Technical White Paper

SECURITY AND IDENTITY

www.novell.com

Novell® Identity Manager 3

Novell®

Table of Contents:

2 . . . . . Manage User Access—Automatically, Securely and Cost-effectively

3 . . . . . Overview

4 . . . . . Capabilities and Benefits

5 . . . . . Deployment Scenarios

8 . . . . . Architectural Overview

12 . . . . . Solution Components

18 . . . . . Configuration and Administration

21 . . . . . Workflow-based Provisioning

22 . . . . . Creating Policies

24 . . . . . Entitlement-based Provisioning

25 . . . . . Password Management

29 . . . . . Logging, Reporting and Auditing

29 . . . . . Server Deployment

30 . . . . . Technical Advantages

32 . . . . . Conclusion

Manage User Access—Automatically, Securely and Cost-effectively

Employee productivity, business agility, regulatory compliance and information security all depend on a comprehensive, well-architected enterprise-wide approach to identity management.

By combining enterprise-wide identity management, metadirectory, provisioning, access control, role-based management, password management and self-service functionality, Novell® Identity Manager provides the most comprehensive solution on the market to address your identity management needs.

Your business success depends on providing the right tools and information to the right people, when they need them. At the same time, your organization needs to protect its IT infrastructures from information theft; comply with regulatory mandates; and ensure the privacy of customer, partner and employee information. This requires your enterprise to cost-effectively secure and protect assets without compromising new business opportunities or reducing operational effectiveness.

Employee productivity, business agility, regulatory compliance and information security all depend on a comprehensive, well architected enterprise-wide approach to identity management. Without a strong identity-management foundation, new employees can sit idle, waiting for access to needed business tools, while former employees continue to have access for days and weeks after they've left the organization. Employees using different systems are unable to communicate or collaborate on joint projects. Even the best processes for complying with today's business regulations cannot succeed without verifiable, accurate and timely control over the identities of the people and resources distributed across your enterprise.

A flexible identity-management solution tears down the unintentional barriers among your business systems and enables the secure flow of information to authorized users. You need an identity-management solution that facilitates the creation and automates the enforcement of business policies that strengthen security, reduce administration costs and improve business productivity.

An identity-management solution should deliver immediate access and extend customized services to your business partners, suppliers and customers based on their unique individual relationships with your business. It should simplify your ability to manage the full user lifecycle by managing their access, identity information and passwords. It should provide workflow-based provisioning that streamlines approval processes and enables delegation of authority. It should provide user self-service features that ease your staff's management burden.

The solution needs to do all of this by leveraging—rather than replacing—your existing business processes, business rules and technology investments.

Overview

Novell Identity Manager helps you securely manage identity and access for your ever-changing user community through complete user lifecycle management. It integrates digital identities across your systems and organizational boundaries. It enables you to deliver first-day access to essential resources, synchronize passwords across connected systems, modify or revoke access rights instantly, and enforce security and regulatory compliance.

New to Identity Manger is complete support for workflow-based provisioning of resources through the Provisioning Module for Identity Manager. This innovative feature streamlines the provisioning process for resources that require human approval—automatically notifying the appropriate owners and enabling them to easily approve or deny resource requests.

Novell Identity Manager eases the IT burden by enabling delegated administration, allowing departmental managers to manage their own users' access needs instead of having to rely on a system administrator. Self-service provisioning and password management further lower IT time and costs while increasing user satisfaction.

Novell Identity Manager eases the IT burden by enabling delegated administration, allowing departmental managers to manage their own users' access needs instead of having to rely on a system administrator.

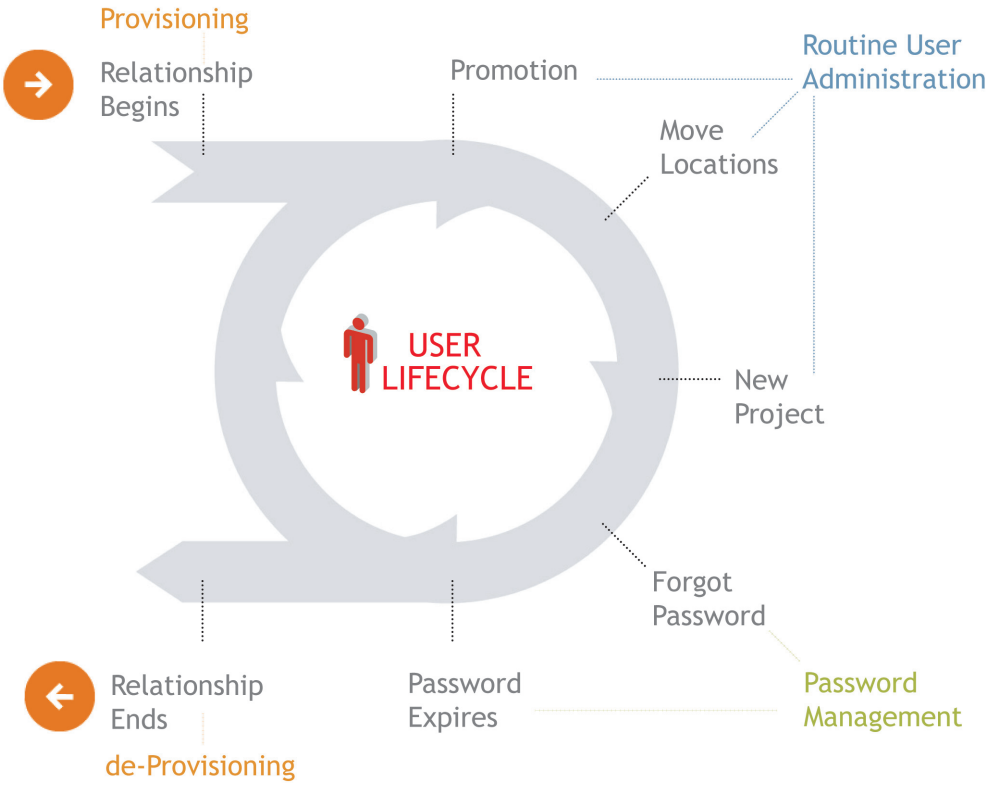

Figure 1. *Managing the Complete User Lifecycle*

Novell Identity Manager gives your enterprise the comprehensive identity management foundation it needs. It allows you to integrate, manage and control your distributed identity information to deliver the right resources to the right people.

Novell Identity Manager gives your enterprise the comprehensive identity management foundation it needs for account provisioning, single sign-on, self-service, authentication, authorization and Web services. It allows you to integrate, manage and control your distributed identity information so you can securely deliver the right resources to the right people—anytime, anywhere.

You can create password policies that define and automatically enforce criteria for passwords across all connected systems. Passwords are always created in compliance with your company policies, ensuring that they're difficult or impossible to "crack."

Capabilities and Benefits

Automated Provisioning

Novell Identity Manager leverages your business rules to automatically provision and de-provision resources based on user roles and/or approval by authorized managers. It also allows you to delegate authority for managing users and their access privileges to appropriate departmental heads or even temporary proxies, ensuring that responsibility always rests where it belongs. Identity Manager streamlines administration by automating routine user-management tasks or enabling users to perform the tasks themselves. As users switch offices, receive promotions, take on special assignments or begin new projects, Identity Manager can automatically update users' rights and information across all systems.

In any organization, it makes sense to provision some resources automatically based on user roles, while other resources should be provisioned only on an "as-needed" basis. The Web-based User Application included with Identity Manager includes a self-service provisioning feature that allows users to request access to the specific resources they need. The administrator retains control over which resources appear in the self-service list for each user group, and any resource requested from the list is subject to defined policies and approvals before it can be provisioned to the user. Self-service provisioning allows users to request the resources they need—when they need them—while ensuring automatic enforcement of policies and approvals.

The new Provisioning Module complements rule-based provisioning by automating human-based approval processes. Identity Manager automatically notifies via e-mail the appropriate person, who simply clicks a link in the e-mail to view and submit the online approval form. The Provisioning Module provides preconfigured templates that greatly simplify workflow-based provisioning, giving you full control over the number, type and sequence of approvals that must be given before a resource is provisioned.

Novell Identity Manager ensures that users have all the resources they need from their first day on the job and as they change roles over time. It prevents former employees and unauthorized users from accessing restricted resources. It also eliminates the expensive, time-consuming process of manually entering and updating user identity on multiple systems, so your IT staff saves money and time and can consequently focus on more strategic projects.

Password Management

You can create password policies that define and automatically enforce criteria for passwords across all connected systems. Passwords are always created in compliance with your company policies, ensuring that they're difficult or impossible to "crack."

Identity Manager enables password synchronization between all eligible configured systems. Because they won't have to remember multiple passwords, users are less likely to forget them or write them in places where they can easily be found and stolen.

When users do forget a password or need to reset an expired one, they can simply turn to the Identity Manager Web-based User Application to solve the problem. The User Application includes a self-service password-management feature that allows users to recover forgotten passwords and reset expired ones without the time and expense of a helpdesk call. The system can be configured to provide password hints and challenge/response question sets that validate user identity and permit authorized users to manage their own passwords in accordance with policy. As a result, users stay productive while IT administrators are relieved of the burden of password management.

Logging, Auditing and Reporting

Novell Identity Manager includes Novell Audit capabilities for centralized logging of identity-management activities for all connected systems and for the Provisioning Module. Reporting features provide easy access to and dissemination of this information. Novell Audit provides out-of-the-box approval workflow monitoring and reporting, and you can easily add more provisioning-related reports to meet your specific needs. The auditing component can also issue alerts when unauthorized access is attempted, alerting security personnel of potential breaches. This rich auditing and reporting functionality can be crucial to maintaining enterprise security, ensuring compliance with company policies, and documenting adherence to government and industry regulations.

Corporate White Pages and Organizational Chart

Novell Identity Manager enhances communication and collaboration between your employees, partners and customers by enabling them to find, connect with and communicate with people when they need to. The white pages and organizational charts delivered as part of the User Application allow users to search and view identity data by name or by skills, geography or organization. Identity information can also be viewed in the form of customizable corporate organization charts that facilitate drilling down to the details of each individual in the organization. Users can customize and save their own searches and views and can initiate contact directly from the displayed employee records. For enterprises that rely on employee collaboration, this can be a great time saver and productivity booster.

Novell Identity Manager enhances communication and collaboration between your employees, partners and customers by enabling them to find, connect with and communicate with people when they need to.

Deployment Scenarios

Novell Identity Manager streamlines and simplifies the process of managing your digital identities—wherever they reside—across all connected systems. As depicted in the following scenarios involving a fictitious enterprise, Digital Hospitals and Medical Centers (DH&MC), Identity Manager helps organizations increase efficiency and reduce costs associated with managing the entire user-identity lifecycle.

Scenario 1—Automatic Provisioning

Role-based Provisioning

When the human-resources manager at DH&MC enters a record in the human-resources system for Waldo Wilkes, a new physician at one of the organization's hospitals, Identity Manager automatically does the following:

- *Captures the information and applies DH&MC business rules to create the appropriate name formats and data replication in all connected applications and systems—for example, creating the name wwilkes based on the company's naming policy*
- *Creates accounts in other applications, which in turn provide authoritative identity information (For example, DH&MC has designated Microsoft* Exchange as the authoritative source for e-mail addresses. Based on this rule, Microsoft Exchange creates the e-mail address wwilkes@digitalhospitals.com, and Identity Manager communicates it to all of the other connected systems.)*
- *Transforms data into appropriate formats for each connected system—for example, formatting the phone number as xxx-xxx-xxxx in PeopleSoft* and as (xxx)xxxxxxx in Microsoft Exchange*
- *Applies the appropriate business rules to update all relevant information in all connected applications (For example, Identity Manager creates a Microsoft Exchange mailbox in the Austin, Texas, container because PeopleSoft—the authoritative source for location information—lists Austin as Wilkes' work location.)*

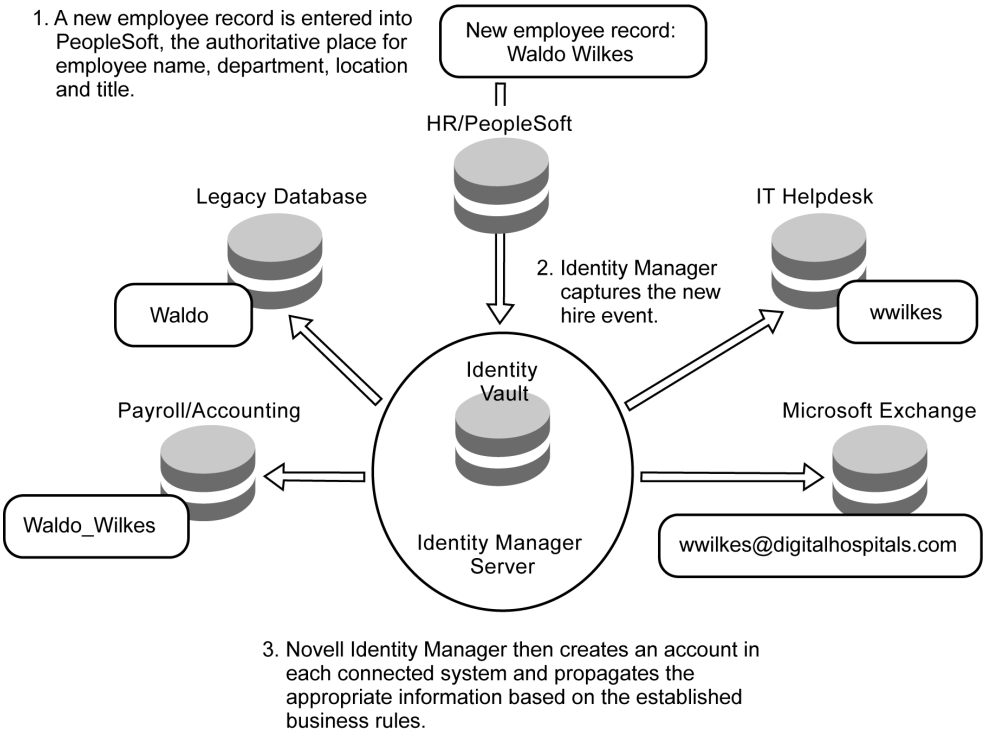

Figure 2. *Identity Manager Provisioning*

Workflow-based Provisioning

Wilkes also requires access to certain hospital information systems and patient-record databases that require approval from his departmental manager as well as the managers of the laboratory, radiology and other ancillary departments. Fortunately, there's no need to track down the manager and an IT administrator to secure this access. Wilkes simply opens the Identity Manager User Application, browses a list of the resources available to him, and requests access to the appropriate systems. He can track each of his requests as they make their way through the approval process.

Novell Identity Manager automatically sends an approval-request e-mail to Wilkes's manager, who clicks a link to call up the required approval forms and complete them online. The hospital chief of staff can also monitor approval requests and delegate approval to an alternate approver if Wilkes's departmental manager does not approve the request within a certain time period, or if he is currently unavailable for approval tasks. The process is repeated until all required approvals have been granted, and Identity Manager provisions Wilkes's access to the requested resources.

Reassignment and Reprovisioning

Waldo Wilkes' promotion to chief of staff at one of DH&MC's major hospitals automatically generates numerous changes in his identity information, based on a single entry in the authoritative source:

- *Wilkes is automatically given access to the new systems he needs as chief of staff.*
- *Access is instantly shut off from the systems he is no longer allowed to use.*
- *His new address becomes available in all the appropriate applications.*
- *His new manager is also automatically captured in connected systems. For example, financial applications are updated to reference his new manager in the expense-report approval process.*

Deprovisioning

When Wilkes decides to take early retirement, the instant his employee status is changed in the PeopleSoft database, Identity Manager immediately triggers the following events:

- *Disabling Wilkes' access to all hospital computer data and system resources*
- *Updating the security system to revoke access-card privileges for secure areas of the hospital*
- *Sending a notice to DH&MC's third-party benefit providers informing them of Wilkes' change in status*
- *Logging all these actions for reporting in Novell Audit, verifying that all access and privileges have been revoked in compliance with DH&MC policies*

Scenario 2—Self-service Password Management

Because of the User Application in Identity Manager, Wilkes' forgetting his password is not a problem. The User Application helps him to remember, create, change and reset his own password without calling the helpdesk and taking up an IT administrator's time.

When Wilkes visits the User Application, he is presented with one of the following administrator-defined options:

- **Password hint.** *The administrator can configure the product to deliver the hint on screen immediately or by e-mail.*
- **Password reset with challenge/response.** *One or more challenge questions are displayed on screen. These can include questions created by Wilkes himself, by the Identity Manager administrator or by a combination of both. When Wilkes answers the questions correctly, he is permitted to change his own password. The new password is automatically checked for policy compliance and then updated and synchronized with all eligible connected systems.*

Self-service capabilities enable both internal and external users to modify their own identity information—for example, to change an address or name.

Scenario 3—Corporate White Pages, Organization Chart and Self-service Profile Management

DH&MC needs to interact electronically with patients, insurance providers, suppliers and other external users. Identity Manager enables DH&MC to create a single virtual identity for every patient, medical professional, administrator and business partner, with corresponding access privileges based on the user's role and/or workflow-based approval.

Self-service capabilities enable both internal and external users to modify their own identity information—for example, to change an address or name—through the User Application served on the DH&MC Web site. Changes are then automatically synchronized across all connected DH&MC and partner systems.

Because Identity Manager employs the best security technologies available, these changes can occur in compliance with governmental regulations for patient privacy such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and International Standards Organization (ISO) 17799 in Europe.

The User Application also allows users to search on a variety of criteria to find other users and instantly make contact with them. Users can customize the display of search results to suit their needs—for example, choosing a "phone book," "org chart" or another type of display—and save their searches and displays for later use.

This gives users an incredibly powerful and flexible way to find people by job title, geographical area, special skills or other criteria. For example, a family doctor who needs to consult a gastroenterologist could browse the hospital organization chart by specialty and immediately launch a Novell GroupWise® session by clicking a link within the search results.

Architectural Overview

Novell Identity Manager simplifies user and password administration through the synchronization of identity information between applications. The applications (not to mention your business) gain the advantages of consistent, common identity without requiring modifications to the applications themselves. Using open standards, data can flow easily between applications and policies with business rules easily applied.

Key Identity Integration Concepts

Novell Identity Manager enables you to address the problems that arise in the typical business scenario of having isolated applications and systems distributed throughout an enterprise. Whether they're human-resource, e-mail, PBX or a multitude of other systems and data repositories existing in organizational or physical isolation, Identity Manager brings these diverse systems together. It gives you a unified identity-management infrastructure, eliminating the need to uproot and replace existing systems.

By enabling you to create associations and specify authoritative data sources, Identity Manager builds an identity interface among existing enterprise systems. This allows them to communicate with each other in a way that provides extraordinary data quality and improves the efficiency of your provisioning process.

Associations

Novell Identity Manager uses associations to virtually link identities across different systems. Associations are a list of identifiers contained by each object stored in Identity Manager. Each identifier contains three values:

- *A reference to a connected application*
- *A value that identifies the object or record in the connected application*
- *A value that identifies the status of connectivity for the object with the application*

The association value is supplied by each connected application and is unique to that application. No modification of the application's identifier is required and no foreign key values need to be introduced into it.

As an example, when Wilkes was hired in Scenario 1 above, his name, birth date, department and other information were entered in the human-resources system and an employee ID was automatically generated. Based on the business rules you define, Identity Manager responds to this creation event in the human-resources system and creates a new user identity in the identity vault with an association to the human-resources system.

Novell Identity Manager uses associations to virtually link identities across different systems. Associations are a list of identifiers contained by each object stored in Identity Manager.

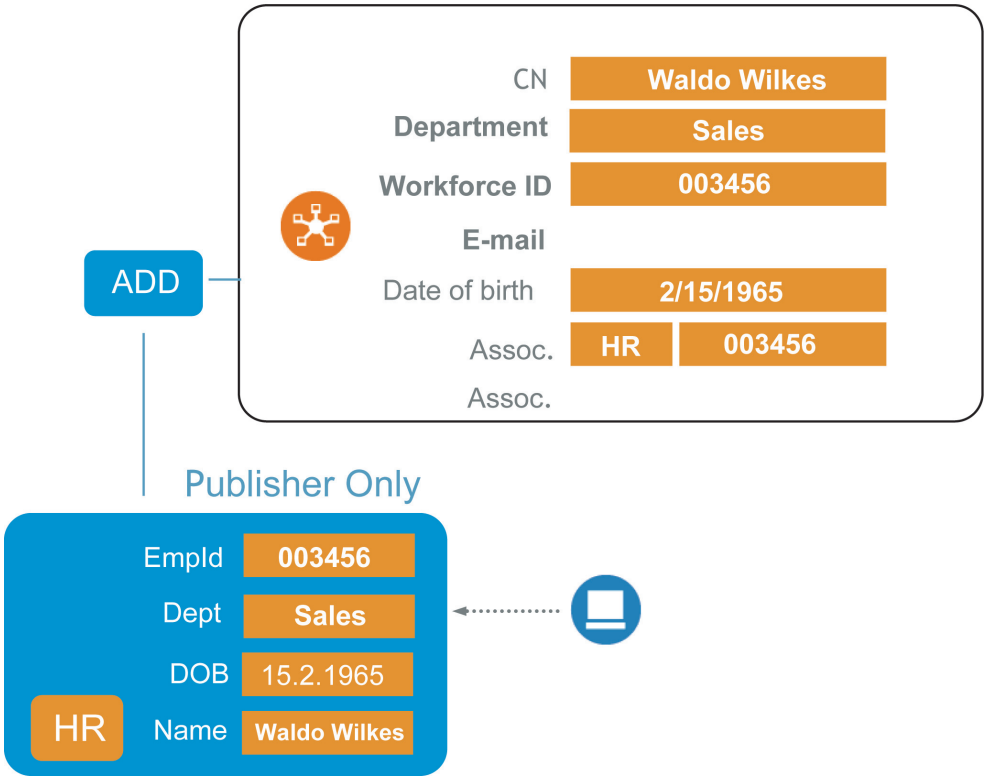

Figure 3. *Identity Manager establishes the initial association for a user created in the HR system.*

Through a set of business policies and rules that you've defined with Identity Manager, the e-mail account is automatically created with the proper associations in a way that allows Identity Manager to maintain a link between Identity Manager and the e-mail system.

In this example, a relationship between Identity Manager and the human-resources system is maintained by associating "HR" with the value of the unique employee ID (provided by the human-resources system) and storing this association as part of the identity. The combined value enables Identity Manager to establish, track and maintain the relationship between employee records in the HR system and in other connected systems—for example, the e-mail system.

To demonstrate how this works, extend the creation event that occurred in human resources to the e-mail system and create an e-mail account for Wilkes. Through a set of business policies and rules that you've defined with Identity Manager, the e-mail account is automatically created with the proper associations in a way that allows Identity Manager to maintain a link between Identity Manager and the e-mail system. In this case, the association reference stored in Identity Manager is "e-mail" and the unique association value is Wilkes's e-mail address, wwilkes@digitalhospitals.com.

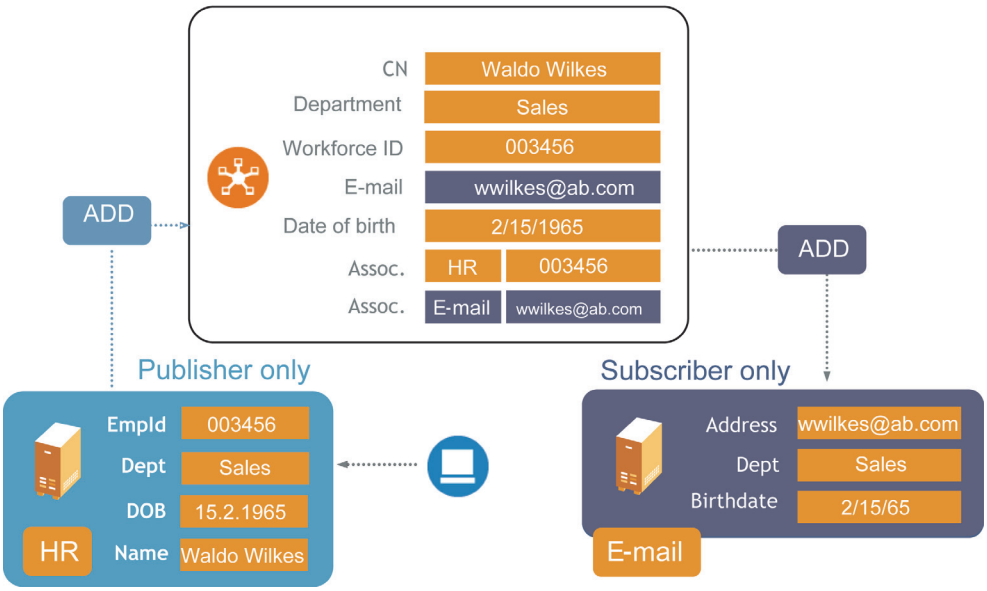

Figure 4. *Identity Manager establishes additional associations between a user in multiple applications.*

In addition to the link between the e-mail system and Identity Manager, a virtual or indirect link has been established between the e-mail system and the human-resources system. This virtual linking via unique association references enables Identity Manager to facilitate the automated sharing and synchronization of data between diverse systems—without requiring those systems to maintain each other's unique IDs and without the need to introduce foreign keys. Each link also includes a value indicating whether or not the link is currently active.

Each system provides the unique object ID for Identity Manager to use in its own system. Whatever that application is using for its unique key, Identity Manager stores that value in its association field. This gives you the ability not only to build a relationship between the individual users in each of these systems, but also to build relationships between the individual attributes themselves. Identity Manager becomes the virtual hub that links users and their identity objects to each of the different systems.

Authoritative Data Sources

Built on an identity-integration framework, Identity Manager connects multiple disparate systems to allow diverse applications in an enterprise to share common identity data. As the common identity data in an application is changed, the updated data can be distributed to all other applications that have a need for it.

Novell Identity Manager gives you the power and flexibility to define which systems are the authoritative sources for individual data elements so that only an authoritative data source can update a particular data item. For example, you could designate the human-resources application as the authoritative source for employee names and identification numbers and the e-mail system as the authoritative source for e-mail addresses. If a human-resources administrator tried to change an employee's e-mail address, Identity Manager would reject the change.

Novell Identity Manager supports authoritative data sources by giving you the ability to specify how and in which direction (either bidirectional or unidirectional) identity-provisioning information can flow.

Novell Identity Manager gives you the power and flexibility to define which systems are the authoritative sources for individual data elements so that only an authoritative data source can update a particular data item.

As an example of unidirectional flow, you can specify that an employee ID number can be communicated only from the human-resources system to Identity Manager—not from Identity Manager to the human-resources system. Unidirectional flow establishes an authoritative source for a data item—in this case, preventing employee IDs from being created or changed outside of the human-resources system. Bidirectional flow, by contrast, enables data items to be changed on either side of the link, enabling distributed authority and supporting existing administrative processes and ownership rather than forcing a particular user-administration model.

Novell Identity Manager supports authoritative data sources by giving you the ability to specify how and in which direction (either bidirectional or unidirectional) identity-provisioning information can flow.

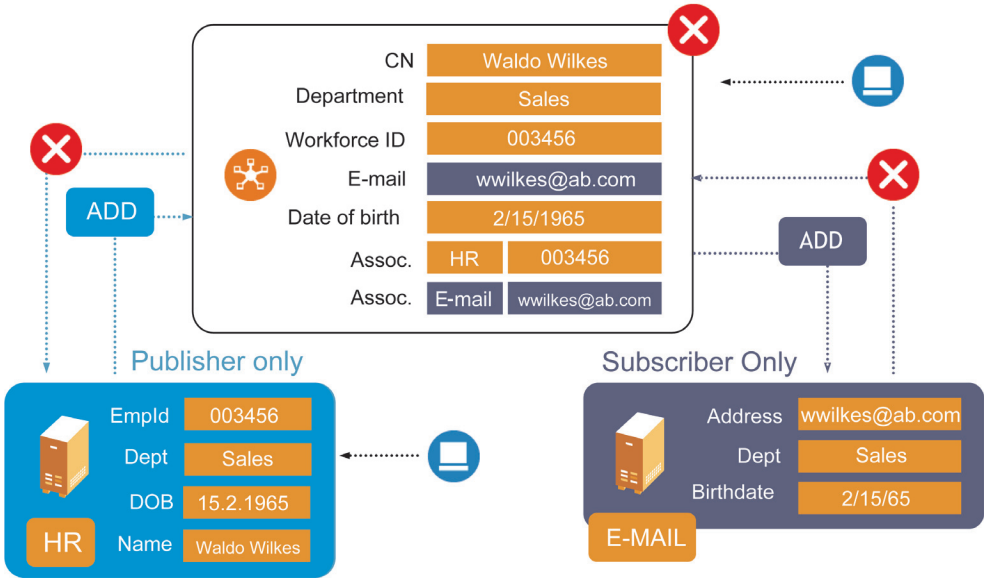

Figure 5. *Controlling the Flow of Information Between Connected Systems by Defining Authoritative Data Sources*

Solution Components

From a high-level architectural standpoint, Identity Manager consists of the following basic components and services:

- *Identity Vault*
- *Identity Manager Metadirectory Engine*
- *Directory Abstraction Layer*
- *Identity Manager Drivers*
- *Filters*
- *Policies*
- *User Application*
- *Searchable White Pages and Organization Chart*
- *Self-service Profile Management*
- *Self-service Password Management*
- *Lightweight User Administration Tools*
- *Workflow*
- *Delegated Administration*

Identity Vault

The identity vault is the repository that stores and maintains identity associations for each user as well as your policies that regulate how information is created and used. By maintaining the common data and associations for all connected applications, the identity vault enables each application (and its individual data requirements) to refer to a coherent set of identity values without needlessly replicating information across systems.

The identity vault facilitates this synchronization by hosting the metadata for your user identities and maintaining the relationships between your users and their applications through the use of associations. Policy definitions for your different connected system drivers, as well as password policies for your users, are also securely stored in the identity vault. By consolidating all this information in a secure, central repository, the identity vault does the following:

- *Enables centralized, unified identity management across all connected systems*
- *Allows many applications to share the same identity data, authentication method and authorization functionality*
- *Allows disparate applications to act as authoritative sources for portions of a unified identity that can then be distributed to other connected systems*
- *Lays a foundation for transparent yet secure access control*
- *Provides platform for role-based personalization based on rights*

Identity Manager Metadirectory Engine

The Identity Manager metadirectory engine is a join engine that interacts with the drivers of each of your connected systems. It also processes and handles all of the business logic for your defined policies. With the metadirectory engine providing synchronization and control, the identity vault can act as a virtual connection between applications. As the interface to the identity vault, the metadirectory engine does the following:

- *Supports the loading of multiple drivers*
- *Guarantees the delivery of events to receiving applications*
- *Provides loop-back detection to prevent endless looping data exchange between the connected application and the identity vault*
- *Performs recursive processing when an event generated by Identity Manager causes a connected application to respond with a similar event*
- *Through loop-back detection, prevents endless looping data exchange between your application and Novell eDirectory™.*

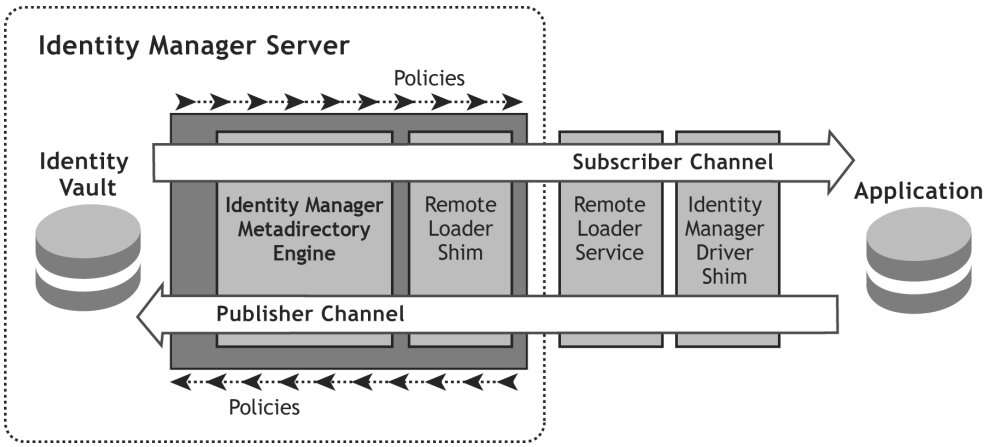

Figure 6. *Identity Manager Metadirectory Engine and Drivers*

Directory Abstraction Layer

The Directory Abstraction Layer is a communication layer that provides a logical view of the identity vault by mapping schema from the identity vault to User Application portlets. It also provides application-specific security and supports localization of the user interface.

The directory abstraction layer defines the objects and attributes that can be used in the User Application, how this data is displayed in the user interface and the relationships available to the organizational-chart portlet. These definitions are created via XML files that are built visually using the directory abstraction layer editor, a tool within Designer for Identity Manager, a new set of visual configuration tools.

Identity Manager Drivers

Identity Manager drivers are XML interfaces that integrate with connected applications through each application's standard public API. Drivers allow applications to communicate directly with the Identity Manager engine, an approach that makes Identity Manager significantly easier to implement than other solutions that require your applications to be modified to use the solutions' proprietary APIs.

Each driver is responsible for reporting object-change events that occur in the associated application. Some applications support an event system that drivers can employ. Others support a change log functionality that can be polled by the driver. Still other applications may support querying for any changes that have occurred since a particular point in time.

Regardless of how the driver determines that an application object has changed, the driver is responsible for constructing an XML document that describes the change. This document is then submitted to the Identity Manager engine via a publisher-channel interface. The engine processes these event-oriented documents according to the applicable rules and filters to create, modify or delete objects within the identity vault.

Identity Manager drivers provide a flexible, scalable method for synchronizing all kinds of identity information—either unidirectionally or bidirectionally—between all kinds of connected systems. Far more than just password synchronization, XML-based application drivers for Identity Manager make it possible to synchronize any identity-related attributes.

Far more than just password synchronization, XML-based application drivers for Identity Manager make it possible to synchronize any identity-related attributes.

The Policy Builder in Identity Manager gives you a simple point-and-click, browser-based interface that makes it easy for you to create policies that support and automatically enforce your organization's unique business.

The Remote Loader Service, which can run on a different server than Identity Manager, enables remote communication between drivers and the Identity Manager engine.

A driver can run either locally on the Identity Manager Server or remotely through the Remote Loader Service. The Remote Loader Service, which can run on a different server than Identity Manager, enables remote communication between drivers and the Identity Manager engine.

Policies

Policies enable you to control and automate the flow and transformation of identity information between connected systems in accordance with your defined business processes and rules.

Government regulations, business risk management and the unique needs of your enterprise all contribute to the organizational policies and business practices that you've established for managing user access rights as well as the creation, modification and deletion of user accounts. Without Identity Manager, however, it can be difficult to consistently enforce those policies and carry them out in a timely manner across all the data sources, applications and services throughout your enterprise.

The Policy Builder in Identity Manager gives you a simple point-and-click, browser-based interface that makes it easy for you to create policies that support and automatically enforce your organization's unique business. These policies ensure the proper and automatic synchronization of information across every designated directory and application in your enterprise and beyond, facilitating your ability to keep your identity information consistently accurate and up to date.

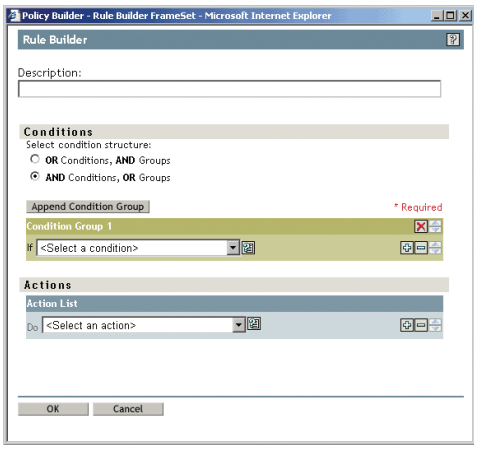

Figure 7. *Configuring Identity Manager Policies with Policy Builder*

Rules, Policies and Policy Sets

A high-level transformation is defined by means of a "policy set." Each policy set consists of one or more "policies," which in turn contain one or more "rules" that each describe an individual set of conditions and actions. To summarize:

- *A rule consists of a set of conditions to be tested and an ordered set of actions to be performed when the conditions are met.*
- *A policy consists of an ordered set of rules.*
- *A policy set is a collection of multiple policies of the same type, chained together with one control point such as a placement policy.*

Filters

A filter is linked to each driver object to define the policies that control what data is to be synchronized between an application and the identity vault. The filter enables you to control whether changes to one of an individual's identity attributes will be synchronized with other systems or ignored. Filters also give you the option to simply notify Identity Manager of a change, allowing policies to use information regarding a data change even though there is no intention of actually synchronizing the information with other systems. Filters also have controls that allow you to specify which system is the authority over a particular element in the event of a conflict during a merge between entities in two different systems. This authority also controls resetting of the value for a specific data item when someone may have inadvertently made a change within the connected system that was against your business policy.

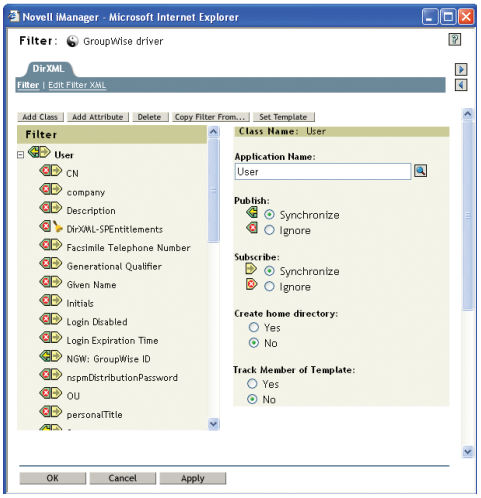

Figure 8. *Defining Filters*

User Application

The User Application runs in a Web-based browser environment, providing a simple and accessible interface for users to manage their own profiles and passwords and to look up identity information for other users. It includes the following:

- *Searchable white pages and organization charts*
- *Self-service profile management*
- *Self-service password management*
- *Lightweight user administration tools*
- *Workflow-based provisioning*

The filter enables you to control whether changes to one of an individual's identity attributes will be synchronized with other systems or ignored.

Identity Manager allows users to search and display employees, partners and customers by name, job roles, skills, user groups, business relationships and more.

Users can be authorized to manage their own profiles, and department managers and team leaders can be authorized to manage the profiles of their subordinates.

Searchable White Pages and Organizational Charts

More than a static list of employees, Identity Manager allows users to search and display employees, partners and customers by name, job roles, skills, user groups, business relationships and more—all in an interactive, graphical format. Each user or group is represented by a virtual "business card" with relationships indicated by a "tree" structure that can be expanded and collapsed to navigate the whole organization level by level. To view the chart, the user chooses "Organization Chart" on the Identity Self-Service tab of the User Application.

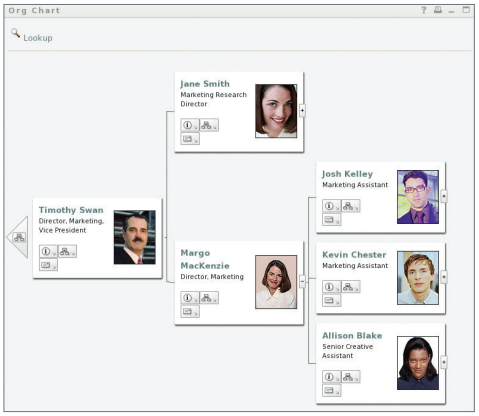

Figure 9. *Browsing the Organization Chart*

A lookup link at the top-left corner of the chart facilitates easy location of any search criteria that the system is configured to support and that the user is allowed to access. Another way to search is by choosing "Directory Search" on the Identity Management tab.

You can enter search criteria and even save particular searches for later use. For example, if employee records contain information such as geographical location and languages spoken, and if the administrator has configured the system to allow searches on these attributes, you could search for users in the St. Louis area who speak German. You could save this search and later modify it to find German speakers in Toronto.

Organization charts and search results can be displayed in configurable views. For example, an employee could be displayed in the context of the user groups he belongs to or in the context of his manager and subordinates. Users can create these customized views to suit their own needs and save them for later use.

A control button on each "business card" allows you to display an individual's profile details—for example, name, title, department, region, manager, e-mail address, telephone number and any other information the system has been configured to display. Another control button addresses an e-mail to the individual or to a manager's entire team with a single click.

Figure 10. *Detailed User Profile*

Self-service Profile Management

Users can be authorized to manage their own profiles, and department managers and team leaders can be authorized to manage the profiles of their subordinates. Because users know their own information better than

anyone else, self-service profile management helps keep identity information accurate and current. Moreover, there's no need to request an IT administrator to make changes and then verify them, which saves both the user's and administrator's time.

To edit your own profile, simply choose the My Profile page from the Identity Self-Service tab of the User Application. The user's own detail page appears, and the user can modify any information that is authorized for self-service. Authorized managers can access and modify profiles for all employees in their groups.

Self-service Password Management

Because Identity Manager enables employees to access all provisioned systems with a single password. With only one password to remember, employees are less tempted to create passwords that are too easy for others to guess—or to write passwords down where they can be stolen. However, passwords can still be forgotten, especially if company policy requires that passwords be periodically changed.

Novell Identity Manager includes self-service password-management features that make it easy for users to manage their own passwords. Administrators can create, view and assign password policies and configure the system to allow users to do the following:

- *Set or change their own passwords in response to challenge questions that verify user identity. These challenge questions can be defined by the administrator (for example, "enter your employee number"), the user (for example, "enter your mother's maiden name") or both.*
- *Recover their forgotten passwords via a hint. Users can set their own hints, and the administrator can choose to have them delivered immediately on-screen or by e-mail.*

In all cases, Identity Manager enforces password length, format, expiration period and other characteristics as defined by the administrator. According to defined policy, passwords can either apply to a single system or be propagated bidirectionally across all eligible connected systems. (An "eligible" system is one that supports the creation and update of passwords and possibly other information through its published API.) Users can access these features by choosing the Password Management page from the Identity Self-Service tab of the User Application.

Lightweight User Administration Tools

Novell Identity Manager goes beyond managing identity and provisioning resources for just your employees. You can also use it for temporary workers, contractors, interns, business partners, customers and others outside the enterprise, managing their identities and giving them consolidated access to the resources they need.

Lightweight user administration tools in Identity Manager enable you to manage users who weren't created in another authoritative source. For example, you can use these tools to give business partners access to the self-service features and application resources they need without having to create a record for them in your human-resources system.

This makes it easy to integrate non-employees into Identity Manager for easy management of all business contacts. It also simplifies provisioning new hires with the resources they need to be productive from day one—adding more identity information and resources as time permits and as employee roles change. Identity Manager adapts to the precise needs of your organization and of each user—both inside and outside the enterprise.

Novell Identity Manager goes beyond managing identity and provisioning resources for just your employees. You can also use it for temporary workers, contractors, interns, business partners, customers and others outside the enterprise.

Designer offers a wealth of powerful design and configuration tools, all accessible through a graphical interface featuring drag-and-drop editing within a familiar environment of views, tabs and menus.

Configuration and Administration

Novell Identity Manager includes two powerful configuration and administration tools:

- **Designer for Identity Manager** *provides a visual design and configuration environment that works outside the production environment and is perfect for system architects, consultants, developers and modelers.*
- **Novell iManager** *provides a Web-based visual environment for administering Identity Manager in the live environment.*

Designer for Identity Manager

Designer is an Eclipse-based rich client that allows you to visually configure, customize and test your Identity Manager implementation independently, without affecting the live environment. It's the right tool for system architects, business analysts and consultants to create and manage users, objects and other entries in the identity vault. It's also ideal for configuring enterprise-specific policies, workflows and provisioning processes.

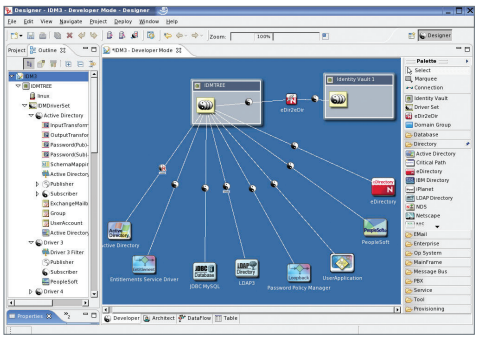

Figure 11. *The Designer User Interface*

Designer offers a wealth of powerful design and configuration tools, all accessible through a graphical interface featuring drag-and-drop editing within a familiar environment of views, tabs and menus. Some of Designer's tools and functions include the following:

- **Project management.** *Use the Project Management area to create, copy or delete projects. You can work on multiple projects at the same time and copy existing projects to use as templates for new projects. There's also a wizard for creating new projects.*
- **Enterprise modeler.** *This feature provides a "big picture" graphic representation of all elements in your Identity Management environment. GUI features such as drag-and-drop make it easy to configure and revise the Identity Manager environment in both architect and developer modes.*
- **Configuration management.** *Designer gives you an easy way to edit properties and global configuration values for the identity vault and application drivers while keeping an eye on the project as a whole.*
- **Import/deploy/export.** *This function allows you to import an existing Identity Manager solution from the identity vault into a project; to import driver sets, drivers, policies and channels; to export driver sets and drivers to a file; to deploy identity vaults, driver sets, drivers, policies or channels; and to manage multiserver environments.*
- **Dataflow modeler.** *This unique feature provides a graphical representation of the objects, object classes and attributes in your project, along with the data flow between these elements. You can manage the data flow by using drag-and-drop functionality to determine the desired relationships and dependencies.*
- **Policy management.** *Designer offers powerful tools for creating, viewing and managing policies for your organization. You can view the policy flow between connected applications and the identity vault; view individual policies in each policy set; and reorder, add or delete policies via a policy script using Policy Builder. Designer also offers a read-only view of policy script conditions and actions, as well as an XML editor for schema maps, filters,*

global configuration values and transformation policy sets.

- **Policy simulation.** *Identity Manager is the only solution available that allows you to test policies in a non-production environment using a real instance of the Identity Manager engine. Designer enables complete policy simulation, including customizable XML input, query simulation, trace output and logging, the ability to call external Java* classes, and simulation by policy set.*
- **Directory tools.** *Designer supports schema management by enabling you to browse the identity vault, import schemas from the vault, and manage schema classes and attributes offline from the production system.*
- **Directory abstraction layer editor.** *Directory abstraction layer editor is also available from within Designer. It provides a graphical interface for defining the relationships that enable Identity Manager to mediate between the unique data representations within different connected applications. Use directory abstraction layer editor to define entities, which are representations of objects in the identity vault—such as users, groups, organizational-chart relationships, devices and so on. For each entity, directory abstraction layer editor allows you to define the attributes that will be used in the directory abstraction layer. This enables data and relationships from multiple connected applications to be displayed in a consistent way in the directory abstraction layer.*
- **Documentation.** *Designer automatically generates technical documentation in PDF format, listing all the implementation details for your organization. You can customize the content and format of the documentation output using the included wizard or XSL:FO, and you can include Enterprise Modeler screenshots for a visual representation of your implementation. You can also control the amount of detail included in the output to create various levels of documentation.*

Novell iManager is a browser-based application for managing Identity Manager in a live environment. It enables location-independent management for all identity vault objects, schema, partitions and other resources.

Novell iManager

Novell iManager is a browser-based application for managing Identity Manager in a live environment. It enables location-independent management for all identity vault objects, schema, partitions and other resources. With the Approvals plug-in, you can manage workflow-based approval processes using the same Web-based graphical interface. With iManager, you can do the following:

- **Administer the metadirectory system.** *The metadirectory system performs all processing required to automatically initiate and fulfill provisioning requests and those requests triggered from the Provisioning Module. Once policies are applied and the applicable approvals have been given, the provisioning system provisions the resource as requested.*
- **Create and activate application drivers and the User Application driver.** *Application drivers are required to connect individual applications to the Identity Management environment. The User Application driver is responsible for starting provisioning workflows in the Provisioning Module and for notifying the User Application of changes in the identity vault. For example, when a new hire is entered in the human-resources system and a corresponding account is created in the identity vault, the User Application driver can trigger a workflow event within the Provisioning Module to automatically request all the resources that require approval.*

The security system handles all aspects of security for a workflow-based provisioning application.

- **Add the Identity Manager application to the Novell Audit server as a log application.** *This enables Audit to report on Identity Manager user activities.*
- **Write queries to run reports against logged data.** *You can also use predefined reports or write your own SQL queries.*
- **Define password self-service policies.** *Examples include specifying password format, hint definitions for recovering forgotten passwords, and challenge/response policies for changing passwords.*
- **Manage the Provisioning Module.** *The Provisioning Module is an add-on to the standard Identity Manager package. When a policy requires one or more approvals, the Provisioning Module coordinates the approval process. During the course of processing, it interacts with the Workflow Database, Scripting Engine, Novell Audit, SMTP and the security system.*
- **Manage the scripting engine.** *The workflow system calls the scripting engine whenever a workflow includes a dynamic expression that must be evaluated. Dynamic expressions can include variables, functions and operators, as well as references to entities in the directory abstraction layer.*
- **Configure and manage Novell Audit.** *To log information about the state of a workflow process, the workflow system interacts with Novell Audit. During the course of its processing, a workflow may log information about various events that have occurred. Users can then use the Novell Audit reporting tools to extract custom reports on the logging data. Crystal Reports* or other JDBC*-compliant reporting tools can also be used to access the Novell Audit database and write reports.*
- **Manage templates for e-mail notification (SMTP).** *A workflow process often sends e-mail notifications at various points in the course of its execution. For example, an e-mail might be sent when a user assigns a workflow activity to a new addressee. To enable this, you can create an e-mail template in iManager and then use this template in a workflow process. Once the template has been created, the workflow system retrieves it from the identity vault and replaces tags with dynamic text suitable for the notification. These notifications are handled through SMTP.*
- **Manage security.** *The security system handles all aspects of security for a workflow-based provisioning application. It protects provisioning and workflow objects from unauthorized use and ensures that the user sees only those provisioning request definitions to which he or she has been granted access. It also allows you to designate delegates to perform specific provisioning work on behalf of another user as well as to authorize proxies to do the same.*
- **Workflow database.** *To track the state of workflows in process, the workflow system stores information in a database. This component is automatically installed and configured. (It is not configured through iManager.) It works behind the scenes to track workflows in process, worklists (queues), workflow addressees and comments added during a workflow process.*

Workflow-based Provisioning

Workflow-based provisioning is the process of managing user access to secure resources in an organization. These resources may include digital entities such as user accounts, applications, databases and distributions lists as well as physical resources such as office space, computers and cell phones—in short, virtually anything the enterprise may need to provide authorized users.

The process of workflow-based provisioning begins with a provisioning request, which is a call to grant or revoke access to organizational resources. Provisioning requests can be initiated directly by end users through the User Application or indirectly in response to events occurring in the identity vault.

When a provisioning request requires approval by one or more individuals in an organization, the request initiates a workflow that automatically coordinates the approvals needed to fulfill the request. Some provisioning requests require approval from a single individual, others may require approval from several individuals (either in sequence or in parallel), and still others may be fulfilled without any approvals.

All of these workflow paths and options can be configured through iManager tools that you can use to build provisioning capabilities into the User Application. These tools give you the ability to configure provisioning requests and also manage workflows that are in process. There are three basic steps in the workflow process:

- *Initiating the request*
- *Approving the request*
- *Fulfilling the request*

Initiating the Request

In the User Application, you will browse a list of resources by category and select one to provision. In the identity vault, the requested resource is bound to a provisioning request definition. This provisioning request definition binds a provisioned resource to a workflow and acts as the means by which the workflow process is exposed to the end user. The provisioning request definition contains all the information required to display the initial request form to the user and to start the flow that follows the initial request.

For example, when a user selects the cell phone request resource, the User Application retrieves the initial request form and the description of the associated initial request data from the provisioning system, which gets these objects from the provisioning request definition. The user completes the request form and clicks to submit it, and the provisioning system creates a workflow that tracks the user who initiated the request, the resource that is being provisioned and the requested operation—either to grant or revoke access to the resource.

Approving the Request

Once the user has initiated a request, the provisioning system starts the workflow process. The appropriate workflow definition coordinates the approval by linking workflow activities together in one or more logical chains, passing data between these activities to build the complete workflow required to approve the request according to your company policies. Workflow activities involved in approving the request include the following:

Provisioning requests can be initiated directly by end users through the User Application or indirectly in response to events occurring in the identity vault.

You can use either iManager or Designer to define creation policies, default-naming policies, placement policies, initial-password policies, schema-mapping policies, event-transformation policies and more.

- **User activities.** *A manager or other user may need to take one or more explicit steps for approval to be granted. After the start activity finishes execution, the workflow system forwards processing to the first user activity defined in the flow. The system then displays a form that enables the user the ability to act on the request by doing one of the following:*
  - Approve
  - Deny
  - Refuse
  - Reassign

  Users may opt to receive approval requests by e-mail and can take action simply by clicking a URL in the message. If the user approves the request, control is forwarded to the next activity in the workflow. If no further approvals are needed, the resource is provisioned.

  If the user denies the request, the workflow process terminates. The user can also refuse the task, returning the request to the person who initiated it. Or, the user can reassign the task, which puts the workflow item in another user's queue. Timeout intervals can also be specified; if a user doesn't respond during the specified interval, the process can be terminated, the activity can be automatically retried, or the activity can be escalated to another user, such as a supervisor.

- **Conditional activities.** *During the course of execution, a workflow process may perform a test and check the outcome to see what to do next. The conditional activity provides this capability. Conditional activities use a scripting expression to define the condition to evaluate.*
- **Branch and merge activities.** *In a workflow that supports parallel processing, the branch activity allows two users to act on different areas of the workflow item in parallel. Once the users have completed their work, the merge activity synchronizes the incoming branches in the flow.*

Fulfilling the Request

Once a provisioning request has been approved, the workflow system can begin the provisioning step. At this point, control passes back to the provisioning system. To fulfill the provisioning request, the provisioning system may execute an entitlement (see the next section) or directly manipulate an identity vault object and its attributes. During the provisioning step, the system creates any related objects and records the results of the provisioning action on the recipient, as specified in the provisioning data definition.

Creating Policies

You can use either iManager or Designer to define creation policies, default-naming policies, placement policies, initial-password policies, schema-mapping policies, event-transformation policies and more.

Policy rules are defined in the Rule Builder window of Policy Builder. This interface enables you to quickly create and modify rules using intelligent drop-down menus. In Rule Builder, you define a set of conditions that must be met before a defined action occurs. Policy Builder also lets you easily construct complex conditions or argument expressions for your rules by using the dynamic Argument Builder graphical interface.

All policies are defined using this basic procedure:

1. *The configuration tool presents you with a list of available drivers.*
2. *You select the driver for the system or application for which you are creating a policy.*

3. *Policy Builder displays a graphical representation of available policies within a flow chart.*
4. *You select the policy that you want to define and then follow the instructions. Policy types are described below.*

Transformation Policies

Transformation policies are used to transform data or events, changing the way they are represented as information is shared between Identity Manager and a connected application. There are four types of transformation policies:

- *[Data] output transformation gives you the ability to manipulate data as it is being pushed out to the application.*
- *[Data] input transformation allows you to manipulate data as it is coming from the application.*
- *Event transformation allows you to change the event type, such as changing an event to delete an account into an event that disables an account.*
- *Command transformation allows you to apply any manipulation policy against data that is coming through, including an exit routine to an external process.*

Schema-mapping Policies

The schema-mapping policy allows you to create a relationship between similar attributes in different systems. For example, even though an employee's date of birth might be referred to as "DOB" in the human-resources system, "Date of Birth" in the identity vault and "Birthdate" in the e-mail system, schema-mapping policies enable you to establish the appropriate relationship between these attributes.

Matching Policies

Matching policies allow you to define the minimum criteria that you need to build an association with users that already exist in your source system and in your identity vault. Matching policies are typically used when you first implement Identity Manager, enabling you to dynamically link and build the proper associations for the multiple identity instances that exist in your different systems.

Each of your applications might have different requirements as to the minimum information needed in order to create a user or entity within the application.

Creation Policies

Creation policies are responsible for defining the minimum information that needs to exist for you to be able to create an object in a target system. For example, in a Novell eDirectory system, the minimum information you might need is surname, while the minimum information you might specify for Active Directory* could be the full name. Each of your applications might have different requirements as to the minimum information needed in order to create a user or entity within the application. A creation policy also allows you to apply other types of policies that are relevant to creating a user for the first time, such as being classified as a certain group member and being assigned the access rights associated with that group.

Placement Policies

Placement policies let you specify where new objects are created in connected applications. For example, a placement policy would be used to select a container for newly created users in a hierarchical directory tree. If a driver is set up to be bidirectional, a placement policy is required on both the publication and subscription channels.

Reusing and Sharing of Policies

Policies constructed with Policy Builder are created as components and can be easily reused, shared and leveraged for any future policy creation activities. This saves time and effort for your IT staff, eliminating the need to perform repetitive policy creation tasks for different systems in your enterprise that use the same or similar policies.

Policies constructed with Policy Builder are created as components and can be easily reused, shared and leveraged for any future policy creation activities.

With entitlement-based provisioning, the appropriate changes are triggered automatically when someone's role changes in the identity vault or when a provisioning request is approved.

Entitlement-based Provisioning

Entitlements provide a method for provisioning resources based on the needs of users in specific workgroups or functional roles within the organization. With entitlement-based provisioning, the appropriate changes are triggered automatically when someone's role changes in the identity vault or when a provisioning request is approved. Entitlements can support both role-based and workflow-based provisioning:

- **Role-based entitlements** *provide a centralized model for administering business policies, reducing the need to configure all the individual drivers for your connected systems. Role-based entitlements let you define what access rights the different roles in your organization will have, automatically assigning those rights to individuals designated with that role and revoking them when they leave that role. These entitlements can include user accounts, membership in e-mail distribution lists, group membership and attribute values for corresponding objects in connected systems. Membership within a role can be granted dynamically based on a condition or statically based on inclusion/exclusion.*
- **Workflow-based entitlements** *can be incorporated in the workflow-based provisioning process described in the previous section. These work similarly to role-based entitlements and are supported by the same application drivers. The difference is that workflow-based entitlements depend on human approval rather than on membership in a role.*

You can create, modify or delete entitlements using iManager or Designer—either manually or using a wizard. Entitlement consists of named XML flags that cause a supported application driver to perform one of several actions:

- *Create/delete/enable/disable an account*
- *Grant/revoke membership in a distribution list*
- *Grant/revoke group membership*
- *Add/remove attributes for the corresponding objects in connected systems, populated with values you specify*
- *Other entitlements that you customize*

An entitlement itself doesn't grant access to anything. Instead, entitlements are "notes" that tell application drivers what to do. The application drivers must be set up with the capability to act upon this information. While any driver can support entitlements, Identity Manager ships with the following drivers preconfigured for entitlement support:

- *Novell eDirectory*
- *Active Directory*
- *Exchange*
- *Novell GroupWise*
- *LDAP*
- *Lotus Notes**
- *NIS*
- *NT Domains*

Dynamic and Static Membership Creation

Role-based entitlements give you the option to have role membership determined either dynamically or statically. Dynamic memberships are defined by the inclusion or exclusion of a combination of attributes. For example, you can define criteria for membership based on attribute values of the user, such as whether their job title includes the word "manager."

Users who meet the specified criteria are automatically part of the role without requiring you to specifically add each user to the role. If an object changes so that it no longer meets the criteria for membership, the entitlements are automatically revoked.

The criteria you specify are automatically converted into an LDAP filter. The dynamic membership is the same as a dynamic group object.

In addition to creating criteria for dynamic membership (an LDAP filter), you can statically include or exclude specific users. You can add members statically who don't meet the criteria of the filter. You can also exclude members who meet the filter's criteria but who, for some other reason, should not be included in the entitlement policy.

Flexible Policy Management

Entitlements also give you the flexibility to control what it means when an account on a connected system is granted or revoked for a user. Each driver provides a list of supported choices for the meaning of "add" or "remove." For example, when adding a GroupWise account, you could specify that "add" actually means to grant the user an account in a disabled state so that the administrator must intervene before the user can access the account. Another choice for the GroupWise driver is "enabled," which is the default.

Determining Your Policy Management Approach

You should carefully analyze your environment to determine whether role-based entitlements and/or workflow-based entitlements are appropriate for use in conjunction with custom policies developed with Policy Builder. With good design, you can take advantage of both methods. The important thing to remember is that the driver configurations for individual connected systems created with Policy Builder always preempt policies based on entitlements. If the methods create conflicting policies, rules defined by Policy Builder for a specific connected system always take precedence over any defined entitlements. With Identity Manager, however, Novell generally recommends triggering provisioning requests from the Provisioning Module to the metadirectory engine through the use of entitlements.

You should carefully analyze your environment to determine whether role-based entitlements and/or workflow-based entitlements are appropriate for use in conjunction with custom policies developed with Policy Builder.

Password Management

When employees have to remember multiple passwords for the different systems they need to do their jobs, the security of your digital resources is at risk. Regardless of the password policies you have established, users will continue to physically record their multiple passwords on sticky notes, in notebooks or on scraps of paper that can easily be found by determined intruders. The answer to this predicament is a password-management solution that enforces password policy while eliminating the need for users to remember multiple passwords.

Novell Identity Manager addresses your password-management concerns, automatically enforcing the password policies that you define and eliminating the need for users to keep track of multiple passwords. It enables users to have a single password for every configured system across your enterprise. When the user resets a forgotten password or changes it in response to a forced periodic change, the new password is distributed to and synchronized with all eligible connected systems. Identity Manager allows users to recover and reset their own passwords securely—without taking an IT administrator's time.

According to Giga, it costs an organization $25 to $50 every time a user calls the helpdesk with a password-related problem. An *eWeek* study puts the cost at $45 each time a password has to be reset because a user has forgotten it.

Novell Identity Manager provides you a suite of password-related security functions:

- **Enterprise-wide Password Policy Enforcement** for strengthening enterprise security by ensuring adherence to password policy on all connected systems
- **Password Self-service** *to empower end-users to help themselves with forgotten passwords, password resetting and password changes*
- **Bidirectional Password Synchronization** *to enable consistent distribution and synchronization of user passwords on specified connected systems, as established in the organization's defined password policy*

Enterprise-wide Password Policy Enforcement

Novell Identity Manager enables you to define password policies that can be automatically applied enterprise-wide or to specific groups of users. A new or changed password is not accepted unless it conforms to the policies you have established.

Some examples of the password controls you can implement through Identity Manager include thresholds for minimum and maximum number of characters, minimum number of uppercase characters and minimum number of numerals. You can also create an exclusion list of passwords that users are not allowed to use, and you can prohibit reuse of passwords that have previously expired or been changed.

If someone updates a password in a connected system in violation of password policy, Identity Manager has the ability to address the violation in several ways. For example, you can configure Identity Manager to reset the user's password back to the last known valid password, inform the user of the invalid password, require a password reset, block user access or take other appropriate actions.

Self-service Password Management

According to Giga, it costs an organization $25 to $50 every time a user calls the helpdesk with a password-related problem. An *eWeek* study puts the cost at $45 each time a password has to be reset because a user has forgotten it. Other studies indicate that that an average large, decentralized company with four to eight applications spends nearly 50 minutes of helpdesk time per user, per year just managing passwords. For an organization with 10,000 users and an average helpdesk pay rate of $15 per hour, this translates into $125,000 wasted annually in managing passwords.

Employee productivity suffers when users forget their passwords and waste time on the phone with the helpdesk, waiting to have their passwords reset. Studies indicate that 70.4 percent of all users call the helpdesk at least once a month to get help with a password—the average call lasting 25.2 minutes. For an organization with 10,000 users and an average employee pay rate of $15 per hour, that results in $532,224 worth of lost productivity.

Novell Identity Manager self-service password management puts you in a position to drastically reduce the number of password-related calls made to your helpdesk, avoiding productivity losses and administration costs. When passwords are forgotten or expire, Identity Manager lets users recover and reset their own passwords—without assistance from the helpdesk—using the Identity Manager User Application or the native password management interface of their connected systems. As a result, employees can stay more productive, your call center can be more responsive to other issues, and your IT staff can minimize busywork and put more effort into strategic projects for the business.

Self-service Password Reset

Novell Identity Manager provides a wizard that administrators can use to configure challenge questions and response options that users must use to prove their identity before they can change their passwords. Challenge options can include any combination of the following:

- **Administrator-defined questions.** *You can create a set of challenge questions to be presented to users wanting to change their passwords.*
- **User-defined questions.** *You can specify that one or more questions must be created by end users themselves.*
- **Random questions.** *When first configuring their own forgotten password challenge sets, users provide answers to an extensive set of questions. However, when trying to change or reset a password, only a random subset of these questions is presented to the user. This can help prevent unauthorized users from figuring out the answers to a known set of challenge questions.*
- **Mandatory questions.** *Administrators can specify that certain mandatory questions must be included in the challenge set, even if other questions are random.*

The Change Password portlet is displayed upon login whenever a user needs to create a new password or reset an invalid one. You can also choose to have give users self-service access to the portlet whenever they decide they want a new password, or you can set expiration times and other policies that automatically display the portlet and require the user to change passwords. If a user forgets a password, you can require a password change or you can use the hint feature described below.

To help users create compliant passwords when they change or create new passwords, the self-service portlet automatically displays your organization's password compliancy policies.

Novell Identity Manager can automatically synchronize passwords across connected applications, giving users just one password to remember.

Forgotten Password Hint

Identity Manager also gives you the option to allow password hints that help users remember forgotten passwords. If this feature is implemented, users can set up their own hints through a self-service portlet. You can configure the portlet to appear automatically when a user logs in and a hint hasn't yet been established, and you can also grant users the option to change their hints anytime from the User Application. Hints can be displayed immediately onscreen or delivered by e-mail for greater privacy.

Notification

Novell Identity Manager also provides a set of five customizable notification templates that can be used to send e-mail notices to your users when certain password-related events occur, such as password expiration, password synchronization failure and failed password resetting.

Bidirectional Password Synchronization

Novell Identity Manager can automatically synchronize passwords across connected applications, giving users just one password to remember. The process for password synchronization proceeds as follows:

1. *The user uses the self-service password portal provided by Identity Manager or the native password change interface of a connected system to set or change the password.*
2. *The new password is checked for compliance with your company's defined password policies.*

Identity Manager also gives you the option to allow password hints that help users remember forgotten passwords.

Novell Identity Manager can greatly simplify password management and end-user convenience by pushing passwords out unidirectionally to these connected systems.

3. *If it complies, the password is set on the user object in the identity vault and the password is distributed to associated user objects on all eligible connected systems.*
4. *If the password does not comply, a failure notice is sent to the user via e-mail and the password is reset on the systems to the most recent valid password.*

Bidirectional Password Synchronization

The following connected systems are eligible and provide full support for bidirectional password synchronization, meaning that the user can initiate a password change within the native password interface of any of these systems:

- *Windows NT* (NT Domains)*
- *Windows* 2000 (Active Directory)*
- *Windows 2003 (Active Directory)*
- *Novell eDirectory (all platforms)*
- *NIS (UNIX*, Linux*)*

Other connected systems can't provide the user's actual password directly to Identity Manager. However, you can still configure other systems to provide a password to Identity Manager via a policy defined in Policy Builder. For example, when a new user is created in PeopleSoft, a policy could be defined that specified an initial password based on last name or employee ID.

Unidirectional Password Synchronization

Additionally, different systems have varying abilities to accept a password from Identity Manager and thus have limited eligibility. Some systems support initial password set for new accounts, but not password-modify events. Others support both. Regardless of which it is, Identity Manager can greatly simplify password management and end-user convenience by pushing passwords out unidirectionally to these connected systems. See the password synchronization of the Identity Manager documentation for complete details on password support for each connected system.

Configuring Password Synchronization

Password synchronization within Identity Manager is configured on a per-application basis. The advanced password rules for password synchronization in Identity Manager give you the following setting options for each driver you configure:

- *Accept passwords published by a connected system.*
- *Enforce policies on passwords coming in from a connected system. If it doesn't comply, don't accept it.*
- *Enforce policies on the connected system by resetting noncompliant passwords.*
- *Notify users when password synchronization is unsuccessful.*

Additionally, as with other attributes for a user account, you can choose your authoritative data sources for password synchronization.

Logging, Reporting and Auditing

Novell Identity Manager provides secure logging and auditing of identity-management activity. This audit data can be useful in lowering liability and risk associated with regulatory compliance and your own business policies. A license to send data to Novell Audit and to do light reporting of Identity Manager events from Novell Audit is included with Identity Manager. Novell Audit data can be centrally collected in a MySQL* database or a flat file. A filter setup wizard helps you configure the events for which you want to receive reports and notifications. Notifications can also be delivered real-time via SMTP.

The inclusion of these Novell Audit capabilities simplifies your efforts in tracking and logging what's actually happening across your enterprise in terms of identity management. It enables you to observe your policies in action and determine whether or not you've accurately implemented your business policies.

Novell Identity Manager provides preconfigured reports, such as a listing of all users who have been granted access to a particular system, or of resources provided to a specific user. All reports are available at runtime through Novell Audit's report utility, LREPORT. LREPORT provides a temporary 10-minute runtime for each start of the program. Purchasing Novell Audit removes the 10-minute timeout restriction. Some of the preformatted reports available are listed below:

- *Administrative action report*
- *Historical approval flow report*
- *Resource provisioning report*
- *Specific user audit trail*
- *Specific user provisioning*
- *User provisioning*

Novell Identity Manager provides preconfigured reports, such as a listing of all users who have been granted access to a particular system, or of resources provided to a specific user.

Server Deployment

The Identity Manager server can be deployed in single and multiple server environments. In a typical single-server environment, the Identity Manager server components coexist on the same physical server as the different applications. In most enterprise environments, however, the Identity Manager Server runs on a separate physical server from the actual enterprise systems that it links together.

In some cases, even if the identity vault and engine are running on a different server than the application, the driver could still run on the same server as the actual application. The most common reason for doing this is when the application is running on a different operating system than Identity Manager, since the driver needs to take advantage of the application's published APIs. For example, this type of deployment would be necessary if the Identity Manager server is running on a Linux server and you have Active Directory running on a Windows server. The driver would need to run on the Windows server since the Active Directory APIs require Windows.

Technical Advantages

Novell Identity Manager is the only solution that gives you a complete technical architecture for managing the full user lifecycle—delivering first-day access to essential resources, synchronizing multiple passwords into a single login, modifying or revoking access rights instantly, and supporting compliance with business policies and government regulations.

Novell Identity Manager also provides self-service features that enable users to maintain their own passwords and profile information. With these capabilities, you will realize tangible business benefits: streamlined administration, increased security, reduced costs and a swift return on investment. It's made possible by the following technical advantages.

Easy Configuration

Novell recently took first place in *InfoWorld*'s Identity Management Shootout, beating offerings from IBM, Microsoft, Sun Microsystems and others. Identity Manager received rave reviews, especially in regards to ease of use, as demonstrated in this summary: "Novell has paid much attention to its front-end tools, producing the easiest solution to configure and manage by far." The new Designer tools received additional praise: "Identity Manager proved to be one of the easiest-to-use solutions in the roundup. The addition of Designer adds even more intuitive functionality on top of this suite."

Highly Flexible and Adaptable Architecture

Novell Identity Manager provides integration services that universally connect applications, data stores and network platforms—even across technical and organizational boundaries. It is built upon proven, robust technology with market-leading security, stability and scalability.

Novell Identity Manager facilitates the flexible mapping and management of relationships between resources, including users, groups, services, devices, applications, connections and more. Accessible from anywhere on the Internet, Identity Manager makes it possible for organizations to manage a wide range of resources from a single console.

Novell Identity Manager supports numerous protocols and standards for compatibility with virtually every system. This provides your existing systems a path to automated management of identity across multiple identity stores and reduces the required number of identity stores in your environment. For example, Identity Manager can ensure that you have one, highly scalable, always up-to-date LDAP directory available to multiple applications that require an LDAP directory.

Novell Identity Manager can run natively on Linux, NetWare®, Solaris*, Windows 2003, Windows XP, Windows 2000 and Windows NT platforms. To securely share and synchronize identity data across the different applications, directories and databases distributed across your enterprise network and partners' systems, Identity Manager drivers are available for the following:

Applications

- *Baan**
- *J.D. Edwards**
- *Lawson**
- *Oracle**
- *PeopleSoft*
- *SAP* HR*
- *SAP R/3 4.6 and SAP Enterprise Systems (BASIS)*
- *SAP Web Application Server (Web AS) 6.20*
- *Siebel**

Databases

- *IBM DB2**
- *Informix**
- *Microsoft SQL Server*
- *MySQL*
- *Oracle*
- *Sybase**
- *JDBC*

Directories

- *Critical Path InJoin* Directory*
- *IBM Directory Server (SecureWay*)*
- *iPlanet* Directory Server*
- *Microsoft Active Directory*
- *Netscape* Directory Server*
- *NIS*
- *NIS +*
- *Novell eDirectory*
- *Oracle Internet Directory*
- *Sun ONE* Directory Server*
- *LDAP*

E-mail systems

- *Microsoft Exchange 2000*
- *Microsoft Exchange 5.5*
- *Novell GroupWise*
- *Lotus Notes*

Mainframe

- *RACF**
- *CA-ACF2**
- *CA-Top Secret**

Midrange

- *i5/OS* (OS/400)*

Operating Systems

- *SUSE® Linux*
- *Debian* Linux*
- *FreeBSD**
- *HP-UX**
- *IBM AIX**
- *Microsoft Windows NT Domain*
- *Red Hat* AS and ES*
- *Red Hat Linux*
- *Solaris*
- *UNIX Files - /etc/passwd*

PBX

- *Avaya* PBX*

Other

- *Delimited Text*
- *DSML*
- *Java Messaging Services (JMS) and IBM WebSphere* MQ*
- *Remedy* (for Helpdesk)*
- *Schools Interoperability Framework (SIF*)*
- *SOAP*
- *SPML*

New drivers are being added on an ongoing basis. For the most up-to-date list, see the Identity Manager Web site: www.novell.com/identitymanager

Distributed Administration

Instead of forcing you into a centralized identity management model, Identity Manager supports distributed management of identity and related information. You can assign control of the different aspects of identity to the business groups and authoritative data sources that best fit your business needs.

Distributed Data Ownership

Novell Identity Manager enables your enterprise's individual groups to retain ownership of data. Whether they reside inside your enterprise or at a partner's site across the firewall, data owners have the ability to enforce authority and ultimately determine the use of the data. For example, your e-mail system can be configured to be the authoritative source for e-mail addresses, allowing e-mail administrators to change users' e-mail addresses, but not any of their other identity information.

Whether they reside inside your enterprise or at a partner's site across the firewall, data owners have the ability to enforce authority and ultimately determine the use of the data.

Novell Identity Manager removes barriers between your business systems and enables information to securely flow to your authorized users.

The real-time, high performance architecture of the Identity Vault ensures that identity repositories are always in sync, eliminating any lag time during which unauthorized access could occur.

Data owners can also designate any directory or database as the "authoritative" source of information. They can define the business rules that govern what happens when data modifications take place and how those modifications are communicated to other information systems. Administrators can configure identity objects to capture data from multiple authoritative sources, giving you the flexibility and power you need to maintain consistent and accurate identity data enterprisewide and allowing you to leverage your resources in a way that best fits your business requirements.

Not only does this distributed model give you the needed flexibility to preserve data ownership and enforce your business workforce policies, it also gives you the power to avoid disruptive internal political struggles over policy and ownership.

Non-repudiatable Auditing

The Novell Audit Starter Pack, included with Identity Manager, supports non-repudiation. Non-repudiation is enabled by a chain of authority between the event and the audit trail stored in a separate secure database. This method of logging prohibits any administrator from manipulating user access or data and easily modifying the audit database records to delete any indication of a change being made. Thus, the audit information is reliable and admissible in court.

High-performance Identity Vault

The real-time, high performance architecture of the Identity Vault ensures that identity repositories are always in sync, eliminating any lag time during which unauthorized access could occur. Other vendor solutions require a very intensive reconciliation process to synchronize identities across systems; the reconciliation process can be very timely, upwards of 10–15 hours for large implementations, and could greatly affect system performance during this time (ex: Slow login times on Active Directory).

Conclusion

Identity is a common thread to many of today's enterprise security issues. Without a common identity foundation, each new solution you add creates another silo of identity and contributes to your security problems.

Novell Identity Manager removes barriers between your business systems and enables information to securely flow to your authorized users. As a key component of the Novell Security and Identity solution, Identity Manager gives your enterprise the identity management foundation you need to securely deliver the right resources to the right people—anytime, anywhere. It puts your business rules into action so your systems recognize and immediately deliver the right resources to the right people, based on who they are and their role or relationship with your organization.

Created with market-leading technology and extensive experience in implementing complex identity management solutions, Identity Manager provides you with a foundation that can support your complex business environment and evolving business practices. As you embrace newer technologies such as Web services, accurate and consistent identity management becomes even more critical. As a leader in both identity management and Web services, Novell can help your business gain the

agility that Web services offer while retaining all the security you've come to expect from Novell.

Novell Identity Manager enables you to streamline and automate your existing identity-management processes, strengthening enterprise security and reducing administration costs. It empowers your users to manage their own passwords and personal identity information, alleviating the burden of IT staffs. It provides the tools you need to achieve and prove regulatory compliance. It unifies identity information across your directory-enabled and non-directory-enabled enterprise systems so you can successfully leverage your existing IT investments. It increases business productivity and success, enabling your employees, customers and partners to have faster access to all the tools and resources they need in their relationships within your organization.

Kent Erickson, vice president of identity and resource management at Novell, said, "Security and compliance are at the top of every CIO's list. Novell's identity management solutions deliver on all fronts: reducing costs, improving compliance and enhancing security. It's a 'must have' for every IT department in the world today."

As a modular, secure identity management solution, Identity Manager enables you to address your most pressing security needs first, while putting in place an identity management foundation that allows you to add capabilities as you need them. Novell secure identity management solutions help you create an environment where your business resources work together, securely connecting the right people with the right information at the right time.

Identity Manager enables you to address your most pressing security needs first, while putting in place an identity management foundation that allows you to add capabilities as you need them.

www.novell.com

Contact your local Novell Solutions Provider, or call Novell at:

1 888 321 4272 U.S./Canada
1 801 861 4272 Worldwide
1 801 861 8473 Facsimile

Novell, Inc.
404 Wyman Street
Waltham, MA 02451 USA

Novell®