

# **Integrated Installation Guide**

## **Identity Manager 4.0.2**

June 2014

## Legal Notices

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

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

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

Copyright © 2012 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.  
1800 South Novell Place  
Provo, UT 84606  
U.S.A.  
[www.novell.com](http://www.novell.com)

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

## Novell Trademarks

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

## Third-Party Materials

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

---

# Contents

<b>About This Guide</b>	<b>5</b>
<b>1 Integrated Installer Overview</b>	<b>7</b>
1.1 Integrated vs. Standalone Installer	7
1.2 Identity Vault Structure	8
1.2.1 Security	9
1.2.2 Data	10
1.2.3 System	10
1.3 Configuring Drivers	11
1.4 Differences in Installing the Identity Manager 4.0.2 Standard Edition and the Advanced Edition	11
<b>2 Identity Manager Components</b>	<b>13</b>
2.1 Metadirectory Server (Identity Vault, Metadirectory Engine, and Remote Loader)	14
2.1.1 Supported Processors	14
2.1.2 Server Operating Systems	14
2.2 Auditing and Reporting	16
2.3 User Application	17
2.4 Role Mapping Administrator	17
2.5 iManager, Designer, and Analyzer	17
2.5.1 Web Browsers	18
<b>3 System Requirements</b>	<b>19</b>
3.1 Supported Platforms	19
3.2 Resource Requirements	21
3.3 Ports Used by the Identity Manager Services	21
<b>4 Installing Identity Manager</b>	<b>23</b>
4.1 Downloading the ISO File	23
4.2 New Installation by Using Physical Media or an ISO	25
4.2.1 Installation	27
4.2.2 Configuration	28
4.3 Post-Installation Procedure	36
4.4 Silent Installation and Configuration	37
4.4.1 Silent Installation	37
4.4.2 Silent Configuration	37
4.5 Language Support for the Identity Manager Installers	38
4.5.1 Non-Installer Language Considerations	39
<b>5 Activating Novell Identity Manager Products</b>	<b>41</b>
5.1 Purchasing an Identity Manager Product License	41
5.2 Installing a Product Activation Credential	41
5.3 Viewing Product Activations for Identity Manager and for Drivers	42
5.4 Activating Identity Manager Drivers	43
5.5 Activating Analyzer	43

5.6	Activating Designer and the Role Mapping Administrator .....	43
<b>6</b>	<b>Upgrading Identity Manager</b>	<b>45</b>
<b>7</b>	<b>Troubleshooting Identity Manager</b>	<b>47</b>
<b>8</b>	<b>Uninstalling Identity Manager</b>	<b>55</b>
8.1	GUI Uninstallation .....	55
8.2	Silent Uninstallation .....	55

---

# About This Guide

Novell Identity Manager 4.0.2 is a data sharing and synchronization service that enables applications, directories, and databases to share information. It links scattered information and enables you to establish policies that govern automatic updates to designated systems when identity changes occur.

Identity Manager provides the foundation for account provisioning, security, single sign-on, user self-service, authentication, authorization, automated workflow, and Web services. It allows you to integrate, manage, and control your distributed identity information so you can securely deliver the right resources to the right people.

This guide contains information about how to install, upgrade, or uninstall an Identity Manager system that is useful for your environment.

- ♦ [Chapter 1, “Integrated Installer Overview,”](#) on page 7
- ♦ [Chapter 2, “Identity Manager Components,”](#) on page 13
- ♦ [Chapter 3, “System Requirements,”](#) on page 19
- ♦ [Chapter 4, “Installing Identity Manager,”](#) on page 23
- ♦ [Chapter 5, “Activating Novell Identity Manager Products,”](#) on page 41
- ♦ [Chapter 6, “Upgrading Identity Manager,”](#) on page 45
- ♦ [Chapter 7, “Troubleshooting Identity Manager,”](#) on page 47
- ♦ [Chapter 8, “Uninstalling Identity Manager,”](#) on page 55

## Audience

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

## 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 and enter your feedback there.

## Documentation Updates

For the most recent version of this document, see the [Identity Manager Documentation Web site](http://www.netiq.com/documentation/idm402/index.html) (<http://www.netiq.com/documentation/idm402/index.html>).

## Additional Documentation

For additional Identity Manager documentation, see the [Identity Manager Documentation Web site](http://www.netiq.com/documentation/idm402/index.html) (<http://www.netiq.com/documentation/idm402/index.html>).

For User Application documentation, see the [Identity Manager Documentation Web site](http://www.novell.com/documentation/idm402/index.html) (<http://www.novell.com/documentation/idm402/index.html>).



---

# 1 Integrated Installer Overview

Identity Manager 4.0 and later provides world-class compliance support and reduced costs for identity management and provisioning from the data center environment to the cloud environment. The integrated installer simplifies Identity Manager deployment for administrators and consultants. It is a simplified installer to help you quickly set up a system, because it avoids the need to separately install each component.

- ♦ [Section 1.1, “Integrated vs. Standalone Installer,” on page 7](#)
- ♦ [Section 1.2, “Identity Vault Structure,” on page 8](#)
- ♦ [Section 1.3, “Configuring Drivers,” on page 11](#)
- ♦ [Section 1.4, “Differences in Installing the Identity Manager 4.0.2 Standard Edition and the Advanced Edition,” on page 11](#)

## 1.1 Integrated vs. Standalone Installer

**Table 1-1** Comparison of the Integrated and the Standalone Installer

Features	Integrated	Standalone
Tree structure	The tree structure is predefined to suit most of the Identity Manager deployments. See the <a href="#">Section 1.2, “Identity Vault Structure,” on page 8</a> for more information on the tree structure.	The tree structure is customizable.
Custom Installation of Drivers	All the drivers are installed by default.	Custom installation of drivers is supported.
Driver Set	Created as a separate partition during the Metadirectory server configuration.	Not created. Can be created manually by using iManager.
Nonroot Installation	Not supported.	Nonroot installation of some components is supported.
iManager Plug-In Installation	Automatically installed.	Manually installed.
Dependencies	Automatically handles dependencies.	Dependencies are manually handled.

Features	Integrated	Standalone
Duration of Installation	Automates several manual steps to quickly set up the system.	Usually takes more time.
User Input Options	The user interface has fewer options, so it requires less user input. Several options assume default values.	The user interface has several options, so you need to have a good understanding of all the components.
Supported Platform Checks	Internally checks the platform differences.	Does not perform a platform check.
Handling Inconsistencies	Has a consistent user experience across components and platforms.	Might experience inconsistencies.
Installation and Configuration Phases	Separate installation and configuration phases.	Differs across various components.

If you are creating an Identity Manager solution where you need to install one or more of the Identity Manager components separately or need a good number of customized options, use the [Identity Manager 4.0.2 Framework Installation Guide](#) to help you with the installation. For installation instructions, see the “[Installation](#)” section in the [Identity Manager 4.0.2 Framework Installation Guide](#).

You use the integrated installer primarily for new installations of Identity Manager 4.0.1. For information on upgrading an existing installation, see [Chapter 6, “Upgrading Identity Manager,” on page 45](#).

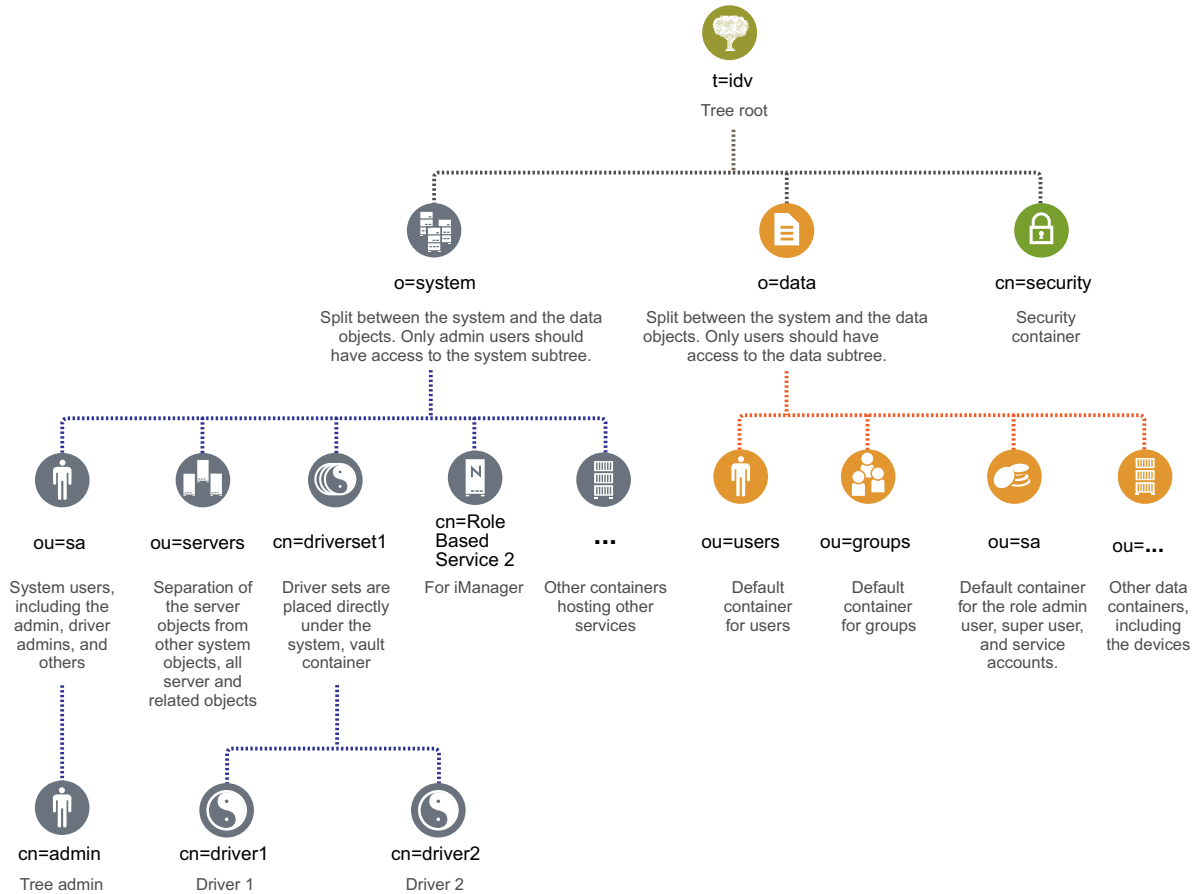
Currently, integrated installer supports two types of installation modes: GUI installation and silent installation. Console mode is not supported.

## 1.2 Identity Vault Structure

The Identity Vault structure is predefined to suit most of your Identity Manager deployments.



**Figure 1-1** Identity Vault Structure



**Figure 1-1** depicts the Identity Vault structure for the Identity Manager. This structure is primarily useful for a single-environment installation. This is the default structure for small and medium Identity Manager deployments. Multi-tenant environments might have a slightly different structure. Also, you cannot organize large and distributed trees in this way. This type of tree structure is created when you create a new tree through the integrated installer.

Identity Manager 4.0 and later mostly uses organization containers, so that users, groups, and service admins are placed in the same container. You should use organizations if possible and use organizational units where it makes sense. The Identity Manager 4.0 and later structure is set up for scalability by having three main components:

- ◆ [Section 1.2.1, “Security,” on page 9](#)
- ◆ [Section 1.2.2, “Data,” on page 10](#)
- ◆ [Section 1.2.3, “System,” on page 10](#)

## 1.2.1 Security

The security container is a special container created during the installation of the Identity Vault. It is designated as `cn=security` instead of `dc`, `o`, or `ou`. This container holds all security objects for the Identity Vault. For example, it contains the certificate authority and password policies.

## 1.2.2 Data

The data container holds groups, users, role admins, devices, and others. This is the data that makes up your system. The groups, users, and sa containers are organizational units. You can have additional organizational units to structure your data according to your organizational practices.

### **ou=sa**

The Service Admins (ou=sa) container holds all user application administrator objects and service administrator accounts.

## 1.2.3 System

The system container is an organization. It is designated as o=system. This container holds all of the technical and configuration information for your Identity Vault and for the Identity Manager system. The system container holds four main subcontainers:

- ♦ sa or service admin users / super user / service accounts
- ♦ servers
- ♦ driver sets
- ♦ services

### **ou=sa**

The Service Admins container holds administrative objects for the Identity Vault and drivers. Only admin users can access the system subtree. The default Identity Vault admin is admin.sa.system.

### **Servers**

The server objects have many different objects associated with them that must reside in the same container as the server object. As you add more servers into your tree, scrolling through all of those objects can become very cumbersome.

You should have all server objects under the servers.system container. However, an administrator can create individual server containers for each of the servers deployed in the environment. The name of the container is the name of the server object. All objects associated with the server (volumes, licenses, certificates) are in place and it is much easier to find the objects you need.

This structure is designed for scalability, so if you have 10 or 100 servers, it is easy to find the objects associated with a single server.

### **Driver Sets**

Driver sets are created as a separate partition during the Metadirectory server configuration. All driver set objects are stored in the system container. Your Identity Manager 4.0.2 system can have multiple driver sets. This structure allows you to scale by adding more driver sets to the system container. Role-based services for iManager are also stored in the system container.

## 1.3 Configuring Drivers

The following Identity Manager 4.0.2 components can be installed and configured by using the integrated installer:

- ◆ Metadirectory Server (Identity Vault, Metadirectory Engine, and Remote Loader)
- ◆ Roles Based Provisioning Module
- ◆ Identity Reporting Module
- ◆ Event Auditing Service
- ◆ Role Mapping Administrator
- ◆ iManager
- ◆ Designer
- ◆ Analyzer

See [System Requirements](#) for a list of supported platforms for the Identity Manager components.

The integrated installer configures the drivers required for the Roles Based Provisioning Module and the Identity Reporting Module. For configuring additional drivers, refer to the [Identity Manager 4.0.1 Drivers documentation Web site \(http://www.novell.com/documentation/idm401drivers/\)](http://www.novell.com/documentation/idm401drivers/).

## 1.4 Differences in Installing the Identity Manager 4.0.2 Standard Edition and the Advanced Edition

Identity Manager 4.0.2 is available in the Advanced Edition and the Standard Edition. There are separate ISOs for each of them. The installation programs for the Advanced Edition and Standard Edition have a few differences:

**The Role Mapping Administrator is not shipped with the Standard Edition:** The Role Mapping Administrator is not included in the list of Identity Manager components in the Select Components page of the integrated installer.

**Configuring the Messaging Gateway Driver is not supported:** You cannot configure the Messaging Gateway Driver through integrated installer in the Standard Edition.

**Two more User Application admin roles have been added:** With the Standard Edition, in addition to the User Application Administrator, the Report Administrator and the Security Administrator roles have been added. You must specify the credentials for the Report Administrator and the Security Administrator while configuring the User Application through the integrated installer.

**New reports have been added to the Identity Reporting Module:** Three new reports have been added to the Identity Reporting module. Some of the reports that report on data such as roles, resources, and workflow processes are not available in the Standard Edition. For more information on new reports, see “[Identity Manager 4.0.2 New Features](#)” section in the [Identity Manager 4.0.2 Overview Guide](#).

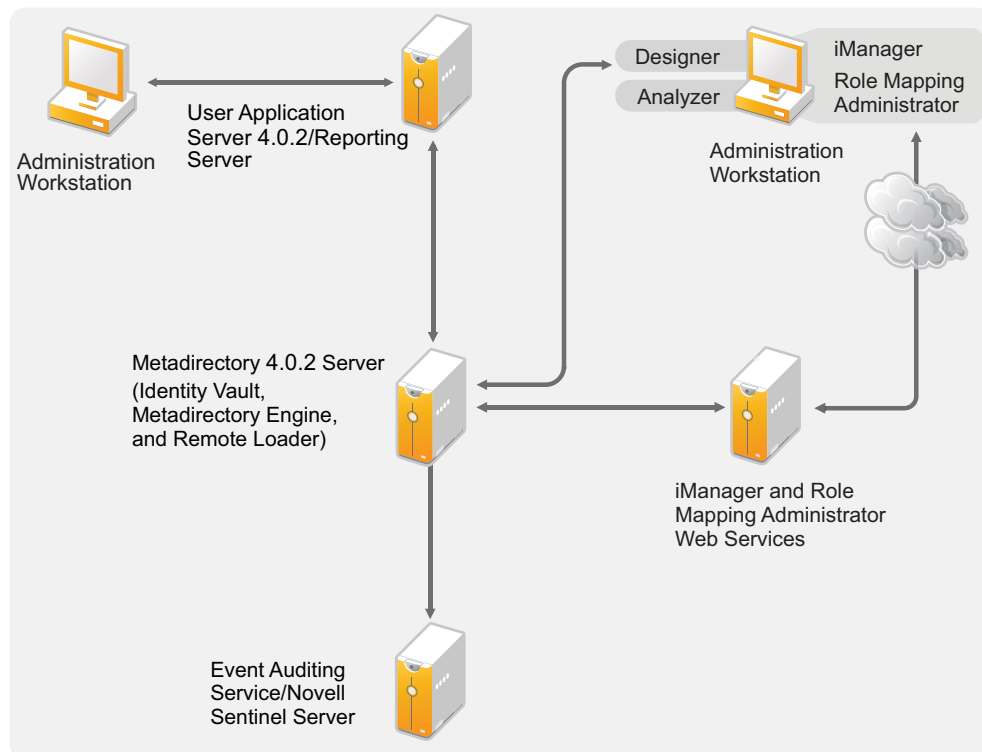
For more information on installing Identity Manager, refer to the [Chapter 4, “Installing Identity Manager,”](#) on page 23.



# 2 Identity Manager Components

You can install the following components by using the Identity Manager integrated installer. The Identity Manager components do not need to be installed on the same system. [Figure 2-1](#) shows which platforms are certified. For a detailed list of certified and supported platforms for the integrated installer, refer to [Table 2-1](#) and [Table 2-2](#).

**Figure 2-1** Identity Manager Integrated Installer Components



- ◆ [Section 2.1, “Metadirectory Server \(Identity Vault, Metadirectory Engine, and Remote Loader\),”](#) on page 14
- ◆ [Section 2.2, “Auditing and Reporting,”](#) on page 16
- ◆ [Section 2.3, “User Application,”](#) on page 17
- ◆ [Section 2.4, “Role Mapping Administrator,”](#) on page 17
- ◆ [Section 2.5, “iManager, Designer, and Analyzer,”](#) on page 17

## 2.1 Metadirectory Server (Identity Vault, Metadirectory Engine, and Remote Loader)

The Metadirectory server processes the events from the drivers.

During the installation of the Identity Manager, Identity Vault is automatically installed.

### 2.1.1 Supported Processors

The processors listed here are the ones that are used during the testing of Identity Manager.

The following 32-bit processors for Linux (SUSE Linux Enterprise Server) and Windows operating systems are supported:

- ◆ Intel x86-32
- ◆ AMD x86-32

The following 64-bit processors for Linux (SUSE Linux Enterprise Server) and Windows operating systems are supported:

- ◆ Intel EM64T
- ◆ AMD Athlon64
- ◆ AMD Opteron

The SPARC processor is used for Solaris testing.

### 2.1.2 Server Operating Systems

You can install the Metadirectory engine as a 32-bit application on a 32-bit operating system and as a 64-bit application on a 64-bit operating system. [Table 2-1](#) contains a list of the certified and supported server operating systems that the Metadirectory server can run on.

---

**IMPORTANT:** Certified platform means that the platform has been fully tested. Supported platform means that the platform has not been tested, but is expected to be functional.

---

**Table 2-1** *Supported and Certified Server Operating Systems*

<b>Certified Server Operating System Version</b>	<b>Supported</b>	<b>Notes</b>
Windows Server 2003 SP2 (32-bit)	Supported on later versions of service packs	The Metadirectory server runs in 32-bit mode.
Windows Server 2008 SP2(32-bit and 64-bit)	Supported on later versions of service packs	The Metadirectory server runs in either 32-bit or 64-bit mode.
Windows Server 2008 R2 SP1 (64-bit)	Supported on later versions of support packs	The Metadirectory server runs only in 64-bit mode.
Red Hat 5.7 (32-bit and 64-bit)	Supported on later versions of support packs	The Metadirectory server runs in either 32-bit or 64-bit mode. Novell recommends that you apply the latest OS patches via the manufacturer's automated update facility before you install Identity Manager.

<b>Certified Server Operating System Version</b>	<b>Supported</b>	<b>Notes</b>
Red Hat 6.2	Red Hat 6.0 (32-bit and 64-bit)	The Metadirectory server runs in either 32-bit or 64-bit mode. Novell recommends that you apply the latest OS patches via the manufacturer's automated update facility before you install Identity Manager.
SUSE Linux Enterprise Server 10 SP4 (32-bit and 64-bit)	Supported on later versions of support packs	The Metadirectory server runs in either 32-bit or 64-bit mode. Novell recommends that you apply the latest OS patches via the manufacturer's automated update facility before you install Identity Manager.
SUSE Linux Enterprise Server 11 SP1, SP2 (32-bit and 64-bit)	Supported on later versions of support packs	The Metadirectory server runs in either 32-bit or 64-bit mode. Novell recommends that you apply the latest OS patches via the manufacturer's automated update facility before you install Identity Manager.
Solaris 10 (64-bit)	Supported on later versions of support packs	The Metadirectory server runs only in 64-bit mode.

**Table 2-2** *Supported and Certified Virtualization Systems*

<b>Certified Server System Version</b>	<b>Supported</b>	<b>Notes</b>
Xen	All platforms listed in <a href="#">Table 2-1</a> and supported by Xen.	Xen is supported when the Xen Virtual Machine is running SLES 10, SLES 11, or Windows 2008 R2 as the guest operating system in paravirtualized mode and SLES 10 SP2 as the host operating system.
Windows Server 2008 R2 Virtualization with Hyper-V	All platforms listed in <a href="#">Table 2-1</a> and supported by Hyper-V.	The Metadirectory server runs in either 32-bit or 64-bit mode.
VMware ESX 4.0, ESXi 4.0, 4.1, ESXi 5.0, 5.1	All the platforms listed in <a href="#">Table 2-1</a> and supported by VMWare ESX and ESXi, VMWare version of SLES 11 SP2 (64-bit) as the guest operating system for VMWare.	
VMware Workstation 6.5	Supported on SLES 11 SP1 as the base operating system. The base operating system can be any system supported by VMware workstation 6.5 and later. All the certified platforms listed in <a href="#">Table 2-1</a> are supported by VMWare workstation as the guest operating system.	

---

**NOTE:** Open Enterprise Server is not supported with the Identity Manager integrated installer.

---

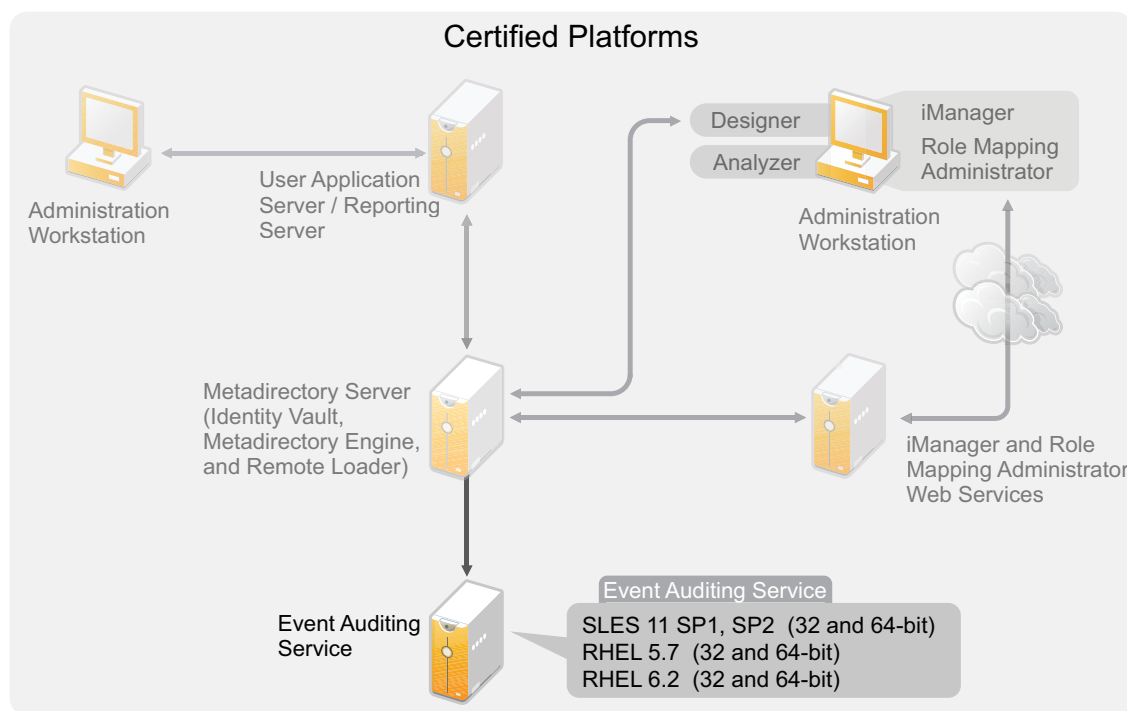
## 2.2 Auditing and Reporting

By adding auditing and reporting, you can meet compliance standards that many companies must abide by. You can create audit trails for any events you need to track, and you can generate reports to meet audit standards for your company.

The Identity Reporting Module and Novell Sentinel are two different tools used to gather auditing and reporting information about Identity Manager.

The Identity Reporting Module is a component of the Identity Manager 4.0.2. Novell Sentinel is not bundled with the Identity Manager, but it is an optional component you can add to your Identity Manager system.

**Figure 2-2** Auditing and Reporting



For more information about the Identity Reporting Module system requirements, see the “[System Requirements](#)” section in the *Identity Reporting Module Guide*. For configuration information about Sentinel with Identity Manager, see the *Identity Manager 4.0.2 Reporting Guide for Novell Sentinel*. For system requirements information about Novell Sentinel, see the *Novell Sentinel Installation Guide* (<http://www.novell.com/documentation/sentinel6/index.html>).



## 2.3 User Application

The Identity Manager User Application is your view into the information, roles, resources, and capabilities of Identity Manager. Your system administrator determines the details of what you can see and do in the Identity Manager User Application.

See the “[System Requirements](#)” section in the *Identity Manager Roles Based Provisioning Module 4.0.2 User Application: Installation Guide* for a list of User Application system requirements.

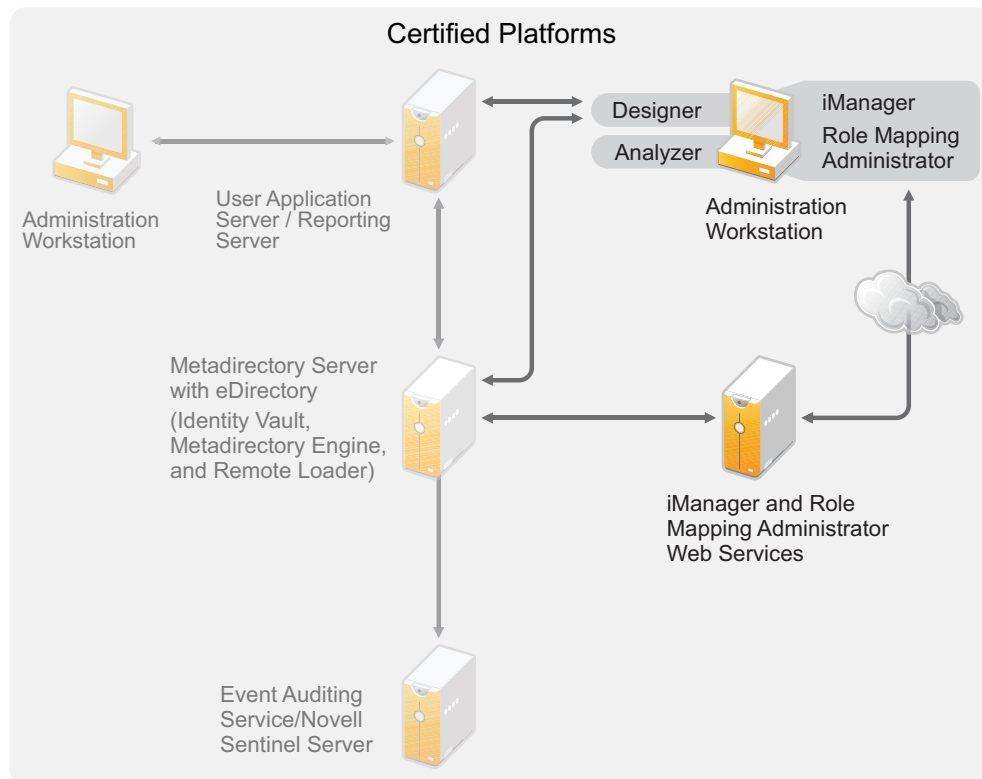
## 2.4 Role Mapping Administrator

The Novell Identity Manager Role Mapping Administrator lets you map managed systems roles, composite roles, and profiles (collectively referred to as authorizations) to Identity Manager roles. When a user is assigned a role through the Identity Manager Roles Based Provisioning Module, he or she receives all authorizations mapped to that role. See the “[System Requirements](#)” section in the *Novell Identity Manager Role Mapping Administrator 4.0.2 User Guide* for a list of Role Mapping Administrator system requirements.

## 2.5 iManager, Designer, and Analyzer

To install iManager, Designer, Analyzer, and the Role Mapping Administrator, select each of them individually from the corresponding check boxes on the Select Components page of the installation. [Figure 2-3](#) illustrates these components.

**Figure 2-3** Tools for Identity Manager



For system requirements information, refer to the individual component documentation.

- ♦ iManager: See the [Installing iManager \(http://www.novell.com/documentation/imanager27/imanager\\_install\\_274/data/alw39eb.html\)](http://www.novell.com/documentation/imanager27/imanager_install_274/data/alw39eb.html) section in the *Novell iManager 2.7 Installation Guide*.
- ♦ Designer: See the “[Hardware Requirements](#)” section in the *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide*.
- ♦ Analyzer: See the “[Installing Analyzer](#)” section in the *Analyzer 4.0.2 for Identity Manager Administration Guide*.
- ♦ Role Mapping Administrator: See the “[System Requirements](#)” section in the *Identity Manager Role Mapping Administrator 4.0.2 Installation and Configuration Guide*.

## 2.5.1 Web Browsers

The supported Web browsers for managing Identity Manager are:

- ♦ Internet Explorer 8 and 9 are certified. The later versions are supported.
- ♦ Firefox 10 is certified and supported.

---

# 3 System Requirements

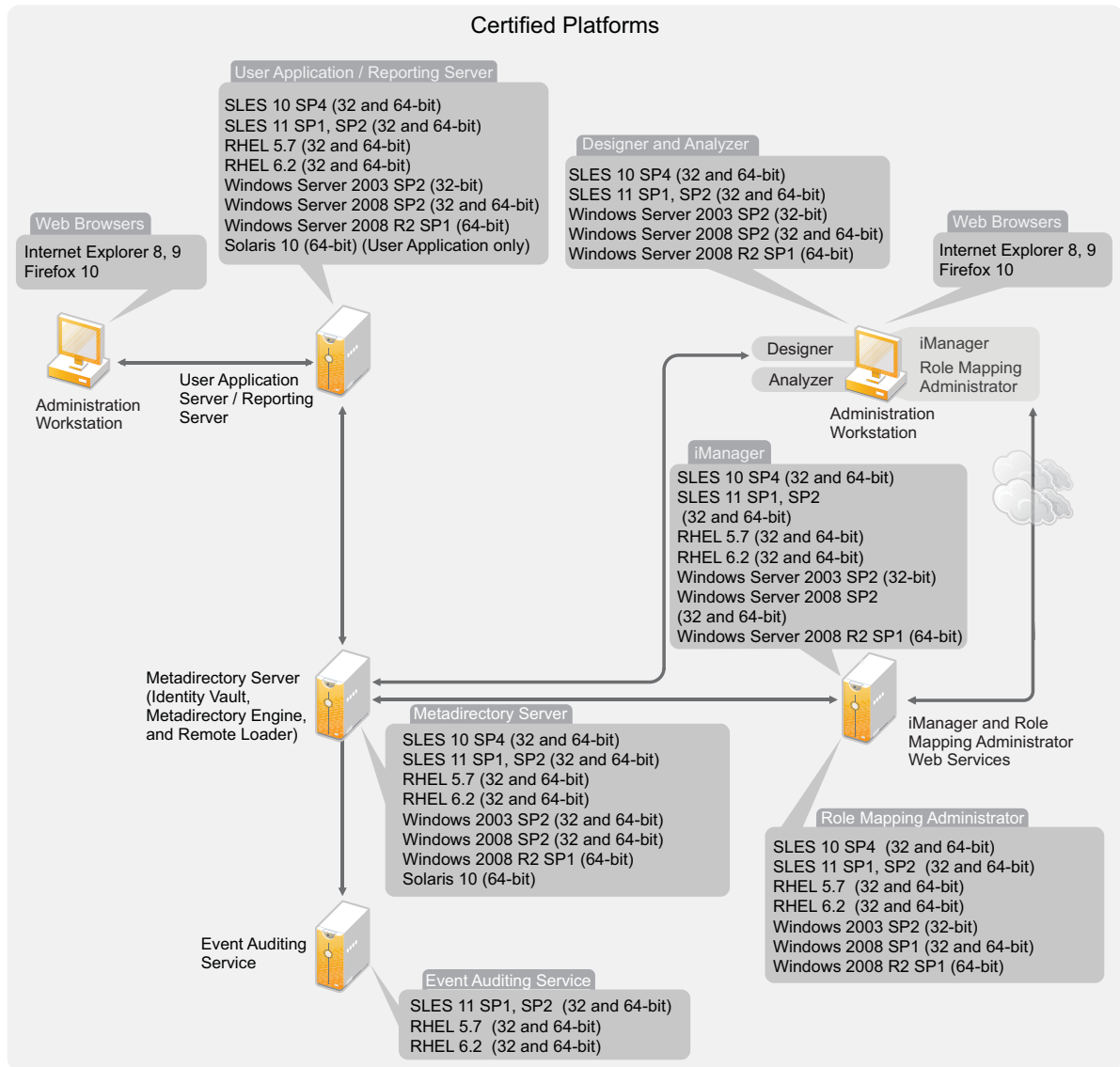
The components of Novell Identity Manager can be installed on multiple systems and platforms by using the integrated installer.

- ♦ [Section 3.1, “Supported Platforms,” on page 19](#)
- ♦ [Section 3.2, “Resource Requirements,” on page 21](#)
- ♦ [Section 3.3, “Ports Used by the Identity Manager Services,” on page 21](#)

## 3.1 Supported Platforms

[Figure 3-1](#) shows platforms supported by the Novell Identity Manager 4.0.2 integrated installer. For a detailed list of supported and certified platforms, refer to [Table 2-1](#) and [Table 2-2](#).

**Figure 3-1** System Requirements for the Identity Manager Integrated Installer



**NOTE:** Open Enterprise Server is not supported with the Identity Manager integrated installer.

With Identity Manager 4.0.2, the Event Auditing Service is supported on the SLES platforms and RHEL 5.7 and above. If Event Auditing Service server is installed on a remote machine, the integrated installer displays an additional field for Identity Reporting configuration that allows you to specify the Event Auditing Service system password for the server. Copy the system password from the `/etc/opt/novell/sentinel_eas/config/activemqusers.properties` file on the machine where Event Auditing Service is installed, and paste it into the Event Auditing Service *system password* field.

You cannot install all Identity Manager components on all platforms. For example, the only component supported on Solaris is Metadirectory server. Event Auditing Service is supported only on Linux and RHEL platforms.

## 3.2 Resource Requirements

In addition to the platform requirements mentioned above, ensure that you have the following resource requirements in order to install and configure all Identity Manager components:

- ♦ A minimum of 4096 MB RAM.
- ♦ 10 GB available disk space to install all the components.
- ♦ Additional disk space to configure and populate data. This might vary depending on your connected systems and number of objects in the Identity Vault.
- ♦ A multi-CPU server with a 2 GHz processor is preferred.

---

**NOTE:** These specifications might vary, depending on your deployment environment.

---

## 3.3 Ports Used by the Identity Manager Services

Ensure that the following ports are free before you start the installation. Run the `netstat -anp | egrep` command to check if these ports are free.

**Table 3-1** Ports used by the Identity Manager Services

Port	Used By Service
389	LDAP
524	NCP
636	LDAP with SSL
5432	Postgres Database for Role-based Provisioning Module
7707	Managed System Gateway
8028	iMonitor (eDirectory)
8080	Tomcat for iManager
8081	Role Mapping Administrator
8180	JBoss
8443	iManager with SSL
15432	Postgres Database for Identity Reporting Module



---

# 4 Installing Identity Manager

You can install and configure all components at the same time or in different runs by using the integrated installer. If you want to install each component separately, use the individual installers to install the Identity Manager components in the order specified in the “[Installing Identity Manager](#)” section in the *Identity Manager 4.0.2 Framework Installation Guide*. For an explanation of the different components, see the *Identity Manager 4.0.2 Overview Guide*.

For a list of the different components that the Identity Manager integrated installer installs, see [Chapter 1, “Integrated Installer Overview,” on page 7](#). For detailed information on each component, see the *Identity Manager 4.0.2 Overview Guide*.

The following sections do not provide step-by-step installation instructions because the installation interface is mostly self-explanatory. They do, however, provide information about important steps in the process that you might need help with.

- ♦ [Section 4.1, “Downloading the ISO File,” on page 23](#)
- ♦ [Section 4.2, “New Installation by Using Physical Media or an ISO,” on page 25](#)
- ♦ [Section 4.3, “Post-Installation Procedure,” on page 36](#)
- ♦ [Section 4.4, “Silent Installation and Configuration,” on page 37](#)
- ♦ [Section 4.5, “Language Support for the Identity Manager Installers,” on page 38](#)

For information about upgrading an existing Identity Manager installation, see [Chapter 6, “Upgrading Identity Manager,” on page 45](#).

## 4.1 Downloading the ISO File

Identity Manager 4.0.2 is available in the Advanced Edition and the Standard Edition. There are separate ISOs for each of them. The Identity Manager 4.0.2 Advanced Edition includes a complete set of features for enterprise-class user provisioning. To meet varying customer requirements, the Identity Manager Standard Edition includes a subset of features available in the Identity Manager Advanced Edition. The Standard Edition continues to provide all the features that were present in the previous versions of Identity Manager. For more information on the Identity Manager 4.0.2 Advanced Edition and Identity Manager Standard Edition, see “[Identity Manager 4.0.2 Features](#)” in the *Identity Manager 4.0.2 Overview Guide*.

You can purchase the edition that most closely meets your business requirements. Or you can download an evaluation copy of Identity Manager and use it for 90 days free of charge. However, the Identity Manager components must be activated within 90 days of installation, or they will shut down. At any time during the 90 days, or afterward, you can choose to purchase a product license and activate Identity Manager. For more information, see [Chapter 5, “Activating Novell Identity Manager Products,” on page 41](#).

To download Identity Manager and its services:

- 1 Go to the [Novell Downloads Web site \(http://download.novell.com\)](http://download.novell.com).
- 2 In the *Product or Technology* menu, select *Novell Identity Manager*, then click *Search*.
- 3 On the Novell Identity Manager Downloads page, click the *Download* button next to a file you want. [Table 4-1](#) contains a description of each file.
- 4 Based on your requirements, select an appropriate ISO. Each ISO contains the 32-bit and 64-bit versions of the product.
- 5 Follow the on-screen prompts to download the file to a directory on your computer.
- 6 Repeat from [Step 3](#) until you have downloaded all the files you need.
- 7 Either mount the downloaded `.iso` file as a volume, or use the `.iso` file to create a DVD of the software. If you haven't already verified that the media you burned is valid, you can check it by using the *Media Check* option.

---

**NOTE:** The Linux ISO files should be copied onto a double layer DVD due to the large size of the ISO files.

---

**Table 4-1** Identity Manager ISO Images

ISO	Platform	Description
Identity_Manager_4.0.2_Linux_Advanced.iso	Linux	Contains the DVD image for the Metadirectory server, Event Auditing Service, Designer, iManager, Role Mapping Administrator, Analyzer, Identity Reporting Module, and Roles Based Provisioning Module.
Identity_Manager_4.0.2_Linux_Standard.iso	Linux	Contains the DVD image for the Metadirectory server, Event Auditing Service, Designer, iManager, Analyzer, Identity Reporting Module, and Roles Based Provisioning Module.
Identity_Manager_4.0.2_Windows_Advanced.iso	Windows	Contains the DVD image for the Metadirectory server, Designer, iManager, Role Mapping Administrator, Analyzer, Identity Reporting Module, and Roles Based Provisioning Module.
Identity_Manager_4.0.2_Windows_Standard.iso	Windows	Contains the DVD image for the Metadirectory server, Designer, iManager, Analyzer, Identity Reporting Module, and Roles Based Provisioning Module.
Identity_Manager_4.0.2_Solaris_Advanced.iso	Solaris	Contains the DVD image for the Metadirectory server. Other components are not supported on the Solaris platform.
Identity_Manager_4.0.2_Solaris_Standard.iso	Solaris	Contains the DVD image for the Metadirectory server. Other components are not supported on the Solaris platform.

---

**IMPORTANT:** The Identity Manager integrated installer ships a convenience installer of JBoss community edition and PostgreSQL database. You can install these components without having to download them separately from their download sites. However, Novell does not provide information on updates, administration, configuration, or tuning for these components beyond what



is outlined in the [RBPM documentation \(http://www.netiq.com/documentation/idm402/install/data/front.html\)](http://www.netiq.com/documentation/idm402/install/data/front.html). For creating a production or staging environment, it is recommended to use individual installers of RBPM with the enterprise application server and database.

---

To switch from the Identity Manager Advanced Edition to the Standard Edition, uninstall the Advanced Edition and then install the Standard Edition. To upgrade from the Standard Edition to the Advanced Edition, use the Identity Manager Advanced Edition ISO. You need to apply the correct activation to be able to upgrade to Advanced Edition. For more information on upgrading from the Standard Edition to the Advanced Edition, see *Identity Manager 4.0.2 Upgrade and Migration Guide*.

## 4.2 New Installation by Using Physical Media or an ISO

The integrated installer helps you to install the binary files for the Identity Manager components and to configure the components.

If you are installing Identity Manager through integrated installer on 64-bit SLES 11 platform, make sure that `libgthread-2_0-0-32bit-2.17.2+2.17.3+20080708+r7171-3.1.x86_64.rpm` compat library is installed before starting the installation.

By default, `libstdc++33-32bit` is not installed on SLES 11SP1 (64-bit). When this library is not present, the integrated installer succeeds with no errors, but logging into iManager fails with a client error. If you run the iManager installer separately, the iManager installer identified that this library is not present and prompts you to install it.

Ensure that you install the following libraries before installing Identity Manager on RHEL 6.x:

- ◆ **For GUI Install:** Before invoking the Identity Manager installer, manually install the dependant libraries.
  - ◆ **For a 64-bit RHEL:** Install the following libraries in the same order:
    1. `libXau-1.0.5-1.el6.i686.rpm`
    2. `libxcb-1.5-1.el6.i686.rpm`
    3. `libX11-1.3-2.el6.i686.rpm`
    4. `libXext-1.1-3.el6.i686.rpm`
    5. `libXi-1.3-3.el6.i686.rpm`
    6. `libXtst-1.0.99.2-3.el6.i686.rpm`
    7. `glibc-2.12-1.7.el6.i686.rpm`
    8. `libstdc++-4.4.4-13.el6.i686.rpm`
    9. `libgcc-4.4.4-13.el6.i686.rpm`
    10. `compat-libstdc++-33-3.2.3-69.el6.x86_64.rpm`
    11. `compat-libstdc++-33-3.2.3-69.el6.i686.rpm`
    12. `libXrender-0.9.7-2.el6.i686.rpm`
  - ◆ **For a 32-bit RHEL:** Install the following library:
    - ◆ `compat-libstdc++-33-3.2.3-69.el6.i686.rpm`
- ◆ **For Package Install on RHEL 6.x:** Before invoking the Identity Manager installer, you must manually set up a repository for the installation media.
  1. (Conditional) If you are copying the ISO to the server, run the following command:

```
#mount -o loop <path to iso>/mnt/rhes62
```

2. (Conditional) If you are copying to a CD or a DVD, and to the server, run the following command:

```
#mount /dev/cdrom/mnt/rhes62
```

3. (Conditional) If you have mounted the ISO, create a repository file in the `/etc/yum.repos.d` location and perform the following configuration steps:

```
#vi /etc/yum.repos.d/rhes.repo
[redhat-enterprise]
name=RedHat Enterprise $releasever - $basearch
baseurl=file:///mnt/rhes62/
enabled=1
```

4. (Optional) If you are using an installation server, configure the following in `vi /etc/yum.repos.d/rhes.repo`:

```
[redhat-enterprise]
name=RedHat Enterprise $releasever - $basearch
baseurl=<url to the installation source>
enabled=1
```

5. Run the following commands after setting up the repository:

```
# yum clean all
# yum repolist
# yum makecache
```

6. To install the 32-bit packages, change “`exactarch=1`” to “`exactarch=0`” in the `/etc/yum.conf` file.

7. Install the GPG key by using the `rpm import <path / url> to RPM-GPG-KEY-redhat-release` command:

```
# rpm --import /mnt/rhes62/RPM-GPG-KEY-redhat-release
```

or

```
# rpm --import http://<url>/RPM-GPG-KEY-redhat-release
```

8. (Optional) To install the required packages for Identity Manager 4.x, execute the following script:

```
#!/bin/bash

PKGS="libXau.i686 libxcb.i686 libX11.i686 libXext.i686 libXi.i686
libXtst.i686
glibc.i686 libstdc++.i686 libgcc.i686 compat-libstdc++-33.i686
compat-libstdc++-33.x86_64"
for PKG in $PKGS ; do
    yum -y install "$PKG"
done
```

---

**NOTE:** The script cannot locate `compat-libstdc++-33.x86_64` library in the 32-bit repository unless you have modified the 64-bit repository and installed the RPM separately.

---

- ♦ **For Non-GUI Install:** Before invoking the Identity Manager installer, manually install the dependant libraries.

- ♦ **For a 64-bit RHEL:** Install the following libraries in the same order:

1. `glibc-2.12-1.7.el6.i686.rpm`
2. `libstdc++-4.4.4-13.el6.i686.rpm`
3. `libgcc-4.4.4-13.el6.i686.rpm`
4. `compat-libstdc++-33-3.2.3-69.el6.x86_64.rpm`

5. `compat-libstdc++-33-3.2.3-69.el6.i686.rpm`
  6. `libXrender-0.9.7-2.el6.i686.rpm`
- ◆ **For a 32-bit RHEL:** Install the following library:
    - ◆ `compat-libstdc++-33-3.2.3-69.el6.i686.rpm`

---

**NOTE:** Ensure that the `unzip` rpm is installed before installing Identity Manager. This is applicable for all Linux platforms.

---

- ◆ [Section 4.2.1, “Installation,” on page 27](#)
- ◆ [Section 4.2.2, “Configuration,” on page 28](#)

## 4.2.1 Installation

- 1 Access the Identity Manager 4.0.2 installation files either by mounting the `.iso` file or accessing the DVD you created from the `.iso` file.

For more information, see [Section 4.1, “Downloading the ISO File,” on page 23](#).

- 2 Go to the mount directory and start the installation by using the correct program for your platform.

**Linux/Solaris:** `./install.bin`

To execute the binary file, enter `./install.bin`.

**Windows:** `install.exe`

- 3 Use the following information to complete the installation:

**Introduction:** Select the language for your installation, then review the components you can install.

**License Agreement:** Read and accept the license agreement.

**Select Components:** Select the desired components to install. The options are:

- ◆ Metadirectory Server
- ◆ Roles Based Provisioning Module
- ◆ Event Auditing Service
- ◆ Identity Reporting Module
- ◆ Role Mapping Administrator
- ◆ iManager
- ◆ Designer
- ◆ Analyzer

---

**NOTE:** You can install Roles Based Provisioning Module and Identity Reporting Module on a system that doesn't have the Identity Vault. But you must always install the Roles Based Provisioning Module and the Identity Reporting Module on the same system.

---

**Choose Installation Folder:** Specify the base folder where Identity Manager and all of the components are to be installed. This option is only applicable for Windows.

UNIX installations have a predefined installation path. The integrated installer installs components in the following predefined installation paths:

- ◆ eDirectory and Identity Manager: `/opt/novell/eDirectory`

- ◆ Roles Based Provisioning Module, Reporting Module, Role Mapping Administrator, Designer, and Analyzer: `/opt/novell/idm`
- ◆ Event Auditing Service: `/opt/novell/sentinel_eas`

**Pre-Installation Summary:** Review the Pre-Installation summary page, which contains information about the selected components, then proceed with the installation. To change any of these settings, click *Previous*.

**Installation Complete Summary:** Review the post-installation summary to verify the installation status of the selected components and the location of the log file for each component. See [Table 4-2 on page 37](#) for information about the location of the log files.

**Continue for Configuration:** (Conditional) This check box is enabled only when the selected components are configurable. If you want to continue with configuration, continue with [Section 4.2.2, “Configuration,” on page 28](#). If you don’t want to continue with the configuration, deselect this check box.

## 4.2.2 Configuration

You can configure the Identity Manager components that you have already installed by using the integrated installer. Verify you have completed [Section 4.2.1, “Installation,” on page 27](#) before preceding with the configuration.

---

**IMPORTANT:** When you are create a new tree or add to an existing tree, if the `/etc/hosts` file contains 127.0.0.2 entry, the configuration fails because default IP certificate is created for the 127.0.0.2 loopback address. For a successful configuration, comment the 127.0.0.2 loopback address and make sure that 127.0.0.1 loopback address and the real IP address is in the file.

---

To configure the Identity Manager components:

- 1 If you are continuing from [Step 3 on page 27](#) in the installation procedure, skip to [Step 2](#). Otherwise, start the configuration with the correct program for your platform:

**Linux:** `./configure.bin`

**Solaris:** `./configure.bin`

To execute the binary file, enter `./configure.bin`.

**Windows:** `configure.exe`

- 2 Select the components you want to configure, click *Next*.
- 3 Select one of the following options to complete the configuration of the Identity Manager components:
  - ◆ [“Creating a New Tree” on page 29](#)
  - ◆ [“Adding to an Existing Tree” on page 33](#)

You must take a note of the following information before proceeding with the configuration of Identity Manager components:

- ◆ If you are adding to an existing tree, run the `NrfCaseUpdate` utility on the primary server to support mixed-case searching on roles and resources if the primary server has Identity Manager 3.6 or above.

If you don’t run the `NrfCaseUpdate` utility, Metadirectory server configuration fails. For more information on running the `NrfCaseUpdate` utility, see [“Running the NrfCaseUpdate Utility” in the Identity Manager Roles Based Provisioning Module 4.0.2 User Application: Installation Guide](#).

- ♦ The integrated installer does not perform a health check before the secondary server addition. You must run `ndscheck` before adding secondary server through integrated installer. On Windows, run the `ndscheck` from the `<install location>\NDS` location. On Linux/Solaris, run it from the `/opt/novell/eDirectory/bin/ndscheck` directory. Specify the mandatory parameters and run the command as follows:

```
ndscheck [-h <hostname port>] [-a <admin FDN>] [[-w <password>]
```

- ♦ The `logevent.cfg` file is modified with the logging server details on both Windows and Linux platforms when either the Roles Based Provisioning Module or the Identity Reporting Module is configured through integrated installer. If you are configuring only Metadirectory server, manually add the logging server details to the `logevent.cfg` file.

## Creating a New Tree

The fields that appear depend on the components you selected to configure in the previous page.

- 1 Use the following information to configure your Identity Manager components if you selected to create a new tree.
  - ♦ [“Identity Vault” on page 29](#)
  - ♦ [“Identity Vault > Advanced” on page 29](#)
  - ♦ [“Roles Based Provisioning Module \(RBPM\)” on page 30](#)
  - ♦ [“Roles Based Provisioning Module \(RBPM\) > Advanced” on page 31](#)
  - ♦ [“Identity Reporting Module” on page 31](#)
  - ♦ [“Identity Reporting Module > Advanced” on page 31](#)
  - ♦ [“Event Auditing Service” on page 32](#)
  - ♦ [“Event Auditing Service > Advanced” on page 32](#)
  - ♦ [“iManager > Advanced” on page 32](#)
- 2 Review the preconfiguration summary, then click *Configure*.
- 3 Review the configuration summary page, then click *Done*.

If there were problems during the configuration, review the configuration logs. For more information, see [“Locating Log Files and Properties Files” on page 37](#).

### Identity Vault

Fill in the following fields to create a new tree:

**New tree name:** Specify a name for the new tree.

**Admin password:** Specify a password for the Identity Vault administrator.

**Confirm admin password:** Specify the password for the Identity Vault administrator again.

### Identity Vault > Advanced

Select *Advanced* if you want to customize the tree that is created. Fill in the following fields to customize the tree:

**Admin name:** Specify the name of the Identity Vault administrator user.

**NCP port:** Either leave the default value of 524 for the NCP port or change the value of the port. NCP is the core eDirectory communications protocol.

**LDAP port:** Either leave the default value of 389 for the LDAP port or change the value of the port.

**LDAP secure port:** Either leave the default value of 636 for the LDAP secure port or change the value of the port.

**HTTP port:** Either leave the default value of 8028 for the HTTP port or change the value of the port.

**HTTP secure port:** Either leave the default value of 8030 for the HTTP secure port or change the value of the port.

**Instance path:** If your server is Linux/UNIX, you can run multiple instances of eDirectory on one server. Specify the path of this eDirectory instance on this server. The default path is `/var/opt/novell/eDirectory`.

**DIB path:** Specify the path for your eDirectory database (DIB). The default location of the DIB is:

- ♦ **Linux/UNIX:** `/var/opt/novell/eDirectory/data/dib`
- ♦ **Windows:** `c:\Novell\IdentityManager\NDS\DIBFiles\`

---

**NOTE:** DIB files must always reside inside the `\NDS` folder. If you change the default location of the DIB on Windows, for example `\NDS\DIBFiles\`, the configuration of the Metadirectory server fails.

---

**Require TLS for simple binds with password:** Select this option to require all LDAP connections to be on the secure port (default 636). If you deselect this option, users authenticating to LDAP server on the clear text port (default 389) pass their passwords in clear text. For more information, see ["Communicating with eDirectory through LDAP"](http://www.novell.com/documentation/edir88/edirin88/data/a7f08y1.html) (<http://www.novell.com/documentation/edir88/edirin88/data/a7f08y1.html>) in the *Novell eDirectory 8.8 Installation Guide* (<http://www.novell.com/documentation/edir88/edirin88/data/a2iii88.html>).

## Roles Based Provisioning Module (RBPM)

Fill in the following fields to configure the RBPM and your Event Auditing Service (EAS), which is part of the Identity Reporting Module:

**EAS server address:** Specify the DNS name or IP address of the server that hosts the EAS. You can either use this server or add another server. The Identity Reporting Module can be configured on only one EAS server.

**idmadmin DB user password:** Specify the password for the database user. This database stores information for reports.

**User Application admin password:** Specify the password for the User Application administrator.

**(Conditional) Security Admin password:** Specify the password for the security administrator.

This field is required only for the Identity Manager Standard Edition.

**(Conditional) Confirm Security Admin password:** Specify the password for the security administrator again.

This field is required only for the Identity Manager Standard Edition.

**(Conditional) Reporting Admin password:** Specify the password for the Identity Reporting administrator.

This field is required only for the Identity Manager Standard Edition.

**(Conditional) Confirm Reporting Admin password:** Specify the password for the Identity Reporting administrator again.

This field is required only for the Identity Manager Standard Edition.

## Roles Based Provisioning Module (RBPM) > Advanced

Select *Advanced* if you want to customize the configuration of the RBPM.

**User Application address:** Specify the DNS name or IP address of the server that hosts the User Application.

**User Application user:** Specify name for the administrative user for the User Application.

**(Conditional) Security Admin name:** Specify the name for the security administrator for the User Application. This role gives members the full range of capabilities within the Security domain. The Security administrator can perform all possible actions for all objects within the Security domain.

This field is required only for the Identity Manager Standard Edition.

**(Conditional) Reporting Admin name:** Specify the name for the Reporting administrator. This user has full range of capabilities within the Reporting domain. The Reporting administrator can perform all actions for all objects within the Reporting domain.

This field is required only for the Identity Manager Standard Edition.

## Identity Reporting Module

Fill in the following fields to configure the Identity Reporting Module:

**EAS system password:** Specify the password for the idmrptsrv user. The idmrptsrv user is the owner of the database schemas and objects for reporting.

**idmrptsrv user password:** Specify the password for the idmrptsrv user. The idmrptsrv user is the owner of the database schemas and objects for reporting.

**idmrptuser password:** Specify the password for the idmrptuser. This is a user with read-only access to the reporting data.

**Database host address:** Specify the DNS name or the IP address of the server that is running your database.

**Database port:** Specify the port of the server that is running your database. Either leave the default value of 15432 for the Database port or change the value of the port.

**EAS dbauser password:** Specify the password for the dbauser (database administrator).

**(Conditional) Managed System Gateway port:** Specify the port that the Managed System Gateway driver communicates on.

This field is required only for the Identity Manager Advanced Edition.

**Data Collection Service address:** Specify the IP address or the DNS name of the Data Collection Service server.

**Identity Vault tree name:** Specify the name of an Identity Vault that your server connects to. The server can connect to an existing tree or a remote Identity Vault.

**Driver set name:** Specify the name for the new driver set that is created during the configuration of the Identity Reporting Module.

## Identity Reporting Module > Advanced

Select *Advanced* to customize the configuration of the Identity Reporting Module. Fill in the following fields to customize the Identity Reporting Module:

**Enable subcontainer search:** Select this option to enable the Identity Reporting Module to perform subcontainer searches to gather information for reports.

**Secure LDAP:** Select whether the server communicates over a secure LDAP connection.

**LDAP port:** If you have selected secure LDAP for communication, specify the LDAP secure port. Otherwise specify the clear text port.

**Token expiration value (in minutes):** Specify the number of minutes to retain the token for authentication.

**Reporting unit:** Select *Day*, *Week*, or *Month*.

**Report retention value:** Specify how long a report is retained. If the reporting unit is set to *Day*, and the report retention value is 1, the reports are maintained for 1 day before they are deleted.

**Subcontainer login attribute:** If you enable subcontainer searches, you need to provide the login attribute that is used for searching the subtree of the user container.

**SMTP server address:** Specify the DNS name or the IP address of the SMTP server to configure e-mails for the report notifications.

**SMTP server port:** Either leave 456 as the default port for the SMTP server port or change it.

**SMTP user e-mail:** Specify the e-mail address to use for authentication, when authentication is enabled.

**SMTP user password:** Specify the password for the SMTP user.

**Default e-mail address:** Specify a default e-mail address to use, if the person who runs the report does not have an e-mail address specified in the Identity Vault.

**SMTP use SSL:** Select this option if the SMTP server uses an SSL connection.

**Server needs authentication:** Select this option if authentication is required for the SMTP server.

## Event Auditing Service

Filling the following fields to configure the Event Auditing Service:

**Admin password:** Specify the password for the administrative user.

**Database admin password:** Specify the password for the database admin.

## Event Auditing Service > Advanced

Select *Advanced* to customize the configuration of the Event Auditing Service:

**PostgreSQL port:** Either leave the default value of 15432 for the PostgreSQL port or change it.

**Enable port forwarding:** Select this option to enable port forwarding or deselect it to disable port forwarding.

## iManager > Advanced

There are only advanced configuration options for iManager. Select *Advanced* to display these options:

**HTTP port:** Either leave the default value of 8080 for the non-secure port or change it.

**HTTP secure port:** Either leave the default value of 8443 for the secure port or change it.



## Adding to an Existing Tree

The fields that appear depend on the components you selected to configure in the previous page.

- 1 Use the following information to configure the Identity Manager components if you selected to add this server to an existing tree.
  - ♦ [“Identity Vault” on page 33](#)
  - ♦ [“Identity Vault > Advanced” on page 33](#)
  - ♦ [“Metadirectory Server” on page 34](#)
  - ♦ [“Roles Based Provisioning Module \(RBPM\)” on page 34](#)
  - ♦ [“Roles Based Provisioning Module \(RBPM\) > Advanced” on page 35](#)
  - ♦ [“Identity Reporting Module” on page 35](#)
  - ♦ [“Event Auditing Service” on page 35](#)
  - ♦ [“iManager > Advanced” on page 35](#)
- 2 Review the configuration summary page, then click *Done*.

If there were problems during the configuration, review the configuration logs. For more information, see [“Locating Log Files and Properties Files” on page 37](#).

### Identity Vault

Fill in the following fields to allow your server to join an existing Identity Vault:

**Existing tree name:** Specify the name for the existing tree.

**Existing server address:** Specify the IP address of a server in your existing tree.

**Existing server port number:** Specify the NCP port of the server specified above. The default port for NCP is 524.

**Existing server admin name:** Specify the name of the existing server admin.

In Windows, the existing server admin name is the existing tree administrator name.

**Existing server admin context DN:** Specify the DN of container where you want this server placed in your existing tree. For example, `ou=server,o=system`.

In Windows, the existing server admin context DN is the existing tree admin context LDAP DN.

**Existing server admin password:** Specify the password for the administrative user specified above.

### Identity Vault > Advanced

Select *Advanced* if you want to customize this Identity Vault. Fill in the following fields to customize the Identity Vault:

**NCP port:** Either leave the default value of 524 for the NCP port or change the value of the port. NCP is the core eDirectory communications protocol.

**LDAP port:** Either leave the default value of 389 for the LDAP port or change the value of the port.

**LDAP secure port:** Either leave the default value of 636 for the LDAP secure port or change the value of the port.

**HTTP port:** Either leave the default value of 8028 for the HTTP port or change the value of the port.

**HTTP secure port:** Either leave the default value of 8030 for the HTTP secure port or change the value of the port.

**Instance path:** If your server is Linux/UNIX, you can run multiple instances of eDirectory on one server. Specify the path of this eDirectory instance on this server. The default path is `/var/opt/novell/eDirectory/data`.

**DIB path:** Specify the path for your eDirectory database (DIB). The default location of the DIB is:

- ♦ **Linux/UNIX:** `/var/opt/novell/eDirectory/data/DIB`
- ♦ **Windows:** `c:\Novell\Identity Manager\NDS\DIBfiles\`

---

**NOTE:** DIB files must always reside inside the `\NDS` folder. If you change the default location of the DIB on Windows, for example `\NDS\DIBfiles\`, the configuration of the Metadirectory server fails.

---

**Require TLS for simple binds with password:** Select this option to require all LDAP connections to be on the secure port (default 636). If you deselect this option, users authenticating to LDAP server on the clear text port (default 389) pass their passwords in clear text. For more information, see “Communicating with eDirectory through LDAP” in the *Novell eDirectory 8.8 Installation Guide* (<http://www.novell.com/documentation/edir88/edirin88/data/a2iii88.html>).

**Enable encrypted replication:** Select this option if you want the replication of your tree encrypted. For more information, see “Encrypted Replication” in the *Novell eDirectory 8.8 Administration Guide* (<http://www.novell.com/documentation/edir88/edir88/data/a2iii88.html>).

## Metadirectory Server

**Driver set name:** Specify the name for the new driver set that is created during the configuration of the Metadirectory server. Ensure that you do not use an existing driver set.

**Driver set context DN:** Specify the context where the new driver set is created in your tree.

## Roles Based Provisioning Module (RBPM)

Fill in the following fields to configure the RBPM and your Event Auditing Service (EAS), which is part of the Identity Reporting Module:

**EAS server address:** Specify the DNS name or IP address of the server that hosts the EAS. You can either use this server or add another server. The Identity Reporting Module can be configured on only one EAS server.

**idmadmin DB user password:** Specify the password for the database user. This database stores information for reports.

**User Application admin DN:** Specify the DN for the User Application administrator in LDAP format. The User Application administrator is authorized to perform all management functions for the Identity Manager User Application, including accessing the Administration tab of the Identity Manager user interface to perform any administration actions that it supports.

---

**IMPORTANT:** Ensure that you specify different DNs for *User App admin DN*, *Security admin DN*, and *Report Admin DN* fields. If these DNs are already present on the primary server, the User Application configuration fails.

---

**User Application admin password:** Specify the password for the User Application administrator.

**Confirm User Application admin password:** Specify the password for the User Application administrator again.

**User Application driver container DN:** Specify the root container DN for the User Application administrator in LDAP format. For example, o=data.

**(Conditional) Security admin DN:** Specify the DN for the security administrator in LDAP format. This role gives members the full range of capabilities within the Security domain. The Security administrator can perform all possible actions for all objects within the Security domain.

This field is required only for the Identity Manager Standard Edition.

**(Conditional) Security admin password:** Specify the password for the security administrator.

This field is required only for the Identity Manager Standard Edition.

**(Conditional) Reporting admin DN:** Specify the DN for the Reporting administrator in LDAP format. This user has full range of capabilities within the Reporting domain. The Reporting administrator can perform all actions for all objects within the Reporting domain.

This field is required only for the Identity Manager Standard Edition.

**(Conditional) Reporting admin password:** Specify the password for the reporting administrator.

This field is required only for the Identity Manager Standard Edition.

## Roles Based Provisioning Module (RBPM) > Advanced

The RBPM Advanced configuration options are the same for new tree and existing tree configurations. Refer to [“Roles Based Provisioning Module \(RBPM\) > Advanced”](#) on page 31.

With the secondary server installation after the RBPM configuration, you must change the *Authentication ID* of the User Application driver:

- 1 Log in to the existing tree through iManager.
- 2 Go to the *Identity Manager Administration > Identity Manager Overview* and select the driver set.
- 3 Click the *Edit Properties* option of the User Application driver, change the value of the *Authentication ID* option to that of the User Application admin in LDAP format.

## Identity Reporting Module

The Identity Reporting Module configuration options are the same for new tree and existing tree configurations. Refer to [“Identity Reporting Module”](#) on page 31 and [“Identity Reporting Module > Advanced”](#) on page 31.

## Event Auditing Service

The Event Auditing Service configuration options are the same for new tree and existing tree configurations. Refer to [“Event Auditing Service”](#) on page 32 and [“Event Auditing Service > Advanced”](#) on page 32.

## iManager > Advanced

The iManager configuration options are same for new tree and existing tree configurations. Refer to [“iManager > Advanced”](#) on page 32.

## 4.3 Post-Installation Procedure

The integrated installation program creates the DirXML-PasswordPolicy object in the Identity Vault and assigns it to the default driver set that it creates. Identity Manager requires this policy to be assigned to every driver set in the Identity Vault.

If the DirXML-PasswordPolicy object does not exist in the Identity Vault, perform the following steps to create it. The process uses the ldapmodify utility, located by default in the /opt/novell/eDirectory/bin directory on Linux servers and the install/utilities directory of the Identity Manager installation kit on Windows servers:

- 1 Create an LDAP Data Interchange Format (LDIF) file with the following attributes:

```
dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: add
nsimPwdRuleEnforcement: FALSE
nspmSpecialAsLastCharacter: TRUE
nspmSpecialAsFirstCharacter: TRUE
nspmSpecialCharactersAllowed: TRUE
nspmNumericAsLastCharacter: TRUE
nspmNumericAsFirstCharacter: TRUE
nspmNumericCharactersAllowed: TRUE
nspmMaximumLength: 64
nspmConfigurationOptions: 596
passwordUniqueRequired: FALSE
passwordMinimumLength: 1
passwordAllowChange: TRUE
objectClass: nspmPasswordPolicy
```

```
dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: modify
add: nsimAssignments
nsimAssignments: <driverset LDAP dn>
```

- 2 Import the attributes from the LDIF file to the Identity Manager server by using the ldapmodify utility.

- ◆ **Linux:** Run the following command:

```
ldapmodify -x -ZZ -c -h hostname_or_IP_address -p 389 -D
"cn=admin,ou=sa,o=system" -w password -f path_to_ldif_file
```

For example,

```
ldapmodify -x -ZZ -c -h server1.test.com -p 389 -D
"cn=admin,ou=sa,o=system" -w test123 -f /root/dirxmlpasswordpolicy.ldif
```

- ◆ **Windows:** Run ldapmodify.exe.

---

**NOTE:** If you are using the LDIF file from [Step 1](#), ensure that you use a text editor for modifying it to suit your requirement. Copying the content as is might insert some hidden special characters in the file. If you are prompted with `ldif_record() = 17` error message, inserting an extra space between the two DNs resolves the issue.

---

This creates the DirXML-PasswordPolicy object in the Identity Vault.

- 3 Assign the DirXML-PasswordPolicy object to each driver set in the Identity Vault.

For more information, see [Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide](#).

## Locating Log Files and Properties Files

The following table contains the location for the installation log (`ii_install.log`), configuration (`ii_configure.log`) logs, and the properties files. There is a properties file for each installed component.

**Table 4-2** Location of Log Files and Properties Files after Installation and Configuration

Platform	Log Files	Installation Properties Files
Windows	<code>&lt;Install_Location&gt;\install\logs</code>  Default location is <code>C:\Novell\IdentityManager\install\logs</code>	<code>&lt;Install_Location&gt;\install\propfiles</code>  Default location is <code>C:\Novell\IdentityManager\install\logs\propfiles\</code>
Linux/ Solaris	<code>/var/opt/novell/idm/install/logs</code>	<code>/var/opt/novell/idm/install/logs/propfiles/</code>

## 4.4 Silent Installation and Configuration

- ♦ [Section 4.4.1, “Silent Installation,” on page 37](#)
- ♦ [Section 4.4.2, “Silent Configuration,” on page 37](#)

### 4.4.1 Silent Installation

In order to run a silent installation of the Identity Manager components, you must create a properties file with the parameters necessary to complete the installation. There is a sample file included on the Identity Manager media:

- ♦ **Linux:** `./install/propfiles/install.properties`
- ♦ **Solaris:** `./install/propfiles/install.properties`
- ♦ **Windows:** `\install\propfiles\install.properties`

Start the silent installation by using the correct program for your platform:

- ♦ **Linux:** `./install.bin -i silent -f <filename>.properties`
- ♦ **Solaris:** `./install.bin -i silent -f <filename>.properties`  
To execute the binary file, enter `./install.bin -i silent -f <filename>.properties`.
- ♦ **Windows:** `\install.exe -i silent -f <filename>.properties`

### 4.4.2 Silent Configuration

You can run a silent configuration of the Identity Manager components by creating a properties file with the parameters necessary to complete the configuration for each component. There are two sample files included on the Identity Manager media. One is used for creating a new tree, and the other is used for adding a server to an existing tree.

- ♦ **Linux/Solaris:** See the following locations:
  - ♦ `./install/propfiles/configure_new_tree.properties`
  - ♦ `./install/propfiles/configure_existing_tree.properties`

- ♦ **Windows:** See the following locations:
  - ♦ `\install\propfiles\configure_new_tree.properties`
  - ♦ `IDM4.0.2_Win:\install\propfiles\configure_existing_tree.properties`

Add the following password variables to the silent properties file before invoking silent configuration:

- ♦ **Metadirectory Server:** `IA_IDVAULT_ADMIN_PASSWORD`.
- ♦ **Roles Based Provisioning Module:** `IA_RBPM_POSTGRESQL_DB_PASSWORD` and `IA_RBPM_USERAPPADMIN_PASSWORD`.
- ♦ **Identity Reporting Module:** `IA_REPORTING_NOVL_DB_USER_PASSWORD`, `IA_REPORTING_IDM_USER_PASSWORD`, and `IA_REPORTING_IDM_SERVER_PASSWORD`.
- ♦ **Event Auditing Service:** `IA_EAS_ADMIN_PWD` and `IA_EAS_DBA_PWD`.

Start the silent configuration by using the correct program for your platform:

- ♦ **Linux/Solaris:** `./configure.bin -i silent -f <filename>.properties`  
 To execute the binary file, enter `./configure.bin -i silent -f <filename>.properties`.
- ♦ **Windows:** `\configure.exe -i silent -f <filename>.properties`

You can use the sample properties files included on the Identity Manager media only when you plan to configure all the components in one run.

To see the mandatory parameters required for configuring each Identity Manager component, run the following command:

```
./install.bin -i silent -DSELECTED_PRODUCTS=<components to be configured> -f <filename>.properties
```

This command performs the following tasks:

- ♦ Checks if the components are installed.
- ♦ Starts configuring the installed components using the properties file.
- ♦ Lists all the mandatory parameters that are required to configure the components.

The description of the IDs for the Identity Manager components is available in the properties file.

Create a properties file with the output of this command, then add `SELECTED_PRODUCTS` with the components that you want to configure and rerun silent configuration for them.

## 4.5 Language Support for the Identity Manager Installers

Each of the Identity Manager installers support different languages.

- ♦ **Metadirectory Server:** French, German, Japanese, Simplified Chinese, and Traditional Chinese.
- ♦ **Integrated Installer:** French, German, Japanese, Simplified Chinese, and Traditional Chinese.
- ♦ **Roles Based Provisioning Module:** Brazilian Portuguese, Danish, Dutch, French, German, Italian, German, Japanese, Russian, Simplified Chinese, Spanish, Swedish, and Traditional Chinese.
- ♦ **Identity Reporting Module:** Brazilian Portuguese, Danish, Dutch, French, German, Italian, German, Japanese, Russian, Simplified Chinese, Spanish, Swedish, and Traditional Chinese.

- ♦ **Designer:** Brazilian Portuguese, Dutch, French, German, Italian, Japanese, Simplified Chinese, Spanish, and Traditional Chinese.

---

**NOTE:** On Linux, install the gettext utilities. The GNU gettext utilities provide a framework for internationalized and multilingual messages.

---

- ♦ **Analyzer:** English.
- ♦ **Role Mapping Administrator:** English.

The following conditions apply when an Identity Manager installer is launched:

- ♦ If the operating system is in a language supported by the Identity Manager installer, the language picker for the Identity Manager installer defaults to that language.
- ♦ If the operating system is in a language not supported by the Identity Manager installer, the language picker for the Identity Manager installer defaults to English.
- ♦ If the operating system is a Latin type language, all of the other Latin type languages will be available from the language picker.
- ♦ If the operating system is Asian or Russian, only the language of the operating system and English will be available in the language picker.

The Identity Manager installers detect the locale of a system and decide which language to support. To install a new language on your system, change the locale on Windows through the *Regional Settings* option. On Linux/Solaris, set the LANG variable in the profile or through the command line.

Identity Manager supports the following Latin type languages:

- ♦ Danish
- ♦ Dutch
- ♦ English
- ♦ French
- ♦ German
- ♦ Italian
- ♦ Portuguese (Brazilian)
- ♦ Spanish
- ♦ Swedish

Other languages supported by Identity Manager are:

- ♦ **Asian languages:** Japanese, Simplified Chinese, and Traditional Chinese.
- ♦ **Cyrillic languages:** Russian.

## 4.5.1 Non-Installer Language Considerations

Although Designer is localized in nine languages, the Identity Manager drivers are localized only in five languages. If the driver language is not supported, the driver configuration defaults to English.

All of the Identity Manager iManager plug-ins are translated into five languages. Four iManager plug-ins are translated into Spanish, Russian, Italian, and Portuguese. On localized systems, the localized plug-ins are translated, and all other plug-ins are in English. On Danish, Dutch, and Swedish systems, all plug-ins are in English.





---

# 5 Activating Novell Identity Manager Products

The information in this section explains how activation works for the Identity Manager components. The Identity Manager components must be activated within 90 days of installation, or they will shut down. At any time during the 90 days, or afterward, you can choose to activate Identity Manager products.

You can activate the Identity Manager components by completing the following tasks:

- ♦ [Section 5.1, “Purchasing an Identity Manager Product License,” on page 41](#)
- ♦ [Section 5.2, “Installing a Product Activation Credential,” on page 41](#)
- ♦ [Section 5.3, “Viewing Product Activations for Identity Manager and for Drivers,” on page 42](#)
- ♦ [Section 5.4, “Activating Identity Manager Drivers,” on page 43](#)
- ♦ [Section 5.5, “Activating Analyzer,” on page 43](#)
- ♦ [Section 5.6, “Activating Designer and the Role Mapping Administrator,” on page 43](#)

## 5.1 Purchasing an Identity Manager Product License

To purchase an Identity Manager product license, so that you can activate the product, see the [Novell Identity Manager How to Buy Web page \(http://www.novell.com/products/identitymanager/howtobuy.html\)](http://www.novell.com/products/identitymanager/howtobuy.html).

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

## 5.2 Installing a Product Activation Credential

You must install the Product Activation Credential via iManager.


- 1 After you purchase a license, Novell sends you an e-mail with your Customer ID. The e-mail contains a link under the Order Detail section to the site where you can obtain your credential. Click the link to go to the site.
- 2 Click the license download link and do one of the following:
  - ♦ Save the Product Activation Credential file to a convenient location.
  - or
  - ♦ Open the Product Activation Credential file, then copy the contents of the Product Activation Credential to your clipboard.

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

---

**WARNING:** If Standard Edition activation is applied to an existing non-activated Advanced Edition system, it stops the Identity Manager Metadirectory server and drivers.

---

- 3 Open iManager.
- 4 Select *Identity Manager > Identity Manager Overview*.
- 5 Click  to browse for and select a driver set in the tree structure.
- 6 On the Identity Manager Overview page, click the driver set that contains the driver to activate.
- 7 On the Driver Set Overview page, click *Activation > Installation*.
- 8 Select the driver set where you want to activate an Identity Manager component, then click *Next*.
- 9 Do one of the following:
  - ◆ Specify where you saved the Identity Manager Activation Credential, then click *Next*.
  - or
  - ◆ Paste the contents of the Identity Manager Activation Credential into the text area, then click *Next*.
- 10 Click *Finish*.



---

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

---

## 5.3 Viewing Product Activations for Identity Manager and for Drivers

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

- 1 Open iManager.
- 2 Click *Identity Manager > Identity Manager Overview*.
- 3 Click  to browse for and select a driver set in the tree structure, then click  to perform the search.
- 4 On the Identity Manager Overview page, click the driver set you want to view the activation information for.
- 5 On the Driver Set Overview page, click *Activation > Information*.

You can view the text of the activation credential or, if an error is reported, you can remove an activation credential.

---

**NOTE:** After installing a valid Product Activation Credential for a driver set, you might still see "Activation Required" next to the driver name. If this is the case, restart the driver and the message should then disappear.

---

## 5.4 Activating Identity Manager Drivers

Your Identity Manager purchase includes activations for service drivers and several common drivers.

- ◆ **Service Drivers:** The following service drivers are activated when you activate the Metadirectory server:
  - ◆ Data Collection Service
  - ◆ Entitlements Services
  - ◆ ID Provider
  - ◆ Loopback Service
  - ◆ Managed System Gateway
  - ◆ Manual Task Service
  - ◆ Null Service
  - ◆ Roles Service
  - ◆ User Application
  - ◆ WorkOrder
- ◆ **Common Drivers:** The following common drivers are activated when you activate the Metadirectory server:
  - ◆ Active Directory
  - ◆ ADAM
  - ◆ eDirectory
  - ◆ GroupWise
  - ◆ LDAP
  - ◆ Lotus Notes

Activations for all other Identity Manager drivers must be purchased separately. The activations for the drivers are sold as Identity Manager Integration modules. An Identity Manager Integration module can contain one or more drivers. You receive a Product Activation Credential for each Identity Manager Integration module that you purchase.

You must perform the steps in [Section 5.2, “Installing a Product Activation Credential,”](#) on page 41 for each Identity Manager Integration module to activate the drivers.

## 5.5 Activating Analyzer

The first time you launch Analyzer, you are prompted for an activation. If you do not enter the activation, you cannot use Analyzer. For more information, see [“Activating Analyzer”](#) in the *Analyzer 4.0.2 for Identity Manager Administration Guide*.

## 5.6 Activating Designer and the Role Mapping Administrator

Designer and the Role Mapping Administrator don't require additional activations beyond activating the Metadirectory server or drivers.



---

# 6 Upgrading Identity Manager

You cannot upgrade Identity Manager components through the integrated installer. Use the individual product installers for upgrading to Identity Manager 4.0.2. Upgrading from the Identity Manager 4.0.2 Standard Edition to the Advanced Edition has a different upgrade procedure, which involves only configuration changes. You do not need to run the Identity Manager installer for this upgrade. For more information on Identity Manager upgrades, refer to the “[Upgrading](#)” section in the *Identity Manager 4.0.2 Upgrade and Migration Guide*.



---

# 7 Troubleshooting Identity Manager

Keep in mind the following information when you install Identity Manager by using the integrated installer:

- ♦ “Figuring out installation issues” on page 47
- ♦ “Passing mandatory parameters during configuration” on page 48
- ♦ “Configuration fails if the hosts file contains 127.0.0.2 entry” on page 48
- ♦ “Installer throws java.io.FileNotFoundException” on page 49
- ♦ “Issues with invoking installer in the GUI mode” on page 49
- ♦ “On Linux, the Remote Loader does not install through integrated installer” on page 49
- ♦ “Tree name is auto generated when the tree name already exists” on page 49
- ♦ “Secondary server installation” on page 49
- ♦ “Check for free ports before starting the installation” on page 49
- ♦ “Detecting the current state of the system” on page 50
- ♦ “Changing password in RBPM” on page 50
- ♦ “The integrated installer does not properly handle the RBPM error codes” on page 51
- ♦ “Error displayed if the Identity Reporting Module and RBPM are separately configured” on page 51
- ♦ “The Restore Default button does not work during Identity Manager installation” on page 51
- ♦ “On Windows, the Metadirectory server uninstallation does not remove the lib directory” on page 51
- ♦ “Integrated installer might hang during the Identity Manager uninstallation on Windows” on page 51
- ♦ “Windows runtime distribution installation might force a reboot because of an install failure” on page 52
- ♦ “Configuring the ISO extracted through third-party ISO extraction tools on UNIX” on page 52
- ♦ “The integrated installer does not add a replica of an existing driver set during configuration” on page 52
- ♦ “Enabling XDAS degrades performance” on page 52
- ♦ “Identity Manager component uninstallation issues” on page 53
- ♦ “NoClassDefFound Exception in IBM WebSphere MQ V7.5” on page 54

## Figuring out installation issues

Action: If errors occur during Identity Manager installation, ensure that you refer to the log files depending on your platform:

- ♦ **Linux/Solaris:** /var/opt/novell/idm/install/logs/

- ◆ **Windows:** The default location is `C:\novell\IdentityManager\install\logs\`. You can change the location of the log files based on the install location you specify.

**Action:** For detecting typical failures, see the `ii_install.log` file for installation issues, `ii_configure.log` file for configuration issues, and `ii_uninstall.log` file for uninstallation issues. In the log files, look for text `exitValue = xxx`. If the value is not 0, a particular command execution has failed which in turn generates a log file. Refer to that log file for further details on the failure.

For example,

```
"/home/siva/build/products/Reporting/IDMReport.bin" -
DIA_USER_JRE_HOME="/opt/nov
ell/idm/jre" -i silent -f "/tmp/idmreporting_configure.properties"
execute command
  exitValue = 1
log file location    :/tmp/idmreporting_configure.properties
log file location    :/opt/novell/idm/rbpm/IDMReporting//
RPT_Install.log
```

The above snippet from the `ii_install.log` file indicates that the command has failed, because the `exitValue` is 1 (non-zero). For further analysis, refer to the `/opt/novell/idm/rbpm/IDMReporting/RPT_Install.log` as displayed in the command.

## Passing mandatory parameters during configuration

**Source:** During configuration, the installer might display the following error message after the configuration parameters are specified:

```
Some of the inputs are not proper. They are highlighted in Red.
```

**Possible Cause:** Based on the highlighted parameter, the cause of the error message could be one of the following:

- ◆ The port number is already in use.
- ◆ The passed DNS hostname is invalid.
- ◆ The DN format is incorrect.

**Action:** Do the following:

- ◆ Use a different port number if the port is already in use.
- ◆ Specify a valid DNS name or specify a valid IP address if you don't want to specify a DNS name.
- ◆ Verify that a valid DN is specified in LDAP format.

## Configuration fails if the hosts file contains 127.0.0.2 entry

**Possible Cause:** If the `/etc/hosts` file has an entry with the 127.0.0.2 loopback address, the default IP certificate is created for the 127.0.0.2 loopback address.

**Action:** Do the following:

Edit the `/etc/hosts` file if the hosts file has an entry with the 127.0.0.2 loopback address.

For example, 127.0.0.2 hostname. Comment it and make sure that the real IP address entry is in the file.



## Installer throws `java.io.FileNotFoundException`

Possible Cause: If the systems `tmp` directory is not present, the installer throws this exception soon after invoking the installer.

Action: Create the systems `tmp` directory.

## Issues with invoking installer in the GUI mode

Possible Cause: An error message displays when integrated installer is invoked in the GUI mode if the required RPMs are not present in the system. The integrated installer automatically switches to the console mode, which is not supported.

Action: Install the required RPMs before invoking the Identity Manager installer.

See [Identity Manager 4.0.2 Readme \(http://www.novell.com/documentation/idm402/readme/data/idm402\\_readme.html#bwnkb9a\)](http://www.novell.com/documentation/idm402/readme/data/idm402_readme.html#bwnkb9a) for a list of RPMs required for a successful installation and configuration of Identity Manager.

## On Linux, the Remote Loader does not install through integrated installer

Possible Cause: This issue occurs only with the `Identity_Manager_4.0.2_Linux_Advanced.iso` or the `Identity_Manager_4.0.2_Linux_Standard.iso` files.

Action: You must install the Remote Loader through the framework installer. Select either a 32-bit Remote Loader or a 64-bit Remote Loader in one installation instance, then run installation separately for each of them. The installation fails if you select both Remote Loaders in one installation instance. Only one Remote Loader can be installed at a time.

Also, port 8000 must be free to ensure a successful Identity Manager installation.

## Tree name is auto generated when the tree name already exists

Source: The integrated installer tries to automatically generate the tree name if that tree name already exists.

## Secondary server installation

Explanation: The integrated installer adds the replica holding the server object on all secondary server installations. It waits for the replica to turn on.

## Check for free ports before starting the installation

Explanation: Some services might not run because the ports required by them are occupied.

Action: Ensure that the following ports are free before you start the installation. Run the `netstat -anp | egrep` command to check if these ports are free.

```
netstat -anp | egrep
': (524|389|636|8028|8030|8090|8000|7707|8006
|8009|8081|8443|8009|8080|8443|1199|1198|119
0|3973|4544|4545|4546|4557|4812|4813|8109|81
83|8180|8543|29007|37022|8180|10013|10014|61
616|61617|1514|15432|5556|1289|1443|1468)'
```

For more information, see [Section 3.3, “Ports Used by the Identity Manager Services,”](#) on page 21.

## Detecting the current state of the system

**Explanation:** Ensure that you back up the installer state file. The integrated state file is an important configuration file used by the installer for information including the current state of the system, installed components, configured components, or uninstalled components.

**Action:** Locate the state file, then take a back up of the file.

- ♦ **Linux/Solaris:** The back up file is in the `/etc/opt/novell/idm/install/conf/install_state.conf` location.
- ♦ **Windows:** The back up file is in the `C:\Novell\conf\install_state.conf` location.

## Changing password in RBPM

**Possible Cause:** The RBPM expects the eDirectory server be set to require the use of `NMASLOGIN_FIRST` environment variable during login. The Identity Manager integrated installer automatically handles this by modifying the `pre_ndsd_start` script for Linux or the `HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\Environment` registry key for Windows.

If you perform a default eDirectory installation and apply a password policy to an existing user, then login as this user and perform a forgotten password procedure, you might see a message that says the Universal Password is not set after answering the challenge response questions.

**Action:** To work around this issue,

- 1 Linux/UNIX:** Add the following two lines to the `pre_ndsd_start` script located at `/opt/novell/eDirectory/sbin` (formerly in `/etc/init.d`):

```
NDSM_TRY_NMASLOGIN_FIRST=true
export NDSM_TRY_NMASLOGIN_FIRST
```

---

**IMPORTANT:** When `NDSM_TRY_NMASLOGIN_FIRST` is set to true, the user's password is set to expired and is configured to permit grace logins. If the user's password policy does not use grace logins, the user is not prompted to use grace logins. Instead, the user is prompted to change the password. This is because NMA removes the `loginGraceLimit` and `loginGraceRemaining` attributes during login if the password policy does not use grace logins.

If `NDSM_TRY_NMASLOGIN_FIRST` is not set to true, eDirectory does not enforce case sensitivity for passwords during login.

---

**Windows:** Right-click *My Computer* and select *Properties*. In the *Advanced* tab, click *Environment Variables*. Under *System Variables*, add the variable and set the value to *True*. This should be done on any server that might handle NMA logins via LDAP.

- 2** Restart eDirectory to apply the change.

## The integrated installer does not properly handle the RBPM error codes

**Possible Cause:** In some situations, the integrated installer does not properly handle the Roles Based Provisioning Module setup errors. This can happen when the Roles Based Provisioning Module configuration fails because of a problem with the driver configuration process. In this case, the integrated installer configuration summary displays a message indicating that the Roles Based Provisioning Module configuration passed, but the Roles Based Provisioning Module configuration has setup errors.

**Action:** When you encounter a problem, review the install logs located in the `logs` folder to determine the cause of the problem (`var\opt\novell\idm\install\logs`).

## Error displayed if the Identity Reporting Module and RBPM are separately configured

**Possible Cause:** The integrated installer displays the following error if Identity Reporting Module and the Roles Based Provisioning Module are separately configured:

```
'Failed to load users/passwords/role files'
```

**Action:** To work around this issue, either stop JBoss before installing the Identity Reporting Module or restart JBoss after installing the Identity Reporting Module.

## The Restore Default button does not work during Identity Manager installation

**Source:** During the Identity Manager installation, if you return to the Installation Location page from the subsequent page, the *Restore Default* button does not work as expected.

## On Windows, the Metadirectory server uninstallation does not remove the lib directory

**Source:** The jar files that reside in the `lib` directory are not removed. The uninstaller uninstalls other installed components.

**Action:** Manually remove the jar files.

## Integrated installer might hang during the Identity Manager uninstallation on Windows

**Possible Cause:** The installer tries to stop all the dependent services before uninstalling Identity Manager. Sometimes installer might not be able to stop the DHost service because some services depend on DHost.

**Action:** Do the following steps to check whether the installer hanged during the Identity Vault uninstallation:

- 1 Goto the *Control Panel*, open the *Novell eDirectory Services*, then click the *Startup* button. If the installer hangs, the following message displays:

Novell eDirectory Service is in a NT service Stop Pending State.

- 2 To continue with the uninstall, manually stop the DHost service from the Task Manager.

## Windows runtime distribution installation might force a reboot because of an install failure

Explanation: The Metadirectory installation fails with the following message in the *<Install Location>\ii\_install.log* file:

```
: \Users\Administrator\IDM4\products\eDirectory\x64\windows\x64\re
dist_pkg\vcredist_x86.exe" /q:a /c:"msiexec /i vcredist.msi /qn /l
C:\Users\ADMINI~1\AppData\Local\Temp\vcredist32_Windows_x64_Insta
ll.log"
execute command exitValue = 3010
```

Action: The 3010 error code returned by the vcredist executable is a success, which means that you must reboot the Windows machine. After the rebooting process, relaunch the installer and the installation continues normally. Rebooting the machine does not affect the earlier successful installations.

## Configuring the ISO extracted through third-party ISO extraction tools on UNIX

Explanation: The Identity Manager 4.0.2 integrated installer fails to configure if the ISO is extracted through third-party ISO extraction tools on UNIX.

Action: For successful configuration, use the `mount -o loop` command.

## The integrated installer does not add a replica of an existing driver set during configuration

Explanation: The integrated installer does not add a replica of an existing driver set during configuration.

Action: To workaroud the issue, perform the following steps:

1. Launch iManager.
2. Click *Roles and Tasks > Partitions and Replicas > Replicas view*, select the existing driver set, then click *Add Replica*.
3. Select the server name from the drop-down list and click *OK*.

## Enabling XDAS degrades performance

Possible Cause: With XDAS event logging enabled, Identity Manager engine performance is degraded without SLP configuration.

Action: SLP should be correctly configured and running to ensure that performance is not affected.

## Identity Manager component uninstallation issues

Source: During uninstallation if one or more components fail to uninstall, the *Uninstall* option is disabled if you retry uninstallation. One of the reasons for the uninstallation failure on Windows could be that the JAVA\_HOME and PATH variables are not set.

Action: Execute the individual component uninstallers as follows:

- ♦ **Linux/Solaris:** Run the following command to uninstall the individual components:

- ♦ **Metadirectory:** Uninstall the Identity Manager framework:

```
/root/idm/Uninstall_Identity_Manager/  
Uninstall_Identity_Manager
```

Uninstall the Identity Vault:

```
/opt/novell/eDirectory/sbin/nds-uninstall
```

- ♦ **JBoss:** Run the following command:

```
$IA_RBPM_POSTGRESQL_INSTALL_PATH$/  
JBossPostgreSQL_Uninstaller/Uninstall_JBossPostgreSQL
```

- ♦ **Roles Based Provisioning Module:** Run the following command:

```
java -jar /opt/novell/idm/rbpm/RemoveUserApp/  
uninstaller.jar
```

- ♦ **Identity Reporting Module:** Run the following command:

```
/opt/novell/idm/rbpm/Uninstall_Identity_Reporting/  
Uninstall_Identity_Reporting
```

- ♦ **Event Auditing Service:** Run the following command:

```
/opt/novell/sentinel_eas/Uninstall_Event_Auditing_Service/  
Uninstall_Event_Auditing_Service
```

- ♦ **Role Mapping Administrator:** Run the following command:

```
/opt/novell/idm/rma/rma-uninstall.sh -s
```

- ♦ **Designer:** Run the following command:

```
/opt/novell/idm/Designer/UninstallDesigner/Uninstall  
Designer_for_Identity_Manager
```

- ♦ **Analyzer:** Run the following command:

```
/opt/novell/idm/Analyzer/UninstallAnalyzer/Uninstall  
Analyzer_for_Identity_Manager
```

- ♦ **iManager:** Run the following command:

```
/var/opt/novell/tomcat5/webapps/nps/UninstallerData/  
UninstalliManager
```

- ♦ **Windows:** Except for the Role Mapping Administrator, uninstall all the components from *Windows > Add/Remove Programs*. To uninstall the Role Mapping Administrator, run `C:\novell\IdentityManager\RMA\rma-uninstall.bat` from the command prompt.

## NoClassDefFound Exception in IBM WebSphere MQ V7.5

Action: When you encounter this error, add `com.ibm.mq.jmqi.jar` in the classes folder.

---

# 8 Uninstalling Identity Manager

The uninstall script documented in section 8.1 “[GUI Uninstallation](#)” uninstalls all Identity Manager components that were installed with the integrated installer. If you want to uninstall a single component, see “[Uninstalling Identity Manager](#)” in the *Identity Manager 4.0.2 Framework Installation Guide*.

## 8.1 GUI Uninstallation

Ensure that the `JAVA_HOME` and `PATH` environment variables point to Java before the integrated uninstaller is invoked.

To uninstall the Identity Manager components:

- 1 Execute the uninstallation by using the correct program for your platform:

- ♦ **Linux/Solaris:** `./Uninstall_Identity_Manager_Components.bin`

The binary file is located by default in the `/root/idm/Uninstall_Identity_Manager` directory.

- ♦ **Windows:** `Uninstall_Identity_Manager_Components.exe`

The uninstaller is located by default in the `C:\Program Files\Novell\Identity Manager` directory. Alternatively, click *Add/Remove* programs to uninstall the Identity Manager components.

---

**NOTE:** The Identity Vault uninstallation does not remove all the files after it is uninstalled. Refer to the [eDirectory uninstallation documentation \(http://www.novell.com/documentation/edir88/edirin88/data/bnn8twh.html\)](http://www.novell.com/documentation/edir88/edirin88/data/bnn8twh.html) for more information.

---

- 2 Select the check box for each component that you want to uninstall, then click *Next*.
- 3 Specify the credentials for each of these components in LDAP format, then click *Next*.  
The uninstaller needs the credentials to deconfigure the components before uninstalling.
- 4 Review the summary for uninstalling the components, then click *Uninstall*.  
If you need to change any of your components, click *Previous*, and make those changes.
- 5 Review the Uninstall Complete Summary page that shows the list of the components that were successfully uninstalled, then click *Done* to complete the uninstallation process.

## 8.2 Silent Uninstallation

In order to run a silent uninstallation of the Identity Manager components, you must create a properties file with the parameters necessary to complete the uninstallation. There is a sample file included on the Identity Manager media:

- ♦ **Linux:** `./install/propfiles/uninstall.properties`

- ♦ **Solaris:** `./install/propfiles/uninstall.properties`
- ♦ **Windows:** `\install\propfiles\uninstall.properties`

Start the silent uninstallation by using the correct program for your platform:

- ♦ **Linux:** `/root/idm/Uninstall_Identity Manager/Uninstall_Identity_Manager.bin -i silent -f filename.properties`
- ♦ **Solaris:** `/root/idm/Uninstall_Identity Manager/Uninstall_Identity_Manager.bin -i silent -f filename.properties`
- ♦ **Windows:** `install location\Uninstall_Identity Manager Components\Uninstall Identity Manager Components.exe -i silent -f filename.properties`