

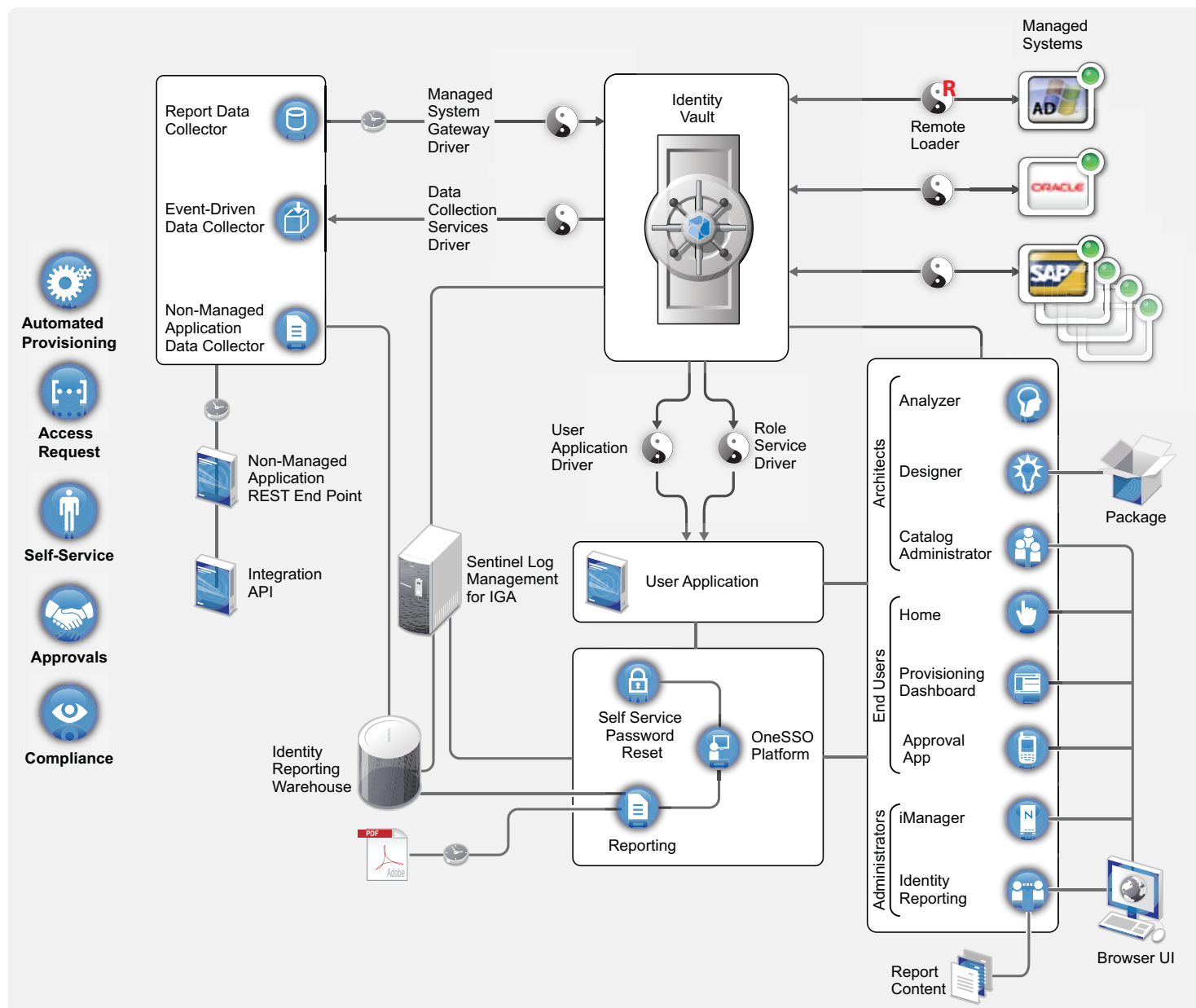
Quick Start Guide for Installing NetIQ Identity Manager 4.6

May 2017



This document provides guidelines to help you quickly understand the Identity Manager 4.6 installation process.

Before beginning, you must understand how different components are integrated in Identity Manager.



For more information, see [Overview of the Components of Identity Manager](#) in the *NetIQ Identity Manager Setup Guide*.

Installation Overview

Installing Identity Manager includes the following tasks:

- 1. Planning your installation
- 2. Installing and configuring the Identity Manager components
- 3. Verifying the installation for each component
- 4. Performing any post-installation tasks

For more information about installing the components, see the respective component installation section in the [NetIQ Identity Manager Setup Guide](#).

Planning Your Installation

Review the following information before installing Identity Manager:

Topic	See...
Feature comparison between Identity Manager Advanced and Standard Edition	Release Notes
Understanding download options	Release Notes
Downloading the installation files	Release Notes
Locating the executables and default installation paths	Release Notes
Installation prerequisites	Release Notes and prerequisites for each component in the NetIQ Identity Manager Setup Guide .
System requirements	System requirements for each component in the NetIQ Identity Manager Setup Guide .

For detailed information, see “Planning to Install Identity Manager” in the [NetIQ Identity Manager Setup Guide](#).

Installing and Configuring Identity Manager

You can install Identity Manager components on the same server or on multiple servers depending on your deployment strategy. Before you start installation, evaluate how you want to implement Identity Manager.

INSTALLATION SEQUENCE

The installation programs for some components require access to the previously installed components. For example, you should install and configure the Identity Vault before installing the Identity Manager engine. You must install the components in the following sequence:

- 1. Identity Vault (eDirectory)

- 2. Sentinel Log Management for Identity Governance and Administration (IGA) (optional if you already have Sentinel in your environment)
- 3. iManager
- 4. Identity Manager Engine
- 5. Apache Tomcat and PostgreSQL (Identity Manager provides a convenience installer to install these components)
- 6. One SSO Provider (OSP)
- 7. Self-Service Password Reset (SSPR)
- 8. Identity applications (not required for Standard Edition)
- 9. Designer (should be installed on a client computer)
- 10. Identity Reporting
- 11. Analyzer (only required for analyzing, cleaning, and preparing an organization’s data for synchronization)

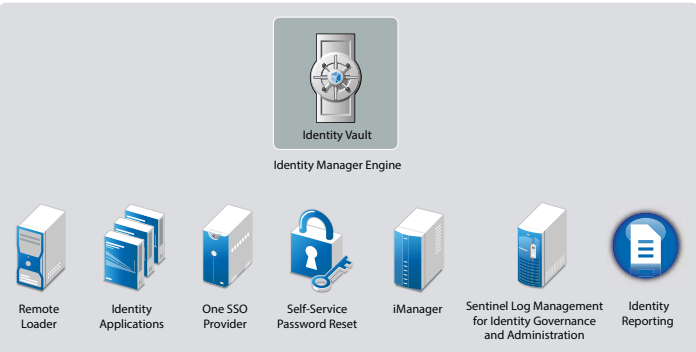
INSTALLATION PROCEDURE

There are different ways to install and configure Identity Manager to take advantage of all of its features. The following scenarios provide an overview of the flexibility built into Identity Manager. Use them to design a deployment strategy that fits the needs of your company. Regardless of the deployment option you choose, verify that your server meets the system requirements for each component that you are planning to install. For more information, see the [NetIQ Identity Manager Setup Guide](#).

IMPORTANT: These deployment scenarios are examples to help you install Identity Manager. You can use these examples for reference purposes. These examples do not reflect best practices or recommended configuration for a production environment. You must reach out to a [NetIQ Consulting Services](#) or a [NetIQ Partner Services](#) professional to help you design the Identity Manager system that is suitable for your environment.

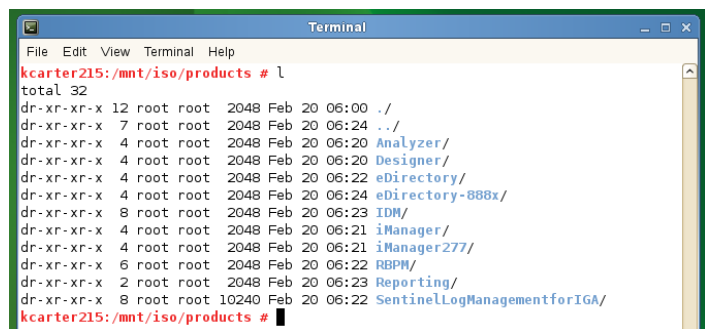
Basic Setup

The most basic deployment option is an all-in-one system that contains all Identity Manager components on a single server.



The all-in-one deployment is suitable only for installing Identity Management Proof-of-Concept (POC). This setup may cause performance issues in production environments. Identity Manager provides integrated installation program to install all components on one Linux or Windows computer except NetIQ Sentinel Log Management for Identity Governance and Administration component, which can be installed only on Linux computers. You can perform this installation by running the installation files (install.bin or install.exe) from the root directory of the .iso image file of the Identity Manager installation package.

To provide scalability to different components, you can extend a basic setup to accommodate the requirements of a production environment where services are distributed across multiple servers by using the standalone installation programs. This type of installation allows you to install Identity Manager components separately or customize a large portion of the settings. The individual installation files are located in the products/ directory within the .iso image file of the Identity Manager installation package.

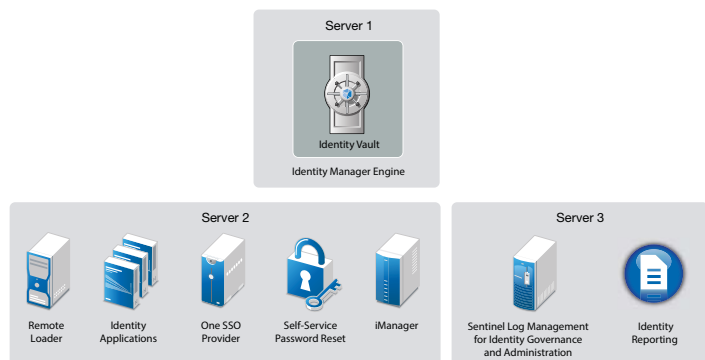


```

File Edit View Terminal Help
kcarter215:/mnt/iso/products # l
total 32
dr-xr-xr-x 12 root root 2048 Feb 20 06:00 ./
dr-xr-xr-x 7 root root 2048 Feb 20 06:24 ../
dr-xr-xr-x 4 root root 2048 Feb 20 06:20 Analyzer/
dr-xr-xr-x 4 root root 2048 Feb 20 06:20 Designer/
dr-xr-xr-x 4 root root 2048 Feb 20 06:22 eDirectory/
dr-xr-xr-x 4 root root 2048 Feb 20 06:24 eDirectory-888x/
dr-xr-xr-x 8 root root 2048 Feb 20 06:23 IDM/
dr-xr-xr-x 4 root root 2048 Feb 20 06:21 iManager/
dr-xr-xr-x 4 root root 2048 Feb 20 06:21 iManager277/
dr-xr-xr-x 6 root root 2048 Feb 20 06:22 RBPM/
dr-xr-xr-x 2 root root 2048 Feb 20 06:23 Reporting/
dr-xr-xr-x 8 root root 10240 Feb 20 06:22 SentinelLogManagementforIGA/
kcarter215:/mnt/iso/products #

```

In a simple approach, you can dedicate one server to Identity Vault and Identity Manager engine and Remote Loader and a second server to the identity applications, iManager, OSP, and SSPR components. You can include an additional server to host the components for reporting service to suffice the system requirements for running the Sentinel Log Management for IGA component.



Perform the following steps to install Identity Manager in this setup:

- 1 Install Identity Vault (eDirectory) on Server 1.
- 2 Install Sentinel Log Management for IGA on Server 3.

This component replaces Event Auditing Service that was included in the previous versions of Identity Manager. You can generate the required audit reports by using Sentinel Log Management for IGA.

- 3 Install the Identity Manager engine on Server 1.

Open the ports required for Identity Vault to communicate with Identity Manager components: 389, 524, 636, 8028, and 8030. For more information about these ports, see “[Understanding Identity Manager Communication](#)” in the *NetIQ Identity Manager Setup Guide*.

- 4 Install and deploy identity applications on Server 2.

Open the ports required by identity applications: 5432, 8005, 8009, 8080, 8109, 8180 and 8443 (also needed by iManager), 8543, 45654. For more information about these ports, see “[Understanding Identity Manager Communication](#)” in the *NetIQ Identity Manager Setup Guide*.

- 5 Install iManager and Remote Loader components on Server 2.

iManager needs port 9009.

Open the Remote Loader ports that you will set in the Remote Loader configuration files. Remote Loader uses port 8090 as the default port for connecting with the drivers. You must open any ports that will be used to connect to the applications running on other servers.

- 6 Install OSP and SSPR on Server 2.
- 7 Install and deploy Identity Reporting on Server 3.

Identity Reporting connects to Sentinel Log Management for IGA that was earlier installed on this server.

Open the ports required for Identity Reporting to communicate with Identity Manager components: 435 and 15432. For more information about these ports, see “[Understanding Identity Manager Communication](#)” in the *NetIQ Identity Manager Setup Guide*.

High Availability Configuration with Load Balancing

High availability ensures efficient manageability of critical network resources including data, applications, and services. You can install the following components in a high-availability environment:

- ♦ Identity Vault
- ♦ Identity Manager engine

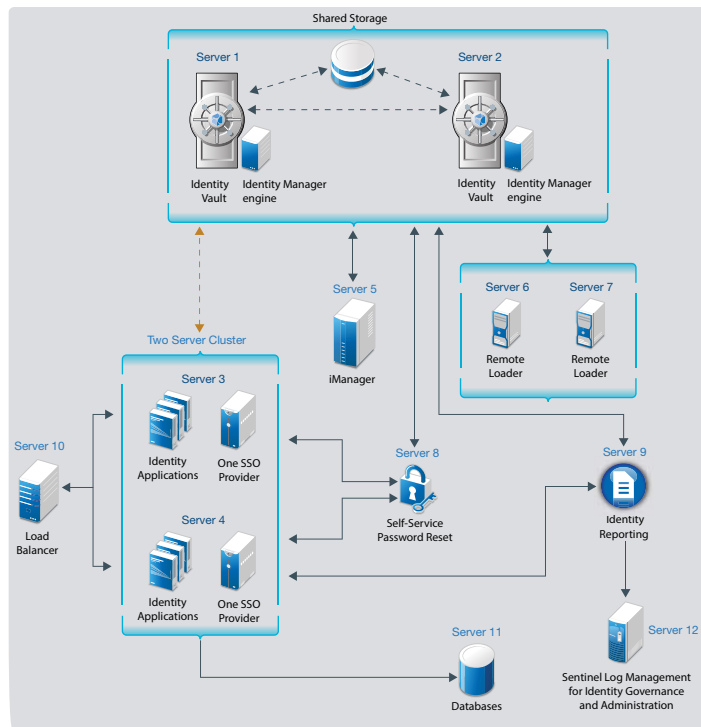
- ♦ Remote Loader
- ♦ Identity applications, except Identity Reporting

When you run the Identity Vault in a clustered environment, the Identity Manager engine is also clustered. In this configuration, the load is distributed across different Identity Vault servers. At any point of time only one node is active.

You can cluster identity applications and OSP and configure these components for load balancing and fault tolerance. The load balancer is typically part of the cluster. It understands the cluster configuration as well as failover policies. In this configuration, all the nodes in the cluster are active at any point of time. The load balancer performs the following actions:

- ♦ Distributes the load across all nodes to ensure that the nodes have roughly the same workload.
- ♦ Diverts the requests to the failed node to the surviving nodes when any of the nodes fail.

You must ensure that session stickiness is enabled for the cluster created in the load balancer software for the identity applications nodes.



You can easily add additional identity applications and OSP servers (or nodes) to handle the load, then add new servers to the L4 switch. When the new servers are added to the cluster, they are automatically sent the cluster configuration.

Perform the following steps to install Identity Manager in this setup:

- 1 Install Identity Vault on Server 1 and Server 2 with shared storage. State data for Identity Vault is located on the shared storage so that it is available to the cluster node that is currently running the Identity Vault. This data includes eDirectory DIB, NCI (NetIQ International Cryptographic Infrastructure) data, eDirectory configuration, and log data. For more information, see [“Sample Identity Manager Cluster Deployment Solution on SLES”](#) or [“Sample Identity Manager Cluster Deployment Solution on Windows”](#) in the *NetIQ Identity Manager Setup Guide*.

- 2 Install Sentinel Log Management for IGA on Server 12.

This component replaces Event Auditing Service that was included in the previous versions of Identity Manager. You can generate the required audit reports by using Sentinel Log Management for IGA.

- 3 Install the Identity Manager engine on both Identity Vaults.

Open the ports required for Identity Vault to communicate with Identity Manager components: 389, 524, 636, 8028, and 8030. For more information about these ports, see [“Understanding Identity Manager Communication”](#) in the *NetIQ Identity Manager Setup Guide*.

- 4 Install all databases on Server 11.

These databases are connected to the identity applications servers.

- 5 Install and deploy identity applications on Server 3 and Server 4.

Both Server 3 and Server 4 combine to form a two-server cluster.

For more information, see [“Sample Identity Applications Cluster Deployment Solution on Tomcat Application Server”](#) in the *NetIQ Identity Manager Setup Guide*.

Open the ports required by identity applications: 5432, 8005, 8009, 8080, 8109, 8180 and 8443 (also needed by iManager), 8543, 45654. For more information about these ports, see [“Understanding Identity Manager Communication”](#) in the *NetIQ Identity Manager Setup Guide*.

- 6 Install iManager on Server 5.

Open port 9009 that is used by iManager.

- 7 Install Remote Loader on Server 6 and Server 7.

Open the Remote Loader ports that you will set in the Remote Loader configuration files. Remote Loader uses port 8090 as the default driver port. You must open any ports that will be used to connect to the applications running on other servers.

- 8 Install OSP on Server 3 and Server 4.

Both Server 3 and Server 4 combine to form a two-server cluster.

9 Install SSPR on Server 8.

10 Install and deploy Identity Reporting on Server 9.

Open the ports required for Identity Reporting to communicate with Identity Manager components: 435 and 15432. For more information about these ports, see “[Understanding Identity Manager Communication](#)” in the *NetIQ Identity Manager Setup Guide*.

11 Deploy the load balancer on Server 10. This is required to balance the load between the Identity Applications servers.

Completing Post-Installation Tasks

After completing the installation of Identity Manager components, perform the necessary tasks. For example, configure the drivers you installed to meet the policies and

requirements defined by your business processes. You also need to configure Sentinel Log Management for IGA to gather audit events. For more information, see “[Post-Installation Tasks](#)” in the *NetIQ Identity Manager Setup Guide*.

Verifying Installed Components

After you install and configure Identity Manager components, verify that the components are properly installed. For example, you should log in to the individual identity applications and be able to switch among them without logging out. For more information, see the individual component section in the *NetIQ Identity Manager Setup Guide*.

Legal Notice: for information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.netiq.com/company/legal/>.

Copyright © 2017 NetIQ Corporation, a Micro Focus company. All Rights Reserved.

