

---

# NetIQ® Identity Manager Integrated Installation Guide

April 2015

## Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

**© 2015 NetIQ Corporation. All Rights Reserved.**

For information about NetIQ trademarks, see <https://www.netiq.com/company/legal/>.

---

# Contents

<b>About this Book and the Library</b>	<b>5</b>
<b>About NetIQ Corporation</b>	<b>7</b>
<b>1 Introduction</b>	<b>9</b>
1.1 Understanding the Differences between the Integrated Installation and the Standalone Installation Programs . . . . .	9
1.2 Understanding the Integrated Installation Process. . . . .	10
1.2.1 Identity Manager Server . . . . .	10
1.2.2 Identity Applications. . . . .	10
1.2.3 Identity Reporting. . . . .	11
1.2.4 Event Auditing Service. . . . .	11
1.2.5 iManager . . . . .	12
1.2.6 Designer . . . . .	12
1.2.7 Analyzer. . . . .	12
1.3 Understanding the Default Identity Vault Structure. . . . .	13
1.3.1 System Container . . . . .	14
1.3.2 Data Container. . . . .	15
1.3.3 Security Container . . . . .	15
<b>2 Planning to Install Identity Manager</b>	<b>17</b>
2.1 Installation Checklist. . . . .	17
2.2 Considerations for Using the Integrated Installation Program . . . . .	18
2.3 Prerequisites and System Requirements . . . . .	18
2.3.1 Prerequisites . . . . .	18
2.3.2 System Requirements . . . . .	20
2.3.3 Default Installation Locations. . . . .	21
<b>3 Installing Identity Manager</b>	<b>23</b>
3.1 Downloading the ISO File . . . . .	23
3.2 Using the Same Password for all Integrated Installation Configuration Parameters . . . . .	23
3.3 Using the Installation Wizard . . . . .	24
3.4 Performing a Silent Installation. . . . .	25
<b>4 Configuring the Identity Manager Components</b>	<b>27</b>
4.1 Considerations for Configuring the Components . . . . .	27
4.2 Using the Configuration Wizard . . . . .	28
4.3 Editing the Properties File for Silent Configuration . . . . .	29
4.4 Performing a Silent Configuration . . . . .	30
<b>5 Understanding the Configuration Parameters</b>	<b>31</b>
5.1 Identity Vault. . . . .	31
5.1.1 Creating a New Tree . . . . .	31
5.1.2 Adding to an Existing Tree. . . . .	33
5.2 Identity Manager Server. . . . .	35
5.3 Event Auditing Service. . . . .	35

5.4	Identity Applications .....	36
5.5	Identity Reporting Module .....	38
5.6	Tools.....	40
<b>6</b>	<b>Final Steps for the Integrated Installation Process</b>	<b>41</b>
6.1	Assigning the Password Policy Object to Driver Sets .....	41
6.1.1	Creating the Password Policy Object .....	41
6.1.2	Assigning the Password Policy Object .....	42
6.2	Configuring Identity Manager Components .....	42
<b>7</b>	<b>Activating Identity Manager Products</b>	<b>43</b>
7.1	Purchasing an Identity Manager Product License .....	43
7.2	Installing a Product Activation Credential .....	43
7.3	Viewing Product Activations for Identity Manager and for Drivers .....	44
7.4	Activating Identity Manager Drivers .....	44
7.5	Activating Analyzer.....	45
7.6	Activating Designer and the Role Mapping Administrator .....	45
<b>8</b>	<b>Uninstalling Identity Manager</b>	<b>47</b>
8.1	Using the Uninstallation Wizard .....	47
8.2	Performing a Silent Uninstallation .....	47
<b>9</b>	<b>Troubleshooting</b>	<b>49</b>
9.1	Locating Log Files and Properties Files .....	49
9.2	Troubleshooting Failed Configurations.....	49
9.3	Troubleshooting Remote Loader Issues on Windows .....	49
9.4	Troubleshooting Uninstallation .....	50

---

# About this Book and the Library

The *Integrated Installation Guide* provides instructions for installing the NetIQ Identity Manager (Identity Manager) product with the integrated installation program. This guide frequently refers to the [NetIQ Identity Manager Setup Guide](#), which provides detailed information about installing Identity Manager using the standalone installation programs.

## Intended Audience

This book provides information for identity architects and identity administrators who want to install Identity Manager for the purposes of evaluating the product as an identity management solution for their organization.

## Other Information in the Library

For more information about the library for Identity Manager, see the [Identity Manager documentation website \(https://www.netiq.com/documentation/idm45/\)](https://www.netiq.com/documentation/idm45/).



---

# About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

## Our Viewpoint

### **Adapting to change and managing complexity and risk are nothing new**

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

### **Enabling critical business services, better and faster**

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

## Our Philosophy

### **Selling intelligent solutions, not just software**

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

### **Driving your success is our passion**

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

## Our Solutions

- ◆ Identity & Access Governance
- ◆ Access Management
- ◆ Security Management
- ◆ Systems & Application Management
- ◆ Workload Management
- ◆ Service Management

## Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

<b>Worldwide:</b>	<a href="http://www.netiq.com/about_netiq/officelocations.asp">www.netiq.com/about_netiq/officelocations.asp</a>
<b>United States and Canada:</b>	1-888-323-6768
<b>Email:</b>	<a href="mailto:info@netiq.com">info@netiq.com</a>
<b>Website:</b>	<a href="http://www.netiq.com">www.netiq.com</a>

## Contacting Technical Support

For specific product issues, contact our Technical Support team.

<b>Worldwide:</b>	<a href="http://www.netiq.com/support/contactinfo.asp">www.netiq.com/support/contactinfo.asp</a>
<b>North and South America:</b>	1-713-418-5555
<b>Europe, Middle East, and Africa:</b>	+353 (0) 91-782 677
<b>Email:</b>	<a href="mailto:support@netiq.com">support@netiq.com</a>
<b>Website:</b>	<a href="http://www.netiq.com/support">www.netiq.com/support</a>

## Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ website in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at [www.netiq.com/documentation](http://www.netiq.com/documentation). You can also email [Documentation-Feedback@netiq.com](mailto:Documentation-Feedback@netiq.com). We value your input and look forward to hearing from you.

## Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit [community.netiq.com](http://community.netiq.com).



---

# 1 Introduction

NetIQ provides two ways to install and configure Identity Manager in your environment: an integrated installation solution and installation programs for each component or a group of components. The **integrated installation** program enables you to install and configure all components, using default values for many of the settings. You can use the integrated installation program to install all components on one computer (Linux only) or in a distributed environment. With the **standalone installation** programs, you can install one or more of the Identity Manager components separately or customize a large portion of the settings.

Before proceeding, ensure that you understand the different Identity Manager components. For more information, see [“Overview of the Components of Identity Manager”](#) in the *NetIQ Identity Manager Setup Guide*.

## 1.1 Understanding the Differences between the Integrated Installation and the Standalone Installation Programs

Use the following information to determine whether you should use the integrated installation program or one of the standalone installation programs.

### Integrated installation program

NetIQ recommends using this program when you want to evaluate Identity Manager or create a test environment. The program bundles all necessary components into one installation process. The integrated installation program has the following capabilities:

- ◆ Applies the default values for most settings
- ◆ Installs all components on one computer or in a small, distributed environment
- ◆ Uses PostgreSQL for all databases
- ◆ Uses Apache Tomcat for all application servers
- ◆ Should not be used in a clustered environment
- ◆ Should not be used in a production environment

### Standalone installation programs

NetIQ recommends using this option for the staging and production environments of your identity management solution. The standalone installation programs give you more flexibility in setting up your environment. This process provides the following capabilities:

- ◆ Allows you to customize component settings
- ◆ Allows you to install in distributed environments
- ◆ Supports multiple database platforms
- ◆ Supports multiple application servers
- ◆ Creates a supported production environment

For more information about using the standalone installation process, see the [NetIQ Identity Manager Setup Guide](#).

## 1.2 Understanding the Integrated Installation Process

The integrated installation process runs the installation programs for the various Identity Manager components. If you are installing in a distributed environment, you can specify which components to install on each computer.

When you begin the installation process, you can specify a password that the process will apply to all password parameters for the installed components. The installation applies default settings to configure the installed components. You can modify the default settings as part of the installation process or make the changes later. For example, when you initiate the process, you can specify the password that you want to apply to all password values.

---

**NOTE:** You cannot use the integrated installation process to upgrade an existing installation.

---

The following sections explain the components that you can install with this process and their default settings.

### 1.2.1 Identity Manager Server

This option installs the following Identity Manager components:

- ◆ Identity Vault
- ◆ Identity Manager engine
- ◆ iManager plug-ins
- ◆ Identity Manager drivers
- ◆ Remote Loader

By default, the administrative account for the Identity Vault is `admin`. You can change that value when you configure the components. The installation process automatically creates the tree structure for the Identity Vault. For more information, see [Section 1.3, “Understanding the Default Identity Vault Structure,” on page 13](#).

### 1.2.2 Identity Applications

This option installs the following Identity Manager components and supporting software:

- ◆ Catalog Administrator
- ◆ Home and Provisioning Dashboard
- ◆ Roles Based Provisioning Module (RBPM)
- ◆ Role and Resource Service driver
- ◆ User Application
- ◆ User Application driver
- ◆ One SSO Provider
- ◆ PostgreSQL
- ◆ Self Service Password Reset
- ◆ Tomcat

The installation process provides an Oracle JRE, open source versions of Apache Tomcat Web Server, Apache ActiveMQ, and PostgreSQL database server as a basis for Identity Manager. This installer lets you install these components without downloading them separately. However, NetIQ does not provide enterprise support for these components.

NetIQ recommends using an enterprise application server for staging and production environments, and creating development environments by using this convenient installer. NetIQ does not provide support and updates for these components, or administration, configuration, or tuning. If you need support, go to the third-party provider of the component.

The installation process creates the following accounts and database:

---

Default item	Description
idmuserappdb	Database for the identity applications
idmadmin	Administrative user account for the idmuserappdb database
uaadmin	Administrative user account for the User Application

---

The installation process also creates and configures the User Application driver and the Role and Resource Service driver. To configure additional drivers, see the [Identity Manager Drivers documentation website \(https://www.netiq.com/documentation/idm45drivers/\)](https://www.netiq.com/documentation/idm45drivers/).

For more information about the identity applications, see “[Understanding the Components for Managing User Provisioning](#)” and “[Installing the Identity Applications](#)” in the *NetIQ Identity Manager Setup Guide*.

## 1.2.3 Identity Reporting

This option installs the following Identity Manager components:

- ♦ Identity Reporting Module
- ♦ Managed System Gateway driver (MSGW)
- ♦ Driver for Data Collection Service (DCS)

Although you might have multiple types of event auditing systems, Identity Reporting can communicate with only one Event Auditing Service computer. To log events, Identity Reporting needs the SIEM database that gets installed with Event Auditing Service.

For more information about Identity Reporting, see “[Identity Reporting](#)” and “[Installing the Identity Reporting Components](#)” in the *NetIQ Identity Manager Setup Guide*.

## 1.2.4 Event Auditing Service

This option installs the following components:

- ♦ NetIQ Event Auditing Service
- ♦ SIEM database

---

**IMPORTANT:** The Event Auditing Service can be installed only on a Linux computer.

---

Event Auditing Service and Identity Reporting use the SIEM database for storing audit, log, and report events. The installation process creates the following user accounts in the database:

---

Default item	Description
dbauser	Administrative user for the database
idmrptsrv	User account for the owner of the database schemas and objects for reporting
idmrptuser	User account with read-only access to the reporting data

---

For more information about EAS, see “[Event Auditing Service](#)” and “[Installing the Event Auditing Service](#)” in the *NetIQ Identity Manager Setup Guide*.

## 1.2.5 iManager

This option installs iManager and its workstation client. During the configuration process, you can modify the default ports that iManager uses for communication. For more information about iManager, see “[iManager](#)” and “[Installing iManager](#)” in the *NetIQ Identity Manager Setup Guide*.

## 1.2.6 Designer

This option installs Designer on the local computer. Designer does not have any user-programmable parameters. For more information about Designer, see “[Designer for Identity Manager](#)” and “[Planning to Install Designer](#)” in the *NetIQ Identity Manager Setup Guide*.

## 1.2.7 Analyzer

This option installs Analyzer on the local computer. Analyzer does not have any user-programmable parameters. For more information about Analyzer, see “[Analyzer for Identity Manager](#)” and “[Installing Analyzer](#)” in the *NetIQ Identity Manager Setup Guide*.

# 1.3 Understanding the Default Identity Vault Structure

To suit most Identity Manager deployments, the integrated installation process creates a default structure for the Identity Vault.

Figure 1-1 Default Identity Vault Structure

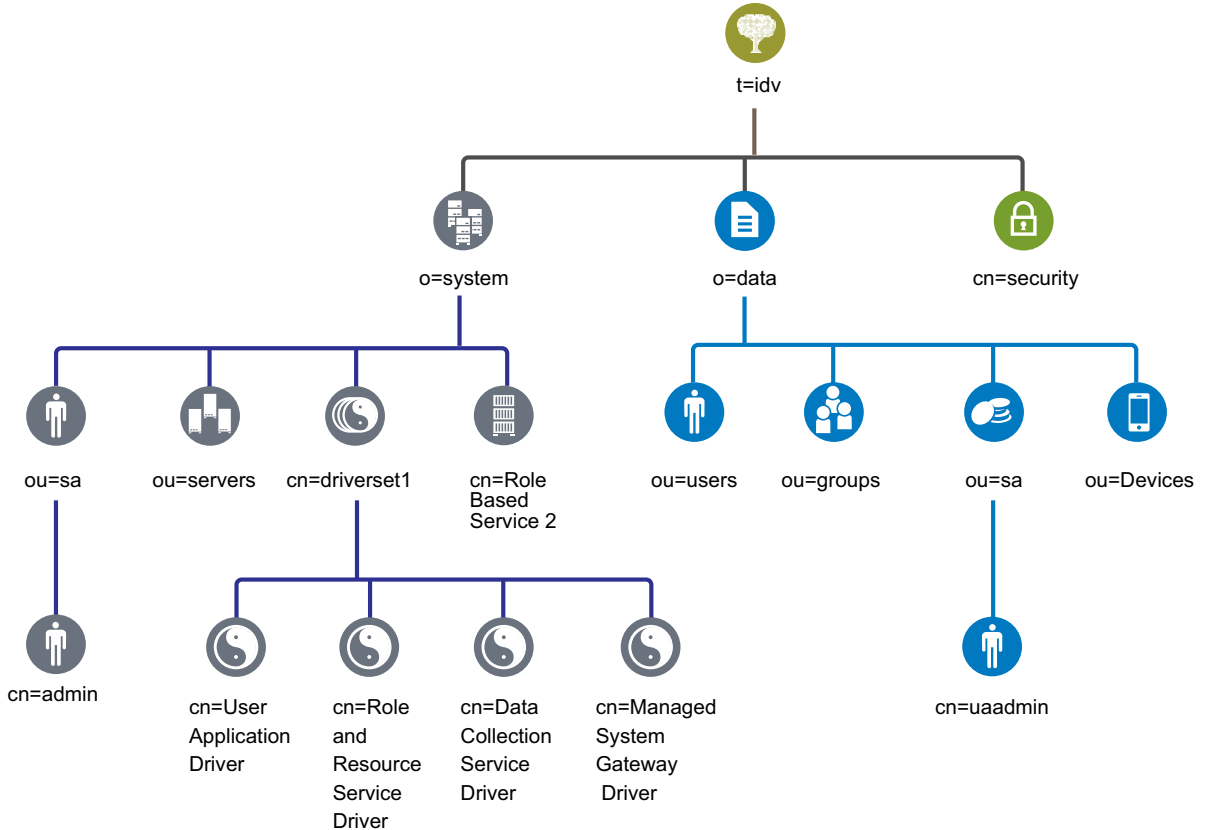


Table 1-1 Identity Vault Object Descriptions

Object	Description
t=idv	The default name of the eDirectory tree is idv.
o=system	All of the system objects for Identity Manager are located in the system organization. Administrators should be the only users that have access to this container and all subcontainers. For more information, see <a href="#">Section 1.3.1, "System Container," on page 14.</a>
ou=sa.o=system	The ou=sa.o=system container holds all of the system users. The system users are administrators, driver administrators, and other administrators.
cn=admin.ou=sa.o=system	This is the administrator account for the tree.
ou=servers.o=system	This container holds the server objects and all objects associated with the servers. This allows you to separate the server objects from the other system objects.
cn=driverset1.o=system	The driver set object contains all of the driver objects. The driver set objects are placed directly under the system container.

Object	Description
cn=User Application Driver.cn=driverset1.o=system	The User Application driver manages all tasks associated with the User Application.
cn=Role and Resource Service Driver.cn=driverset1.o=system	The Role and Resource Service driver manages all tasks associated with the Roles Based Provisioning Module.
cn=Data Collection Service Driver.cn=driverset1.o=system	The Data Collections Service driver manages tasks associated with the Identity Reporting Module.
cn=Managed System Gateway Driver.cn=driverset1.o=system	The Managed System Gateway driver manages tasks associated with the Identity Reporting Module.
cn=Role Based Service 2.o=system	This container holds object that help iManager work for Identity Manager.
o=data	All of the data objects for Identity Manager locations in the data organization. Administrators should ensure that all users have access to this container and all subcontainers. For more information, see <a href="#">Section 1.3.2, "Data Container," on page 15.</a>
ou=users.o=data	The default container for all user objects in the Identity Vault.
ou=groups.o=data	The default container for all group objects in the Identity Vault.
ou=sa.o=data	The default container for the role admin user, super user, and service accounts for the User Application, the Roles Based Provisioning Module, and the Identity Reporting Module.
cn=uaadmin.ou=sa.o=data	The User Applications administrator object.
ou=Devices.o=data	The default container for devices.
cn=security	The security container holds all security objects for the tree and Identity Manager. Ensure that only administrators have access to this container and all subcontainers. For more information, see <a href="#">Section 1.3.3, "Security Container," on page 15.</a>

This default structure is primarily useful for a single-environment installation. For example, this is a good Identity Vault 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.

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

## 1.3.1 System Container

The system container is an organization. By default, 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 the following main subcontainers:

## **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`. The objects in this container might be referred to as `sa` or service admin users / super user / service accounts.

## **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.

This structure is designed for scalability. All objects associated with the server (volumes, licenses, certificates) are in place to help you find the objects that you need.

## **Driver Sets**

Driver sets are created as a separate partition during the Identity Manager engine configuration. The Identity Vault stores the driver set objects in the system container. 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.

## **1.3.2 Data Container**

The data container holds groups, users, role admins, devices, and other objects. 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. For example, the Service Admins (`ou=sa`) container holds all user application administrator objects and service administrator accounts.

## **1.3.3 Security Container**

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.





---

# 2 Planning to Install Identity Manager

This section provides valuable information for planning your Identity Manager environment, including the prerequisites and system requirements for each Identity Manager component. You do not need to install the components on the same computer. However, the integrated installation program does not support installing in a clustered environment.

You do not need an activation code to install or initially run Identity Manager. However, without an activation code, Identity Manager stops functioning 90 days after installation. You can activate Identity Manager at any time during the 90 days or afterward.

## 2.1 Installation Checklist

The following checklist provides high-level steps for planning an installation of Identity Manager in your test or evaluation environment.

---

### Checklist Items

---

- 1. Learn about the interaction among Identity Manager components. For more information, see [Chapter 1, “Introduction,” on page 9](#).
  - 2. Review the considerations for installing the components to ensure that the computers meet the prerequisites and requirements:
    - ◆ Prerequisites specific to the integrated installation process: [Section 2.2, “Considerations for Using the Integrated Installation Program,” on page 18](#).
    - ◆ Prerequisites for each component: [Section 2.3, “Prerequisites and System Requirements,” on page 18](#).

**IMPORTANT:** The identity applications and the Identity Reporting features require the Event Auditing Service to be installed. The Event Auditing Service can only be installed on a Linux computer. If you are using Windows computers, you must have at least one Linux computer for the Event Auditing Service.
  - 3. Review the components, software, and default settings that the integrated installation process adds to your servers. For more information, see [Chapter 5, “Understanding the Configuration Parameters,” on page 31](#).
  - 4. Review the default setup for the Identity Vault. For more information, see [Section 1.3, “Understanding the Default Identity Vault Structure,” on page 13](#).
  - 5. (Conditional) When installing components in a Red Hat Enterprise Linux 6.x environment, ensure that the computer has the correct libraries. For more information, see [“Installing Identity Manager on an RHEL 6.x or 7.x Server”](#) in the *NetIQ Identity Manager Setup Guide*.
  - 6. Run the integrated installation process:
    - ◆ For a guided installation, see [Section 3.3, “Using the Installation Wizard,” on page 24](#).
    - ◆ For a silent installation, see [Section 3.4, “Performing a Silent Installation,” on page 25](#).
-

---

### Checklist Items

---

- 7. Configure the installed components:
    - ◆ For a guided process, see [Section 4.2, “Using the Configuration Wizard,”](#) on page 28.
    - ◆ For a silent configuration, see [Section 4.4, “Performing a Silent Configuration,”](#) on page 30.
  - 8. Complete the installation. For more information, see [Chapter 6, “Final Steps for the Integrated Installation Process,”](#) on page 41.
  - 9. Activate Identity Manager. For more information, see [Chapter 7, “Activating Identity Manager Products,”](#) on page 43.
- 

## 2.2 Considerations for Using the Integrated Installation Program

This section describes the considerations for using the integrated installation program to install all Identity Manager components. Unless otherwise noted here, your servers and workstations must also meet the prerequisites and requirements listed in [Section 2.3, “Prerequisites and System Requirements,”](#) on page 18.

- You cannot use the integrated installation process to upgrade an existing installation.
- You must use a supported version of the Apache Tomcat application server for components such as the User Application. As a convenience, the integrated installation program includes an option to install Tomcat.
- If you want to install all components on a single computer, it must be a Linux computer. If you are using Windows computers, you must have at least one Linux computer for the Event Auditing Service. The identity applications and the Identity Report Module requires the Event Auditing Service to be installed.

## 2.3 Prerequisites and System Requirements

You can install all of the components on one computer for evaluation purposes or you can use the integrated installer to install different components of Identity Manager on multiple systems and platforms. In order to do this, you must run through the integrated installation program multiple times and select the appropriate components.

### 2.3.1 Prerequisites

Ensure that you have completed the following prerequisites before starting the integrated installation program.

## All Platforms

---

**IMPORTANT:** The Event Auditing Service runs only in Linux environments. If you want to evaluate the identity applications and the Identity Reporting features in Identity Manager, you must install the Event Auditing Service on a Linux computer before using the integrated installer on a Windows computer.

---

- Before installing eDirectory, you must have a method for resolving tree names to server referrals. NetIQ recommends using Service Location Protocol (SLP) services. Releases of NetIQ eDirectory before version 8.8 included SLP in the installation. However, after version 8.8, you must separately install SLP. For more information, see “[Using OpenSLP or hosts.nds for Resolving Tree Names](#)” in the *NetIQ Identity Manager Setup Guide*.
- You must configure a static IP address on the server for the eDirectory infrastructure to perform efficiently. If you use DHCP addresses on the server, eDirectory might have unpredictable results. Ensure that the DNS name of the computer can be resolved. If not, add an entry for this computer in the `/etc/hosts` file so that the DNS name is resolvable.
- Synchronize time across all network servers. NetIQ recommends using the Network Time Protocol (NTP) option.

## Linux

- (Conditional) When installing components in a Red Hat Enterprise Linux 6.x environment, ensure that the computer has the correct libraries. For more information, see “[Installing Identity Manager on an RHEL 6.x or 7.x Server](#)” in the *NetIQ Identity Manager Setup Guide*.
- (Conditional) To install on a SLES 11 (64-bit) platform, ensure that the following compatible library is installed:

```
libgthread-2_0-0-32bit-2.17.2+2.17.3+20080708+r7171-3.1.x86_64.rpm
```

- Ensure that the `unzip` rpm is installed on any Linux platform you are using.
- (Conditional) To install on a SLES 11 Service Pack 3 (64-bit) platform, ensure that the `libstdc++33-32 bit` library is installed. When this library is not present, the integrated installation succeeds with no errors, but you cannot log in to iManager. However, if you install iManager separately, the iManager installation program prompts you to install the library.
- The `/etc/hosts` file can contain only one loopback address. If there is more than one loopback address, remove it by using an editor or system tools to correct the configuration. For example:

```
127.0.0.1 localhost.localdomain localhost #loopback
#127.0.02 server1
123.45.678.9 server1
```

## Windows

- You must have administrative rights to the Windows computer in order to install Identity Manager with the integrated installer.
- Your Windows operating system should be running the latest service packs before you begin the installation process.

## 2.3.2 System Requirements

The following requirements are applicable when you are installing all of the components, or most of the components, on the same computer. If you need to know requirements for a specific component, see “[Considerations and Prerequisites for Installation](#)” in the *NetIQ Identity Manager Setup Guide*.

Use the following information to ensure that you can successfully install and configure your Identity Manager system.

Category	Requirement
Processor	A multi-CPU computer with a 2 GHz processor.
Memory	A minimum of 6 GB.
Disk Space	A minimum of 40 GB.  <b>NOTE:</b> You will need additional disk space to configure and populate data. This amount might vary depending on your connected systems and number of objects in the Identity Vault.
Operating System	One or more of the following: <ul style="list-style-type: none"><li>♦ Red Hat 6.5 (64-bit)</li><li>♦ SUSE Linux Enterprise Server 11 SP3 (64-bit)</li><li>♦ Windows Server 2012 R2 (64-bit)</li></ul>
Virtual Systems	One of the following: <ul style="list-style-type: none"><li>♦ Hyper-V in the Windows Server 2012 R2</li><li>♦ VMWare ESXi 5.5</li></ul> <b>IMPORTANT:</b> NetIQ supports Identity Manager on enterprise-class virtual systems that provide official support for the operating systems where NetIQ products are running. As long as the vendors of the virtual systems officially support these operating systems, NetIQ supports the entire Identity Manager stack on them.
Operating System Hotfixes	Before installing Identity Manager, NetIQ recommends that you apply the latest operating system patches according to the manufacturer’s automated update facility.

Category	Requirement
Web Browsers	<p><b>Desktop Computer:</b> (at a minimum)</p> <ul style="list-style-type: none"> <li>◆ Apple Safari 5.1.7 for Windows</li> <li>◆ Apple Safari 7.0.1</li> <li>◆ Google Chrome 37</li> <li>◆ Microsoft Internet Explorer 11</li> <li>◆ Mozilla Firefox 32</li> </ul> <p><b>iPad:</b> (at a minimum)</p> <ul style="list-style-type: none"> <li>◆ Apple Safari 7</li> <li>◆ Google Chrome 37</li> </ul> <p><b>NOTE:</b> To access the identity applications, the browser must have cookies enabled. If cookies are disabled, the product does not work.</p>

### 2.3.3 Default Installation Locations

The integrated installation program installs the Identity Manager components in the locations specified in [Table 2-1](#). On a Windows computer, you can specify the location of the installed components. On Linux computers, the installation process places the components in predefined locations.

*Table 2-1 Default Installation Locations Set by the Integrated Installation Program*

Identity Manager Components	Default Installation Paths
<b>Linux</b>	
Identity Vault (eDirectory)	/opt/novell/eDirectory
Identity Manager engine	/opt/novell/eDirectory
Remote Loader	/opt/novell/dirxml
Event Auditing Service	/opt/novell/sentinel_eas (Linux only)
Identity applications	/opt/netiq/idm/apps
Identity Reporting Module	/opt/netiq/idm/apps
iManager and plug-ins	/var/opt/novell/iManager
Analyzer	/opt/netiq/idm/tools/Analyzer
Designer	/opt/netiq/idm/tools/Designer
<b>Windows</b>	
Identity Vault (eDirectory)	C:\NetIQ\IdentityManager\NDS
Identity Manager engine	C:\NetIQ\IdentityManager\NDS
Remote Loader	C:\NetIQ\IdentityManager\RemoteLoader

---

<b>Identity Manager Components</b>	<b>Default Installation Paths</b>
Identity Applications	C:\NetIQ\IdentityManager\apps
Identity Reporting Module	C:\NetIQ\IdentityManager\apps
iManager	C:\NetIQ\IdentityManager\iManager
Analyzer	C:\NetIQ\IdentityManager\tools\Analyzer
Designer	C:\NetIQ\IdentityManager\tools\Designer

---

---

# 3 Installing Identity Manager

The integrated installer installs the binary files for all of the Identity Manager components and configures the components. You can install the components and configure the components at the same time or these can be separate procedures.

## 3.1 Downloading the ISO File

You must download the installation files from the NetIQ download site.

**To download the .iso file:**

- 1 Access the [NetIQ download website \(https://dl.netiq.com/index.jsp\)](https://dl.netiq.com/index.jsp).
- 2 On the **Product or Technology** menu, select **Identity Manager**.
- 3 In the **Select Version** field, select **Identity Manager 4.5**, then click **Submit Query**.
- 4 Click the **Identity Manager 4.5** link, then click **proceed to download**.
- 5 Log in with your NetIQ Customer Center ID.
- 6 Select the appropriate .iso file for your platform, then follow the on-screen prompts to download the file.

The integrated installation files (`install.exe` or `install.bin`) are located in the top level of the Identity Manager .iso files. Access the Identity Manager installation files either by mounting the .iso file or accessing the DVD you created from the .iso file.

## 3.2 Using the Same Password for all Integrated Installation Configuration Parameters

Many of the Identity Manager components require you to specify a password during the configuration phase. For faster configuration, you can instruct the process to apply the same password to all integrated installation configuration parameters.

The password must be a minimum of six characters.

### Linux

Before invoking the installation or configuration program, enter the following command:

```
export USER_SUPPLIED_PASSWORD=password
```

For example:

```
export USER_SUPPLIED_PASSWORD=test123
```

### Windows

Perform one of the following actions:

- ♦ In **System Properties > Environment Variables**, add `USER_SUPPLIED_PASSWORD` and specify a value for the variable.
- ♦ Before invoking the installation or configuration program, enter the following command:

```
set USER_SUPPLIED_PASSWORD=password
```

For example:

```
set USER_SUPPLIED_PASSWORD=test123
```

---

**NOTE:** On Windows servers, the installation process does not apply the specified password variable to **EAS system password**. Instead, for that parameter, specify the system-generated password for the EAS installation on its remote Linux server.

---

## 3.3 Using the Installation Wizard

The following procedure describes how to install Identity Manager on a Linux or Windows platform using the installation wizard. To perform a silent, unattended installation, see [Section 3.4, “Performing a Silent Installation,” on page 25](#).

To prepare for the installation, review the prerequisites and system requirements listed in [Section 2.1, “Installation Checklist,” on page 17](#). Also, see the latest Release Notes for pertinent installation information.

For your convenience, you can specify a password that the installation process applies to most passwords that you must configure for Identity Manager.

### To install Identity Manager using the wizard:

- 1 Log in as a root or administrative user to the computer where you want to install the components.
- 2 Mount the `.iso` file or create a DVD from the `.iso` file. For more information, see [Section 3.1, “Downloading the ISO File,” on page 23](#).
- 3 (Optional) Instruct the installation process to apply the same password for all integrated installation configuration parameters. For more information, see [Section 3.2, “Using the Same Password for all Integrated Installation Configuration Parameters,” on page 23](#).
- 4 From the root directory of the `.iso` file, access the installation files, then complete one of the following actions:
  - ♦ **Linux:** Enter `./install.bin`
  - ♦ **Windows:** Run `install.exe`
- 5 On the title page, select the appropriate language from the drop-down list, then click **OK**.
- 6 On the Introduction page, view the different Identity Manager components you can install, then click **Next**.
- 7 Read and accept the license agreement, then click **Next**.

---

**NOTE:** You must read through and scroll to the end of the license agreement, before you can accept the license agreement.

---

- 8 Specify the components that you want to install on the local server, then click **Next**.  
For more information about the component options, see [Section 1.2, “Understanding the Integrated Installation Process,” on page 10](#).
- 9 (Conditional) On a Windows server, specify the installation folder, and then click **Next**.
- 10 Review the pre-installation summary, then click **Install**.

---

**NOTE:** Depending on the selected components, the installation process might take some time to complete.

---



- 11 When the installation completes, perform one of the following actions to configure the installed components:
  - ♦ **To configure immediately:** Select **Continue Now**.
  - ♦ **To configure later:** Deselect **Continue Now**.

You can modify the configuration parameters at any time. However, you cannot run Identity Manager until you specify many of the parameters. For more information, see [Chapter 4, “Configuring the Identity Manager Components,”](#) on page 27.

---

**NOTE:** Some components such as Designer and Analyzer, do not require configuration.

---

- 12 Click **Done**.

## 3.4 Performing a Silent Installation

A silent (non-interactive) installation does not display a user interface or ask the user any questions. Instead, the system uses information from the properties files. To perform a guided installation, see [Section 3.3, “Using the Installation Wizard,”](#) on page 24. To prepare for the installation, review the prerequisites and system requirements listed in [Section 2.1, “Installation Checklist,”](#) on page 17. Also, see the latest Release Notes for pertinent installation information.

For your convenience, you can specify a password that the installation process applies to the single sign-on passwords that you must configure for Identity Manager. For more information, see [Section 4.1, “Considerations for Configuring the Components,”](#) on page 27.

### To perform a silent installation:

- 1 Log in as `root` or an administrator to the computer where you want to install the components.
- 2 After you have mounted the `.iso` file, navigate to the directory containing the installation files, located by default in the `osp_sspr` directory.
- 3 Edit the `install.properties` file for the silent installation, located by default in the following directories:
  - ♦ **Linux:** `install/propfiles`
  - ♦ **Windows:** `install\propfiles`
- 4 (Optional) Instruct the installation process to apply the same password for all integrated installation configuration parameters. For more information, see [Section 3.2, “Using the Same Password for all Integrated Installation Configuration Parameters,”](#) on page 23.
- 5 To run the silent installation, issue one of the following commands:
  - ♦ **Linux:** `install.bin -i silent -f path_to_install.properties`
  - ♦ **Windows:** `install.exe -i silent -f path_to_install.properties`
- 6 Continue to the configuration phase of the process. For more information, see [Chapter 4, “Configuring the Identity Manager Components,”](#) on page 27.



---

# 4 Configuring the Identity Manager Components

The integrated installation process can guide you through configuring the Identity Manager components that you have installed or you can perform a silent configuration. Some components, such as Designer and Analyzer, might not require configuration. For more information about the configuration parameters, see [Chapter 5, “Understanding the Configuration Parameters,” on page 31](#).

---

**NOTE:** To ensure that users can log in to the identity applications, the configuration process assigns a sample password policy to `admin.sa.system`, `uaadmin.sa.data`, and `users.data`. As part of this action, the process also enables the **Allow admin to retrieve passwords** setting under the Password Retrieval options.

---

## 4.1 Considerations for Configuring the Components

Before you use the integrated installation process to configure the installed components, review the following considerations:

- ◆ You can configure only the components installed on the local computer.
- ◆ Before installing or configuring, you can instruct the process to apply the same password to all integrated installation configuration parameters. For more information, see [Section 3.2, “Using the Same Password for all Integrated Installation Configuration Parameters,” on page 23](#).
- ◆ Ensure that the `/etc/hosts` file includes entries for the 127.0.0.1 loopback address and the real IP address. For more information, see [Section 2.3, “Prerequisites and System Requirements,” on page 18](#).
- ◆ If you are configuring the identity applications and the Identity Reporting components, you must select **Advanced Settings** and change any field that contains `localhost` to a valid IP address or DNS name. If you do not change the value from `localhost`, the configuration fails.
- ◆ If you are configuring only the Identity Manager server, manually add the logging server details to the `logevent.conf` (Linux) and `logevent.cfg` (Windows) file. The integrated installation process updates the file with the logging server details only when you configure the identity applications or Identity Reporting.
- ◆ Before adding a secondary server to an existing tree, you should perform a health check. The integrated installation process does not perform the health check for you.
- ◆ When you add a secondary server to the tree, the server receives only a copy of the root and its own driver set partition.
  - ◆ If you also use the Data Collection Service driver as primary on this second server, the driver cannot see object changes that it needs to report. To configure the Data Collection Service driver on this server, see [“Configuring the Driver for Data Collection Service” in the \*NetIQ Identity Manager Setup Guide\*](#).
  - ◆ If the Data Collect Service driver is on this section server, it must hold a copy of the tree partition to function.

For more information about the configuration values, see [Chapter 5, “Understanding the Configuration Parameters,” on page 31](#).

## 4.2 Using the Configuration Wizard

The Configuration wizard walks you through the configuration of all of the Identity Manager components you selected when you performed the installation.

### To configure the Identity Manager components:

1 (Conditional) To add a secondary server to an existing tree, complete the following steps:

1a Navigate to the `ndscheck` utility, located by default in the following directories:

- ♦ **Linux:** `/opt/novell/eDirectory/bin/ndscheck`
- ♦ **Windows:** `install_location\NDS`

1b Specify the mandatory parameters and run the following command:

```
ndscheck [-h hostname port] [-a admin_FDN] [-w password]
```

2 (Conditional) If you are continuing from [Step 12 on page 25](#) in the installation procedure, skip to [Step 6 on page 28](#).

3 (Optional) Instruct the configuration process to apply the same password for all integrated installation configuration parameters. For more information, see [Section 3.2, "Using the Same Password for all Integrated Installation Configuration Parameters," on page 23](#).

4 (Conditional) To start the configuration manually, perform one of the following actions:

- ♦ **Linux (GUI):** Enter `./configure.bin`
- ♦ **Windows:** Run `configure.exe`

5 On the title page, select the appropriate language for the drop-down list, then click **OK**.

6 Review the components that are installed on your system, then click **Next**.

7 Select the components that you want to configure on the local server, and then click **Next**.

8 Use the following information to configure the different components:

- ♦ **Identity Vault:** Specify whether you want to create a new tree in the Identity Vault or are modifying an existing one, then configure the tree for your environment. For more information, see [Section 5.1, "Identity Vault," on page 31](#).
- ♦ **Event Auditing Service:** Specify the configuration information for your Event Auditing Service. For more information, see [Section 5.3, "Event Auditing Service," on page 35](#).

---

**IMPORTANT:** The Event Auditing Service can be installed only on Linux computers. However, a functioning Event Auditing Service is required to configure the Identity Reporting Module.

---

- ♦ **Identity Applications:** Specify the configuration information for your identity applications. You must include an IP address or DNS name of an audit server, otherwise the configuration fails. For more information, see [Section 5.4, "Identity Applications," on page 36](#).

---

**IMPORTANT:** You must select **Advanced Settings** and change any field that contains `localhost` to be a valid IP address or DNS name. If you do not change the default parameter from `localhost`, the configuration fails.

---

- ♦ **(Conditional) Identity Manager Server:** Specify the existing Identity Manager server information if you are installing into an existing eDirectory tree. For more information, see [Section 5.2, "Identity Manager Server," on page 35](#).

- ♦ **Identity Reporting Module:** You must have the Event Auditing Service installed and configured to use the Identity Reporting Module. You can only install the Event Auditing Service on a Linux computer. If you are using a Windows computer, you must install the Event Auditing Service on a Linux computer before you can configure the Identity Reporting Module on a Windows computer.

Specify the configuration information for your Identity Reporting Module. For more information, see [Section 5.5, “Identity Reporting Module,” on page 38](#).

- ♦ **Tools:** Linux only. Select **Advanced Settings** to change the default HTTP ports. For more information, see [Section 5.6, “Tools,” on page 40](#).

- 9 Click **Next** to perform the configuration of the different components.
- 10 Review the summary of the configuration information, then click **Configure**.
- 11 Review the configuration summary, then click **Done**.

---

**NOTE:** If there were any errors during the configuration, the integrated installer displays the location of the installation logs. Review the installation logs to find out why the configuration failed.

---

## 4.3 Editing the Properties File for Silent Configuration

You can run a silent configuration of the Identity Manager components by creating or modifying a properties file with the parameters necessary to complete the configuration for each component. The Identity Manager media provides two sample files that you can use if you installed all the components on a single server.

### To edit the properties file:

- 1 (Conditional) If you installed all components on the same server, edit one of the sample properties files for the silent configuration, located by default in the following directories:

- ♦ **Linux:** `install/propfiles`
- ♦ **Windows:** `install\propfiles`

For example, use the `configure_new_tree.properties` file to create a new tree.

- 2 (Conditional) If you did not install all components on the same server, complete the following steps to generate a properties file for the installed components:

- 2a Run the following command:

```
./install.bin -i silent -DSELECTED_PRODUCTS=components_to_be_configured -f filename.properties
```

where `filename.properties` represents one of the sample properties files.

The program verifies that the specified components are installed and then generates a list of the mandatory parameters for the components.

- 2b Using the output from the command in [Step 2a](#), create a new properties file.
- 2c Add a `SELECTED_PRODUCTS` variable to the file, then specify the components that you want to configure.
- 3 In the properties file, specify the settings for the installed components. For more information, see [Chapter 5, “Understanding the Configuration Parameters,” on page 31](#).
- 4 Add the following password variables to the properties file:

Password Variable	Applicable User Account or Service
IA_IDVAULT_ADMIN_PASSWORD	Identity Vault administrator
IA_RBPM_POSTGRESQL_DB_PASSWORD	Identity applications database administrator (idmadmin)
IA_RBPM_USERAPPADMIN_PASSWORD	User Application administrator (uaadmin)
IA_REPORTING_NOVL_DB_USER_PASSWORD	Identity Reporting database administrator
IA_REPORTING_IDM_SERVER_PASSWORD	Identity Reporting server user (idmrptsrv)
IA_REPORTING_IDM_USER_PASSWORD	Identity Reporting user (idmrptuser)
IA_EAS_DBA_PWD	Event Auditing Service database administrator (dbauser)
IA_EAS_ADMIN_PWD	Event Auditing Service administrator (admin)
-DUSER_SUPPLIED_PASSWORD	Single sign-on service

If you included the `duser_supplied_password` variable when you initiated the silent installation, the program already applied that value to the single sign-on passwords.

- 5 Save and close the file.

## 4.4 Performing a 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. The Identity Manager media provides two sample files that you can use if you installed all the components on a single server.

For more information about the parameters that you can configure, see [Chapter 5, “Understanding the Configuration Parameters,”](#) on page 31.

### To perform a silent configuration:

- 1 (Conditional) To add a secondary server to an existing tree, complete the following steps:
  - 1a Navigate to the `ndscheck` utility, located by default in the following directories:
    - ♦ **Linux:** `/opt/novell/eDirectory/bin/ndscheck`
    - ♦ **Windows:** `install_location\NDS`
  - 1b Specify the mandatory parameters and run the following command:
 

```
ndscheck [-h hostname port] [-a admin_FDN] [-w password]
```
- 2 (Optional) Instruct the configuration process to apply the same password for all integrated installation configuration parameters. For more information, see [Section 3.2, “Using the Same Password for all Integrated Installation Configuration Parameters,”](#) on page 23.
- 3 To run the silent configuration, issue one of the following commands:
  - ♦ **Linux:** `configure.bin -i silent -f path_to_properties_file`
  - ♦ **Windows:** `configure.exe -i silent -f path_to_properties_file`

---

# 5 Understanding the Configuration Parameters

This section defines the parameters that you need to specify to appropriately configure your Identity Manager installation. You can use the installation program to configure the components immediately after installing them.

---

**NOTE:** Many of the components have a password that you must specify. You can use the same password for all the parameters. To do so, specify the password when you initiate the installation process. For more information, see the installation instructions.

---

## 5.1 Identity Vault

This section defines the settings for the eDirectory tree for the Identity Vault. Some parameters apply to configuring a new tree versus an existing tree. Also, the program displays the basic parameters. To view all parameters, click [Advanced Settings](#).

### 5.1.1 Creating a New Tree

Use the following parameters if you do not have an existing eDirectory tree. All of the parameters in this section help you create a new tree.

#### Create a new tree

Select this option to create a new eDirectory tree for your Identity Vault.

#### Tree name

Specifies the name of the tree that you want to create. The tree name must meet the following requirements:

- ◆ The tree name must be unique in your network.
- ◆ The tree name must be 2 to 32 characters long.
- ◆ The tree name must contain only characters such as letters (a-zA-Z), numbers (0-9), hyphens (-), and underscores (\_).

If you have separate trees, creating a corporate standard for the tree names makes it easier to merge trees in the future.

#### Administrator password

Specifies the password for the Administrator object. For example, `netiq123`. The installation program configures this password for the Administrator object that the installation program creates.

#### Advanced Settings

All of the remaining settings are under [Advanced Settings](#). If you do not make any changes to the [Advanced Settings](#), the configuration program uses the default settings listed.

## Identity Vault Administrator

Specifies the relative distinguished name (RDN) of the administrator object in the tree that has full rights, at least to the context to which this server is added. The default name is `admin`.

The installation program uses this account to perform all operations in the tree.

## NCP port

*Applies to Linux servers only*

Specifies the NetWare Core Protocol (NCP) port that the Identity Vault uses to communicate with the Identity Manager components. The default value is 524.

## LDAP port

Specifies the port on which the Identity Vault listens for LDAP requests in clear text. The default value is 389.

For more information about using LDAP, see “Using LDAP to Communicate with the Identity Vault” in the *NetIQ Identity Manager Setup Guide*.

## Secure LDAP port

Specifies the port on which the Identity Vault listens for LDAP requests using Secure Sockets Layer (SSL) protocol. The default value is 636.

If a service already loaded on the server (before you install eDirectory) uses the default port, you must specify a different port. For more information about using LDAP, see “Using LDAP to Communicate with the Identity Vault” in the *NetIQ Identity Manager Setup Guide*.

## HTTP port

Specifies the port on which the HTTP stack operates in clear text. The default value is 8028.

The specified HTTP stack ports must be different than the HTTP stack ports that you use for iManager. For more information, see the *iManager Administration Guide* ([http://www.netiq.com/documentation/imanager27/imanager\\_admin\\_275/data/hk42s9ot.html](http://www.netiq.com/documentation/imanager27/imanager_admin_275/data/hk42s9ot.html)).

## Secure HTTP port

Specifies the port on which the HTTP stack operates using TLS/SSL protocol. The default value is 8030.

The specified HTTP stack ports must be different than the HTTP stack ports that you use for iManager. For more information, see the *iManager Administration Guide* ([http://www.netiq.com/documentation/imanager27/imanager\\_admin\\_275/data/hk42s9ot.html](http://www.netiq.com/documentation/imanager27/imanager_admin_275/data/hk42s9ot.html)).

## eDirectory Instance path

*Applies to Linux servers only*

Specifies the path of this eDirectory instance on this server. The default path is `/var/opt/novell/eDirectory`. You can run multiple instances of eDirectory on one server.

## DIB path

Specifies the path in the local system where you want to install the Directory Information Base (DIB) files. By default, the installation program places the files in the following locations:

- **Linux:** `/var/opt/novell/eDirectory/data/dib`
- **Windows:** `C:\NetIQ\IdentityManager\NDS\DIBFiles\`

The DIB data files are your eDirectory database files. You might want to specify a different path if the DIB data files for your environment require more space than is available in the default location.



---

**IMPORTANT:** DIB files must reside in the \NDS directory on Windows. The configuration of the Identity Manager engine fails if you change the default location of the DIB files on Windows.

---

### **Require TLS for simple binds with password**

(Optional) Select whether the Identity Vault requires Transport Layer Security (TLS) protocol when receiving LDAP requests in clear text. This option is enabled by default.

### **Enable Secretstore**

*Applies to Windows servers only*

(Optional) Select whether to enable SecretStore during the configuration of eDirectory. For more information, see [SecretStore Integration with eDirectory \(https://www.netiq.com/documentation/edir88/edirin88/data/bv50u8n.html\)](https://www.netiq.com/documentation/edir88/edirin88/data/bv50u8n.html).

## **5.1.2 Adding to an Existing Tree**

If you already have an existing eDirectory tree, use the following parameters to add this new server into the existing tree.

---

**IMPORTANT:** Ensure that you understand the implications of adding a new server into an existing tree. For more information, see [Section 4.1, “Considerations for Configuring the Components,” on page 27](#).

---

### **Add to an existing tree**

Select this option to if you have an existing tree that you want to modify for the Identity Vault.

### **Existing tree name**

Specify your existing eDirectory tree name.

### **Existing server address**

Specify the IP address of the server that holds the master replica of the root partition.

### **Existing port number**

Specify the NCP port of the server specified above. The default port for NCP is 524.

### **Existing server context DN**

Specify the LDAP DN of the context where you want this server placed in your existing tree. The default value is ou=servers,o=system from the Identity Vault structure that the integrated installer creates. For more information, see [Section 1.3, “Understanding the Default Identity Vault Structure,” on page 13](#).

### **Existing server admin name**

Specify the name of the eDirectory administrator. The default name is admin. For more information, see [Section 1.3, “Understanding the Default Identity Vault Structure,” on page 13](#).

### **Existing server admin context DN**

Specify the LDAP DN of the context where the eDirectory administrator resides in the existing tree. The default value is ou=sa,o=system from the Identity Vault structure that the integrated installer creates. For more information, see [Section 1.3, “Understanding the Default Identity Vault Structure,” on page 13](#).

### **Existing server admin password**

Specify the password of the eDirectory administrator.

## Advanced Settings

All of the remaining settings are under **Advanced Settings**. If you do not make any changes to the **Advanced Settings**, the configuration program uses the default settings listed.

### LDAP port

Specifies the port on which the existing eDirectory tree listens for LDAP requests in clear text. The default value is 389.

For more information about using LDAP, see “Using LDAP to Communicate with the Identity Vault” in the *NetIQ Identity Manager Setup Guide*.

### Secure LDAP port

Specifies the port on which the existing eDirectory tree listens for LDAP requests using Secure Sockets Layer (SSL) protocol. The default value is 636.

For more information about using LDAP, see “Using LDAP to Communicate with the Identity Vault” in the *NetIQ Identity Manager Setup Guide*.

### HTTP port

Specifies the port on which the HTTP stack operates in clear text. The default value is 8028.

The specified HTTP stack ports must be different than the HTTP stack ports that you use for iManager. For more information, see the *iManager Administration Guide* ([http://www.netiq.com/documentation/imanager27/imanager\\_admin\\_275/data/hk42s9ot.html](http://www.netiq.com/documentation/imanager27/imanager_admin_275/data/hk42s9ot.html)).

### Secure HTTP port

Specifies the port on which the HTTP stack operates using TLS/SSL protocol. The default value is 8030.

The specified HTTP stack ports must be different than the HTTP stack ports that you use for iManager. For more information, see the *iManager Administration Guide* ([http://www.netiq.com/documentation/imanager27/imanager\\_admin\\_275/data/hk42s9ot.html](http://www.netiq.com/documentation/imanager27/imanager_admin_275/data/hk42s9ot.html)).

### DIB path

Specifies the path in the local system where you want to install the Directory Information Base (DIB) files. By default, the installation program places the files in the following locations:

- **Linux:** /var/opt/novell/eDirectory/data/dib
- **Windows:** C:\NetIQ\IdentityManager\NDS\DIBFiles\

The DIB data files are your eDirectory database files. You might want to specify a different path if the DIB data files for your environment require more space than is available in the default location.

---

**IMPORTANT:** DIB files must reside in the \NDS directory on Windows. The configuration of the Identity Manager engine fails if you change the default location of the DIB files on Windows.

---

### Require TLS for simple binds with password

(Optional) Select whether the Identity Vault requires Transport Layer Security (TLS) protocol when receiving LDAP requests in clear text. This option is enabled by default.

### Enable Secretstore

*Applies to Windows servers only*

(Optional) Select whether to enable SecretStore during the configuration of eDirectory. For more information, see *SecretStore Integration with eDirectory* (<https://www.netiq.com/documentation/edir88/edirin88/data/bv50u8n.html>).

## 5.2 Identity Manager Server

The integrated installation program displays the **Identity Manager Server** fields only if you choose to add your server into an existing eDirectory tree.

---

**IMPORTANT:** The integrated installer does not support upgrades. If you have an existing Identity Manager deployment, you must use the regular installers to upgrade your Identity Manager solution. For more information, see “[Upgrading Identity Manager](#)” in the *NetIQ Identity Manager Setup Guide*.

---

### Driver set name

Specify a name for a new Identity Manager driver set object. This object must be created for Identity Manager to work. If you create a new tree, the integrated installer creates this object for you.

### Driver set context DN

Specify the LDAP DN of the container where you want to create the driver set object. The default location is `o=system` from the Identity Vault structure that the integrated installer creates. For more information, see [Section 1.3, “Understanding the Default Identity Vault Structure,”](#) on [page 13](#).

## 5.3 Event Auditing Service

The Event Auditing Service is a feature Identity Manager provides that allows you to audit your Identity Manager components. However, the Event Auditing Service can be installed only on Linux computers. The Event Auditing Service is required to be installed and running before configuring the identity applications and the Identity Reporting features. Otherwise, the configuration of the identity applications and the Identity Reporting features fails.

### Administrator password

Specify the password for the Event Auditing Service utilities administrator. The installation process creates this account.

---

**NOTE:** On a SUSE Linux (SLES) server, the password must meet the systems password policy for SLES.

---

### dbuser password

Specifies the password for the `admin` account that can modify the Identity Information Warehouse (database on the EAS server). The installation process creates this account.

---

**NOTE:** On a SUSE Linux (SLES) server, the password must meet the systems password policy for SLES.

---

### Advanced Settings

All of the remaining settings are under **Advanced Settings**. If you do not make any changes to the **Advanced Settings**, the configuration program uses the default settings listed.

### PostgreSQL port

Specify the port through which the PostgreSQL database communicates. The default port is 15432.

### Enable port forwarding

Select whether you want to support port forwarding packets with the Event Auditing Service. By default, this option is enabled.

## 5.4 Identity Applications

This section defines the settings for the identity applications, such as the User Application. The program displays the basic parameters. To view all parameters, click [Advanced Settings](#).

---

**IMPORTANT:** You must select [Advanced Settings](#) and change any field that contains `localhost` to be a valid IP address or DNS name. If you do not change the default parameter from `localhost`, the configuration fails.

---

### OSP server host

Specifies the DNS name or IP address of the server where you plan to install OSP and which becomes the LDAP authentication server. Do not use `localhost`.

For more information about OSP, see “[Using Single Sign-on Access in Identity Manager](#)” in the [NetIQ Identity Manager Setup Guide](#).

### OSP keystore password

Specifies the password that you want to create for loading the new keystore on the OAuth server. The password must be a minimum of six characters.

### SSPR config password

Specifies the password that you want to create for configuring Self-Service Password Reset (SSPR).

By default, SSPR does not have a configuration password. Without the password, any user who can log in to SSPR can also modify the configuration settings.

### Service password

Specifies the password for the single sign-on client used by SSPR, the identity applications, and Identity Reporting.

The password must be a minimum of six characters.

### Identity Applications admin password

Specifies the password for the administrator of the User Application. The installation process creates this account in the Identity Vault with rights to perform administrative tasks for the specified user container for User Application. The following considerations apply to this setting:

- ◆ By default, the account name is `uaadmin`.
- ◆ If you have started the application server hosting the User Application, you cannot change this setting with the `configupdate.sh` or `configupdate.bat` files.
- ◆ To change this assignment after you deploy the application, use the [Administration > Security](#) page in the User Application.

- ◆ This user account has the right to use the **Administration** tab of the User Application to administer the portal.
- ◆ If the User Application Administrator participates in workflow administration tasks exposed in iManager, Designer, or the User Application (**Requests & Approvals** tab), you must grant this administrator appropriate trustee rights to object instances contained in the User Application driver. For more information, see the [User Application Administration Guide](https://www.netiq.com/documentation/idm45/agpro/data/agpropartadminapp.html) (<https://www.netiq.com/documentation/idm45/agpro/data/agpropartadminapp.html>).

#### **idmadmin DB user password**

Specifies the password for the administrator of the database for the identity applications.

By the default, the account is `idmadmin`.

#### **Tomcat shutdown port**

Specifies the port that you want to use for cleanly shutting down all webapps and Tomcat. The default is 8105.

#### **Tomcat HTTP port**

Specifies the port that you want the Tomcat server to use for communication with client computers. The default is 8080. To use SSL, the default is 8443. For more information on [Enabling SSL with a signed certificate](#) see, [NetIQ Identity Manager Setup Guide](#).

#### **Tomcat redirect port**

(Conditional) When you do not use TLS/SSL protocols, specifies the port to which the application server redirects requests that require SSL transport. The default value is 8543.

#### **Tomcat AJP port**

(Optional) Specifies the port that you want the application server to use for communication with a web connector using the AJP protocol instead of HTTP. The default value is 8109.

Use this parameter when you want the application server to manage the static content contained in the web application, or utilize the application server's SSL processing.

#### **Audit server host**

Specifies the DNS name or IP address of the server that hosts the SIEM database that the Event Auditing Service and Identity Reporting use (Identity Information Warehouse). Do not use `localhost`.

You can specify the server for an alternative auditing service, such as the Event Auditing Service or NetIQ Sentinel.

---

**IMPORTANT:** You must have your audit server installed and running before you configure the identity applications. If the integrated installation program cannot communicate with the audit server, the configuration fails.

---

#### **Advanced Settings**

All of the remaining settings are under **Advanced Settings**. You must change the **Identity Application host** field from `localhost` to an IP address or DNS name. If you do not make any changes to the **Advanced Settings**, the configuration program uses the default settings listed and the configuration fails.

#### **Identity Applications Administrator**

Specifies the name of the administrator account for the identity applications. The default value is `uadmin`.

### Identity Applications host

Specifies the URL setting that connects to the User Application client on the application server.  
Do not use `localhost`.

## 5.5 Identity Reporting Module

This section defines the settings for the Identity Reporting Module. The program displays the basic parameters. To view all parameters, click [Advanced Settings](#).

---

**IMPORTANT:** The Identity Reporting Module requires an Event Auditing Service. The Event Auditing Service runs only on Linux computers. If you are installing on a Windows computer, you must install the Event Auditing Service on a Linux computer first before you can continue with the configuration of the Identity Reporting Module on Windows.

---

### EAS System Password

*Applies to Windows servers or if the Event Auditing Service is not running on the local computer.*

Specify the system password of your EAS system that is installed on a Linux computer. The system password is found in the `activemqusers.properties` file located in the `/etc/opt/novell/sentinel_eas/config` directory on your Linux computer.

### idmrptsrv password

Specifies the password for the owner of the database schemas and objects for reporting.

The installation process creates the `idmrptsrv` account.

### idmrptuser password

Specifies the password for the user with read-only access to the reporting data.

The installation process creates the `idmrptuser` account.

### dbauser password

Specifies the password for the administrator of the SIEM database that the Event Auditing Service and Identity Reporting use (Identity Information Warehouse).

The installation process creates the `dbauser` account.

### EAS server host

*Applies to Windows servers or if the Event Auditing Service is not running on the local computer.*

Specify the IP address or DNS name of the server that is running your Event Auditing Service and the PostgreSQL database.

### Database port

*Applies to Windows servers or if the Event Auditing Service is not running on the local computer.*

Specify the port through which the PostgreSQL database communicates. The default port is 15432.

### EAS dbauser password

Specify the password of the `dbauser` of the PostgreSQL database.

### Managed System Gateway port

Specifies the port that you want the MSGW driver to use for communicating with the Identity Vault.

The default value is 7707.

### **Data Collection Service host**

Specifies the DNS name or IP address of the server that hosts Data Collection Service. Do not use `localhost`.

### **Advanced Settings**

All of the remaining settings are under **Advanced Settings**. If you do not make any changes to the **Advanced Settings**, the configuration program uses the default settings listed.

### **Enable subcontainer search**

Select whether the Identity Reporting Modules support subcontainer searches. By default, this option is enabled.

### **Use secure LDAP connections**

Select whether you want the server to communicate over a secure LDAP connection.

You must also specify the **LDAP port**.

### **LDAP port**

Specifies the port for communication with the server that hosts the Identity Vault. Specify the same value that you specified for **LDAP secure port** in [Section 5.1, "Identity Vault," on page 31](#).

Alternatively, you can specify a clear text port for non-secure communication. If you do so, do not select **Use secure LDAP connections**.

### **Token expiration value (in minutes)**

Specify the length of time to retain a token for authentications. The default value is 60 minutes.

### **Retain completed reports: Duration and Units**

Select the amount of time that the Identity Reporting Module retains completed reports before deleting them. For example, to specify six months, select **Month** for the duration and then specify **6** for the units.

### **Subcontainer login attribute**

Specifies the login attribute that Identity Manager uses to search the subtree of a specified user container when gathering data for reports. The default value is `cn`.

---

**NOTE:** If you specify a DN that includes special characters, you might need to escape those characters. For more information, see [RFC 2253/4514 Section 2](#).

---

### **SMTP server host**

Specifies the DNS name or IP address of the email server that you want the Identity Reporting Module to use when sending notifications. The default value is `localhost`. Change to a valid IP address or DNS name.

### **SMTP server port**

Specifies the port number for the email server. The default value is 435.

### **SMTP userID**

(Conditional) When using authentication for communication with the email server, specifies the email address that you want to use for authentication.

You must also select **Requires server authentication for SMTP**.

### **SMTP user password**

Specifies the password associated with the email address that you want to use for authentication.

**Default email address**

Specifies the email address that you want Identity Reporting to use as the origination for email notifications.

**Use SSL for SMTP**

Specifies whether you want to use SSL for communication with the email server. By default, this option is not enabled.

**Require server authentication for SMTP**

Specifies whether you want to use authentication for communications with the email server.

You must also specify values for **SMTP userid** and **SMTP user password**. By default, this option is not enabled.

## 5.6 Tools

This section defines the settings for Identity Manager tools: iManager, Analyzer, and Designer. At this time, only iManager has programmable parameters. These parameters appear only on Linux computers during the configuration. To view the parameters, click **Advanced Settings**.

---

**NOTE:** The specified HTTP stack ports must be different than the HTTP stack ports that you use for the Identity Vault. For more information, see the *iManager Administration Guide* ([https://www.netiq.com/documentation/imanager27/imanager\\_admin/data/hk42s9ot.html](https://www.netiq.com/documentation/imanager27/imanager_admin/data/hk42s9ot.html)).

---

**HTTP port**

Specifies the number of the stack port that iManager uses to communicate in clear text. The default value is 8080.

**Secure HTTP port**

Specifies the number of the stack port that iManager uses to communicate with TLS/SSL protocol. The default value is 8443.



---

# 6 Final Steps for the Integrated Installation Process

After the integrated installer completes, the Identity Manager components are installed and basic configuration has been completed. However, you must still create drivers and perform additional configuration steps for the different components to be fully functional.

## 6.1 Assigning the Password Policy Object to Driver Sets

You must assign the `DirXML-PasswordPolicy` object to each driver set in a tree in the Identity Vault. The integrated installation process does not add the policy object to the Identity Vault. However, you can create the object.

- ♦ [Section 6.1.1, “Creating the Password Policy Object,” on page 41](#)
- ♦ [Section 6.1.2, “Assigning the Password Policy Object,” on page 42](#)

### 6.1.1 Creating the Password Policy Object

If the `DirXML-PasswordPolicy` object does not exist in the Identity Vault, use the following steps to create it.

- 1 In a text editor, 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>
```

---

**NOTE:** Copying the content as is might insert some hidden special characters in the file. If you receive a `ldif_record() = 17` error message when you add these attributes to the Identity Vault, insert an extra space between the two DNS.

---

- 2 To add the `DirXML-PasswordPolicy` object in the Identity Vault, import the attributes from the file by performing one of the following actions:

**Linux:**

From the directory containing the `ldapmodify` utility, enter the following command:

```
ldapmodify -x -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
```

The `ldapmodify` utility is located by default in the `/opt/novell/eDirectory/bin` directory.

**Windows:**

Run `ldapmodify.exe` from the `install/utilities` directory of the Identity Manager installation kit.

## 6.1.2 Assigning the Password Policy Object

You must assign the `DirXML-PasswordPolicy` object to each driver set in a tree. For more information, see [Creating Password Policies](#) in the *Password Management 3.3.2 Administration Guide*.

## 6.2 Configuring Identity Manager Components

After installation, you need to configure some of the Identity Manager components.

- ♦ **Drivers:** Each driver has a specific guide that explains how to install and configure that driver. For more information, see the [Identity Manager 4.5 Drivers documentation website \(https://www.netiq.com/documentation/idm45drivers/\)](https://www.netiq.com/documentation/idm45drivers/).
- ♦ **Identity Applications:** You must configure the different identity applications to work in your environment. For more information, see following guides:
  - ♦ [NetIQ Identity Manager Setup Guide](#)
  - ♦ [NetIQ Identity Manager User Application: Administration Guide](#)
- ♦ **Identity Reporting:** You must configure Identity Reporting for your environment. For more information, see the [NetIQ Identity Reporting Module Guide](#).

---

# 7 Activating 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. Use the information in the following sections to activate the Identity Manager components.

## 7.1 Purchasing an Identity Manager Product License

To purchase an Identity Manager product license, so that you can activate the product, see the [NetIQ Identity Manager How to Buy web page \(https://www.netiq.com/products/identity-manager/advanced/how-to-buy/\)](https://www.netiq.com/products/identity-manager/advanced/how-to-buy/).

After you purchase a product license, NetIQ sends you a Customer ID. The email also contains a URL to the NetIQ website where you can obtain a Product Activation credential. If you do not remember your Customer ID or do not receive it, contact your sales representative.

## 7.2 Installing a Product Activation Credential

You must install the Product Activation Credential via iManager.

### To install the Product Activation Credential:

- 1 After you purchase a license, NetIQ sends you an email with your Customer ID. The email 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----).
- 3 Open iManager.
- 4 Select **Identity Manager > Identity Manager Overview**.
- 5 Browse to 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.

---

## 7.3 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 Identity Manager engine and Identity Manager drivers:

- 1 Open iManager.
- 2 Click **Identity Manager > Identity Manager Overview**.
- 3 Browse to 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 for which you want to view the activation information.
- 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.

---

## 7.4 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 Identity Manager engine:
  - ◆ 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 Identity Manager engine:
  - ♦ 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 7.2, “Installing a Product Activation Credential,”](#) on page 43 for each Identity Manager Integration module to activate the drivers.

## 7.5 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.

## 7.6 Activating Designer and the Role Mapping Administrator

Designer and the Role Mapping Administrator do not require additional activations beyond activating the Identity Manager engine and drivers.



# 8

## Uninstalling Identity Manager

You can uninstall all Identity Manager components that were installed using either the integrated installer wizard or by performing a silent uninstallation.

### 8.1 Using the Uninstallation Wizard

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

**To uninstall the Identity Manager components:**

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

- ♦ **Linux:** `./Uninstall_Identity_Manager`

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/NetIQ/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. For more information, see the [eDirectory uninstallation documentation \(https://www.netiq.com/documentation/edir88/edirin88/data/bnn8twh.html\)](https://www.netiq.com/documentation/edir88/edirin88/data/bnn8twh.html).

---

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 DN 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 Performing a 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`
- ♦ **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`

- ♦ **Windows:** `install location\Uninstall_Identity Manager Components\Uninstall Identity Manager Components.exe -i silent -f filename.properties`



---

# 9 Troubleshooting

Use the following information to troubleshoot issues with the integrated installation program.

## 9.1 Locating Log Files and Properties Files

The integrated installation program generates log files for installation and configuration processes. The installer also creates a `logfiles.txt` file, which contains the list of log and properties files.

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

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

## 9.2 Troubleshooting Failed Configurations

Use the following information to troubleshoot a failed configuration of components:

**Issue:** The configuration of the identity applications fails.

**Suggested Action:** Access the log files as described in [Section 9.1, “Locating Log Files and Properties Files,” on page 49](#). Search for the word `localhost`. If you find this word in the logs, it means that you did not change the default value of `localhost` to a valid IP address or DNS name under **Advanced Settings** during the configuration. Rerun the configuration and provide a valid IP address or DNS name under the **Advanced Settings**. For more information about configuring the Identity Applications, see [Section 5.4, “Identity Applications,” on page 36](#).

## 9.3 Troubleshooting Remote Loader Issues on Windows

By default, the integrated installation program installs all Identity Manager components to the `C:\NetIQ` directory. All drivers use the `C:\Novell` as the default directory. However, you can make the drivers work by manually changing the directory for the drivers.

**To make Remote Loader drivers work:**

- 1 Launch the Remote Loader console.
- 2 Add an instance of the appropriate driver.

- 3 Change the default path from `C:\Novell` to `C:\NetIQ`.
- 4 Continue with your normal configuration steps.

## 9.4 Troubleshooting Uninstallation

Review the following information to help you troubleshoot uninstallation issues. If the problem persists, contact your NetIQ representative.

**Issue:** Uninstallation process reports as incomplete, but the log file shows no failures.

**Suggested Action:** The process failed to delete the `netiq` directory that contains the installation files by default. You can delete the directory manually if you have removed all NetIQ software from your computer.