO</
parameter>
         <parameter class="java.lang.String">TopicTemplate</parameter>
         <parameter class="java.lang.String">A template for JMS topic *-
service.xml deployments</parameter>
      </constructor>
      <property name="destinationType">TopicTemplate</property>
   </bean>

</deployment>
```

5 Replace the `postgresql-persistence-service.xml` file with the `%jboss-root%/docs/examples/jms/postgresql-persistence-service.xml` file and copy it to `%jboss-root%/server/IDMProv/deploy/messaging/`.

NOTE: Step 5 through Step 8 refer specifically to the PostgreSQL database. If you use a different database in your environment, find and modify the persistence service configuration file for your particular database.

6 Edit the `postgresql-persistence-service.xml` file and replace the text `DefaultDS` with the text `IDMUADataSource`.

7 In the `postgresql-persistence-service.xml` file, also comment out the following lines within the `Clustered` attribute:

```
<attribute name="Clustered">false</attribute>

      <!-- All the remaining properties only have to be specified if the post
office is clustered.
           You can safely comment them out if your post office is non clustered
-->

      <!-- The JGroups group name that the post office will use -->

      <!--attribute
name="GroupName">${jboss.messaging.groupname:MessagingPostOffice}</attribute>-
->

      <!-- Max time to wait for state to arrive when the post office joins the
cluster -->

      <!--attribute name="StateTimeout">30000</attribute>-->

      <!-- Max time to wait for a synchronous call to node members using the
MessageDispatcher -->

      <!--attribute name="CastTimeout">30000</attribute>-->

      <!-- Set this to true if you want failover of connections to occur when a
node is shut down -->

      <!--<attribute name="FailoverOnNodeLeave">false</attribute>

      <depends
optional-attribute-
name="ChannelFactoryName">jboss.jgroups:service=ChannelFactory</depends>
      <attribute name="ControlChannelName">jbm-control</attribute>
      <attribute name="DataChannelName">jbm-data</attribute>
      <attribute
name="ChannelPartitionName">${jboss.partition.name:DefaultPartition}-JMS</
attribute>-->
   </mbean>
```

8 Also, in `postgresql-persistence-service.xml`:

8a Find this line:

```
POPULATE.TABLES.3  = INSERT INTO JBM_USER (USER_ID, PASSWD, CLIENTID)
VALUES ('john', 'needle', 'DurableSubscriberExample')
```

Replace it with this line:

```
POPULATE.TABLES.3  = INSERT INTO JBM_USER (USER_ID, PASSWD,
CLIENTID) VALUES ('p_user', 'changeit', 'IDMNotificationDurableTopic')
```

8b Find this line:

```
POPULATE.TABLES.8  = INSERT INTO JBM_ROLE (ROLE_ID, USER_ID) VALUES
('john','guest')
```

Replace it with this line:

```
POPULATE.TABLES.8  = INSERT INTO JBM_ROLE (ROLE_ID, USER_ID)
VALUES ('p_user','guest')
```

8c Find this line:

```
POPULATE.TABLES.9  = INSERT INTO JBM_ROLE (ROLE_ID, USER_ID) VALUES
('subscriber','john')
```

Replace it with this line:

```
POPULATE.TABLES.9  = INSERT INTO JBM_ROLE (ROLE_ID, USER_ID)
VALUES ('subscriber','p_user')
```

8d Find this line:

```
POPULATE.TABLES.10 = INSERT INTO JBM_ROLE (ROLE_ID, USER_ID) VALUES
('publisher','john')
```

Replace it with this line:

```
POPULATE.TABLES.12 = INSERT INTO JBM_ROLE (ROLE_ID, USER_ID)
VALUES ('durpublisher','p_user')
```

9 Start JBoss.

If you are configured correctly, you will see this information in the server log:

```
INFO  [ServerPeer] JBoss Messaging 1.4.7.GA server [0] started
{About 7 lines down}
INFO  [TopicService] Topic[/topic/IDMNotificationDurableTopic] started,
fullSize=200000, pageSize=2000, downCacheSize=2000
```

In addition, you will see this information further down in the log:

```
INFO  [RBPM] [com.novell.soa.notification.impl.jms.JMSConnectionMediator:init]
Starting JMS notification system
INFO  [STDOUT] INFO  [RBPM]
[com.novell.soa.notification.impl.NotificationThread:run] Starting
asynchronous
notification system
```

In addition, the `stop-jboss.sh` script that is created during the installation process needs to be modified. The JBoss administrator's user ID and password must be appended to the end of the shutdown command:

```
shutdown.sh -s jnp://localhost:1199 -u %value% -p %value%
```

For example:

```
shutdown.sh -s jnp://localhost:1199 -u admin -p novell
```

5.3 Testing the Installation

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):

`/etc/init.d/jboss_init start` (Linux and Solaris)

`start-jboss.bat` (Windows)

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 -Dfile.encoding=UTF-8 -
Dsun.jnu.encoding=UTF-8 -server -Xms1024m -Xmx1024m -XX:MaxPermSize=512m
```

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 Start the Role and Resource Service driver, following the steps shown above for the User Application driver.

5 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, 8180 by default on JBoss). *ApplicationName* is *IDMProv* 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 appears.

6 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 9.9, “Troubleshooting,” on page 120.

6 Installing the User Application on WebSphere

This section describes how to install the User Application for the Roles Based Provisioning Module on a WebSphere Application Server with the graphical user interface version of the installer.

Run the installer as root You need to run the installer as the root user.

Data Migration For information on migrating, see the *RBPM and Reporting Migration Guide* (http://www.netiq.com/documentation/idm402/index.html).

6.1 Installing and Configuring the User Application WAR

NOTE: For WebSphere 7.0, the installation program requires the 1.6 JDK from IBM. If you use a different version, the installation procedure does not successfully configure the User Application WAR file. The installation appears to succeed, but you encounter errors when trying to start the User Application.

1. Navigate to the directory containing your installation files.
2. You must apply the unrestricted policy files to the IBM JDK. You can refer to your WebSphere documentation for a link to these files from IBM and instructions for applying them. Apply these files to your IBM JDK environment before proceeding any further with the installation. The JAR file for unrestricted policy files need to be placed in JAVA_HOME\jre\lib\security.

   Without these unrestricted policy files, an error will occur that says "Illegal key size". The root cause of this problem is the lack of unrestricted policy files, so be sure to use the correct IBM JDK.
3. Launch the installer using the IBM Java environment, as shown below:

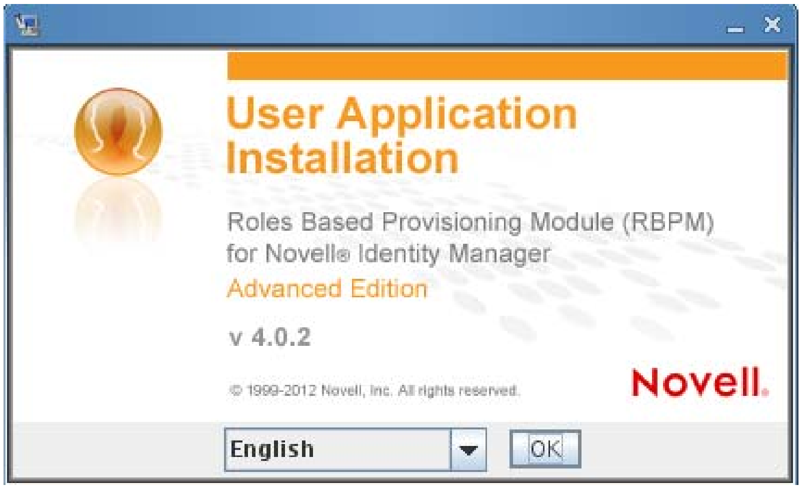
   Linux or Solaris

   ```
   $ /opt/WS/IBM/WebSphere/AppServer/java/bin/java -jar IdmUserApp.jar
   ```

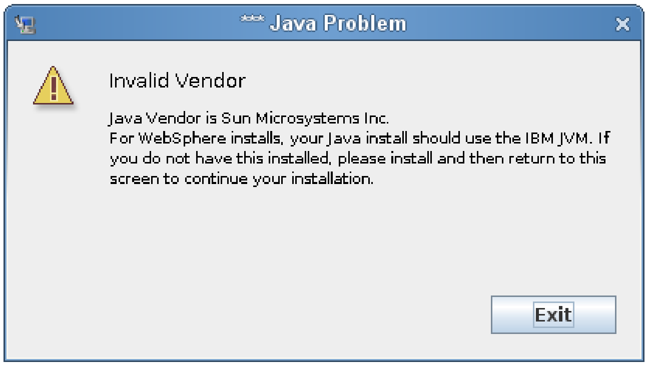
   Windows

   ```
   C:\WS\IBM\WebSphere\AppServer\java\bin\java -jar IdmUserApp.jar
   ```

   When the installation program launches, you are prompted for the language:


User Application Installation
Roles Based Provisioning Module (RBPM)
for Novell® Identity Manager
Advanced Edition
v 4.0.2
© 1999-2012 Novell, Inc. All rights reserved.
Novell.
English
OK

4 Use the following information to select the language, confirm the license agreement, and select the Application Server platform:

Installation Screen	Description
User Application Installation	Select the language for the installation program. The default is English.
License Agreement	Read the License Agreement, then select *I accept the terms of the License Agreement*.
Application Server Platform	Select *WebSphere.* If the User Application WAR file is in a different directory from the installer, the installer prompts for the path to the WAR. 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. When you're installing on WebSphere, you need to launch the installation program by using the IBM Java environment. If you select WebSphere as the application server, and do not use IBM's Java to launch the installation, you will see a pop-up error message, and the installation will terminate:  Invalid Vendor Java Vendor is Sun Microsystems Inc. For WebSphere installs, your Java install should use the IBM JVM. If you do not have this installed, please install and then return to this screen to continue your installation.

5 Use the following information to choose an install folder and configure the database:

Installation Screen	Description
Choose Install Folder	Specify where you want the installer to put the files.
Database Platform	Select the database platform. The database and JDBC driver must already be installed. For WebSphere, the options include the following: ◆ Oracle ◆ Microsoft SQL Server ◆ IBM DB2 ◆ PostgreSQL
Database Host and Port	*Host*: Specify the database server's hostname or IP address. For a cluster, specify the same hostname or IP address for each member of the cluster. *Port*: Specify the database's listener port number. For a cluster, specify the same port for each member of the cluster.

Database Username and Password	*Database Name* (or SID): For DB2, MS SQL Server, or PostgreSQL provide the name of your preconfigured database. For Oracle, provide the Oracle System Identifier (SID) that you previously created. For a cluster, specify the same database name or SID for each member of the cluster.
	Database Username: Specify the database user. For a cluster, specify the same database user for each member of the cluster.
	Database Password: Specify the database password. For a cluster, specify the same database password for each member of the cluster.
	Database Driver JAR file: Provide the Thin Client JAR for the Database Server. This is required.
	IMPORTANT: The browse button for the *Database Driver JAR File* field allows you to select only one (1) jar. For DB2, you must provide two (2) jars:
	◆ db2jcc.jar
	◆ db2jcc_license_cu.jar
	Therefore, you can select one JAR, but will have to manually enter the second one using the correct file separator for the operating system that the install program is running on. Alternatively, you can manually enter both entries.
	For example, on Windows:
	`c:\db2jars\db2jcc.jar;c:\db2jars\db2jcc_license_cu.jar`
	For example, on Solaris and Linux:
	`/home/lab/db2jars/db2jcc.jar:/home/lab/db2jcc_license_cu.jar`

Database Administrator	This screen is pre-populated with the same username and password from the Database Username and Password page. If the database user that was specified earlier does not have enough permissions to create tables in the Database Server, then a different user ID that has the necessary rights needs to be entered.

Installation Screen	Description
Create Database Tables	Specify when the database tables should be created.
New Database or Existing Database	If the database that will be used is new or empty, then select the *New Database* button. If the database is an existing one from a previous installation, select the *Existing Database* button.
Test Database Connection	To confirm that the information provided in the previous screens was correct, you can test the database connection by selecting *Test Database Connection*. The installer needs to connect to the database both for creating tables directly and for creating the .SQL file. If you test the database connection and it fails, you may still continue with installation. In this case, you will need to create the tables after installation, as described in the *User Application: Administration Guide* (http://www.netiq.com/documentation/idm402/agpro/?page=/documentation/idm402/agpro/data/bncf7rj.html).

6 Use the following information to configure Java and Identity Manager, as well as audit settings and security.

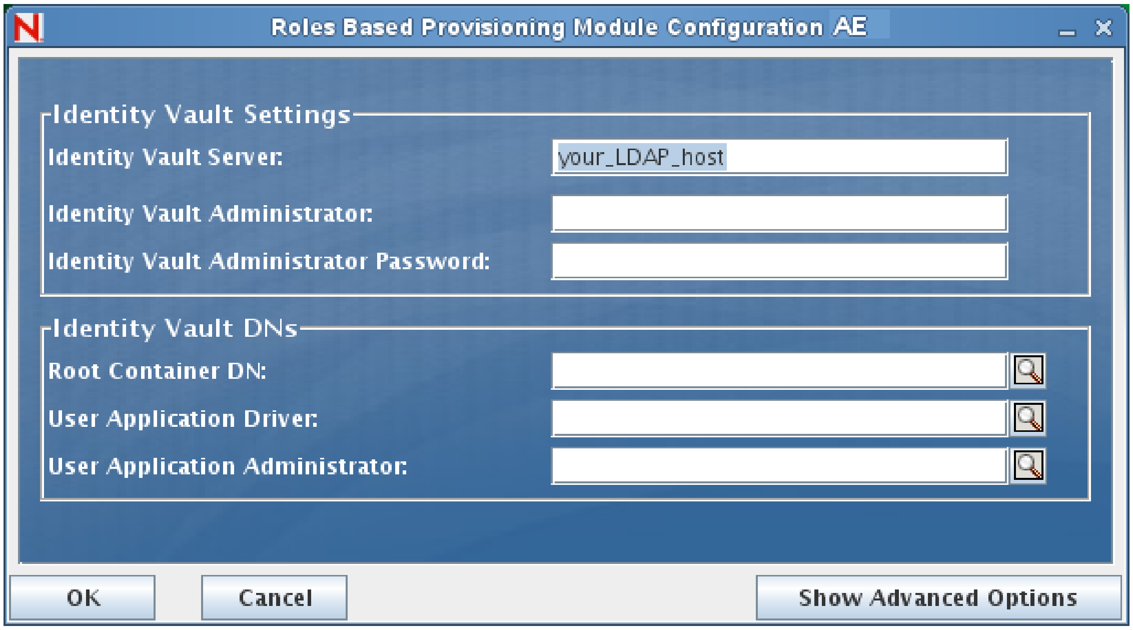
Installation Screen	Description
Java Install	Specify the Java root install folder. The Java Install provides the path to Java based on your JAVA_HOME environment variable and gives you the option to correct it. At this point, the Installation program also validates that the Java selected is the correct one for the Application Server selected. In addition, it validates that it can write to the cacerts in the JRE that was specified.
IDM Configuration	*Application Context*: The name of the application server configuration, the name of the application WAR file, and the name of the URL context. The installation script creates a server configuration and by default names the configuration based on *Application name*. Make a note of the application name and include it in the URL when you start the User Application from a browser.
Select Audit Logging Type	To enable logging, click *Yes*. To disable logging, click *No*. The next panel prompts you to specify the type of logging. Choose from the following options: ◆ *Novell Identity Audit or Novell Sentinel*: Enables logging through a N0ovell client for the User Application. ◆ *OpenXDAS*: Events are logged to your OpenXDAS logging server. For more information on setting up logging, see the *User Application: Administration Guide*.
Novell Identity Audit or Novell Sentinel	*Server*: If you enable logging, specify the hostname or IP address for the server. If you turn logging off, this value is ignored. *Log Cache Folder*: Specify the directory for the logging cache.

Installation Screen	Description
Security - Master Key	*Yes*: Allows you to Import an existing master key. If you choose to import an existing encrypted master key, cut and paste the key into the install procedure window. *No*: Creates a new master key. After you finish the installation, you must manually record the master key as described in Section 9.1, "Recording the Master Key," on page 115. The installation procedure writes the encrypted master key to the `master-key.txt` file in the installation directory. 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.

7 If you would like to configure RBPM now, select *Configure Now* and click *Next*.

(If you are not prompted for this information, you might not have completed the steps outlined in Section 2.5, "Installing the Java Development Kit," on page 27.)

The default view of the Roles Based Provisioning Module Configuration panel shows these six fields:



Roles Based Provisioning Module Configuration AE

Identity Vault Settings

Identity Vault Server: your_LDAP_host

Identity Vault Administrator:

Identity Vault Administrator Password:

Identity Vault DNs

Root Container DN:

User Application Driver:

User Application Administrator:

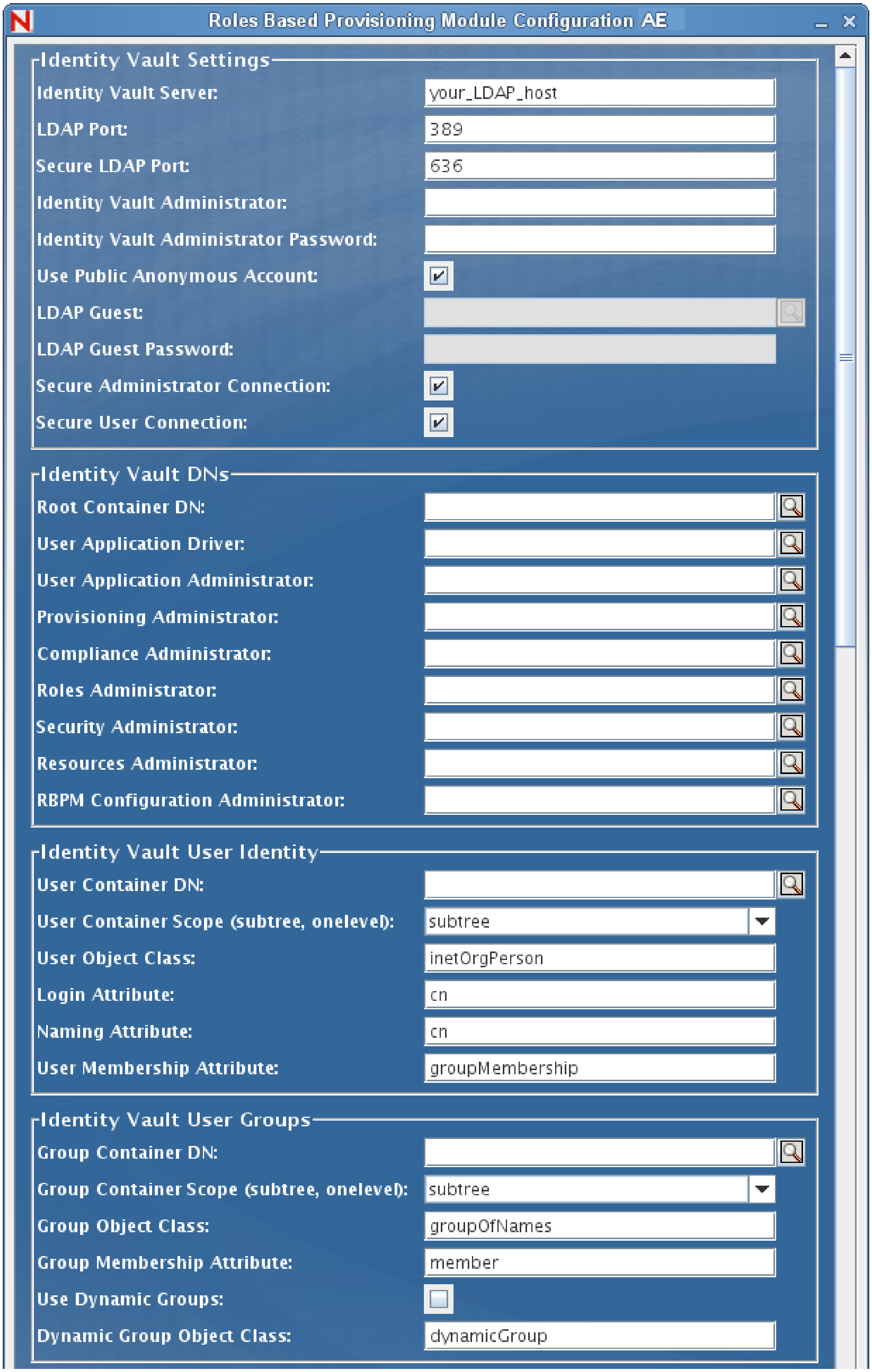
The Installation program will take the value from the Root Container DN and apply it to the following values:

- User Container DN
- Group Container DN

The Installation program will take the value from the User Application Administrator fields and apply it to the following values:

- Provisioning Administrator
- Compliance Administrator
- Roles Administrator
- Security Administrator
- Resources Administrator
- RBPM Configuration Administrator

If you want to be able to specify these values explicitly, you can click the *Show Advanced Options* button and change them:



Roles Based Provisioning Module Configuration AE

Identity Vault Settings

Identity Vault Server: your_LDAP_host

LDAP Port: 389

Secure LDAP Port: 636

Identity Vault Administrator:

Identity Vault Administrator Password:

Use Public Anonymous Account: ☑

LDAP Guest:

LDAP Guest Password:

Secure Administrator Connection: ☑

Secure User Connection: ☑

Identity Vault DNs

Root Container DN:

User Application Driver:

User Application Administrator:

Provisioning Administrator:

Compliance Administrator:

Roles Administrator:

Security Administrator:

Resources Administrator:

RBPM Configuration Administrator:

Identity Vault User Identity

User Container DN:

User Container Scope (subtree, onelevel): subtree

User Object Class: inetOrgPerson

Login Attribute: cn

Naming Attribute: cn

User Membership Attribute: groupMembership

Identity Vault User Groups

Group Container DN:

Group Container Scope (subtree, onelevel): subtree

Group Object Class: groupOfNames

Group Membership Attribute: member

Use Dynamic Groups: ☐

Dynamic Group Object Class: dynamicGroup

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.

See Appendix A, "User Application Configuration Reference," on page 123 for a description of each option.

8 Use the following information to complete the installation.

Installation Screen	Description
Pre-Installation Summary	Read the Pre-Installation Summary page to verify your choices for the installation parameters. If necessary, use *Back* to return to earlier installation pages to change installation parameters. The User Application configuration page does not save values, so after you re-specify earlier pages in the installation, you must re-enter the User Application configuration values. When you are satisfied with your installation and configuration parameters, return to the Pre-Install Summary page and click *Install*.
Install Complete	Indicates that the installation is finished.

6.1.1 Viewing Installation Log Files

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.

6.2 Configuring the WebSphere Environment

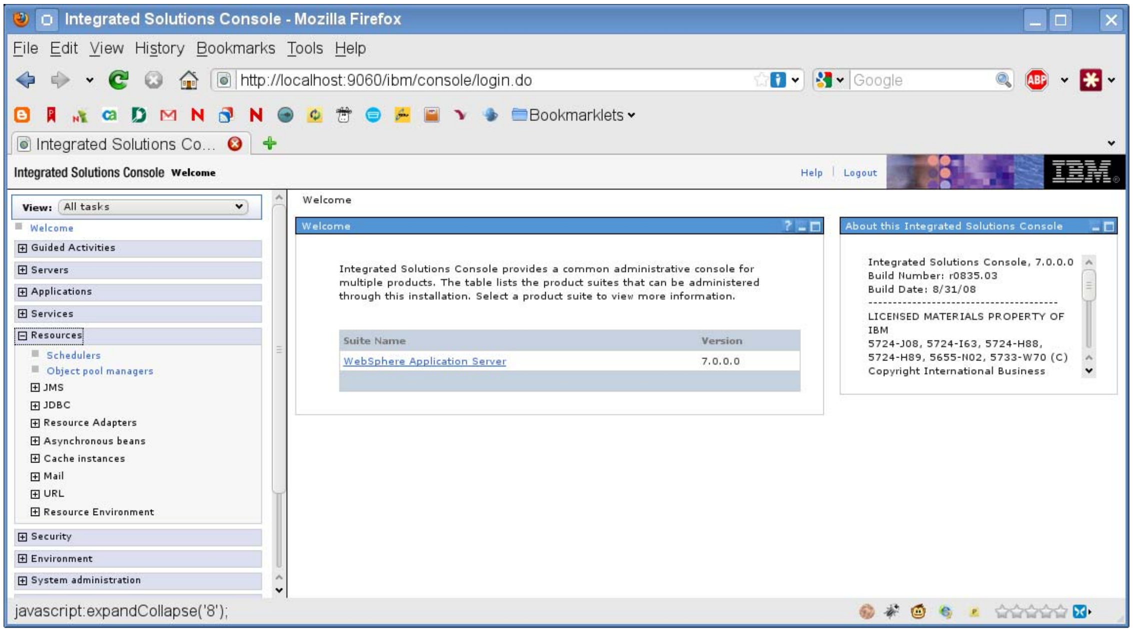
- Section 6.2.1, "Creating a Data Source," on page 74
- Section 6.2.2, "Deploying the WAR File," on page 82
- Section 6.2.3, "Adding User Application Configuration Files and JVM System Properties," on page 82
- Section 6.2.4, "Configuring the Shared Library," on page 83
- Section 6.2.5, "Applying the Shared Library to a New Class Loader," on page 86
- Section 6.2.6, "Importing the eDirectory Trusted Root to the WebSphere Keystore," on page 86
- Section 6.2.7, "Applying the Unrestricted Policy Files for the IBM JDK," on page 87
- Section 6.2.8, "Passing the preferIPv4Stack Property to the JVM," on page 87

6.2.1 Creating a Data Source

To configure a database for use with WebSphere, you need to create a JDBC Provider and a data source. This section provides instructions for creating the provider and the data source.

To create a JDBC Provider:

1 Expand *Resources* on the left side of the Integrated Solutions Console page:



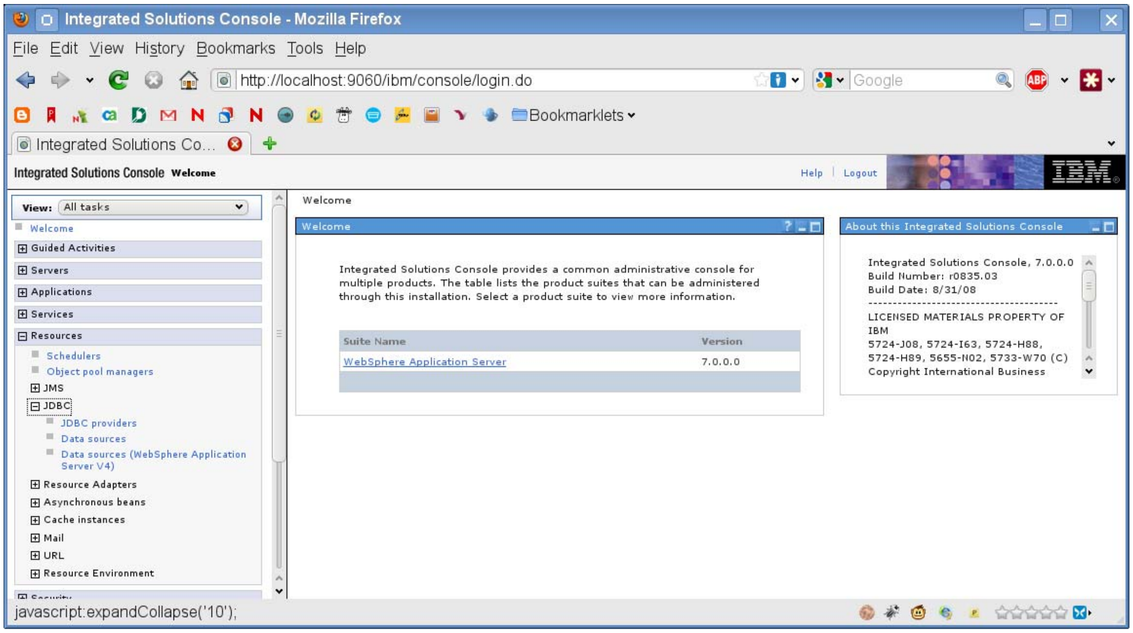
Integrated Solutions Console provides a common administrative console for multiple products. The table lists the product suites that can be administered through this installation. Select a product suite to view more information.

Suite Name	Version
WebSphere Application Server	7.0.0.0

```
Integrated Solutions Console, 7.0.0.0
Build Number: r0835.03
Build Date: 8/31/08
--------------------------------------
LICENSED MATERIALS PROPERTY OF
IBM
5724-J08, 5724-I63, 5724-H88,
5724-H89, 5655-N02, 5733-W70 (C)
Copyright International Business
```

```
javascript:expandCollapse('8');
```

2 Expand *JDBC*:


Integrated Solutions Console - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:9060/ibm/console/login.do
Google
Bookmarklets
Integrated Solutions Co...
Integrated Solutions Console Welcome
Help | Logout
View: All tasks
Welcome
Guided Activities
Servers
Applications
Services
Resources
Schedulers
Object pool managers
JMS
JDBC
JDBC providers
Data sources
Data sources (WebSphere Application Server V4)
Resource Adapters
Asynchronous beans
Cache instances
Mail
URL
Resource Environment
Welcome
Welcome
About this Integrated Solutions Console

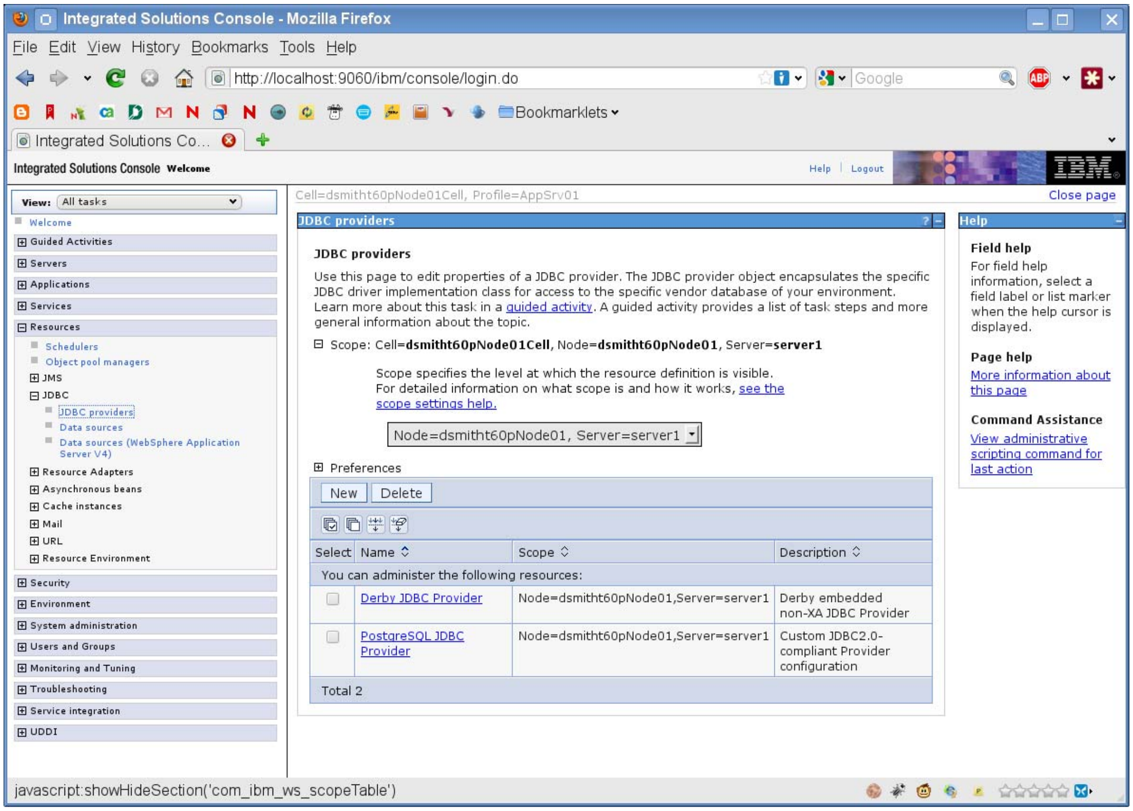
Integrated Solutions Console provides a common administrative console for multiple products. The table lists the product suites that can be administered through this installation. Select a product suite to view more information.

Suite Name	Version
WebSphere Application Server	7.0.0.0

```
Integrated Solutions Console, 7.0.0.0
Build Number: r0835.03
Build Date: 8/31/08
--------------------------------------
LICENSED MATERIALS PROPERTY OF
IBM
5724-J08, 5724-I63, 5724-H88,
5724-H89, 5655-N02, 5733-W70 (C)
Copyright International Business
```

```
javascript:expandCollapse('10');
```

3 Click *JDBC providers*:



Cell=dsmitht60pNode01Cell, Profile=AppSrv01

JDBC providers

JDBC providers

Use this page to edit properties of a JDBC provider. The JDBC provider object encapsulates the specific JDBC driver implementation class for access to the specific vendor database of your environment. Learn more about this task in a guided activity. A guided activity provides a list of task steps and more general information about the topic.

⊟ Scope: Cell=**dsmitht60pNode01Cell**, Node=**dsmitht60pNode01**, Server=**server1**

Scope specifies the level at which the resource definition is visible. For detailed information on what scope is and how it works, see the scope settings help.

Node=dsmitht60pNode01, Server=server1

⊞ Preferences

Select	Name	Scope	Description
You can administer the following resources:			
□	Derby JDBC Provider	Node=dsmitht60pNode01,Server=server1	Derby embedded non-XA JDBC Provider
□	PostgreSQL JDBC Provider	Node=dsmitht60pNode01,Server=server1	Custom JDBC2.0-compliant Provider configuration
Total 2			

Help

Field help

For field help information, select a field label or list marker when the help cursor is displayed.

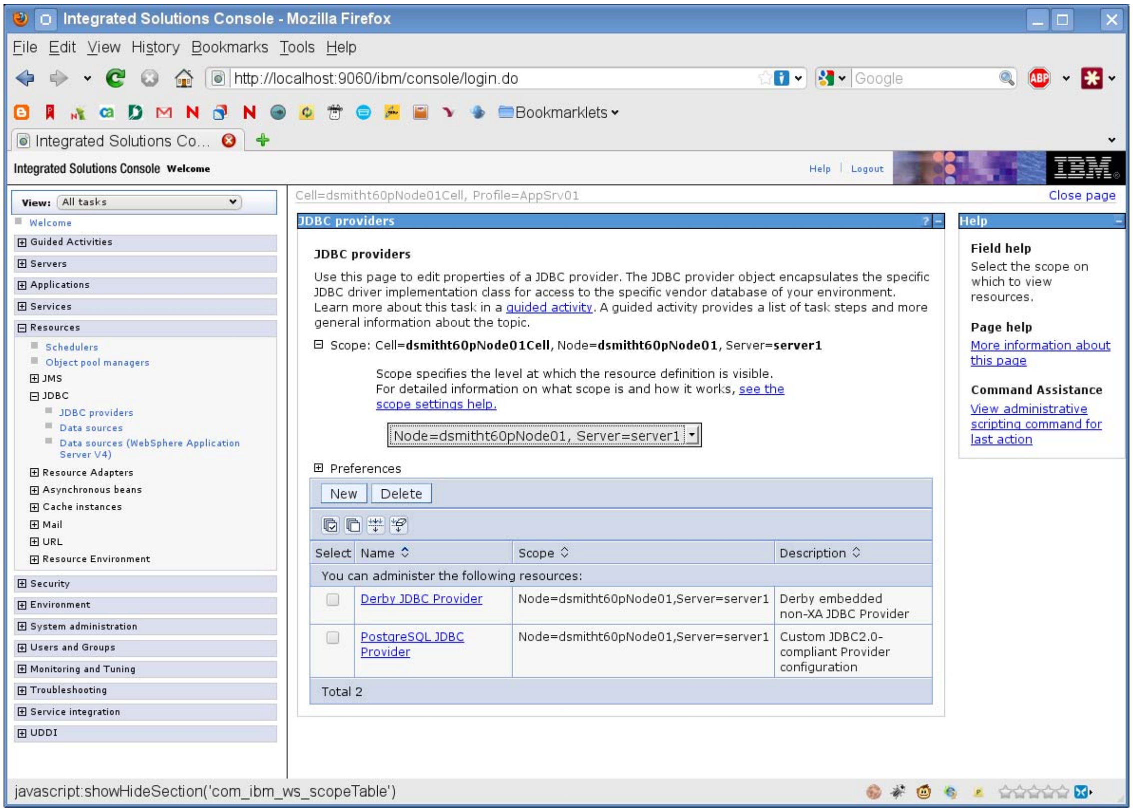
Page help

More information about this page

Command Assistance

View administrative scripting command for last action

4 Expand *Scope*:



Cell=dsmitht60pNode01Cell, Profile=AppSrv01

JDBC providers

JDBC providers

Use this page to edit properties of a JDBC provider. The JDBC provider object encapsulates the specific JDBC driver implementation class for access to the specific vendor database of your environment. Learn more about this task in a guided activity. A guided activity provides a list of task steps and more general information about the topic.

⊟ Scope: Cell=**dsmitht60pNode01Cell**, Node=**dsmitht60pNode01**, Server=**server1**

Scope specifies the level at which the resource definition is visible. For detailed information on what scope is and how it works, see the scope settings help.

Node=dsmitht60pNode01, Server=server1

⊞ Preferences

Select	Name	Scope	Description
You can administer the following resources:			
□	Derby JDBC Provider	Node=dsmitht60pNode01,Server=server1	Derby embedded non-XA JDBC Provider
□	PostgreSQL JDBC Provider	Node=dsmitht60pNode01,Server=server1	Custom JDBC2.0-compliant Provider configuration
Total 2			

Help

Field help

Select the scope on which to view resources.

Page help

More information about this page

Command Assistance

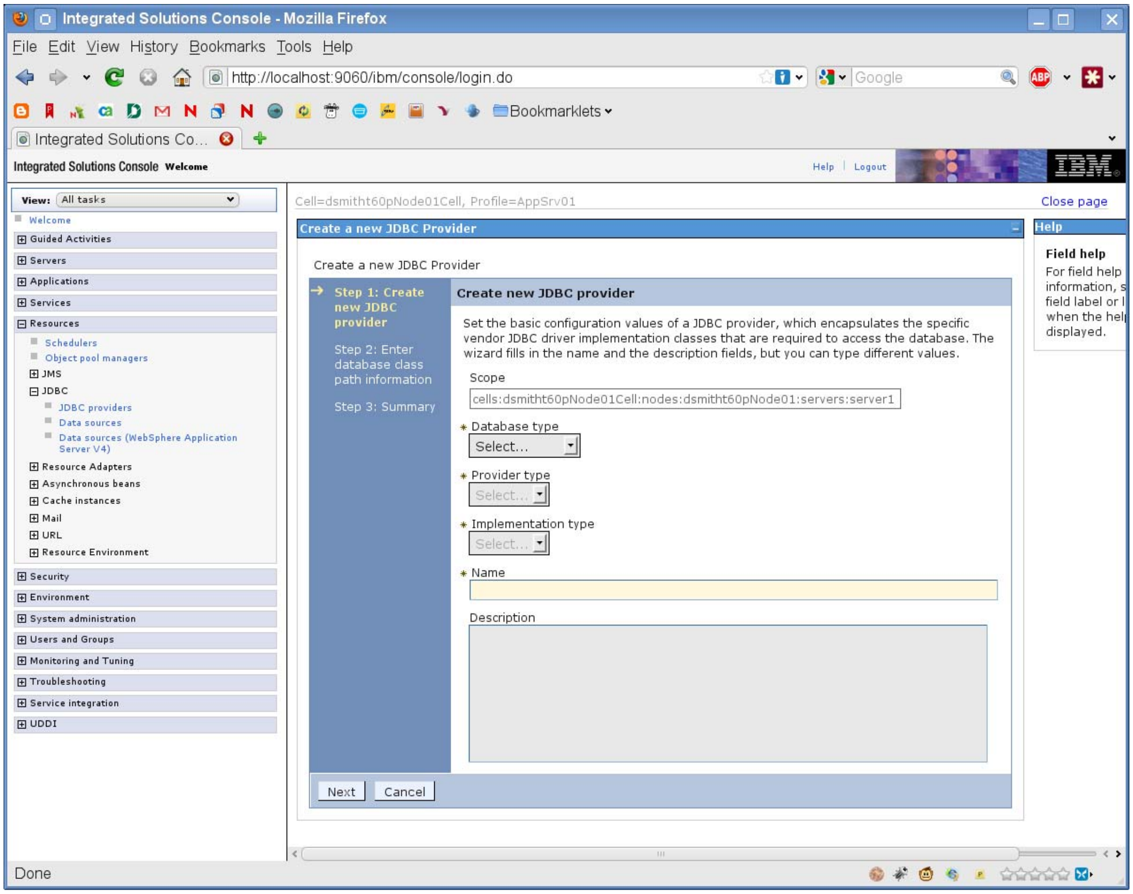
View administrative scripting command for last action

5 Select *Node=yourservername, Server=server1*.

6 Click the *New* button.

7 Select the *Database Type* (for example, DB2).

8 Click *Next*.



Cell=dsmitht60pNode01Cell, Profile=AppSrv01

Create a new JDBC Provider

Create a new JDBC Provider

→ Step 1: Create new JDBC provider

Step 2: Enter database class path information

Step 3: Summary

Create new JDBC provider

Set the basic configuration values of a JDBC provider, which encapsulates the specific vendor JDBC driver implementation classes that are required to access the database. The wizard fills in the name and the description fields, but you can type different values.

Scope

cells:dsmitht60pNode01Cell:nodes:dsmitht60pNode01:servers:server1

* Database type

Select...

* Provider type

Select...

* Implementation type

Select...

* Name

Description

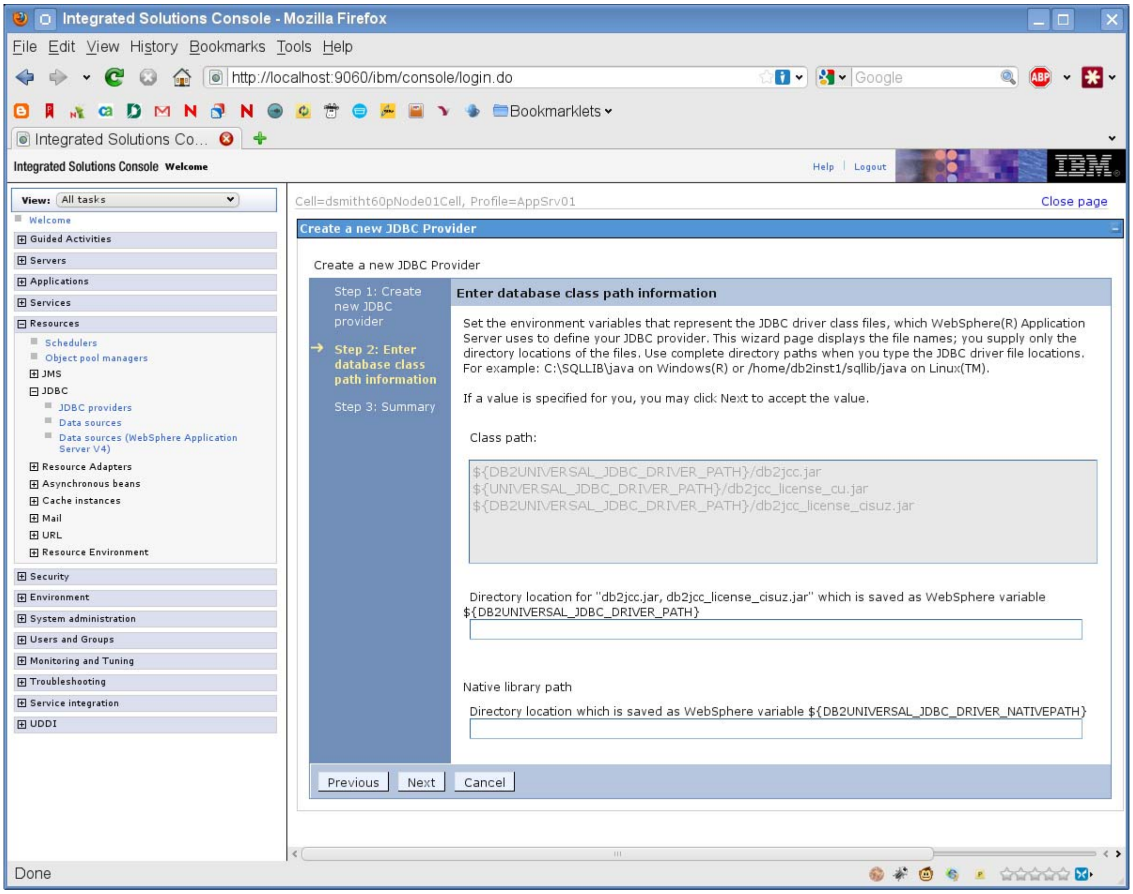
Next | Cancel

Help

Field help

For field help information, s field label or l when the help displayed.

9 Enter the JDBC classpath information.



Create a new JDBC Provider

Create a new JDBC Provider

Enter database class path information

Set the environment variables that represent the JDBC driver class files, which WebSphere(R) Application Server uses to define your JDBC provider. This wizard page displays the file names; you supply only the directory locations of the files. Use complete directory paths when you type the JDBC driver file locations. For example: C:\SQLLIB\java on Windows(R) or /home/db2inst1/sqllib/java on Linux(TM).

If a value is specified for you, you may click Next to accept the value.

Class path:

```
${DB2UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc.jar
${UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cu.jar
${DB2UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cisuz.jar
```

Directory location for "db2jcc.jar, db2jcc_license_cisuz.jar" which is saved as WebSphere variable ${DB2UNIVERSAL_JDBC_DRIVER_PATH}

Native library path

Directory location which is saved as WebSphere variable ${DB2UNIVERSAL_JDBC_DRIVER_NATIVEPATH}

10 Click *Next*.

11 Click *Finish*.

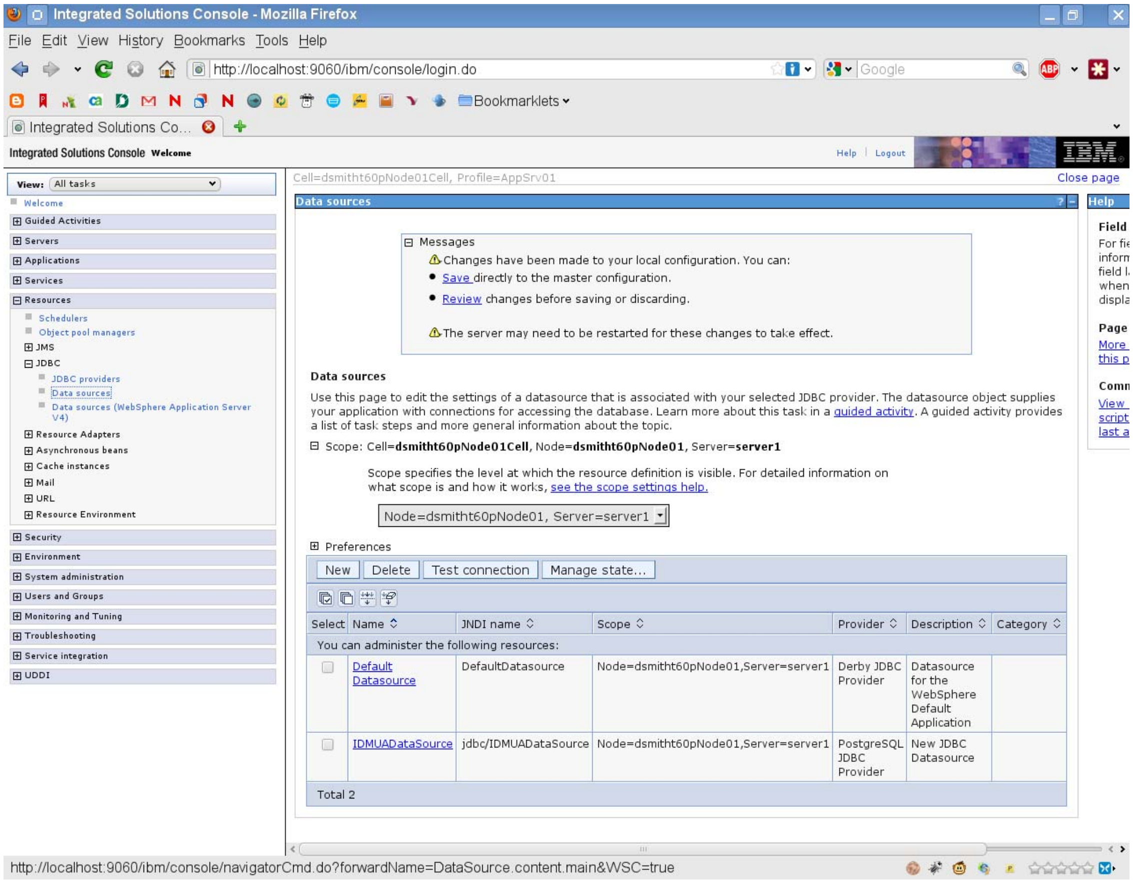
12 Click the *Save* link.

To create a data source:

1 Expand *Resources* on the left side of the page.

2 Expand *JDBC*.

3 Click *Data sources*.



Cell=dsmitht60pNode01Cell, Profile=AppSrv01

Data sources

Messages

⚠ Changes have been made to your local configuration. You can:

- Save directly to the master configuration.
- Review changes before saving or discarding.

⚠ The server may need to be restarted for these changes to take effect.

Data sources

Use this page to edit the settings of a datasource that is associated with your selected JDBC provider. The datasource object supplies your application with connections for accessing the database. Learn more about this task in a guided activity. A guided activity provides a list of task steps and more general information about the topic.

Scope: Cell=**dsmitht60pNode01Cell**, Node=**dsmitht60pNode01**, Server=**server1**

Scope specifies the level at which the resource definition is visible. For detailed information on what scope is and how it works, see the scope settings help.

Node=dsmitht60pNode01, Server=server1

Select	Name	JNDI name	Scope	Provider	Description	Category
You can administer the following resources:						
□	Default Datasource	DefaultDatasource	Node=dsmitht60pNode01,Server=server1	Derby JDBC Provider	Datasource for the WebSphere Default Application	
□	IDMUADataSource	jdbc/IDMUADataSource	Node=dsmitht60pNode01,Server=server1	PostgreSQL JDBC Provider	New JDBC Datasource	
Total 2						

http://localhost:9060/ibm/console/navigatorCmd.do?forwardName=DataSource.content.main&WSC=true

4 Expand *Scope*.

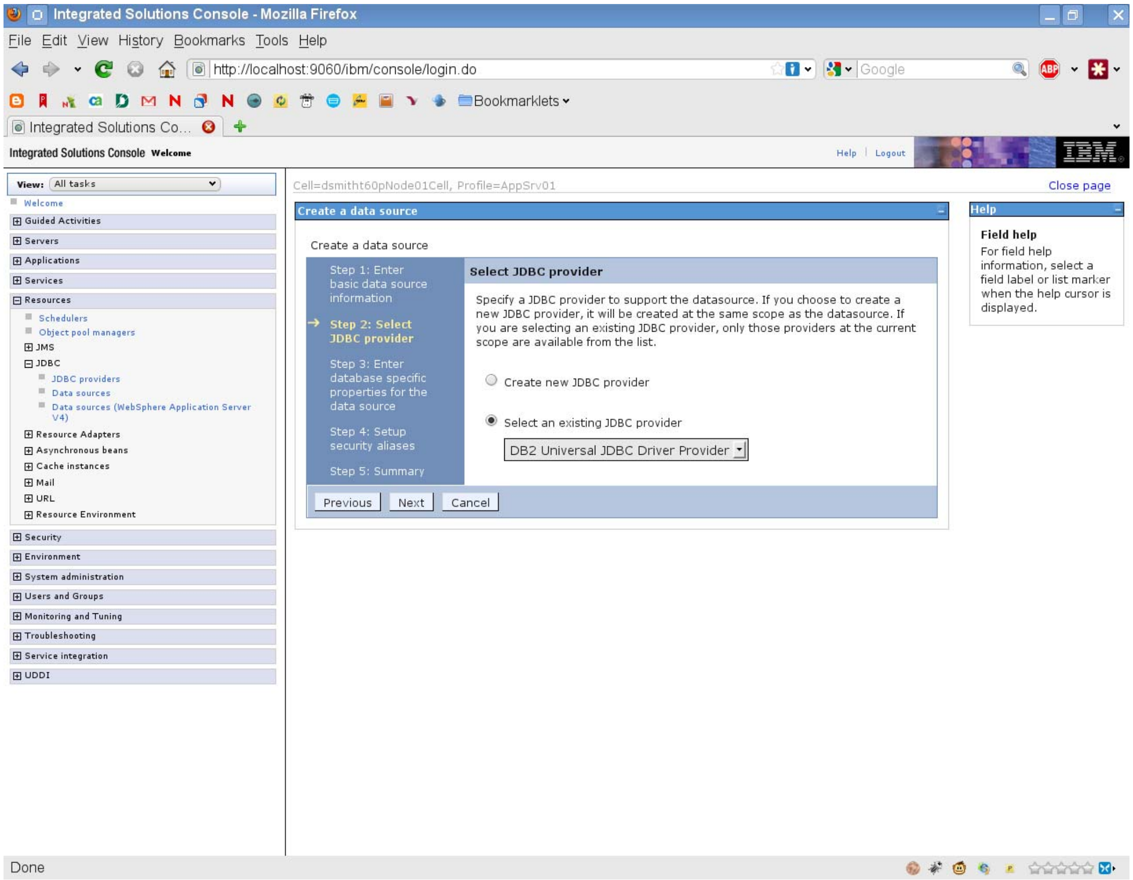
5 Select *Node=yourservername, Server=server1*.

6 Click the *New* button.

7 Enter the DataSource name and JNDI name (for example, IDMUADataSource for both).

8 Click *Next*.

9 Click *Select an existing JDBC provider*.



Cell=dsmitht60pNode01Cell, Profile=AppSrv01

Create a data source

Create a data source

Step 1: Enter basic data source information

→ Step 2: Select JDBC provider

Step 3: Enter database specific properties for the data source

Step 4: Setup security aliases

Step 5: Summary

Select JDBC provider

Specify a JDBC provider to support the datasource. If you choose to create a new JDBC provider, it will be created at the same scope as the datasource. If you are selecting an existing JDBC provider, only those providers at the current scope are available from the list.

○ Create new JDBC provider

● Select an existing JDBC provider

DB2 Universal JDBC Driver Provider

Help

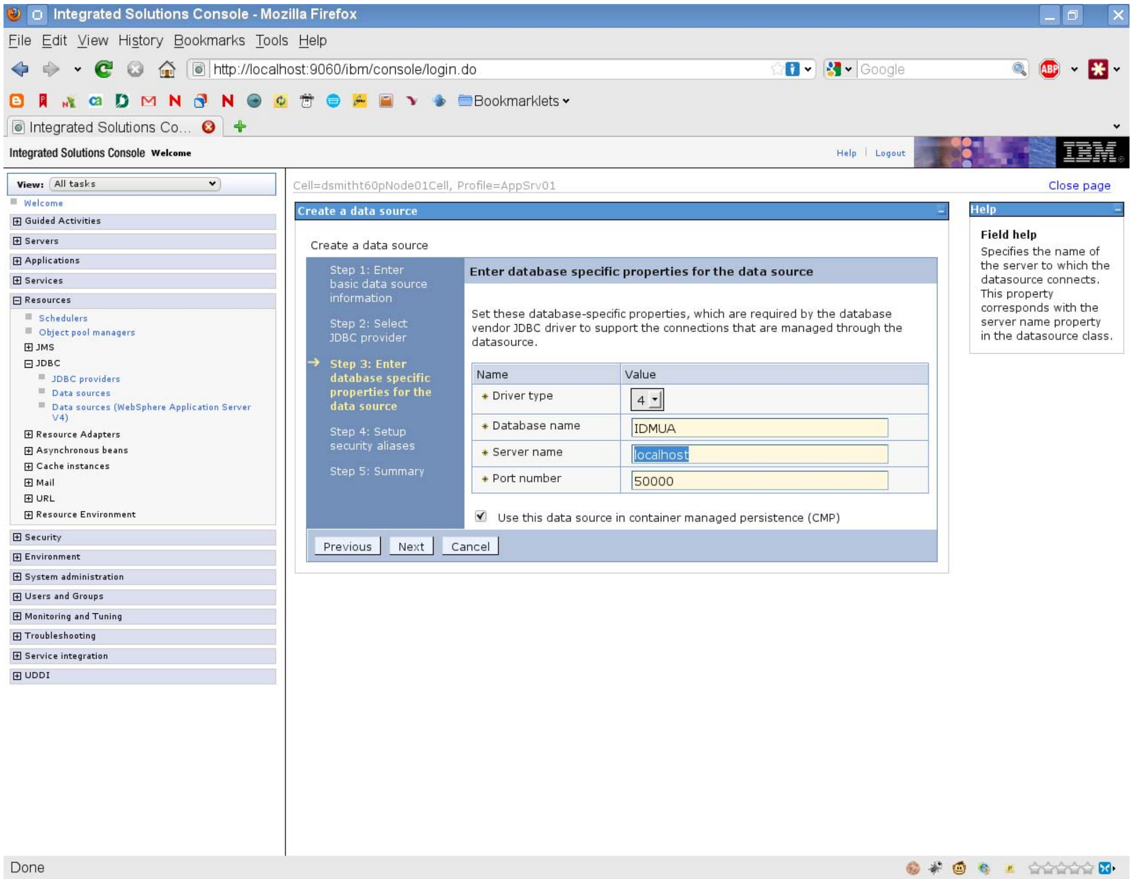
Field help

For field help information, select a field label or list marker when the help cursor is displayed.

10 Select the JDBC Provider you created above.

11 Click *Next*.

12 Enter the database information required for the DataSource (databasename, server name, port, username, and password).



Cell=dsmitht60pNode01Cell, Profile=AppSrv01

Create a data source

Create a data source

Step 1: Enter basic data source information

Step 2: Select JDBC provider

→ Step 3: Enter database specific properties for the data source

Step 4: Setup security aliases

Step 5: Summary

Enter database specific properties for the data source

Set these database-specific properties, which are required by the database vendor JDBC driver to support the connections that are managed through the datasource.

Name	Value
* Driver type	4
* Database name	IDMUA
* Server name	localhost
* Port number	50000

☑ Use this data source in container managed persistence (CMP)

Help

Field help

Specifies the name of the server to which the datasource connects. This property corresponds with the server name property in the datasource class.

13 Click *Next*.

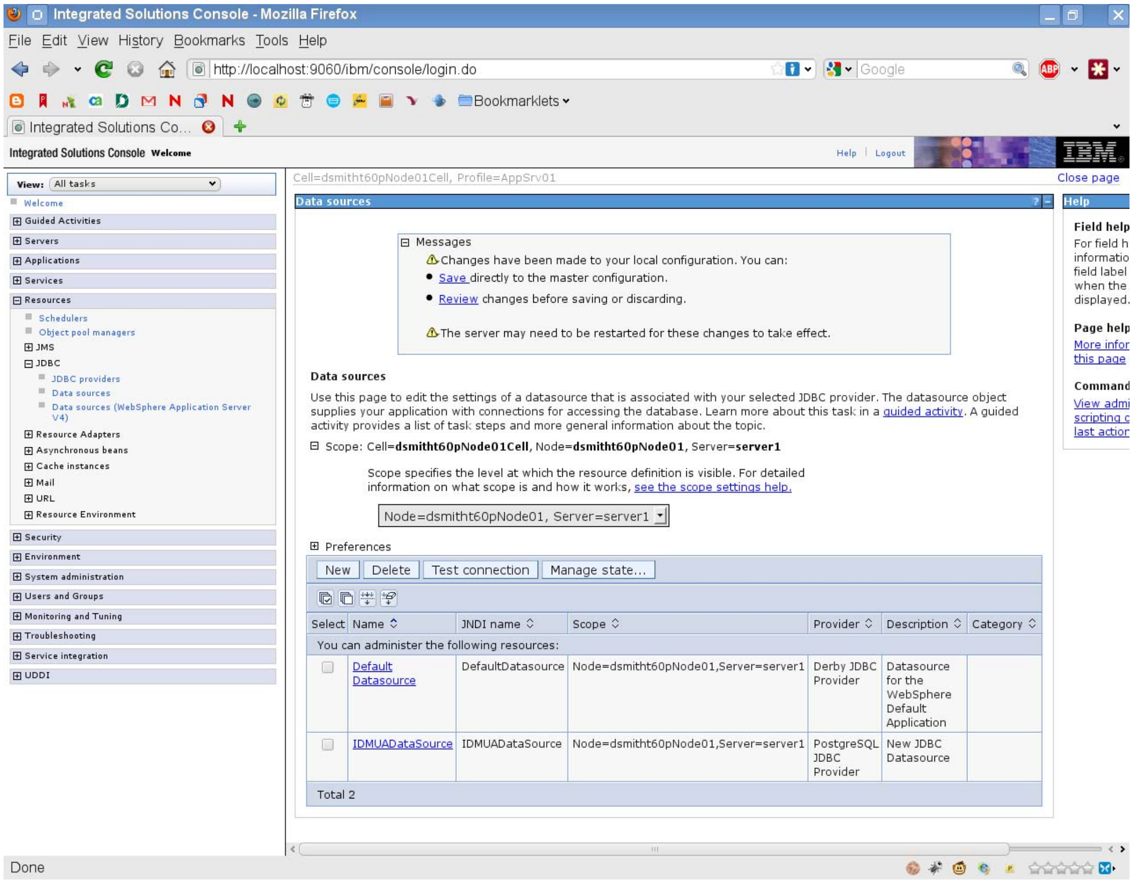
14 Enter Security Alias information or leave defaults.

15 Click *Next*.

16 Click *Finish*.

17 Click *Save*.

18 Select your new DataSource by clicking the checkbox to the left of the name.



Cell=dsmitht60pNode01Cell, Profile=AppSrv01

Data sources

⊟ Messages

⚠ Changes have been made to your local configuration. You can:

- Save directly to the master configuration.
- Review changes before saving or discarding.

⚠ The server may need to be restarted for these changes to take effect.

Data sources

Use this page to edit the settings of a datasource that is associated with your selected JDBC provider. The datasource object supplies your application with connections for accessing the database. Learn more about this task in a guided activity. A guided activity provides a list of task steps and more general information about the topic.

⊟ Scope: Cell=**dsmitht60pNode01Cell**, Node=**dsmitht60pNode01**, Server=**server1**

Scope specifies the level at which the resource definition is visible. For detailed information on what scope is and how it works, see the scope settings help.

Node=dsmitht60pNode01, Server=server1

⊞ Preferences

New | Delete | Test connection | Manage state...

Select	Name	JNDI name	Scope	Provider	Description	Category
You can administer the following resources:						
□	Default Datasource	DefaultDatasource	Node=dsmitht60pNode01,Server=server1	Derby JDBC Provider	Datasource for the WebSphere Default Application	
□	IDMUADataSource	IDMUADataSource	Node=dsmitht60pNode01,Server=server1	PostgreSQL JDBC Provider	New JDBC Datasource	
Total 2						

19 Click the *Test Connection* button, and make sure it returns *Success*.

6.2.2 Deploying the WAR File

Deploy the WAR file using the WebSphere deployment tools.

6.2.3 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.

IMPORTANT: Configupdate.sh will update the local version of this file. In the future, if you run configupdate.sh, you must update WebSphere's version of this file by copying it again. As a precaution, you should also make backups of all of the versions of this file.

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.

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

NOTE: If you plan to configure a clustered environment, you should also specify the workflow engine ID explicitly as a JVM system property. To specify the engine ID, add a system property with the name `com.novell.afw.wf.engine-id` (following the steps you used to define the other JVM system properties) and specify any value you would like for the ID.

6.2.4 Configuring the Shared Library

If you are using WebSphere 7.0 with Version 4.0.2 of the RBPM, you need to be aware that several JAR files have been upgraded to the latest available versions in this release of RBPM. You will encounter class loading problems with JAR files that have shipped with WebSphere if you do not configure a shared library for RBPM. This will ensure that WebSphere uses the RBPM versions of these JAR files.

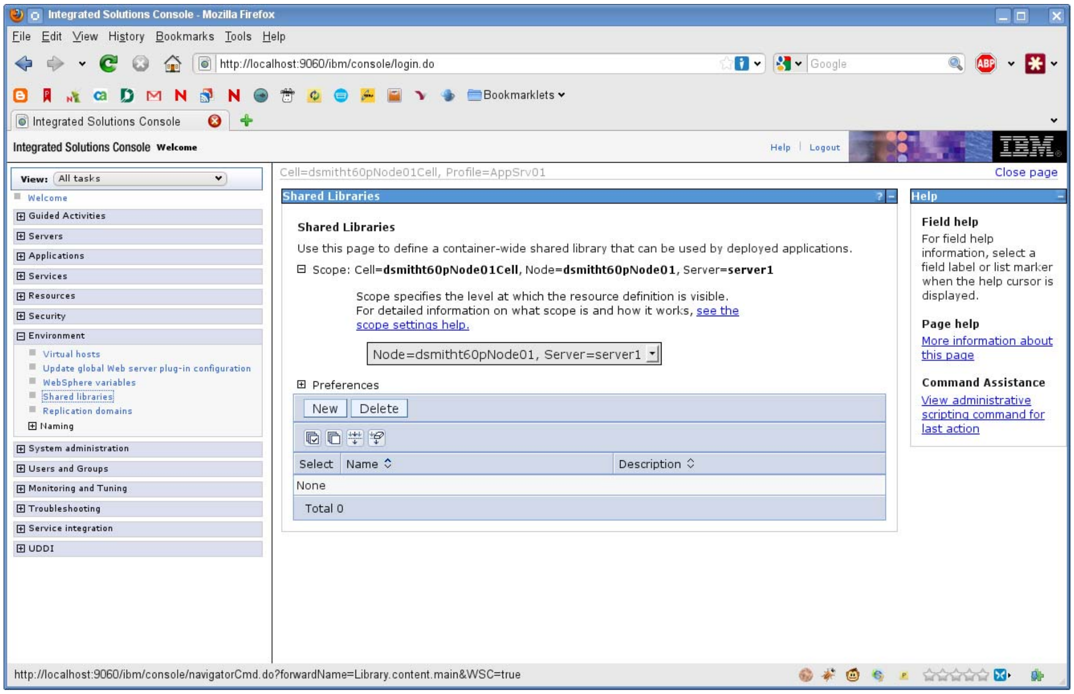
WebSphere class loading problems can be manifest as the following kinds of exceptions:

- ClassCastException
- ClassNotFoundException
- NoClassDefFoundException
- UnsatisfiedLinkError
- LinkageError

To configure the shared library:

1 Click on *Environment* in the left-navigation menu.

2 Click *Shared Libraries*.


Integrated Solutions Console - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:9060/ibm/console/login.do
Google
Bookmarklets
Integrated Solutions Console
Integrated Solutions Console Welcome
Help | Logout
IBM
View: All tasks
Welcome
Guided Activities
Servers
Applications
Services
Resources
Security
Environment
Virtual hosts
Update global Web server plug-in configuration
WebSphere variables
Shared libraries
Replication domains
Naming
System administration
Users and Groups
Monitoring and Tuning
Troubleshooting
Service integration
UDDI
Close page
New
Delete
http://localhost:9060/ibm/console/navigatorCmd.do?forwardName=Library.content.main&WSC=true

Cell=dsmitht60pNode01Cell, Profile=AppSrv01

Shared Libraries

Shared Libraries

Use this page to define a container-wide shared library that can be used by deployed applications.

⊟ Scope: Cell=**dsmitht60pNode01Cell**, Node=**dsmitht60pNode01**, Server=**server1**

Scope specifies the level at which the resource definition is visible.
For detailed information on what scope is and how it works, see the scope settings help.

Node=dsmitht60pNode01, Server=server1

⊞ Preferences

Select	Name ⇕	Description ⇕
None		
Total 0		

Help

Field help
For field help information, select a field label or list marker when the help cursor is displayed.

Page help
More information about this page

Command Assistance
View administrative scripting command for last action

3 Click the *New* button.

4 Enter a name (such as IDMUA Classpath).

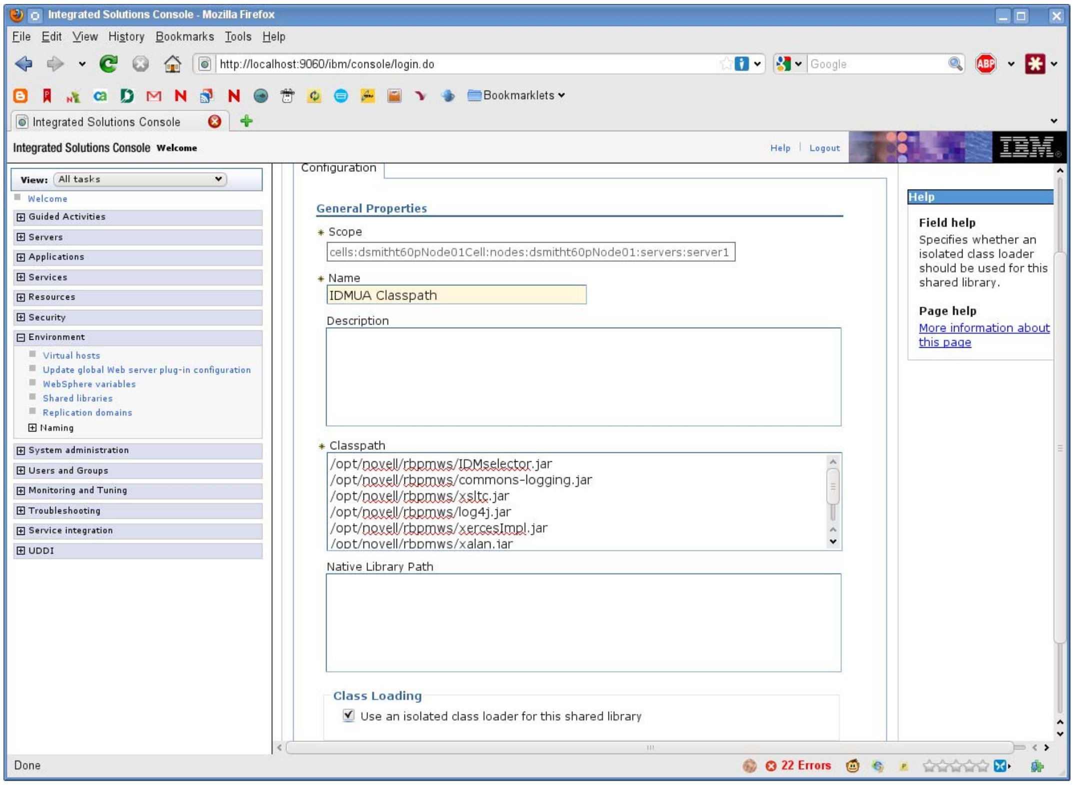
5 Enter the list of required JAR files into the Classpath field:

- `antlr.jar`
- `log4j.jar`
- `commons-logging.jar`

  NOTE: You need to download this JAR file from the Apache site.

- `xalan.jar`
- `xercesImpl.jar`
- `xsltc.jar`
- `jaxb-impl.jar`

6 Select *Use an isolated class loader for this shared library*.



Configuration

General Properties

* Scope
cells:dsmitht60pNode01Cell:nodes:dsmitht60pNode01:servers:server1

* Name
IDMUA Classpath

Description

* Classpath
```
/opt/novell/rbpmws/IDMselector.jar
/opt/novell/rbpmws/commons-logging.jar
/opt/novell/rbpmws/xsltc.jar
/opt/novell/rbpmws/log4j.jar
/opt/novell/rbpmws/xercesImpl.jar
/opt/novell/rbpmws/xalan.jar
```

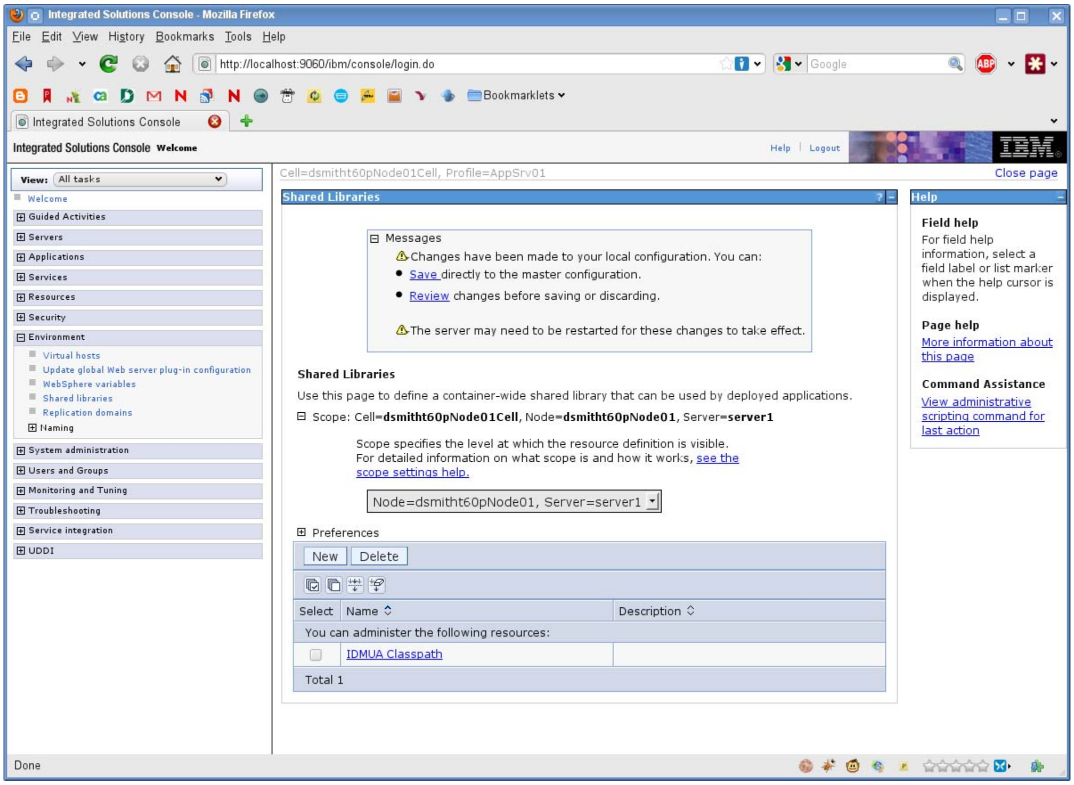
Native Library Path

Class Loading
☑ Use an isolated class loader for this shared library

Specifies whether an isolated class loader should be used for this shared library.

7 Click *OK*.

8 Click the *Save* link.



Cell=dsmitht60pNode01Cell, Profile=AppSrv01

Shared Libraries

Messages

⚠ Changes have been made to your local configuration. You can:

- Save directly to the master configuration.
- Review changes before saving or discarding.

⚠ The server may need to be restarted for these changes to take effect.

Shared Libraries

Use this page to define a container-wide shared library that can be used by deployed applications.

Scope: Cell=**dsmitht60pNode01Cell**, Node=**dsmitht60pNode01**, Server=**server1**

Scope specifies the level at which the resource definition is visible. For detailed information on what scope is and how it works, see the scope settings help.

Node=dsmitht60pNode01, Server=server1

Preferences

New | Delete

Select	Name	Description
You can administer the following resources:		
□	IDMUA Classpath	
Total 1		

For field help information, select a field label or list marker when the help cursor is displayed.

6.2.5 Applying the Shared Library to a New Class Loader

The shared library must now be applied to a new class loader.

To apply the shared library to a new class loader:

1. Create the shared library, as outlined in Section 6.2.4, "Configuring the Shared Library," on page 83.
2. Go to *Application servers* > *server-name* > *Class loader*.

   NOTE: By default, this option is collapsed under the *Java and Process Management* section.

3. Click *New* to create a new class loader and choose *Classes loaded with local class loader first (parent last)*.
4. Click *Apply*.
5. Choose *Shared library references*.
6. Click *Add* and choose the shared library you created earlier.
7. Click *Apply*.
8. Click *OK*.
9. Click *Save* to save the changes to the master configuration.

6.2.6 Importing the eDirectory Trusted Root to the WebSphere Keystore

1. Copy the eDirectory trusted root certificates to the machine hosting the WebSphere server.

   The User Application installation procedure exports the certificates to the directory in which you install the User Application.

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 86) or through the command line ("Importing Certificates with the Command Line" on page 87).

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 *Related Items*.
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.
10. Click *Save* link at the top of the screen.

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 is 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.

6.2.7 Applying the Unrestricted Policy Files for the IBM JDK

In Section 6.1, "Installing and Configuring the User Application WAR," on page 67, which describes installation of RBPM on WebSphere, the IBM JDK policy files were applied for the installer's IBM JDK. These unrestricted policy files must also be applied for each WebSphere IBM JDK server that is running RBPM.

Review each WebSphere server IBM JDK to ensure you have applied the unrestricted policy files. Without these unrestricted policy files, the error "Illegal key size" will occur during startup of RBPM.

6.2.8 Passing the preferIPv4Stack Property to the JVM

The User Application uses JGroups for the caching implementation. In some configurations, JGroups requires that the preferIPv4Stack property be set to true in order to ensure that the mcast_addr binding is successful.

Without this option, the following error may be observed:

```
[10/1/09 16:11:22:147 EDT] 0000000d UDP           W org.jgroups.util.Util
createMulticastSocket could not bind to /228.8.8.8 (IPv4 address); make sure
your mcast_addr is of the same type as the IP stack (IPv4 or IPv6).
```

Alternatively, you may also see this error:

```
[3/21/12 10:04:32:470 EDT] 00000024 UDP      E org.jgroups.protocols.TP down
failed sending message to null (131 bytes)
        java.lang.Exception: dest=/228.8.8.8:45654 (134 bytes)
    at org.jgroups.protocols.UDP._send(UDP.java:353)
```

The parameter `java.net.preferIPv4Stack=true` is a system property that can be set in the same manner as other system properties such as `extend.local.config.dir`. For instructions on setting system properties, see Section 6.2.3, "Adding User Application Configuration Files and JVM System Properties," on page 82.

6.3 Starting and Accessing the User Application

To start the User 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.

To access the User Application

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`

7 Installing the User Application on WebLogic

The WebLogic installer configures the User Application WAR file based on your input. This section provides details for:

- Section 7.1, “WebLogic Installation CheckList,” on page 89
- Section 7.2, “Installing and Configuring the User Application WAR,” on page 90
- Section 7.3, “Preparing the WebLogic Environment,” on page 96
- Section 7.4, “Deploying the User Application WAR,” on page 99
- Section 7.5, “Accessing the User Application,” on page 99

To learn about installing using a non-graphical user interface, see Chapter 8, “Installing from the Console or with a Single Command,” on page 101.

Run the installer as root You need to run the installer as the root user.

Data Migration For information on migrating, see the *RBPM and Reporting Migration Guide* (http://www.netiq.com/documentation/idm402/index.html).

7.1 WebLogic Installation CheckList

❒ Install WebLogic.

Follow the installation instructions in the WebLogic documentation.

❒ Create a WebLogic-enabled WAR.

Use the Identity Manager User Application installer to perform this task. See Section 7.2, “Installing and Configuring the User Application WAR,” on page 90.

❒ Prepare the WebLogic environment for the WAR’s deployment by copying configuration files to the appropriate WebLogic locations.

See Section 7.3, “Preparing the WebLogic Environment,” on page 96.

❒ Deploy the WAR.

See Section 7.4, “Deploying the User Application WAR,” on page 99.

7.2 Installing and Configuring the User Application WAR

NOTE: For WebLogic 10.3, the installation program requires the Java 2 Platform Standard Edition Development Kit version 1.6 JDK from JRockit. If you use a different version, the installation procedure does not successfully configure the User Application WAR file. The installation appears to succeed, but you encounter errors when trying to start the User Application.

1 Navigate to the directory containing your installation files.

2 Launch the installer for your platform from the command line, using the JRockit Java environment (with version 1.6_17):

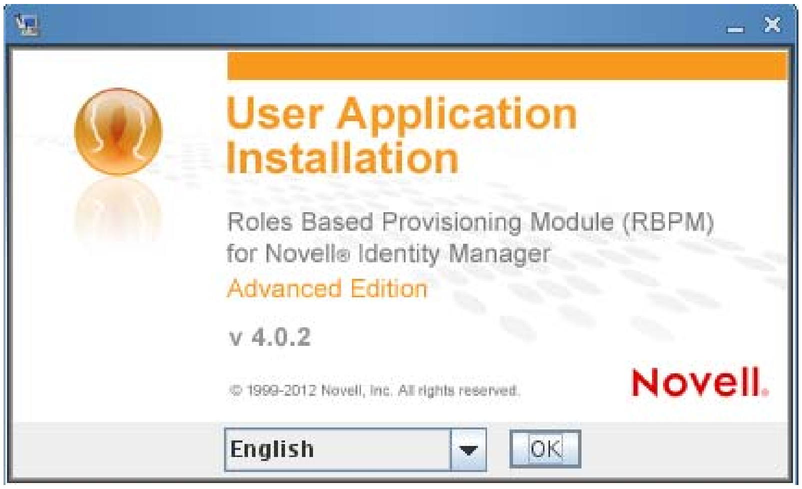
Solaris

```
$ /opt/WL/bea/jrockit_160_17/bin/java -jar IdmUserApp.jar
```

Windows

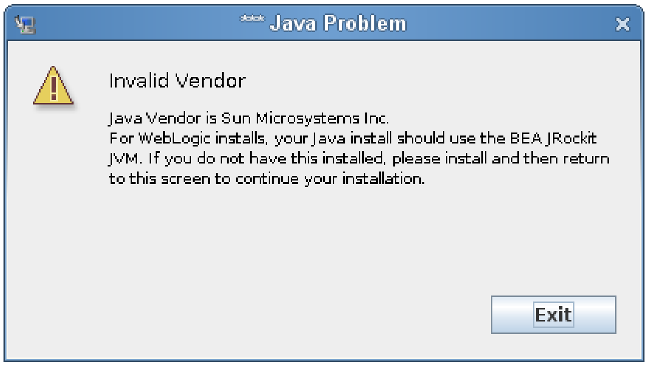
```
C:\WL\bea\jrockit_160_17\bin\java -jar IdmUserApp.jar
```

When the installation program launches, you are prompted for the language.


User Application Installation
Roles Based Provisioning Module (RBPM)
for Novell® Identity Manager
Advanced Edition
v 4.0.2
© 1999-2012 Novell, Inc. All rights reserved.
Novell.
English
OK

3 Use the following information to select the language, confirm the license agreement, and select the Application Server platform:

Installation Screen	Description
User Application Installation	Select the language for the installation program. The default is English.
License Agreement	Read the License Agreement, then select *I accept the terms of the License Agreement*.

Installation Screen	Description
Application Server Platform	Select *WebLogic.* If the User Application WAR file is in a different directory from the installer, the installer prompts for the path to the WAR. 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. When you're installing on WebLogic, you need to launch the installation program by using the BEA's Java environment (jrockit). If you select WebLogic as the application server, and do not use jrockit to launch the installation, you will see a pop-up error message, and the installation will terminate:  Invalid Vendor Java Vendor is Sun Microsystems Inc. For WebLogic installs, your Java install should use the BEA JRockit JVM. If you do not have this installed, please install and then return to this screen to continue your installation.

4 Use the following information to choose an install folder and configure the database:

Installation Screen	Description
Choose Install Folder	Specify where you want the installer to put the files.
Database Platform	Select the database platform. The database and JDBC driver must already be installed. For WebLogic, the options include the following: ◆ Oracle ◆ Microsoft SQL Server ◆ PostgreSQL
Database Host and Port	*Host*: Specify the database server's hostname or IP address. For a cluster, specify the same hostname or IP address for each member of the cluster. *Port*: Specify the database's listener port number. For a cluster, specify the same port for each member of the cluster.

Installation Screen	Description
Database Username and Password	*Database Name* (or SID): For MS SQL Server or PostgreSQL provide the name of your preconfigured database. For Oracle, provide the Oracle System Identifier (SID) that you previously created. For a cluster, specify the same database name or SID for each member of the cluster. *Database Username*: Specify the database user. For a cluster, specify the same database user for each member of the cluster. *Database Password*: Specify the database password. For a cluster, specify the same database password for each member of the cluster. *Database Driver JAR file*: Provide the Thin Client JAR for the Database Server. This is required.
Database Administrator	This screen is pre-populated with the same username and password from the Database Username and Password page. If the database user that was specified earlier does not have enough permissions to create tables in the Database Server, then a different user ID that has the necessary rights needs to be entered.
Create Database Tables	Specify when the database tables should be created.
New Database or Existing Database	If the database that will be used is new or empty, then select the *New Database* button. If the database is an existing one from a previous installation, select *Existing Database*.
Test Database Connection	To confirm that the information provided in the previous screens was correct, you can test the database connection by selecting *Test Database Connection*. The installer needs to connect to the database both for creating tables directly and for creating the .SQL file. If you test the database connection and it fails, you may still continue with installation. In this case, you will need to create the tables after installation, as described in the *User Application: Administration Guide* (http://www.netiq.com/documentation/idm402/agpro/?page=/documentation/idm402/agpro/data/bncf7rj.html).

5 Use the following information to configure Java and Identity Manager, as well as audit settings and security.

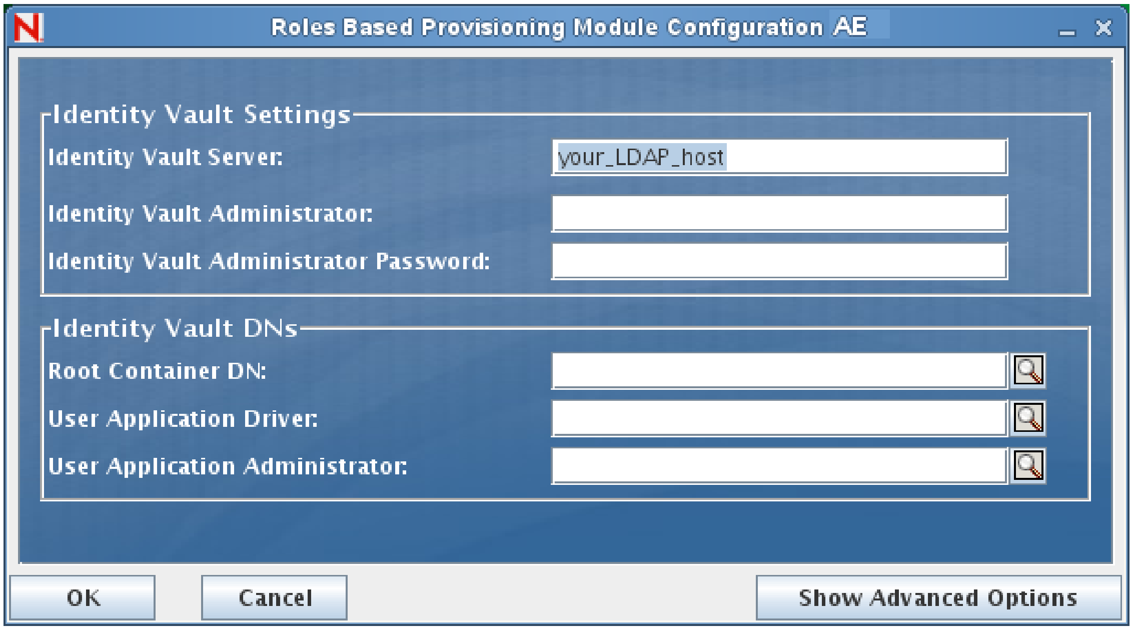
Installation Screen	Description
Java Install	Specify the Java root install folder. The Java Install provides the path to Java based on your JAVA_HOME environment variable and gives you the option to correct it. At this point, the Installation program also validates that the Java selected is the correct one for the Application Server selected. In addition, it validates that it can write to the cacerts in the JRE that was specified.
IDM Configuration	*Application Context*: The name of the application server configuration, the name of the application WAR file, and the name of the URL context. The installation script creates a server configuration and by default names the configuration based on *Application name*. Make a note of the application name and include it in the URL when you start the User Application from a browser.

Installation Screen	Description
Select Audit Logging Type	To enable logging, click *Yes*. To disable logging, click *No*. The next panel prompts you to specify the type of logging. Choose from the following options: ◆ *Novell Identity Audit or Novell Sentinel*: Enables logging through a Novell auditing client for the User Application. ◆ *OpenXDAS*: Events are logged to your OpenXDAS logging server. For more information on setting up logging, see the *User Application: Administration Guide*.
Novell Identity Audit or Novell Sentinel	*Server*: If you enable logging, specify the hostname or IP address for the server. If you turn logging off, this value is ignored. *Log Cache Folder*: Specify the directory for the logging cache.
Security - Master Key	*Yes*: Allows you to Import an existing master key. If you choose to import an existing encrypted master key, cut and paste the key into the install procedure window. *No*: Creates a new master key. After you finish the installation, you must manually record the master key as described in Section 9.1, “Recording the Master Key,” on page 115. The installation procedure writes the encrypted master key to the `master-key.txt` file in the installation directory. 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.

6 If you would like to configure RBPM now, select *Configure Now* and click *Next*.

(If you are not prompted for this information, you might not have completed the steps outlined in Section 2.5, “Installing the Java Development Kit,” on page 27.)

The default view of the Roles Based Provisioning Module Configuration panel shows these six fields:



Roles Based Provisioning Module Configuration AE

Identity Vault Settings

Identity Vault Server: your_LDAP_host

Identity Vault Administrator:

Identity Vault Administrator Password:

Identity Vault DNs

Root Container DN:

User Application Driver:

User Application Administrator:

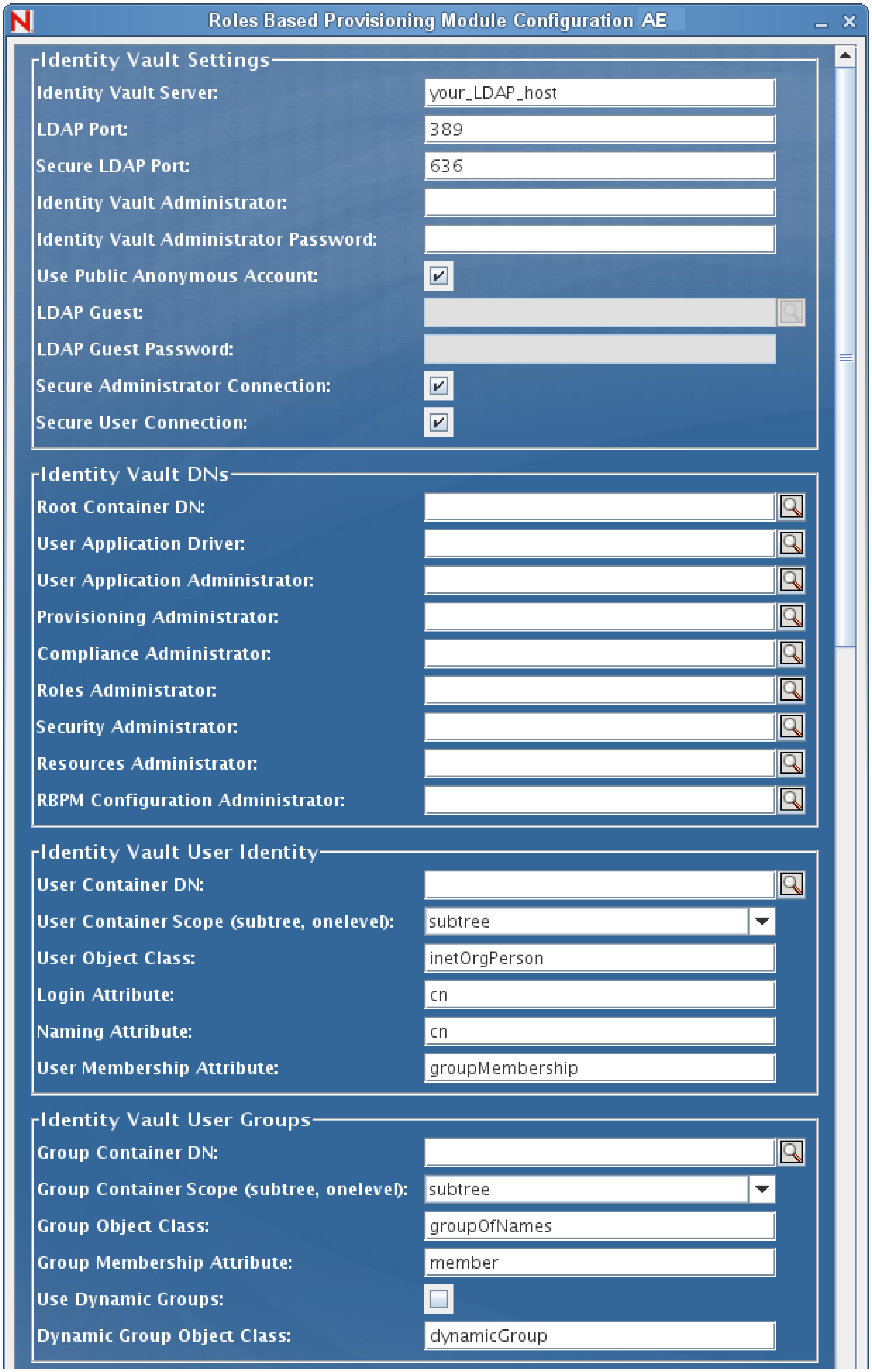
The Installation program will take the value from the Root Container DN and apply it to the following values:

- User Container DN
- Group Container DN

The Installation program will take the value from the User Application Administrator fields and apply it to the following values:

- Provisioning Administrator
- Compliance Administrator
- Roles Administrator
- Security Administrator
- Resources Administrator
- RBPM Configuration Administrator

If you want to be able to specify these values explicitly, you can click the *Show Advanced Options* button and change them:



Roles Based Provisioning Module Configuration AE

Identity Vault Settings

Identity Vault Server:	your_LDAP_host
LDAP Port:	389
Secure LDAP Port:	636
Identity Vault Administrator:	
Identity Vault Administrator Password:	
Use Public Anonymous Account:	☑
LDAP Guest:	
LDAP Guest Password:	
Secure Administrator Connection:	☑
Secure User Connection:	☑

Identity Vault DNs

Root Container DN:	
User Application Driver:	
User Application Administrator:	
Provisioning Administrator:	
Compliance Administrator:	
Roles Administrator:	
Security Administrator:	
Resources Administrator:	
RBPM Configuration Administrator:	

Identity Vault User Identity

User Container DN:	
User Container Scope (subtree, onelevel):	subtree
User Object Class:	inetOrgPerson
Login Attribute:	cn
Naming Attribute:	cn
User Membership Attribute:	groupMembership

Identity Vault User Groups

Group Container DN:	
Group Container Scope (subtree, onelevel):	subtree
Group Object Class:	groupOfNames
Group Membership Attribute:	member
Use Dynamic Groups:	□
Dynamic Group Object Class:	dynamicGroup

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.

See Appendix A, "User Application Configuration Reference," on page 123 for a description of each option.

7 Use the following information to complete the installation.

Installation Screen	Description
Pre-Installation Summary	Read the Pre-Installation Summary page to verify your choices for the installation parameters. If necessary, use *Back* to return to earlier installation pages to change installation parameters. The User Application configuration page does not save values, so after you re-specify earlier pages in the installation, you must re-enter the User Application configuration values. When you are satisfied with your installation and configuration parameters, return to the Pre-Install Summary page and click *Install*.
Install Complete	Indicates that the installation is finished.

7.2.1 Viewing Installation and Log Files

If your installation completed without error, continue with Preparing the WebLogic Environment. 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.

7.3 Preparing the WebLogic Environment

7.3.1 Configuring the Data Source

❐ Copy your database driver JAR files to the domain where you will deploy the User Application.

❐ Create your datasource.

Follow the instructions for creating a datasource in the WebLogic documentation.

Note that the JNDI name for the datasource must be `jdbc/IDMUADataSource`, regardless of what name you specified for the datasource or for the database when you created the User Application WAR.

7.3.2 Specifying RBPM Configuration File Locations

The WebLogic user application needs to know how to locate the sys-configuration-xmldata.xml file, the idmuserapp_logging.xml file, and the wl_idmuserapp_logging.xml file. Therefore, you need to add the location of the files to the setDomainEnv.cmd file.

To make them available to the application server, specify the locations in the setDomainEnv.cmd or setDomainEnv.sh file:

1. Open setDomainEnv.cmd or setDomainEnv.sh file.
2. Locate the line that looks like this:

   ```
   set JAVA_PROPERTIES
   ```

   ```
   export JAVA_PROPERTIES
   ```

3. Below the JAVA_PROPERTIES entry, add entries for:
   - -Dextend.local.config.dir==<directory-path>: Specify the folder (not the file itself) that contains the sys-configuration.xml file.
   - -Didmuserapp.logging.config.dir==<directory-path>: Specify the folder (not the file itself) that contains the idmuserapp_logging.xml file.
   - -Dlog.init.file==<file-name>: Specify the wl_idmuserapp_logging.xml file, which is used for log4j configuration. This file handles the appender and logger configurations required for the User Application in situations where multiple applications are installed on the same application server.

   For example on Windows:

   ```
   set JAVA_OPTIONS=-Dextend.local.config.dir=c:\novell\idm
   set JAVA_OPTIONS=%JAVA_OPTIONS% -Didmuserapp.logging.config.dir=c:\novell\idm
   set JAVA_OPTIONS=%JAVA_OPTIONS%
   -Dlog.init.file=wl_idmuserapp_logging.xml
   ```

4. Set the environment variable EXT_PRE_CLASSPATH to point to the following JAR files:
   - antlr-2.7.6.jar
   - IDMselector.jar
   - log4j.jar
   - commons-logging.jar

     NOTE: You need to download this JAR file from the Apache site.

   - xalan.jar
   - xercesImpl.jar
   - xsltc.jar
   - serializer.jar

   NOTE: An alternative approach to adding these JAR files to the EXT_PRE_CLASSPATH variable would be to copy these files into WEB-INF/lib directory within the IDMProv.war file.

   4a. Locate this line:

   ```
   ADD EXTENSIONS TO CLASSPATH
   ```

   4b. Add the EXT_PRE_CLASSPATH below it. For example, on Windows:

```
set EXT_PRE_CLASSPATH=C:\bea\user_projects\domains\base_domain\lib\antlr-
2.7.6.jar;C:\bea\user_projects\domains\base_domain\lib\IDMselector.jar;C:\
bea\user_projects\domain\base_domain\lib\log4j.jar;C:\bea\user_projects\do
mains\base_domain\lib\commons-
logging.jar;C:\bea\user_projects\domains\base_domain\lib\xalan.jar;C:\bea\
user_projects\domains\base_domain\lib\xercesImpl.jar;C:\bea\user_projects\
domains\base_domain\lib\xsltc.jar;C:\bea\user_projects\domains\base_domain
\lib\serializer.jar
```

For example, on Linux:

```
export EXT_PRE_CLASSPATH=/opt/bea/user_projects/domains/base_domain/lib/
antlr-2.7.6.jar:/opt/bea/user_projects/domains/base_domain/lib/
IDMselector.jar:/opt/bea/user_projects/domain/base_domain/lib/log4j.jar:/
opt/bea/user_projects/domains/base_domain/lib/commons-logging.jar:/opt/
bea/user_projects/domains/base_domain/lib/xalan.jar:/opt/bea/
user_projects/domains/base_domain/lib/xercesImpl.jar:/opt/bea/
user_projects/domains/base_domain/lib/xsltc.jar:/opt/bea/user_projects/
domains/base_domain/lib/serializer.jar
```

5 Save and exit the file.

The XML files are also used by the configured utility; therefore, you need to edit the `configupdate.bat` or `configupdate.sh` files as follows:

1 Open `configupdate.bat` or `configupdate.sh`.

2 Locate the following line:

```
-Duser.language=en -Duser.region="
```

3 Update the existing line to include the path to the sys-configuration.xml file:

For example, on Windows:

```
-Dextend.local.config.dir=c:\novell\idm
```

For example, on Linux:

```
-Dextend.local.config.dir=/opt/novell/idm
```

4 Save and close the file.

5 Run the configupdate utility to install the certificate into the keystore of the JDK under BEA_HOME.

When you run `configupdate`, you are prompted for the `cacerts` file under the JDK you are using. If you are not using that same JDK that was specified during the installation you must run `configupdate` on the WAR. Pay attention to the JDK specified because this entry must point to the JDK used by WebLogic. This is done to import a certificate file for the connection to the Identity Vault. The purpose for this is to import a certificate for the connection to eDirectory.

The Identity Vault Certificates value in the configupdate utility must point to the following location:

```
c:\jrockit\jre\lib\security\cacerts
```

7.3.3 Removing OpenSAML JAR Files

The OpenSAML JAR files that WebLogic uses conflict with the ones needed for the User Application. Therefore, you need to remove the ones in the WebLogic /WL103/modules directory to ensure that the User Application is installed properly on WebLogic. This requirement applies to any User Application that does not have SSO enabled.

Be sure to remove the following JAR files in the WebLogic /WL103/modules directory:

```
com.bea.core.bea.opensaml_1.0.0.0_5-0-2-0.jar
com.bea.core.bea.opensaml2_1.0.0.0_5-0-2-0.jar
```

7.3.4 Workflow Plug-In and WebLogic Setup

The Workflow Administration plug-in to iManager is unable to connect to the User Application Driver running on WebLogic if the `enforce-valid-basic-auth-credentials` flag is set to true. For this connection to succeed, you must disable this flag.

To disable the enforce-valid-basic-auth-credentials flag, follow these instructions:

1. Open the `config.xml` file in the `<*WLHome*>\user_projects\domains\idm\config\` folder.
2. Add the following line in the `<security-configuration>` section right before the closing of this section:

   ```
   <enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-
   credentials>
   </security-configuration>
   ```

3. Save the file and restart the server.

After making this change, you should be able to login to the Workflow Administration plug-in.

7.4 Deploying the User Application WAR

At this point, you can deploy the User Application WAR using the standard WebLogic deployment procedure.

7.5 Accessing the User Application

Navigate to the User Application URL:

```
http://application-server-host:port/application-context
```

For example:

```
http://localhost:8180/IDMProv
```

8 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 5, “Installing the User Application on JBoss,” on page 53. Topics include:

- Section 8.1, “Installing the User Application from the Console,” on page 101
- Section 8.2, “Installing the User Application with a Single Command,” on page 102
- Section 8.3, “Running the JBossPostgreSQL Utility in Silent or Console Mode,” on page 111
- Section 8.4, “Running the RIS Installer in Silent or Console Mode,” on page 112

8.1 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.

NOTE: The installation program requires at least the Java 2 Platform Standard Edition Development Kit version 1.5. If you use an earlier version, the installation procedure does not successfully configure the User Application WAR file. The installation appears to succeed, but you encounter errors when trying to start the User Application.

1. Once you have obtained the appropriate installation files described in Table 2-1 on page 15, log in and open a terminal session.
2. Launch the installer for your platform with Java as described below:

   ```
   java -jar IdmUserApp.jar -i console
   ```
3. Follow the same steps described for the graphical user interface under Chapter 5, “Installing the User Application on JBoss,” on page 53, reading the prompts at the command line and entering responses at the command line, through the steps on importing or creating the master key.
4. 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 A.1, “User Application Configuration: Basic Parameters,” on page 123.
5. 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.
6. Continue with Chapter 9, “Post-Installation Tasks,” on page 115.

8.2 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 15.

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 8-1 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 8-1** User Application Configuration Parameters for a Silent Install*

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

User Application Parameter Name in silent.properties	Equivalent Parameter Name in the User Application Configuration Parameters File
NOVL_CONFIG_COMPLIANCECONTAINERDN	The Compliance Module Administrator is a system role that allows members to perform all functions on the *Compliance* tab. This user must exist in the Identity Vault prior to being designated as the Compliance Module Administrator.
NOVL_CONFIG_USERCONTAINERDN=	Meta-Directory User Identity: User Container DN. Specify the LDAP distinguished name (DN) or fully qualified LDAP name of the user container. This defines the search scope for users and groups. Users in this container (and below) are allowed to log in to the User Application. **IMPORTANT:** Be sure the User Application Administrator specified during User Application driver set up exists in this container if you want that user to be able to execute workflows.
NOVL_CONFIG_GROUPCONTAINERDN=	Meta-Directory User Groups: Group Container DN. Specify the LDAP distinguished name (DN) or fully qualified LDAP name of the group container. Used by entity definitions within the directory abstraction layer.
NOVL_CONFIG_KEYSTOREPATH=	eDirectory Certificates: Keystore Path. Required. Specify the full path to your keystore (`cacerts`) file of the JRE that the application server application server is using. The User Application installation modifies the keystore file. On Linux or Solaris, the user must have permission to write to this file.
NOVL_CONFIG_KEYSTOREPASSWORD=	eDirectory Certificates: Keystore Password. Specify the `cacerts` password. The default is `changeit`.
NOVL_CONFIG_SECUREADMINCONNECTION=	eDirectory Connection Settings: Secure Admin Connection. Required. Specify *True* to require that all communication using the admin account be done using a secure socket (this option can have adverse performance implications). This setting allows other operations that don't require SSL to operate without SSL. Specify *False* if the admin account does not use secure socket communication.

User Application Parameter Name in silent.properties	**Equivalent Parameter Name in the User Application Configuration Parameters File**
NOVL_CONFIG_SECUREUSERCONNECTION=	eDirectory Connection Settings: Secure User Connection. Required. Specify *True* to require that all communication done on the logged-in user's account be done using a secure socket (this option can have severe adverse performance implications). This setting allows other operations that don't require SSL to operate without SSL. Specify *False* if the user’s account does not use secure socket communication.
NOVL_CONFIG_SESSIONTIMEOUT=	Miscellaneous: Session Timeout. Required. Specify an application session timeout interval.
NOVL_CONFIG_LDAPPLAINPORT=	eDirectory Connection Settings: LDAP Non-Secure Port. Required. Specify the non-secure port for your LDAP server, for example 389.
NOVL_CONFIG_LDAPSECUREPORT=	eDirectory Connection Settings: LDAP Secure Port. Required. Specify the secure port for your LDAP server, for example 636.
NOVL_CONFIG_ANONYMOUS=	eDirectory Connection Settings: Use Public Anonymous Account. Required. Specify *True* to allow users who are not logged in to access the LDAP Public Anonymous Account. Specify *False* to enable NOVL_CONFIG_GUEST instead.
NOVL_CONFIG_GUEST=	eDirectory Connection Settings: LDAP Guest. Allows users who are not logged in to access permitted portlets. You must also deselect *Use Public Anonymous Account*. The Guest user account must already exist in the Identity Vault. To disable the Guest user, select *Use Public Anonymous Account*.
NOVL_CONFIG_GUESTPASS=	eDirectory Connection Settings: LDAP Guest Password.
NOVL_CONFIG_EMAILNOTIFYHOST=	Email: Notify Template HOST token. Specify the application server hosting the Identity Manager User Application. For example: `myapplication serverServer` This value replaces the $HOST$ token in e-mail templates. The URL that is constructed is the link to provisioning request tasks and approval notifications.

User Application Parameter Name in silent.properties	Equivalent Parameter Name in the User Application Configuration Parameters File
NOVL_CONFIG_EMAILNOTIFYPORT=	Email: Notify Template Port token. Used to replace the $PORT$ token in e-mail templates used in provisioning request tasks and approval notifications.
NOVL_CONFIG_EMAILNOTIFYSECUREPORT=	Email: Notify Template Secure Port token. Used to replace the $SECURE_PORT$ token in e-mail templates used in provisioning request tasks and approval notifications
NOVL_CONFIG_NOTFSMTPEMAILFROM=	Email: Notification SMTP Email From. Required. Specify e-mail From a user in provisioning e-mail.
NOVL_CONFIG_NOTFSMTPEMAILHOST=	Email: Notification SMTP Email Host. Required. Specify the SMTP e-mail host that provisioning e-mail is using. This can be an IP address or a DNS name.
NOVL_CONFIG_USEEXTPWDWAR=	Password Management: Use External Password WAR. Specify *True* if you are using an external password management WAR. If you specify *True*, you must also supply values for *NOVL_CONFIG_EXTPWDWARPTH* and *NOVL_CONFIG_EXTPWDWARRTNPATH*. Specify *False* to use the default internal Password Management functionality, `./jsps/pwdmgt/ForgotPassword.jsp` (without the http(s) protocol at the beginning). This redirects the user to the Forgot Password functionality built into the User Application, rather than to an external WAR.
NOVL_CONFIG_EXTPWDWARPATH=	Password Management: Forgot Password Link. Specify the URL for the Forgot Password functionality page, `ForgotPassword.jsp`, in an external or internal password management WAR. Or, accept the default internal password management WAR. For details, see "Configuring External Forgot Password Management" on page 118.
NOVL_CONFIG_EXTPWDWARRTNPATH=	Password Management: Forgot Password Return Link. Specify the Forgot Password Return Link so that the user can click after performing a forgot password operation.

User Application Parameter Name in silent.properties	Equivalent Parameter Name in the User Application Configuration Parameters File
NOVL_CONFIG_FORGOTWEBSERVICEURL=	Password Management: Forgot Password Web Service URL. This is the URL that the External Forgot Password WAR will use to call back to the User Application to perform core forgot password functionalities. The format of the URL is: `https://<idmhost>:<sslport>/<idm>/pwdmgt/service`
NOVL_CONFIG_USEROBJECTATTRIBUTE=	Meta-Directory User Identity: User Object Class. Required. The LDAP user object class (typically inetOrgPerson).
NOVL_CONFIG_LOGINATTRIBUTE=	Meta-Directory User Identity: Login Attribute. Required. The LDAP attribute (for example, CN) that represents the user’s login name.
NOVL_CONFIG_NAMINGATTRIBUTE=	Meta-Directory User Identity: Naming Attribute. 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.
NOVL_CONFIG_USERMEMBERSHIPATTRIBUTE=	Meta-Directory User Identity: User Membership Attribute. Optional. Required. The LDAP attribute that represents the user’s group membership. Do not use spaces in this name.
NOVL_CONFIG_GROUPOBJECTATTRIBUTE=	Meta-Directory User Groups: Group Object Class. Required. The LDAP group object class (typically groupofNames).
NOVL_CONFIG_GROUPMEMBERSHIPATTRIBUTE=	Meta-Directory User Groups: Group Membership Attribute. Required. Specify the attribute representing the user’s group membership. Do not use spaces in this name.
NOVL_CONFIG_USEDYNAMICGROUPS=	Meta-Directory User Groups: Use Dynamic Groups. Required. Specify *True* to use dynamic groups. Otherwise, specify *False*.
NOVL_CONFIG_DYNAMICGROUPOBJECTCLASS=	Meta-Directory User Groups: Dynamic Group Object Class. Required. Specify the LDAP dynamic group object class (typically dynamicGroup).

User Application Parameter Name in silent.properties	Equivalent Parameter Name in the User Application Configuration Parameters File
NOVL_CONFIG_TRUSTEDSTOREPATH=	Trusted Key Store: Trusted Store Path.
	The Trusted Key Store contains all trusted signers' certificates. If this path is empty, the User Application gets the path from System property `javax.net.ssl.trustStore`. If the path isn't there, it is assumed to be `jre/lib/security/cacerts`.
NOVL_CONFIG_TRUSTEDSTOREPASSWORD=	Trusted Key Store: Trusted Store Password.
NOVL_CONFIG_ICSLOGOUTENABLED=	Access Manager and iChain Settings: Simultaneous Logout Enabled.
	Specify *True* 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 *False* 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.
NOVL_CONFIG_EMAILNOTIFYPROTOCOL=	Email: Notify Template PROTOCOL token.
	Refers to a non-secure protocol, HTTP. Used to replace the $PROTOCOL$ token in e-mail templates used in provisioning request tasks and approval notifications.
NOVL_CONFIG_EMAILNOTIFYSECUREPROTOCOL=	Email: Notify Template Secure Port token.
NOVL_CONFIG_OCSPURI=	Miscellaneous: OCSP URI.
	If the client installation uses the On-Line Certificate Status Protocol (OCSP), supply a Uniform Resource Identifier (URI). For example, the format is `http://`*`hstport`*`/ocspLocal`. The OCSP URI updates the status of trusted certificates online.
NOVL_CONFIG_AUTHCONFIGPATH=	Miscellaneous: Authorization Config Path.
	The fully qualified name of the authorization configuration file.

User Application Parameter Name in silent.properties	Equivalent Parameter Name in the User Application Configuration Parameters File
NOVL_CONFIG_CREATEDIRECTORYINDEX	Miscellaneous:Create eDirectory Index Specify true if you want the silent installer to create indexes on the manager, ismanager, and srvprvUUID attributes on the eDirectory server specified in the NOVL_CONFIG_SERVERDN. If this parameter is set to true, NOVL_CONFIG_REMOVEEDIRECTORYINDEX cannot be set to true. For best performance results, the index creation should be complete. The indexes should be in Online mode before you make the User Application available.
NOVL_CONFIG_REMOVEDIRECTORYINDEX	Miscellaneous: Remove eDirectory Index Specify true if you want the silent installer to remove indexes on the server specified in the NOVL_CONFIG_SERVERDN. If this parameter is set to true NOVL_CONFIG_CREATEEDIRECTORYINDEX cannot be true.
NOVL_CONFIG_SERVERDN	Miscellaneous: Server DN Specify the eDirectory server where indexes should be created or removed.
NOVL_CREATE_DB	Indicates how the database will be created. Choices are: ◆ now - Creates the database right away. ◆ file - Writes SQL output to a file ◆ startup - Creates the database at application startup
NOVL_DATABASE_NEW	Indicates whether the database is new or existing. Specify *True* if it’s a new database. Specify *False* if it’s an existing database.
NOVL_RBPM_SEC_ADMINDN	Security Administrator This role gives members the full range of capabilities within the Security domain. The Security Administrator can perform all possible actions for all objects within the Security domain. The Security domain allows the Security Administrator to configure access permissions for all objects in all domains within the Roles Based Provisioning Module. The Security Administrator can configure teams, and also assign domain administrators, delegated administrators, and other Security Administrators.

User Application Parameter Name in silent.properties	Equivalent Parameter Name in the User Application Configuration Parameters File
NOVL_RBPM_RESOURCE_ADMINDN	Resources Administrator This role gives members the full range of capabilities within the Resource domain. The Resources Administrator can perform all possible actions for all objects within the Resource domain.
NOVL_RBPM_CONFIG_ADMINDN	This role gives members the full range of capabilities within the Configuration domain. The RBPM Configuration Administrator can perform all possible actions on all objects within the Configuration domain. The RBPM Configuration Administrator controls access to navigation items within the Roles Based Provisioning Module. In addition, the RBPM Configuration Administrator configures the delegation and proxy service, the provisioning user interface, and the workflow engine.
RUN_LDAPCONFIG=	Specifies when you want to configure LDAP settings now or later. Values are: ◆ Now - Executes the LDAP configure right away by populating the WAR with the LDAP configuration settings provided ◆ Later - Just installs the User Application files without configuring LDAP settings.

8.2.1 Setting Passwords in the Environment for a Silent Install

If you do not want to specify the passwords in the silent.properties file, you can set the passwords in the environment instead. In this case, the silent installer will read the passwords from the environment, rather than from the silent.properties file. This can provide some additional security.

The following passwords need to be set for the User Application Installer:

- NOVL_DB_USER_PASSWORD
- NOVL_CONFIG_DBADMIN_PASSWORD
- NOVL_CONFIG_LDAPADMINPASS
- NOVL_CONFIG_KEYSTOREPASSWORD

To set a password on Linux, use the `export` command, as shown in the following example:

```
export NOVL_DB_USER_PASSWORD=myPassWord
```

To set a password on Windows, use the `set` command, as shown in the following example:

```
set NOVL_DB_USER_PASSWORD=myPassWord
```

8.3 Running the JBossPostgreSQL Utility in Silent or Console Mode

You can run the JBossPostgreSQL utility in console or silent mode. Before running the utility in silent mode, you need to edit the properties file for the JBossPostgreSQL utility. Once you've edited the properties file, launch it with this command:

```
JBossPostgreSQL -i silent -f <path to the properties file>
```

For example:

```
JBossPostgreSQL -i silent -f /home/jdoe/idm-install-files/silent.properties
```

Here are the properties for a JBossPostgreSQL silent install:

Table 8-2 *JBossPostgreSQL Configuration Properties*

Property	Description
USER_INSTALL_DIR	Path to where you want JBoss and the JRE installed. Required if installing JBoss; otherwise, leave blank.
NOVL_DB_NAME	Name of the database to use. The default database name is idmuserappdb. Required if installing PostgreSQL. If you are not installing PostgreSQL, this value will be ignored.
NOVL_DB_PASSWORD	Database root password. Required if installing PostgreSQL. If you are not installing PostgreSQL, this value will be ignored.
NOVL_DB_PASSWORD_CONFIRM	Confirms the database root password. Required if installing PostgreSQL. If you are not installing PostgreSQL, this value will be ignored.

CHOSEN_INSTALL_FEATURE_LIST	Install sets to install.
	Required. You can choose both JBoss and PostgreSQL, or install just one of these products.
	Examples:
	`CHOSEN_INSTALL_FEATURE_LIST=JBoss, PostgreSQL`
	`CHOSEN_INSTALL_FEATURE_LIST=JBoss,""`

USER_MAGIC_FOLDER_1	Name of the installation directory for PostgreSQL. Required if installing PostgreSQL. This property will be ignored if CHOSEN_INSTALL_FEATURE_LIST does not include PostgreSQL.
START_DB	Indicates whether the installer will start the database at installation time. Assign the value Start if you want the installer to start the database; otherwise, leave this property blank. Optional.

JBossPostgreSQL installer might display a pop-up in silent mode on Windows PostgreSQL requires several Microsoft VC++ libraries when running on Windows. If these libraries are not installed on the Windows server, the PostgreSQL installer automatically installs them. When you run the JBossPostgreSQL installer in silent mode on Windows, a pop-up window appears for about three seconds while these libraries are being installed, if those libraries are not already installed on the machine.

8.3.1 Setting Passwords in the Environment for a Silent Install

If you do not want to specify the passwords in the silent.properties file, you can set the passwords in the environment instead. In this case, the silent installer will read the passwords from the environment, rather than from the silent.properties file. This can provide some additional security.

The following passwords need to be set for the User Application Installer:

- NOVL_DB_PASSWORD
- NOVL_DB_USER_PASSWORD

To set a password on Linux, use the `export` command, as shown in the following example:

```
export NOVL_DB_USER_PASSWORD=myPassWord
```

To set a password on Windows, use the `set` command, as shown in the following example:

```
set NOVL_DB_USER_PASSWORD=myPassWord
```

8.4 Running the RIS Installer in Silent or Console Mode

This release ships with a separate installer that you can use to configure the Rest Information Services (RIS) facility. This facility configures the `RIS.war` file, which supports REST resources. The REST resources exposed through RIS make SOAP calls to gather information from various RBPM systems.

You can run the RIS installer in console or silent mode. Before running the installer, you need to edit the properties file for the RIS installer. Once you've edited the properties file, launch it with this command:

```
RisWarUpdate -i silent -f <path to the properties file>
```

For example:

```
RisWarUpdate -i silent -f /home/jdoe/idm-install-files/silent.properties
```

The installer requires the following information:

- Where `RIS.war` is located
- Which port the User Application is configured to run on
- What context has been defined for the User Application
- What host name `RIS.war` will be installed on

Here are the properties for an RIS install:

Table 8-3 RIS Configuration Properties

Property	Description
NOVL_INSTALL_HOST	Name of the host where RIS.war will be installed. This name cannot be localhost. Required.
NOVL_USERAPP_PORT	Port on which the RBPM User Application is configured to run. Required.
NOVL_CONTEXT_NAME	Context name for the User Application. Required.
RIS_INSTALL_DIRECTORY	Directory in which RIS.war is located. Required.
RIS_WAR_FILE	Name of the RIS.war file. Do not change this value.
RIS_INSTALL_LOG	Name of the log file for the installer. You can name the file whatever you like. The installer writes the file to the location specified in the RIS_INSTALL_DIR property. If you leave this property blank, the default log file is RIS-Install.log. Optional.

9 Post-Installation Tasks

This section describes post-installation tasks. Topics include:

9.1 Recording the Master Key

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

NOTE: If you installed the User Application from the console, the installation program did not automatically create the `master-key.txt` file. Instead, you must manually copy the master key from the `/opt/novell/idm/jboss/server/IDMProv/conf/sys-configuration-xmldata.xml` file.

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.

9.2 Configuring the User Application

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

- "Configuring the User Application Environment," in the *User Application: Administration Guide*.
- The *User Application: Design Guide*

9.2.1 Setting up Logging

To configure logging, follow the directions in "Setting Up Logging," in the *User Application: Administration Guide*.

9.3 Configuring eDirectory

- Section 9.3.1, "Creating Indexes in eDirectory," on page 116
- Section 9.3.2, "Installing and Configuring SAML Authentication Method," on page 116

9.3.1 Creating Indexes in eDirectory

To improve User Application performance, the eDirectory Administrator should create indexes for the manager, ismanager and srvprvUUID attributes. Without indexes on these attributes, User Application users can experience impeded performance, particularly in a clustered environment.

These indexes can be created automatically during installation if you select *Create eDirectory Indexes* on the *Advanced* tab of the User Application Configuration Panel (described in Table A-2 on page 125), or refer to the *Novell eDirectory Administration Guide* (https://www.netiq.com/documentation/edir88/) for directions on using Index Manager to create indexes.

9.3.2 Installing and Configuring SAML Authentication Method

This configuration is only required if you want to use the SAML authentication method and are not also using Access Manager. If you are using Access Manager, your eDirectory tree will already include the method. The procedure includes:

❒ Installing the SAML Method in your eDirectory tree.

❒ Editing eDirectory attributes using iManager

Installing the SAML method in your eDirectory tree

1 Locate then unzip the `nmassaml.zip` file.

2 Install the SAML methods into your eDirectory tree:

2a Extend the schema stored in `authsaml.sch`. Refer to "Extending the eDirectory Schema for Roles Based Provisioning Module" on page 44 for more information. If eDirectory is installed on Linux, you can use the following command to extend the schema:

```
ndssch -h edir_ip edir_admin authsaml.sch
```

2b Install the SAML method. Refer to "How to Install NMAS Method" (https://www.netiq.com/documentation/nmas33/admin/data/a49tuwk.html), in the *Novell Modular Authentication Services Administration Guide* (https://www.netiq.com/documentation/nmas33/admin/data/a20gkue.html), for more information. If eDirectory is installed on Linux, you can use the following command to install the method:

```
nmasinst -addmethod edir_admin tree ./config.txt
```

Editing eDirectory Attributes

1 Open iManager and go to *Roles and Tasks* > *Directory Administration* > *Create Object*.

2 Select *Show all object classes*.

3 Create a new object of class `authsamlAffiliate`.

4 Select `authsamlAffiliate`, then click *OK*. (You may name this object any valid name.)

5 To specify the Context, select the *SAML Assertion.Authorized Login Methods.Security* container object in the tree, then click *OK.*

6 You must add attributes to the class object `authsamlAffiliate`.

   6a Go to the iManager *View Objects* > *Browse* tab and find your new affiliate object in the SAML Assertion.Authorized Login Methods.Security container.

   6b Select the new affiliate object, then select *Modify Object*.

   6c Add an *authsamlProviderID* attribute to the new affiliate object. This attribute is used to match an assertion with its affiliate. The contents of this attribute must be an exact match with the Issuer attribute sent by the SAML assertion.

   6d Click the *OK*.

   6e Add *authsamlValidBefore* and *authsamlValidAfter* attributes to the affiliate object. These attributes define the amount of time, in seconds, around the *IssueInstant* in an assertion when the assertion is considered valid. A typical default is 180 seconds.

   6f Click *OK*.

7 Select the Security container, then select *Create Object* to create a *Trusted Root Container* in your Security Container.

8 Create a *Trusted Root* objects in the Trusted Root Container.

   8a Return to *Roles and Tasks* > *Directory Administration* then select *Create Object*.

   8b Select *Show all object classes* again.

   8c To create a *Trusted Root* object for the certificate that your affiliate will use to sign assertions. You must have a der encoded copy of the certificate to do this.

   8d Create new trusted root objects for each certificate in the signing certificate's chain up to the root CA certificate.

   8e Set the Context to the Trusted Root Container created earlier, then click *OK*.

9 Return to the Object Viewer.

10 Add an *authsamlTrustedCertDN* attribute to your affiliate object, then click *OK*.

   This attribute should point to the "Trusted Root Object" for the signing certificate that you created in the previous step. (All assertions for the affiliate must be signed by certificates pointed to by this attribute, or they will be rejected.)

11 Add an *authsamlCertContainerDN* attribute to your affiliate object, then click *OK*.

   This attribute should point to the "Trusted Root Container" that you created before. (This attribute is used to verify the certificate chain of the signing certificate.)

9.4 Reconfiguring the User Application WAR File after Installation

To update your WAR file, you can run the configupdate utility as follows:

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

   For information on ConfigUpdate utility parameters, see Section A.1, "User Application Configuration: Basic Parameters," on page 123, Table 8-1 on page 102.

2. Deploy the new WAR file to your application server.

   For WebLogic and WebSphere, redeploy the WAR file to the application server. For JBoss single server, the changes are applied to the deployed WAR. If you are running in a JBoss cluster, the WAR file needs to be updated in each JBoss server in the cluster.

9.5 Configuring External Forgot Password Management

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 9.5.1, "Specifying an External Forgot Password Management WAR," on page 118
- Section 9.5.2, "Specifying an Internal Password WAR," on page 119
- Section 9.5.3, "Testing the External Forgot Password WAR Configuration," on page 119
- Section 9.5.4, "Configuring SSL Communication between JBoss Servers," on page 119

9.5.1 Specifying an External Forgot 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:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp.` An external password WAR can be outside the firewall protecting the User Application.

4. For the *Forgot Password Return Link*, specify the link shown after the user finishes performing the forgot password procedure. When the user clicks this link, the user is redirected to the link specified.
5. For the *Forgot Password Web Service URL*, supply the URL for the Web Service that the external forward password WAR uses to call back to the User Application. The format must URL is as follows: `https://<idmhost>:<sslport>/<idm>/pwdmgt/service`.

   The return link must use SSL to ensure secure Web Service communication to the User Application. See also Section 9.5.4, "Configuring SSL Communication between JBoss Servers," on page 119.

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

9.5.2 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*.

9.5.3 Testing the External Forgot Password WAR Configuration

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:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp`.
- At the User Application login page, click the *Forgot Password* link.

9.5.4 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 External Forgot Password Management WAR file. Refer to your JBoss documentation for directions.

9.6 Updating Forgot Password Settings

You can change the values of *Forgot Password Link*, *Forgot Password Return Link*, and *Forgot Password Web Service URL* 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:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp`)
- *Forgot Password Return Link* (for example: `http://localhost/IDMProv`)
- *Forgot Password Web Service URL* (for example: `https://`*`<idmhost>`*`:`*`<sslport>`*`/`*`<idm>`*`/pwdmgt/service`)

9.7 Security Considerations

During the installation process, the install program writes log files to the installation directory. These files contain information about your configuration. Once your environment is configured, you should consider deleting these log files or storing them in a secure location.

During the installation process, you may choose to write the database schema to a file. Since this file contains descriptive information about your database, you should move to a secure location after the installation process is complete.

9.8 Increasing the Identity Manager Java Heap Size

In an enterprise environment, the Role and Resource Service driver will require more maximum Java heap than the default amount defined in Identity Manager. A maximum Java heap size of 256mb is suggested in order to avoid OutOfMemoryError conditions.

The Java heap size can be specified via iManager under the Misc section of the Driver Set properties or by setting the DHOST_JVM_INITIAL_HEAP and DHOST_JVM_MAX_HEAP environment variables. See the Identity Manager Common Driver Administration Guide (http://www.netiq.com/documentation/idm402/idm_common_driver/index.html?page=/documentation/idm402/idm_common_driver/data/front.html) for more information on configuring Java VM options.

9.9 Troubleshooting

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

Issue	Suggested Actions

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

Exceptions are thrown when application server starts up, with a log message `port 8180 already in use`.	Shut down any instances of Tomcat (or other server software) that might already be running. If you decide to reconfigure the application server to use a port other than 8180, remember to edit the `config` settings for the User Application driver.
When the application server starts, you see a message that no trusted certificates were found.	Make sure that you start application server by using the JDK specified in the installation of the User Application.
You can't log into the portal admin page.	Make sure that the User Application Administrator account exists. Don't confuse this with your iManager admin account. They are two different admin objects (or should be).
You can log in as admin, but you can't create new users.	The User Application Administrator must be a trustee of the top container and needs to have Supervisor rights. As a stopgap, you can try setting the User Application Administrator's rights equivalent to the LDAP Administrator's rights (using iManager).

Issue	Suggested Actions
You encounter keystore errors when starting the application server.	Your application server is not using the JDK specified at the installation of the User Application. Use the `keytool` command to import the certificate file: `keytool -import -trustcacerts -alias aliasName -file certFile -keystore ..\lib\security\cacerts -storepass changeit` ◆ Replace *aliasName* with a unique name of your choice for this certificate. ◆ Replace *certFile* with the full path and name of your certificate file. ◆ The default keystore password is `changeit` (if you have a different password, specify it).

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

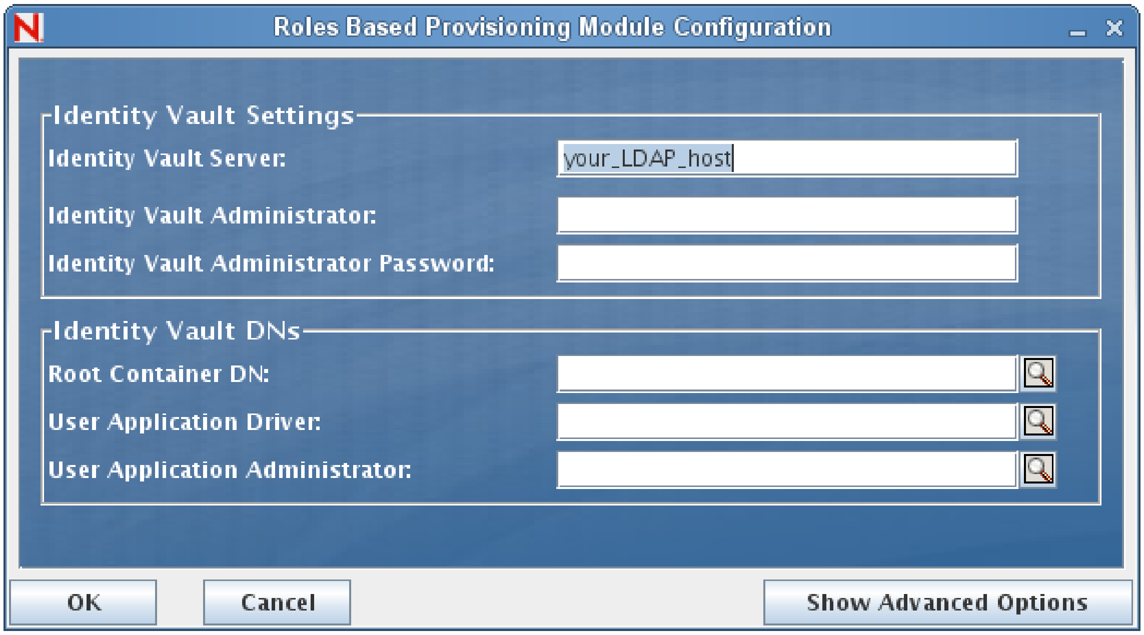
A User Application Configuration Reference

This section describes the options to supply values for during User Application installation or a configuration update.

- Section A.1, "User Application Configuration: Basic Parameters," on page 123
- Section A.2, "User Application Configuration: All Parameters," on page 125

A.1 User Application Configuration: Basic Parameters

Figure A-1 User Application Configuration Basic Options



Roles Based Provisioning Module Configuration

Identity Vault Settings

Identity Vault Server: your_LDAP_host

Identity Vault Administrator:

Identity Vault Administrator Password:

Identity Vault DNs

Root Container DN:

User Application Driver:

User Application Administrator:

Table A-1 *User Application Configuration Basic Options*

Type of Setting	Option	Description
Identity Vault Settings	*Identity Vault Server*	Required. Specify the hostname or IP address for the server that is hosting the User Application Driver. For example: `myLDAPhost`
	Identity Vault Administrator	Required. Specify the credentials for the LDAP Administrator. This user must already exist. The User Application uses this account to make an administrative connection to the Identity Vault. This value is encrypted, based on the master key. You can use configupdate utility to modify this setting as long as you have not modified it using the User Application's Administration tab.
	Identity Vault Administrator Password	Required. Specify the LDAP Administrator password. This password is encrypted, based on the master key. You can use configupdate utility to modify this setting as long as you have not modified it using the User Application's Administration tab.
Identity Vault DNs	*Root Container DN*	Required. Specify the LDAP distinguished name of the root container. This is used as the default entity definition search root when no search root is specified in the directory abstraction layer.
	User Application Driver DN	Required. Specify the distinguished name of the User Application driver. For example, if your driver is UserApplicationDriver and your driver set is called myDriverSet, and the driver set is in a context of o=myCompany, you would type a value of: `cn=UserApplicationDriver,cn=myDriverSet, o=myCompany`
	User Application Administrator	Required. An existing user in the Identity Vault who has the rights to perform administrative tasks for the User Application user container specified. This user can use the *Administration* tab of the User Application to administer the portal. If the User Application Administrator participates in workflow administration tasks exposed in iManager, Novell Designer for Identity Manager, or the User Application (*Requests & Approvals* tab), you must grant this administrator appropriate trustee rights to object instances contained in the User Application driver. Refer to the *User Application: Administration Guide* for details. To change this assignment after you deploy the User Application, you must use the *Administration* > *Security* pages in the User Application. You cannot change this setting via configupdate if you have started the application server hosting the User Application.
	RBPM Context name	Displays the current context name.
	RBPM Reporting Admin	Points to the Reporting Administrator. By default, the installer sets this value to the same user as the other security fields.

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.

A.2 User Application Configuration: All Parameters

This table includes the configuration parameters available when you click *Show Advanced Options*.

Table A-2 *User Application Configuration: All Options*

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

Type of Setting	Option	Description
Identity Vault DNs	*Root Container DN*	Required. Specify the LDAP distinguished name of the root container. This is used as the default entity definition search root when no search root is specified in the directory abstraction layer.
	User Application Driver DN	Required. Specify the distinguished name of the User Application driver. For example, if your driver is UserApplicationDriver and your driver set is called myDriverSet, and the driver set is in a context of o=myCompany, you type a value of: `cn=UserApplicationDriver,cn=myDriverSet, o=myCompany`
	User Application Administrator	Required. An existing user in the Identity Vault who has the rights to perform administrative tasks for the User Application user container specified. This user can use the *Administration* tab of the User Application to administer the portal. If the User Application Administrator participates in workflow administration tasks exposed in iManager, Novell Designer for Identity Manager, or the User Application (*Requests & Approvals* tab), you must grant this administrator appropriate trustee rights to object instances contained in the User Application driver. Refer to the *User Application: Administration Guide* for details. To change this assignment after you deploy the User Application, you must use the *Administration* > *Security* pages in the User Application. You cannot change this setting via configupdate if you have started the application server hosting the User Application.
	Provisioning Administrator	The Provisioning Administrator manages Provisioning Workflow functions available throughout the User Application. This user must exist in the Identity Vault prior to being designated the Provisioning Administrator. To change this assignment after you deploy the User Application, use the *Administration* > *Administrator Assignments* page in the User Application.
	Compliance Administrator	The Compliance Administrator is a system role that allows members to perform all functions on the *Compliance* tab. This user must exist in the Identity Vault prior to being designated as the Compliance Module Administrator. During a configupdate, changes to this value only take effect if you do not have a valid Compliance Administrator assigned. If a valid Compliance Administrator exists, then your changes are not saved. To change this assignment after you deploy the User Application, use the *Administration* > *Administrator Assignments* page in the User Application.

Type of Setting	Option	Description
	Roles Administrator	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. To change this assignment after you deploy the User Application, use the *Administration > Administrator Assignments* page in the User Application. During a configupdate, changes to this value only take effect if you do not have a valid Roles Administrator assigned. If a valid Roles Administrator exists, then your changes are not saved.
	Security Administrator	This role gives members the full range of capabilities within the Security domain. The Security Administrator can perform all possible actions for all objects within the Security domain. The Security domain allows the Security Administrator to configure access permissions for all objects in all domains within the Roles Based Provisioning Module. The Security Administrator can configure teams, and also assign domain administrators, delegated administrators, and other Security Administrators. To change this assignment after you deploy the User Application, use the *Administration > Administrator Assignments* page in the User Application.
	Resources Administrator	This role gives members the full range of capabilities within the Resource domain. The Resources Administrator can perform all possible actions for all objects within the Resource domain. To change this assignment after you deploy the User Application, use the *Administration > Administrator Assignments* page in the User Application.
	RBPM Configuration Administrator	This role gives members the full range of capabilities within the Configuration domain. The RBPM Configuration Administrator can perform all possible actions on all objects within the Configuration domain. The RBPM Configuration Administrator controls access to navigation items within the Roles Based Provisioning Module. In addition, the RBPM Configuration Administrator configures the delegation and proxy service, the provisioning user interface, and the workflow engine. To change this assignment after you deploy the User Application, use the *Administration > Administrator Assignments* page in the User Application.
	RBPM Reporting Admin	Points to the Reporting Administrator. By default, the installer sets this value to the same user as the other security fields.
	Reinitialize RBPM Security	Check box that allows you to reset security.
	IDMReport URL	URL that points to the user interface for the Identity Reporting Module.

Type of Setting	Option	Description
Identity Vault User Identity	*User Container DN*	Required. Specify the LDAP distinguished name (DN) or fully qualified LDAP name of the user container. Users in this container (and below) are allowed to log in to the User Application. You cannot change this setting via configupdate if you have started the application server hosting the User Application. **IMPORTANT:** Be sure the User Application Administrator specified during User Application driver set up exists in this container if you want that user to be able to execute workflows.
	User Container Scope	This defines the search scope for users.
	User Object Class	The LDAP user object class (typically inetOrgPerson).
	Login Attribute	The LDAP attribute (for example, CN) that represents the user's login name.
	Naming Attribute	The LDAP attribute used as the identifier when looking up users or groups. This is not the same as the login attribute, which is used only during login, and not during user/group searches.
	User Membership Attribute	Optional. The LDAP attribute that represents the user's group membership. Do not use spaces in this name.
Identity Vault User Groups	*Group Container DN*	Required. Specify the LDAP distinguished name (DN) or fully qualified LDAP name of the group container. Used by entity definitions within the directory abstraction layer. You cannot change this setting via configupdate if you have started the application server hosting the User Application.
	Group Container Scope	This defines the search scope for groups.
	Group Object Class	The LDAP group object class (typically groupofNames).
	Group Membership Attribute	The attribute representing the user's group membership. Do not use spaces in this name.
	Use Dynamic Groups	Select this option if you want to use dynamic groups.
	Dynamic Group Object Class	The LDAP dynamic group object class (typically dynamicGroup).

Type of Setting	Option	Description
Identity Vault Certificates	*Keystore Path*	Required. Specify the full path to your keystore (`cacerts`) file of the JRE that the application server application server is using to run, or else click the small browser button and navigate to the `cacerts` file. The User Application installation modifies the keystore file. On Linux or Solaris, the user must have permission to write to this file. **WebSphere note** The keystore path field needs to be set to the installation directory of RBPM, not the location of the JDK cacerts file as in JBoss installations. The default value is set to the correct location.
	Keystore Password	Required. Specify the `cacerts` password. The default is `changeit`.
	Confirm Keystore Password	
Trusted Key Store	*Trusted Store Path*	The Trusted Key Store contains all trusted signers' certificates. If this path is empty, the User Application gets the path from System property `javax.net.ssl.trustStore`. If the path isn't there, it is assumed to be `jre/lib/security/cacerts`.
	Trusted Store Password	If this field is empty, the User Application gets the password from System property `javax.net.ssl.trustStorePassword`. If the value is not there, `changeit` is used. This password is encrypted, based on the master key.
	Keystore Type JKS	Indicates what type of digital signing you want to use. If this field is checked, this indicates that the trusted store path is of type JKS.
	Keystore Type PKCS12	Indicates what type of digital signing you want to use. If this field is checked, this indicates that the trusted store path is of type PKCS12.
Novell Audit Digital Signature and Certificate Key		Contains the digital signature key and certificate for the audit service.
	Novell Audit Digital Signature Certificate	Displays the digital signature certificate for the audit service.
	Novell Audit Digital Signature Private Key	Displays the digital signature private key. This key is encrypted, based on the master key.
Access Manager Settings	*Simultaneous Logout Enabled*	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.
	Simultaneous Logout Page	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	Option	Description
Email Server Configuration	*NotificationTemplate HOST*	Specify the application server hosting the Identity Manager User Application. For example: `myapplication serverServer` This value replaces the $HOST$ token in e-mail templates. The URL that is constructed is the link to provisioning request tasks and approval notifications.
	Notification Template PORT	Used to replace the $PORT$ token in e-mail templates used in provisioning request tasks and approval notifications.
	Notification Template SECURE PORT	Used to replace the $SECURE_PORT$ token in e-mail templates used in provisioning request tasks and approval notifications.
	Notification Template PROTOCOL	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.
	Notification Template SECURE PROTOCOL	Refers to a secure protocol, HTTPS. Used to replace the $SECURE_PROTOCOL$ token in e-mail templates used in provisioning request tasks and approval notifications.
	Notification SMTP Email From:	Specify e-mail from a user in provisioning e-mail.
	SMTP Server Name:	Specify the SMTP e-mail host that provisioning e-mail is using. This can be an IP address or a DNS name.
Password Management		
	Use External Password WAR	This feature enables you to specify a Forgot Password page residing in an external Forgot Password WAR and a URL that the external Forgot Password WAR uses to call back the User Application through a Web service. If you select *Use External Password WAR*, you must supply values for *Forgot Password Link*, *Forgot Password Return Link*, and *Forgot Password Web Service URL*. If you do not select *Use External Password WAR,* Identity Manager uses the default internal Password Management functionality, `./jsps/pwdmgt/ForgotPassword.jsp` (without the http(s) protocol at the beginning). This redirects the user to the Forgot Password functionality built into the User Application, rather than to an external WAR.
	Forgot Password Link	This URL points to the Forgot Password functionality page. Specify a `ForgotPassword.jsp` file in an external or internal password management WAR.
	Forgot Password Return Link	Specify the *Forgot Password Return Link* so the user can click after performing a forgot password operation.

Type of Setting	Option	Description
	Forgot Password Web Service URL	This is the URL that the External Forgot Password WAR will use to call back to the User Application to perform core forgot password functionalities. The format of the URL is: `https://<idmhost>:<sslport>/<idm>/pwdmgt/service`
Miscellaneous	*Session Timeout*	The application session timeout.
	OCSP URI	If the client installation uses the On-Line Certificate Status Protocol (OCSP), supply a Uniform Resource Identifier (URI). For example, the format is http://host:port/ocspLocal. The OCSP URI updates the status of trusted certificates online.
	Authorization Config Path	Fully qualified name of the authorization configuration file.
	Create Identity Vault Index	Select this check box, if you want the installation utility to create indexes on the manager, ismanager, and srvprvUUID attributes. Without indexes on these attributes, User Application users can experience impeded performance of the User Application, particularly in a clustered environment. You can create these indexes manually by using iManager after you install the User Application. See Section 9.3.1, "Creating Indexes in eDirectory," on page 116. For best performance, the index creation should be complete. The indexes should be in Online mode before you make the User Application available.
	Remove Identity Vault Index	Removes indexes on manager, ismanager, and srvprvUUID attributes.
	Server DN	Select the eDirectory server where the indexes should be created or removed. **NOTE:** To configure indexes on multiple eDirectory servers, you must run the configupdate utility multiple times. You can only specify one server at a time.
Container Object	*Selected*	Select each Container Object Type to use.
	Container Object Type	Select from the following standard containers: locality, country, organizationalUnit, organization, and domain. You can also define your own containers in iManager and add them under *Add a new Container Object*.
	Container Attribute Name	Lists the Attribute Type name associated with the Container Object Type.
	Add a New Container Object: Container Object Type	Specify the LDAP name of an object class from the Identity Vault that can serve as a container.
	Add a New Container Object: Container Attribute Name	Supply the attribute name of the container object.