AUTHORIZED DOCUMENTATION

# User Application: Installation Guide

# Novell®
# Identity Manager Roles Based Provisioning Module

**3.6.1**

July 23, 2008

www.novell.com

## Legal Notices

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

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

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



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

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

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

## Novell Trademarks

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

## Third-Party Materials

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

# Contents

# About This Guide

This guide describes how to install the Novell® Identity Manager Roles Based Provisioning Module 3.6.1 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 Roles Based Provisioning Module, see the Identity Manager Documentation Web site (http://www.novell.com/documentation/lg/dirxmldrivers/index.html).

### Documentation Conventions

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

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

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

# Roles Based Provisioning Module Installation Overview

1

This section provides an overview of the steps for installing the Roles Based Provisioning Module. It can also assist you with additional installation and configuration of the User Application Standard Edition that is included with the Metadirectory Server installation. Topics include:



**What’s in the Standard Edition** The Standard Edition is the non-provisioning version of the User Application. It includes password self service and the identity portlets (Org Chart, Detail, and Directory Search), but does not provide support for workflows, roles, or attestation. The Standard Edition is a free version of the User Application that comes with a purchase of Identity Manager.

**What’s in the Roles Based Provisioning Module** The Roles Based Provisioning Module (RBPM) is the full version of the User Application. It includes support for workflows, roles, and attestation, as well as password self service and the identity portlets. The Roles Based Provisioning Module must be purchased separately.

If you are migrating from an earlier version of the User Application or Roles Based Provisioning Module, refer to the *User Application: Migration Guide* (http://www.novell.com/documentation/idmrbpm361/index.html)

## 1.1 Installation Checklist

To install the Novell® Identity Manager Roles Based Provisioning Module or the User Application Standard Edition, you must perform the following tasks:

- ❑ Verify that your software meets the system requirements. See Section 1.3, “System Requirements,” on page 11.
- ❑ Download the Identity Manager 3.6.1 Roles Based Provisioning Module. See Section 2.2, “Downloading the Roles Based Provisioning Module,” on page 17.
- ❑ 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 17.
  - ❑ Install and configure an application server. See Section 2.3, “Installing an Application Server,” on page 19.
  - ❑ Install and configure a database. See Section 2.4, “Installing a Database,” on page 21.

- ❑ If you are migrating from an earlier version of the User Application and continue to use the Identity Manager 3.5.1 metadirectory, perform the following tasks:
  - ❑ Run the Role Service and User Application Driver installation utility to extend the Identity Vault schema and install the required Role Service and User Application driver configuration files, and copy any additional files as necessary. For more information, see Section 2.6, "Installing Additional Files for Metadirectory 3.5.1," on page 23.

    **NOTE:** The Identity Manager 3.6 metadirectory runs the Role Service and User Application driver installation utility silently. This ensures that you have all of the necessary files.

  - ❑ Copy the contents of the `iManager_icons_for_roles.zip` to the correct iManager location. See Section 2.6.3, "Copying iManager Icons," on page 24.
  - ❑ Copy the `afadmin.jar` file to the correct location. See "Copying afadmin.jar" on page 25.
- ❑ Create the User Application driver in iManager or Designer for Identity Manager 3.0.
  - For iManager: Section 3.1, "Creating the User Application Driver in iManager," on page 27.
  - For Designer: User Application: Design Guide (http://www.novell.com/documentation/idmrbpm361/index.html).
- ❑ Create the Role Service driver in iManager or Designer for Identity Manager 3.0.
  - For iManager: Section 3.2, "Creating the Role Service Driver in iManager," on page 29.
  - For Designer: User Application: Design Guide (http://www.novell.com/documentation/idmrbpm361).
- ❑ Install and configure the Novell Identity Manager User Application or Roles Based Provisioning Module. (You must have the correct JDK* installed before you start the installation program. See Section 2.5, "Installing the Java Development Kit," on page 22.)

  You can launch the installation program in one of three modes:
  - Graphical user interface. See one of the following:
    - Chapter 4, "Installing on JBoss by Using the GUI Installer," on page 33.
    - Chapter 5, "Installing on a WebSphere Application Server by Using the GUI Installer," on page 41.
    - Chapter 6, "Installing on a WebLogic Application Server with the GUI Installer," on page 49.
  - Console (command line) interface. See Section 7.1, "Installing the User Application from the Console," on page 57.
  - Silent install. See Section 7.2, "Installing the User Application with a Single Command," on page 58.
- ❑ Carry out the post-installation tasks described in Chapter 8, "Post-Installation Tasks," on page 67.

## 1.2 About the Installer Program

The User Application installation program does the following:

- Designates an existing version of an application server to use.
- Designates an existing version of a database to use, for example MySQL*, Oracle*, DB2*, or Microsoft* SQL Server*. The database stores User Application data and User Application configuration information.
- Configures the JDK's certificates file so that the User Application (running on the application server) can communicate with the Identity Vault and the User Application driver securely.
- Configures and deploys the Java* Web Application Archive (WAR) file for the Novell Identity Manager User Application to the Application Server. On WebSphere* and WebLogic*, you must manually deploy the WAR.
- Enables Novell Audit logging or OpenXDAS logging if you select to do so.
- Enables you to import an existing master key to restore a specific Roles Based Provisioning Module installation and to support clusters.
- Migrates existing data from a 3.5.1 Provisioning Module or 3.6 Roles Based Provisioning Module to the required data format for 3.6.2.

## 1.3 System Requirements

To use the Novell Identity Manager Roles Based Provisioning Module 3.6.1, you must have one of each of the required components listed in Table 1-1.

***Table 1-1*** *System Requirements*

| Required System Component | System Requirements |
|---|---|
| Identity Manager 3.5.1 (Metadirectory System) | SUSE® Linux Enterprise Server (SLES) 10 with the latest Support Pack (both 32-bit and 64-bit are supported)<br>eDirectory™: 8.8.2<br>Security Services 2.0.5 (NMAS™ 3.1.3) |
| Identity Manager 3.6 (Metadirectory System) | One of the following operating systems:<br>◆ Windows Server* 2003 SP2 (32-bit)<br>◆ Linux Red Hat 5.0 (32-bit) with the latest support pack<br>◆ SLES* 10 SP2 (32-bit) with the latest support pack<br>◆ Solaris* 10<br>◆ AIX* 5L v5.3<br>◆ VMWare ESX<br>eDirectory 8.8.3 with IDM Metadirectory 3.,6.0 (32 bit only)<br>eDirectory 8.8.5 with IDM Metadirectory 3.6.1 (32 & 64 bit) |

| Required System Component | System Requirements |
|---|---|
| Web-based Administration Server<br>◆ iManager 2.6 and plug-ins (with Metadirectory 3.5.1 only)<br>◆ iManager 2.7 and plug-ins | One of the following operating systems:<br>◆ Novell Open Enterprise Server (OES) 1.0 on NetWare with the latest Support Pack<br>◆ Novell Open Enterprise Server 2.0<br>◆ NetWare 6.5 with the latest Support Pack<br>◆ Windows 2000 Server with the latest Service Pack (32-bit)<br>◆ Windows Server 2003 with the latest Service Pack (32-bit)<br>◆ Microsoft Windows Vista*<br>◆ Red Hat Linux 3.0, 4.0, or 5.0 ES or AS (both 32-bit and 64-bit are supported)<br>◆ Solaris 9 or 10 with latest Support Pack<br>◆ SUSE Linux Enterprise Server 9 or 10 with the latest Support Pack (both 32-bit and 64-bit are supported)<br>Operating systems supported via iManager Workstation:<br>◆ Windows 2000 Professional with the latest Service Pack<br>◆ Windows XP with SP2<br>◆ Windows Vista Ultimate and Business Editions (iManager 2.7 only)<br>◆ SUSE Linux Enterprise Desktop 10<br>◆ SUSE Linux 10.1<br>◆ openSUSE® 10.3 (iManager 2.7 only)<br>The following software:<br>◆ Novell iManager 2.6 or 2.7 with the latest Support Pack and plug-ins |

| Required System Component | System Requirements |
| --- | --- |
| Secure Logging Service<br>◆ The Secure Logging Server<br>◆ The Platform Agent (client component)<br>◆ Novell Audit 2.0.2 or Sentinel™ 5.1.3 or Sentinel 6.1 (Metadirectory 3.6 only) | For the Secure Logging Server, one of the following operating systems:<br>◆ Novell Open Enterprise Server 1.0 or 2.0 with the latest Support Pack<br>◆ NetWare 6.5 with the latest Support Pack<br>◆ Windows 2000 Server with the latest Service Pack (32-bit)<br>◆ Windows Server 2003 with the latest Service Pack (32-bit)<br>◆ Linux Red Hat Linux 3.0, 4.0, or 5.0 ES or AS (32-bit or 64-bit, although Novell Audit runs only in 32-bit mode)<br>◆ Solaris 9 or 10 with latest support pack<br>◆ SUSE Linux Enterprise Server 9 or 10 with the latest Support Pack (32-bit and 64-bit, although Novell Audit runs only in 32-bit mode)<br>◆ Novell eDirectory 8.7.3.6 or 8.8 with latest support pack (must be installed on the Secure Logging Server)<br>For the Platform Agent, one of the following operating systems:<br>◆ Novell Open Enterprise Server 1.0 SP1 or the latest Support Pack<br>◆ NetWare 6.5 with the latest Support Pack<br>◆ Windows 2000 or 2000 Server, XP, or Windows Server 2003 with the latest Service Pack (32-bit)<br>◆ Red Hat Linux 3 or 4 AS or ES (32-bit or 64-bit, although Novell Audit runs only in 32-bit mode)<br>◆ Solaris 8, 9, or 10<br>◆ SUSE Linux Enterprise Server 9 or 10 (32-bit and 64-bit, although Novell Audit runs only in 32-bit mode)<br>iManager 2.6 or 2.7 with the latest Support Pack and plug-ins |

| Required System Component | System Requirements |
|---|---|
| User Application Application Server | The User Application runs on JBoss*, WebSphere*, and WebLogic* as described below.<br><br>The User Application with JBoss 4.2.2 GA requires JRE* 1.5.0_15 and is supported on:<br><br>◆ Novell Open Enterprise Server (OES) 1.0 SP2 or the latest Support Pack--Linux only<br>◆ SUSE Linux Enterprise Server 9 SP2 (included in OES 1.0 SP2)<br>◆ SUSE Linux Enterprise Server 10 SP1 (32 bit or 64 bit)<br>◆ Windows 2003 Server with SP1 (64-bit and 32-bit)<br>◆ Solaris 10 Support Pack dated 6/06<br>◆ Red Hat Linux 5 (32-bit)<br><br>The User Application on WebSphere 6.1 requires the IBM JDK. The minimum fixpack level is 6.1.0.9 with the unrestricted policy files applied. It is supported on these platforms:<br><br>◆ Solaris 10 (64-bit)<br>◆ Windows 2003 SP1 (64-bit and 32-bit)<br><br>The User Application on WebLogic 10 requires JRockit* 1.5.0_06 and is supported on these platforms.<br><br>◆ Solaris 10 (32-bit or 64-bit)<br>◆ Windows 2003 SP1<br><br>The User Application also runs on VMWare ESX. |
| User Application Browser | The User Application supports both Firefox* and Internet Explorer*, as described below.<br><br>Firefox* 2 is supported on:<br><br>◆ Windows XP with SP2<br>◆ Windows Vista<br>◆ SUSE Linux 10.1<br>◆ SUSE Linux Enterprise Desktop 10<br>◆ openSUSE 10<br><br>Internet Explorer 7 is supported on:<br><br>◆ Windows XP with SP2<br>◆ Windows Vista Enterprise<br><br>Internet Explorer 6 SP1 is supported on:<br><br>◆ Windows XP with SP2 |

| Required System Component | System Requirements |
|---|---|
| Database Server for the User Application | The following databases are supported with JBoss:<br>◆ MySQL Version 5.0.51<br>◆ Oracle 9i (9.2.0.1.4)<br>◆ Oracle 10g Release 2 (10.2.0.1.0)<br>◆ MS SQL 2005 SP1<br>The following databases are supported with WebSphere:<br>◆ Oracle 10g Release 2 (10.2.0)<br>◆ MS SQL 2005 SP1<br>◆ DB2 DV2 v9.1.0.0<br>The following databases are supported with WebLogic:<br>◆ Oracle 10g Release 2 (10.2.0)<br>◆ MS SQL 2005 SP1<br>The following JDBC drivers are supported:<br>MS SQL Server Version 1.2.2828.100<br>Oracle thin driver: Oracle JDBC Driver Version 10.2.0.1.0<br>Oracle OCI driver: Oracle JDBC Driver Version 10.2.0.2.0<br>MySQL Connector/J 5.0.8<br>DB2 Driver Version 1.4.2 |
| Workstations<br>◆ Designer 3.0 for Identity Manager 3.6<br>◆ iManager Web access | Designer has been tested on the following platforms:<br>Windows:<br>◆ Windows XP SP2<br>◆ Microsoft Windows Vista<br>Linux:<br>◆ SUSE Linux Enterprise Server 10 (for Designer only)<br>◆ SUSE Linux Enterprise Desktop 10<br>◆ openSUSE 10 |
| Audit | Novell Audit 2.0.2 |
| OpenXDAS | OpenXDAS version 0.5.257 |
| User Application SSO integration | Requires Novell Access Manager 3.0.1 |

# Prerequisites

# 2

This section describes the software and components you must install or configure before you can install the Identity Manager Roles Based Provisioning Module or User Application Standard Edition. Topics include:



## 2.1 Installing the Identity Manager Metadirectory

The Roles Based Provisioning Module 3.6.1 can be used with the Identity Manager 3.5.1 or 3.6 metadirectory.

For instructions on installing Identity Manager 3.6 metadirectory, see *Novell Identity Manager 3.6 Installation Guide* (http://www.novell.com/documentation/idm36/).

If you have the Identity Manager 3.5.1 metadirectory, you must update several files before the Roles Based Provisioning Module 3.6.1 will work. For more information, see Section 2.6, “Installing Additional Files for Metadirectory 3.5.1,” on page 23. This is not necessary for the Identity Manager 3.6 metadirectory because the files are installed automatically as part of installation of the Identity Manager 3.6 metadirectory.

## 2.2 Downloading the Roles Based Provisioning Module

Obtain the Identity Manager Roles Based Provisioning Module 3.6.1 product from Novell Downloads (http://download.novell.com/index.jsp).Download the `.iso` image files for your product shown in Table 2-1.

***Table 2-1*** *The .iso Download Files*

| For this product | Download this .iso |
|---|---|
| Roles Based Provisioning Module | `Identity_ Manager_3_6_1_User_Application_Provisioning.iso` |
| User Application Standard Edition | `Identity_Manager_3_6_1_User_Application_NON_Provisioning.iso` |

If you have the Identity Manager 3.5.1 metadirectory, you must also download the `Roles_Driver_Install_Utility.iso`. You do not have to download the `Roles_Driver_Install_Utility.iso` if you are an Identity Manager 3.6 metadirectory user because the files included in this `.iso` are already part of the installation of the Identity Manager 3.6 metadirectory.

Table 2-2 describes the installation files from the Roles Based Provisioning Module or User Application Standard Edition `.iso` file.

***Table 2-2*** *Files and Scripts Delivered in the iso*

| File | Description |
|---|---|
| `IDMProv.war` | The Roles Based Provisioning Module WAR. It includes the Identity Manager 3.6.1 User Application with Identity Self-Service features and the Roles Based Provisioning Module. |
| `IDM.war` | The User Application Standard Edition WAR. It includes the Identity Manager 3.6.1 User Application, which supports the Identity Self-Service features. |
| `IDMUserApp.jar` | The Roles Based Provisioning Module and 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. |
| `JBossMySQL.bin` or `JBossMySQL.exe` | A convenience utility to install the JBoss application server and MySQL database. |
| `nmassaml.zip` | Contains an eDirectory method to support SAML. Only needed if you are not using Access Manager. |
| `afadmin.jar` | Required only for Identity Manager 3.5.1 Metadirectory. |
| `prerequisitefiles.zip` | Required only for Identity Manager 3.5.1 Metadirectory.<br><br>Contains other files that must be manually copied to the correct location. |

The system where you install the Identity Manager Roles Based Provisioning Module or User Application Standard Edition 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



## 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 11 for the supported version.
- Use the JBossMySQL utility provided with the Roles Based Provisioning Module download to install a JBoss Application Server (and optionally MySQL). For directions, see “Installing the JBoss Application Server and the MySQL Database” on page 19.

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 2-3*** *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 | 8080 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:<br>◆ Enable SSL for the JBoss servers on which you deploy the Identity Manager Roles Based Provisioning Module and `IDMPwdMgt.war` file.<br>◆ Ensure that the SSL port is open on your firewall.<br>For information on enabling SSL, see your JBoss documentation.<br>For information on the `IDMPwdMgt.war file`, see Section 8.5, “Configuring External Password Management,” on page 70 and also see the *User Application: Administration Guide* (http://www.novell.com/documentation/idmrbpm361/index.html). |

### Installing the JBoss Application Server and the MySQL Database

The JBossMySQL utility installs the JBoss Application Server and MySQL on your system. This utility does not support a console mode; it requires a graphical user interface environment. For Linux/Unix users, it is recommended that you install this as a non-root user.

1 Locate and execute `JBossMySQL.bin` or `JBossMySQL.exe` from the .iso.

`/linux/jboss/JBossMySQL.bin` (for Linux)

`/nt/jboss/JBossMySQL.exe` (for Windows)

The utility is not available for Solaris.

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.<br>• *JBoss*: Installs the JBoss Application server in the directory you specify along with scripts to start and stop it.<br>**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 20.<br>• *MySQL*: Installs MySQL and creates a MySQL 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 MySQL parent folder | Click *Choose* to select an installation folder other than the default. |
| MySQL Info | Specify the following:<br>• *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.<br>• *'root' user password* (and confirm password): Specify the root password (and confirm it) for this database. |
| PreInstallation Summary | Review the Summary page. If the specifications are correct, click *Install*. |

The utility displays a successful-completion message after it installs the products you selected. If you installed the MySQL database, continue to Section 2.4.1, "Configuring a MySQL Database," on page 21.

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

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

**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://wiki.jboss.org/wiki/Wiki.jsp?page=RunJBossAsAServiceOnWindows (http://wiki.jboss.org/wiki/Wiki.jsp?page=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://wiki.jboss.org/wiki/Wiki.jsp?page=JavaService (http://wiki.jboss.org/wiki/Wiki.jsp?page=JavaService).

### 2.3.2 Installing the WebLogic Application Server

If you plan to use the WebLogic Application Server 10, download and install it. See Section 1.3, “System Requirements,” on page 11 for information about the supported versions.

### 2.3.3 Installing the WebSphere Application Server

If you plan to use the WebSphere Application Server 6.1, download and install it. See Section 1.3, “System Requirements,” on page 11 for information about the supported versions.

## 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 or User Application, you must have one of the supported databases for your platform installed and configured. This includes:

- ❑ Installing your database and database driver.
- ❑ Creating a database or a database instance.
- ❑ Recording the following database parameters for use in the installation procedure for the Identity Manager Roles Based Provisioning Module:
  - host and port
  - database name, username, and user password
- ❑ Creating a datasource file that points to the database.

  The method varies according to your application server. For JBoss, the Identity Manager Roles Based Provisioning Module install program creates an application server datasource file pointing to the database and names the file based on the name of the Identity Manager Roles Based Provisioning Module WAR file. For WebSphere and WebLogic, configure the datasource manually prior to the install.
- ❑ Databases must be enabled for UTF-8.

---

**NOTE:** If you are migrating to a new version of the Roles Based Provisoining 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 Configuring a MySQL Database

The User Application requires certain configuration options for MySQL.If you install MySQL yourself, you configure these settings. If you install MySQL by using the JBossMySQL utility, the utility sets the correct values for you, but you need to know the values to maintain for the following:

- “INNODB Storage Engine and Table Types” on page 22
- “Character Set” on page 22
- “Case Sensitivity” on page 22

### INNODB Storage Engine and Table Types

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

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

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

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

### Character Set

Specify 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;connectionCollati
on=utf8_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.

## 2.5 Installing the Java Development Kit

The Roles Based Provisioning Module and User Application Standard Edition installation programs require that you use the Java 2 Platform Standard Edition Development Kit version 1.5. Version 1.6 is not supported.

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.

**NOTE:** For 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. You must use the Sun JDK.

# 2.6 Installing Additional Files for Metadirectory 3.5.1

If you use the Identity Manager metadirectory 3.5.1, you must perform the additional steps described in these sections:


- Section 2.6.1, “Installing the Role Service Driver by Using the GUI,” on page 23
- Section 2.6.2, “Installing the Role Service Driver from the Console,” on page 24
- Section 2.6.3, “Copying iManager Icons,” on page 24
- Section 2.6.4, “Copying afadmin.jar,” on page 25


For Linux/Unix users, install this as a root user.

## 2.6.1 Installing the Role Service Driver by Using the GUI

This is only required when you are using the Identity Manager 3.5.1 metadirectory. If you installed the Identity Manager 3.6 metadirectory, these files were already installed.

The Role Service and User Application driver installation utility provides options to do the following:

- Extend your Identity Vault schema to support the User Application and Roles Based Provisioning Module
- Install the Role Service driver and User Application driver configuration files to the metadirectory server.
- Install the Role Service and User Application driver configuration files to iManager.

You will have to run this installer on both the metadirectory and iManager machines.

**NOTE:** Your metadirectory must be installed in the default location to use this installer.

Access the `Roles_Driver_Install_Utility.iso`

1 Locate and execute the installer for your operating system:

| Operating System | Role Service Driver Installer |
|---|---|
| AIX | `roles_driver_install.aix.bin` |
| Linux | `roles_driver_install.linux.bin` |
| Solaris | `roles_driver_install.solaris.bin` |
| Windows | `roles_dirver_install.exe` |

2 Use the following information to complete the installation:

| Installation Screen | Description |
|---|---|
| License Agreement | Read the License Agreement, then select *I accept the terms of the License Agreement*. |
| Select Components | *Drivers*: Installs the Role Service driver and the User Application driver to the metadirectory server, and updates supporting library JARs.<br><br>*Schema*: Updates the metadirectory schema to include the objects needed for the Roles Based Provisioning Module and the User Application Standard Edition. It installs the `nrf-extensions.sch` file and the srvprv.sch file, and runs the command (`NdsCons.exe` for windows and `ndssch` for UNIX/Linux) for the current platform.<br><br>*Driver Configuration Files*: Installs the Role Service driver and User Application driver configuration files. These files are used when you create the new drivers in iManager. You must run this on the machine hosting iManager. |
| Authentication | When you select *Schema Extensions*, you must specify a username and password. This user must have administrative rights to the Identity Vault. For example, *cn=admin,o=novell*. |
| Select Location for Driver | If you selected to install the Role Service and User Application driver, you are prompted for the location on the eDirectory server. These are typically installed to the metadirectory's /lib/dirxml/classes directory. |
| Install Location for Driver Configuration Files | Specify where the installer should put the Driver Configuration files on the iManager machine. These are typically installed to the iManager's /nps/Dirxml.Drivers directory. |
| Pre-Installation Summary | Read the Pre-Install Summary page to verify your choices for the installation parameters and complete the installation. |

## 2.6.2 Installing the Role Service Driver from the Console

To run the installer in console (character) mode, issue the following command:

```
roles_driver_install_<operatingsystemfile> -i console
```

Follow the same steps described for the graphical user interface under Section 2.6.1, "Installing the Role Service Driver by Using the GUI," on page 23, reading the prompts and entering responses at the command line.

## 2.6.3 Copying iManager Icons

**NOTE:** This procedure is not necessary if you have installed iManager 2.7 along with the latest plug-ins.

1 In your downloaded `.iso` image, locate the `prerequisites.zip` file.

2 Unzip the file, then locate the `iManager_icons_for_roles.zip` file.

This contains the iManager icons for roles objects in the eDirectory.

3 Unzip the file, then copy the extracted icons to the `nps/portal/modules/dev/images/dir` directory.

4 Restart iManager so it uses the new icons.

## 2.6.4 Copying afadmin.jar

**NOTE:** This procedure is not necessary if you have installed iManager 2.7 along with the latest plug-ins.

1 In your downloaded `.iso` image, locate the `prerequisites.zip`.

You can find it in the `/36MetaDirSupport` directory.

2 Unzip the file, then locate the `afadmin.jar` file.

3 Copy the `afadmin.jar` file to the `/iManager/nps/WEB-INF/lib` directory.

# Creating Drivers

# 3

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



---

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

---

The driver configuration support allows you to do the following:

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

## 3.1 Creating the User Application Driver in iManager

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

You must create a separate User Application driver for each Identity Manager Roles Based Provisioning Module, except for Roles Based Provisioning Modules that are members of a cluster. Roles Based Provisioning Modules that are part of the same cluster must share a single User Application driver. For information on running the Roles Based Provisioning Module in a cluster, see the *User Application: Administration Guide* (http://www.novell.com/documentation/idmrbpm361/index.html).

---

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

---

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

1. Open iManager in a Web browser.

   Use iManager 2.6 (for Identity Manager 3.5.1) or iManager 2.7 (for Identity Manager 3.6).

2. Go to *Roles and Tasks* > *Identity Manager Utilities* and select *New Driver* or *Import Configuration* (depending on the version of the plug-ins you are using).

   For Identity Manager 3.5.1, use the *New Driver* link.

   For Identity Manager 3.6, use the *Import Configuration* link.

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

   or

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

**3a** Specify a name, a context, and a server for the new driver set. The context is the eDirectory™ context where the server object is located.

**3b** Click *Next*.

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

**5** Select the User Application driver configuration file from the drop-down list. The file name is:

*UserApplication_3_6_1-IDM3_5_1-V1.xml*

If this file is not in the list, the Role Service driver might not be installed correctly. Refer to Section 2.6.1, “Installing the Role Service Driver by Using the GUI,” on page 23.

**6** Click *Next*.

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

| Field | Description |
|---|---|
| *Driver Name* | The name of the driver you are creating. |
| *Authentication ID* | The distinguished name of the User Application Administrator. This is a User Application Administrator to whom you are giving rights to administer the User Application portal. Use the eDirectory™ format, for example admin.orgunit.novell, or browse to find the user. This is a required field. |
| *Password* | Password of the User Application Administrator specified in the Authentication ID. |
| *Application Context* | The User Application context. This is the context portion of the URL for the User Application WAR file. The default is *IDM*. |
| *Host* | The hostname or IP address of the application server where the Identity Manager User Application is deployed.<br><br>If the User Application is running in a cluster, type the dispatcher’s hostname or IP address. |
| *Port* | The port for the host you listed above. |
| *Allow Override Initiator:* | Select *Yes* to allow the Provisioning Administrator to start workflows in the name of the person for whom the Provisioning Administrator is designated as proxy. |

**8** Click *Next*.

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

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

**10** (Optional, but recommended) Click *Exclude Administrative Roles*.

**11** Click *Add*, select users you want to exclude for driver actions (such as administrative roles), click *OK* twice, then click *Next*.

12 Click *OK* to close the Security Equals window, then click *Next* to display the summary page.

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

---

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

---

# 3.2 Creating the Role Service Driver in iManager

---

**NOTE:** You do not need to perform the steps in this section if you are using the User Application Standard Edition.

---

To create and configure the Role Service driver in iManager:

1 Open iManager in a Web browser.

Use 2.6 (for Identity Manager 3.5.1) or iManager 2.7 (for Identity Manager 3.6).

2 Under *Identity Manager* > *Identity Manager Overview*, select the driver set where you want to install the Role Service driver.

Install the User Application driver before installing the Role Service driver. Use Version 3.6.1 of the User Application driver (`UserApplication_3_6_1-IDM3_5_1-V1.xml`) with the Role Service driver. If you use a different version of the User Application driver, the Roles Catalog is not available.

3 Click *Add Driver*.

4 In the wizard, keep the default of *In an existing driver set*. Click *Next*.

5 Select *RoleService_3_6_1-IDM3_5_1-V1.xml* from the drop-down list. This is the Role Service driver configuration file that supports the Roles Based Provisioning Module.

If it is not in this drop-down list, you did not copy this file to the correct location. Refer to Section 2.6.1, “Installing the Role Service Driver by Using the GUI,” on page 23.

Click *Next*.

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

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

If so, the iManager application might not have picked up your new Roles schema yet. The new schema is necessary for the Role Service driver. Try restarting iManager and eDirectory to ensure that all new schema changes are picked up properly.

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

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

7. After the information is filled in, click *Next*.
8. Click *Define Security Equivalences* to open the Security Equals window. Browse to and select an administrator or other Supervisor object, then click *Add*.

   This step gives the driver the security permissions it needs. Details about the significance of this step can be found in your Identity Manager documentation.
9. (Optional, but recommended) Click *Exclude Administrative Roles*.
10. Click *Add*, select users you want to exclude for driver actions (such as administrative roles), click *OK* twice, then click *Next*.

11 Click *OK* to close the Security Equals window, then click *Next* to display the summary page.

12 If the information is correct, click *Finish*.

# Installing on JBoss by Using the GUI Installer

# 4

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

- Section 4.1, “Installing and Configuring the User Application WAR,” on page 33
- Section 4.2, “Testing the Installation,” on page 39

If you prefer to use the command line for installation, see Chapter 7, “Installing from the Console or with a Single Command,” on page 57.

Run the installer as a non-root user.

**What’s in the Standard Edition WAR** The Standard Edition is the non-provisioning version of the User Application. It includes password self service and the identity portlets (Org Chart, Detail, and Directory Search), but does not provide support for workflows, roles, or attestation. The Standard Edition is a free version of the User Application that comes with a purchase of Identity Manager.

**What’s in the Roles Based Provisioning Module WAR** The Roles Based Provisioning Module (RBPM) is the full version of the User Application. It includes support for workflows, roles, and attestation, as well as password self service and the identity portlets. The Roles Based Provisioning Module must be purchased separately.

## 4.1 Installing and Configuring the User Application WAR

**NOTE:** The installation program requires the Java 2 Platform Standard Edition Development Kit version 1.5. If you use an earlier or later 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.

Be sure to use the version of the Sun JDK to start the User Application installer as follows:

**Linux/Solaris**

```
$ /opt/jdk1.5.0_10/bin/java -jar IdmUserApp.jar
```

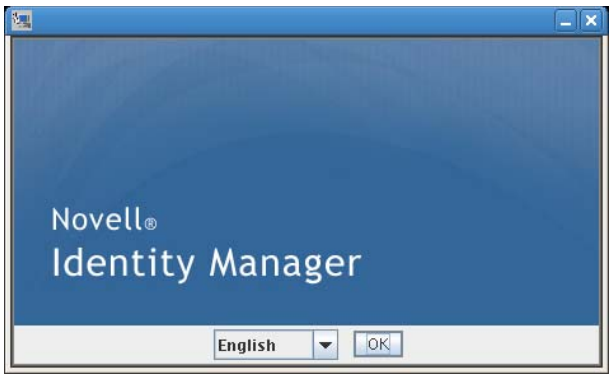
**Windows**

```
C:\Novell\InstallFiles\> "C:\Program Files\Java\jdk1.5.0_10\bin\java.exe"
-jar IdmUserApp.jar
```

When the installation procedure asks for the full path of your Java installation, provide the root path of the Sun JDK. For example, the root path on Linux could be `/opt/jkd1.5.0_10`.

**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.

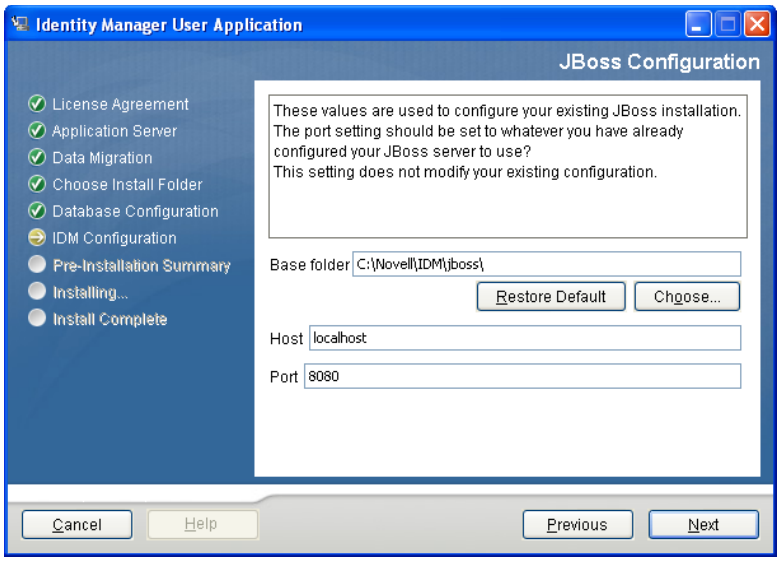



2 Use the following information along with the instructions on each installation panel to complete the installation:

| Installation Screen | Description |
|---|---|
| Novell Identity Manager | 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 *JBoss*. |
| Standard or Provisioning | *Standard*: Select this option if you are installing the User Application Standard Edition.<br><br>*Roles Based Provisioning*: Select this option if you are installing the Roles Based Provisioning Module. |
| Data Migration | Accept the default (verify that *Yes* is not selected).<br><br>**WARNING:** Do not select *Yes*, If Yes is selected, you will encounter problems starting the User Application.<br><br>For information on migrating, see the *User Application: Migration Guide* (http://www.novell.com/documentation/idmrbpm361/index.html). |
| Where is the WAR? | If the Identity Manager User Application WAR file is in a different directory from the installer, the installer prompts for the path to the WAR. |
| 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. Options include:<br>◆ MySQL<br>◆ Oracle (you are prompted for the Oracle version)<br>◆ MS SQL Server |

| Installation Screen | Description |
|---|---|
| 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.<br><br>*Port*: Specify the database's listener port number. For a cluster, specify the same port for each member of the cluster. |
| Database Name and Privileged User | *Database name* (or sid): For MySQL or MS SQL Server, provide the name of your preconfigured database. For Oracle, provide the Oracle System Identifier (SID) that you previously created. For a cluster, specify the same database name or SID for each member of the cluster.<br><br>*Database user*: Specify the database user. For a cluster, specify the same database user for each member of the cluster.<br><br>*Database password/Confirm password*: Specify the database password. For a cluster, specify the same database password for each member of the cluster. |
| Java Install | Specify the Java root install folder. |

You are prompted for information about where your JBoss application server is installed.

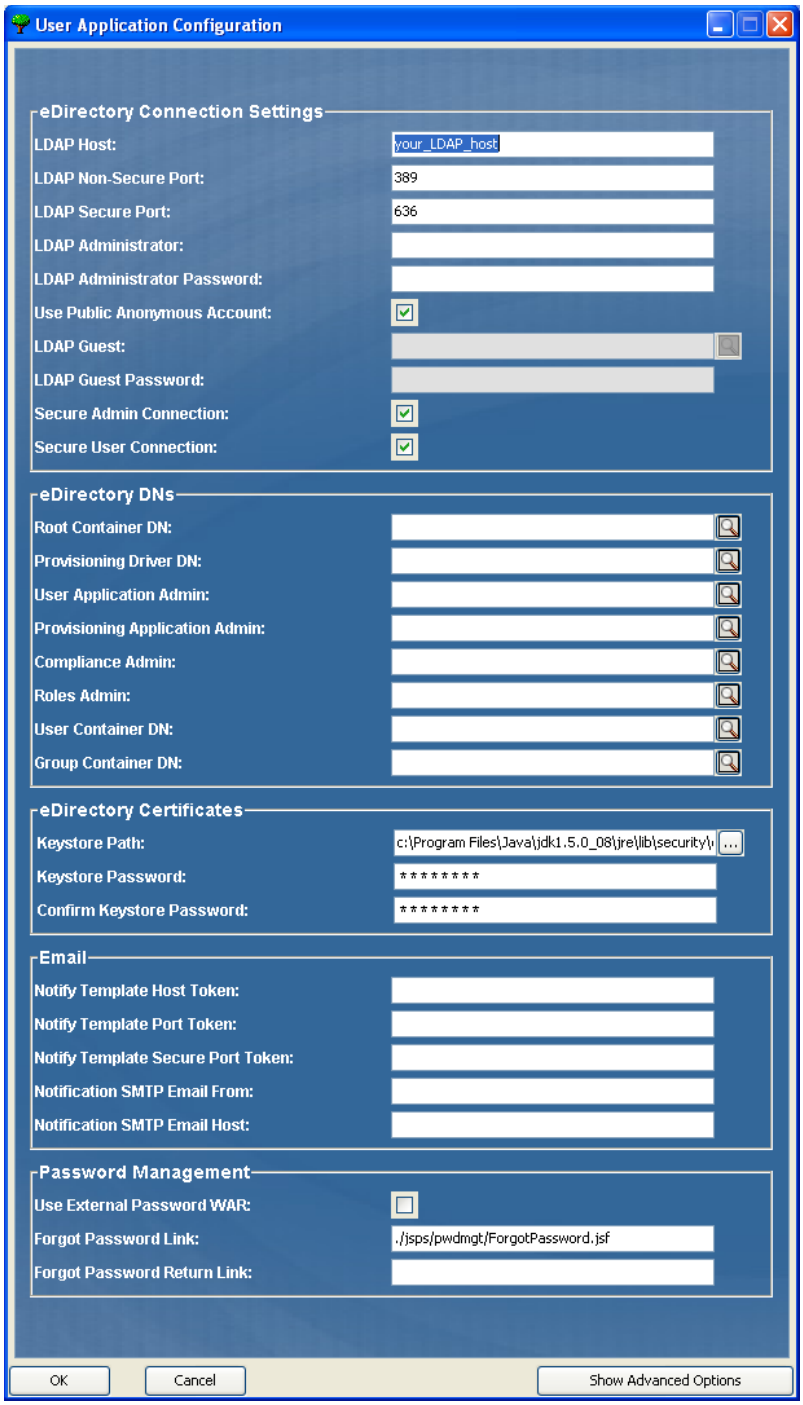



**3** Use the following information to complete this panel and to continue with the installation.

| Installation Screen | Description |
|---|---|
| JBoss Configuration | Tells the User Application where to find the JBoss Application Server.<br><br>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 MySQL Database” on page 19.<br><br>*Base folder*: Specify the location of the application server.<br><br>*Host*: Specify the application server’s hostname or IP address.<br><br>*Port*: Specify the application server’s listener port number. The JBoss default port is 8080. |
| IDM Configuration | Select the type of application server configuration:<br>◆ Select *all* if this installation is part of a cluster<br>◆ Select *default* if this installation is on a single node that is not part of a cluster<br>If you select *default* and decide you need a cluster later, then you must reinstall the User Application.<br><br>*Application name*: 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.<br><br>*Workflow Engine ID*: Each server in a cluster must have a unique Workflow Engine ID. Workflow Engine IDs are described in the *User Application: Administration Guide* in Section 3.5.4, “Configuring Workflows for Clustering”. |
| Audit Logging | To enable logging, click *Yes*. The next panel prompts you to specify the type of logging. Choose from the following options:<br>◆ *Novell Audit*: Enables Novell® Audit Logging for the User Application.<br>◆ *OpenXDAS*: Events are logged to your OpenXDAS logging server.<br><br>For more information on setting up Novell Audit or OpenXDAS logging, see the *User Application: Administration Guide*. |
| Novell Audit | *Server*: If you enable Novell Audit logging, specify the hostname or IP address for the Novell Audit server. If you turn logging off, this value is ignored.<br><br>*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.<br><br>*No*: Creates a new master key. After you finish the installation, you must manually record the master key as described in Section 8.1, "Recording the Master Key," on page 67.<br><br>The installation procedure writes the encrypted master key to the `master-key.txt` file in the installation directory.<br><br>Reasons to import an existing master key include:<br>◆ 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.<br>◆ 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).<br>◆ 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. |

**4** You are prompted for the information that the installation program uses to configure the User Application WAR file. (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 22.


User Application Configuration
eDirectory Connection Settings
LDAP Host:
your_LDAP_host
LDAP Non-Secure Port:
389
LDAP Secure Port:
636
LDAP Administrator:
LDAP Administrator Password:
Use Public Anonymous Account:
LDAP Guest:
LDAP Guest Password:
Secure Admin Connection:
Secure User Connection:
eDirectory DNs
Root Container DN:
Provisioning Driver DN:
User Application Admin:
Provisioning Application Admin:
Compliance Admin:
Roles Admin:
User Container DN:
Group Container DN:
eDirectory Certificates
Keystore Path:
c:\Program Files\Java\jdk1.5.0_08\jre\lib\security\
Keystore Password:
********
Confirm Keystore Password:
********
Email
Notify Template Host Token:
Notify Template Port Token:
Notify Template Secure Port Token:
Notification SMTP Email From:
Notification SMTP Email Host:
Password Management
Use External Password WAR:
Forgot Password Link:
./jsps/pwdmgt/ForgotPassword.jsf
Forgot Password Return Link:
OK
Cancel
Show Advanced Options

5 Use the following information to complete the panel and continue with the installation.

| Installation Screen | Description |
|---|---|
| User Application Configuration | 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.<br><br>For a cluster, specify identical User Application configuration parameters for each member of the cluster.<br><br>See Appendix A, "IDM User Application Configuration Reference," on page 75 for a description of each option. |
| Pre-Installation Summary | Read the Pre-Installation Summary page to verify your choices for the installation parameters.<br><br>If necessary, use *Back* to return to earlier installation pages to change installation parameters.<br><br>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. |

### 4.1.1 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.

## 4.2 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):

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

`start-jboss.bat` (Windows)

To stop the application server, use `stop-jboss.sh` or `stop-jboss.bat`, or close the window in which `start-jboss.sh` or `start-jboss.bat` is running.

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

```
JAVA_OPTS="-Djava.awt.headless=true -server -Xms256M -Xmx256M
```

```
-XX:MaxPermSize=256m"
```

3 Start the User Application driver. This enables communication to the User Application driver.

**3a** Log into iManager.

**3b** In the Roles and Tasks display in the left navigation frame, select *Identity Manager Overview* under *Identity Manager*.

**3c** In the content view that appears, specify the driver set that contains the User Application driver, then click *Search*. A graphic appears, showing the driver set with its associated drivers.

**3d** Click the red and white icon on the driver.

**3e** Select *Start Driver*. The driver status changes to the yin-yang symbol, indicating that the driver is now started.

The driver, upon starting, attempts a "handshake" with the User Application. If your application server isn't running or if the WAR wasn't successfully deployed, the driver returns an error.

4 To launch and log in to the User Application, use your Web browser to go to the following URL:

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

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

The Novell Identity Manager User Application landing page appears.

5 In the upper right corner of that page, click *Login* to log in to the User Application.

If the Identity Manager User Application page does not appear in your browser after completing these steps, check the terminal console for error messages and refer to Section 8.7, "Troubleshooting," on page 71.

# Installing on a WebSphere Application Server by Using the GUI Installer

5

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



Run the installer as a non-root user.

## 5.1 Installing and Configuring the User Application WAR

**NOTE:** The installation program requires the Java 2 Platform Standard Edition Development Kit version 1.5. If you use an earlier or later 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 using the IBM Java environment, as shown below:

   **Solaris**

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

   **Windows**

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

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

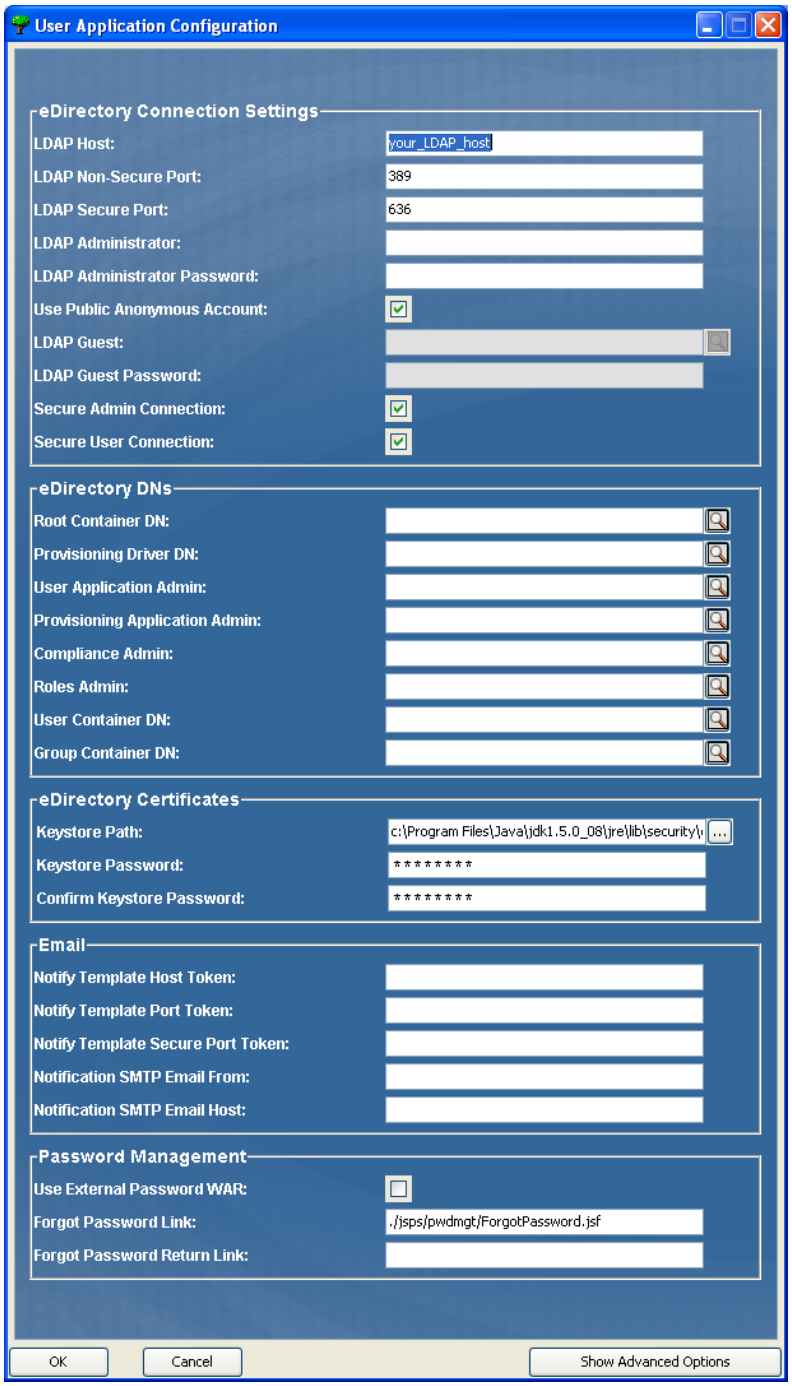
   When the installation program launches, you are prompted for the language.

**3** Use the following information along with the instructions on each installation panel to complete the installation:

| Installation Screen | Description |
|---|---|
| Novell Identity Manager | 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*.<br><br>If the User Application WAR file is in a different directory from the installer, the installer prompts for the path to the WAR.<br><br>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. |
| Standard or Provisioning | *Standard*: Select this option if you are installing the User Application Standard Edition.<br><br>*Roles Based Provisioning*: Select this option if you are installing the Roles Based Provisioning Module. |
| Data Migration | Accept the default (verify that *Yes* is not selected).<br><br>**WARNING:** Do not select *Yes*, If Yes is selected, you will encounter problems starting the User Application.<br><br>For information on migrating, see the *User Application: Migration Guide* (http://www.novell.com/documentation/idmrbpm361/index.html). |
| Where is the WAR? | If the Identity Manager User Application WAR file is in a different directory from the installer, the installer prompts for the path to the WAR. |
| 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. Options include:<br>◆ Oracle (you are prompted for the Oracle version)<br>◆ MS SQL Server<br>◆ DB2 |
| Java Install | Specify the Java root install folder.<br><br>**NOTE:** With WebSphere, you must use the IBM JDK that has the unrestricted policy files applied. |
| IDM Configuration | Specify the application context |

| Installation Screen | Description |
|---|---|
| Audit Logging | To enable logging, click *Yes*. the next panel prompts you to specify the type of logging. Choose from the following options:<br>◆ *Novell Audit*:: Enables Novell Audit Logging for the User Application. For more information on setting up Novell Audit logging, see the *Identity Manager User Application: Administration Guide*.<br>◆ *OpenXDAS*: Events are logged to your OpenXDAS logging server.<br>For more information on setting up Novell Audit or OpenXDAS logging, see the *User Application: Administration Guide*. |
| Novell Audit | *Server*: If you turn Novell Audit logging on, specify the hostname or IP address for the Novell Audit server. If you turn logging off, this value is ignored.<br>*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.<br>*No*: Creates a new master key. After you finish the installation, you must manually record the master key.<br>The installation procedure writes the encrypted master key to the `master-key.txt` file in the installation directory.<br>Examples of reasons to import an existing master key include:<br>◆ 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.<br>◆ 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).<br>◆ 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. |

**4** You are prompted for the information that the installation program uses to configure the User Application WAR file. (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 22.


User Application Configuration
eDirectory Connection Settings
LDAP Host:
your_LDAP_host
LDAP Non-Secure Port:
389
LDAP Secure Port:
636
LDAP Administrator:
LDAP Administrator Password:
Use Public Anonymous Account:
LDAP Guest:
LDAP Guest Password:
Secure Admin Connection:
Secure User Connection:
eDirectory DNs
Root Container DN:
Provisioning Driver DN:
User Application Admin:
Provisioning Application Admin:
Compliance Admin:
Roles Admin:
User Container DN:
Group Container DN:
eDirectory Certificates
Keystore Path:
c:\Program Files\Java\jdk1.5.0_08\jre\lib\security\
Keystore Password:
********
Confirm Keystore Password:
********
Email
Notify Template Host Token:
Notify Template Port Token:
Notify Template Secure Port Token:
Notification SMTP Email From:
Notification SMTP Email Host:
Password Management
Use External Password WAR:
Forgot Password Link:
./jsps/pwdmgt/ForgotPassword.jsf
Forgot Password Return Link:
OK
Cancel
Show Advanced Options

5 Use the following information to complete the panel and continue with the installation.

| Installation Screen | Description |
|---|---|
| User Application Configuration | 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.<br><br>For more information, see Appendix A, "IDM User Application Configuration Reference," on page 75. |
| Pre-Installation Summary | Read the Pre-Install Summary page to verify your choices for the installation parameters.<br><br>If necessary, use *Back* to return to earlier installation pages to change installation parameters.<br><br>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 installation is finished. |

### 5.1.1 Viewing Installation Log Files

If your installation completed without error, continue with Section 5.2.1, "Adding User Application Configuration Files and JVM System Properties," on page 45.

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 Configuring the WebSphere Environment



### 5.2.1 Adding User Application Configuration Files and JVM System Properties

The following steps are required for a successful WebSphere installation:

1 Copy the `sys-configuration-xmldata.xml` file from the User Application install directory to a directory on the machine hosting the WebSphere server, for example `/UserAppConfigFiles`.

The User Application install directory is the directory in which you installed the User Application.

2 Set the path to the `sys-configuration-xmldata.xml` file in the JVM system properties. Log in to the WebSphere admin console as an admin user to do this.

3 From the left panel, go to *Servers* > *Application Servers*

4 Click the server name in the server list, for example server1.

5 In the list of settings on the right, go to *Java and Process Management* under *Server Infrastructure*.

6 Expand the link and select *Process Definition*.

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

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

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

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

**9b** For the *Value*, specify the name of the install folder (directory) that you specified during installation.

The installer wrote the `sys-configuration-xmldata.xml` file to this folder.

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

**9d** Click *OK* to save the property.

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

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

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

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

**10d** Click *OK* to save the property.

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

## 5.2.2 Import 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 47) or through the command line ("Importing Certificates with the Command Line" on page 47).

3 After you import certificates, proceed to Section 5.3, "Deploying the WAR File," on page 47.

### Importing Certificates with the WebSphere Administrator's Console

1. Log in to the WebSphere administration console as an admin user.
2. From the left panel, go to *Security* > *SSL Certificate and Key Management*.
3. In the list of settings on the right, go to *Key stores and certificates* under *Additional Properties*.
4. Select *NodeDefaultTrustStore* (or the trust store you are using).
5. Under *Additional Properties* on the right, select *Signer Certificates*.
6. Click *Add*.
7. Type the Alias name and full path to the certificate file.
8. Change the Data type in the drop-down list to *Binary DER data*.
9. Click *OK*. You should now see the certificate in the list of signer certificates.

### 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.

## 5.3 Deploying the WAR File

Deploy the WAR file using the WebSphere deployment tools.

## 5.4 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`

# Installing on a WebLogic Application Server with the GUI Installer

6

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

- Section 6.1, “WebLogic Installation CheckList,” on page 49
- Section 6.2, “Installing and Configuring the User Application WAR,” on page 49
- Section 6.3, “Preparing the WebLogic Environment,” on page 53
- Section 6.4, “Deploying the User Application WAR,” on page 55
- Section 6.5, “Accessing the User Application,” on page 55

To learn about installing using a non-graphical user interface, see Chapter 7, “Installing from the Console or with a Single Command,” on page 57.

Run the installer as a non-root user.

## 6.1 WebLogic Installation CheckList

- ❑ Create a WebLogic-enabled WAR.

  Use the Identity Manager User Application installer to perform this task. See Section 6.2, “Installing and Configuring the User Application WAR,” on page 49.
- ❑ Prepare the WebLogic environment for the WAR’s deployment by copying configuration files to the appropriate WebLogic locations.

  See Section 6.3, “Preparing the WebLogic Environment,” on page 53.
- ❑ Deploy the WAR.

  See Section 6.4, “Deploying the User Application WAR,” on page 55.

## 6.2 Installing and Configuring the User Application WAR

---

**NOTE:** The installation program requires the Java 2 Platform Standard Edition Development Kit version 1.5. If you use an earlier or later 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 the installer for your platform from the command line, using the JRockit Java environment:

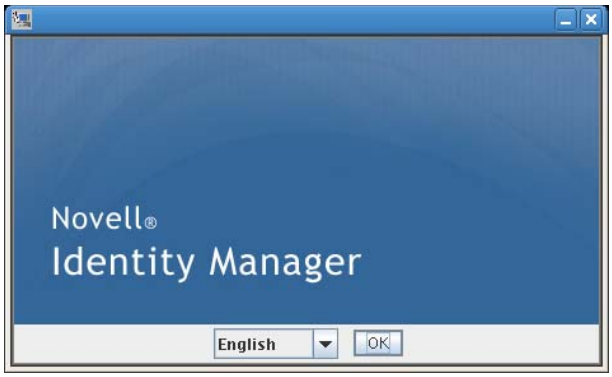
   **Solaris**

```
$ /opt/WL/bea/jrocket_150_11/bin/java -jar IdmUserApp.jar
```

**Windows**

```
C:\WL\bea\jrocket_150_11\bin\java -jar IdmUserApp.jar
```

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

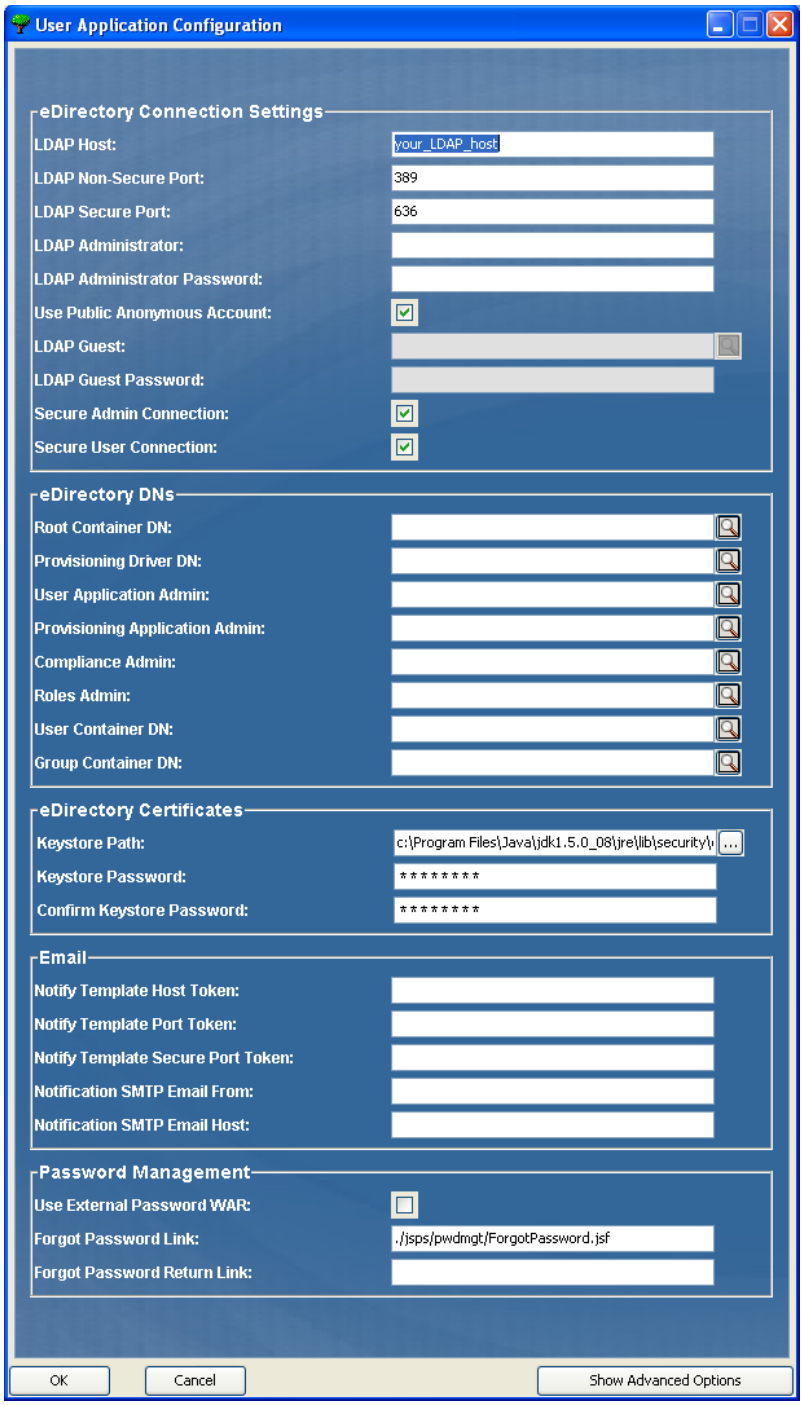



**3** Use the following information along with the instructions on each installation panel to complete the installation:

| Installation Screen | Description |
|---|---|
| Novell Identity Manager | 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 *WebLogic* for the application server. |
| Standard or Provisioning | *Standard*: Select this option if you are installing the User Application Standard Edition.<br><br>*Roles Based Provisioning*: Select this option if you are installing the Roles Based Provisioning Module. |
| Data Migration | Accept the default (verify that *Yes* is not selected).<br><br>**WARNING:** Do not select *Yes*, If Yes is selected, you will encounter problems starting the User Application.<br><br>For information on migrating, see the *User Application: Migration Guide* (http://www.novell.com/documentation/idmrbpm361/index.html). |
| Where is the WAR? | If the Identity Manager User Application WAR file is in a different directory from the installer, the installer prompts for the path to the WAR. |
| 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. Options include:<br>◆ Oracle (you are prompted for the version)<br>◆ MS SQL Server |

| Installation Screen | Description |
|---|---|
| Java Install | Specify the Java root install folder. |
| IDM Configuration | Specify the application context. This will be the part of the URL when you start the User Application from a browser. |
| Audit Logging | To enable logging, click *Yes*. The next panel prompts you to specify the type of logging. Choose from the following options:<br>◆ *Novell Audit*: Enables Novell Audit Logging for the User Application.<br>◆ *OpenXDAS*: Events are logged to your OpenXDAS logging server.<br>For more information on setting up Novell Audit or OpenXDAS logging, see the *User Application: Administration Guide*. |
| Novell Audit | *Server*: If you enable Novell Audit logging, specify the hostname or IP address for the Novell Audit server. If you turn logging off, this value is ignored.<br>*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.<br>*No*: Creates a new master key. After you finish the installation, you must manually record the master key as described in Section 8.1, "Recording the Master Key," on page 67.<br>The installation procedure writes the encrypted master key to the `master-key.txt` file in the installation directory.<br>Reasons to import an existing master key include:<br>◆ 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.<br>◆ 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).<br>◆ 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. |

4 You are prompted for the information that the installation program uses to configure the User Application WAR file. (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 22.


User Application Configuration
eDirectory Connection Settings
LDAP Host:
your_LDAP_host
LDAP Non-Secure Port:
389
LDAP Secure Port:
636
LDAP Administrator:
LDAP Administrator Password:
Use Public Anonymous Account:
LDAP Guest:
LDAP Guest Password:
Secure Admin Connection:
Secure User Connection:
eDirectory DNs
Root Container DN:
Provisioning Driver DN:
User Application Admin:
Provisioning Application Admin:
Compliance Admin:
Roles Admin:
User Container DN:
Group Container DN:
eDirectory Certificates
Keystore Path:
c:\Program Files\Java\jdk1.5.0_08\jre\lib\security\
Keystore Password:
********
Confirm Keystore Password:
********
Email
Notify Template Host Token:
Notify Template Port Token:
Notify Template Secure Port Token:
Notification SMTP Email From:
Notification SMTP Email Host:
Password Management
Use External Password WAR:
Forgot Password Link:
./jsps/pwdmgt/ForgotPassword.jsf
Forgot Password Return Link:
OK
Cancel
Show Advanced Options

| Installation Screen | Description |
|---|---|
| User Application Configuration | 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.<br><br>For more information, see Appendix A, "IDM User Application Configuration Reference," on page 75 |
| Pre-Installation Summary | Read the Pre-Installation Summary page to verify your choices for the installation parameters.<br><br>If necessary, use *Back* to return to earlier installation pages to change installation parameters.<br><br>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 the installation is finished. |

### 6.2.1 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.

## 6.3 Preparing the WebLogic Environment



### 6.3.1 Configure the Connection Pool

- ❑ 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.

  The JNDI name for the datasource must be the same name as the database you specified when creating the User Application WAR, for example, `jdbc/IDMUADataSource`.
- ❑ Copy `antlr-2.7.6.jar` from the User Application install directory to the domain lib folder.

## 6.3.2 Specify User Application Configuration File Locations

The WebLogic user application needs to know how to locate the `sys-configuration-xmldata.xml` file and the `idmuserapp_logging.xml` file. You can do so by adding the location of the files to the `setDomainEnv.cmd` file.

To make them available to the application server, specify its location 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`: Specify the folder (not the file itself) that contains the `sys-configuration.xml` file.
   - `-Didmuserapp.logging.config.dir`: Specify the folder (not the file itself) that contains the `idmuserapp_logging.xml` file.

   For example on Windows:

   ```
   set JAVA_OPTIONS=-Dextend.local.config.dir=c:/bea/user_projects/domains/
   base_domain/idm.local.config.dir
   -Didmuserapp.logging.config.dir=c:/bea/user_projects/domains/base_domain/
   idm.local.config.dir
   ```

4. Set the environment variable `EXT_PRE_CLASSPATH` to point to the `antlr.jar`.

   **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
   ```

   For example, on Linux:

   ```
   export EXT_PRE_CLASSPATH=/opt/bea/user_projects/domains/base_domain/
   lib/antlr-2.7.6.jar
   ```

5. Save and exit the file.

The XML files are also used by the configupdate 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. Add the following entry below it:

   ```
   Add -Dextend.local.config.dir=<directory-path>\extend.local.config.dir
   ```

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 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.

### 6.3.3 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/base_domain/config/` folder.

2 Add the following line in the `<security-configuration>` section:

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

3 Save the file and restart the server.

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

## 6.4 Deploying the User Application WAR

- ❑ Deploy the jsf-ri-1.1.1.war as a library.
- ❑ Copy the updated User Application WAR file from the install directory (typically `Novell\IDM` to the application domain. For example:

  ```
  bea\user_projects\domains\base_domain\servers\AdminServer\upload
  ```

- ❑ Deploy the User Application WAR using the standard WebLogic deployment procedure.

## 6.5 Accessing the User Application

- ❑ Navigate to the User Application URL:

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

  For example:

  ```
  http://localhost:8080/IDMProv
  ```

# Installing from the Console or with a Single Command

# 7

This section describes installation methods you can use instead of installing with a graphical user interface, which was described in Chapter 4, "Installing on JBoss by Using the GUI Installer," on page 33. Topics include:

- Section 7.1, "Installing the User Application from the Console," on page 57
- Section 7.2, "Installing the User Application with a Single Command," on page 58

## 7.1 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 the Java 2 Platform Standard Edition Development Kit version 1.5. If you use an earlier or later 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 2-2 on page 18, 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 4, "Installing on JBoss by Using the GUI Installer," on page 33, 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 75.
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 8, "Post-Installation Tasks," on page 67.

# 7.2 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 2-2 on page 18.
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 7-1 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 7-1*** *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.<br><br>Specify the hostname or IP address for your LDAP server. |
| NOVL_CONFIG_LDAPADMIN= | eDirectory Connection Settings: LDAP Administrator.<br><br>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.<br><br>Specify the LDAP Administrator password. This password is encrypted, based on the master key. |

| User Application Parameter Name in silent.properties | Equivalent Parameter Name in the User Application Configuration Parameters File |
|---|---|
| NOVL_CONFIG_ROOTCONTAINERNAME= | eDirectory DNs: Root Container DN.<br><br>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. |
| NOVL_CONFIG_PROVISIONROOT= | eDirectory DNs: Provisioning Driver DN.<br><br>Specify the distinguished name of the User Application driver that you created earlier in Section 3.1, “Creating the User Application Driver in iManager,” on page 27. 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:<br><br>`cn=UserApplicationDriver,cn=myDriverSet,o=myCompany` |
| NOVL_CONFIG_LOCKSMITH= | eDirectory DNs: User Application Admin.<br><br>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.<br><br>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.<br><br>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.<br><br>This role 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.<br><br>To change this assignment after you deploy the User Application, you must use the *Administration* > *Security* pages in the User Application. |

| User Application Parameter Name in silent.properties | Equivalent Parameter Name in the User Application Configuration Parameters File |
|---|---|
| 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.<br><br>To change this assignment after you deploy the User Application, use the *Roles* > *Role Assignment* page in the User Application. |
| 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.<br><br>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.<br><br>**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.<br><br>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.<br><br>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.<br><br>Specify the `cacerts` password. The default is `changeit`. |

| User Application Parameter Name in silent.properties | Equivalent Parameter Name in the User Application Configuration Parameters File |
|---|---|
| NOVL_CONFIG_SECUREADMINCONNECTION= | eDirectory Connection Settings: Secure Admin Connection.<br><br>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.<br><br>Specify *False* if the admin account does not use secure socket communication. |
| NOVL_CONFIG_SECUREUSERCONNECTION= | eDirectory Connection Settings: Secure User Connection.<br><br>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.<br><br>Specify *False* if the user's account does not use secure socket communication. |
| NOVL_CONFIG_SESSIONTIMEOUT= | Miscellaneous: Session Timeout.<br><br>Required. Specify an application session timeout interval. |
| NOVL_CONFIG_LDAPPLAINPORT= | eDirectory Connection Settings: LDAP Non-Secure Port.<br><br>Required. Specify the non-secure port for your LDAP server, for example 389. |
| NOVL_CONFIG_LDAPSECUREPORT= | eDirectory Connection Settings: LDAP Secure Port.<br><br>Required. Specify the secure port for your LDAP server, for example 636. |
| NOVL_CONFIG_ANONYMOUS= | eDirectory Connection Settings: Use Public Anonymous Account.<br><br>Required. Specify *True* to allow users who are not logged in to access the LDAP Public Anonymous Account.<br><br>Specify *False* to enable NOVL_CONFIG_GUEST instead. |

| User Application Parameter Name in silent.properties | Equivalent Parameter Name in the User Application Configuration Parameters File |
|---|---|
| NOVL_CONFIG_GUEST= | eDirectory Connection Settings: LDAP Guest.<br><br>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.<br><br>Specify the application server hosting the Identity Manager User Application. For example:<br><br>`myapplication serverServer`<br><br>This value replaces the $HOST$ token in e-mail templates. The URL that is constructed is the link to provisioning request tasks and approval notifications. |
| NOVL_CONFIG_EMAILNOTIFYPORT= | Email: Notify Template Port token.<br><br>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.<br><br>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.<br><br>Required. Specify e-mail From a user in provisioning e-mail. |
| NOVL_CONFIG_NOTFSMTPEMAILHOST= | Email: Notification SMTP Email Host.<br><br>Required. Specify the SMTP e-mail host that provisioning e-mail is using. This can be an IP address or a DNS name. |

| User Application Parameter Name in silent.properties | Equivalent Parameter Name in the User Application Configuration Parameters File |
|---|---|
| NOVL_CONFIG_USEEXTPWDWAR= | Password Management: Use External Password WAR.<br><br>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*.<br><br>Specify *False* to use the default internal Password Management functionality, `./jsps/pwdmgt/ForgotPassword.jsf` (without the http(s) protocol at the beginning). This redirects the user to the Forgot Password functionality built into the User Application, rather than to an external WAR. |
| NOVL_CONFIG_EXTPWDWARPATH= | Password Management: Forgot Password Link.<br><br>Specify the URL for the Forgot Password functionality page, `ForgotPassword.jsf`, in an external or internal password management WAR. Or, accept the default internal password management WAR. For details, see "Configuring External Password Management" on page 70. |
| NOVL_CONFIG_EXTPWDWARRTNPATH= | Password Management: Forgot Password Return Link.<br><br>If you are using an external password management WAR, supply the path that the external Password Management WAR uses to call back the User Application through Web Services, for example `https://idmhost:sslport/idm`. |
| NOVL_CONFIG_USEROBJECTATTRIBUTE= | Meta-Directory User Identity: User Object Class.<br><br>Required. The LDAP user object class (typically inetOrgPerson). |
| NOVL_CONFIG_LOGINATTRIBUTE= | Meta-Directory User Identity: Login Attribute.<br><br>Required. The LDAP attribute (for example, CN) that represents the user's login name. |
| NOVL_CONFIG_NAMINGATTRIBUTE= | Meta-Directory User Identity: Naming Attribute.<br><br>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.<br><br>Required. The LDAP attribute that represents the user's group membership. Do not use spaces in this name. |

| User Application Parameter Name in silent.properties | Equivalent Parameter Name in the User Application Configuration Parameters File |
|---|---|
| NOVL_CONFIG_GROUPOBJECTATTRIBUTE= | Meta-Directory User Groups: Group Object Class.<br><br>Required. The LDAP group object class (typically groupofNames). |
| NOVL_CONFIG_GROUPMEMBERSHIPATTRIBUTE= | Meta-Directory User Groups: Group Membership Attribute.<br><br>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.<br><br>Required. Specify *True* to use dynamic groups. Otherwise, specify *False*. |
| NOVL_CONFIG_DYNAMICGROUPOBJECTCLASS= | Meta-Directory User Groups: Dynamic Group Object Class.<br><br>Required. Specify the LDAP dynamic group object class (typically dynamicGroup). |
| NOVL_CONFIG_PRIVATESTOREPATH= | Private Key Store: Private Keystore Path.<br><br>Specify the path to the private keystore that contains the User Application's private key and certificates. Reserved. If you leave this empty, this path is `/jre/lib/security/cacerts` by default. |
| NOVL_CONFIG_PRIVATESTOREPASSWORD= | Private Key Store: Private Keystore Password. |
| NOVL_CONFIG_PRIVATEKEYALIAS= | Private Key Store: Private Key Alias.<br><br>This alias is `novellIDMUserApp` unless you specify otherwise. |
| NOVL_CONFIG_PRIVATEKEYPASSWORD= | Private Key Store: Private Key Password. |
| NOVL_CONFIG_TRUSTEDSTOREPATH= | Trusted Key Store: Trusted Store Path.<br><br>The Trusted Key Store contains all trusted signers' certificates used to validate digital signatures. If this path is empty, the User Application gets the path from System property `javax.net.ssl.trustStore`. If the path isn't there, it is assumed to be `jre/lib/security/cacerts`. |
| NOVL_CONFIG_TRUSTEDSTOREPASSWORD= | Trusted Key Store: Trusted Store Password. |
| NOVL_CONFIG_AUDITCERT= | Novell Audit Digital Signature Certificate |
| NOVL_CONFIG_AUDITKEYFILEPATH= | Novell Audit Digital Signature Private Key File path. |

| User Application Parameter Name in silent.properties | Equivalent Parameter Name in the User Application Configuration Parameters File |
|---|---|
| NOVL_CONFIG_ICSLOGOUTENABLED= | Access Manager and iChain Settings: Simultaneous Logout Enabled.<br><br>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.<br><br>Specify *False* to disable simultaneous logout. |
| NOVL_CONFIG_ICSLOGOUTPAGE= | Access Manager and iChain Settings: Simultaneous Logout Page.<br><br>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.<br><br>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.<br><br>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.<br><br>The fully qualified name of the authorization configuration file. |
| NOVL_CONFIG_CREATEDIRECTORYINDEX | Miscellaneous:Create eDirectory Index<br><br>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.<br><br>For best performance results, the index creation should be complete. The indexes should be in Online mode before you make the User Application available. |

| User Application Parameter Name in silent.properties | Equivalent Parameter Name in the User Application Configuration Parameters File |
|---|---|
| NOVL_CONFIG_REMOVEDIRECTORYINDEX | Miscellaneous: Remove eDirectory Index<br><br>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<br><br>Specify the eDirectory server where indexes should be created or removed. |

# Post-Installation Tasks

8

This section describes post-installation tasks. Topics include:



## 8.1 Recording the Master Key

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

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

---

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

---

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

## 8.2 Configuring the User Application

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

- In the *Novell IDM Roles Based Provisioning Module 3.6.1 Administration Guide*, the section entitled “Configuring the User Application Environment.”
- The *Novell IDM Roles Based Provisioning Module 3.6.1 Design Guide*

### 8.2.1 Setting up Novell Audit

Copy the `dirxml.lsc` file (located in the prerequisites.zip file) to the Audit server according to the directions in the section titled “Setting Up Logging” in the User Application: Administration Guide (http://www.novell.com/documentation/idmrbpm361/index.html).

## 8.3 Configuring eDirectory

## 8.3.1 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 82), or refer to the *Novell eDirectory Administration Guide* (http://www.novell.com/documentation) for directions on using Index Manager to create indexes.

## 8.3.2 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 in the `.iso`.
2. Install the SAML method into your eDirectory tree.
   - **2a** Extend the schema stored in the `authsaml.sch`

     The following example shows how to perform this on Linux:

     ```
     ndssch -h <edir_ip> <edir_admin> authsaml.sch
     ```
   - **2b** Install the SAML method.

     The following example shows how to perform this on Linux:

     ```
     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.)

## 8.4 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 75, Table 7-1 on page 58.

**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.

# 8.5 Configuring External 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.



## 8.5.1 Specifying an External Password Management WAR

1. Use either the install procedure or the configupdate utility.
2. In the User Application configuration parameters, select the *Use External Password WAR* configuration parameter check box.
3. For the *Forgot Password Link* configuration parameter, specify the location for the external password WAR.

   Include the host and port, for example `http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf`. An external password WAR can be outside the firewall protecting the User Application.
4. For the *Forgot Password Return Link*, supply the path that the external Password Management WAR uses to call back the User Application through Web Services, for example `https://idmhost:sslport/idm`.

   The return link must use SSL to ensure secure Web Service communication to the User Application. See also Section 8.5.4, "Configuring SSL Communication between JBoss Servers," on page 71.
5. Do one of the following:
   - If you are using the installer, read the information in this step and proceed to Step 6.
   - If you are using the configupdate utility to update the external password WAR in the installation root directory, read this step and manually rename the WAR to the first directory you specified in *Forgot Password Link*. Then, proceed to Step 6.

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

## 8.5.2 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*.

### 8.5.3 Testing the External 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:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf`.
- At the User Application login page, click the *Forgot Password* link.

### 8.5.4 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 `IDMPwdMgt.war` file. Refer to your JBoss documentation for directions.

## 8.6 Updating Forgot Password Settings

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

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

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

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

## 8.7 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:<br>◆ Identity Vault connections and certificates<br>◆ E-mail settings<br>◆ Metadirectory User Identity, User Groups<br>◆ Access Manager or iChain® settings | Run the configuration utility independent of the installer.<br>On Linux and Solaris, run the following command from the installation directory (by default, `/opt/novell/idm`):<br>`configupdate.sh`<br>On Windows, run the following command from the installation directory (by default, `c:\opt\novell\idm`):<br>`configupdate.bat` |
| Exceptions are thrown when application server starts up, with a log message `port 8080 already in use`. | Shut down any instances of Tomcat (or other server software) that might already be running. If you decide to reconfigure the application server to use a port other than 8080, remember to edit the `config` settings for the User Application driver in iManager. |
| When the application server starts, you see a message that no trusted certificates were found. | Make sure that you start application server 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). |
| When starting the application server, there are MySQL connection errors. | Don't run as `root`. (This issue is unlikely if you are running the version of MySQL supplied with Identity Manager.)<br>Make sure MySQL is running (and that the correct copy is running). Kill any other instances of MySQL. Run `/idm/mysql/start-mysql.sh`, then `/idm/start-jboss.sh`.<br>Examine `/idm/mysql/setup-mysql.sh` in a text editor and correct any values that appear suspicious. Then run the script, and run `/idm/start-jboss.sh`. |

| 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.<br><br>Use the `keytool` command to import the certificate file:<br><br>`keytool -import -trustcacerts -alias aliasName -file certFile -keystore ..\lib\security\cacerts -storepass changeit`<br><br>◆ Replace *aliasName* with a unique name of your choice for this certificate.<br>◆ Replace *certFile* with the full path and name of your certificate file.<br>◆ 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.<br><br>On Linux or Solaris, run this command from the installation directory (by default, `/opt/novell/idm`):<br><br>`configupdate.sh`<br><br>On Windows, run this command from the installation directory (by default, `c:\opt\novell\idm`):<br><br>`configupdate.bat` |

# IDM User Application Configuration Reference

A

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



## A.1 User Application Configuration: Basic Parameters

***Figure A-1*** *User Application Configuration Basic Options*

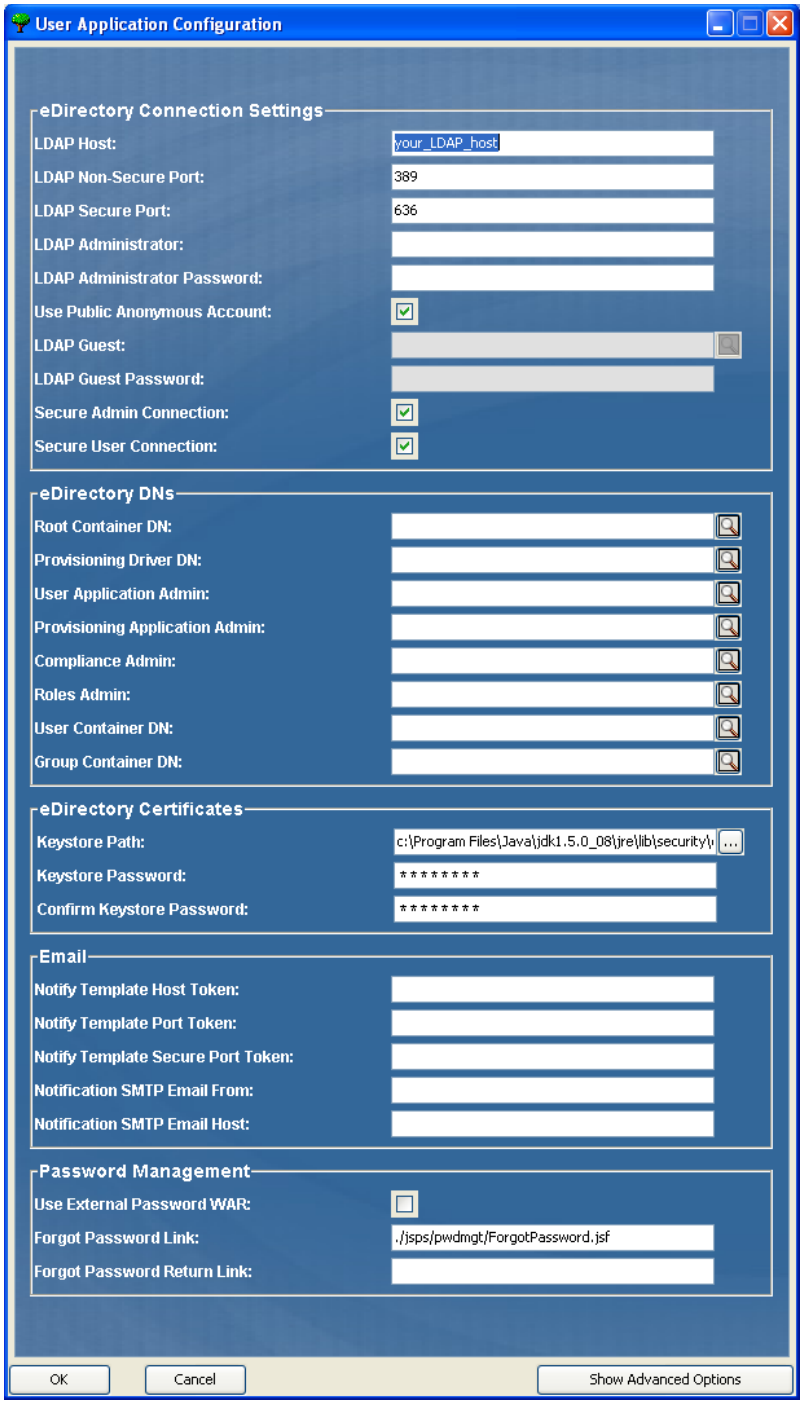


***Table A-1*** *User Application Configuration: Basic Options*

| Type of Setting | Option | Description |
|---|---|---|
| eDirectory® Connection Settings | *LDAP Host* | Required. Specify the hostname or IP address for your LDAP server and its secure port. For example:<br>`myLDAPhost` |
| | *LDAP Non-Secure Port* | Specify the non-secure port for your LDAP server. For example: 389. |
| | *LDAP Secure Port* | Specify the secure port for your LDAP server. For example: 636. |
| | *LDAP Administrator* | Required. Specify the credentials for the LDAP Administrator. This user must already exist. The User Application uses this account to make an administrative connection to the Identity Vault. This value is encrypted, based on the master key.<br>You can use configupdate utility to modify this setting as long as you have not modified it using the User Application's Administration tab. |
| | *LDAP Administrator Password* | Required. Specify the LDAP Administrator password. This password is encrypted, based on the master key.<br>You can use configupdate utility to modify this setting as long as you have not modified it using the User Application's Administration tab. |
| | *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 the LDAP Guest, you must deselect *Use Public Anonymous Account*. To disable the Guest User, select *Use Public Anonymous Account*. |
| | *LDAP Guest Password* | Specify the LDAP Guest password. |
| | *Secure Admin Connection* | Select this option to require that all communication using the admin account be done using a secure socket. (This option can have adverse performance implications). This setting allows other operations that don't require SSL to operate without SSL. |
| | *Secure User Connection* | Select this option to require that all communication using the logged-in user's account be done using a secure socket. (This option can have adverse performance implications). This setting allows other operations that don't require SSL to operate without SSL. |

| Type of Setting | Option | Description |
|---|---|---|
| eDirectory DNs | *Root Container DN* | Required. Specify the LDAP distinguished name of the root container. This is used as the default entity definition search root when no search root is specified in the directory abstraction layer. |
| | *Provisioning Driver DN* | Required. Specify the distinguished name of the User Application driver (described in Section 3.1, “Creating the User Application Driver in iManager,” on page 27). 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:<br><br>`cn=UserApplicationDriver,cn=myDriverSet,o=myCompany` |
| | *User Application Admin* | Required. An existing user in the Identity Vault who has the rights to perform administrative tasks for the User Application user container specified. This user can use the *Administration* tab of the User Application to administer the portal.<br><br>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.<br><br>To change this assignment after you deploy the User Application, you must use the *Administration* > *Security* pages in the User Application.<br><br>You cannot change this setting via configupdate if you have started the application server hosting the User Application. |
| | *Provisioning Application Admin* | 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.<br><br>To change this assignment after you deploy the User Application, you must use the *Administration* > *Security* pages in the User Application. |

| Type of Setting | Option | Description |
|---|---|---|
| | *Compliance Admin* | 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.<br><br>During a configupdate, changes to this value only take effect if you do not have a valid Compliance Module Administrator assigned. If a valid Compliance Module Administrator exists, then your changes are not saved.<br><br>To change this assignment after you deploy the UserApplication, use the *Roles* > *Role Assignment* page in the User Application. |
| eDirectory DNs (continued) | *Roles Administrator* | 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.<br><br>To change this assignment after you deploy the User Application, use the *Roles* > *Role Assignment* page in the User Application.<br><br>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. |
| | *User Container DN* | Required. Specify the LDAP distinguished name (DN) or fully qualified LDAP name of the user container. This defines the search scope for users and groups. Users in this container (and below) are allowed to log in to the User Application.<br><br>**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.<br><br>You cannot change this setting via configupdate if you have started the application server hosting the User Application. |
| | *Group Container DN* | Required. Specify the LDAP distinguished name (DN) or fully qualified LDAP name of the group container.<br><br>Used by entity definitions within the directory abstraction layer.<br><br>You cannot change this setting via configupdate if you have started the application server hosting the User Application. |

| Type of Setting | Option | Description |
|---|---|---|
| eDirectory Certificates | *Keystore Path* | Required. Specify the full path to your keystore (`cacerts`) file of the JDK that the application server application server is using to run, or click the small browser button and navigate to the `cacerts` file.<br><br>On Linux or Solaris, the user must have permission to write to this file. |
| | *Keystore Password/ Confirm Keystore Password* | Required. Specify the `cacerts` password. The default is `changeit`. |
| E-mail | *Notify Template Host Token* | Specify the application server hosting the Identity Manager User Application. For example:<br><br>`myapplication serverServer`<br><br>This value replaces the $HOST$ token in e-mail templates. The URL that is constructed is the link to provisioning request tasks and approval notifications. |
| | *Notify Template Port Token* | Used to replace the $PORT$ token in e-mail templates used in provisioning request tasks and approval notifications. |
| | *Notify Template Secure Port token* | Used to replace the $SECURE_PORT$ token in e-mail templates used in provisioning request tasks and approval notifications. |
| | *Notification SMTP Email From:* | Specify e-mail to come from a user in provisioning e-mail. |
| | *Notification SMTP Email Host:* | Specify the SMTP e-mail host that provisioning e-mail is using. This can be an IP address or a DNS name. |
| 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.<br><br>If you select *Use External Password WAR*, you must supply values for *Forgot Password Link* and *Forgot Password Return Link*.<br><br>If you do not select *Use External Password WAR,* IDM uses the default internal Password Management functionality, `./jsps/pwdmgt/ForgotPassword.jsf` (without the http(s) protocol at the beginning). This redirects the user to the Forgot Password functionality built into the User Application, rather than to an external WAR. |
| | *Forgot Password Link* | This URL points to the Forgot Password functionality page. Specify a `ForgotPassword.jsf` file in an external or internal password management WAR. For details, see “Configuring External Password Management” on page 70. |
| | *Forgot Password Return Link* | If you are using an external password management WAR, supply the path that the external Password Management WAR uses to call back the User Application through Web Services, for example `https://idmhost:sslport/idm`. |

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

| Type of Setting | Option | Description |
|---|---|---|
| eDirectory DNs | *Root Container DN* | Required. Specify the LDAP distinguished name of the root container. This is used as the default entity definition search root when no search root is specified in the directory abstraction layer. |
| | *Provisioning Driver DN* | Required. Specify the distinguished name of the User Application driver (described in Section 3.1, “Creating the User Application Driver in iManager,” on page 27). 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:<br><br>`cn=UserApplicationDriver,cn=myDriverSet,o=myCompany` |
| | *User Application Admin* | Required. An existing user in the Identity Vault who has the rights to perform administrative tasks for the User Application user container specified. This user can use the *Administration* tab of the User Application to administer the portal.<br><br>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.<br><br>To change this assignment after you deploy the User Application, you must use the *Administration* > *Security* pages in the User Application.<br><br>You cannot change this setting via configupdate if you have started the application server hosting the User Application. |
| | *Provisioning Application Admin* | The Provisioning Application Administrator manages Provisioning Workflow functions available through the *Requests and Approvals* tab of the User Application. This user must exist in the Identity Vault prior to being designated the Provisioning Application Administrator.<br><br>To change this assignment after you deploy the User Application, you must use the *Administration* > *Security* pages in the User Application. |
| | *Compliance Admin* | 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.<br><br>During a configupdate, changes to this value only take effect if you do not have a valid Compliance Module Administrator assigned. If a valid Compliance Module Administrator exists, then your changes are not saved.<br><br>To change this assignment after you deploy the User Application, use the *Roles* > *Role Assignment* page in the User Application. |

| Type of Setting | Option | Description |
|---|---|---|
| | *Roles Administrator* | 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.<br><br>To change this assignment after you deploy the User Application, use the *Roles* > *Role Assignment* page in the User Application.<br><br>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. |
| Meta-Directory User Identity | *User Container DN* | Required. Specify the LDAP distinguished name (DN) or fully qualified LDAP name of the user container.<br><br>Users in this container (and below) are allowed to log in to the User Application.<br><br>You cannot change this setting via configupdate if you have started the application server hosting the User Application.<br><br>**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. |

| Type of Setting | Option | Description |
|---|---|---|
| Meta-Directory User Groups | *Group Container DN* | Required. Specify the LDAP distinguished name (DN) or fully qualified LDAP name of the group container. Used by entity definitions within the directory abstraction layer.<br><br>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). |
| eDirectory Certificates | *Keystore Path* | Required. Specify the full path to your keystore (`cacerts`) file of the JRE that the application server application server is using to run, or else click the small browser button and navigate to the `cacerts` file.<br><br>The User Application installation modifies the keystore file. On Linux or Solaris, the user must have permission to write to this file. |
| | *Keystore Password* | Required. Specify the `cacerts` password. The default is `changeit`. |
| | *Confirm Keystore Password* | |
| Private Key Store | *Private Keystore Path* | The private keystore contains the User Application's private key and certificates. Reserved. If you leave this empty, this path is `/jre/lib/security/cacerts` by default. |
| | *Private Keystore Password* | This password is `changeit` unless you specify otherwise. This password is encrypted, based on the master key. |
| | *Private Key Alias* | This alias is `novellIDMUserApp` unless you specify otherwise. |
| | *Private Key Password* | This password is `novellIDM` unless you specify otherwise. This password is encrypted, based on the master key. |

| Type of Setting | Option | Description |
|---|---|---|
| Trusted Key Store | *Trusted Store Path* | The Trusted Key Store contains all trusted signers' certificates used to validate digital signatures. If this path is empty, the User Application gets the path from System property `javax.net.ssl.trustStore`. If the path isn't there, it is assumed to be `jre/lib/security/cacerts`. |
| | *Trusted Store Password* | If this field is empty, the User Application gets the password from System property `javax.net.ssl.trustStorePassword`. If the value is not there, `changeit` is used. This password is encrypted, based on the master key. |
| Novell Audit Digital Signature and Certificate Key | | Contains the Novell Audit digital signature key and certificate. |
| | *Novell Audit Digital Signature Certificate* | Displays the digital signature certificate. |
| | *Novell Audit Digital Signature Private Key* | Displays the digital signature private key. This key is encrypted, based on the master key. |
| Access Manager and iChain 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 | *Notify Template HOST token* | Specify the application server hosting the Identity Manager User Application. For example:<br>`myapplication serverServer`<br>This value replaces the $HOST$ token in e-mail templates. The URL that is constructed is the link to provisioning request tasks and approval notifications. |
| | *Notify Template PORT token* | Used to replace the $PORT$ token in e-mail templates used in provisioning request tasks and approval notifications. |
| | *Notify Template SECURE PORT token* | Used to replace the $SECURE_PORT$ token in e-mail templates used in provisioning request tasks and approval notifications. |
| | *Notify Template PROTOCOL token* | Refers to a non-secure protocol, HTTP. Used to replace the $PROTOCOL$ token in e-mail templates used in provisioning request tasks and approval notifications. |
| | *Notify Template SECURE PROTOCOL token* | Refers to a secure protocol, HTTPS. Used to replace the $SECURE_PROTOCOL$ token in e-mail templates used in provisioning request tasks and approval notifications. |
| | *Notification SMTP Email From:* | Specify e-mail from a user in provisioning e-mail. |
| | *Notification SMTP Email Host:* | Specify the SMTP e-mail host that provisioning e-mail is using. This can be an IP address or a DNS name. |
| 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.<br>If you select *Use External Password WAR*, you must supply values for *Forgot Password Link* and *Forgot Password Return Link*.<br>If you do not select *Use External Password WAR,* IDM uses the default internal Password Management functionality, `./jsps/pwdmgt/ForgotPassword.jsf` (without the http(s) protocol at the beginning). This redirects the user to the Forgot Password functionality built into the User Application, rather than to an external WAR. |
| | *Forgot Password Link* | This URL points to the Forgot Password functionality page. Specify a `ForgotPassword.jsf` file in an external or internal password management WAR. |
| | *Forgot Password Return Link* | If you are using an external password management WAR, supply the path that the external Password Management WAR uses to call back the User Application through Web Services, for example `https://idmhost:sslport/idm`. |

| Type of Setting | Option | Description |
|---|---|---|
| Miscellaneous | *Session Timeout* | The application session timeout. |
| | *OCSP URI* | If the client installation uses the On-Line Certificate Status Protocol (OCSP), supply a Uniform Resource Identifier (URI). For example, the format is http://host:port/ocspLocal. The OCSP URI updates the status of trusted certificates online. |
| | *Authorization Config Path* | Fully qualified name of the authorization configuration file. |
| | *Create eDirectory Index* | 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 8.3.1, "Creating Indexes in eDirectory," on page 68.<br><br>For best performance, the index creation should be complete. The indexes should be in Online mode before you make the User Application available. |
| | *Remove eDirectory Index* | Removes indexes on manager, ismanager, and srvprvUUID attributes. |
| | *Server DN* | Select the eDirectory server where the indexes should be created or removed.<br><br>**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.<br><br>For information on containers, see the *Novell iManager 2.6 Administration Guide (http://www.novell.com/documentation/imanager26/pdfdoc/imanager_admin_26/imanager_admin_26.pdf)*. |
| | *Add a New Container Object: Container Attribute Name* | Supply the attribute name of the container object. |