AUTHORIZED DOCUMENTATION

Overview

Novell®
Identity Manager

3.6

July 23, 2008

www.novell.com

Legal Notices

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

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

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

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

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

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

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide

This guide introduces you to the business issues that Novell® Identity Manager can help you solve and provides a technical overview of the Identity Manager software components and tools you can use in your solution. The guide is organized as follows:

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.

Documentation Updates

For the most recent version of this document, see the Identity Manager Documentation Web site (http://www.novell.com/documentation/idm36/index.html).

Additional Documentation

For documentation on other Identity Manager drivers, see the Identity Manager Drivers Web site (http://www.novell.com/documentation/idm36drivers/index.html).

Documentation Conventions

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

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

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

Identity Manager and Business Process Automation

1

The following information identifies some of the business processes you can automate through the implementation of a Novell® Identity Manager system. If you are already aware of the business automation solutions provided by Identity Manager, you might want to skip to the technical introduction provided in Chapter 2, "Identity Manager Architecture," on page 19.

Managing identity needs is a core function of most businesses. For example, imagine that it's early Monday morning. You scroll down the list of requests in your queue:

- Jim Taylor's cell phone number has changed. You need to update it in the HR database and four other independent systems.
- Karen Hansen, just returning from an extended leave of absence, has forgotten her e-mail password. You need to help her retrieve or reset it.
- Jose Altimira just hired a new employee. You need to give the employee network access and an e-mail account.
- Ida McNamee wants access to the Oracle* financial database, which requires you to get approval from three different managers.
- John Harris just moved from the Accounts Payable department to the Legal department. You need to give him access to the same resources as the other members of the Legal team and remove his access to Accounts Payable resources.
- Karl Jones, your own boss, saw a copy of Ida McNamee's request for access to the Oracle financial database and is concerned about the number of people with access. You need to generate a report for him that shows everyone who has access to the database.

You take a deep breath and start in on the first request, knowing that you'll be hard-pressed to keep up with all of the requests, let alone have time to finish the other projects assigned to you.

If this sounds like a common workday for you or someone in your organization, Identity Manager can help. In fact, the core Identity Manager capabilities, introduced in the following illustration, can help you automate all of these tasks and more. Centered on multi-system data synchronization driven by your business policies, the capabilities—workflow, roles, attestation, self-service, auditing, and reporting—combine to automate the processes involved in provisioning users and managing passwords, two of the most difficult and time-consuming duties of an IT organization.

Figure 1-1 *Identity Manager Core Capabilities*

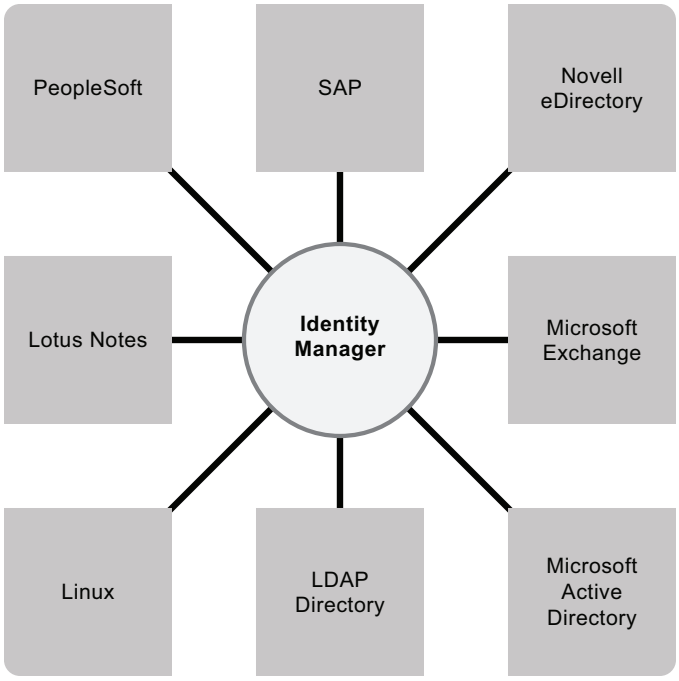
The following sections introduce you to these Identity Manager capabilities and how they can help you successfully meet the identity needs of your organization:

1.1 Data Synchronization

If your organization is like most, you have identity data stored in multiple systems. Or, you have identity data stored in one system that you could really use in another system. Either way, you need to be able to easily share and synchronize data between systems.

Identity Manager lets you synchronize, transform, and distribute information across a wide range of applications, databases, operating systems, and directories such as SAP*, PeopleSoft*, Lotus Notes*, Microsoft* Exchange, Microsoft Active Directory*, Novell eDirectory™, Linux and UNIX, and LDAP directories.

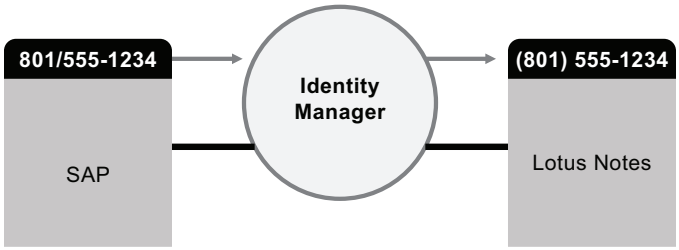
Figure 1-2 *Identity Manager Connecting Multiple Systems*



You control the flow of data among the connected systems. Among other things, you 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.

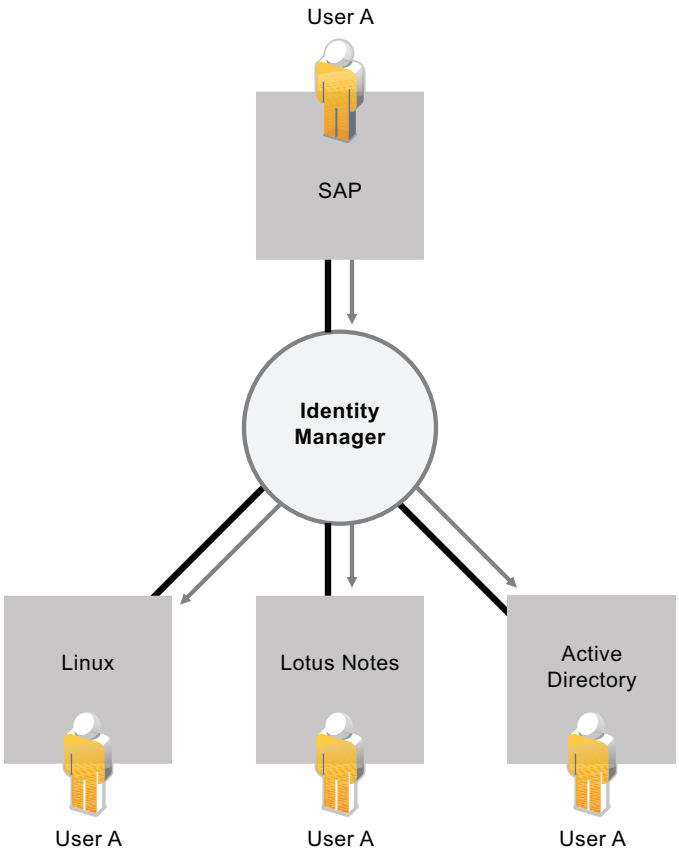
In the following diagram, the SAP HR database is the authoritative source for a user's telephone number. The Lotus Notes system also uses telephone numbers, so Identity Manager transforms the number into the required format and shares it with the Lotus Notes system. Whenever the telephone number changes in the SAP HR system, it is synchronized to the Lotus Notes system.

Figure 1-3 *Data Synchronization between Connected Systems*



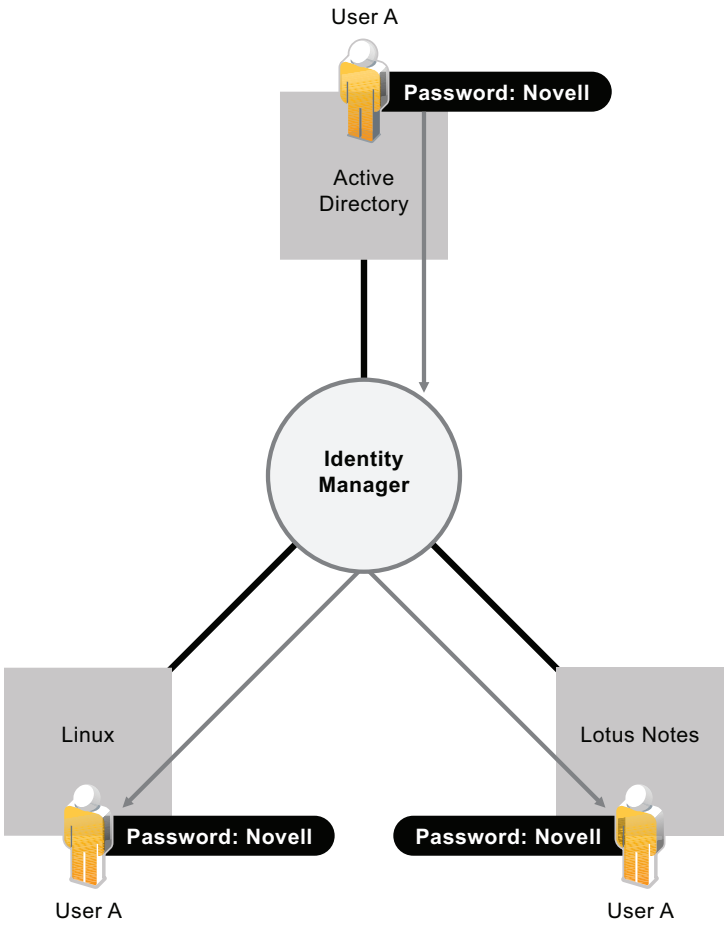
Managing data for existing users is just the beginning of the data synchronization capabilities of Identity Manager. In addition, Identity Manager can create new user accounts and remove existing accounts in directories such as Active Directory, systems such as PeopleSoft and Lotus Notes, and operating systems such as UNIX and Linux. For example, when you add a new employee to your SAP HR system, Identity Manager can automatically create a new user account in Active Directory, a new account in Lotus Notes, and a new account in a Linux NIS account management system.

Figure 1-4 *User Account Creation in Connected Systems*



As part of its data synchronization capability, Identity Manager can also help you synchronize passwords between systems. For example, if a user changes his or her password in Active Directory, Identity Manager can synchronize that password to Lotus Notes and Linux.

Figure 1-5 *Password Synchronization among Connected Systems*

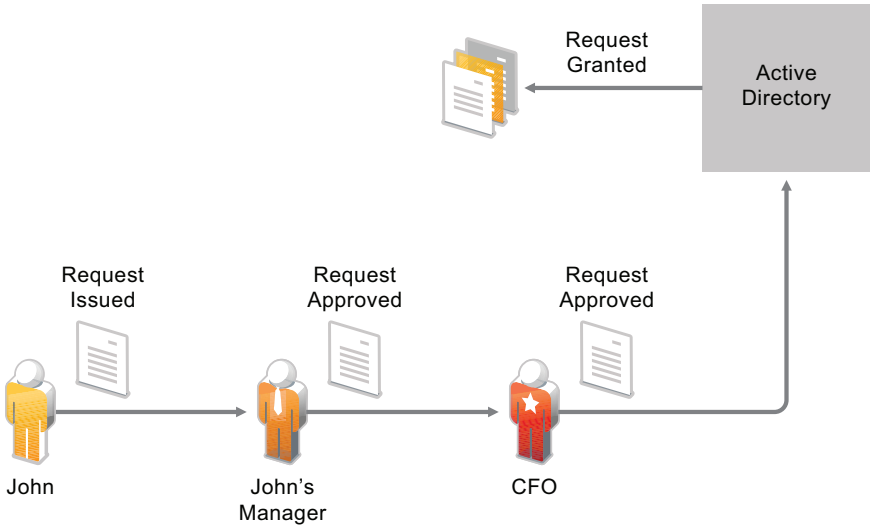


1.2 Workflow

More than likely, user access to many of the resources in your organization doesn't require anyone's approval. However, access to other resources might be restricted and require approval from one or more individuals.

Identity Manager 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've 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.

Figure 1-6 *Approval Workflow for User Provisioning*



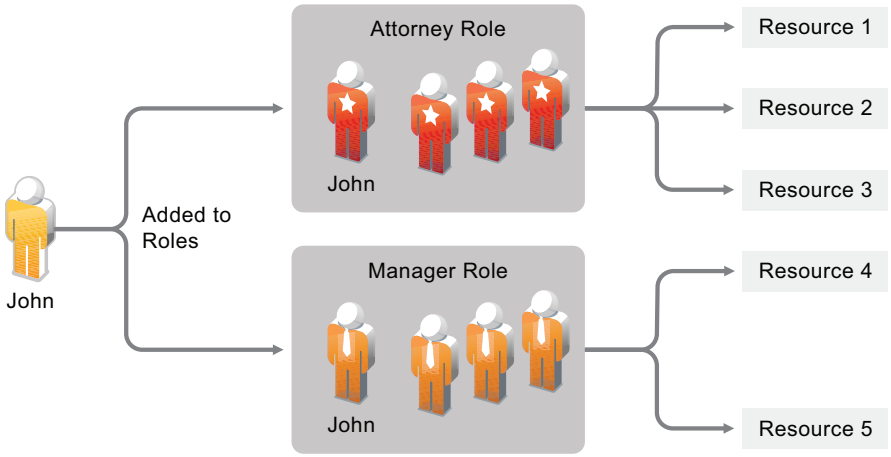
Workflows can be initiated automatically whenever a certain event occurs (for example, a new user is added to your HR system) or initiated manually through a user request. To ensure that approvals take place in a timely manner, you can set up proxy approvers and approval teams.

1.3 Roles and Attestation

Oftentimes, users require access to resources based upon their roles in the organization. For example, a law firm's attorneys might require access to a different set of resources than the firm's paralegals.

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. If a user is assigned multiple roles, he or she receives access to the resources associated with all of the roles, as shown in the following illustration.

Figure 1-7 *Role-Based Provisioning of Resources*



You can have users automatically added to roles as a result of events that occur in your organization (for example, a new user being added to your SAP HR database with the job title of Attorney). If approval is required for a user to be added 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, you might have roles that 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. Identity Manager helps you validate the correctness of your role assignments through an attestation process. Using this process, responsible individuals within your organization certify the data associated with roles:

- **User profile attestation:** Selected users attest to their own profile information (first name, last name, title, department, e-mail, and so forth) and correct any incorrect information. Accurate profile information is essential to correct role assignments.
- **Separation of Duties violation attestation:** Responsible individuals review a Separation of Duties violation report and attest to the accuracy of the report. The report lists any exceptions that allow a user to be assigned conflicting roles.
- **Role assignment attestation:** Responsible individuals review a report listing selected roles and the users, groups, and roles assigned to each role. The responsible individuals must then attest to the accuracy of the information.
- **User assignment attestation:** Responsible individuals review a report listing selected users and the roles to which they are assigned. The responsible individuals must then attest to the accuracy of the information.

These attestation reports are designed primarily to help you ensure that role assignments are accurate and that there are valid reasons for allowing exceptions for conflicting roles.

1.4 Self-Service

You probably have business managers and departments clamoring to manage their own users' information and access needs instead of relying on you or your staff. How many times have you heard "Why can't I change my own cell phone number in our corporate directory?" or "I'm in the Marketing department. Why do I have to call the Help Desk to get access to the Marketing Information database?"

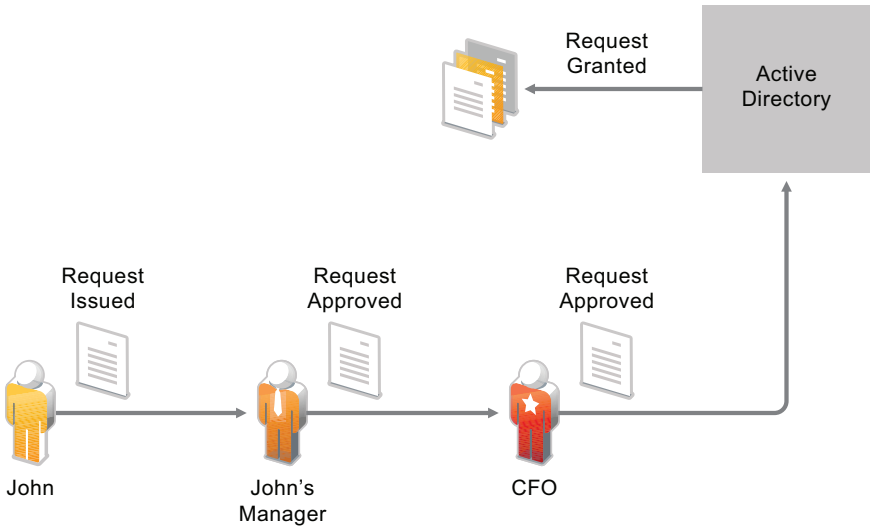
With Identity Manager, you can delegate administrative duties to the people who should be responsible for them. For example, you can enable individual users to:

- Manage their own personal data in the corporate directory. Rather than having you change a cell phone number, they can change it in one place and have it changed in all the systems you've synchronized through Identity Manager.

- Change their passwords, set up a hint for forgotten passwords, and set up challenge questions and responses for forgotten passwords. Rather than asking you to reset a password because they've forgotten it, they can do it themselves after receiving a hint or responding to a challenge question.
- 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, consider the scenario used in Section 1.2, "Workflow," on page 13 and shown below.

Figure 1-8 *Provisioning Workflow with Self-Service*



Not only does John use the Identity Manager self-service capability to request access to the documents he needs, but John's manager and the CFO use the self-service capability to 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 needed by John to access and view the financial documents.

1.5 Auditing and Reporting

Without Identity Manager, provisioning users can be a tedious, time-consuming, and costly effort. That effort, however, can pale in comparison to verifying that your provisioning activities have complied with your organization's policies, requirements, and regulations. Do the right people have access to the right resources? Are the wrong people shut out of those same resources? Does the employee who started yesterday have access to the network, his e-mail, and the six other systems required for his job? Has the access been canceled for the employee who left last week?

With Identity Manager, you can relax in your knowledge that all of your user provisioning activities are being tracked and logged for auditing purposes. Identity Manager issues event messages for all activities that occur. Using Novell Audit or Novell Sentinel™, you can collect these messages in order to generate the following types of reports:

- All approval workflows over a specific period of time, with the actions (started, forwarded, denied, approved, and so forth) recorded for each workflow.
- All resources provisioned over a specific period of time, with the actions (submitted, granted, revoked, success, and so forth) recorded for each resource.
- All workflow statuses, password changes, and administrative changes for a user over a specific period of time.
- All resource provisioning for a user over a specific period of time.
- All resource provisioning for all users over a specific period of time.

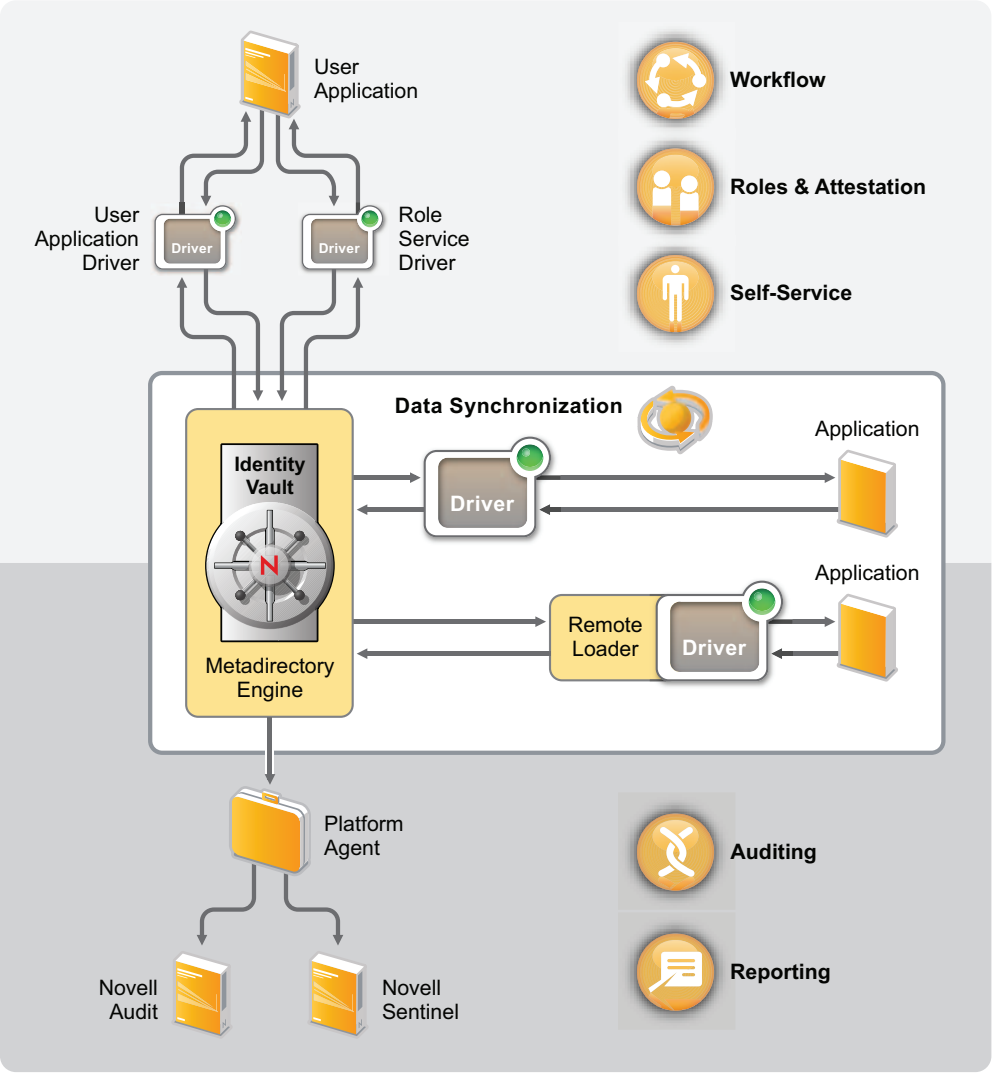
Novell Audit and Novell Sentinel are sold separately from Identity Manager. However, Novell Audit provides a starter pack at no charge so that you can generate basic provisioning reports for both users and resources.

Identity Manager Architecture

2

The following diagram shows the high-level architecture components that provide the Novell® Identity Manager capabilities introduced in Chapter 1, "Identity Manager and Business Process Automation," on page 9: data synchronization, workflow, roles, attestation, self-service, and auditing/reporting.

Figure 2-1 *Identity Manager High-Level Architecture*



Each of the components is introduced in the following sections:

- Section 2.1, "Data Synchronization," on page 20
- Section 2.2, "Workflow, Roles, Attestation, and Self-Service," on page 23
- Section 2.3, "Auditing and Reporting," on page 26

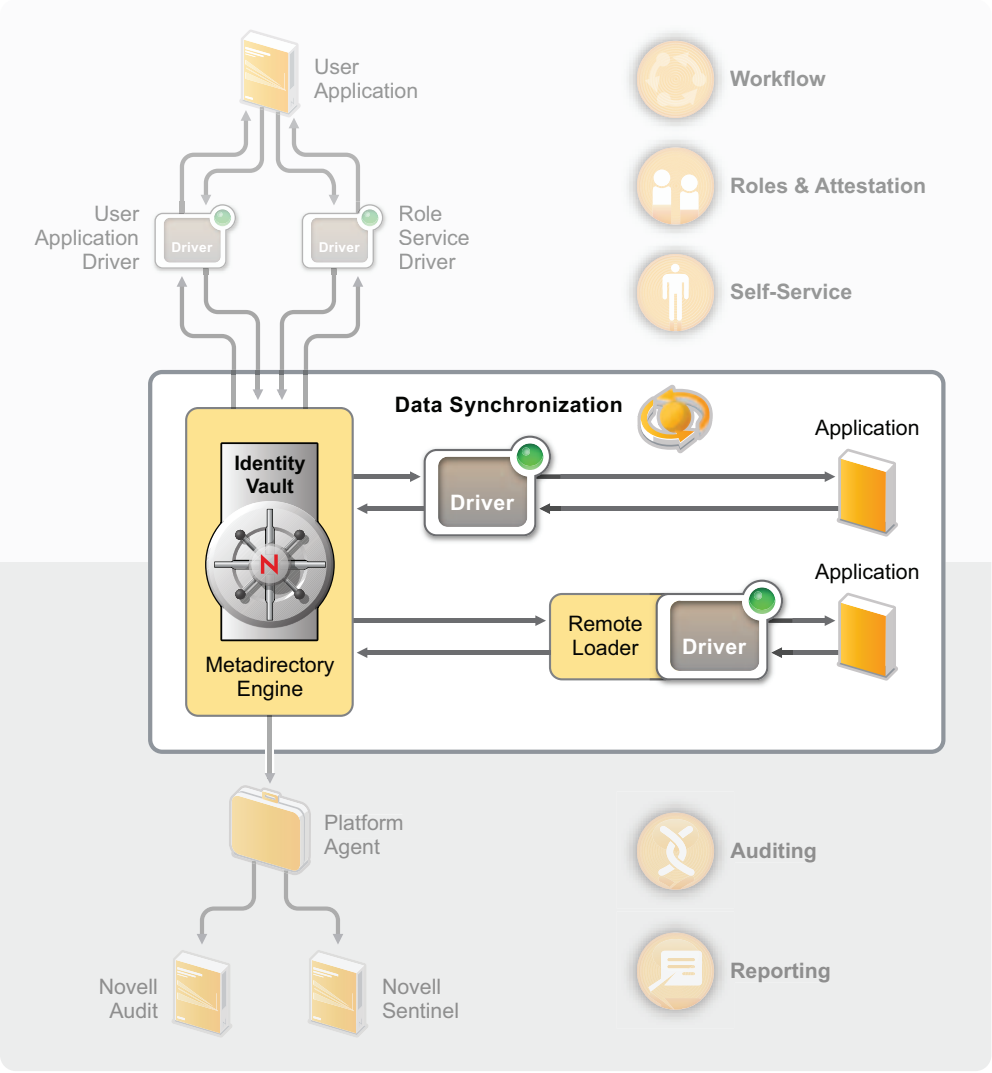
2.1 Data Synchronization

Data synchronization provides the foundation for automating business processes. In its simplest form, data synchronization is the movement of data from the location where a data item is changed to other locations where the data item is needed. For example, if an employee's phone number is changed in a company's Human Resources system, the change would ideally appear automatically in all other systems that store the employee's phone number.

Identity Manager is not limited to the synchronization of identity data. Identity Manager can synchronize any type of data stored in the connected application or in the Identity Vault.

Data synchronization, including password synchronization, is provided by the five base components of the Identity Manager solution: the Identity Vault, Metadirectory engine, drivers, Remote Loader, and connected applications. These components are shown in the following diagram.

Figure 2-2 *Identity Manager Architecture Components*



The following sections provide descriptions of each of these components and explain the concepts you should understand to effectively synchronize data among systems in your organization:

2.1.1 Components

Identity Vault: The Identity Vault serves as a metadirectory of the data you want synchronized between applications. For example, data synchronized from a PeopleSoft system to Lotus Notes is first added to the Identity Vault and then sent to the Lotus Notes system. In addition, the Identity Vault stores information specific to Identity Manager, such as driver configurations, parameters, and policies. Novell eDirectory™ is used for the Identity Vault.

Metadirectory Engine: When data changes in the Identity Vault or a connected application, the Metadirectory engine processes the changes. 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. The Metadirectory engine is also referred to as the *Identity Manager engine*.

Driver: Drivers connect to the applications whose identity information you want to manage. A driver has two basic responsibilities: 1) reporting data changes (events) in the application to the Metadirectory engine, and 2) carrying out data changes (commands) submitted by the Metadirectory engine to the application.

Remote Loader: Drivers must be installed and run on the same server as the application to which they are connecting. If the application is located on the same server as the Metadirectory engine, all you need to do is install the driver to that server. However, if the application is not located on the same server as the Metadirectory engine (in other words, it is remote to the engine’s server rather than local), you must install the driver and the Remote Loader to the application’s server. The Remote Loader loads the driver and communicates with the Metadirectory engine on behalf of the driver.

Application: A system, directory, database, or operating system that a driver connects to. 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*.

2.1.2 Key Concepts

Channels: Data flows between the Identity Vault and a connected system along two separate *channels*. The *Subscriber channel* provides data flow from the Identity Vault to a connected system; in other words, the connected system subscribes to data from the Identity Vault. The *Publisher channel* provides data flow from a connected system to the Identity Vault; in other words, the connected system publishes data to the Identity Vault.

Data Representation: Data flows through a channel as *XML documents*. An XML document is created when a change occurs in the Identity Vault or the connected system. The XML document is passed to the Metadirectory engine, which processes the document through the set of filters and policies associated with the driver’s channel. When all processing has been applied to the XML

document, the Metadirectory engine uses the document to initiate the appropriate changes to the Identity Vault (Publisher channel), or the driver uses the document to initiate the appropriate changes in the connected system (Subscriber channel).

Data Manipulation: As XML documents flow through a driver channel, the document data is affected by the *policies* associated with the channel.

Policies are used for many things, including changing data formats, mapping attributes between the Identity Vault and the connected system, conditionally blocking the flow of data, generating e-mail notifications, and modifying the type of data change.

Data Flow Control: *Filters*, or *filter policies*, control the flow of data. Filters specify which items of data are synchronized between the Identity Vault and a connected system. For example, user data is typically synchronized between systems. Therefore, the user data is listed in the filter for most connected systems. However, printers are generally not of interest to most applications, so printer data does not appear in the filter for most connected systems.

Each relationship between the Identity Vault and a connected system has two filters: a filter on the Subscriber channel that controls data flow from the Identity Vault to the connected system, and a filter on the Publisher channel that controls data flow from the connected system to the Identity Vault.

Authoritative Sources: Most items of data associated with identity have a conceptual owner. The owner of a data item is considered the *authoritative source* for the item. In general, only the authoritative source for a data item is allowed to make changes to the data item.

For example, the corporate e-mail system is generally considered the authoritative source for an employee's e-mail address. If an administrator of the corporate white pages directory changes an employee's e-mail address in that system, the change has no effect on whether the employee actually receives e-mail at the changed address because the change must be made to the e-mail system to be effective.

Identity Manager uses filters to specify authoritative sources for an item. For example, if the filter for the relationship between the PBX system and the Identity Vault allows an employee's telephone number to flow from the PBX system into the Identity Vault but not from the Identity Vault to the PBX system, then the PBX system is the authoritative source for the telephone number. If all other connected system relationships allow the telephone number to flow from the Identity Vault to the connected systems, but not vice versa, the net effect is that the PBX system is the only authoritative source for employee telephone numbers in the enterprise.

Automated Provisioning: Automated provisioning refers to Identity Manager's ability to generate user provisioning actions other than the simple synchronization of data items.

For example, in a typical Identity Manager system where the Human Resource database is the authoritative source for most employee data, the addition of an employee to the HR database triggers the automatic creation of a corresponding account in the Identity Vault. The creation of the Identity Vault account in turn triggers the automatic creation of an e-mail account for the employee in the e-mail system. Data used to provision the e-mail system account is obtained from the Identity Vault and might include employee name, location, telephone number, and so forth.

The automatic provisioning of accounts, access, and data can be controlled in various ways, including:

- *Data item values*: For example, the automatic creation of an account in the access databases for various buildings can be controlled by a value in an employee's location attribute.

- *Approval workflows*: For example, the creation of an employee in the finance department can trigger an automatic e-mail to the finance department head requesting approval for a new employee account in the finance system. The finance department head is directed by the e-mail to a Web page where the department head approves or rejects the request. Approval can then trigger the automated creation of an account for the employee in the finance system.
- *Role assignments*: For example, an employee is given the role of Accountant. Identity Manager provisions the employee with all accounts, access, and data assigned to the Accountant role, either through system workflows (no human intervention), human approval flows, or a combination of both.

Entitlements: An entitlement represents a resource in a connected system, such as an account or a group membership. When a user meets the criteria established for an entitlement in a connected system, Identity Manager processes an event for the user that results in the user being granted access to the resource. This, of course, requires that all of the policies be in place to enable access to the resource. For example, if a user meets the criteria for an Exchange account in Active Directory, the Metadirectory engine processes the user through the set of Active Directory driver policies that provide an Exchange account.

The key benefit of entitlements is that you can define the business logic for access to a resource in one entitlement rather than multiple driver policies. For example, you can define an Account entitlement that gives a user an account in four connected systems. The decision of whether or not to provide the user with an account is determined by the entitlement, which means that policies for each of the four drivers do not need to include the business logic. Instead, the policies only need to provide the mechanism for granting the account. If you need to make a business logic change, you change it in the entitlement instead of in each driver.

Jobs: For the most part, Identity Manager acts in response to data changes or user requests. For example, when a piece of data changes in one system, Identity Manager changes the corresponding data in another system. Or, when a user requests access to a system, Identity Manager initiates the appropriate processes (workflows, resource provisioning, and so forth) to provide the access.

Jobs enable Identity Manager to perform actions not initiated by data changes or user requests. A job consists of configuration data stored in the Identity Vault and a corresponding piece of implementation code. Identity Manager includes predefined jobs that perform such actions as starting or stopping drivers, sending e-mail notifications of expiring passwords, and checking the health status of drivers. You can also implement custom jobs to perform other actions; a custom job requires you (or a developer/consultant) to create the code required to perform the desired actions.

Work Orders: Typically, changes to data in the Identity Vault or a connected application are immediately processed. Work orders enable you to schedule tasks to be performed on a specific date and time. For example, a new employee is hired but is not scheduled to start for a month. The employee needs to be added to the HR database, but should not be granted access to any corporate resources (e-mail, servers, and so forth) until the start date. Without a work order, the user would be granted access immediately. With work orders implemented, a work order is created that initiates account provisioning only on the start date.

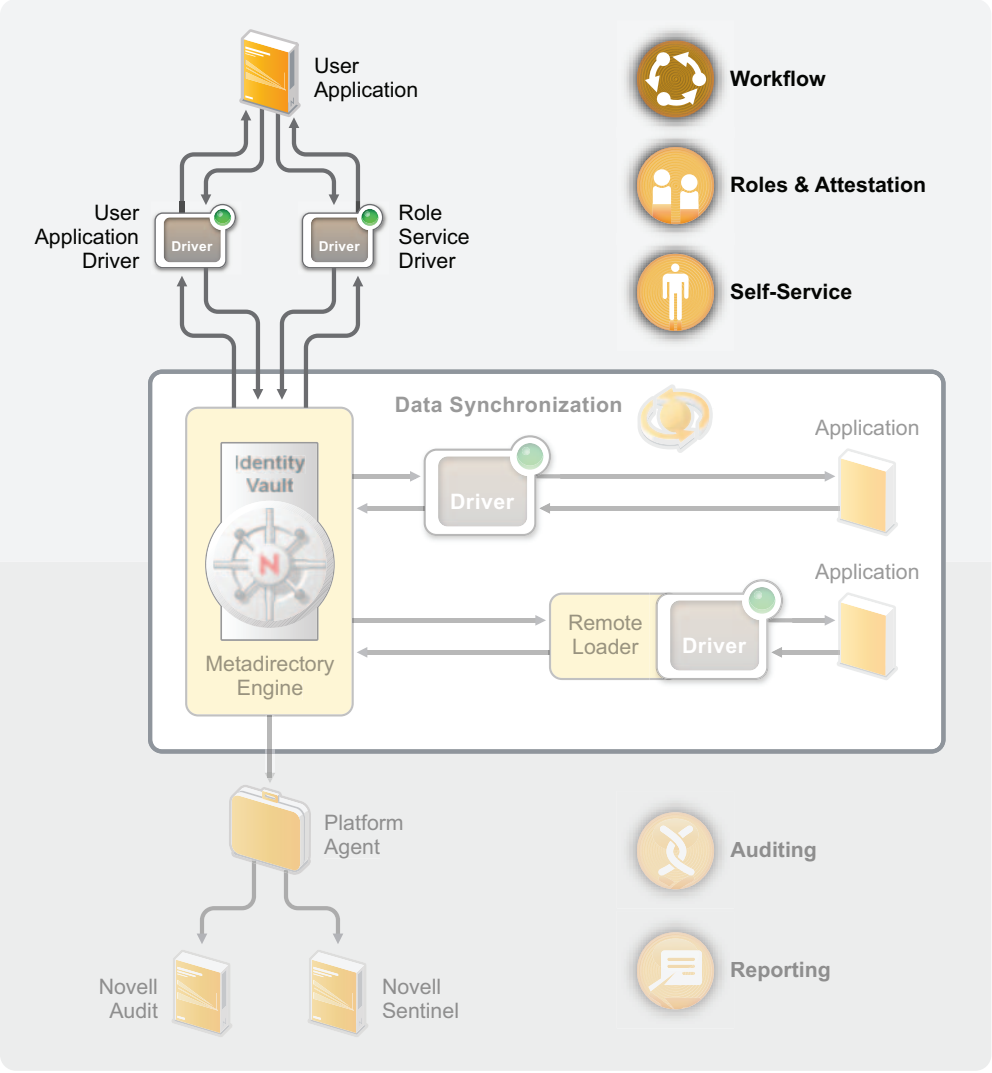
2.2 Workflow, Roles, Attestation, and Self-Service

Identity Manager provides a specialized application, the User Application, that provides approval workflows, role assignments, attestation, and identity self-service.

The standard User Application is included with Identity Manager. The standard version provides password self-service to help users remember or reset forgotten passwords, organization charts to manage user directory information, user management functionality that enables creation of users in the Identity Vault, and basic identity self-service such as management of user profile information.

The User Application Roles Based Provisioning Module is a separately sold add-on to Identity Manager. When you add the Roles Based Provisioning Module, the standard User Application functionality is extended to include advanced self-service, approval workflow, roles-based provisioning, Separation of Duties constraints, and attestation.

Figure 2-3 *Identity Manager User Application*



The following sections provide descriptions of each of these components and explain the concepts you should understand to effectively implement and manage the components:

- Section 2.2.1, “Components,” on page 25
- Section 2.2.2, “Key Concepts,” on page 25

2.2.1 Components

User Application: The User Application is a browser-based Web application that 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.

User Application Driver: The User Application driver stores configuration information and notifies the User Application whenever changes occur in the Identity Vault. It can also be configured to allow events in the Identity Vault to trigger workflows and to report success or failure of a workflow's provisioning activity to the User Application so that users can view the final status of their requests.

Role Service Driver: The Role Service driver manages all role assignments, starts workflows for role assignment requests that require approval, and maintains indirect role assignments according to group and container memberships. The driver also grants and revokes entitlements for users based on their role memberships, and performs cleanup procedures for requests that have been completed.

2.2.2 Key Concepts

Workflow-based Provisioning: Workflow-based provisioning provides a way for users to request access to resources. A provisioning request is routed through a predefined workflow that might include approval from one or more individuals. If all approvals are granted, the user receives access to the resource. Provisioning requests can also be initiated indirectly in response to events occurring in the Identity Vault. For example, adding a user to a group might initiate a request to have the user granted access to a specific resource.

Roles-based Provisioning: Roles-based provisioning provides a way for users to receive access to specific resources based upon the roles assigned to them. Users can be assigned one or more roles. If a role assignment requires approval, the assignment request starts a workflow.

Separation of Duties: To prevent users from being assigned to conflicting roles, the User Application Roles Based Provisioning Module provides a Separation of Duties feature. You can establish Separation of Duties *constraints* that define which roles are considered to be in conflict. When roles conflict, Separation of Duties *approvers* can approve or deny any *exceptions* to the constraints. Approved exceptions are recorded as Separation of Duties *violations* and can be reviewed through the attestation process described below.

Roles Management: Management of roles must be done by individuals assigned to the *Roles Module Administrator* and *Roles Manager* system roles.

The Roles Module Administrator creates new roles, modifies existing roles, and removes roles; modifies relationships between roles; grants or revokes role assignments for users; and creates, modifies, and removes Separation of Duties constraints.

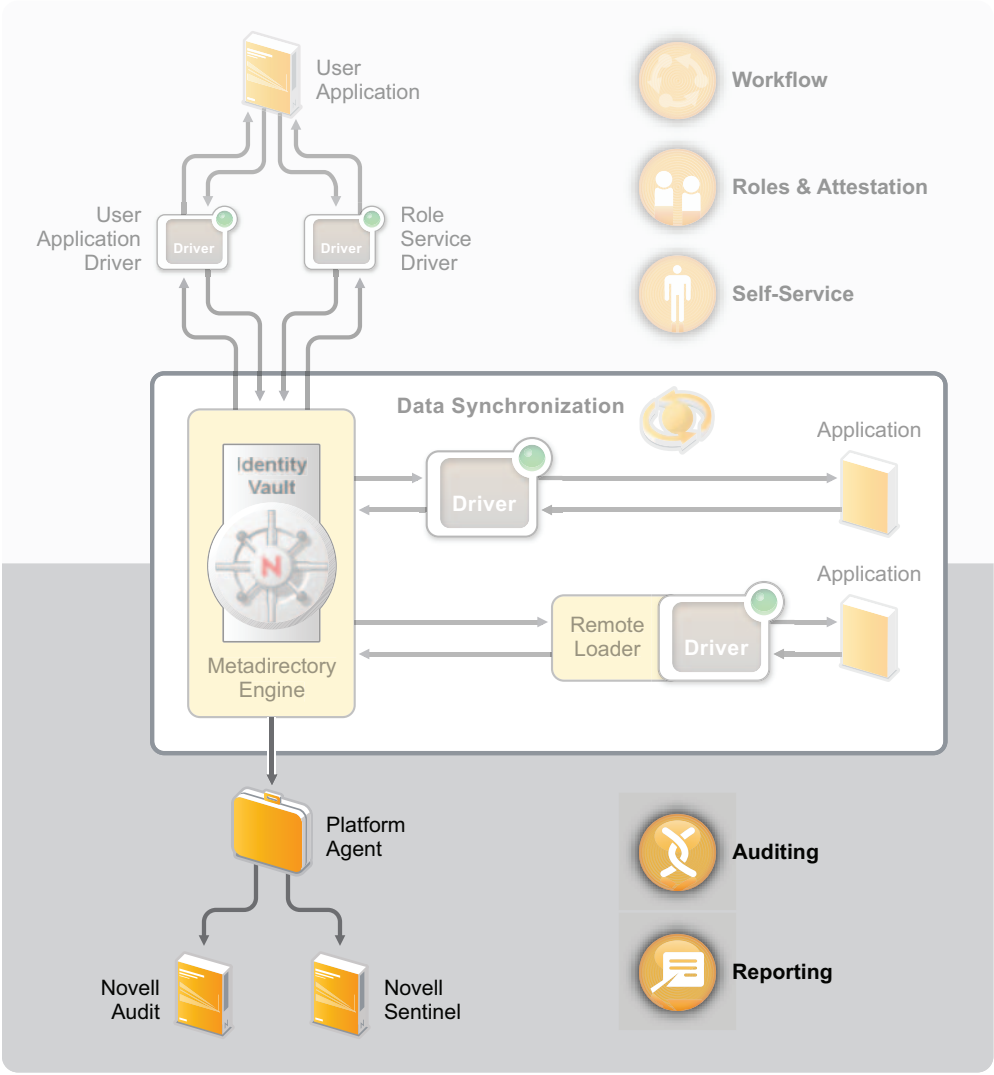
The Roles Manager can do the same things as the Roles Module Administrator with the exception of managing Separation of Duties constraints, configuring the Roles system, and running all reports. In addition, whereas the Roles Module Administrator has unlimited scope within the Roles system, the Roles Manager scope is limited to specifically-designated users, groups, and roles.

Attestation: Role assignments determine a user's access to resources within your organization, and incorrect assignments could jeopardize compliance with both corporate and government regulations. Identity Manager helps you validate the correctness of role assignments through an attestation process. Using this process, individual users can validate their own profile information and roles managers can validate role assignments and Separation of Duties violations.

2.3 Auditing and Reporting

Auditing and reporting is provided by integration with Novell Audit and Novell Sentinel™, as shown in the following diagram.

Figure 2-4 *Identity Manager Auditing and Reporting*



Platform Agent: The Platform Agent captures events from the Metadirectory engine and sends the events to the Novell Audit or Novell Sentinel system.

Novell Audit: Novell Audit is a centralized, cross-platform auditing service. It collects event data from multiple applications across multiple platforms and writes the data to a single, non-repudiatable data store. Novell Audit is sold separately. However, you can use the Novell Audit Starter Pack, available without charge from the Novell download site (http://www.novell.com/download), to generate basic provisioning reports.

For a more complete introduction to Novell Audit, including how to purchase the product, see the Novell Audit site (http://www.novell.com/products/audit/).

Novell Sentinel: Novell Sentinel is a security information and event management (SIEM) solution that automates the collection, analysis, and reporting of system network, application, and security logs. Novell Sentinel is sold separately.

For a more complete introduction to Novell Sentinel, including how to purchase the product, see the Novell Sentinel site (http://www.novell.com/products/sentinel/).

Identity Manager Tools

3

Identity Manager provides three primary tools to help you set up and maintain your Identity Manager system: Designer, iManager, and the User Application administration console.

You use Designer to create and configure your Identity Manager system in an off-line environment and then deploy your changes to your live system. You can use iManager to perform the same tasks as Designer and also monitor the health of your system; however, changes you make in iManager are deployed immediately, so we recommend that you use iManager for simple administration tasks and Designer for more complex configuration tasks that require modeling and testing prior to deployment.

You use the User Application administration console to manage the application's look and feel by creating and modifying pages and portlets. You can also modify application settings, such as caching and logging settings, and configure delegation and proxy settings specific to the User Application's provisioning functionality.

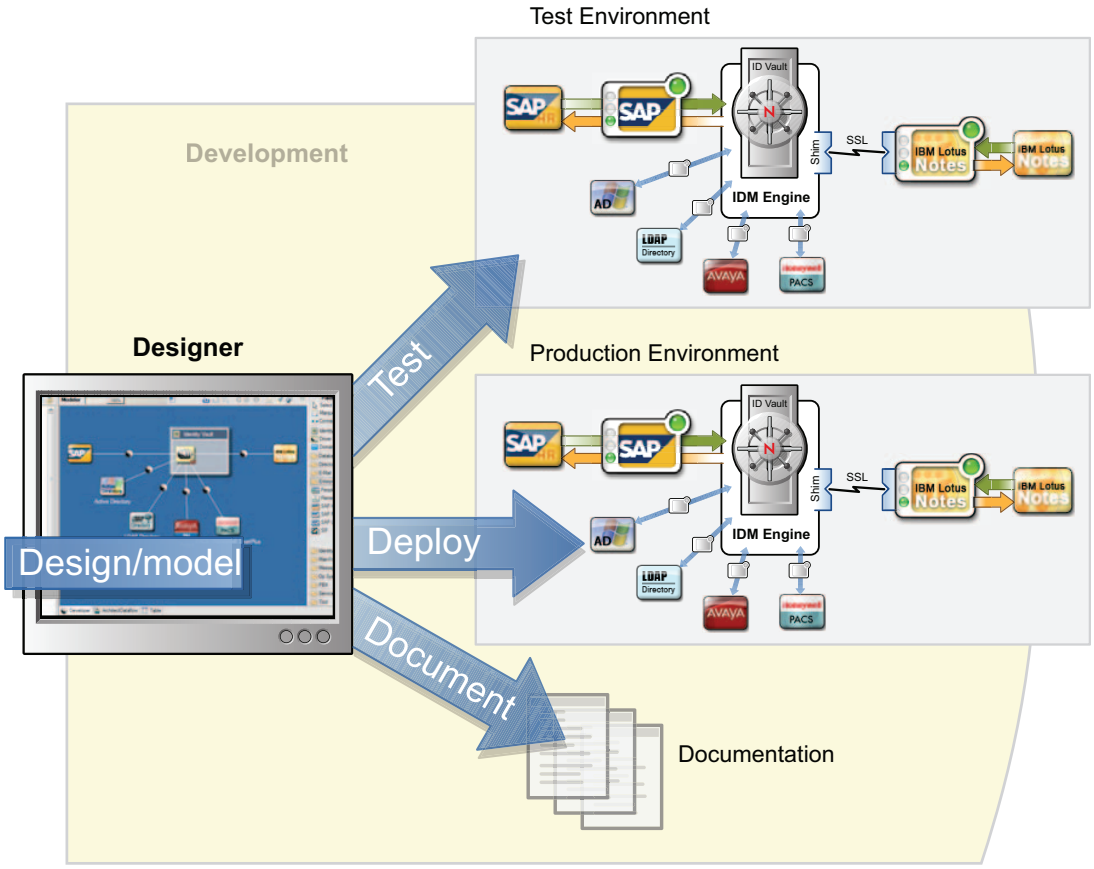
More information about each of these tools is provided in the following sections:

- Section 3.1, "Designer," on page 29
- Section 3.2, "iManager," on page 30
- Section 3.3, "User Application Administration Console," on page 31

3.1 Designer

Designer is an Eclipse*-based tool that helps you design, deploy, and document your Identity Manager system. Using Designer's graphical interface, you can design and test your system in an offline environment, deploy the system into your production environment, and document all details of your deployed system.

Figure 3-1 *Designer for Identity Manager*



Although it is possible to set up an Identity Manager system without using Designer, it is much more difficult and is not recommended.

Design: Designer provides a graphical interface through which you can model your system. This includes views that allow you to create and control the connections between Identity Manager and applications, configure policies, and manipulate how data flows between connected applications.

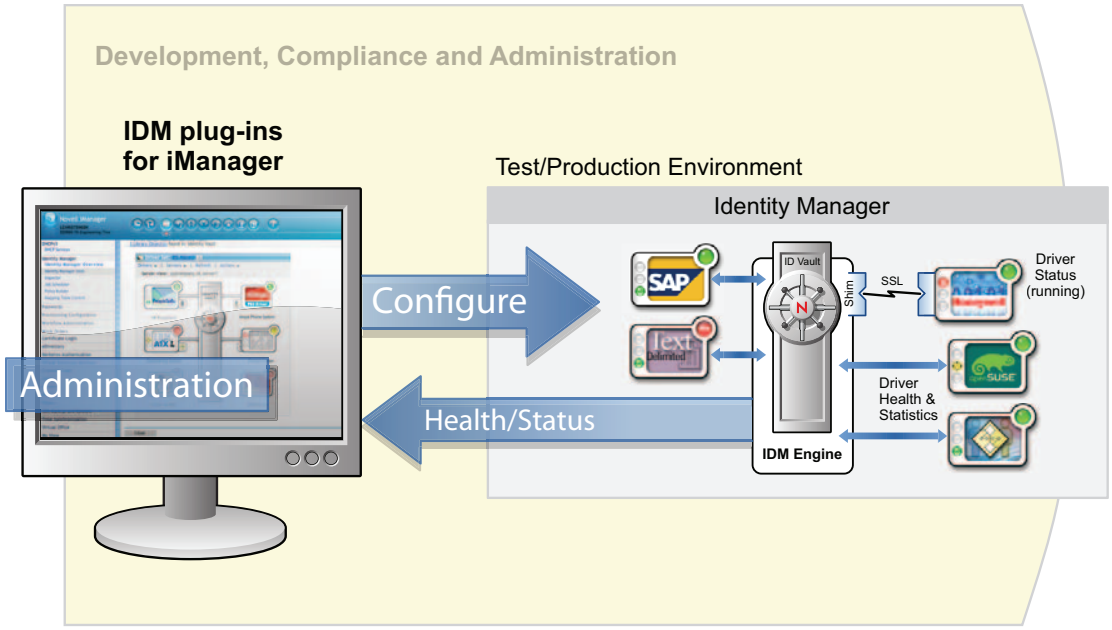
Deploy: The work you do in Designer is deployed to your production environment only when you initiate the deployment. This gives you the freedom to experiment, test the results, and resolve any issues before going live in your production environment.

Document: You can generate extensive documentation that shows your systems hierarchy, driver configurations, policy configurations, and much more. Basically, you have all the information needed to understand the technical aspects of your system while helping you verify compliance with your business rules and policies.

3.2 iManager

Novell® iManager is a browser-based tool that provides a single point of administration for many Novell products, including Identity Manager. By using the Identity Manager plug-ins for iManager, you can manage Identity Manager and receive real-time health and status information about your Identity Manager system.

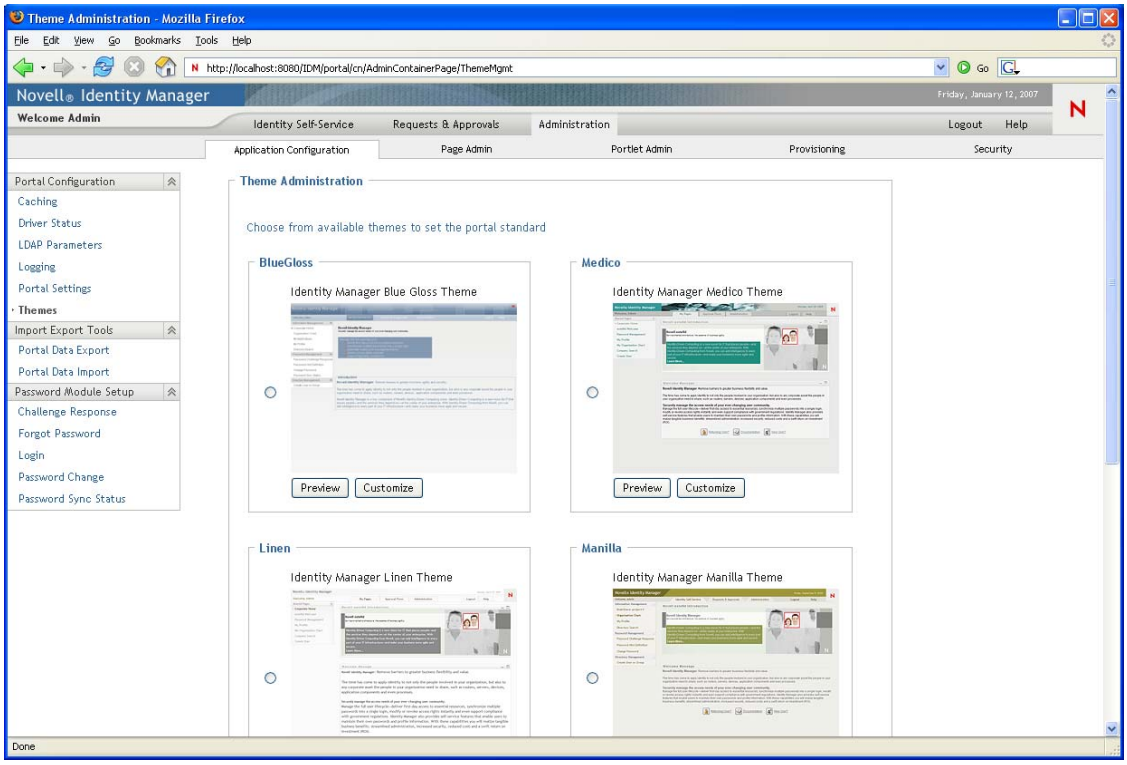
Figure 3-2 *Novell iManager*



3.3 User Application Administration Console

The User Application provides a Web-based administration console that allows you to configure, manage, and customize password self-service, roles, and provisioning. The administration console is added as an *Administration* tab in the User Application for anyone who has been assigned administrative rights.

Figure 3-3 *User Application Administration Pages*



The User Application Administration page provides the following tabs:

- **Application Configuration:** Lets you configure caching, LDAP parameters, logging, themes, and password module setup.
- **Page Administration:** Lets you create new pages or customize existing Identity Self-Service pages
- **Portlet Administration:** Lets you create new portlets or customize the existing portlets used on the Identity Self-Service pages.
- **Provisioning:** Lets you configure delegation, proxy, tasks, the digital signature service, and engine and cluster settings.
- **Security:** Lets you define who has Provisioning Administrator and User Application Administrator privileges.