NetIQ® Identity Manager

Overview and Planning Guide

May 2024

Legal Notice

Copyright 2009 - 2024 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

For additional information, such as certification-related notices and trademarks, see http://www.microfocus.com/about/legal/ (http://www.microfocus.com/about/legal/).

Contents

About this Book and the Library 7

Part I Identity Manager Overview 9

1 How Identity Manager Solves Business Challenges 11

Synchronizing Identity Information 12
Automating Business and IT Processes with Workflows 13
. . . . . Providing
Role-Based
Access to
Users 15
Enabling Self-Service for Users. 15
Auditing, Reporting, and Complying with Regulations 17

2 Identity Manager Editions 19

3 Identity Manager Architecture 21

How Identity Manager Works 22
Identity Vault 22
Identity Manager Engine. 22
Remote Loader. 23
Connected System 23
Identity Manager Driver 23
Identity Manager Driver Set 23
Identity Reporting 24
Identity Applications 24
Designer for Identity Manager 25
Analyzer for Identity Manager 26
Identity Console. 26
Key Features and Benefits of Architecture 26
Staged Deployment 26
Flexibility and Extensibility 28
Reuse of Existing Infrastructure 28
Extensive Identity Integration. 29
Built-in Audit and Compliance 29

4 Identity Manager Integration Solutions with Existing IT Infrastructure and Applications 31

Out-of-Box Drivers. 31
Identity Manager Driver Development Kit 31
SOAP and REST API Support for Identity Applications 32

5 Identity Manager Deployment Configurations **33**

Basic Configuration . . . 33
High Availability Configuration . . . 35

6 Understanding Identity Manager Localization **37**

Translated Components and Installation Programs . . . 37
Special Considerations for Language Support . . . 38

7 Where to Get Identity Manager **39**

8 Understanding Licensing and Activation **43**

Activating Identity Manager . . . 43
Installing a Product Activation Credential . . . 43
Reviewing Product Activations for Identity Manager and Drivers . . . 44
Activating Identity Manager Drivers . . . 45
Activating Specific Identity Manager Components . . . 45

Part II Planning **49**

9 Creating a Project Plan **51**

Discovery Phase . . . 51
Discovering Current Business Processes . . . 52
Defining How the Identity Manager Solution Affects the Current Business Processes . . . 54
Identifying the Key Business and Technical Stakeholders . . . 54
Interviewing All Stakeholders . . . 54
Creating a High-level Strategy and an Agreed Execution Path . . . 55
Requirements and Design Analysis Phase . . . 55
Defining the Business Requirements . . . 56
Analyzing Your Business Processes . . . 57
Designing an Enterprise Data Model . . . 58
Proof of Concept . . . 60
Data Validation and Preparation . . . 60
Quality Assurance . . . 61
Production Roll-out Planning . . . 61
Production Deployment . . . 62

10 Setting Up a Development Environment **63**

11 Technical Guidelines **65**

Components to Install . . . 65
Identity Manager Configurations . . . 65
Technical Guidelines . . . 65
Management Tools Guidelines . . . 66
Analyzer Guidelines . . . 67
Designer Guidelines . . . 68
Identity Console Guidelines . . . 68
Identity Manager Server Guidelines . . . 68

Considerations for Installing Drivers with the Identity Manager Engine. 68
Considerations for Installing Drivers with the Remote Loader 69
Identity Vault Guidelines 70
Understanding Identity Manager Objects in Identity Vault 70
Replicating the Objects that Identity Manager Needs on the Server 70
Using Scope Filtering to Manage Users on Different Servers 72
Improving Identity Vault Performance. 74
Identity Applications Guidelines 74
Auditing and Reporting Guidelines 76

About this Book and the Library

This guide introduces you to NetIQ Identity Manager, a product that manages identity and access across physical, virtual, and cloud environments. This guide explains business issues that Identity Manager can help you solve while reducing costs and ensuring compliance. It also contains a technical overview of the Identity Manager components and tools you can use to create your Identity Manager solution.

Intended Audience

This guide is intended for administrators, consultants, and network engineers who require a high-level introduction to Identity Manager business solutions, technologies, and tools.

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/identity-manager-49/).

Identity Manager Overview

NetIQ Identity Manager is an end-to-end identity administration and user provisioning solution. It helps you build a secure and intelligent identity environment. Identity Manager includes enterprise-wide access control, password management, and self-service functionalities. These capabilities help your organization to manage identities and resources efficiently. Identity Manager also improves productivity, mitigate risks, reduce administration cost and support regulatory compliance efforts.

Identity Manager provides policy-driven access control to resources from the data center to the cloud, and also helps you ensure risk management and compliance.

- Chapter 1, “How Identity Manager Solves Business Challenges,” on page 11
- Chapter 2, “Identity Manager Editions,” on page 19
- Chapter 3, “Identity Manager Architecture,” on page 21
- Chapter 4, “Identity Manager Integration Solutions with Existing IT Infrastructure and Applications,” on page 31
- Chapter 5, “Identity Manager Deployment Configurations,” on page 33
- Chapter 6, “Understanding Identity Manager Localization,” on page 37
- Chapter 7, “Where to Get Identity Manager,” on page 39
- Chapter 8, “Understanding Licensing and Activation,” on page 43

1 How Identity Manager Solves Business Challenges

Most organizations have their identity data stored on multiple systems. In this case, managing identities and monitoring user activity on physical and virtual environments is important. Identity Manager solution provides an automated environment to solve these challenges by:

- Synchronizing the identity data across connected systems.
- Ensuring that users have access only to the resources required for their jobs.
- Provisioning or deprovisioning user access based on their roles.
- Providing compliance with your business policies and other regulatory requirements

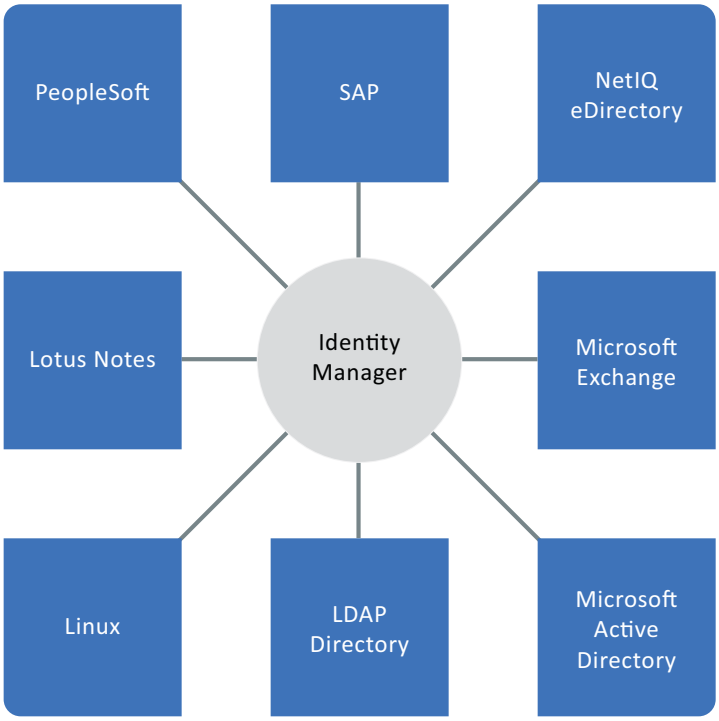
The following sections explain the features of Identity Manager that provides a solution for these challenges:

- "Synchronizing Identity Information" on page 12
- "Automating Business and IT Processes with Workflows" on page 13
- "Providing Role-Based Access to Users" on page 15
- "Enabling Self-Service for Users" on page 15
- "Auditing, Reporting, and Complying with Regulations" on page 17

Synchronizing Identity Information

Identity Manager lets you synchronize, transform, and share information across a wide range of connected systems, such as SAP, PeopleSoft, Microsoft SharePoint, Lotus Notes, Microsoft Exchange, Microsoft Active Directory, NetIQ eDirectory, Oracle, among many others. Figure 1-1 represents how Identity Manager synchronizes information with multiple systems.

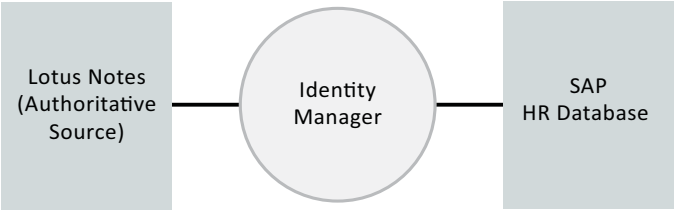
Figure 1-1 *Identity Manager Connecting Multiple Systems*



Identity Manager lets you do the following activities:

- Control the flow of data among the connected systems.
- Determine what data is shared, which system is the authoritative source for a piece of data, and how the data is interpreted and transformed to meet the requirements of other systems.

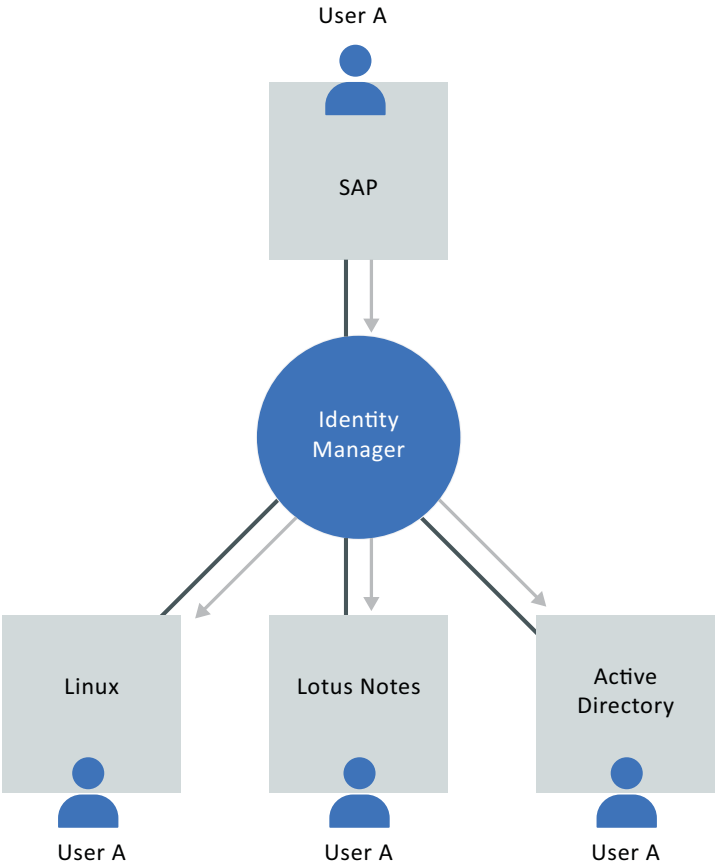
  In the following diagram, the Lotus Notes system is the authoritative source for a user's e-mail address. The SAP HR database also uses e-mail addresses, so Identity Manager transforms the e-mail address into the required format and shares it with the SAP HR database. When the e-mail address changes in the Lotus Notes system, it is synchronized to the SAP HR database.



  If an administrator of the SAP HR database changes a user's e-mail address in that system, the change has no effect because the change must be made to the Lotus Notes system to be effective. Identity Manager uses filters to specify authoritative sources for an item.

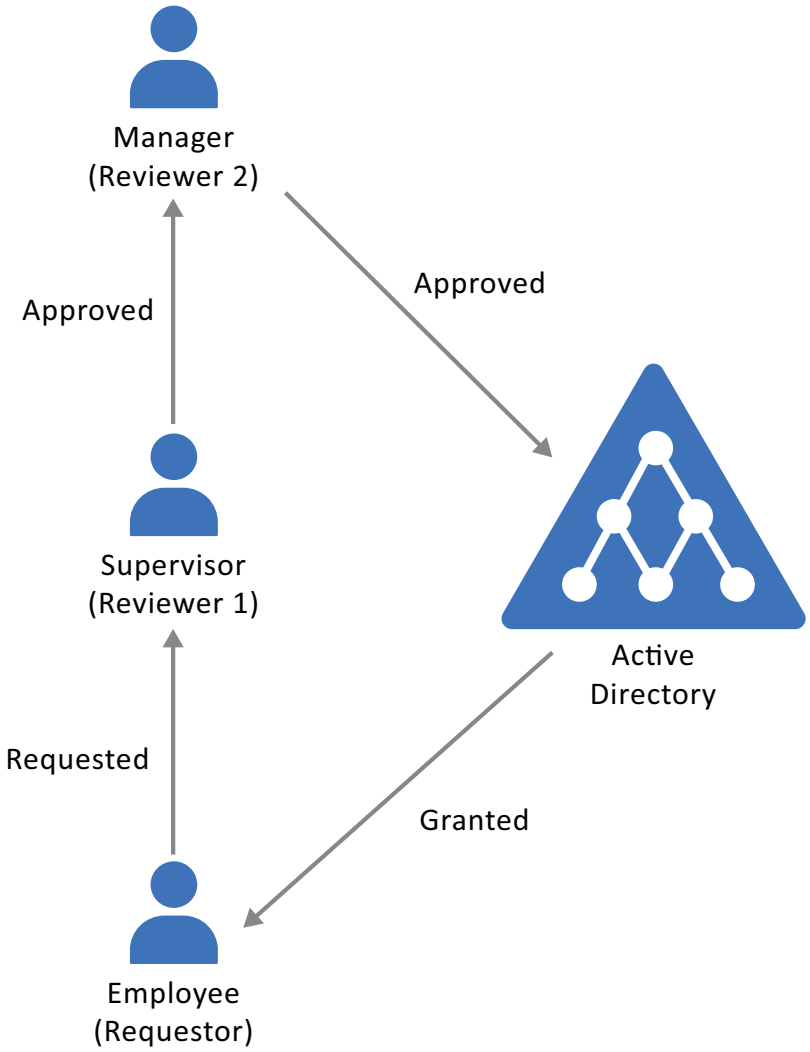
- Synchronize passwords between systems. For example, if a user changes his or her password in Active Directory, Identity Manager can synchronize that password to other connected systems. For example, Lotus Notes, SAP, or Oracle.
- Create new user accounts and remove existing accounts in connected systems. For example, when you hire a new employee in the SAP HR application, Identity Manager can automatically create a new user account in other connected systems.

Figure 1-2 *User Account Creation in Connected Systems*



Automating Business and IT Processes with Workflows

In an organization, users often require access to various resources to accomplish tasks based on their roles. Identity Manager provides workflow capabilities to ensure that your provisioning processes involve the appropriate resource approvers.



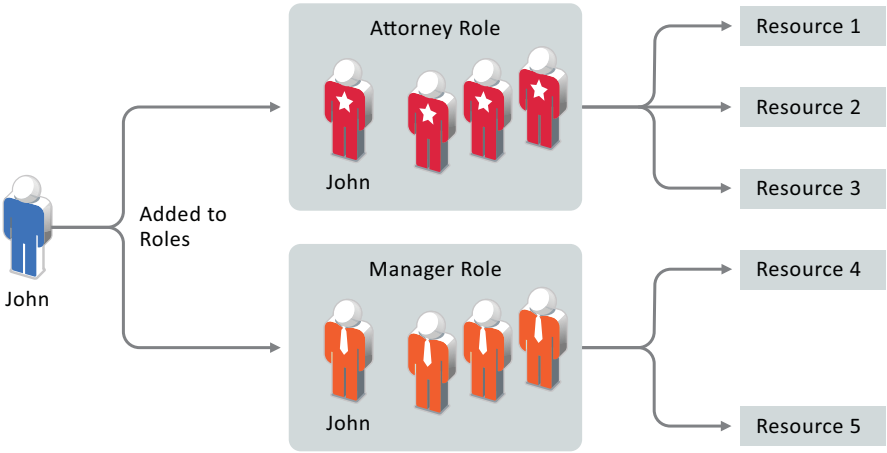
Identity Manager also provides workflow capabilities to ensure that your provisioning processes involve the appropriate resource approvers. For example, assume that John, who has already been provisioned with an Active Directory account, needs access to some financial reports through Active Directory. This requires approval from both John's immediate manager and the CFO. Fortunately, you have set up an approval workflow that routes John's request to his manager and, after approval from his manager, to the CFO. Approval by the CFO triggers automatic provisioning of the Active Directory rights needed by John to access and view the financial documents.

Workflows are highly flexible and capable of supporting varying business requirements through template definition, escalation, parallel approvals, serial approvals and multi-step approvals. Workflows can be initiated automatically when a certain event occurs (for example, a new user is added to your HR system) or initiated manually through a user request.

Providing Role-Based Access to Users

Provisioning involves automating the process of adding, modifying and deleting users and their attributes. This includes managing users' profile attributes, including their role memberships and their associated access rights. Identity Manager lets you provision users based on their roles in the organization.

Identity Manager lets you provision users based on their roles in the organization. You define the roles and make the assignments according to your organizational needs. When a user is assigned to a role, Identity Manager provisions the user with access to the resources associated with the role. Users that have multiple roles receive access to the resources associated with all of the roles, as shown in the following illustration:



You can have users automatically added to roles as a result of events that occur in your organization. For example, you might add to your SAP HR database a new user with the job title of Attorney. If approval is required for adding a user to a role, you can establish workflows to route role requests to the appropriate approvers. You can also manually assign users to roles.

In some cases, certain roles should not be assigned to the same person because the roles conflict. Identity Manager provides Separation of Duties functionality that lets you prevent users from being assigned to conflicting roles unless someone in your organization makes an exception for the conflict.

Because role assignments determine a user's access to resources within your organization, ensuring correct assignments is critical. Incorrect assignments could jeopardize compliance with both corporate and government regulations.

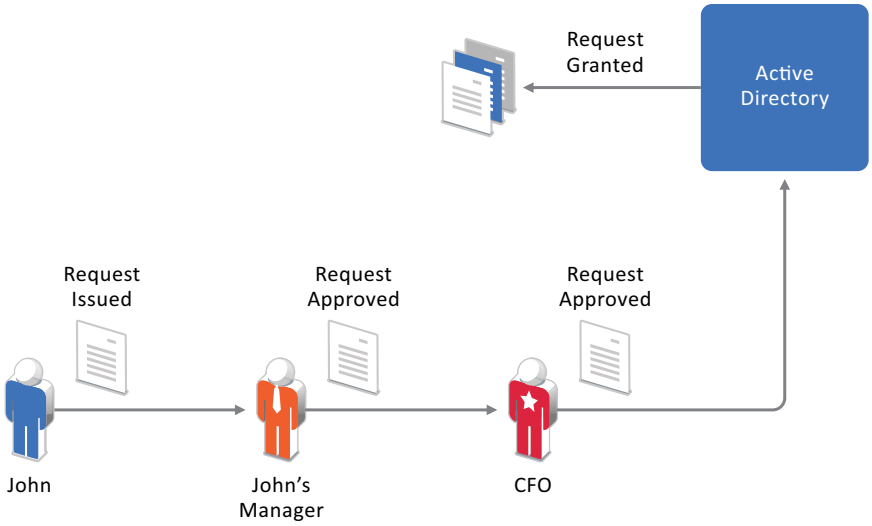
Enabling Self-Service for Users

Identity Manager uses identity as the basis for authorizing users access to systems, applications, and databases. Each user's roles managed in Identity Manager can come with specific access rights to connected applications. For example, users who are identified as managers can access salary

information about their direct reports, but not about other employees in their organization. With Identity Manager, you can delegate administrative duties to the people who should be responsible for them. For example, you can enable individual users to accomplish the following goals:

- **Manage Personal Data:** Users can view and edit their own personal data in the corporate directory by using the self-service interface of Identity Manager. The data is automatically changed in all the systems you have synchronized through Identity Manager. This reduces administrative overhead and provides users with control over their identity profiles.
- **Change Password:** Users can change their passwords, set up a hint for forgotten passwords, and set up challenge questions and responses for forgotten passwords. Identity Manager includes a comprehensive set of password management services which increase security by enforcing consistent password policies across the organization. These also combine with self-service password reset capabilities to reduce the cost of password-related help desk calls.
- **Request Access:** Users can request access to resources such as databases, systems, and directories. Rather than calling you to request access to an application, they can select the application from a list of available resources.

  In addition to self-service for individual users, Identity Manager provides self-service administration for functions (management, Help Desk, and so forth) that are responsible for assisting, monitoring, and approving user requests. For example, John uses the Identity Manager self-service feature to request access to the documents that he needs. John's manager and the CFO receive the request through the self-service feature and can approve the request. The established approval workflow allows John to initiate and monitor the progress of his request and allows John's manager and CFO to respond to his request. Approval of the request by John's manager and the CFO triggers the provisioning of the Active Directory rights that John needs to access and view the financial documents.



You can initiate workflows automatically when a certain event occurs (for example, a new employee is hired in the SAP HR application) or manually through a user request.

Auditing, Reporting, and Complying with Regulations

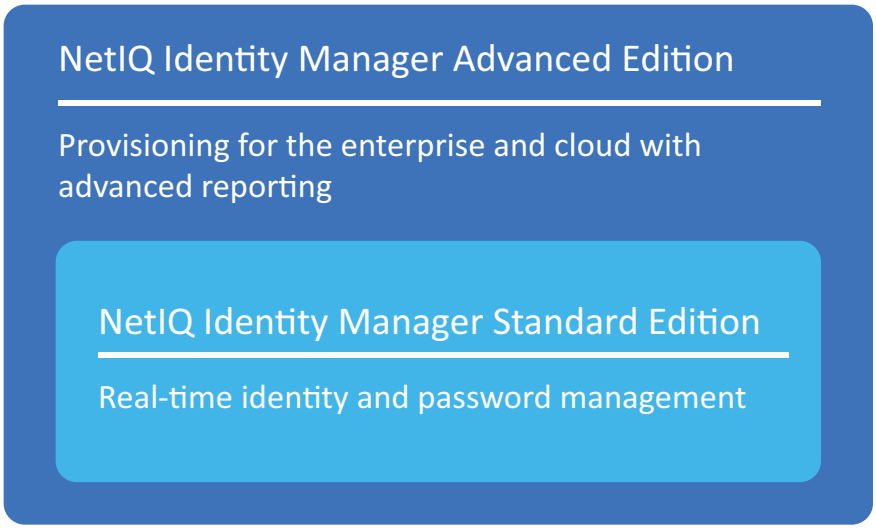
Identity Manager has an inbuilt auditing service that captures a complete trail of events that occur in your Identity Management system. All of your user provisioning activities, past and present, are being tracked and logged for auditing purposes. The auditing system also captures data generated by its workflow and policies. By combining this data along with identity data, you can have all the required data to address any identity and access-related audit queries.

Identity Manager reports on both historical data and the current state of the provisioning environment. Using Identity Manager you can retrieve all the information you need to ensure that your organization is compliant with relevant business laws and regulations. Some of the identity data captured by Identity Manager includes user identity profile history, user group membership history, user resource access, and fine-grained entitlement history.

Identity Manager provides standard reports that let you perform queries against the information warehouse to demonstrate compliance for business, IT, and corporate policies. You can also create custom reports if the predefined reports don’t meet your needs. Custom reports may include the modification of a standard report or the creation of a unique report using the audit and log data.

2 Identity Manager Editions

Identity Manager offers Advanced and Standard Editions targeted for different use cases. The complete set of functionality is included in Advanced Edition. Standard Edition includes a subset of the features provided in Advanced Edition.



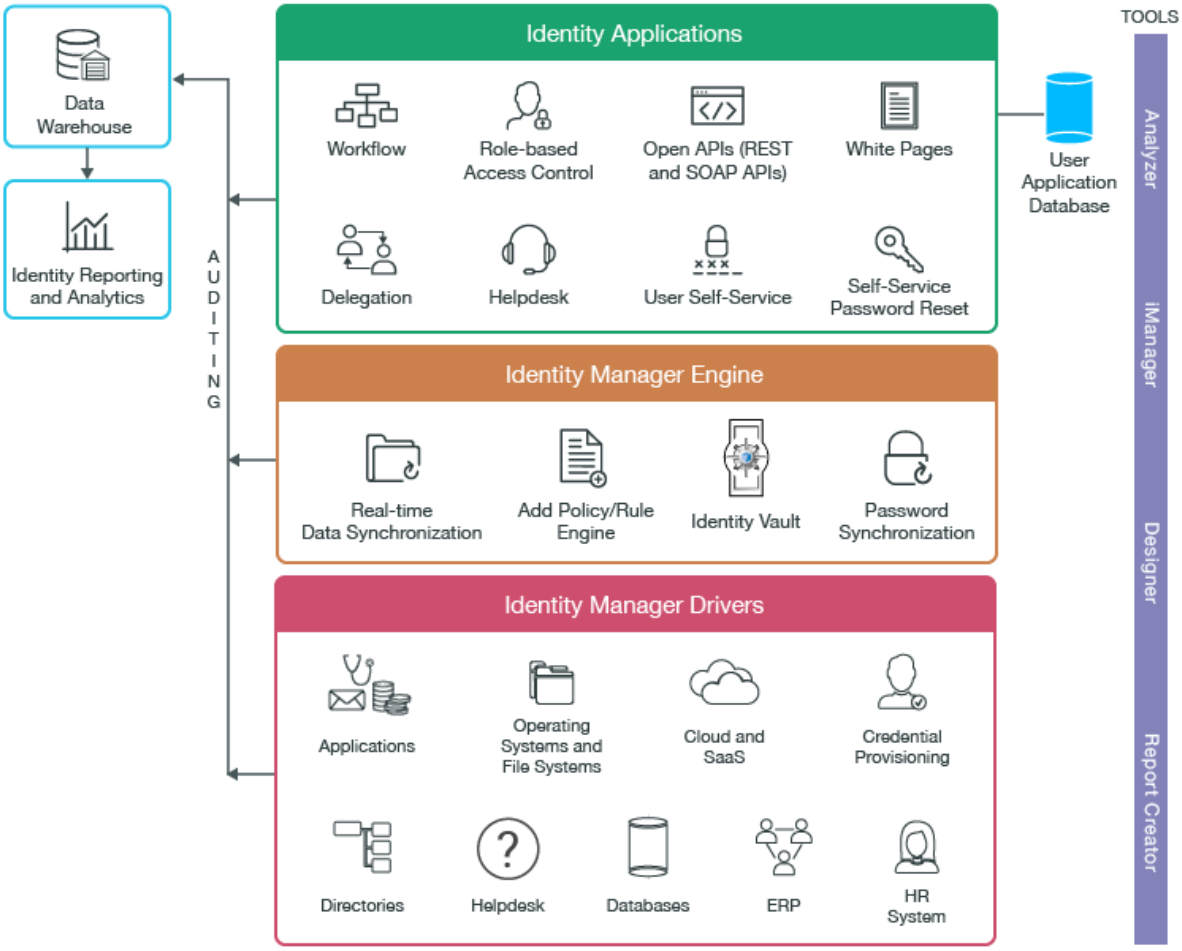
The following table provides a comparison of features available in Identity Manager Advanced and Standard Editions:

Feature	Advanced Edition	Standard Edition
Rule-based automated user provisioning	Yes	Yes
Real-time identity synchronization	Yes	Yes
Password management and password self-service	Yes	Yes
Uniform identity information tool (Analyzer)	Yes	Yes
REST APIs and single sign-on support	Yes	Yes (limited support)
Current state reporting	Yes	Yes
Role-based enterprise-level provisioning	Yes	No
Automated approval workflows for business policy enforcement	Yes	No
Advanced self-service in the identity applications	Yes	No
Resource model and catalog for easy resource provisioning	Yes	No
Historical state reporting	Yes	No
Connected systems reporting	Yes	No

Feature	Advanced Edition	Standard Edition
Role and resource administration	Yes	No

3 Identity Manager Architecture

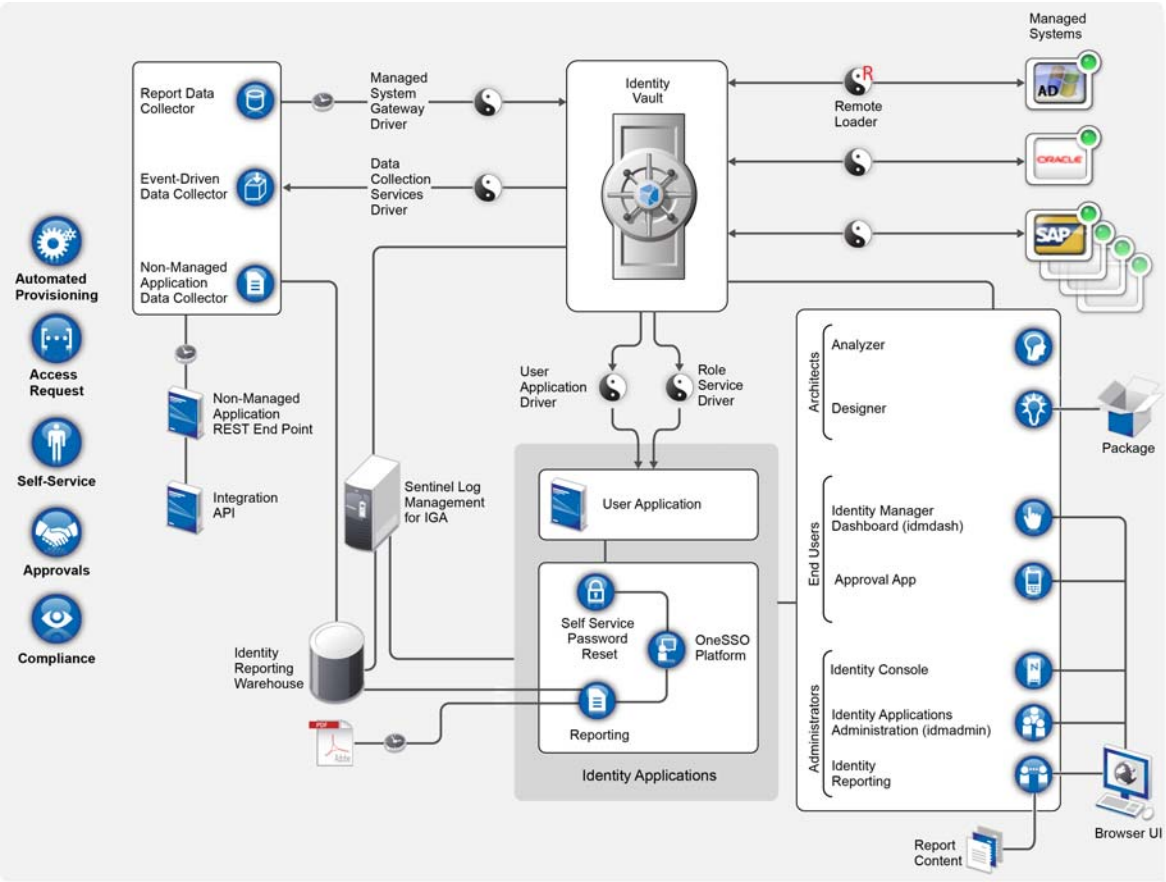
Identity Manager consists of logically separate front-end components from the back-end provisioning engine. This enables tremendous scalability capable of supporting the requirements of even the largest enterprises. This distributed computing approach enables you to implement high availability and disaster recovery at each layer. It also provides deployment flexibility, allowing you to start with a basic implementation and add capacity and functionality over time.



For information about Identity Manager components, see "How Identity Manager Works" on page 22.

How Identity Manager Works

The following diagram shows how the high-level components interact with one another to provide the NetIQ Identity Manager capabilities: data synchronization, workflow, roles, self-service, and auditing/reporting.



Identity Vault

The **Identity Vault** contains all information that Identity Manager requires. The Identity Vault saves the data that you want to synchronize among the connected systems. For example, data synchronized from a SAP system to Lotus Notes is first added to the Identity Vault and then sent to the Lotus Notes system. The Identity Vault also stores information specific to Identity Manager, such as driver configurations, parameters, and policies.

The Identity Vault uses a NetIQ eDirectory database. For more information about using eDirectory see the *NetIQ eDirectory 9.2 Administration Guide*.

Identity Manager Engine

The **Identity Manager engine** processes all data changes that occur in the Identity Vault or a connected application. For events that occur in the Identity Vault, the engine processes the changes and issues commands to the application via the driver. For events that occur in the application, the engine receives the changes from the driver, processes the changes, and issues commands to the

Identity Vault. **Drivers** connect the Identity Manager engine to the applications. A driver has two basic responsibilities: reporting data changes (events) in the application to the Identity Manager engine and carrying out data changes (commands) submitted by the Identity Manager engine to the application. Drivers must be installed on the same server as connected application. For more information, see the individual driver guides on the Identity Manager Drivers Documentation page.

The Identity Manager engine has also been referred to as Metadirectory engine. The server on which the Identity Manager engine runs is referred to as the **Identity Manager server**. You can have more than one Identity Manager server in your environment, depending on server workload.

Remote Loader

The **Identity Manager Remote Loader** loads drivers and communicates with the Identity Manager engine on behalf of drivers installed on remote servers. If the application runs on the same server as the Identity Manager engine, you can install the driver on that server. However, if the application does not run on the same server as the Identity Manager engine, you must install the driver on the application's server. To help with the workload or configuration of your environment, you can install Remote Loader on a server separate from the servers that have Tomcat and the Identity Manager server.

Connected System

In Identity Manager, a managed system, also called a connected system or application, is any system, directory, database, or operating system whose identity information you want to manage. For example, connected systems can be the PeopleSoft application or an LDAP directory. A driver, such as Active Directory driver, provides the connection between Microsoft Active Directory and the Identity Vault. The application must provide APIs that a driver can use to determine application data changes and effect application data changes. Applications are frequently referred to as connected systems.

Identity Manager Driver

Drivers connect to the applications whose identity information you want to manage. It also enables data synchronization and sharing between systems.

A driver has two basic responsibilities: reporting data changes (events) in the application to the Identity Manager engine, and carrying out data changes (commands) submitted by the Identity Manager engine to the application. It also enables data synchronization and sharing between systems.

Identity Manager Driver Set

Identity Manager stores drivers and library objects in a container called a driver set. When you create an Identity Vault, a driver set is added to the vault by default.

Only one driver set can be active on a server at a time. However, more than one server might be associated with one driver set. Also, a driver can be associated with more than one server at a time. However, the driver should be running on only one server at a time. The driver should be in a disabled state on the other servers. Any server that is associated with a driver set must have the Identity Vault installed on it.

Identity Reporting

Identity Manager includes the **Identity Information Warehouse**, which is an intelligent repository of information about the actual and desired states of the Identity Vault and the connected systems within your organization. The Identity Information Warehouse gives you a 360-degree view of your business entitlements, providing the knowledge you need to see the past and present state of authorizations and permissions granted to identities in your organization.

When you query the Identity Information Warehouse, you can retrieve all of the information that you need to ensure that your organization is in full compliance with relevant business laws and regulations. With this knowledge, you can answer even the most sophisticated Governance Risk and Compliance (GRC) queries. For more information, see the *Administrator Guide to NetIQ Identity Reporting*.

Identity Applications

The identity applications comprise of the following high-level components:

User Application

The Identity Manager **User Application** gives your users and business administrators a view into the information, resources, and capabilities of Identity Manager. The User Application is a browser-based web application that gives the user the ability to perform a variety of identity self-service and roles provisioning tasks. Users can manage passwords and identity data, initiate and monitor provisioning and role assignment requests, manage the approval process for provisioning requests, and verify attestation reports.

The User Application runs on the **Roles Based Provisioning Module** (RBPM) framework, which includes the workflow engine that controls the routing of requests through the appropriate approval process.

Users can access the User Application from any supported web browser. For more information about the User Application, see the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Identity Applications Administration

The **Identity Applications Administration** interface allows you to manage the following tasks with an appropriate Administrator role:

- Create and manage roles, resources and their assignments
- Set the Separation of Duties (SoD) constraints to avoid conflicts between two different roles in the system
- Configure the ability for users to approve permission requests through email
- Configure the default settings of your identity applications components such as roles, resources, and delegation.

Administrators can access the Administration page with any supported web browser, from either a computer or a tablet. For more information, see the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Identity Manager Dashboard

The **Identity Manager Dashboard** (the Dashboard) includes a personalized view of each user's permissions, tasks, and requests. This helps users focus on the following basic areas of functionality:

I want something.

If you need an item, whether the item is a piece of equipment like a laptop or something intangible like access to a particular server or application, you can request that item.

I need to do something.

If you want to know what tasks you need to manage, **My Tasks** page shows all of your pending approval or provisioning tasks in the Identity Manager system.

What do I have?

If you want to see your current permissions, the **My Permissions** page provides a list of the roles and resources to which you have access.

How did I get it?

If you want to see a list of past requests, the **Requests History** page shows everything that you have requested recently, as well as the status of your pending requests.

If you have an administrative role for the identity applications, you can customize the **Applications** page in the Dashboard for all users. You can configure the page to show items and links that your users need to see, organized into categories that make sense for your enterprise. You can include the following types of items:

- Identity Manager functions, such as creating groups or running reports
- Permissions that most users need to request
- Links to commonly accessed websites or web-based applications
- REST endpoints
- Badges, such as the number of items of a certain type that a user can access

Users can access the Dashboard with any supported web browser, from either a computer or a tablet. For more information, see the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Designer for Identity Manager

Designer for Identity Manager (Designer) helps you design, test, document, and deploy Identity Manager solutions in a network or test environment. You can configure your Identity Manager project in an off-line environment, and then deploy to your live system. From a design perspective, Designer helps do the following:

- Graphically view all of the components that comprise your Identity Manager solution and observe how they interact.
- Modify and test your Identity Manager environment to ensure it performs as expected before you deploy part or all of your test solution to your production environment.

Designer keeps track of your design and layout information. With a click of a button, you can print that information in a format of your choice. Designer also enables teams to share work on enterprise-level projects.

For more information about using Designer, see the *NetIQ Designer for Identity Manager Administration Guide*.

Analyzer for Identity Manager

Analyzer for Identity Manager (Analyzer) provides data analysis, cleansing, reconciliation, and reporting to help you adhere to internal data quality policies. Analyzer lets you analyze, enhance, and control all data stores throughout the enterprise. Analyzer includes the following features:

- Analyzer's schema map associates an application's schema attributes to the corresponding schema attributes in Analyzer's base schema. This lets you ensure that your data analysis and cleaning operations properly associate similar values between the disparate systems. To accomplish this, Analyzer leverages the schema mapping features in Designer.
- The Analysis Profile editor lets you configure a profile for analyzing one or more data set instances. Each analysis profile contains one or more metrics against which you can evaluate attribute values to see how the data conforms to your defined data format standards.
- The Matching Profile editor lets you compare values in one or more data sets. You can check for duplicate values within a specified data set and check for matching values between two data sets.

For more information about using Analyzer, see the *NetIQ Analyzer for Identity Manager Administration Guide (https://www.netiq.com/documentation/identity-manager-48/analyzer_admin/data/netiq-identity-manager-analyzer-admin.html)*.

Identity Console

NetIQ Identity Console is a state-of-the-art Web-based administration console that provides virtual, secure and customized access to network administration utilities from anywhere over the Internet and Web browser. Identity Console makes the decentralization of the administrative tasks much easier. Identity Console is a replacement for iManager.

With Identity Console, you can perform similar tasks as performed with Designer and also monitor the health of your system. NetIQ recommends that you use Identity Console for administrative tasks. Use Designer for configuration tasks that require changes to packages, modeling, and testing prior to deployment.

For more information about Identity Console, see the *Identity Console Administration Guide (https://www.netiq.com/documentation/identity-console/identity_console-admin/data/bookinfo.html)*.

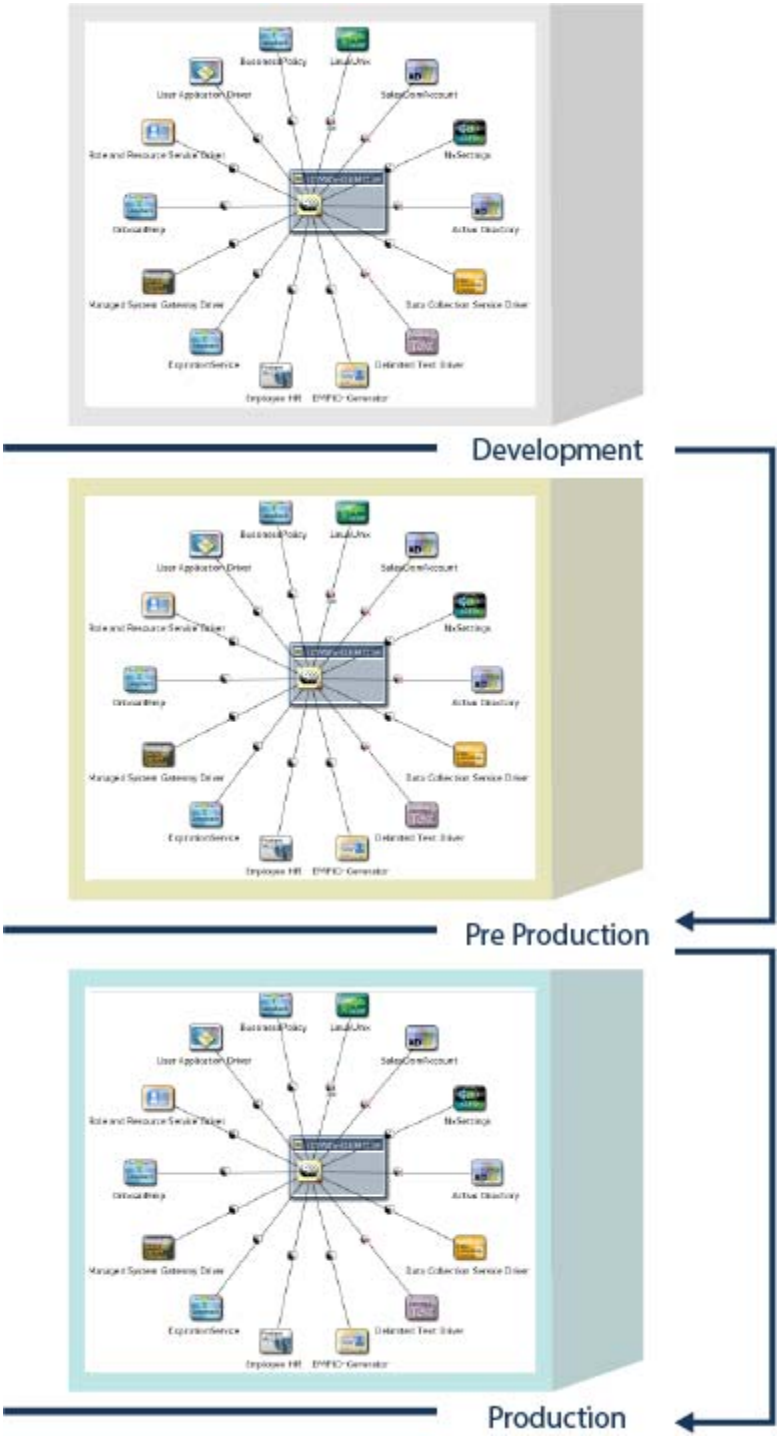
Key Features and Benefits of Architecture

The Identity Manager architecture is flexible and scalable, and provides the following features:

Staged Deployment

To avoid risk to your production Identity Manager environment, you can deploy Identity Manager in separate stages. For example, deploying to a development environment, then to a test environment, and finally to production. This process allows you to apply improvements and test changes in the project in each stage. Staging provides the flexibility to validate applications in real time to ensure no

data loss and uniformity across all stages. It helps you to reduce complexity in your deployment process because you can to test your Identity Manager project at multiple stages before the project is live.



The simplest, most efficient way to stage your Identity Manager project is by using the package management functionality in Designer. Packages are configured to keep server-specific settings separate from the actual Identity Manager content. You move all of your policies, rather than your server configurations, from one stage to the next.

Flexibility and Extensibility

You can deploy Identity Manager to single or multiple server instances, depending on the functionality that you need. Multiple server instances provide optimal configuration options by supporting geographically dispersed users and resources for increased flexibility, performance, and control.

You can install Identity Manager in a clustered environment for achieving high availability in some environments. Clustering is supported for Identity Manager engine and Identity Applications. components. For more information about high availability implementations, see the Setup Guide.

The architecture of NetIQ Identity Manager includes a built-in Identity Vault so you do not need to create and manage a separate directory structure for identity purposes. The Identity Vault is basically an eDirectory tree. It serves as a database that contains centralized identity and access information.

Depending on the extent of data that propagates from connected system into the Identity Vault, you can customize the Identity Vault. If you are installing your first Identity Manager system, use the default settings to help you quickly set up a system. For deploying Identity Manager in large enterprises, you can install individual components on different servers and customize the settings to suit your requirements.

Due to its object-oriented design and a distributed deployment support, Identity Vault is scalable to manage billions of objects. With its powerful schema management and granular data replication, it enables each application to reference a coherent set of identity values without needlessly replicating information across systems. As with all Identity Manager components, the Identity Vault can run in a wide range of operating environments. Additionally, its deployment as a central identity repository does not limit your ability to use other credential store technologies for other application or infrastructure uses.

Reuse of Existing Infrastructure

Identity Manager is built on an open architecture. This allows Identity Manager to integrate with the existing IT infrastructure and leverage existing software and already running applications of an organization. For example, if your Identity Manager implementation requires integrating with an existing company portal or a user management system, you can make use of standards-based APIs, such as REST, SOAP, SPML, JDBC, LDAP, and more. This allows you to customize the Identity Manager solution to meet the specific needs of the organization. You can also create connections to other applications with Google* Web Toolkit or Microsoft* Silverlight*. Using the APIs, Identity Manager can easily integrate various end-user activities such as password changes, password challenges, and role requests into existing environments, such as a company web portal.

For users to create, modify, and request permission for roles and resources, Identity Manager provides browser-based interfaces that they can access from workstations or mobile platforms. These interfaces support single sign-on access. Administrators, managers, and resource owners can carry out operational activities such as monitoring open workflows, workflow reassignment, and role and resource management.

Extensive Identity Integration

Identity Manager provides an identity integration framework that connects and synchronizes identity information across the organization environment.

The identity integration infrastructure enables administrators to create and modify identity information once and then have that data propagated to all their connected systems. For fast and low-cost deployments, Identity Manager provides this level of data synchronization through its unique and extensible integration architecture and preconfigured drivers. When the drivers are deployed, Identity Vault maintains driver configurations in a set of directory objects. For information about preconfigured drivers, see the Identity Manager Driver Documentation Website.

Identity Manager also enables you to define user organizational hierarchies and user groups with the use of its built-in hierarchy and inheritance, as well as native role-based access control. Administrators can easily and quickly use simple policies and access control lists to regulate information access, manage change authorization and enable self-service without heavy credentials.

Identity Manager also helps you to manage application parameters and entitlements, and to view a history of resource allocations. In addition, it provides delegated administration with permission settings for user management.

Identity Manager contains a web-based user self-service portal that can be customized. This portal helps you extensively in user management. It gives users and business administrators the ability to perform a variety of identity self-service and roles provisioning tasks, including managing passwords and identity data, initiating and monitoring provisioning and role assignment requests, managing the approval process for provisioning requests, and verifying attestation reports. It includes the workflow engine that controls the routing of requests through the appropriate approval process. For more information, see the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Built-in Audit and Compliance

The core identity management architecture includes auditing and compliance capabilities. When you bring a resource under identity management, the connection can be leveraged for both provisioning and compliance use, avoiding duplication of integration cost. Its integrated reporting provides the visibility into user entitlements and associated activities for compliance audits, with out-of-the-box support for regulations. The audit service can optionally integrate with NetIQ Sentinel for report analysis. For more information, see the *Administrator Guide to NetIQ Identity Reporting*.

4 Identity Manager Integration Solutions with Existing IT Infrastructure and Applications

Identity Manager provides out-of-the-box drivers for integrating with your existing IT infrastructure and applications in a fast and scalable manner. The business policies you implement using drivers can help to reduce management costs, increase productivity and security, and provide event reporting and auditing.

Out-of-Box Drivers

Identity Manager includes a broad set of pre-built drivers that provide provisioning integration with many popular applications, databases, operating systems, directories, SaaS, and other identity-aware systems that are widely used. Each driver supports a wide range of identity management functions.The SaaS drivers enable you to integrate your enterprise identities with cloud applications by providing capabilities such as provisioning, deprovisioning, request/approval processes, password changes, identity profile updates, and reporting. The drivers are designed specifically for a business application or a technology application and offers the quickest integration method. The drivers use the APIs that the applications provide to determine application data changes and effect application data changes. You can further modify the drivers to meet your unique requirements by using Designer. Depending on the load, network topology and network security requirements of your environment, one or more drivers may be deployed. The drivers can be co-located with the Identity Manager server or distributed on remote computers.

Identity Manager also integrates with custom-developed applications through common application protocol drivers such as JDBC, JMS, LDAP and SOAP. If you have a custom application, you can develop a custom driver to support provisioning to your application.

Identity Manager Driver Development Kit

To integrate Identity Manager with a home-grown application or a repository that has no technology interface and cannot leverage out-of-box drivers, Identity Manager provides the ability to develop a custom driver to enable data synchronization to a variety of other systems.

The sample policies that Identity Manager ships can be customized to provide the ability to automatically generate user provisioning actions in addition to simple synchronization of data items and reporting and auditing features. Developing a new driver heavily depends on the amount of customization needed in the sample policies that are shipped with Identity Manager. You can build a new driver from scratch.

Designer’s driver configuration template facilitates the development of custom drivers without coding or scripting. Identity Manager provides an SDK for developing Java-based custom drivers. This is the same SDK that Identity Manager uses to develop the out-of-the-box drivers.

SOAP and REST API Support for Identity Applications

Identity Applications provide several open integration points for connecting with external applications by calling a REST endpoint written specifically for each application. These are those applications that are within your enterprise but not connected to the Identity Vault.

5 Identity Manager Deployment Configurations

NetIQ Identity Manager enables you to retain control at the enterprise level by managing, provisioning, and deprovisioning identities within the firewall and extending to the cloud.

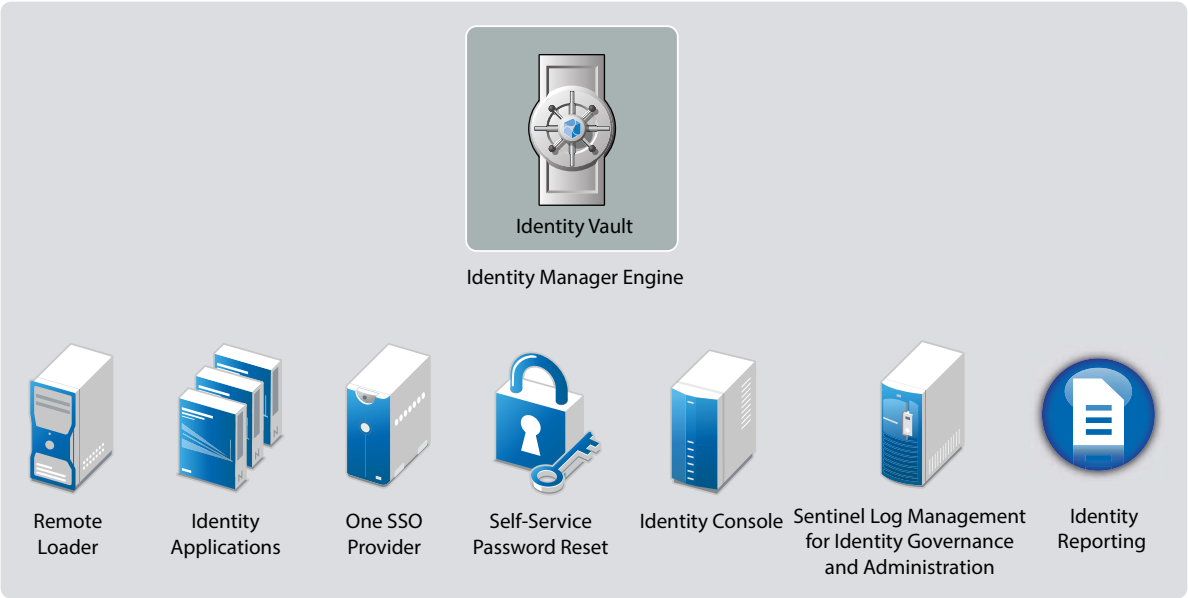
- Stores user account and organizational data in Identity Vault (LDAP directory)
- Runs in a Tomcat application server environment, either in a single-server or clustered configuration
- Stores historical and transactional data in a database server
- Provides administration from a client interface in a Web browser that communicates through an HTTPS server

Based on the functionality you need, select the Identity Manager components to install. There are different ways to install and configure Identity Manager to take advantage of all of its features. Before you install Identity Manager, you must determine how to configure Identity Manager engine, Remote Loader, and identity applications components in a single-server or a cluster configuration.

The following sections illustrate some high level implementation examples that you can use 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.

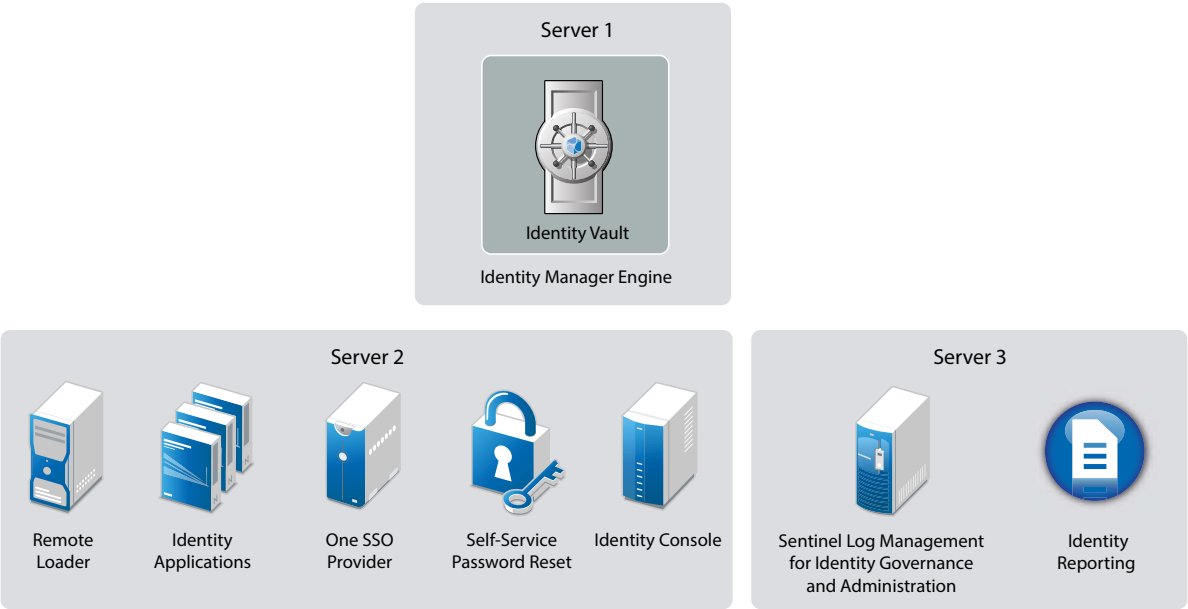
Basic Configuration

The most basic deployment configuration includes all Identity Manager components on one computer. You must ensure that the computer has the required memory, speed, and available disk space to meet the workload.



The all-in-one deployment is suitable only for installing Identity Management Proof-of-Concept (POC). Depending on the size and complexity of your environment, a single-server configuration might not be appropriate to implement a comprehensive identity management solution.

Optionally, you can install Identity Manager engine on one server and install all other required applications on one or more additional servers. The following figure illustrates this configuration:



In this configuration, components such as identity applications, Identity Console, OSP, and SSPR run on a separate server. 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. The server that has the Identity Applications requires Apache Tomcat Web application server, which includes the Tomcat embedded messaging server and client; and a JDBC driver. The JDBC driver enables Identity Applications to communicate with a database. Identity Manager supports JDBC driver types that connect to the supported databases.

High Availability Configuration

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:

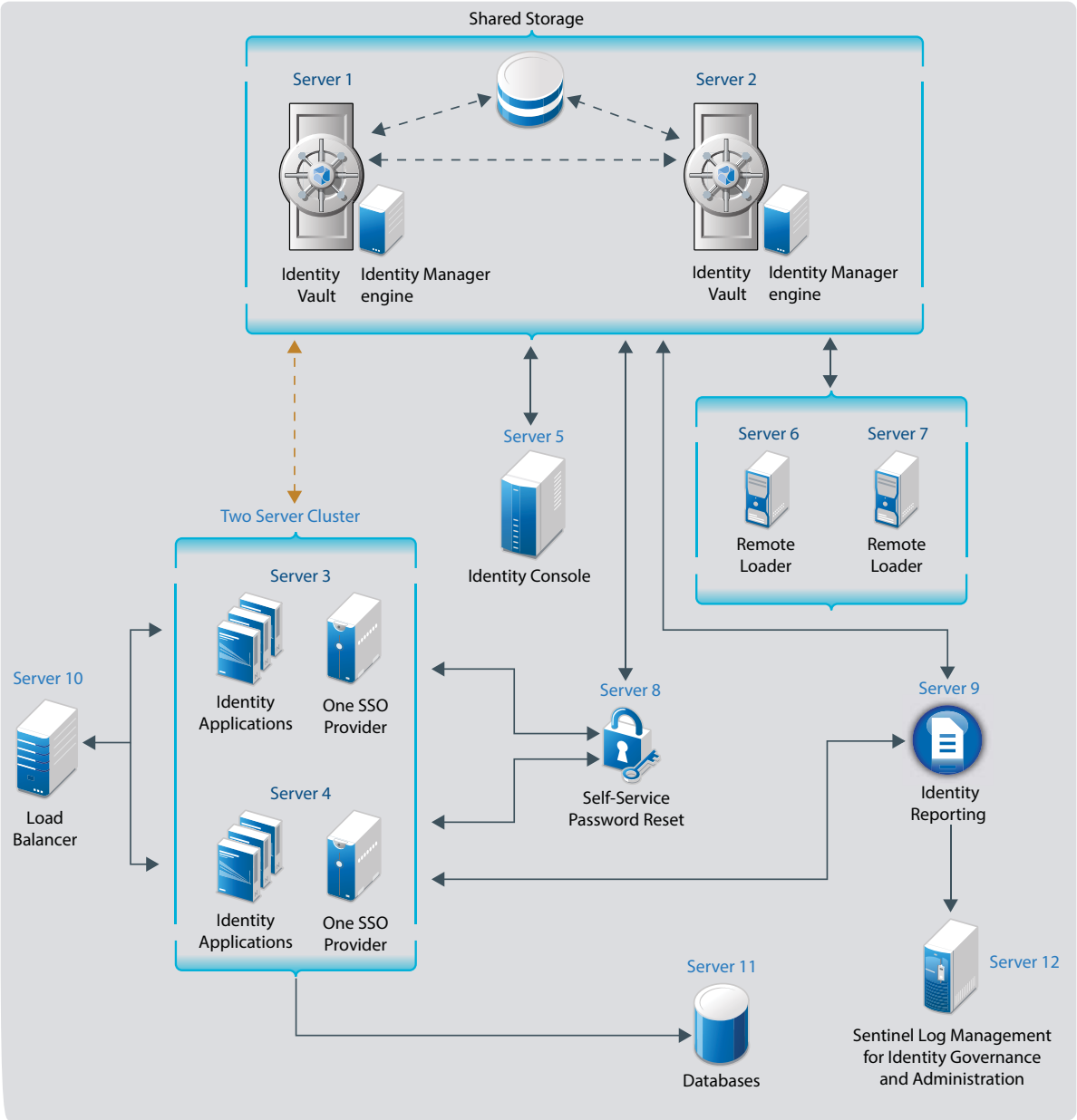
- Identity Vault
- Identity Manager engine
- Remote Loader
- Identity applications, except Identity Reporting

When you run Identity Vault in a clustered environment, the Identity Manager engine is also clustered. In this configuration, only one node is active at any point of time. If the active node fails, the service fails over to another node in the cluster.

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 balances 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.

For quick instructions about installing Identity Manager in the specified deployment scenarios, see *Quick Start Guide for Installing NetIQ Identity Manager 4.9*.

6 Understanding Identity Manager Localization

NetIQ translates (localizes) the interface for Identity Manager and its installation programs to support the operating system language on your local computers. However, we cannot support all languages. During installation, some installation programs check the locale of the computer to determine the language for the installation process.

To run the installation program in a specific language, change the locale through the **Regional Settings** option.

Translated Components and Installation Programs

The following table lists the available translations per component installation. Components not listed in the table are available in English only. If the component is not translated to the language of the operating system, the program defaults to English. Also, the End User License Agreement in the installation program might not be available in all supported languages.

Locale	Designer	Identity Manager Engine	Identity Console	Identity Applications*
Chinese Simplified	Yes	Yes	Yes	Yes
Chinese Traditional	Yes	Yes	Yes	Yes
Czech	–	–	–	Yes**
Danish	–	–	–	Yes
Dutch	Yes	–	–	Yes
English	Yes	Yes	Yes	Yes
French	Yes	Yes	Yes	Yes
German	Yes	Yes	Yes	Yes
Italian	Yes	–	Yes	Yes
Japanese	Yes	Yes	Yes	Yes
Norwegian	–	–	–	Yes**
Portuguese (Brazilian)	Yes	–	Yes	Yes
Russian	–	–	Yes	Yes
Spanish	Yes	–	Yes	Yes
Swedish	–	–	–	Yes
Hebrew	–	–	–	Yes**

Locale	Designer	Identity Manager Engine	Identity Console	Identity Applications*
Polish	–	–	Yes	Yes**

* Represents the Dashboard, Identity Applications Administration, Identity Reporting, Identity Approvals, and the User Application.

** Represents the end-user facing screens of Identity Applications.

Special Considerations for Language Support

NetIQ recommends that you review the following considerations when deciding whether to use a translated version of Identity Manager.

- In general, if an Identity Manager component does not support the language of the operating system, the component's interface defaults to English. For example, the Identity Manager drivers are available in the same languages as the Identity Manager Engine. When Identity Manager does not support the driver language, the driver configuration defaults to English.
- When you launch the installation program for an Identity Manager component, the following conditions apply:
  - If the operating system is in a language supported by the installation program, the program defaults to that language. However, you can specify a different language for the installation process.
  - If the installation program does not support the language of the operating system, the installation program defaults to English.
  - If the operating system uses a Latin-based language, the installation program allows you to specify any of the Latin-based languages.
  - If the operating system uses a supported Asian-based language or Russian, the installation program allows you to specify only the language matching the operating system or English.

7 Where to Get Identity Manager

NetIQ provides ISO files that contain all components for a full Identity Manager installation. Each file includes the versions of the product. The name of the ISO file identifies the platform. For example, `Identity_Manager_version_Linux.iso`. For information about the features available in Identity Manager Advanced and Standard Editions, see Chapter 2, "Identity Manager Editions," on page 19.

You can download an evaluation copy of Identity Manager and use it for 90 days free of charge. However, the Identity Manager components must be activated within 90 days of installation, or they will shut down. At any time during the 90 days, or afterward, you can choose to purchase a product license and activate Identity Manager. For more information, see Chapter 8, "Understanding Licensing and Activation," on page 43.

To download Identity Manager and its services:

1. Go to the Software License and Download portal (https://sld.microfocus.com).
2. In the **Product or Technology** menu, select **Identity Manager**, then click **Search**.
3. On the NetIQ Identity Manager Downloads page, click the **Download** button next to a file you want.

File Name	Description
`Identity_Manager_4.9_Linux.iso`	Contains Identity Manager Server (Identity Manager Engine, Remote Loader, Fan-Out Agent, Identity Console), Identity Applications, and Identity Reporting.
`Identity_Manager_4.9_RL_Linux.iso`	Contains the Identity Manager Remote Loader for Linux
`Identity_Manager_4.9_Containers.tar.gz`	Contains individual container images for Identity Manager Engine, Remote Loader, Fanout Agent, ActiveMQ, PostgreSQL, Form Renderer, OSP, Identity Applications, Identity Reporting, SSPR and Identity Console (for SLES platforms)
`Identity_Manager_4.9_Windows.iso`	Contains Identity Manager Server (Identity Manager Engine, Remote Loader, Fan-Out Agent, Identity Console), Identity Applications, and Identity Reporting.
`Identity_Manager_4.9_RL_Windows.iso`	Contains the Identity Manager Remote Loader for Windows
`Identity_Manager_4.9_Designer_Linux.tar.gz`	Contains Designer for Linux platforms
`Identity_Manager_4.9_Designer_Windows.zip`	Contains Designer for Windows platforms
`Identity_Manager_4.9_Designer_MacOSX.dmg`	Contains Designer files for macOS Sonoma

File Name	Description
`SentinelLogManagementForIGA8.6.1.0.tar.gz`	Contains Sentinel Log Management for Identity Governance and Administration (IGA) This installation is supported only on Linux.

To switch from Identity Manager Advanced Edition to Standard Edition, uninstall the Advanced Edition and then install the Standard Edition ISO from the Identity Manager media. To upgrade from Standard Edition to Advanced Edition, use the Identity Manager Advanced Edition ISO. You need to apply the correct activation to be able to upgrade to Advanced Edition. For more information about upgrading from Standard Edition to Advanced Edition, see Upgrading Identity Manager in the *NetIQ Identity Manager Install and Upgrade Guide for Linux* or Upgrading Identity Manager on the *NetIQ Identity Manager Install and Upgrade Guide for Windows*.

4 Follow the on-screen prompts to download the file to a directory on your computer.

5 Repeat Step 3 until you have downloaded all of the files you need.

6 Either mount the downloaded file as a volume, or use the file to create a DVD of the software.

NOTE: The ISO images are large files. Ensure that you download them to a volume or DVD that supports the file size.

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

- **Service Drivers:** The following is a list of service drivers that are activated when you active the Identity Manager server:
  - Data Collection Service
  - Entitlements Services
  - ID Provider
  - Loopback Service
  - Managed System Gateway
  - Manual Task Service
  - Null Service
  - Role and Resource Service
  - User Application
  - WorkOrder
- **Common Drivers:** The following is a list of common drivers that are activated when you active the Identity Manager server:
  - Active Directory
  - 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 you purchase. For more information, see NetIQ Identity Manager Technical Information website (https://www.microfocus.com/en-us/products/netiq-identity-manager/specs).

Identity Manager Advanced and Standard Editions have separate activations. For more information, refer to "Understanding Licensing and Activation" on page 43. Switching from Identity Manager Advanced Edition to Standard Edition is not supported. To use the Identity Manager Standard Edition, you need to install it from the Identity Manager media.

Identity Applications components are included with your Identity Manager purchase. Identity Applications add a powerful roles based approval workflow to managing your users' identities.

Your Identity Manager purchase also includes the several tools to help design, create, and manage your Identity Manager solution:

- Designer
- Identity Console
- Analyzer

Identity Reporting components allow you to audit and create reports about your Identity Manager solution. You can use the reports to help meet compliance regulations for your business.

For more information about the Identity Manager components, see "How Identity Manager Works" on page 22.

8 Understanding Licensing and Activation

Identity Manager comprises of a broad spectrum of functionality. In order to meet different customer needs, Identity Manager functionality is delivered in Advanced and Standard Editions. Identity Manager includes the complete set of functionality in Advanced Edition. Standard Edition includes a subset of the features provided in Advanced Edition. For a comparison of features available in Advanced and Standard Editions, see Identity Manager Version Comparison. NetIQ provides different licensing models for each edition.

NetIQ delivers both editions in a single ISO file to improve its delivery of new features, patches, documentation, and support, while allowing customers to select the solution capabilities that best match their needs.

You can install an evaluation copy of Identity Manager and use it for 90 days free of charge. However, you must activate the Identity Manager components within 90 days of installation, or they will stop functioning. You can purchase a product license and activate Identity Manager either during the evaluation period of 90 days or later. For more information, "Activating Identity Manager" on page 43.

Depending on which edition you purchase, NetIQ will provide you with the appropriate license keys to enable the right functionality within Identity Manager. To purchase an Identity Manager product license, see the NetIQ Identity Manager How to Buy website (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.

Activating Identity Manager

Some Identity Manager components activate automatically the first time that you log in. Other components require a procedure for activation.

- "Installing a Product Activation Credential" on page 43
- "Reviewing Product Activations for Identity Manager and Drivers" on page 44
- "Activating Identity Manager Drivers" on page 45
- "Activating Specific Identity Manager Components" on page 45

Installing a Product Activation Credential

NetIQ recommends that you use Identity Console to install the Product Activation Credential.

NOTE: For each driver that you want to use, activate the driver set that has a driver. You can activate any tree with the credential.

1. After you purchase a license, NetIQ sends you an e-mail with your Customer ID. The e-mail also 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 then complete one of the following actions:
   - Open the Product Activation Credential file, then copy the contents of the Product Activation Credential to your clipboard.
   - Save the Product Activation Credential file.
   - If you chose to copy the contents, do not include any extra lines or spaces. 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. Log in to Identity Console.
4. Select **Identity Manager > Identity Manager Overview**.
5. To select a driver set in the tree structure, click the browse icon ( ).
6. On the **Identity Manager Overview** page, click the driver set that contains the driver that you want 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, and then click **Next**.
9. (Conditional) If you saved the Product Activation Credential file, specify the saved location.
10. (Conditional) If you copied the contents of the Product Activation Credential file, paste the contents into the text area.
11. Click **Next**.
12. Click **Finish**.

    NOTE: Identity Manager does not show the correct Identity Manager Edition after applying the Bundle Edition activation.

Reviewing Product Activations for Identity Manager and Drivers

For each of your driver sets, you can view the Product Activation Credentials you have installed for the Identity Manager engine server and Identity Manager drivers. You can also 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. The message should disappear.

1. Log in to Identity Console.
2. Click **Identity Manager** > **Identity Manager Overview.**
3. To select a driver set in the tree structure, use the browse icon ( ) and the search icon ( ).

4 On the **Identity Manager Overview** page, click the driver set for which you want to review 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.

Activating Identity Manager Drivers

When you activate the Identity Manager engine, you also activate the following drivers:

Service Drivers	Common Drivers
Data Collection Service	Active Directory
ID Provider	Bidirectional Driver for eDirectory
Managed System Gateway	eDirectory
Role and Resource Service	GroupWise 2014
User Application	LDAP
	Lotus Notes

To activate other Identity Manager drivers, you must purchase additional Identity Manager Integration modules, which might contain one or more drivers. You receive a Product Activation Credential for each Identity Manager Integration module that you purchase. After receiving the credential, perform the procedure listed in "Installing a Product Activation Credential" on page 43. For more information about the drivers, see the Identity Manager Drivers documentation website.

Activating Specific Identity Manager Components

This section provides information about activating specific components for Identity Manager.

- "Activating Designer" on page 45
- "Activating Analyzer" on page 45
- "Activating Sentinel Log Management for IGA" on page 46

Activating Designer

When you activate the Identity Manager engine or the Identity Manager drivers, you also activate Designer.

Activating Analyzer

When you launch the Analyzer perspective without a license, Analyzer opens the activation page, from which you can manage Analyzer licenses.

NOTE: If you close the Activation dialog box, Analyzer remains locked until you provide a license to activate it. When you are ready to add a license, click **Activate Analyzer** in the `Project View` to open the Activation dialog box.

1. Launch Analyzer.
2. In the **Analyzer Activation** window, you can Add a new license or Access customer center for license.
3. (Conditional) To add a new license:
   - **3a** Click **Add a new license**.
   - **3b** In the **License** window, type the activation code that you downloaded from the NetIQ Customer Care Portal, and then click **OK**.
4. (Conditional) To access customer center for license:
   - **4a** Click **Access Customer Center for license**.
   - **4b** Click **Visit the Micro Focus Customer Center**.
   - **4c** Browse to and select the Analyzer license.
   - **4d** Copy the activation code and then close the Customer Care Portal.
   - **4e** In the **License** window, type the activation code and then click **OK**.
5. In the **Analyzer Activation** window, review the details of the license that you just installed.
6. Click **OK** to begin using Analyzer.

Activating Sentinel Log Management for IGA

You can add a license key when installing Sentinel. This section provides information about adding the license key after the Sentinel installation.

If you are using an evaluation license key that is installed by default, you must activate Sentinel before the evaluation key expires to avoid any interruption in the Sentinel functionality. For information about how to purchase the license, see the Identity Manager Product Website.

You can add a license key either by using the Sentinel Main interface or through the command line.

- "Adding a License Key By Using the Sentinel Main Interface" on page 46
- "Adding a License Key through the Command Line" on page 47

Adding a License Key By Using the Sentinel Main Interface

1. Log in to the Sentinel Main interface as an administrator.
2. Click **About** > **Licenses**.
3. In the Licenses section, click **Add License**.
4. Specify the license key in the **Key** field.

   After you specify the license, the following information is displayed in the Preview section:
   - **Features:** The features that are available with the license.
   - **Hostname:** This field is for internal NetIQ use only.
   - **Serial:** This field is for internal NetIQ use only.

- **EPS:** Event rate built into the license key. Beyond this rate, Sentinel generates warnings but will continue to collect data.
- **Expires:** Expiry date of the license. You must specify a valid license key before the expiry date to prevent an interruption in functionality.

5 Click **Save**.

Adding a License Key through the Command Line

If you are using the Sentinel traditional installation, you can add the license through the command line by using the `softwarekey.sh` script.

1 Log in to the Sentinel server as root.

2 Change to the `/opt/novell/sentinel/bin` directory.

3 Enter the following command to change to the novell user:

```
su novell
```

4 Specify the following command to run the `softwarekey.sh` script.

```
./softwarekey.sh
```

5 Enter **1** to insert the license key.

6 Specify the license key, then press **Enter**.

II Planning

Identity Manager helps you manage the identities and resources in your business. It also automates many business processes for you that are currently manual tasks.

If you have any questions about the different components that make up an Identity Manager solution, see Overview for more information about each component.

To create an effective Identity Manager solution for your environment, you first must take time to plan and design the solution. There are two major aspects to planning: setting up a test lab to become familiar with the products and creating a project plan to implement an Identity Manager solution. When you create a project plan, you define your business process and create an implementation plan. Most companies have many different business processes that are managed by many different people. A complete Identity Manager solution affects most of these processes. It is extremely important to take the time to plan an Identity Manager solution, so that it can be effectively implemented in your environment.

- Chapter 9, “Creating a Project Plan,” on page 51
- Chapter 10, “Setting Up a Development Environment,” on page 63
- Chapter 11, “Technical Guidelines,” on page 65

9 Creating a Project Plan

This planning material provides an overview of the activities that are usually part of an Identity Manager project, from its inception to its full production deployment. Implementing an identity management strategy requires you to discover what all of your current business processes are, what are the needs for these processes, who the stakeholders are in your environment, and then design a solution, get buy-in from stakeholders, and test and roll out the solution. This section is intended to provide you with sufficient understanding of the process so that you can maximize the benefit from working with Identity Manager.

This section is not exhaustive; it is not intended to address all possible configurations, nor is it intended to be rigid in its execution. Each environment is different and requires flexibility in the type of activities to be used.

- "Discovery Phase" on page 51
- "Requirements and Design Analysis Phase" on page 55
- "Proof of Concept" on page 60
- "Data Validation and Preparation" on page 60
- "Quality Assurance" on page 61
- "Production Roll-out Planning" on page 61
- "Production Deployment" on page 62

Discovery Phase

The Identity Manager solution affects many aspects of your business. In order to create an effective solution, you must take time to discover all relevant business processes for the planned Identity Management solution, then identify how an implementation of Identity Manager reflects/adapts these processes, who these changes affect, and how the changes are implemented.

The discovery phase provides a common understanding of the issues and solutions for all stakeholders. It creates a plan or road map that contains the key business and systems information that are affected by the Identity Manager solution. It also allows all stakeholders to participate in the creation of the Identity Manager solution so they understand how it can affect their area of the business.

The following list indicates the steps needed to have a successful discovery phase. There might be additional items you find that you need to add to the list as you proceed through the discovery and design phases.

- "Discovering Current Business Processes" on page 52
- "Defining How the Identity Manager Solution Affects the Current Business Processes" on page 54
- "Identifying the Key Business and Technical Stakeholders" on page 54

- "Interviewing All Stakeholders" on page 54
- "Creating a High-level Strategy and an Agreed Execution Path" on page 55

Discovering Current Business Processes

Identity Manager automates business processes to easily manage identities in your environment. For example, your company might have the following business processes:

- Hire a new employee
- Organizational change for an existing employee
- Change of the manager of an organizational unit
- Start of temporary absence of an employee
- Return from temporary absence of an employee
- Retirement of an employee
- Change in the contract
- Movement between company subsidiaries
- Termination of an employee
- Change of an employee's name
- Change of an employee's telephone number

All these business processes do have their source application/system, influence multiple target systems and can involve approval workflows. If you do not know what the current business processes are, you cannot design an Identity Manager solution that automates those processes. Business processes are governed by business rules. Business rules represent specific directives that constrain or define a business activity. Business rules are designed to help an organization achieve its goals. For example, your company might identify the following business rules:

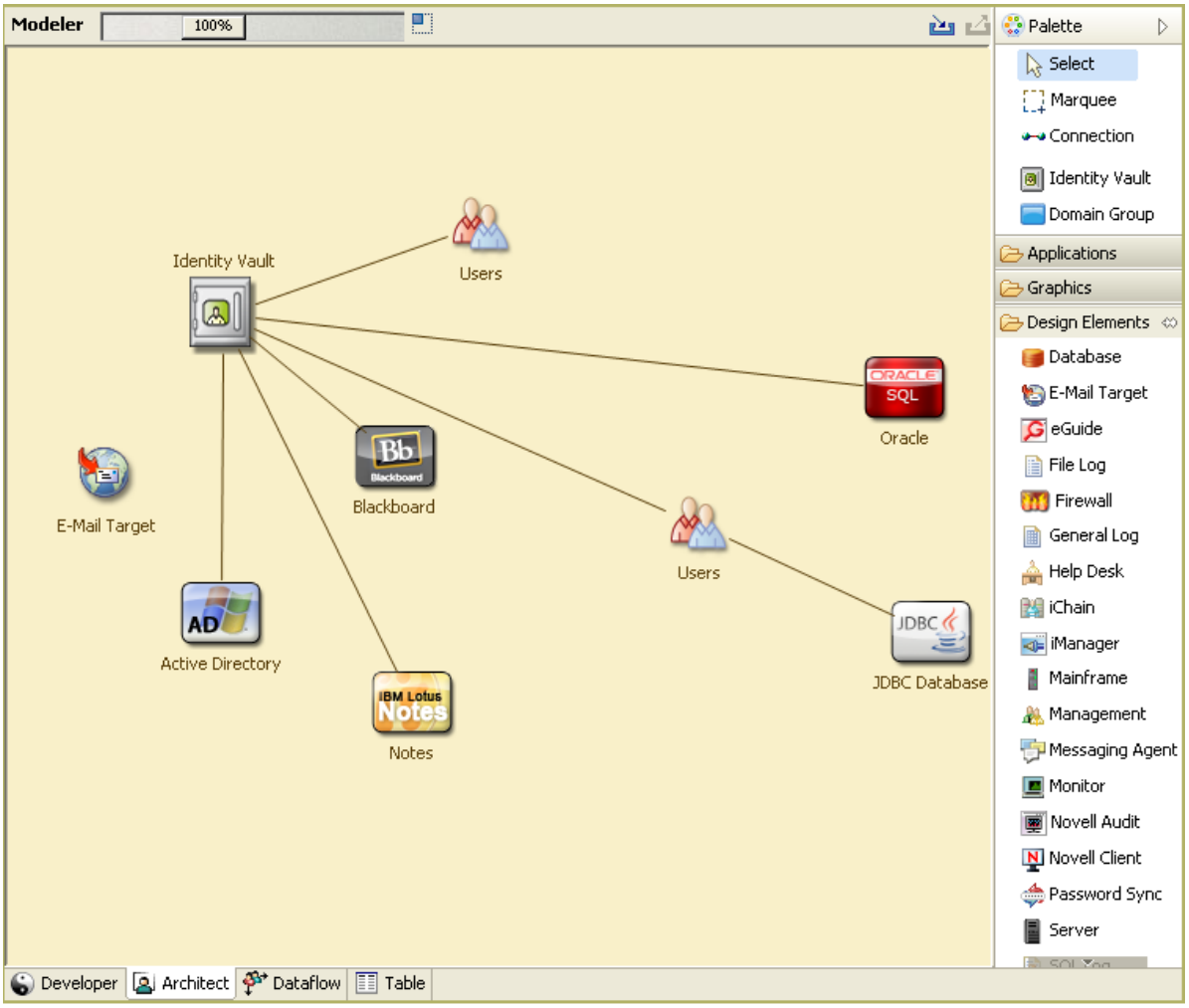
- When an employee is terminated, the user account in the e-mail system is deleted, but the user's account in all other systems is disabled, not deleted.
- The format for a user's e-mail address.
- The systems or resources that sales employees can access.
- The systems or resources that managers can access.
- What systems generate new accounts? Is it the human resource system or is it through a workflow request?
- A password policy for the company that defines how often a password changes, how complex the password is, and which systems are synchronizing the password.

As you define your business processes, use the following list of items to help you understand all of the processes:

- Define or clarify the current business issues.
- Determine what initiatives are required to address these issues.
- Determine which services and systems are affected by these initiatives.

This step allows you to create a high-level overview of what your business is currently doing and what processes need to be involved. For example, Figure 9-1 uses Designer to show the data flow for new user accounts that are generated from the HR application employee records. They are synchronized into the Identity Vault and then synchronized into Lotus Notes and Active Directory. Passwords are being synchronized between Active Directory and the Identity Vault. Accounts are synchronizing into the Notes system, but no accounts are synchronizing back to the Identity Vault.

Figure 9-1 *Example of Business Processes*



After you determine processes, you start to identify how Identity Manager can be involved. Continue with "Defining How the Identity Manager Solution Affects the Current Business Processes" on page 54.

Defining How the Identity Manager Solution Affects the Current Business Processes

After you have defined your current business processes, you need to decide how these processes can be incorporated into an Identity Manager solution.

It is best to look at the entire solution and then prioritize which processes should be implemented. Identity Manager encompasses so many aspects of your business, it is easier to plan the entire solution rather than approach each business process as its own solution.

Create a list of which business processes are a priority to automate, then identify which systems these changes will affect. Then continue with "Identifying the Key Business and Technical Stakeholders" on page 54.

Identifying the Key Business and Technical Stakeholders

Identifying all stakeholders involved in the Identity Manager solution is important for the success of the solution. In most companies, there is not just one person you can contact who understands all business and technical aspects of the business processes. You must identify which services and systems are going to be affected by the Identity Manager solution, and you must also identify the person who is responsible for that service or system.

For example, if you are integrating an e-mail system into your solution, you would need to list what the e-mail system is, who the e-mail system administrator is, and what the contact information is. You can add all of this information into the Designer project. Each application icon has a place where you can store information about the system and the system administrator. For more information, see "Configuring Application Properties" in the *NetIQ Designer for Identity Manager Administration Guide*.

After you have identified all of the people involved in each business process, the next step is in "Interviewing All Stakeholders" on page 54.

Interviewing All Stakeholders

Interviews with key business and technical stakeholders allow you to gather information needed for a complete design of the Identity Manager solution. The interviews also allow you to educate each stakeholder about the Identity Manager solution and how the solution affects them. Here is a list of items to cover when you do the interviews:

- Define or clarify the business processes being addressed by the Identity Manager solution. The person you are interviewing might have information that can change the current plan.
- Determine how the solution will impact the stakeholders and address any concerns they have. Also ask the stakeholders how much time their part of the solution might take. They might or might not have an estimate, but gathering this information helps to determine the scope of the solution.
- Capture key business and systems information from the stakeholders. Sometimes a proposed plan might adversely affect a business process or a system. By capturing this information, you can make educated decisions about the Identity Manager solution.

After you have interviewed the key stakeholders, the next step is in "Creating a High-level Strategy and an Agreed Execution Path" on page 55.

Creating a High-level Strategy and an Agreed Execution Path

After all of the information is gathered, you need to create a high-level strategy or road map for the Identity Manager solution. Add all of the features you want to be included in the Identity Manager solution. For example, new user accounts are generated from a request through a workflow, but the type of user depends upon the resources the user is given access to.

Present this high-level strategy to all of the stakeholders in the same meeting, if possible. This allows you to accomplish several things:

- Verify that the included initiatives are the most correct and identify which ones have the highest priority.
- Identify planning activities in preparation for a requirements and design phase
- Determine what it would take to carry out one or more of these initiatives.
- Create an agreed execution path for the Identity Manager solution.
- Define additional education for stakeholders.

Discovery provides a common understanding of the issues and solutions for all stakeholders. It provides an excellent primer for the analysis phase, which is a phase that requires stakeholders to have a basic knowledge of directories, NetIQ eDirectory, NetIQ Identity Manager, and XML integration in general.

After you have completed the discovery phase, proceed to "Requirements and Design Analysis Phase" on page 55.

Requirements and Design Analysis Phase

Take the high-level road map that was created in the discovery phase as a starting point for this analysis phase. The document and the Designer project both need technical and business details added. This produces the data model and high-level Identity Manager architecture design used to implement the Identity Manager solution.

The focus of the design should be specifically on identity management; however, many of the elements traditionally associated with a resource management directory, can also be addressed. Identity Manager synchronizes user accounts to directories that do not have direct access to the operating system's file system. For example, you can have a user account in Active Directory, but that does not grant you access to the file system on the Active Directory server.

Using the information gathered in the discovery phase, answer the following sample questions to see what other information needs to be gathered. This might require additional interviews with stakeholders.

- How is the business process flow provided by the Identity Management solution?
- Which process can be automated and which cannot be?
- Which Identity Manager components need to be involved?
- Do all connected applications have the appropriate data?
- How can data migration take place?

- What is needed for cleansing the data before integrating the applications?

  Identity Manager contains a tool to help you simplify the process of analyzing and cleaning your data. For more information, see *NetIQ Analyzer for Identity Manager Administration Guide (https://www.netiq.com/documentation/identity-manager-48/analyzer_admin/data/netiq-identity-manager-analyzer-admin.html)*.

Review the information in Chapter 11, "Technical Guidelines," on page 65 to help make the correct decisions for your environment.

After the requirements analysis, you can establish the scope and project plan for the implementation, and determine if any prerequisite activities need to occur. To avoid costly mistakes, be as complete as possible in gathering information and documenting requirements. Here is a list of possible requirements:

- Data model showing all systems, authoritative data sources, events, information flow, data format standards, and mapping relationships between connected systems and attributes within Identity Manager.
- Appropriate Identity Manager architecture for the solution.
- Details for additional system connection requirements.
- Strategies for data validation and record matching.
- Directory design to support the Identity Manager infrastructure.

The following tasks should be completed during the requirements and design assessment:

- "Defining the Business Requirements" on page 56
- "Analyzing Your Business Processes" on page 57
- "Designing an Enterprise Data Model" on page 58

Defining the Business Requirements

In the discovery phase, you gathered your organization's business processes and the business requirements that define these business processes. Create a list of these business requirements and then start mapping these processes in Designer by completing the following tasks:

- Create a list of the business requirements and determine which systems are affected by this process. For example, a business requirement for terminating an employee might be that the employee's network and e-mail account access must be removed the same day the employee is terminated. The e-mail system and the Identity Vault are affected by this termination process.
- Establish the process flows, process triggers, and data mapping relationships.

  For example, if something is going to happen in a certain process, what other processes are triggered?
- Map data flows between applications. Designer allows you to see this information. For more information, see "Managing the Flow of Data" in the *NetIQ Designer for Identity Manager Administration Guide*.
- Identify data transformations that need to take place from one format to another, such as 2/25/2017 to 25 Feb 2017, and use Analyzer to change the data. For more information, see the *NetIQ Analyzer for Identity Manager Administration Guide (https://www.netiq.com/documentation/identity-manager-48/analyzer_admin/data/netiq-identity-manager-analyzer-admin.html)*.

- Document the data dependencies that exist.

  If a certain value is changed, it is important to know if there is a dependency on that value. If a particular process is changed, it is important to know if there is a dependency on that process.

  For example, selecting a “temporary” employee status value in a human resources system might mean that the IT department needs to create a user object in Identity Vault with restricted rights and access to the network during certain hours.

- List the priorities.

  Not every requirement, wish, or desire of every party can be immediately fulfilled. Priorities for designing and deploying the provisioning system will help plan a road map.

  It might be advantageous to divide the deployment into phases that enable implementation of a portion of the deployment earlier and other portions of the deployment later, or use a phased deployment that is based on groups of people within the organization.

- Define the prerequisites.

  The prerequisites required for implementing a particular phase of the deployment should be documented. This includes access to the connected systems that need to interface with Identity Manager.

- Identify authoritative data sources.

  Learning early on which items of information that system administrators and managers feel belong to them can help in obtaining and keeping buy-in from all parties.

  For example, the account administrator might want ownership over granting rights to specific files and directories for an employee. This can be accommodated by implementing local trustee assignments in the account system.

After you have defined your business requirements, proceed to “Analyzing Your Business Processes” on page 57.

Analyzing Your Business Processes

After you complete the analysis of your business requirements, there is more information you need to gather to help focus the Identity Manager solution. You need to interview essential individuals such as managers, administrators, and employees who actually use the application or system. Issues to be addressed include:

- Where does the data originate?
- Where does the data go?
- Who is responsible for the data?
- Who has ownership for the business function to which the data belongs?
- Who needs to be contacted to change the data?
- What are all the implications of the data being changed?
- What work practices exist for data handling (gathering and/or editing)?
- What types of operations take place?
- What methods are used to ensure data quality and integrity?
- Where do the systems reside (on what servers, in which departments)?
- What processes are not suitable for automated handling?

For example, you could use the following questions for an administrator for a SAP system in Human Resources:

- What data are stored in the SAP database?
- What appears in the various panels for an employee account?
- What actions must be reflected across the provisioning system (such as add, modify, or delete)?
- Which of these are required? Which are optional?
- What actions need to be triggered based on actions taken in SAP?
- What operations/events/actions are to be ignored?
- How is the data to be transformed and mapped to Identity Manager?

Interviewing key people can lead to other areas of the organization that can provide a more clear picture of the entire process.

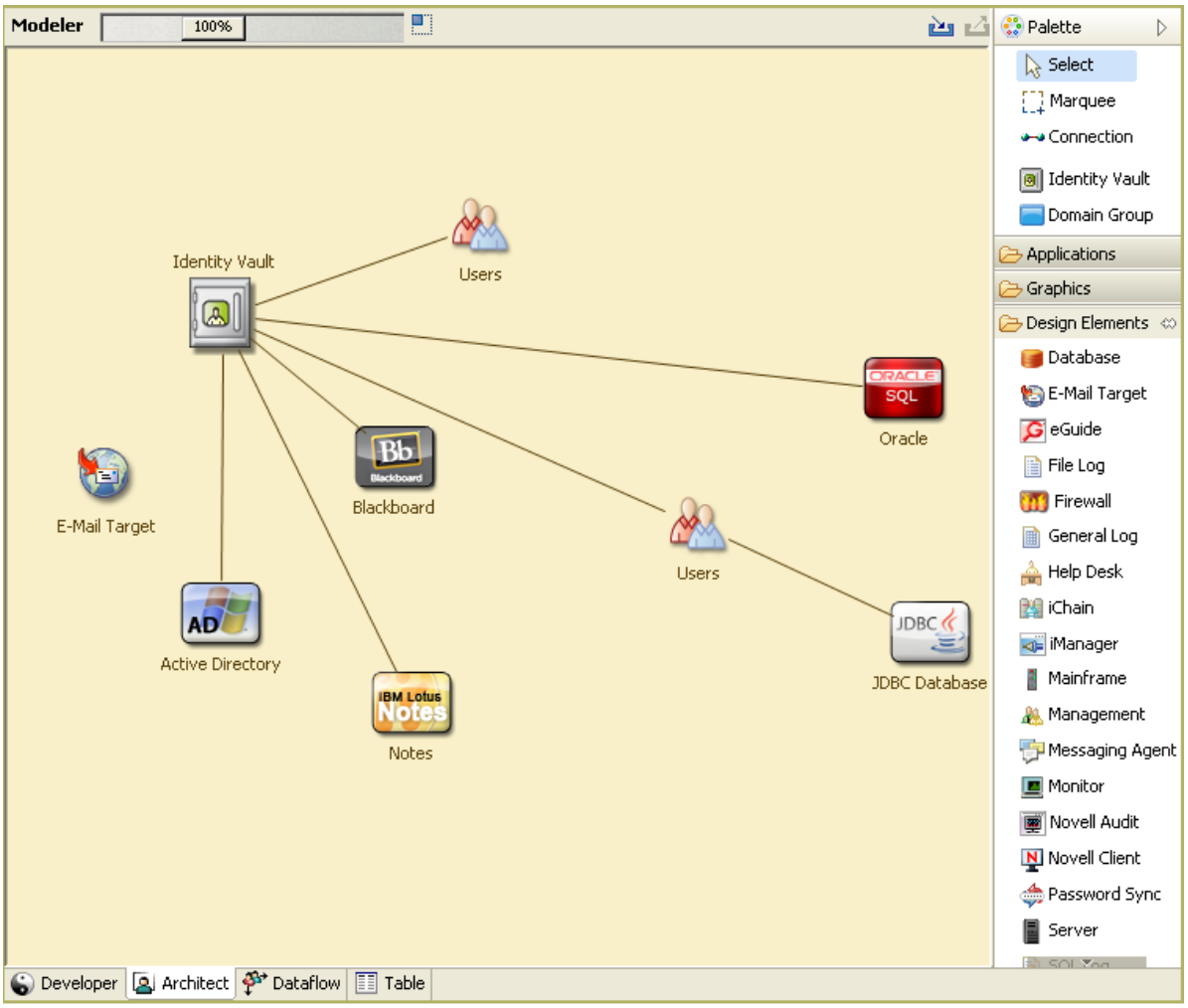
After you have gathered all of this information, you can design a correct enterprise data model for your environment. Proceed to "Designing an Enterprise Data Model" on page 58 to start the design.

Designing an Enterprise Data Model

After your business processes have been defined, you can use Designer to design a data flow model as an technical outcome of the business process discovery.

The model in Designer illustrates where data originates, where it moves to, and where it can't move. It can also account for how critical events affect the data flow. For example, Figure 9-2 shows data flow between Identity Vault and different connected systems.

Figure 9-2 Data Flow through Designer



You might also want to develop a diagram that illustrates the proposed business process and the advantages of implementing automated provisioning in that process.

The development of this model begins by answering questions such as the following:

- What types of objects (users, groups, etc.) are being moved?
- Which events are of interest?
- Which attributes need to be synchronized?
- What data is stored throughout your business for the various types of objects being managed?
- Is the synchronization one-way or two-way?
- Which system is the authoritative source for which attributes?

It is also important to consider the interrelationships of different values between systems.

For example, an employee status field in SAP might have three set values: employee, contractor, and intern. However, the Active Directory system might have only two values: permanent and temporary. In this situation, the relationship between the “contractor” status in SAP and the “permanent” and “temporary” values in Active Directory needs to be determined.

The focus of this work should be to understand each connected system/application, how they relate to each other, and what objects and attributes need to be synchronized across the systems. After the design is complete, the next step is to create a proof of concept. Proceed to "Proof of Concept" on page 60.

Proof of Concept

You create and test your proof of concept by using a sample implementation in a lab environment in order to reflect your company's business policy and data flow. The implementation is based on the design of the data model developed during the requirement analysis and design and is a final step before the production pilot. You perform the tests in the lab you created in Chapter 10, "Setting Up a Development Environment," on page 63.

NOTE: This step is often beneficial in gaining management support and funding for a final implementation effort.

Chapter 11, "Technical Guidelines," on page 65 contains information that can help you validate your proof of concept. It contains technical guidelines to help make your Identity Manager deployment successful.

As you create the proof of concept, you need to also create a plan to validate the data that you have in your systems. This step helps you make sure that conflicts don't occur between systems. Proceed to "Data Validation and Preparation" on page 60 to make sure these conflicts do not occur.

Data Validation and Preparation

The data in production systems can be of varying quality and consistency and therefore might introduce inconsistencies when synchronizing systems. This phase presents an obvious point of separation between the resources implementation team and the business units or groups who "own" or manage the data in the systems to be integrated. At times, the associated risk and cost factors might not belong in a provisioning project.

You need to use the data model that you completed in the analysis and design phases. You should also have a possible record matching and data format strategy in order to prepare the data correctly. With the data model and format strategy defined, you can complete two important steps:

- Create production data sets appropriate for loading into the Identity Vault (as identified in the analysis and design activities). This includes the probable method of loading (either bulk load or via connectors). The requirement for data that is validated or otherwise formatted is also identified.
- Identify performance factors and validate these factors against equipment being used and the overall distributed architecture of the deployment of Identity Manager.

After the data is prepared, proceed to "Quality Assurance" on page 61.

Quality Assurance

The production pilot is the first step in migrating into a production environment. During this phase, there might be additional customization that occurs. In this limited introduction, the desired outcomes of the preceding activities can be confirmed and agreement obtained for the production rollout. The pilot validates the plan that has been created to this point in the process.

NOTE: This phase can provide the acceptance criteria for the solution and the necessary milestone en route to full production.

The pilot solution provides live proof of concept and validation for the data model and desired process outcomes. After the pilot is completed, proceed to "Production Roll-out Planning" on page 61.

Production Roll-out Planning

This phase is where the production deployment is planned. The plan should do several things:

- Confirm the desired outcomes of the preceding activities and agreement is obtained for the production roll-out
- Confirm server platforms, software revisions, and service packs
- Confirm the general environment
- Confirm the design of the Identity Vault in a mixed coexistence
- Confirm that the business logic is correct
- Confirm that the data synchronization is occurring as planned
- Plan the legacy process cut-over
- Plan a rollback contingency strategy

Quality assurance is the first step in migrating into a production environment. During this phase, there might be additional customization that occurs. The desired outcomes of the preceding activities are confirmed and agreement is obtained for the production roll-out. This step provides live proof of concept and validation for the data model and desired process outcomes of the plan that has been created to this point in the process.

NOTE: This phase can provide the acceptance criteria for the solution and the necessary milestone en route to full production.

After the quality assurance step, proceed to the production deployment.

The deployment plan needs to contain implementation and completion dates for each step in the roll-out. Each stakeholder provides input for these dates and agrees that these dates work for them. This allows each person involved in the roll-out to know when the changes are coming and when they should be completed.

With the production rollout plan completed, proceed to the "Production Deployment" on page 62.

Production Deployment

The production deployment phase puts all of the plans into action so that the Identity Manager solution is created in the live environment. Use the production roll-out plan to put the different pieces of the Identity Manager solution into place. Depending on the complexity of the plan, this might be accomplished quickly or it might take some time to complete.

10 Setting Up a Development Environment

Setting up a development environment where you can test, analyze, and develop your Identity Manager solution allows you to learn about each component of Identity Manager and find unforeseen issues that can arise. For example, when you synchronize information between different systems, the information is presented differently for each system. Changing the data to see how it synchronizes between these two systems allows you to see if this change affects other systems that use this same information.

Another major reason to set up a development environment is to make sure your solutions work before you apply them to live data. Identity Manager manipulates and deletes data. Having the test environment allows you to make changes without any loss to the data in your production environment. When you start the project with a reasonable deployment order, it allows you to gain significant value quickly, and helps you evaluate the changing needs of your implementation over time. This allows you to develop your environment for best performance and scalability. For example, you can start with deploying self-service and password management, and then follow it with other capabilities. This enables your organization to incrementally verify that the functions and capabilities of Identity Manager are installed, configured, and tested as expected before they are introduced to your production environment. Phased roll-out helps to deliver manageable change to your organization.

You use Designer to create a project plan that includes the business information as well as the technical information. It allows you to develop, test, and then deploy your solution in stages from the test environment to the production environment. For more information about Designer, see *NetIQ Designer for Identity Manager Administration Guide*.

Development: The implementation team develops detailed configurations for the solution based on the results of the previous phases of the life cycle. The solution is developed in a controlled environment that represents a production environment but is not actually a production environment. The implementation team develops installation and configuration scripts or procedures, builds detailed product and tool configurations, and prepares the required documentation and performance metrics. Supporting processes and organizational changes required by the identity management solution are the outcome of this stage. To set up your development environment, use the information in Chapter 1, “How Identity Manager Solves Business Challenges,” on page 11. It is an installation checklist of all of the Identity Manager components. Use this list to make sure you have installed and configured all components for Identity Manager that you can use to develop a project plan. Use the information in Chapter 11, “Technical Guidelines,” on page 65 as you set up your development environment, so you can learn about technical considerations as you install and configure each component of Identity Manager.

Testing: The implementation procedures are validated in a controlled environment. The environment must qualify to test all aspects of the design prior to the production deployment. For example, the implementation team can apply a pilot project to a subset of the systems and applications in a production environment. This allows the team to make adjustments with minimal impact to your operations. Based on the outcome of the tests, the deployment team makes all required adjustments to either the implementation procedures or to the design, and then revalidates the procedures and configuration.

Deployment: The new design is fully deployed in the production environment. The implementation team uses the results of the testing stage to create an enterprise-wide plan. Any pending equipment procurement is finalized in this stage. The metrics developed in the development stage should be used to measure the success of the implementation. Towards the end of the initial deployment and before handing over to formal production, impart the required training for the operations and support staff. When deployment is completed, your organization will have a fully functional and documented production environment.

After the plan is implemented you are likely to make adjustments to the implementation due to organizational changes, performance issues, new technologies, or other factors. When you make adjustments to the plan, document the changes as part of a change control system that can be accessed and referenced by the appropriate members of the project team.

11 Technical Guidelines

The information that you gather in Designer allows you to make the technical decisions such as installation location and configuration options about each component of Identity Manager. For an introduction to each component, see Part I, "Identity Manager Overview," on page 9.

Components to Install

The following table lists the components to install to support the functionality that you want to implement. For instructions on installing these components, see the Setup Guide for your platform on the Identity Manager Documentation Website (https://www.netiq.com/documentation/identity-manager-48/quick_start_installing/data/quick_start_installing.html).

Functionality	Component to Install
Manage user identities in a corporate directory	Identity Manager Server
Provision accounts in connected systems	Identity Applications
	Identity Manager Drivers
	Designer
	For instructions on installing Identity Manager drivers, see the driver implementation guide for the type of driver that you want to install on the Identity Manager Drivers Documentation Website (https://www.netiq.com/documentation/identity-manager-48-drivers/).
Authentication	One Single Sign-On Provider
Password Management	Self Service Password Management
Generate reports on Identity Manager activity	Identity Reporting

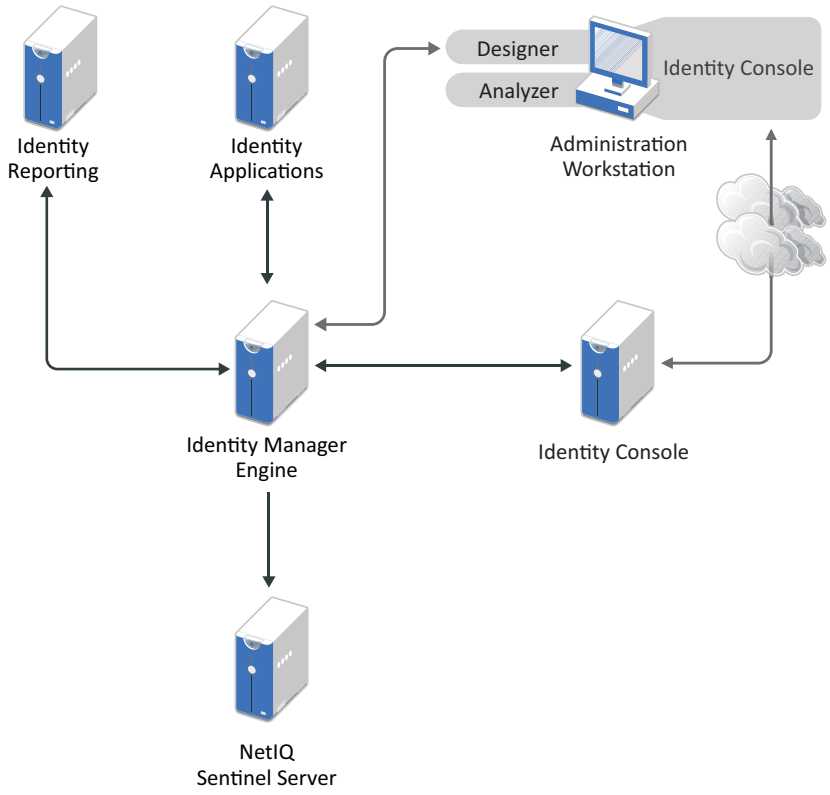
Identity Manager Configurations

The hardware that you need for an Identity Manager installation depends on the functionality that you want to implement and the size of your deployment. For an overview of basic configurations that you must consider before installing Identity Manager, see Chapter 5, "Identity Manager Deployment Configurations," on page 33.

Technical Guidelines

Figure 11-1 is one possible configuration of an Identity Manager solution.

Figure 11-1 Identity Manager Components

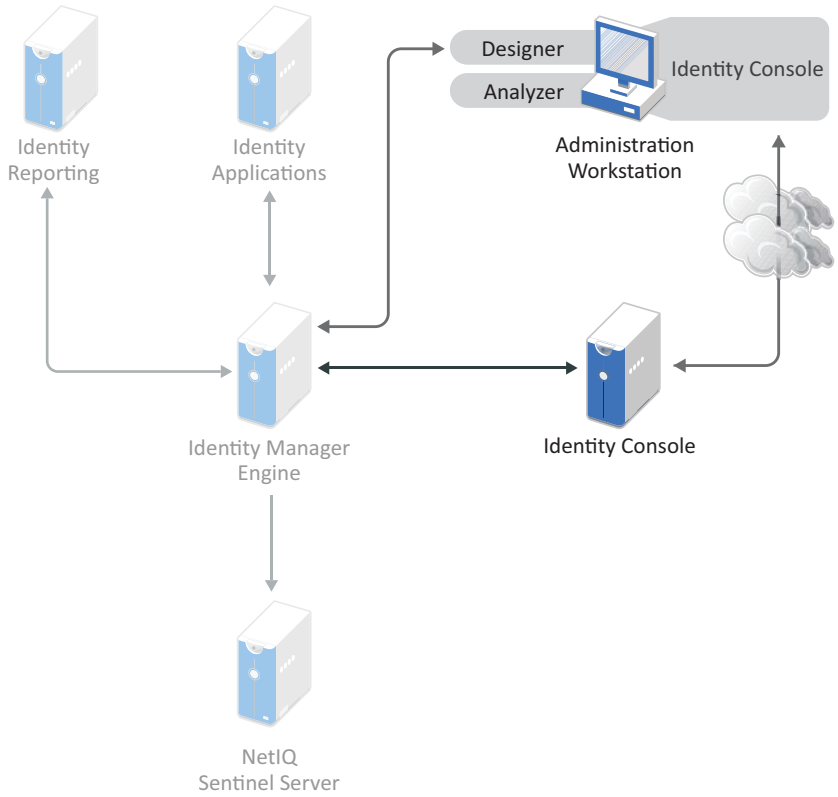


Identity Manager is very customizable. The following sections contain technical best practices guidelines to help set up and configure the Identity Manager solution that works best for your environment. Variables that affect how these guidelines apply to your environment include the type of hardware you have for your servers, how your WAN is configured, and how many objects are being synchronized.

Management Tools Guidelines

The two main management tools for the Identity Manager solution are Designer and Identity Console, as illustrated in Figure 11-2. Designer is used during the planning and creation of the Identity Manager solution, and Identity Console is used for daily management tasks of the Identity Manager solution.

Figure 11-2 Identity Manager Management Tools



- "Analyzer Guidelines" on page 67
- "Designer Guidelines" on page 68
- "Identity Console Guidelines" on page 68

Analyzer Guidelines

Analyzer is a thick client that is installed on a workstation. Analyzer is used to examine and clean the data in the systems that you want to add to your Identity Manager solution. Using Analyzer during the planning phase helps you see what changes need to be made and how best to make those changes.

There are no major considerations for using Analyzer. For more information, see the *NetIQ Analyzer for Identity Manager Administration Guide (https://www.netiq.com/documentation/identity-manager-48/analyzer_admin/data/netiq-identity-manager-analyzer-admin.html)*.

Designer Guidelines

Designer is a thick client that is installed on a workstation. Designer is used to design, test, document, and then deploy your Identity Manager solution. Using Designer throughout the planning phase helps you capture information in one place. It also helps you see issues you might not be aware of as you look at all of the components of the solution together.

There are no major considerations for using Designer, unless you have multiple people working on the same project. Designer allows for version control of the project. For more information, see "Version Control" in the *NetIQ Designer for Identity Manager Administration Guide*.

Identity Console Guidelines

Identity Console is a Web application that is the administration tool for Identity Manager. When you install Identity Manager, the installation expects that you already have an Identity Console server installed in your eDirectory tree.

If you have more than 10 administrators constantly working in Identity Console at one time, you should have a server that hosts only Identity Console. Figure 11-2 represents this configuration of your Identity Manager solution. If you have only one administrator, you can run Identity Console on your Identity Manager server without complications.

Identity Manager Server Guidelines

You can have one or more Identity Manager servers in your Identity Manager solution, depending on the server workload. The Identity Manager server requires that eDirectory be installed as shown in Figure 11-3. You can add a Remote Loader server, not represented in the figure, to help with the workload or configuration of your environment.

Considerations for Installing Drivers with the Identity Manager Engine

Many variables affect the performance of the server where you install the Identity Manager engine, including the number of drivers running on the server. When planning where to install the drivers, NetIQ provides the following recommendations:

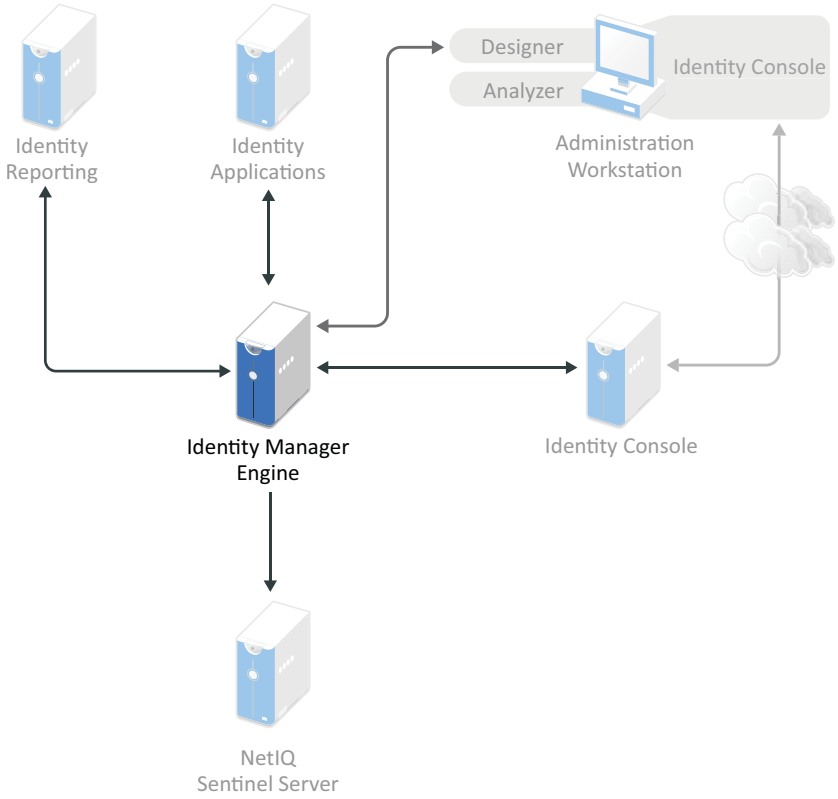
- In general, the number of drivers running on the server depends on the load that the drivers place on the server. Some drivers process a large quantity of objects while other drivers do not.
- If you plan to synchronize millions of objects with each driver, limit the number of drivers on the server. For example, deploy fewer than 10 drivers of these drivers.
- If you plan to synchronize 100 objects or fewer per driver, you might be able to run more than 10 drivers on the server.
- To create a baseline on server performance which helps you determine the optimum number of drivers, use the health monitoring tools in Identity Console. For more information about the health monitoring tools, see "Monitoring Driver Health" in the *NetIQ Identity Manager Driver Administration Guide*.

Considerations for Installing Drivers with the Remote Loader

Drivers must run on the same server as the connected application. For example, to configure the Active Directory driver, the server in Figure 11-3 must be a member server or a domain controller. If you do not want to install eDirectory and Identity Manager on a member server or domain controller, then you can install the Remote Loader on a member server or a domain controller. The Remote Loader sends all of the events from Active Directory to the Identity Manager server. The Remote Loader receives any information from the Identity Manager server and passes that to the connected application.

The Remote Loader provides added flexibility for your Identity Manager solution. For more information, see *Deciding Whether to Use the Remote Loader* in the *NetIQ Identity Manager Driver Administration Guide*.

Figure 11-3 *Identity Manager Sever*



There are many variables that affect the performance of the server. The standard recommendation is that you have no more than ten drivers running on an Identity Manager server. However, if you are synchronizing millions of objects with each driver, you might not be able to run ten drivers on a server. On the other hand, if you are synchronizing 100 objects per driver, you can probably run more than ten drivers on one server.

Setting up the Identity Manager solution in a lab environment gives you the opportunity to test how the servers will perform. You can use the health monitoring tools to obtain a baseline and then be able to make the best decisions for your environment. For more information about the health monitoring tools, see "Monitoring Driver Health" in the *NetIQ Identity Manager Driver Administration Guide*.

For considerations for each driver, see the Identity Manager Drivers documentation Web site (https://www.netiq.com/documentation/identity-manager-49-drivers/). Driver-specific information is provided in each driver guide.

Identity Vault Guidelines

Identity Vault (eDirectory) stores the objects that are synchronized through the Identity Manager solution. The following sections contain guidelines that help you plan your deployment of Identity Vault.

- "Understanding Identity Manager Objects in Identity Vault" on page 70
- "Replicating the Objects that Identity Manager Needs on the Server" on page 70
- "Using Scope Filtering to Manage Users on Different Servers" on page 72
- "Improving Identity Vault Performance" on page 74

Understanding Identity Manager Objects in Identity Vault

The following list indicates the major Identity Manager objects that are stored in Identity Vault and how they relate to each other. No objects are created during the installation of Identity Manager. The Identity Manager objects are created during the configuration of the Identity Manager solution.

- **Driver Set:** A driver set is a container that holds Identity Manager drivers and library objects. Only one driver set can be active on a server at a time. However, more than one server might be associated to one driver set. Also, a driver can be associated with more than one server at a time. However, the driver should only be running on one server at a time. The driver should be in a disabled state on the other servers. Any server that is associated with a driver set must have the Identity Manager server installed on it.
- **Library:** The Library object is a repository of commonly used policies that can be referenced from multiple locations. The library is stored in the driver set. You can place a policy in the library so that every driver in the driver set can reference it.
- **Driver:** A driver provides the connection between an application and the Identity Vault. It also enables data synchronization and sharing between systems. The driver is stored in the driver set.
- **Job:** A job automates a recurring task. For example, a job can configure a system to disable an account on a specific day, or initiate a workflow to request an extension of a person's access to a corporate resource. The job is stored in the driver set.

Replicating the Objects that Identity Manager Needs on the Server

If your Identity Manager environment calls for multiple servers in order to run multiple Identity Manager drivers, your plan should make sure that certain Identity Vault objects are replicated on servers where you want to run these Identity Manager drivers.

You can use filtered replicas, as long as all of the objects and attributes that the driver needs to read or synchronize are included in the filtered replica.

Keep in mind that you must give the Identity Manager Driver object sufficient Identity Vault rights to any objects it is to synchronize, either by explicitly granting it rights or by making the Driver object security equivalent to an object that has the desired rights.

An Identity Vault server that is running an Identity Manager driver (or that the driver refers to, if you are using the Remote Loader) must hold a master or read/write replica of the following:

- The Driver Set object for that server.

  You should have one Driver Set object for each server that is running Identity Manager. Unless you have specific needs, don't associate more than one server with the same Driver Set object.

  NOTE: When you create a Driver Set object, the default setting is to create a separate partition. Novell recommends creating a separate partition on the Driver Set object. For Identity Manager to function, the server is required to hold a full replica of the Driver Set object. If the server has a full replica of the location where the Driver Set object is installed, the partition is not required.

- The Server object for that server.

  The Server object is necessary because it allows the driver to generate key pairs for objects. It is also important for Remote Loader authentication.

- The objects that you want this instance of the driver to synchronize.

  The driver cannot synchronize objects unless a replica of those objects is on the same server as the driver. In fact, an Identity Manager driver synchronizes the objects in *all* the containers that are replicated on the server unless you create rules for scope filtering to specify otherwise.

  For example, if you want a driver to synchronize all user objects, the simplest way is to use one instance of the driver on a server that holds a master or read/write replica of all your users.

  However, many environments don't have a single server that contains a replica of all the users. Instead, the complete set of users is spread across multiple servers. In this case, you have three choices:

  - **Aggregate users onto a single server.** You can create a single server that holds all users by adding replicas to an existing server. Filtered replicas can be used to reduce the size of the eDirectory database if desired, as long as the necessary user objects and attributes are part of the filtered replica.
  - **Use multiple instances of the driver on multiple servers, with scope filtering.** If you don't want to aggregate users onto a single server, you need to determine which set of servers holds all the users, and set up one instance of the Identity Manager driver on each of those servers.

    To prevent separate instances of a driver from trying to synchronize the same users, you need to use scope filtering to define which users each instance of the driver should synchronize. Scope filtering means that you add rules to each driver to limit the scope of the driver's management to specific containers. See "Using Scope Filtering to Manage Users on Different Servers" on page 72.
  - **Use multiple instances of the driver on multiple servers, without scope filtering.** If you want to have multiple instances of a driver running on different servers without using filtered replicas, you need to define policies on the different driver instances that enable the driver to process different sets of objects within the same Identity Vault.

- The Template objects you want the driver to use when creating users, if you choose to use templates.

Identity Manager drivers do not require you to specify Identity Vault Template objects for creating users. However, if you specify that a driver should use a template when creating users in Identity Vault, the Template object must be replicated on the server where the driver is running.

- Any containers you want the Identity Manager driver to use for managing users.

  For example, if you have created a container named Inactive Users to hold user accounts that have been disabled, you must have a master or read/write replica (preferably a master replica) of that container on the server where the driver is running.

- Any other objects that the driver needs to refer to (for example, work order objects for the SAP User Management driver).

  If the other objects are only to be read by the driver, not changed, the replica for those objects on the server can be a read-only replica.

Using Scope Filtering to Manage Users on Different Servers

Scope filtering means adding rules to each driver to limit the scope of the driver's actions to specific containers. The following are two situations in which you would need to use scope filtering:

- You want the driver to synchronize only users that are in a particular container.

  By default, an Identity Manager driver synchronizes objects in all the containers that are replicated on the server where it is running. To narrow that scope, you must create scope filtering rules.

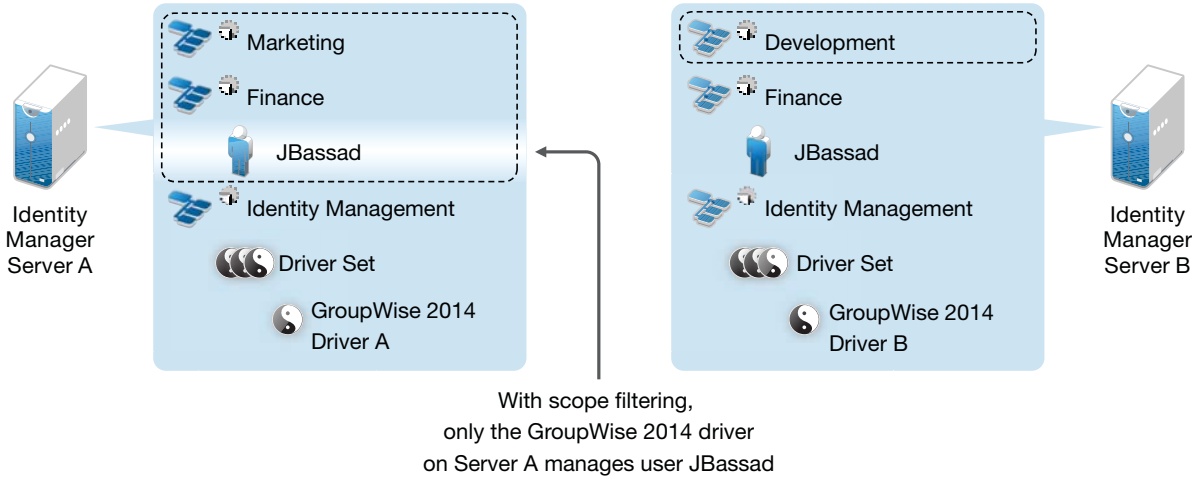
- You want an Identity Manager driver to synchronize all users, but you do not want all users to be replicated on the same server.

  To synchronize all users without having them replicated on one single server, you need to determine which set of servers holds all the users, and then create an instance of the Identity Manager driver on each of those servers. To prevent two instances of the driver from trying to synchronize the same users, you need to use scope filtering to define which users each instance of the driver should synchronize.

NOTE: You should use scope filtering even if your server's replicas don't currently overlap. In the future, replicas could be added to your servers and an overlap could be created unintentionally. If you have scope filtering in place, your Identity Manager drivers do not try to synchronize the same users, even if replicas are added to your servers in the future.

Figure 11-4 shows an example of an Identity Vault with three containers that hold users: Marketing, Finance, and Development. It also shows an Identity Management container that holds the driver sets. Each of these containers is a separate partition. In this example, the Identity Manager administrator has two Identity Vault servers, Server A and Server B. Neither server contains a copy of all the users. Each server contains two of the three partitions, so the scope of what the servers hold is overlapping.

Figure 11-4 Scope Filtering Defines Which Drivers Synchronize Each Container



The administrator wants all the users in the tree to be synchronized by the GroupWise 2014 driver, but does not want to aggregate replicas of the users onto a single server. He chooses instead to use two instances of the GroupWise 2014 driver, one on each server. He installs Identity Manager and sets up the GroupWise 2014 driver on each Identity Manager server.

Server A holds replicas of the Marketing and Finance containers. Also on the server is a replica of the Identity Management container, which holds the driver set for Server A and the GroupWise 2014 Driver object for Server A.

Server B holds replicas of the Development and Finance containers, and the Identity Management container holding the driver set for Server B and the GroupWise Driver object for Server B.

Because Server A and Server B both hold a replica of the Finance container, both servers hold the user JBassad, who is in the Finance container. Without scope filtering, both GroupWise Driver A and GroupWise Driver B would synchronize JBassad. Scope filtering prevents both instances of the driver from managing the same user, because it defines which drivers synchronize each container.

Identity Manager comes with predefined rules. There are two rules that help with scope filtering. “Event Transformation - Scope Filtering - Include Subtrees” and “Event Transformation - Scope Filtering - Exclude Subtrees” are documented in *NetIQ Identity Manager Understanding Policies Guide*.

For this example, you would use the Include Subtrees predefined rule for Server A and Server B. You would define the scope for each driver differently so that they would only synchronize the users in the specified containers. Server A would synchronize Marketing and Finance. Server B would synchronize Development.

Improving Identity Vault Performance

eDirectory, the underlying infrastructure for the Identity Vault, is I/O intensive application rather than being processor-intensive. Two factors increase performance of Identity Vault: more cache memory and faster processors. For best results, cache as much of the Directory Information Base (DIB) Set as the hardware allows.

While eDirectory scales well on a single processor, you might consider using multiple processors. Adding processors improves performance in areas such as user logins. Also, having multiple threads active on multiple processors improves performance.

The following table provides a general guideline for server settings, based on the expected number of objects in your Identity Vault.

Objects	Memory	Hard Disk
100,000	8 GB	16 GB
1 million	8 GB	32 GB
10 million	16 GB	40 GB

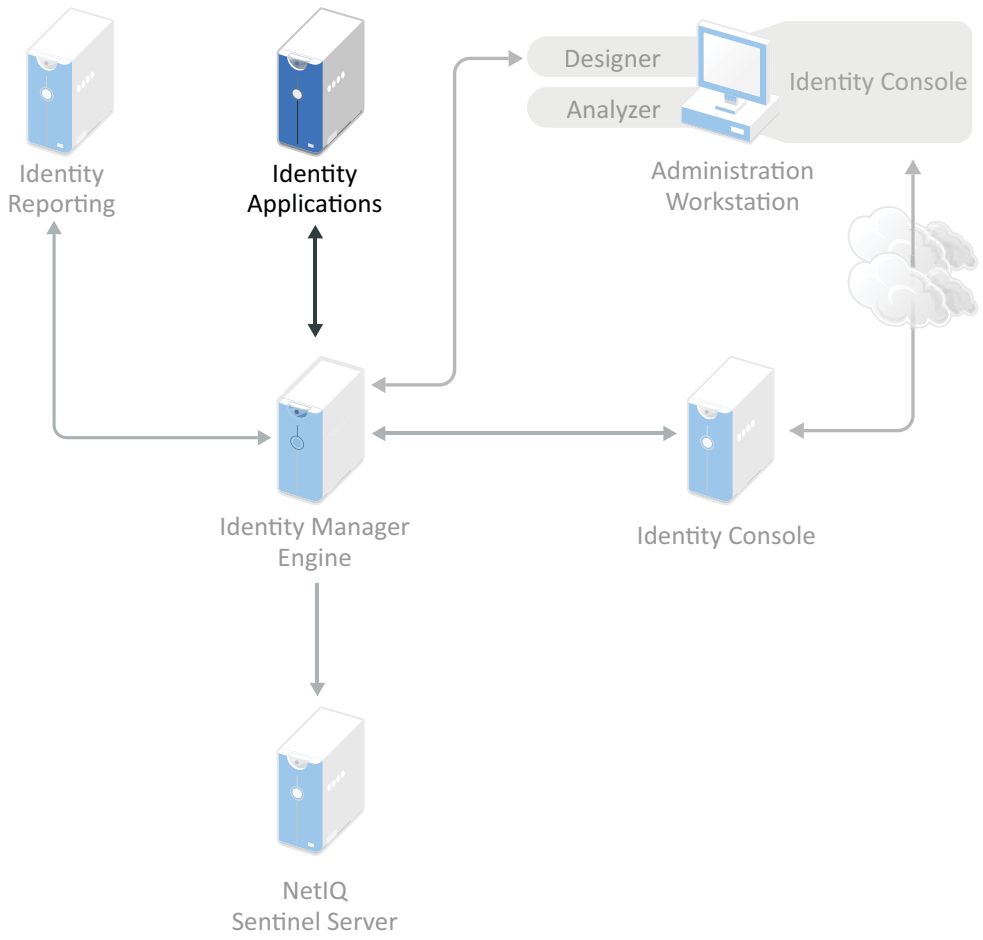
For example, a base installation of Identity Vault with the standard schema requires about 2 GB of disk space for every 50,000 users. However, if you add a new set of attributes or completely fill in every existing attribute, the object size grows. These additions affect the disk space, processor, and memory needed. Also, requirements for processors depend on additional services available on the computer as well as the number of authentications, reads, and writes that the computer is handling. Processes such as encryption and indexing can be processor intensive.

Identity Applications Guidelines

The Identity Applications installation program installs several components that provide the underlying framework for this component to work.

- Identity Manager Dashboard
- Identity Manager Administration Console
- User Application
- User Application driver (UAD)
- Role and Resource Service driver (RRSD)

Figure 11-5 *Identity Applications*



You can deploy identity applications on a single or multiple servers depending on the size and complexity of the resources that are managed by Identity Manager. A single-server configuration can be viewed as a cost-effective means to incrementally test and introduce Identity Manager functions into the production environment. To increase processing concurrency and data throughput, you might consider clustering the applications on multiple servers. Before you install Identity Applications in a cluster, you must determine how to configure the application server, either in a single-server or a cluster configuration.

The overall performance of the system depends on the individual performance of different features and components. This requires you to configure various aspects of the Identity Applications environment to meet the needs of your organization because a number of considerations come into play when making the transition from a pre-production environment to a production environment. You must consult with individuals who have an in-depth knowledge of Identity Applications to ensure that the considerations for the availability and tuning of the system are sufficiently addressed. Use the information in the Tuning the Performance of the Applications section of the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* to determine the best way to configure your Identity Applications server.

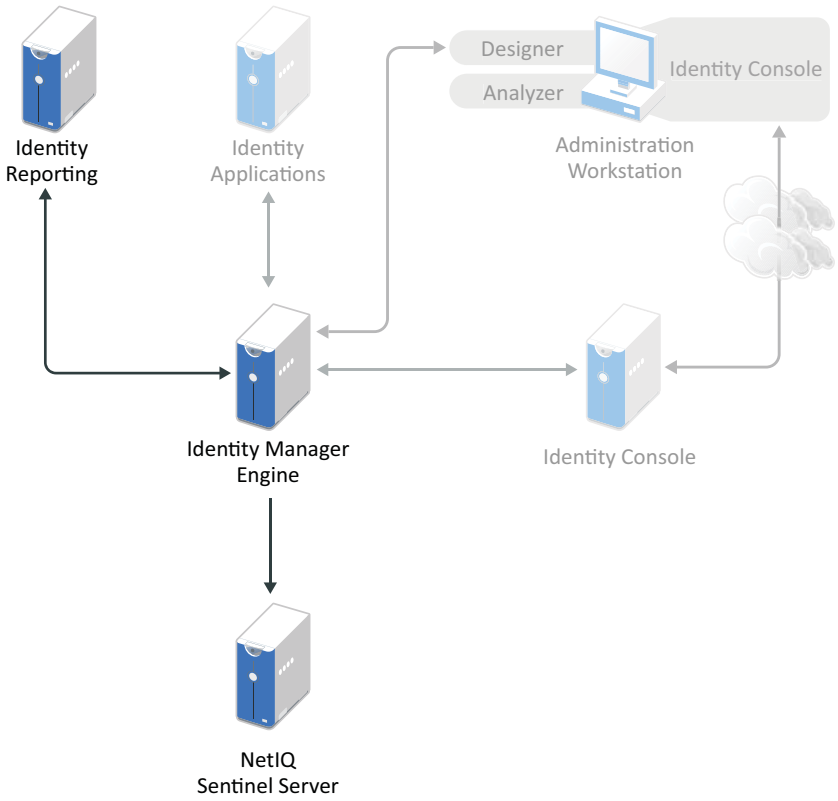
Auditing and Reporting Guidelines

Identity Manager auditing enables you to collect and store data for auditing, reporting, compliance verification, and event monitoring.

To include auditing and reporting as part of the Identity Manager solution, you must implement Identity Audit or NetIQ Sentinel. Identity Manager provides event forwarding capabilities to Sentinel by configuring Sentinel Link using Sentinel Event Source Management (ESM).

You should run Sentinel on its own server, as shown in Figure 11-6. The number of servers that are required for your solution depends on how many drivers you have in your environment and how many events you have defined to audit.

Figure 11-6 *Auditing Framework*



For more information, see *NetIQ Identity Manager - Configuring Auditing in Identity Manager*.