Novell® Identity Manager 4
Advanced Edition
Table of Contents:

2 . . . . The Most Agile and Cost-effective Identity Foundation Built for Security and Compliance

3 . . . . How Novell Identity Manager Works

10 . . . . Intelligent Management Tools

11 . . . . Key Novell Identity Manager Differentiators

14 . . . . Conclusion
Novell Identity Manager takes a unique and innovative approach to automating all of an organization’s identity management tasks, including user provisioning and deprovisioning, password management and more.

Enterprises need the confidence that their business is secure and that they can meet the increasingly complex regulatory landscape, but not at the expense of business agility or overwhelming cost. Additionally, as they look at computing paradigms shifting to the cloud, they want to be sure their cloud environment has the same level of security and policy controls as their enterprise environment before they move resources to the cloud. However, maintaining control over who is accessing what, how access is being granted, separation of duties and how they generate reports for internal visibility and compliance across all their physical, virtual and cloud environments can be a significant challenge.

While effective user identity management is core to addressing these challenges, too many enterprises have yet to take an efficient, unified and automated approach to identity management. Provisioning new hires with network access, e-mail accounts and other application accesses often requires a series of manual tasks. A change in a user’s cell phone number might require different administrators to make updates in a variety of individual systems in addition to the human resources (HR) database. Requests for access to certain systems often require slow-moving and time-consuming approval and provisioning processes. Whether to meet audit requirements or satisfy a manager’s concern, simply generating a report on who has access to what can be a monumental task as well.

Through its workflow, role management, role attestation, user self-service, auditing, reporting and multi-system data synchronization capabilities, Novell Identity Manager takes a unique and innovative approach to automating all of an organization’s identity management tasks, including user provisioning and deprovisioning, password management and more. It translates business policies and compliance mandates into IT controls, and then consistently enforces them across business domains. It reduces cost and complexity by integrating seamlessly with an enterprise’s existing environment. It enforces access control business policies that provide a secure foundation to manage resources on both sides of the firewall and to support compliance. Its integrated reporting provides the visibility into user entitlements and associated activities for compliance audits, with out-of-the-box support for regulations such as the Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA) and the Federal Information Security Management Act (FISMA).

As the foundation for secure and compliant organizations, Novell Identity Manager simplifies identity management across the entire enterprise.
How Novell Identity Manager Works

Novell Identity Manager secures enterprises through an intelligent identity foundation that provides policy-driven access control across resources from the data center to the cloud, helping to ensure risk management and compliance. It accomplishes this through the following key capabilities:

- Enterprise-wide identity integration
- Advanced workflow capabilities
- Roles-based provisioning and attestation
- Auditing and reporting
- Identity and password self-service
- Cloud connectors

Enterprise-wide Identity Integration

Identity management solutions can provide organizations an integration framework that connects and synchronizes their distributed, application-specific identity stores across their environment. This enables administrators to create and modify identity information once and then have that data propagated to all their connected systems. Novell Identity Manager provides this level of data synchronization through its unique and extensible integration framework.

Data synchronization in Novell Identity Manager serves as the foundation for automating business processes. It provides granular, event-driven, near real-time, policy-controlled and bi-directional data synchronization services between the central identity repository and each connected application. In its simplest form, data synchronization is the movement of data from the location where a data item is changed to other locations where the data item is needed. For example, if an employee’s phone number is changed in a company’s HR system, the change would automatically appear in all other systems that store the employee’s phone number.

Novell Identity Manager lets enterprises synchronize, transform and distribute information across a wide range of applications, databases, operating systems, directories and systems.

Novell Identity Manager lets enterprises synchronize, transform and distribute information across a wide range of applications, databases, operating systems, directories and systems.
The Identity Vault in Novell Identity Manager acts as the repository that stores and associates user identity information from all connected systems and applications. It also maintains the policies and driver configurations that regulate replication data flows between Identity Manager and those systems. The Identity Vault enables each application to reference a coherent set of identity values without needlessly replicating information across systems. By consolidating all this information in a secure, central repository, the Identity Vault provides the following:

- Centralized, unified identity management across all connected systems
- Sharing of identity data, authentication methods and authorization functionality between several different applications

Novell Identity Manager 4 Advanced Edition provides workflow, role management, role attestation, user self-service, auditing, reporting and multi-system data synchronization.
The ability for disparate applications to act as authoritative sources for portions of a unified identity that can then be distributed to other connected systems

A foundation for transparent yet secure access control

A platform for role-based personalization based on rights

The Identity Vault features an object-oriented design, distributed deployment support, scalable capacity to manage billions of objects, powerful schema management, granular data replication and a real-time event system. As with all Novell Identity Manager components, the Identity Vault can run in a wide range of operating environments. Additionally, its deployment as a central identity repository does not limit an organization’s ability to use other credential store technologies for other application or infrastructure uses.

Synchronization Engine
As a join engine, the synchronization engine in Novell Identity Manager manages the synchronization relationships between the Identity Vault and the drivers associated with each connected system. When data changes in the Identity Vault or a connected application, the synchronization engine processes those changes. For events that occur within the Identity Vault, the engine processes the changes and issues commands to the connected application via a driver. For events that occur in a connected application, the engine receives the changes from the driver, processes the changes and issues the appropriate commands to the Identity Vault. The synchronization engine provides loopback detection to prevent endless looping data exchange between the connected application and the Identity Vault. The synchronization engine also provides schema mapping between the Identity Vault and its connected systems, placement rules and transformation rules.

Novell Identity Manager Drivers
The drivers in Novell Identity Manager provide a flexible and scalable method for both bidirectional and unidirectional synchronization of a wide variety of identity information between several types of directories, databases and business applications. The drivers connect to the applications that have the identity information that needs to be managed, and then they carry out two basic responsibilities, which include reporting data change events in the application to the Identity Manager engine, and then executing data change commands submitted by the Identity Manager engine to the application. The business policies that organizations implement using drivers can help reduce management costs, increase productivity and security, and provide event reporting and auditing.

Remote Loader
The remote loader enables the synchronization engine and Identity Vault in Novell Identity Manager to exchange data with different processes on different servers. This allows additional drivers to run on servers where Identity Manager is not installed. This functionality may be needed when the Identity Manager server’s operating system does not support running a driver natively. For example, if a company was running their Identity Manager server on Linux*, the remote loader would allow them to connect to an Active Directory* driver which otherwise could only run on a Windows* server.

Using the remote loader also allows for significant workload distribution to improve the scalability and performance of the Novell Identity Manager server by offloading driver commands to the remote applications or databases. It also helps ensure data integrity in the Identity Vault by providing a common approach to standard connection, security and error handling with remote application programming interfaces (APIs).
Data synchronization in Novell Identity Manager is the key to its ability to automatically generate user provisioning actions in addition to simple synchronization of data items.

Connected Applications
Novell Identity Manager can synchronize data between a variety of different types of connected applications, including systems, directories, databases and operating systems. To allow a Novell Identity Manager driver to connect to these applications, the application must provide APIs that the driver can use to determine application data changes and effect application data changes.

Other Aspects of Enterprise-wide Identity Integration
The following aspects of Novell Identity Manager also contribute to its ability to provide enterprise-wide identity integration:

- **Authoritative sources**
- **Data flow control**
- **Automated provisioning**

Authoritative Sources
Novell Identity Manager relies on the concept of authoritative sources to ensure the proper synchronization of data. Most items of data associated with identity have a conceptual owner. The owner of a data item is considered the authoritative source for the item. In general, only the authoritative source for a data item is allowed to make changes to the data item. For example, the corporate e-mail system is generally considered the authoritative source for an employee’s e-mail address. If an administrator of the corporate white pages directory changes an employee’s e-mail address in that system, the change has no effect on whether the employee actually receives e-mail at the changed address because the change must be made to the e-mail system to be effective.

Data Flow Control
To allow organizations to control data creation and flow, Novell Identity Manager links a filter to each driver object that executes a customizable set of policies. These filters and policies regulate which data is synchronized between the different applications and the Identity Vault. They also determine how data should be transformed during replication and which systems will act as the authoritative sources for individual data elements. They enforce the authoritative source by resetting the attribute to the authoritative value if it is changed from a non-authoritative source. Filters and policies also regulate how a schema in one application will map to those in another, what actions will be triggered by an event and a variety of other control and automation functions. For example, if the filter for the relationship between the PBX system and the Identity Vault allows an employee’s telephone number to flow from the PBX system into the Identity Vault but not from the Identity Vault to the PBX system, then the PBX system is the authoritative source for the telephone number. If all other connected system relationships allow the telephone number to flow from the Identity Vault to the connected systems, but not vice versa, the net effect is that the PBX system is the only authoritative source for employee telephone numbers in the enterprise.

Automated Provisioning
Data synchronization in Novell Identity Manager is the key to its ability to automatically generate user provisioning actions in addition to simple synchronization of data items. For example, in a typical Novell Identity Manager system where the HR database is the authoritative source for most employee data, the addition of an employee to the HR database can trigger the automatic creation of a corresponding account in the Identity Vault. The creation of the account in the Identity Vault in turn can trigger the automatic creation of an e-mail account for the employee in the e-mail system. Data used to provision the e-mail system account would be obtained from the Identity Vault and might include employee name, location, telephone number and so forth.

The automatic provisioning of accounts, access and data can be controlled in various ways, including the use of data item values, role assignments, entitlements, predefined and custom jobs, and work orders.
Advanced Workflow Capabilities

Novell Identity Manager includes a specialized user application interface for workflow approvals, role assignments, attestation and identity self-service. The workflow capabilities in Novell Identity Manager help ensure provisioning processes involve the appropriate resource approvers. For example, John might have been provisioned with an Active Directory account, but he needs access to some financial reports through Active Directory, which requires approval from both John’s immediate manager and the CFO. An approval workflow can be set up that routes John’s request to his manager and then routes it to the CFO after approval from his manager. Approval by the CFO could then trigger automatic provisioning of the Active Directory rights needed by John to access and view the financial documents.

Workflow-based provisioning in Novell Identity Manager can be initiated automatically whenever a certain event occurs (e.g., adding a new user to the HR system) or initiated manually via a user request. Proxy approvers and approval teams can also be configured in a workflow to ensure that approvals occur in a timely manner.

Roles-based Provisioning and Attestation

In addition to workflow-based provisioning, Novell Identity Manager Advanced Edition lets organizations provision users based on their roles. When a user is assigned to a role, Identity Manager automatically provisions the user with access to the resources associated with the role. If a user is assigned multiple roles, he or she receives access to the resources associated with all of the roles. If a particular role assignment requires approval, the assignment request can initiate the appropriate approval workflow. Likewise, user role changes due to promotion, reassignment or termination could automatically modify—or even terminate—access rights in the appropriate manner.

Novell Identity Manager provides roles-based provisioning by leveraging the following base components (see Figure 1 on page 4):

- Workflow engine
- User Application Interface
- Role Service Driver

Workflow Engine and User Application

The workflow engine manages the state of provisioning requests. It consumes decision support information from the Identity Vault, writes provisioning information back to the Vault and logs all activity execution. The user application integrates with the workflow engine to provide an intuitive interface for the management of provisioning requests and approvals.

Role Service Driver

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

Other Aspects of Roles-based Provisioning

The following aspects of Novell Identity Manager also contribute to its ability to provide easy-to-use roles-based provisioning:

- Roles management
- Resource model
- Separation of duties

Roles Management

To facilitate roles management, the roles system in Novell Identity Manager includes several different built-in roles that provide differing levels of access rights to the role-based provisioning system. Someone assigned to administer the Roles Module, for example, has unlimited scope within the
Leveraging a resource model approach, Novell Identity Manager provides an easy-to-understand view of an organization’s resources and their associated user entitlements based on user identity and role.

Roles system, but someone assigned to just manage roles is limited to specifically designated users, groups and roles.

Additionally, Novell Identity Manager simplifies the integration of different role repositories into one consolidated location. This eliminates the need to manage separate sources of identity information.

Resource Model
Leveraging a resource model approach, Novell Identity Manager provides an easy-to-understand view of an organization’s resources and their associated user entitlements based on user identity and role. Presented in a business-friendly, self-service manner, the resource model view eliminates “tech-speak” to make it easy for business managers to make decisions about who should get access to what.

The resource model also allows IT personnel to quickly see what users have access to what, what resources are available, and which rights and resources are assigned to what roles. Additionally, it streamlines provisioning approval and decision processes by automatically e-mailing users about important provisioning tasks and status changes.

Separation of Duties
To prevent users from being assigned conflicting roles, Novell Identity Manager includes a separation-of-duties (SoD) feature that lets organizations establish SoD constraints that define which roles are considered to be in conflict. When roles conflict, SoD approvers can approve or deny any exceptions to the constraints. Identity Manager records approved exceptions and SoD violations with details that can be reviewed through the user application interface or run as a report for auditing and compliance purposes.

Attestation
Novell Identity Manager also has a unique, built-in attestation feature for access certification. For enterprises that need to prove they have mechanisms in place to control who has access to critical systems, Identity Manager provides the option to set up an expiration on specific user entitlements. While this is not needed for all users or all connected systems, it can be a great benefit for those systems that are most critical from an audit or compliance perspective. If desired, it can be configured to give users periodic alerts of expirations so they can re-request access.

To help organizations stay in compliance with internal policies and government regulations, Novell Identity Manager provides an attestation process that helps validate the correctness of role assignments. Using this process, individual users can validate their own profile information and roles managers can validate role assignments and SoD violations.

To help organizations ensure that role assignments are accurate and that there are valid reasons for allowing exceptions for conflicting roles, Novell Identity Manager provides the following attestation reports and processes:

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

Novell Identity Manager simplifies the process of verifying that an organization’s provisioning activities comply with its policies, requirements and regulations. Its auditing and reporting capabilities help organizations determine if the right people have access to the right resources, or if the wrong people are shut out of those same resources. They can easily verify that the employee who started yesterday has access to the network, his or her e-mail and the six other systems required for his or her job. It can also verify that access has been canceled for the employee who left last week.

With Novell Identity Manager, organizations can relax in the knowledge that all of their user provisioning activities—past and present—are being tracked and logged for auditing purposes. Identity Manager contains an intelligent repository of information about the actual state and the desired state of the Identity Vault and of the managed systems within an organization. By querying the warehouse, organizations can retrieve all of the information they need to ensure that they are in full compliance with relevant business laws and regulations.

The Novell Identity Manager warehouse provides a 360-degree view of business entitlements, providing the needed knowledge to see the past and present state of authorizations and permissions granted to users in the organization. This knowledge makes it easy to answer even the most sophisticated governance, risk and compliance (GRC) queries.

The Identity Reporting Module in Novell Identity Manager generates reports that show critical business information about various aspects of an organization’s Identity Manager configuration, including current and historical information collected from identity vaults and managed systems such as Active Directory or SAP. The reporting module provides a set of predefined report definitions that can be used to generate reports, and it provides the ability to import custom reports defined in a third-party tool. The user interface for the reporting module makes it easy to schedule reports to run at off-peak times to optimize performance.

The following represent some of the key components that make up the Identity Reporting Module (see Figure 1 on page 4):

- **Event Auditing Service.** Captures log events associated with actions performed within the Roles Based Provisioning Module and the Role Mapping Administrator.
- **Identity Information Warehouse.** Repository for report definitions, report schedules, completed reports, database views used for reporting, configuration information, identity data collected by the Novell Identity Manager collection service and auditing data.
- **Data Collection Service.** Collects information from various sources within an organization using the Report Data Collector, which retrieves data from one or more Identity Vault data sources; Event-Driven Data Collector, which gathers event data captured by the Data Collection Service driver; and the Non-Managed Application Data Collector, which retrieves data from one or more nonmanaged applications by calling a REST end point written specifically for each application. (Note: Nonmanaged applications are applications within an enterprise that are not connected to the Identity Vault.)
- **Data Collection Service Driver.** Captures changes to objects stored in the Identity Vault, such as accounts, roles, resources, groups and team memberships. The Data Collection Service driver registers itself with the Data Collection Service and pushes change events (such as data synchronization and add, modify and delete events) to the Data Collection Service.

With Novell Identity Manager, organizations can relax in the knowledge that all of their user provisioning activities—past and present—are being tracked and logged for auditing purposes. Identity Manager contains an intelligent repository of information about the actual state and the desired state of the Identity Vault and of the managed systems within an organization.
Identity Manager helps ensure that security is consistent across the enterprise, no matter where users work or where systems are hosted.

- **Managed System Gateway Driver.** Collects information from managed systems by querying the Identity Vault for lists of all managed systems; lists of all accounts for the managed systems; and entitlement types, values, assignments and user account profiles for the managed systems.

- **Integration API.** Allows the implementation of a REST end point for a nonmanaged application.

To simplify and enhance customized report creation, Novell Identity Manager utilizes the JasperReports* format—one of the most popular open source reporting formats. Reports can be viewed or printed in HTML and PDF or easily converted by third-party applications to Excel*, OpenOffice* and Word*. For even more flexibility in report design, the Identity Reporting module can also import custom-designed reports from third-party tools such as iReport* that have been packaged in .rpz format.

The Identity Reporting module also provides a graphical report management and scheduling interface. The calendar-based report scheduler interface allows one-time setup of recurring reports that can be distributed automatically to key business, compliance or security stakeholders within an organization.

**Identity and Password Self-service**

The Novell Identity Manager User Application provides basic password and user profile self-service capabilities. It allows users to manage their basic profile information and helps them remember, change or reset forgotten passwords. The User Application also provides visual organizational charts to facilitate management of user directory information and relationships, as well the capability to create users in the Identity Vault.

**Cloud-ready Drivers**

For more than a decade, Novell Identity Manager has offered a comprehensive set of drivers for a variety of applications, operating systems and platforms. The new drivers for software-as-a-service (SaaS) applications in Novell Identity Manager now give organizations cloud provisioning capabilities. This allows organizations to use Identity Manager to extend their enterprise-compliant processes to the cloud and perform all of the same identity management capabilities they rely on for SaaS applications within the firewall, such as provisioning, deprovisioning, initiating request and approval processes, changing passwords, updating identity profiles and reporting.

Novell Identity Manager lets organizations base access to resources in the cloud on the business policies they establish rather than the requirements of third-party hosting services or managed-service providers. As a result, Identity Manager helps ensure that security is consistent across the enterprise, no matter where users work or where systems are hosted.

**Intelligent Management Tools**

Novell Identity Manager includes the following set of intelligent management tools to facilitate the implementation, customization and maintenance of the solution:

- **Analyzer**
- **Designer**
- **Role Mapping Administrator**
- **Novell iManager**

**Analyzer**

Analyzer for Novell Identity Manager is an Eclipse-based identity management toolset that is used to analyze, clean and prepare an organization’s data for synchronization as part of its Identity Manager implementation. It helps organizations ensure that internal data quality policies are adhered to by providing data analysis, data cleansing, data reconciliation, and data monitoring and reporting. Analyzer lets organizations analyze, enhance and control all data stores throughout the enterprise.
**Designer**

Designer for Novell Identity Manager is an Eclipse-based tool that helps organizations design, simulate, deploy and document their Identity Manager system. From a design perspective, it provides a graphical interface that organizations can use to model their complete system. It includes views that allow organizations to create and control the connections between Identity Manager and applications, configure policies and manipulate how data flows between connected applications. The Designer tool allows consultants to use a simple drag-and-drop interface to model, configure and test a customer’s policy framework in a sandbox environment, greatly reducing the time, cost and risk to implementation.

Designer has the ability to work in offline mode. This allows organizations to evaluate, test, experiment and resolve any issues with the operation of their Novell Identity Manager system before deploying it live in their production environment. Additionally, Designer can generate extensive documentation that shows an organization’s systems hierarchy, driver configurations, policy configurations and much more.

**Content Package Manager**

The content package manager in Designer allows for easy creation, distribution, consumption and control of policy content through packages. Packages are the modular building blocks of all policies. By using the content package manager in Designer, with a few simple mouse-clicks policies can be easily added, modified, maintained or eliminated across all connected systems.

In addition, the content package manager automatically provides notifications regarding conflicts and dependencies between policies and helps resolve them, reducing any unintended impacts. To provide visibility into any policy modification or tampering and help with policy troubleshooting, the content package manager detects updated or modified packages and stores the older versions for roll-back purposes. It also provides the ability to restore back to “factory-mode” operation.

**Role Mapping Administrator**

A key differentiator for Novell Identity Manager, the Role Mapping Administrator is a web service that discovers authorizations and permissions that can be granted within an enterprise’s major IT systems by mapping third-party roles and profiles across connected systems. It allows business analysts, not just IT administrators, to define and maintain which authorizations are associated with which business roles. The Role Mapping Administrator replaces coding with easy-to-use drag-and-drop functionality—for tying entitlements to roles within an organization.

**Novell iManager**

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

**Key Novell Identity Manager Differentiators**

A general consensus exists on the core requirements that should be offered by enterprise-class identity management solutions. Even though many vendors offer solutions that appear on the surface to be compliant or have a functional equivalence with these requirements, there are significant differences in the way that many of these solutions are conceived and developed. These differences ultimately yield great disparity in the lifecycle costs of implementation and maintenance, the security of the protected resources, the ability to demonstrate compliance and the adaptability of the secured environment.
By supporting most applications, web sites and terminal servers, as well as popular directories and clients, Novell Identity Manager allows organizations to leverage their investments in existing systems and avoid expensive hardware upgrades.

Novell Identity Manager takes a unique and innovative approach to identity management that addresses these challenges and elevates it above competing offerings. Identity Manager is the only solution that securely manages identity and access across physical, virtual and cloud environments through an intelligent identity framework that enables organizations to leverage their existing IT assets and new computing models such as SaaS, while reducing cost and ensuring compliance. Identity Manager is the foundation for a secure enterprise. It translates business policies and compliance mandates into IT controls that are consistently enforced across business domains. Novell Identity Manager simplifies identity management across the entire enterprise.

**Real-time, Event-based Automation**

Unlike the reconciliation model of competitive offerings, Novell Identity Manager is built on an event-based, automated provisioning engine. In large organizations with thousands of users and applications, the reconciliation approach has an inherent time lag when reconciling actual identity states with the desired identity states. This time lag can lead to delayed productivity when users have to wait for their access to be granted. The time lag involved in reconciliation can also open security holes that allow access to systems and information for days or weeks after an employee, partner or contractor should have had their access rescinded. Only Novell Identity Manager can address this issue by providing real-time system updates triggered by a single event in an enterprise’s authoritative source, such as the HR system.

**Tightly Integrated IAM Solutions**

Identity and Access Management (IAM) solutions from Novell offer the most-tightly integrated suite in the market with a common code base, resource sharing, I/O architecture and user experience. Novell solutions integrate all of the key capabilities organizations need to create an optimal environment that addresses identity and access management, as well as security management and compliance management challenges. This integration helps organizations streamline the process of managing their identity infrastructure and securing access to resources—even across domain and business boundaries. It also means organizations can deploy a solution that addresses their most-pressing challenges first—whether that’s provisioning or single sign-on—and then expand the solution to address additional needs as the business evolves. Industry leading products from Novell leverage the collective wisdom of 25 years of expertise in managing identities and directory information, a series of industry firsts and awards, and more than 6,000 customer deployments worldwide.

**Interoperability**

Novell builds its solutions with interoperability in mind and links core systems such as HR, e-mail, phone, user and collaborative storage, directory and network operating systems, and even partner systems. By supporting most applications, web sites and terminal servers, as well as popular directories and clients, Novell Identity Manager allows organizations to leverage their investments in existing systems and avoid expensive hardware upgrades.

**Simplified Deployment and Management Tools**

Novell is unique among IAM vendors because it emphasizes developing intelligent tools that greatly simplify implementation. The Analyzer, Designer and Role Mapping Administrator tools for Novell Identity Manager are unmatched in the industry. A recent worldwide independent total-cost-of-ownership (TCO) study by Rencana (Rencana LLC.
“The Impact of Total Cost of Ownership in IAM Investment.” Steve Curtis. 2010.) found that Novell consistently offered IAM solutions with the lowest TCO among the major IAM vendors (Novell, Oracle*, IBM*, CA*, Courion*). Novell solutions cost 23–25 percent less to implement because they are easier to configure, integrate and administer. (Note: The full study can be downloaded at www.novell.com/lowestTCO.)

Inheritance-based Ease of Management

With the Identity Vault as an object-oriented repository, the fabric of Novell Identity Manager has built-in hierarchy and inheritance, as well as native role-based access control. Administrators can easily and quickly use simple policies and access control lists to regulate information access, manage change authorization and enable self-service without heavy credentials.

Native Interface Connectors for Extensive Connectivity

A wide array of Novell Identity Manager drivers enable connectivity with dozens of enterprise business applications, databases, directories, e-mail systems, mainframes, midrange compute platforms and server operating systems. As a result of leveraging several years of Novell integration expertise and development investment, nearly all the drivers utilize their target environment’s native interfaces.

Innovative Content Package Manager

Novell has made it easy to modify, change and even roll back policies through its innovative content package manager, delivering agile and flexible policy management. To simplify and enhance an organization’s policy management efforts and strategies further, Novell Identity Manager provides valuable out-of-the-box policy content based on more than a decade of identity management best practices. Due to its modular package architecture, it also makes it easy to incorporate new or customized packages or policies.

Reports for Proving Compliance

Novell Identity Manager provides advanced reporting and metrics, which include both present state and historic reporting. Reports offer detailed views of any user’s identity and access privileges. Unique to Novell Identity Manager, it can also generate provisioning activity level reports. And as reporting needs increase, organizations can easily build and customize a wide variety of additional reports as required.

Easy Customization and Integration

Novell Identity Manager excels at bringing flexible connectivity and choice among several interfaces. Its open architecture presents modular services that can be accessed through an array of standards-based APIs, including REST, SOAP, SPML, JDBC, LDAP and more.

Providing compatibility with standards-based APIs such as REST and SOAP makes it simple to connect to Novell Identity Manager and create truly customized user interfaces. It even facilitates the creation of connected applications through the use of the Google* Web Toolkit or Microsoft* Silverlight*. Using the APIs, various end-user activities such as password changes, password challenges and role requests can easily be integrated into existing environments, such as a company web portal. The ability to use mobile devices to carry out operational activities such as monitoring open workflows, workflow reassignment, and role and resource management can be offered through the use of these APIs as well.

Novell Identity Manager provides valuable out-of-the-box policy content based on more than a decade of identity management best practices.
Conclusion

As the industry’s first cloud-ready identity management solution, Novell Identity Manager 4 secures corporate resources across physical, virtual and cloud deployments in an intelligent manner. With a scalable, flexible infrastructure to extend policy driven controls across resources beyond the firewall, manage cost of change and provide built in reporting, enterprises can ensure risk management and compliance without sacrificing business agility. Identity Manager 4 translates business policies and compliance mandates into IT controls, consistently enforced across business domains to simplify identity management across the enterprise. The flexibility inherent to Novell Identity Manager 4 lets organizations leverage existing IT assets and new computing models—such as SaaS—helping them stay agile and secure at a lower cost.

“The incorporation of programmatic events gives us tremendous efficiencies. If a colleague moves to a new department, changes a phone number, address, cost center or access privileges, Novell Identity Manager propagates those changes across all connected systems in a matter of seconds. It doesn’t get better than that.”

Mark Edson
Manager of Enterprise Desktop and Directory Services
Huntington Bank

Contact your local Novell Solutions Provider, or call Novell at:
1 800 714 3400 U.S./Canada
1 801 861 1349 Worldwide
1 801 861 8473 Facsimile

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