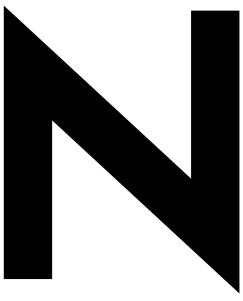
A Superior Foundation for Secure Identity Management Solutions

www.novell.com

ARCHITECTURAL GUIDE



Novell®

Table of Contents

A Superior Foundation for Secure Identity Management Solutions

The Need for Comprehensive Secure Identity Management Solutions

Due to the complexity of heterogeneous IT environments, corporations face significant challenges in managing the security and access control for their computing systems and the multitude of users that rely upon them for their daily productivity and organizational competitiveness. As the size of a corporation's user base grows, and as IT systems and applications proliferate, so do problems associated with resource availability, scalability of management, flexibility of the management solutions, system reliability and security of the IT environment as a whole.

Scalable resource access management is a critical issue:

As a corporation's user population grows and changes, IT personnel are faced with the problem of providing timely, accurate access to resources. Employees, partners, customers and suppliers must be provided access to all resources necessary to achieve maximum productivity, but to ensure security, they must be restricted from accessing systems and information not relevant to their tasks. Managing such access can be daunting, and corporate competitiveness consistently requires managing more users with fewer IT resources. A solution must be found that greatly simplifies resource access management while providing the required levels of security.

Enterprise-wide security is the ultimate goal:

Security also becomes a critical concern as IT solutions begin to span the broad landscape of enterprise systems and users. How can organizations enforce Identity-based Policy when so many systems, administrators, end users and external partners require individualized, dynamically changing access to internal and external resources? Corporations require a solution that uniformly manages and ensures that all users are properly authenticated and authorized to access all of the necessary resources, and only the necessary resources, required to perform their duties, while also protecting against potential security threats such as:

- administrative mistakes, in which privileges are granted to inappropriate individuals, or in which privileges are not revoked when access is no longer required
- disgruntled employees, in which individuals intentionally abuse their legitimate access to resources, or their administrative rights to grant access to resources, to do harm to the corporation or perform actions for personal gain
- external attacks, in which individuals outside the corporation take advantage of security

weaknesses to obtain unintended access to systems in order to deface, destroy or illegally obtain internal information

Additional security-related concerns must also be addressed:

- compliance with applicable governmental security-related regulations, despite usage of a myriad of unrelated systems that provide no unified method of management, and no comprehensive secure logging and auditing capability to prove compliance
- enforcement of strong passwords and strong authentication across all systems, especially when those systems don't natively support such capabilities
- graceful accommodation and leveraging of emerging standards that enable federated authentication, authorization and Identity exchange, even when existing systems lack such features
- uniformly enforcing security across complex distributed systems regardless of the hardware, applications, operating systems and variety of Web services components involved

From a broad perspective, security is about ensuring that each user has access to only the appropriate resources necessary to achieve success in their efforts. The decision of which individuals should be granted access to each resource is established through development of Policy—a set of high level rules that define a "desired state" for overall resource availability. Policy is subsequently enacted by IT administrators through management of the IT systems that control protected corporate resources and data. Corporations are faced with the task of mandating effective Policy, comprehensively reflecting that desired state in each managed system, scalably managing those systems according to the dynamic needs of the organization, and then ensuring that Policies are correctly enforced as mandated.

Many current Identity Management products don't provide adequate solutions:

Corporations also face problems associated with making their individual systems, each of which may attractively solve a particular problem, work together as a unified whole. Many systems and applications contain Identity and privilege information, and solutions may already be implemented to address specific Identity Management issues; however, these "silos" of Identity, whether existing in applications or limited-purpose Identity Management solutions, are obscured behind organizational, political and security boundaries and therefore are only partial approaches to the greater problem of Identity Management across the entire enterprise. These boundaries force corporations to engage in duplicate, uncoordinated Identity Management efforts that raise system administration costs while resulting in inconsistent data, degraded application quality and error. Furthermore, while Web services promise to revolutionize the construction and architecture of corporate solutions, they hold the potential to escalate this problem by forcing corporations to deal with applications consisting of a multitude of independent distributed components with each acting as an island of Identity. Corporations are faced with the need for highly

flexible, cost-effective Identity Management solutions that can meet their unique needs across all platforms, systems and applications, and across all users—employees, customers, partners and suppliers.

Novell® Nsure™ provides a superior foundation for Secure Identity Management solutions:

Corporations can achieve significant benefit from Identity Management solutions, but they need to seek approaches that provide a uniform, secure solution for the entire enterprise. A unified framework of Secure Identity Management is needed upon which to build evolutionary, not revolutionary, solutions to unique issues, and upon which corporations can create additional solutions as needs evolve to encompass a greater portion of their enterprise. The preferable Secure Identity Management approach is the one that conforms to existing business processes and immediate needs while accommodating unanticipated future requirements, without creating additional silos of Identity or requiring significant re-engineering or replacement as needs change. Novell Nsure Secure Identity Management solutions provide an exceptional foundation for secure access management by fully accommodating immediate and future needs while unifying all Policy-based solutions under a single, comprehensive framework that delivers a superior return on investment.

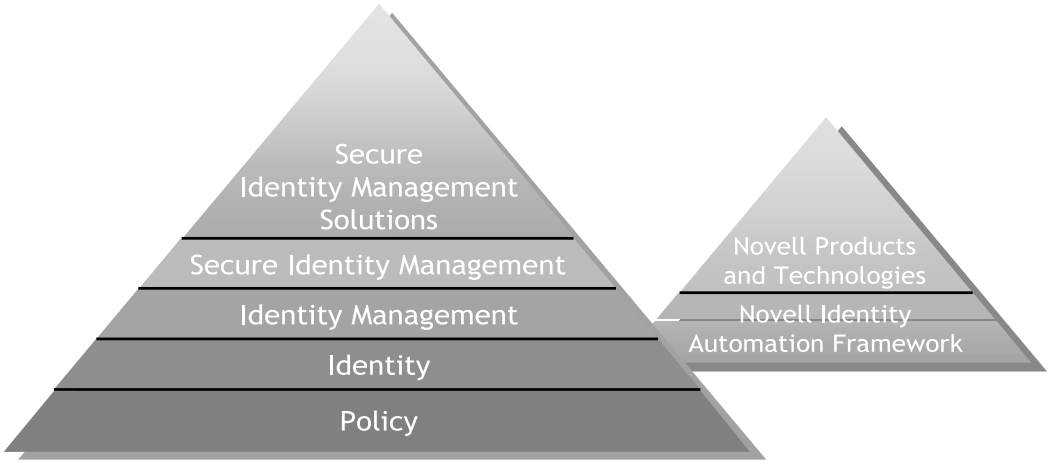


Figure 1: Understanding Novell Secure Identity Management

This paper provides a technical overview of Novell Secure Identity Management technologies and solutions. Topics are presented such that each builds upon those previously discussed, as illustrated in Figure 1, thus gradually creating a comprehensive picture of the Novell approach. Information is organized into three general sections:

1. This paper begins by building an understanding of the Novell perspective on Policy, followed by a discussion of Identity and the elements that must be included in an effective Identity Management solution. The section culminates by providing a full understanding of what constitutes a thorough suite of "Secure Identity Management" technologies.

2. To provide perspective on the highly tangible value of Secure Identity Management technologies, this paper then provides a brief technical overview of five popular Secure Identity Management solutions currently offered by Novell.
3. Finally, this paper provides a technical introduction to Novell Identity Automation Framework—the highly flexible technical architecture underlying the future of all of its Secure Identity Management solutions—as well as a brief discussion of distinctive technologies that uniquely allow Novell to accommodate the broad landscape of customer requirements.

POLICY-BASED MANAGEMENT FOR THE ENTERPRISE

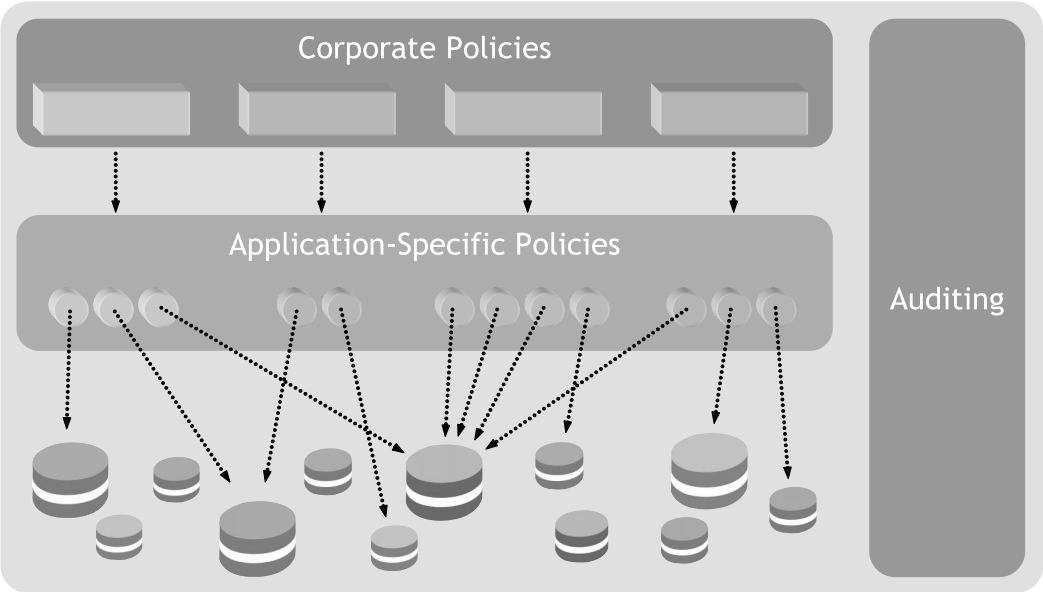
Secure Identity Management is the application of Corporate Policies onto enterprise systems to ensure that users have appropriate access to the right resources at the right times. Policies are established at the highest level to support the business goals of the corporation, and are implemented throughout the breadth of enterprise systems to enforce the appropriate access rights to systems and information by employees, partners, customers and suppliers in pursuit of the corporate mission. As business goals change, Secure Identity Management strategically supports such change by adjusting resource access to ensure the continued security of corporate assets. At the heart of Secure Identity Management is "Identity"—information that defines the attributes and rights of users, systems, applications and other manageable entities throughout the enterprise.

Secure Identity Management must provide a framework upon which corporations can enable universal access to Identity information, establish Policies that act upon Identity information to enforce access control and other aspects of managed systems, and enable auditing to ensure that systems are being administered and utilized as intended. Secure Identity Management must provide the ability to scalably manage Identity attributes regardless of where they originate, and allow other applications across the enterprise to easily and securely utilize those attributes as authorized. In summary, Secure Identity Management must securely manage Identity information and enable its usage through the implementation of Policies.

What are "Policies"?

In the context of Identity Management, Policies utilize Identity attributes as the basis of decision making in order to establish a "desired state" within a system. Policies need to be expressed at two levels: Corporate Policy and Application-Specific Policy.

Figure 2: Policy-Based Administration



In their most general form, Corporate Policies are established by an organization to guide the usage of its assets as well as associated automated and manual procedures. Corporate Policies are independent of the systems utilized to manage access to or maintain data, and as such are abstract expression of a desired state. For example, the Policy "everyone in the Finance department has rights to view the most recent revenue forecast" makes no assumptions of how users are classified as being members of the Finance department, how privileges to view the revenue forecast are expressed, or how the revenue forecast is stored. While Policies of this type are abstract, they are necessary for an organization to comprehensively control the security of its systems and data. To function coherently, a corporation must ensure that it has established a comprehensive set of Corporate Policies.

Application-Specific Policies are implemented to enforce Corporate Policies within managed systems. Application-Specific Policies utilize the underlying mechanisms of the managed platform for expression, and therefore are very precise. For example, the Corporate Policy "everyone in the Finance department has rights to view the most recent revenue forecast" might be implemented by the following two Application-Specific Policies:

- The Group named "Finance" within the Directory Service is assigned "view" rights for the file "\finance\forecasts\current.doc" on the server "XYZCorp_Finance".
- The Group named "Finance" within the Directory Service is assigned "read" rights for the file "www.intranet.xyzcorp.com\finance\reports\forcasts\current.html".

In this example, a single Corporate Policy is instantiated through two Application-Specific Policies, one enforced by a network file server and one enforced by a Web server. From this extremely simple example, several facts should become evident:

1. Policies can be used to manage virtually anything within the enterprise IT infrastructure. While Policies are often used to manage the access rights of users, they can also be used to manage various aspects of Roles, workstations, servers, operating systems, handheld devices, applications, Web services, network devices, etc. Such managed entities are collectively referred to as "Principals" throughout the remainder of this paper.
2. Application-Specific Policies are specific to the data they manage and the mechanisms they use to manage that data.
3. A single Corporate Policy can result in a multitude of Application-Specific Policies.
4. Organizations need mechanisms to facilitate the creation of both Corporate Policy and Application-Specific Policy, and for mapping one to another to facilitate auditing processes designed to ensure that the desired state is being achieved.

Policies are at the heart of IT administration, and are the mechanism by which all Principals are managed; however, Policies are limited in capability by the qualities of the system through which they are expressed, as well as the scope of Identity information they can utilize to make decisions. Novell Secure Identity Management solutions are designed to remove this limitation by providing uniform access to selected Identity attributes regardless of the application in which they originate, and by allowing other applications across the enterprise to easily utilize those attributes as authorized. As well, Novell Secure Identity Management solutions will provide additional robust capabilities for authoring and applying complex Application-Specific Policies beyond those offered natively by many applications, particularly when it comes to the task of implementing enhanced security on top of disparate systems.

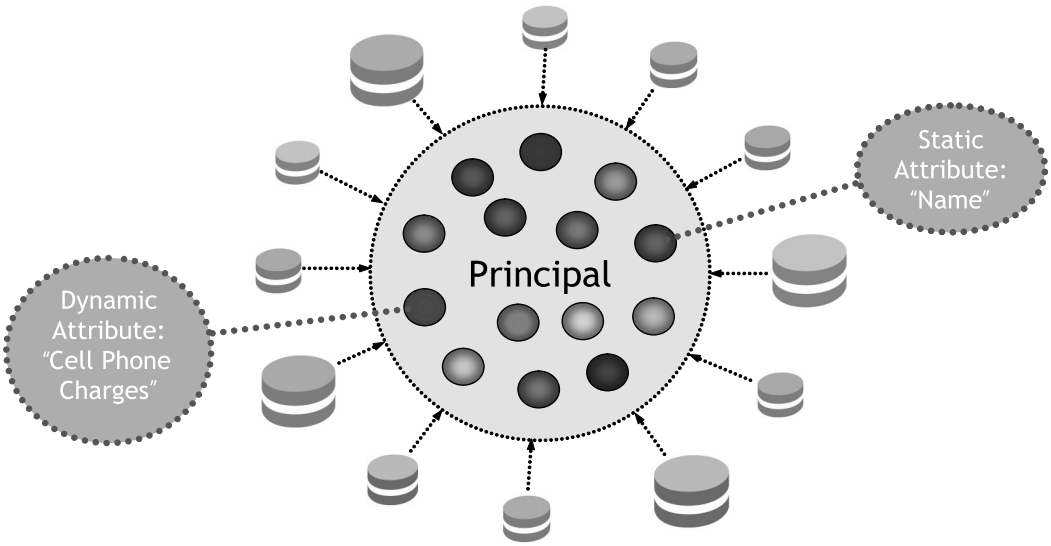
What is "Identity"?

In an abstract sense, "Identity" consists of information that defines managed Principals throughout the enterprise (with users being the most common Principals). Identity can represent a wide variety of shared information such as personal information, data regarding privileges granted within IT systems, application-specific information relevant to usage of a given application, or anything else that relates to Principals. As one example, Identity of a user (illustrated in Figure 2) might consist of some of the following:

- static attributes describing the person such as name, title, department, location, education, etc.
- dynamic attributes describing recent actions of the person, such as Web sites visited, internal application usage patterns, recently conducted corporate travel, cell phone charges, etc.
- history and audit trail information documenting critical activities such as system administration actions
- individual access rights and other privileges granted to the user by IT personnel

- security equivalences, allowing the user to assume privileges that are granted to other selected Principals, such as specific Groups, Roles or other users
- policies that dynamically influence the privileges of the user, and the behavior of the system, based upon other specified Identity attributes (such as the assignment of a corporate cell phone because of job title)

Figure 3: Identity



While users are the primary focus of Identity Management today, it is important to recognize that Identity Management applies equally well to any Principals in the network, including Groups, Roles, applications, processes, Web services, workstations, servers, etc:

- In one example, workstations might be inventoried to establish Identity, and then Policy might be defined based upon that Identity in conjunction with user Identity to automatically maintain the workstation's software and operating system configuration.
- In another example, Identity might be established for a firewall system, including the desired configuration as well as information regarding the systems it protects, such that Policy could be stated that would allow the firewall to intelligently determine which connections to allow through the firewall, by which users, and under what circumstances.
- In a third example, Policies might be established to control customer access to various purchasing transactions being implemented through the integration of a variety of distributed Web services, wherein each Web service utilizes the common Identity and Policies to enforce uniform authentication and authorization for each transaction such that the system appears a single manageable entity rather than a set of disparate independent components.

The Identity of a Principal must be the aggregated total of all shared attributes that apply

to it, regardless of the nature of those attributes or the system from which they originate. For some organizations, centralizing Identity information into a single corporate directory service may be sufficient, while for many others this approach may be highly unrealistic. For these organizations, Identity originates from a wide variety of applications and systems throughout the enterprise, and those systems may be independently managed. As such, each source of Identity attributes may be an "Authoritative Source," acting as the only true source for the information it creates and holds.

Because Identity can originate in so many systems, and because ownership and responsibility for those systems and their data can be physically and politically distributed, centralized Identity simply isn't possible for many corporations, and may not be the best solution to support business needs. For instance, a Human Resources system may be the Authoritative Source for employee salary-related Identity information, and it might be unrealistic or perhaps even impossible for HR personnel to stop using their internal applications to maintain employee Identity in favor of using a centralized Identity repository and its associated interfaces. "Integrated Identity" provides a solution to this problem by fully accommodating multiple distributed Authoritative Sources of Identity.

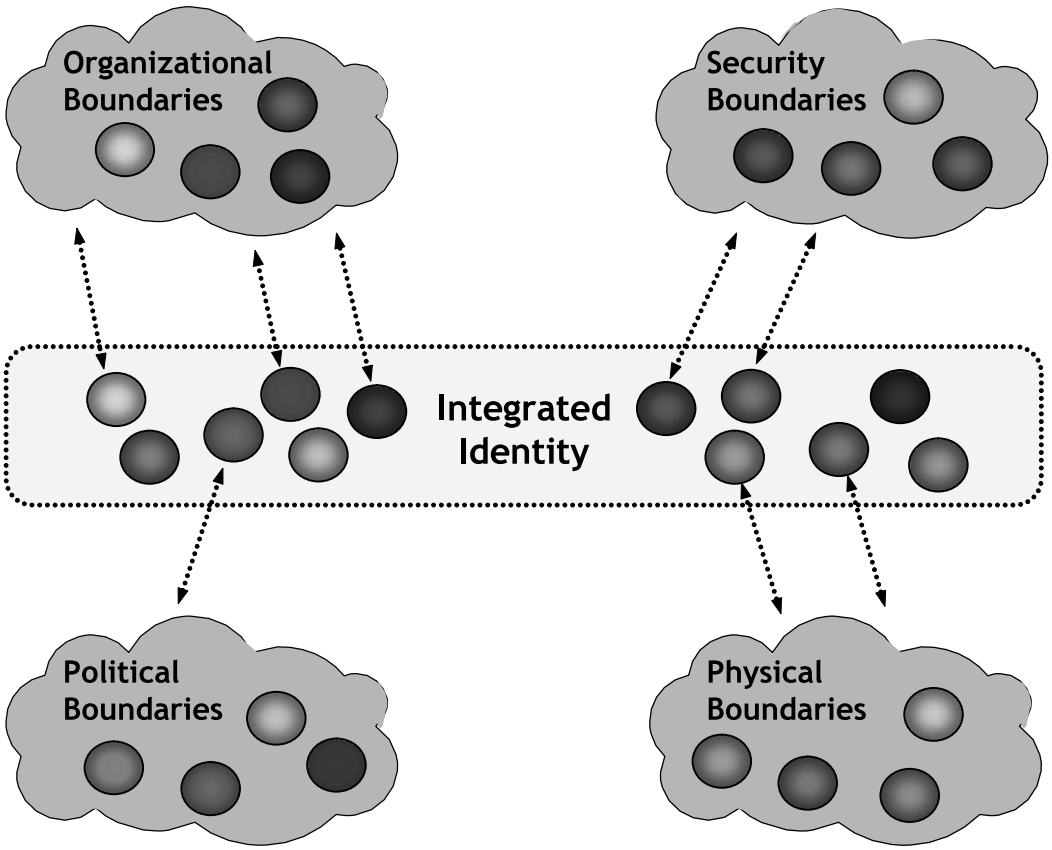


Figure 4: Integrated Identity

Novell Integrated Identity provides systems that enforce Policy with a unified view of all available shared Identity information anywhere within the enterprise. It can be configured to respect Authoritative Sources by not allowing others to change the authoritative Identity attributes, and it supports real-time bi-directional synchronization of selected Identity information between the connected systems so that the Integrated Identity remains up-to-date and available from distributed sources. It allows connected systems to act upon the Integrated Identity in application-specific ways, and its operations are fully customizable and manageable via Policies.

Because Novell Integrated Identity respects Authoritative Sources and provides selective bi-directional synchronization, a number of important administrative benefits are provided:

- Existing applications working against the Identity stored in native systems or LDAP directories need not be modified in order to fully participate in Identity Management solutions.
- Administrators can continue to use the native system administration utilities that they are familiar with, thus eliminating the need for significant additional training and expertise.
- While Novell offers robust administrative tools for managing its Integrated Identity, its support for continued use of native system administration utilities flexibly accommodates existing administration methodologies, management structures and domain-specific system ownership.

Novell Integrated Identity represents an evolutionary, incremental enhancement to existing systems, data, skills and processes that eliminates the need for disruptive changes to IT infrastructure while enabling comprehensive Identity Management solutions that respect organizational, political, security and physical boundaries.

What components must "Identity Management" include?

Enterprises require scalable administration of Identity, enabling a small number of system administrators to manage the Policies associated with a large number of users and other Principals throughout the myriad Authoritative Sources in the enterprise. Effective Identity Management should apply a set of proven, advanced management techniques (as shown in Figure 5) to Integrated Identity to automate, accelerate and simplify Identity creation and maintenance.

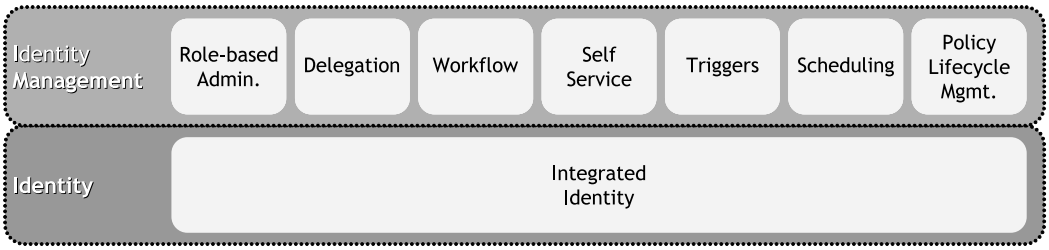


Figure 5: Identity Management

- *Role-Based Administration*

  Effective Identity Management must include Role-based administration that enables scalable management of users and other Principals by grouping them together so that administrative actions, such as granting access to a specific resource, can be applied to all members of the Role at one time. This capability should eliminate repetitive administrative actions, thereby saving time and money, and reducing the likelihood of administrator error.

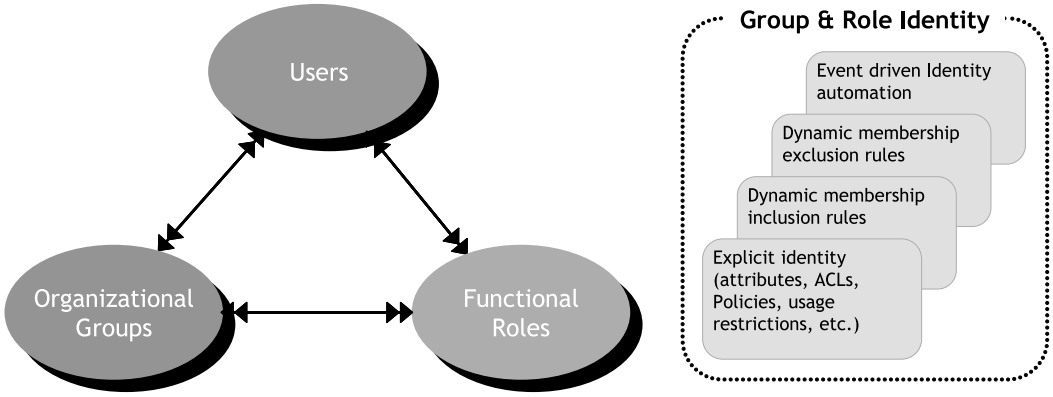


Figure 6: Role-Based Administration

Role-based administration should start by defining "Groups" and "Roles." While the two are very similar in capability, Groups should provide a way to *organizationally* aggregate Principals together, while Roles should provide a way to *functionally* aggregate Principals together. A Group might include all customers at the same loyalty program level, while a Role might include all employees that share the same job title. Groups and Roles should have Identity attributes and access rights wherein their members inherit those attributes and rights, and they should support hierarchical organization to enable scalable, re-usable administration through multiple inheritance. To facilitate the use of Groups and Roles as a common administration paradigm for all systems, Role-based administration should also provide the ability to easily determine the effective (total aggregate) rights of a user or Principal at any time.

To illustrate the value of Groups and Roles and the scalable management they provide, consider the example of a Group that contains one hundred members. Through use of the Group, the act of granting each of the users access to a particular resource would require only a single administrative action rather than one hundred. Similarly, removing a user from the Group would revoke all privileges granted to the user through Group membership.

Groups and Roles should provide further value through support of Dynamic Membership Inclusion Rules. These Rules must allow the administrator to specify common criteria (for example, one or more LDAP queries)

that define membership. As Identity information for users and Principals is created and changed, these Rules must be automatically re-evaluated and membership adjusted accordingly. Dynamic Membership Inclusion Rules should provide a mechanism allowing Group and Role membership to be easily defined through simple statements.

While defining Groups and Roles through inclusion is important, the ability to easily exclude members can significantly help reduce the number of Roles necessary to meet enterprise needs. Dynamic Membership Exclusion Rules, as with Inclusion Rules, should be provided that allow the administrator to utilize common criteria to define the set of users or Principals that are to be excluded from membership. Without exclusion capabilities, defining a large set of users in which only a small set are excluded would require multiple, nearly identical Inclusion Rules, Groups or Roles. This proliferation of Groups and Roles is problematic because it creates more entities to be managed, thus raising rather than reducing costs as originally intended; however, with Exclusion Rules the total set of intended users could be expressed with a single Group or Role.

Consider an example in which a hotel desires to offer special incentives to members of its frequent visitors program, which consists of "normal", "silver", "gold" and "platinum" levels. To easily create a single Role that could offer incentives to only elite members, the Role would use a single Dynamic Inclusion Rule that would include all members of its frequent visitors program, and a single Dynamic Exclusion Rule that would exclude all members at the "normal" level.

Finally, the scalability of Role-based management should be further enhanced through support for Identity Automation (discussed in detail later in this paper) that provides the ability to automatically respond to real-time events triggered by changes to Identity, thus allowing custom actions to be invoked in response to those changes, such as sending alerts, initiating workflows, commencing provisioning activities, etc. Identity Automation would provide significant value by allowing advanced customization of Role-based administration through logical expressions, complex integration with other processes, and coordination of system activity to create the desired actions.

- *Delegated Administration*
  Significant administrative efficiencies can be gained when management duties are distributed such that the administrator most familiar with a given task is the person that actually performs that task. As well, to achieve a secure administrative environment, such distributed rights need to be limited so that each administrator has the rights to perform only the tasks specifically assigned to them. These capabilities, known as Delegated Administration, must be offered to ensure the secure scalability of enterprise IT management.

Delegated Administration must provide each system administrator with a view of only the management tasks and information they have been authorized to act upon, therefore increasing productivity by helping them focus on their assigned efforts and increasing security by preventing them from performing potentially undesirable actions. Because all administrative rights should be managed through Roles, Delegated Administration should build upon Roles by allowing the delegation of rights to subordinate administrators through the creation and definition of subordinate Roles.

Through Delegated Administration, a system administrator should be able to define subordinate administrators that have any or all of the rights that they have been granted. The subordinate might be restricted to only a portion of those rights, and might be restricted to managing only a portion of the IT infrastructure managed by the administrator. For instance, an administrator responsible for managing installation, configuration and access rights to all document repositories across the enterprise might delegate to a subordinate administrator specifically serving the legal department the responsibility for managing those same aspects of the corporation's legal contracts repository. The legal department administrator might also be granted the right to further delegate such rights, therefore having the ability to delegate management of user access rights to the department's executive assistant.

Delegated Administration must be designed to add efficiency to management efforts by hiding complexity and allowing administrators to distribute the workload, therefore lowering costs. Delegated Administration should also accommodate political and security boundaries by allowing administration to be flexibly distributed, thus speeding changes to Identity information through the elimination of bottlenecks.

- *Workflow*

  To increase operational efficiencies, enterprises require Workflow mechanisms for formalizing, documenting and automating business processes associated with Identity maintenance. Unlike traditional Workflow focused on document collaboration, effective Identity Management Workflow solutions must support automation of processes of any kind, whether the process is as simple as manually enabling a network port, or as complex as ensuring that new internal employees have immediate access to all of the physical and IT resources necessary to perform their duties as appropriate for their specific job assignment. Workflow should apply equally well to automation of extranet tasks, such as ensuring that partner employees are granted appropriate access to product information, technical support and partnership collaboration facilities. Workflow must provide extremely flexible, greatly simplified solution customization that can manage not only the tasks of IT personnel but also the automated sequencing of systems integration functions,

without custom code, while supporting interaction between Principals, components, applications, Web services and systems of all kinds.

Enterprises can benefit when IT processes are expressed through workflow due to the assurance that relevant actions are consistently carried out quickly and completely. At any time, it must be possible to monitor active processes to determine which tasks have been completed, which tasks remain pending, and to whom each task has been assigned.

Workflow must also speed the management of Identity. All process coordination and sequencing must be automated and performed by the system, ensuring that necessary approvals are acquired, that tasks are immediately delegated when primary personnel are unavailable, and that parallel tasks are managed to ensure that all prerequisite tasks are completed prior to assigning subsequent tasks.

Workflow should further enhance the security of the corporation's systems. By formalizing and automating processes, Workflow must ensure that nothing is forgotten. For example, the Workflow automation of a de-provisioning process should ensure that all privileges are removed, relevant accounts are deleted, and all physical resources are returned for re-use when a user is removed from the system. Furthermore, the de-provisioning process must further ensure that no privileges are mistakenly left active that might create opportunities for intrusion attacks.

- *Self Service*

  Organizations with a large number of users can require a significant number of Help Desk and IT personnel just to keep up with simple tasks such as maintaining personal information for each user, resetting forgotten passwords, etc. As a result, Enterprises require the ability to place the power and responsibility for maintaining various selected attributes of each user's personality Identity into the hands of the end users themselves, thereby decreasing the need for Help Desk and IT resources while also increasing end user satisfaction and productivity.

  Effective Self Service solutions must include the following capabilities:

  — **Access Request Automation**—IT departments require automation techniques enabling them to scalably respond in a timely manner to individual end user requests for access to information. Self Service must integrate with Workflow to enable secure, approval-based fulfillment of such requests via process automation, thus enabling IT to accept requests, monitor associated efforts, and ensure that all proper authorizations are obtained.

  — **Password Reset**—In many corporations, a large portion of Help Desk efforts involve assisting end users with resetting forgotten passwords—a problem that could be addressed by Self Service Password Reset. End users should first be

authenticated by answering a variety of questions regarding their personal Identity, after which their password should automatically reset without burdening Help Desk personnel.

- **Self Registration**—Self Service should include Self Registration, a capability enabling end users to sign up for an account without requiring the intervention of IT personnel. Users might be granted limited access to public, non-confidential resources by default, and might also request access to additional, protected resources via subsequent automated access requests.
- **Identity Update through Restricted Views**—End users must be able to edit, whenever desired and without IT assistance, authorized portions of their Identity profile such as information regarding their personal information including address, phone number, preferences, etc. Restricted Views must ensure that, during Identity update activities, end users have access to view and modify only the minimum information necessary to perform the task, thus increasing security by ensuring that confidential Identity information is protected.
- **Self Subscription to Groups and Roles**—Personalization is the ability for end users to customize their computing environment as necessary to maximize information availability toward achieving their business goals. One method of personalization that should be provided is selective subscription to optional public Groups (and Roles) in order to easily gain access to resources such as distribution lists. Each available public Group might deliver information relevant to a specific topic or provide links to pertinent services and resources. Self Subscription to Groups must allow end users to automatically gain access to the right amount of information needed while eliminating the clutter associated with unwanted, unused resources.

- *Triggers*

  While many Policy decisions such as access control may often be based solely upon Identity, it is sometimes also desirable to consider external influences such as values from various databases, events, business logic and application states. For instance, the creation of a trouble ticket in a help desk application might trigger the initiation of a workflow process to manage completion of the task. To support such needs, Triggers must be provided that enable non-Identity input of all types to influence the enforcement of Policy, thereby providing corporations with a simple paradigm for integrating existing systems into Identity Management solutions.

- *Scheduling*

  Enterprises require the ability for any action of the Identity Management system to be scheduled to occur on a time and date basis.

For instance, a set of values in a corporate database could be scheduled to be examined automatically at 9:00 a.m. on the first Monday of every month, and if those values reach a given level, a specified workflow could be automatically initiated. Scheduling should simplify administration by enabling frequent, repeatable or predictable tasks and processes to occur automatically, thereby further formalizing those tasks to increase quality of service, eliminate error and reduce administrative costs.

- *Policy Lifecycle Management*
  We've illustrated how Identity Management must include Role-Based Administration, Delegated Administration, Workflow, Self Service, Triggers and Scheduling to simplify and automate the implementation of Policy, but as the number of Policies grows, so does the need for mechanisms for ensuring that Policies are developed, implemented, periodically reviewed and updated effectively. Within a large corporation, at any time there might be dozens of system administrators authoring Identity information and establishing Policies, therefore mechanisms are needed to ensure that those changes are coordinated, that they don't conflict, and that they achieve the desired state:
  - **Versioning**—Policy Lifecycle Management must include versioning capabilities that allow the development of Policies, changes to Identity and the implementation of Identity Automation Rules to be performed in a distributed manner, wherein each administrator's changes are tracked, past revisions are maintained, and a historical record of all changes is available. Versioning must also allow administrators to provide context for their changes through association with specific Projects and change requests, thus allowing incremental Project development as well as easy deployment and undo.
  - **Testing**—Working in conjunction with versioning, testing capabilities should allow a system administrator to assess proposed changes, without actually putting them into production, to determine whether changes will have the intended affect upon the system.
  - **Ownership**—In a large organization, administrators come and go and IT plans evolve over time, making it highly likely that various Policies and their reason for implementation may be lost and forgotten. Identity Management must include ownership tracking mechanisms enabling the system to associate a specific administrator or project with each Application-Specific Policy, as well as the context for its implementation and the Corporate Policy with which it is associated.
  - **Evaluation**—As the number of Policies in the system grows, it may become difficult to predict the aggregate affect of Policies upon a specific user or Principal. The system must include evaluation capabilities allowing an administrator

to determine the total affect of Policies by viewing the real time privileges currently granted to a user, or the set of users currently having access to a selected resource and the Policies granting those privileges.

- **Reconciliation**—The distributed creation of a large number of Policies may create circumstances in which Policies conflict, wherein one Policy may grant a user access to a particular resource while another Policy may deny access. Reconciliation functions should be included that provide the capability to automatically detect such discrepancies, determine which Policies are responsible for the discrepancies, and assist in the resolution.

In summary, Identity Management must provide mechanisms to simplify the creation and management of Identity information and Policies, enabling them to be scalably implemented with a minimum of IT personnel and with reduced impact upon Help Desk resources; however, while providing outstanding efficiencies, Identity Management would not significantly address the need for increased security across systems and management efforts, therefore additional capabilities are required to provide *Secure* Identity Management.

What constitutes effective "Secure Identity Management"?

Secure Identity Management (SIM) enhances the efficiency-oriented concepts of Identity Management discussed above with additional capabilities (as shown in Figure 7) to ensure the "confidentiality," "integrity" and "availability" of business system resources. Confidentiality ensures that a corporation's resources can be accessed only by authorized Principals. Integrity ensures that the corporation's resources can be created, accessed, used, configured and maintained only as intended, and only in authorized ways. Availability ensures that the corporation's resources are always accessible by authorized Principals in a timely manner. These three attributes (confidentiality, integrity and availability), which are generally considered by experts to define "security," must be provided to enhance the enterprise's ability to protect its assets and ensure that access to resources is consistently available to only the intended Principals.

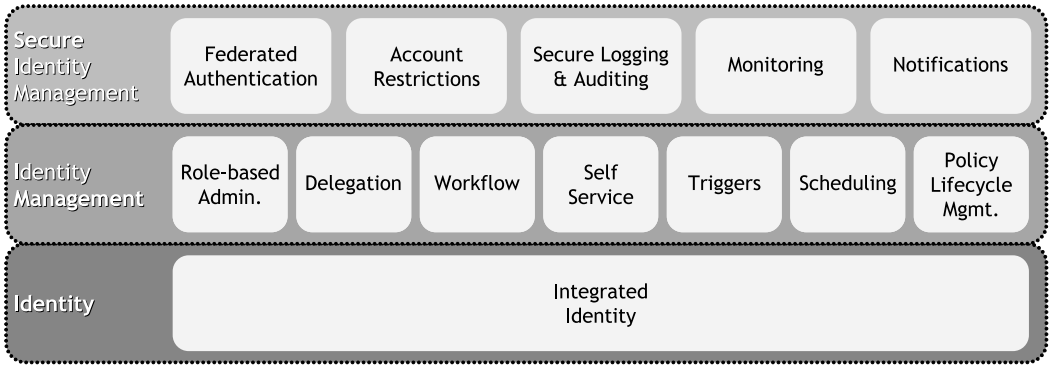


Figure 7: Secure Identity Management

- *Federated Authentication*

  SIM solutions must provide modular support for a large number of authentication techniques, ranging from implementation of simple username and password to strong authentication techniques such as digital certificates, hardware tokens and biometric devices. Support is also needed for standards-based federation techniques such as Security Assertion Markup Language (SAML) and Liberty. From a single point of administration and implementation, corporations must be able to enforce authentication methods that match the confidentiality of their resources.

  Graded authentication is also required in order to achieve added security by protecting each resource with the appropriate level of security, wherein less-confidential marketing documents might be protected by a simple password while access to confidential financial information could require automatically prompted re-authentication via digital certificate. Even stronger security should be provided through support for chaining (sequential combination) of security methods such as requiring something that you know (such as a password) with something that you have (such as a smart card token), in addition something that is part of you (such as a fingerprint).

- *Account Restrictions*

  Enterprise administrators need the ability to control the creation and usage of user accounts and passwords. Consistent support for strong password composition policies is required to ensure that users can't create simplistic passwords that are easily guessed or compromised through dictionary attacks and other standard password cracking techniques. Account and password expiration policies are required to enable enforced periodic resetting of strong passwords, as well as the ability to create single-use and short-lived accounts. Policies regulating the time, duration and location of user login are also needed to further enforce security by ensuring that accounts are utilized only during the time intended, and at the places intended (such as secure locations, during business hours only), thus helping to prevent against attack from unintended sources.

- *Secure Logging and Auditing*

  Secure Identity Management must include Secure Logging that allows selective filtered recording of administrative changes and end user actions such that those changes can be monitored for desirable and undesirable occurrences. Secure Logging could be used to detect system break-ins, administrators and end users utilizing inappropriate privileges, and systems experiencing problems or other abnormal behavior. Logging might also be used to validate that required administrative changes have been made as mandated by Policy.

  Through Secure Logging, all logged information should be stored securely to prevent tampering and to support non-repudiation, thus facilitating audit compliance with

internal policies and external governmental security regulations such as the European Data Protection Directive (applicable to personal information confidentiality), HIPAA (applicable to U.S. health care institutions), Gramm-Leach-Bliley (applicable to U.S. financial institutions) and Sarbanes-Oxley (relevant to the financial accountability of U.S. corporate officers). It must be the case that any deletions, additions or changes to logged information can be detected to ensure the integrity of results gleaned from the data.

To simplify compliance and auditing efforts, Secure Logging must also include the capability to easily generate a variety of reports summarizing the recorded actions, and it must be possible to use popular third-party reporting tools to generate custom reports to meet virtually any auditing need. Furthermore, industry-standard databases should be supported to act as the log repository, thus facilitating high-volume logging and advanced log data handling.

- *Monitoring*

  Monitoring must also be provided to facilitate security by providing real-time views of the status, configuration and resource utilization of all components in the system. Administrators must be able to ensure that components are not functioning outside of their intended configuration, operational trends should be identifiable through historical charts, and component-specific alerts should allow the identification of potential issues.

- *Notifications*

  System administrators require the ability to respond immediately to security- and system-related events, thus ensuring that IT systems can be adjusted accordingly to ensure proper operation. To support this need, Notifications must be provided that consist of real-time alerts regarding system status change, unusual occurrences, system failures, security intrusions and other conditions matching Notification filter specifications. Administrators must be able to select the types of alerts desired, the method of delivery for each alert (e-mail, SNMP, pager, JMS event, etc.), and the Principal to whom each type of alert is to be delivered.

"Secure Identity Management" means that the confidentiality, integrity and availability of Identity is strongly maintained by the system and that the integrity of the solution is verifiable. Support for confidentiality must be robustly provided by Federated Authentication; integrity must be delivered through Secure Logging and reports; and availability must be ensured through Identity Management automation techniques such as Workflow, Role-based administration and Policy-based, automated access control enforcement. All components, including Secure Logging, Notifications and Monitoring must work together to form a comprehensive solution enabling immediate response to obvious security-related events, historical analysis of logged information to detect complex security issues evident from the correlation of data, and the detection of security of monitored systems.

NOVELL SECURE IDENTITY MANAGEMENT SOLUTIONS

Secure Identity Management provides the foundation for secure administration and application of Identity across the enterprise. Novell SIM technologies enable robust access control and scalable administration through implementation of secure, efficiency-oriented management mechanisms and Integrated Identity.

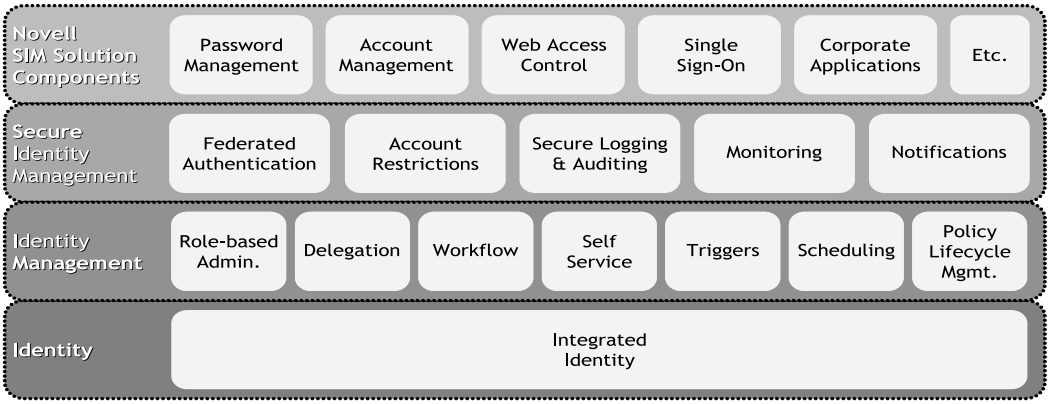


Figure 8: The Novell Comprehensive Suite of Secure Identity Management Technologies

The Novell comprehensive suite of SIM technologies includes, as illustrated in Figure 8, additional SIM components enabling the creation of powerful solutions including Self Service Password & Identity Management, Provisioning, Web Access Control, Single Sign-On and Secure Logging & Auditing. Due to the strength of the Novell SIM technologies and their unique flexibility accommodating advanced customization, many additional solutions are possible, but herein we'll explore only a few of the solutions from which most enterprises can derive significant benefit.

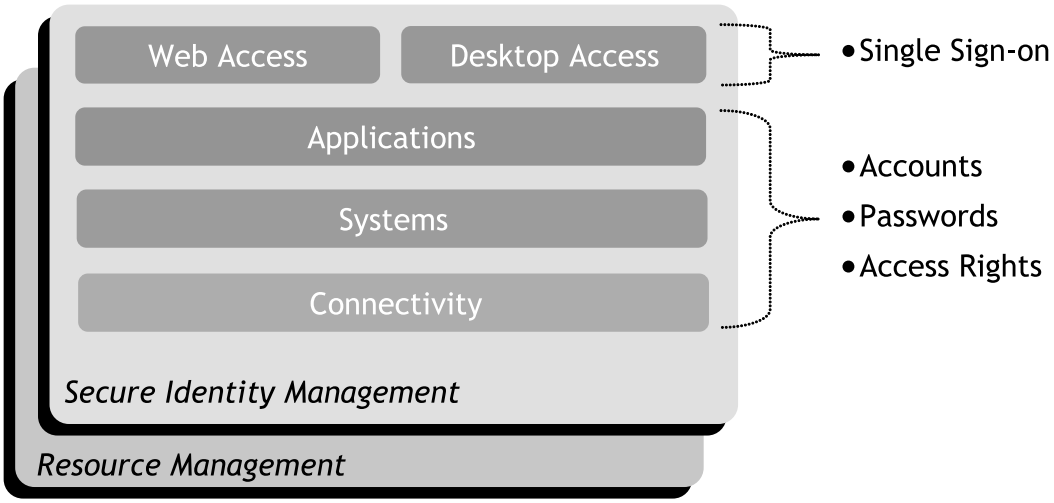


Figure 9: The Novell Complete SIM Solutions Approach

Novell Secure Identity Management Solutions work together (as shown in Figure 9) to provide a total solution to enterprise needs for secure access to corporate resources. The Novell solutions utilize Identity to provide powerful management of accounts, passwords and access rights across all systems, and simplify access to systems through single sign-on services. Novell also provides Policy-based Resource Management that addresses security-related system configuration issues—a powerful capability totally unique to the Novell offering. This comprehensive approach reduces complexity, lowers costs and avoids the pitfalls created by alternative limited-purpose solutions.

Self Service Password & Identity Management Solutions

Password resets and personal Identity updates, seemingly minor concerns among the myriad of issues faced by IT organizations today, impose a significantly larger burden on corporations than might be expected. Because of the large number of systems in corporate networks, users often must deal with a sizeable number of accounts, passwords and personal Identity attributes; however, passwords are often forgotten and personal information changes, and therefore users end up frequently calling the Help Desk for assistance. The cost to corporations for the associated Help Desk efforts and lost user productivity can be surprisingly high—a problem that proportionately worsens as corporate systems proliferate. In the case of global eBusinesses dependent upon personal customer relationships, these costs can be especially acute because of the frequency of password maintenance requests and the highly tangible negative affects resulting from account access problems.

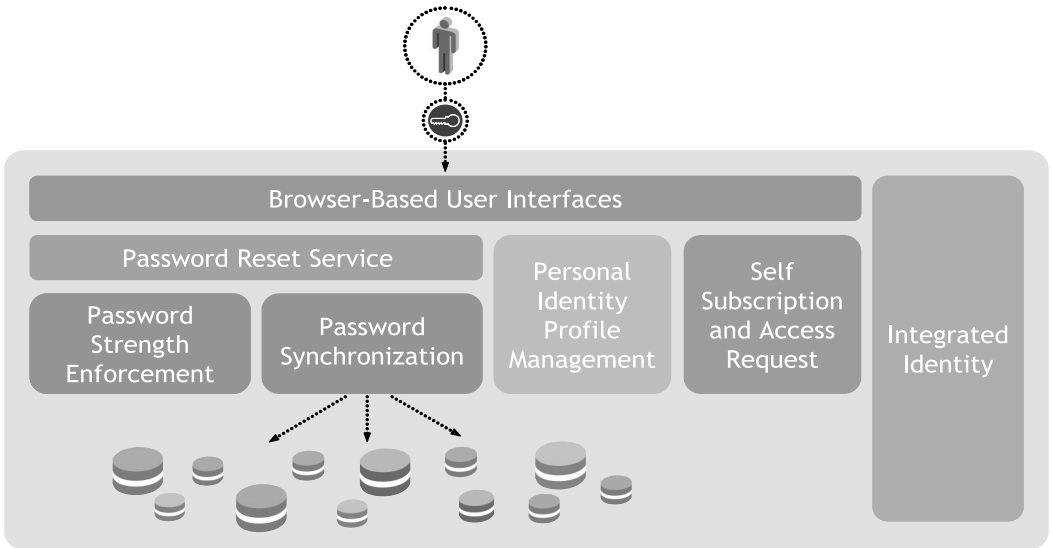


Figure 10: The Novell Self Service Password & Identity Management Solution Components

The Novell Self Service Password & Identity Management components leverage Novell Integrated Identity to provide a solution to the problem of managing Identity and forgotten passwords:

- **Self Service Password Reset**—Through simple browser-based interfaces, end users can easily and quickly initiate password resets as necessary. All reset capabilities are fully automated and therefore do not require assistance from Help Desk personnel (although the interfaces are available to them as well). To properly authenticate users in the absence of a password, the system challenges the user with a series of questions drawn from their Identity profile, such as birth date, mother's maiden name, employment start date, etc. The list of questions asked, and the number of questions asked, is fully configurable by the corporation to ensure the desired level of authentication. Following authentication, the user's password may be reset to a given value, or may be e-mailed to them for subsequent use.
- **Selective Password Synchronization**—While some enterprises may choose to enable single sign-on through password synchronization following password resets, others may choose to limit synchronization to avoid potential security issues associated with having the same password on multiple systems. Novell Self Service Password Reset features are flexible enough to support the unique password synchronization policies and needs of each enterprise, whatever those might be.
- **Password Strength Policy Enforcement**—Password Management includes the capability to establish Policy enforcing the strength of all new passwords set through its interfaces. Policy can control the length, formation, required and/or prohibited characters, use of dictionary words, reuse of previous passwords, etc. Password Strength Policy Enforcement enhances security by ensuring that users do not choose passwords that are easily guessed or attacked.
- **Self Service Identity Profile Management**—Self Service Identity Profile Management enables end users to manage the personal information in their Identity without requiring IT assistance. Self service interfaces allow the end user to view and edit profile information as authorized, including the ability to edit information relevant to the challenge-response questions involved in password resets.

Self Service Password & Identity Management provides seemingly simple but compelling value. Through consistent enforcement of strong passwords, corporations increase security. Through self service password resets, corporations reduce costs by decreasing the need for Help Desk assistance. Through timely password resets, corporations increase profitability through enhanced employee productivity. The Novell suite of solution components provides a solid foundation for the development of customized Self Service Password & Identity Management solutions based upon the proven principals of Secure Identity Management.

Provisioning Solutions

How can corporations deal with the administrative tasks associated with large, dynamically changing user populations, frequent organizational changes, mergers, acquisitions and evolving extranet partnerships? As a user's responsibilities change, so do their requirements for resource access, wherein existing privileges must be revoked in favor of privileges relevant to new responsibilities. Provisioning provides a solution to the administrative problems caused by frequent workforce changes by combining the end user self service components of Secure Identity Management with Policy-based synchronization of user accounts and passwords across the broad myriad of enterprise platforms and applications to ensure that end users have timely access to the resources they require. Furthermore, as employee, partner, customer and supplier access is no longer appropriate, Provisioning enables fast, easy deactivation of privileges to ensure the continued security of information assets.

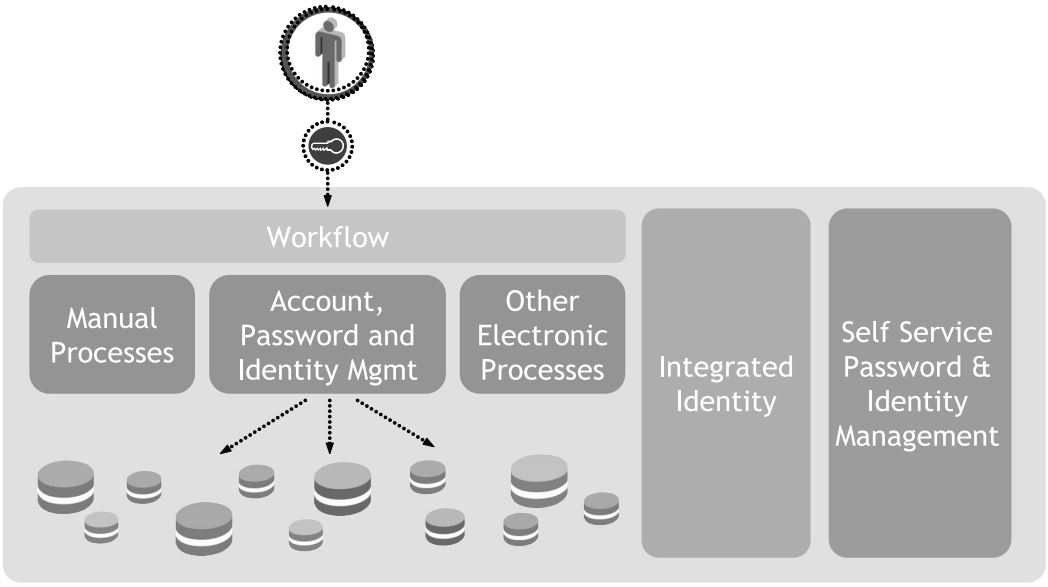


Figure 11: Novell Provisioning Solution Components

Provisioning accommodates frequent changes to user accounts by formalizing repeatable IT account management processes, both physical and electronic, into structured workflows that can be automatically triggered and executed to ensure fast, reliable Identity-based service without burdening IT personnel. Provisioning actions are further automated by integrating with corporate platforms representing Authoritative Sources of Identity, such as human resources applications, to enable automated functions to be triggered by changes in Identity. For instance, when a new employee is hired and Human Resources personnel enter their information into the Human Resources database, the changes are automatically detected by the Provisioning solution that subsequently creates user accounts on appropriate servers and applications throughout the company. Provisioning relies upon Policy to determine the set of systems on which to

create accounts, based upon Identity attributes of the employee such as the department and job functions to which they are assigned.

The Novell Provisioning components provide powerful solutions to the IT account management burden resulting from frequent employee workforce changes:

- By integrating with corporate applications through Integrated Identity, Provisioning respects Authoritative Sources and organizational, political and security boundaries to trigger resource access management.
- By speeding the granting of access to resources, and by including SIM functionality such as self service of Identity and self-subscription to resources, Provisioning increases employee productivity.
- By automating account management activities, Provisioning decreases administrative and Help Desk costs.
- By enforcing the comprehensive de-provisioning of resource access through formalized automated processes, Provisioning increases security and facilitates the consistency and accuracy of system status.
- By supporting standards-based system integration via XML, Novell Provisioning solutions work with today's IT environments and are engineered to accommodate additional systems as corporate needs change.

For corporations experiencing rapid workforce change, Novell Provisioning provides solutions for resource access management that scalably enables IT personnel to keep up with the never-ending need to manage a multitude of privileges while simultaneously delivering consistently high levels of customer service.

Web Access Control Solutions

Due to inherent limitations in Web servers, many enterprise Web-based applications lack the ability to properly authenticate and authorize users. One historical approach to solving this problem has been to build custom methods for authentication and authorization into Web applications themselves, but doing so simply increases the management burden on IT as each application requires separate administration of user accounts and privileges. The scope of this problem becomes significantly greater as corporations implement a large number of Web applications and attempt to scale their administration of access rights across all those systems. What corporations need is a single solution that uniformly secures access to enterprise Web applications, simplifies and speeds access rights management, reduces associated management costs, increases security and enhances usability as a whole.

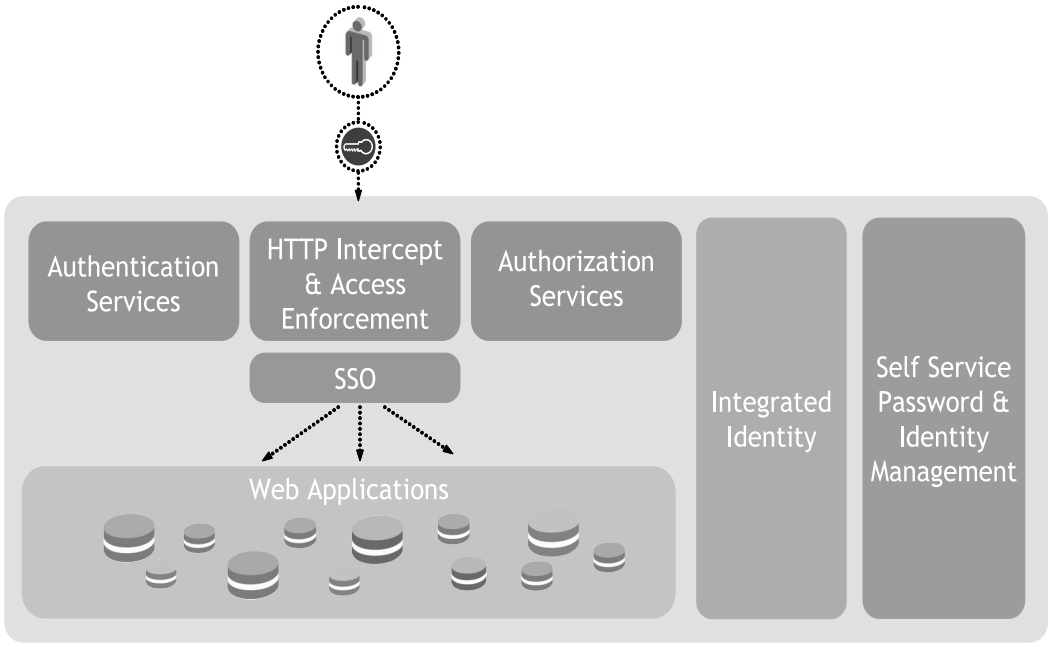


Figure 12: Novell Web Access Control Solution Components

Novell Web Access Control solutions provide the following high-level capabilities:

- **Uniform Authentication & Authorization**—Web Access Control provides uniform authentication and authorization for access to enterprise Web applications. As users attempt to access protected systems, Web Access Control intercepts the request and enforces a consistent secure Web-based login regardless of whether the application was developed in-house, by Novell or by some other vendor. Web Access Control inherits the full services of Novell Federated Authentication, thus supporting everything from simple passwords to strong, graded and multi-factor authentication. Once authenticated, Web Access Control checks the user's Identity to ensure that the user has been granted access rights. If authentication and authorization are both successful, access to the Web-based application is allowed.
- **Web Single Sign-On**—Web Single Sign-On enables end users to authenticate just once to access all protected corporate Web applications. Once authenticated by Novell Federated Authentication to ensure that Single Sign-On services cannot be abused, all subsequent access to other protected corporate Web applications during that session leverage the prior authentication. Having to remember only a single password and enter credentials only once increases user satisfaction and simplifies user access, thus increasing productivity. Web Single Sign-On also provides automated HTML form fill-in services, therefore automatically remembering and inserting credentials into login pages presented by Web applications that already include integrated authentication and authorization services.

- **Federated Authentication**—Web Access Control enables trusted authentication, under corporate control, to extranet business partner Web services and applications (sometimes referred to as "Affiliate Services") through support for SAML-based Federated Authentication and Liberty-based single sign-on. When used for this purpose, Federated Authentication enables an employee who authenticates to internal applications to subsequently enjoy access to protected extranet partner Web applications without an additional login.
- **Simplified Web Application Development**—While Web Access Control provides automatic form fill-in to support legacy Web applications that prompt for authentication, its capability to provide uniform authentication and authorization, as well as enabling personalization, for any Web application means that corporate developers no longer have to worry about these issues when creating applications, thus simplifying and speeding development.

As with Novell Provisioning, Novell Web Access Control leverages Secure Identity Management to gain efficiencies in administration that overcome the problems associated with management of privileges for a large, dynamic user population. Web Access Control leverages Workflow capabilities to automate access rights management, integrates with Self Service to permit users to easily create accounts and request access to protected resources, and provides Role-based Administration and Delegation to enable privileges to be scalably managed by a small number of administrators.

Single Sign-On Solutions

As the number of internal systems that users interact with increases, so do problems associated with their usage of account names and passwords. In many cases IT may intentionally choose to pursue strategies in which end users have a different account name and password on each managed system, thus increasing the chances of forgotten passwords and reduced end user productivity as a result of multiple logins and the frequent need for password resets. Novell Single Sign-On solutions securely facilitate usage of accounts in environments where IT desires to maintain different account names and passwords on each system by enabling end users to authenticate just once at their workstation and subsequently enjoy automatic login to all intranet, Internet and extranet systems.

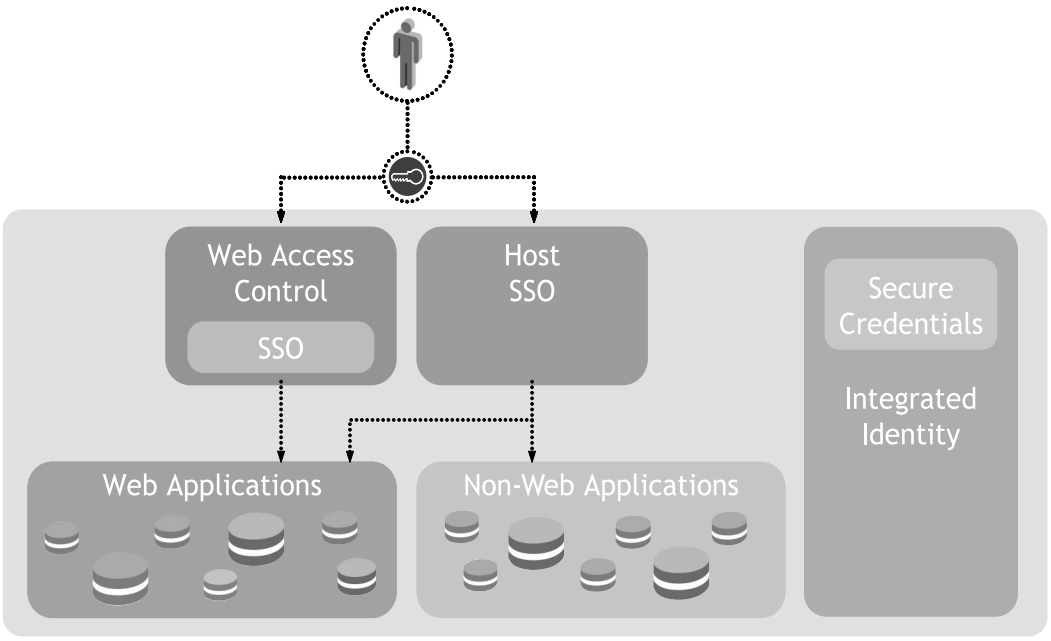


Figure 13: Novell Single Sign-On Solution Components

Novell Single Sign-On solutions provide the following high level capabilities:

- **Web Single Sign-On**—Single Sign-On to Web applications, provided by Novell Web Access Control solutions, enables end users to authenticate just once to access all protected corporate Web applications. Following strong authentication by Novell Federated Authentication services, all subsequent access to other protected corporate Web applications during that session leverages the prior authentication. Web Single Sign-On also provides automated HTML form fill-in services, therefore automatically remembering and inserting credentials into login pages presented by Web applications that already include integrated authentication and authorization services.
- **Host Single Sign-On**—Host Single Sign-On is a desktop-centric solution that supports automated login to corporate applications of all types, including Windows*-based desktop applications, Java* applications, browser-based applications, terminal emulators, servers, Citrix* sessions, Telnet and client-server systems. Host Single Sign-On components installed on the workstation detect login prompts within each of these types of applications and automatically submit the appropriate credentials. Credentials are associated with login prompts through easy-to-use wizard interfaces.
- **Uniform Support for Strong Authentication**—Host Single Sign-On capabilities are enabled through a single initial login at the workstation. When implemented in conjunction with Directory Services, administrators can mandate the form of authentication that must be performed during this login. Because Host

Single Sign-On includes integration with Novell Federated Authentication technologies, enterprises can easily choose to enforce usage of strong and multi-factor authentication, capabilities that are simplified through centralized management of authentication configuration and associated services.

- **Password Policy Enforcement**—Host Single Sign-On also includes features enabling administrators to enforce the strength of all passwords created by end users. Policy can control the length and other characteristics required for each password, thus enhancing security by ensuring that users do not choose passwords that are easily guessed or attacked. Administrators can optionally choose to have passwords automatically generated according to Policy, thus eliminating the burden of password creation from end users, and increasing security by ensuring that a different password is created for each system.
- **Secure Credentials Storage**—When used in conjunction with Novell eDirectory™, Host Single Sign-On provides patented secure storage of login credentials that ensures that each user's passwords cannot be retrieved by anyone else, including system administrators.
- **Support for Disconnected Usage**—Host Single Sign-On supports the needs of mobile users by providing secure local caching of login credentials such that Single Sign-On can continue to be performed regardless of whether the end user is connected to the corporate network.

Through Novell Single Sign-on solutions, enterprises can solve usability and security problems associated with authentication to heterogeneous systems. Web Single Sign-On simplifies user access to Web-based systems, while Host Single Sign-On provides desktop-centric services simplifying access to enterprise systems of all types. Single Sign-On enhances employee productivity and satisfaction, and increases security through uniform enforcement of strong authentication, secure storage of credentials, support for different passwords on each system and policy-based enforcement of password strength. Novell Single Sign-On solutions also help reduce costs by automating the creation and usage of passwords, therefore making it significantly less likely that end users will burden the Help Desk with account usage issues and password reset requests.

Secure Logging & Auditing Solutions

Enterprises are faced with the need to ensure that their resources can be created, accessed, used, configured and maintained only as intended, and only in authorized ways. While proper administration practices, accurate assignment of access rights and Federated Authentication all assist greatly in protecting the integrity of systems and data, the only sure way that enterprises can determine if their systems are being utilized as intended is by periodically reviewing their actual usage for expected, and unexpected, activities. To aid such efforts, Novell provides a powerful secure logging service facilitating the security and auditing of Identity Management solutions and other enterprise systems.

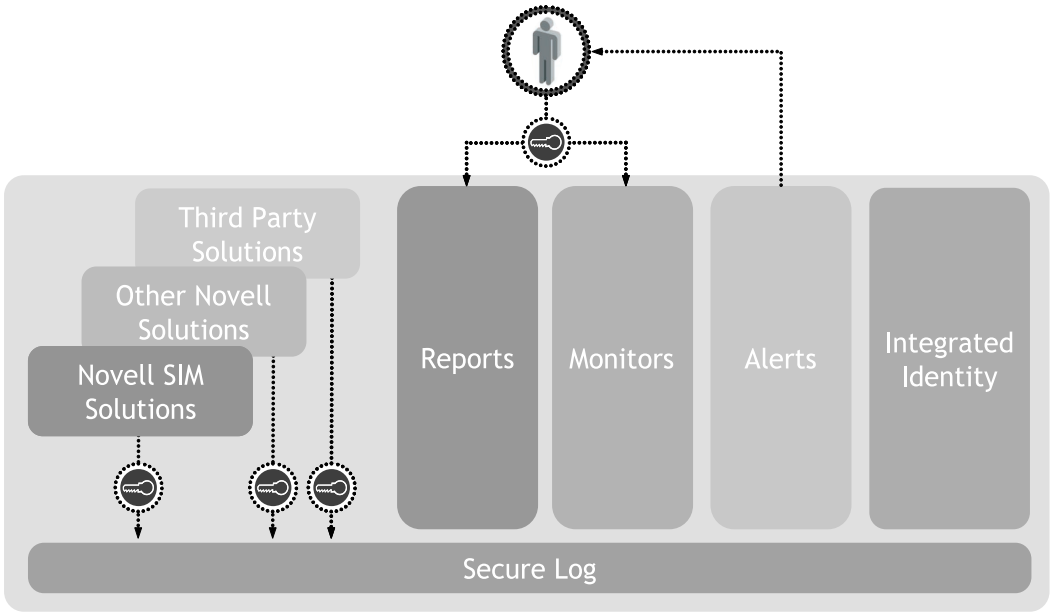


Figure 14: Novell Secure Logging & Auditing Solution Components

Novell Secure Logging & Auditing Solutions provide the following high-level capabilities:

- *Secure capture, filtering and storage of logged information*

  The Novell secure logging service collects information from all Novell Secure Identity Management components as well as from other Novell solutions and third-party products, and allows selective (filtered) logging of that information as necessary to meet unique auditing needs. System administrators can choose the systems from which to accept information and the types of information items to be logged.

  The Novell secure logging service comprehensively ensures the integrity of logged data. Prior to accepting information from an application, the logging server and application can be required to employ mutual authentication to ensure that information is being received from, and logged to, authorized systems. All information can then be digitally signed to ensure that it isn't tampered with before or after arriving at the logging server, and can also be encrypted during transmission to prevent unintended review by unauthorized parties. To further strengthen the system by ensuring that any tampering with logged information can be detected, sequential information items can be signed using digital signature chaining techniques to protect against subsequent deletions, additions or modifications.

  The Novell secure logging service supports a variety of storage formats including high performance databases to facilitate the scalability and performance of the solution.

- *Support for occasionally connected applications*

  The Novell secure logging service supports logging of information from occasionally

connected applications and systems, thus enabling the auditing of mobile systems as well as those accessible via intermittent network links. Such systems continue to provide information even when the logging server is inaccessible, and all captured information is automatically sent to the logging server when a subsequent connection is eventually established. Through this capability, the Novell secure logging service robustly supports the increasingly distributed and mobile nature of enterprise systems.

- *Reports*

  The Novell secure logging service provides a variety of pre-configured reports that enable logged information to be easily reviewed and analyzed. Third-party reporting tools may also be used, thus enabling the system to meet virtually any reporting and auditing need. To facilitate use of logged information, Novell has carefully organized the data to ensure that it can be quickly and easily searched, correlated and reported upon.

- *Real-time monitors*

  The Novell secure logging service includes real-time monitors that allow the filtered display of logged information as it is being captured. Monitors allow enterprises to observe resource usage and therefore identify system running outside of their desired configuration, such as can occur during password and Denial of Service attacks. The Novell secure logging service can be configured to display only the exact information desired, and only from selected systems and applications.

- *Real-time alerts*

  The Novell secure logging service also allows real-time notification of selected log information via alerts. The system administrator can select the information items that are to be forwarded as alerts, and subsequent occurrences will trigger immediate delivery so that administrative action can be taken to deal with the associated security-related occurrences or unexpected operational states. System administrators can choose whether to receive each Alert via e-mail, SNMP, SYSLOG entries, flat file entries or Java JMS messages. The Novell solution also provides alerts allowing the value of a selected directory services attribute to be automatically reset to a pre-defined value if the attribute is changed in any way, thus ensuring the continued proper configuration of the associated system or application.

- *Open and extensible cross-platform service*

  The Novell secure logging service is open and extensible, providing a variety of APIs enabling any type of system or application to easily log information, send alerts via alternative delivery mechanisms, and to store logged information in additional repositories. Full support for all functionality of the system is provided on a variety of platforms including Windows, UNIX*, Linux* and NetWare® systems.

Novell Secure Logging & Auditing Solution enables enterprises to confirm that Policy is being correctly and comprehensively implemented throughout their Secure Identity Management solutions, and allows detection of system break-ins and other undesirable occurrences. By analyzing event logs and alerts, enterprises can determine when their systems are being utilized, by whom, and in what manner. Log analysis further aids the effort to properly enforce privileges and ensure that compliance with applicable governmental regulations is being achieved.

TECHNICAL OVERVIEW OF NOVELL SIM ARCHITECTURE

Novell has created a Secure Identity Management architecture that is uniquely capable of meeting current and future needs for highly customizable Policy-based solutions that work together to create a unified, manageable secure access environment. Novell recognizes that every customer has different needs, they have a different set of systems and applications that must be managed, those systems are configured and utilized in unique ways, and every customer has a unique set of Corporate Policies that they desire to enforce. Corporate Policies change over time, as do systems and applications and IT infrastructure, therefore Secure Identity Management must be adaptable and evolve to accommodate such change. As well, enterprises desire to adopt new solutions through an evolutionary, rather than revolutionary, approach and therefore Identity Management must allow graceful implementation of increasingly sophisticated solutions, integrating existing systems as well as new standards such as Web services, that work together as needs mature. Secure Identity Management is fundamentally about creating robust solutions based upon each enterprise's unique needs for Policy-based management, whatever those needs might be, and therefore enterprises should be looking for vendors offering flexibility, an enduring vision for the future and a comprehensive approach supporting all possible Identity Management solutions.

Novell Identity Automation Framework

The Novell *Identity Automation Framework* is designed to provide a flexible foundation for meeting the demanding needs of Secure Identity Management customers. This framework, depicted in Figure 15, is designed to encompass all of the components of Secure Identity Management while also accommodating integration with third-party applications and other systems as required.

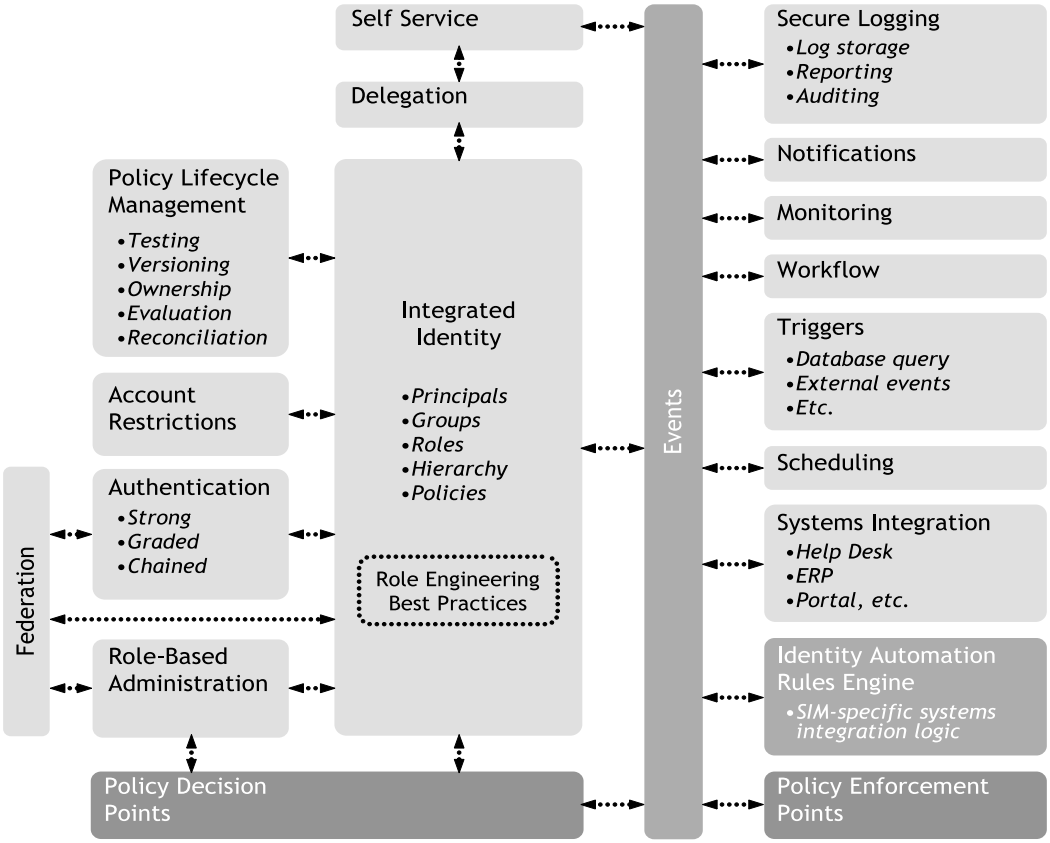


Figure 15: Novell Identity Automation Framework

The following features of the Identity Automation Framework will enable Novell to excel in its ability to deliver Secure Identity Management solutions:

- *Powerful Event Driven Architecture*

  The key foundational advantage of the Identity Automation Framework is that it is designed to be an "event driven" system. In this paradigm, all components of the system expose their high-level functionality via input events (command-related) and output events (information-related). For example, a Workflow module might produce and consume the following events (among others):

  - it might comply with a command event requesting it to begin execution of a specific workflow process
  - it might produce an informational event indicating that it is beginning to execute a specific workflow process
  - it might produce an informational event indicating that it is beginning to execute a specific task within a specific workflow process
  - it might produce an informational event indicating that a specific workflow process definition has been changed
  - it might produce an informational event indicating that a specific task within a specific workflow process has failed

Events provide the fundamental capability enabling Secure Identity Management components to work together in ultimately flexible ways. For instance, the following example of a provisioning process to provide an employee with remote VPN access to the corporate network demonstrates how one component might utilize events to control the execution of a simple, highly customized process involving actions by other components in the Identity Automation Framework:

1. The employee uses a Web-based self service interface, constructed by IT using Self Service components, to request that his laptop be enabled with VPN access. Upon completion of the Web-based request form, the Self Service module sets an attribute in the employee's Identity indicating that VPN access is requested.
2. The Provisioning system detects the change to the employee's Identity and begins by sending a command event to the corporate certificate server requesting that a digital certificate be minted for the employee for use during VPN authentication.
3. The Provisioning system automatically creates an account for the user on the VPN server.
4. The Provisioning system queries the corporate resource management system to determine whether the employee's laptop has a network adapter installed. If no network adapter is present, the Provisioning system sends a command event to the Workflow module to initiate the process to procure and install a network adapter.
5. The Provisioning system sends a command event to the Workflow module to initiate the process to install and configure the VPN client software.
6. The Provisioning system registers the newly minted digital certificate for VPN authentication with the desktop single sign-on service, thus enabling seamless, secure VPN login for the employee following authentication to the desktop.
7. The Provisioning system sends a command event to the Scheduling module to schedule the delivery of an e-mail, after seven days, soliciting the employee to complete a customer satisfaction survey regarding the quality of IT service delivered.

This example demonstrates a few important points that should be appreciated:

— **Customization Without Custom Code**— The actions in the example describe a highly customized process that could be realized very simply. The hypothetical process was executed by a number of independent services, each of which provided a specific function (user interface, provisioning, workflow, scheduling, etc.). The modules operated completely independently, and asynchronously, based upon their own activities as well as the actions of other components as expressed through events. Other architectures would require this process to be described

through custom code (C++ or Java), or might not support this process at all, whereas the Identity Automation Framework is designed to allow the process to be expressed by simply specifying the input and output of events associated with the desired user interface activities, provisioning activities, workflow steps and scheduled tasks.

- **Highly Extensible**—The Identity Management components involved in this example process represent highly modular services communicating through a standards-based event mechanism. The association of events with automation services such as Workflow tasks supports easy extensibility because no service-specific APIs were called, therefore framework service components could be easily replaced or upgraded, and doing so would cause no disruption to existing solutions as long as the new components process the same events. As well, additional new framework service components could be easily introduced at any time and utilized simply by associating their new service-specific events with provisioning tasks and other Secure Identity Management functions.
- **Simplified Distributed Operation**—The framework service components in this example could easily be widely distributed across geographical boundaries, and yet the processes involved would continue to function identically. The Identity Automation Framework is designed to leverage the event abstraction in which the complexities of distributed and disconnected communications are embedded within the framework to ensure that events can be sent whenever desired and are subsequently reliably delivered when network conditions allow. By eliminating the need for services to be designed for robust distributed operation, new framework components will be easier to develop and existing systems and applications can be made to fully participate in enterprise-wide Secure Identity Management.

The Identity Automation Framework's event driven architecture is designed to provide a unique, flexible foundation for implementation of Secure Identity Management solutions. Solutions gain the benefits of modularity and simplicity as well as flexibility to meet almost any need. Event-based communication is designed to fully support LAN, WAN and occasionally disconnected implementation, transactional operations, client-server as well as peer-to-peer and many-to-many usage, and is a mature computing paradigm that has been well proven through mission critical distributed enterprise deployments.

- *Identity Automation Rules*

  While process automation features such as Workflow, Notification, Triggers and Scheduling

can associate simple events with the execution of Secure Identity Management tasks, the Novell architecture is also designed to support the inclusion of advanced business logic to further facilitate solution development. The Novell Identity Automation Rules are designed to allow the solution developer to easily develop SIM-related business logic through the use of simple point-and-click interfaces, thereby greatly simplifying and speeding implementation while also reducing the need for advanced developer resources.

Identity Automation Rules are designed to provide the following benefits:

- *Customized solutions through advanced business logic*
  Identity Automation Rules are designed to allow the solution developer to create Identity Management-oriented business logic including logical operators (AND, OR, NOT), conditional control (IF, THEN, ELSE), data variables and other logic constructs through an easy-to-use wizard-based interface. Identity Automation Rules will allow calls to other rules as well as procedures exposed by external processes such as Web services. Identity Automation Rules are designed to interact with framework service components in the same manner as other components—by sending and receiving events, therefore enabling them to powerfully integrate the actions of those components to achieve the desired solution behavior.
- *Simple integration with all Identity Automation Framework components*
  Identity Automation Rules are designed to be individually invoked by any framework system component simply by issuing the appropriate command event. The Identity Automation Rules engine will detect the event and execute the referenced rule as requested. Direct interaction between individual framework service components via events or APIs might be used to handle simple integration needs, while components could easily invoke Identity Automation Rules to satisfy more-sophisticated tasks, which could then in turn invoke other framework service components via events as appropriate.
- *Simplified solution customization*
  Identity Automation Rules are designed to simplify and empower solution development by moving customization logic out of C++ and Java and into the point-and-click interface of the Identity Automation Framework where they can be securely managed and easily modified as needed throughout the life of the solution. This moves business rules development and maintenance from the hands of application-level programmers into the hands of business analysts and similar personnel responsible for implementation of Policy and process.

- *Rules capabilities for applications natively lacking Rules*
  Because Identity Automation Rules are designed as a component of the Identity Automation Framework, they can be used in conjunction with any application, Web service or platform that integrates with the framework by producing and consuming events (either directly, or through an agent adapter). As such, Identity Automation Rules are architected to enhance applications, including legacy and third-party applications, never designed with such capabilities in mind, and therefore could be used to thoroughly integrate them into Secure Identity Management solutions. For example, an Identity Automation Rule could be associated with Web access control to an existing application offering premium services to hotel guests so that access is now allowed only by elite status customers, even though the application performs no such verification of elite status itself.

- *Fully extensible*
  Identity Automation Rules are designed to be fully extensible, allowing the rules engine and authoring environment to support additional new service-specific logical operators, variables and commands as needed to support the unique functionality of each framework service component. Through this easy extensibility, the Identity Automation Rules architecture allows graceful upgrades of existing framework service components, and introduction of new components, without disrupting the operation of existing solutions.

The Novell Identity Automation Rules are designed to leverage the proven concepts of modularity, event-based systems and "wizard" interfaces to enable the creation of highly customized Secure Identity Management solutions faster and with fewer resources. Identity Automation Rules will empower the solution developer to integrate Novell Secure Identity Management components with third-party applications and custom Policy Decision Points to enforce Policy however and wherever necessary.

- *Support For All Types of Integration*
  While the Identity Automation Framework incorporates event-based distributed communication services, and Identity Automation Rules are designed to enable powerful integration of framework service components via sending and receiving events, it is also possible to integrate components through direct means as desired using traditional C and Java APIs, standards-based Web services interfaces and popular application server technologies such as J2EE*.

  The Identity Automation Framework architecture also supports integration with third-party applications through powerful data

synchronization technologies that enable support for Authoritative Sources of information, dynamic data transformation, application-specific rules and event generation. This system provides the foundation for Novell Integrated Identity capability, and also acts as a powerful universal framework for the development of application-specific drivers (sometimes called "agents" or "connectors"). Whereas other Identity Management vendors offer single-purpose agents, Novell drivers are fully extensible to meet unique customer needs.

- *Policy Decision Point Independent*
  While Novell offers popular Secure Identity Management solutions including Self Service Password & Identity Management, Provisioning, Web Access Control and Secure Logging & Auditing, the Novell framework is designed to allow additional Policy Decision Points and Policy Enforcement Points to take equal advantage of its capabilities to powerfully enable them with Secure Identity Management capabilities as well.

  From a general perspective, "Policy Decision Points" (PDPs) are applications that make Policy-based decisions, such as access control decisions, using Identity and other information. "Policy Enforcement Points" (PEPs) are application components that enforce the Policy decisions made by their corresponding PDP. For example, Novell iChain®, which provides Web Access Control, is a PDP in that it utilizes Identity to determine which users have been granted access rights to protected internal Web applications, and is also a PEP in that it enforces those access rights by preventing unauthorized access to the protected applications. The Novell Identity Automation Framework is designed to enable any type of PDP and PEP to participate in Secure Identity Management by leveraging the management efficiencies and framework services it offers.

- *Secure Foundation*
  In addition to providing security-related services such as Federated Authentication, Secure Logging & Auditing, Account Restrictions, Notification and Monitoring, The Novell Identity Automation Framework is also designed to enhance the confidentiality, integrity and availability of solutions through the following features:

  — Novell architecture supports the use of Novell Federated Authentication services to authenticate all framework service components, all users and all administrators of the system.
  — Novell architecture supports the encryption of all communications between Identity Automation Framework components.
  — Novell architecture supports the protected access to information residing in the Integrated Identity service, and as well as access to all events, through proper authorization.

- Novell architecture accommodates Authoritative Sources to ensure the integrity of Integrated Identity
- Novell architecture supports secure logging for auditing of all events, whether generated by an administrative action or created as part of an Identity-based solution.
- Novell architecture supports the monitoring of all Identity Automation Framework components, and is designed to allow alerts to be generated when security-related events occur.

Meeting Architectural Challenges

Novell has designed its Secure Identity Management architecture to address the following technical challenges:

- *Integrated Identity*

  For many enterprises, centralized Identity Management is an unrealistic requirement. For these enterprises, organizational, political and security boundaries, as well as numerous technical realities, require Integrated Identity in which multiple Authoritative Sources of Identity are fully supported. The Novell architecture uniquely supports federation of Identity between existing internal systems, as well as federation with external trusted sources via standards-based mechanisms. The Novell architecture provides robust management and enterprise-wide availability of all Integrated Identity information.

- *Comprehensive, Unified Solution Framework*

  To achieve the ROI promised by Secure Identity Management, all solutions must work seamlessly together to ensure that customers do not end up with disparate solution silos. Adopting multiple independent Identity Management solutions can result in increased complexity due to the need to integrate those systems, increased technical support and training costs, and difficultly achieving compliance with Corporate Policies and governmental regulations due to the lack of a unified secure logging and auditing infrastructure. Solution silos also don't scale well, as each additional disparate system adds to these business issues while it attempts to solve some other problem. The Novell architecture is designed to address these issues by enabling a common set of powerful components to be utilized as the foundation for all possible Secure Identity Management solutions across all platforms.

- *Reduced Cost of Ownership*

  A fundamental value of Secure Identity Management is the implementation of Role-based Administration, Delegation, Workflow, Self Service, Triggers, Scheduling and Policy Lifecycle Management to dramatically reduce the cost of resource access management; however, the corporate need to maintain existing organizational, political and security boundaries and use of associated native system administration techniques results in significant additional expense as Identity must

often be duplicated across disparate systems. The Novell architecture is designed to deliver a superior ROI by eliminating duplicate Identity Management efforts across disparate systems while respecting Authoritative Sources, and by providing a common underlying framework that can be leveraged again and again for all possible Secure Identity Management solutions.

- *Flexible Customization Capabilities*
  Every customer has unique Identity Management needs, therefore many Identity Management solutions require customization. Identity Management solutions built from inflexible, monolithic products offering limited capabilities cannot easily accommodate such customization. Enterprises require an Identity Management foundation that anticipates total customization as a priority. The Novell architecture is designed to uniquely accommodate customization through modular shared components, a variety of programmability and scripting methods, robust distributed operation and an ultimately flexible event driven operational paradigm.

- *Simplified Customization*
  Solution customization via complex APIs requires expensive development personnel and lengthens implementation times. Because Identity Management solutions can require significant customization to meet unique customer needs, API-based customization can have a significant impact on overall costs. The Novell architecture is designed to uniquely simplify customization by moving, when appropriate, business and integration logic out of API-based code and into an extensible Identity Automation Rules engine where such logic can be developed through simple point-and-click interfaces without requiring the assistance of a C++ or Java programmer.

- *Support for Third-party and Corporate Applications*
  Identity Management is more than a layer on top of existing systems—it also involves complex integration with corporate systems and third-party applications. Identity Management solutions designed as a single-purpose layer cannot accommodate systems integration without significant advanced development efforts. The Novell architecture is designed to uniquely enable systems integration as a fundamental component of Secure Identity Management by providing a robust infrastructure supporting standards-based technologies, Authoritative Sources, application-specific Policies, use of automation rules on a system-specific basis, a general purpose agent/connector framework and bi-directional synchronization of data.

- *Support for Occasionally Disconnected Systems*
  Today's typical corporate IT environment consists of a broad variety of systems, including those that are occasionally disconnected from the network. Mobile systems such as laptops and handhelds, as well as servers and applications

located across intermittent WAN links, need to be supported by Identity Management solutions to the same degree as LAN-based systems. The Novell architecture is designed to fully support the development of Secure Identity Management capabilities across all corporate systems regardless of when and where they are connected.

- *Enhanced Partner Opportunity*

  The need for highly customized Secure Identity Management solutions is great, and the Novell architecture is designed to uniquely enable development of these solutions with less effort, fewer development resources and reduced time. Solution Providers and other channel partners seeking to offer Secure Identity Management solutions will find that the Novell architecture represents a solid foundation for their future solutions practice.

- *Forward Looking*

  The highly flexible Novell architecture is designed to provide a generalized framework for empowering systems with a comprehensive set of Identity Management features. As such, the Novell architecture makes no assumptions about the nature of the systems being integrated, the location of those systems, the platforms on which they run, or the type of Identity-based solution being implemented through the framework. As a result, the Novell architecture is uniquely forward looking—being designed to enable today's popular Secure Identity Management solutions while also fully accommodating unforeseen customer needs, new technologies such as Web services, and other standards and developments that will arise in the future.

Unique Novell Technology Advantages

With the Identity Automation Framework, Novell is building toward an optimal Secure Identity Management architecture. Its unique flexibility is designed to enable Novell to effectively meet the needs of enterprises by ensuring a complete, uniform administrative solution for Identity-based solutions of all types. While the Identity Automation Framework is being delivered in phases as part of the Novell solution offerings, strategic portions of the framework are available today and are already being utilized by Novell to ensure customer success:

- *Novell eDirectory*

  Novell eDirectory, the market-leading, LDAP-compliant directory service, provides the foundation for Integrated Identity—the basis of all Secure Identity Management solutions. eDirectory, with over 1.4 billion active user licenses, offers a proven scalable foundation for Policy-based applications, capable of true cross platform enterprise-wide deployment.

  Novell eDirectory also enables management of users and other Principals within the Integrated Identity. eDirectory includes iManager, a portal-based Web administrative console that enables easy creation and modification of users, Principals, Organizational Units and all other entities within the

hierarchical structure of the directory. Because it acts as the repository for Groups and Roles, eDirectory also provides the foundation for Role-Based Administration.

Being the access point for Integrated Identity, eDirectory provides, through support for multi-master replication, distributed access to a comprehensive set of events resulting from administrative actions, changes to Identity and other relevant information. These events are critical to the capabilities delivered by the Identity Automation Framework as they allow application-specific customization based upon Identity changes.

- *Novell DirXML®*
  Novell DirXML is the Novell solution for enabling shared Identity across disparate systems and enforcing attribute level authority—the critical feature required to effectively enable Integrated Identity. DirXML supports robust, highly flexible bi-directional synchronization of Identity between the Integrated Identity repository and Authoritative Sources, thereby respecting organizational, political and security boundaries. DirXML's capabilities are provided in real time, permitting changes in individual Identity applications to be quickly propagated to the Integrated Identity and, from there, into other Identity applications throughout the enterprise as needed.

  The DirXML architecture is uniquely capable of facilitating Secure Identity Management and Provisioning by providing complex data transformation services and flexible application-specific rules that expedite systems integration, including the ability to transform application-specific actions and states into generalized events and Triggers for solution providers to act upon when creating customized Identity Management solutions.

  Novell DirXML includes drivers (sometimes called "agents" or "connectors") that support a wide variety of directory services, databases, computing platforms and corporate applications; however, unlike many Identity Management vendors that offer single-purpose agents, Novell drivers provide a generalized solution capable of being extended to meet a wide range of application-specific needs. As such, DirXML can be utilized to develop Policy Enforcement Points of all types, thus simplifying Secure Identity Management by providing a uniformly integrated and managed agent infrastructure.

- *Novell Modular Authentication Service*
  Novell Modular Authentication Service (NMAS™) provides support for a large number of authentication techniques and enables them to be uniformly applied to all Identity Automation Framework-based solutions. Enterprises can implement simple authentication such as username and password, or can centrally enforce strong authentication based upon digital certificates, hardware tokens and biometric devices.

  NMAS simplifies the enforcement of custom levels of security for protected resources. Graded authentication allows less-confidential resources to be protected by simple password,

while access to sensitive information could require automatically prompted re-authentication via a digital certificate. Chaining further enhances per-resource security by supporting multi-factor authentication in which access to resources can require credentials consisting of something that you know (such as a password), something that you have (such as a smart card token), and something that is part of you (such as a fingerprint).

Novell also enables standards-based authentication federation by fully supporting SAML and Liberty—open standards that are being widely adopted by information technology vendors. Through SAML and Liberty, Identity can be federated and single login solutions can be provided across internal systems as well as those of trusted extranet business partners.

- *Novell iChain*

  Novell iChain is the cornerstone of Novell Web Access Control solutions. iChain provides a complete system for securing access to Web applications—even when such applications have not been designed to support advanced authentication and authorization. iChain includes a reverse-proxy server that intercepts all requests to protected Web applications, prompts the user for authentication credentials if they have not previously logged in, and then determines whether the user has been granted rights to access the Web application in question. Once authenticated, subsequent attempts to access other protected Web applications leverage the prior authentication, thus simplifying application usage through single sign-on.

  iChain uniformly enhances security and lowers IT costs. iChain increases security by preventing unauthorized access to applications, and helps deter direct attacks against applications and servers by hiding network addresses through URL re-writing. iChain further increases security by supporting the use of strong, multi-factor authentication uniformly across all Web applications. While increasing security, iChain also leverages the Novell suite of Secure Identity Management technologies to ease administration, automate management tasks and lower associated costs.

- *Novell Nsure Audit*

  Novell Nsure Audit provides the basis for the Novell Secure Logging & Auditing solutions, enabling enterprises to ensure that their resources can be created, accessed, used, configured and maintained only as intended, and only in authorized ways. The Novell open and extensible secure logging service collects information from all Novell Nsure, secure identity management components as well as from other Novell solutions and third-party products, and allows selective (filtered) logging of that information as necessary to meet unique auditing needs. Logged data from all systems is securely captured and stored, even from systems that are occasionally disconnected. Novel Nsure Audit facilitates auditing through inclusion of a variety of pre-built reports, and supports the use of popular reporting packages capable of meeting almost any auditing requirements. Novell Nsure Audit also

enables proactive management of security related issues by providing monitors and alerts that allow enterprises to observe the status of their systems in real time. Through its advanced capabilities, Nsure Audit enables enterprises to immediately identify security threats, demonstrate compliance with governmental security regulations, and confirm that Policy is being correctly and comprehensively implemented throughout their Secure Identity Management solutions.

- *Novell SecureLogin*

  Novell SecureLogin, a component of the Novell Single Sign-On solutions, facilitates usage of accounts in environments where IT desires to maintain different account names and passwords on each system. Novell SecureLogin enables end users to authenticate just once at their workstation and subsequently enjoy automatic login to IT systems of all types. Novell SecureLogin increases security through support for secure credential storage, the uniform enforcement of strong authentication to enable single sign-on across all systems, the enforcement of password policy to ensure the strength of all created passwords, and the automatic generation of passwords to ensure uniqueness. Novell SecureLogin even supports mobile users through secure local caching of login credentials. While helping secure the enterprise, Novell SecureLogin also enhances employee productivity and reduces costs by automating the creation and usage of passwords, therefore making it significantly less likely that end users will burden the Help Desk with account usage issues and password reset requests.

- *Novell eGuide*

  Novell eGuide is a cross-platform, Web-based component of Novell Nsure, secure identity management solutions that provides fully searchable corporate white pages and organizational charts, as well as self service management of personal Identity attributes. With eGuide, users can look up information through an easy-to-use interface that supports "and/or" Boolean searches on any data items, and displays results in a format that operates similar to an address book. eGuide supports the use of any LDAP-compliant directory service, such as Novell eDirectory, as the source for searchable information, and can even be configured to search multiple directory services simultaneously. Administrators can also easily allow users to manage selected attributes of their own personal Identity information such as phone numbers and mail stops through simple self service interfaces. As a result of this capability to delegate management of selected personal Identity attributes to end users, eGuide helps lower costs by reducing the burden on IT and Help Desk personnel while also increasing user productivity and reducing application error.

- *Novell exteNd Composer™*

  Novell exteNd Composer provides an advanced development environment for the creation of

J2EE-compatible applications and components that can customize and enhance Secure Identity Management solutions. Composer includes powerful mechanisms facilitating systems integration, including the ability to access applications on any platform and to incorporate data from repositories across the enterprise. Composer further allows the development of advanced business logic in conjunction with full-featured process design and management. Through its implementation of the Java Message Service (JMS) standard, Composer also fully supports the event-based operational paradigm upon which the Identity Automation Framework is founded, therefore enabling advanced development of automated processes and systems integration-based Secure Identity Management solutions.

Novell exteNd Composer completes the Novell strategy for enabling customization of Secure Identity Management by all types of personnel involved in solution development. exteNd Composer's full-featured Java J2EE development environment accommodates programmers implementing advanced systems integration modules of any type, while Novell Identity Automation Rules accommodate the rapid creation of customization logic through simple point-and-click Web interfaces requiring less programming expertise. For non-programmers such as corporate business analysts responsible for process definition and implementation, customization can also be performed through highly graphical Workflow definition. Finally, Web-based system configuration options enable IT personnel to easily customize the behavior of many operational aspects of the solution. Through these mechanisms, which work together as a cohesive whole, Novell is accommodating the unique needs of each customer, reducing complexity and speeding implementation.

- *Novell Ngage*℠

  Ngage is the Novell solution for applying the power of technology and the expertise of Novell experienced partners and professionals to work for enterprises of all types. With Ngage, corporations can transform the way they work: enabling, optimizing and supporting business without boundaries. Novell Ngage assists enterprises in creating solutions such as Secure Identity Management that are driven by corporate and IT strategy, rapidly delivering business value while leveraging existing infrastructure. Through collaborative, iterative client interaction, Novell and its partners can apply proven project management skills and methodologies to select and implement Secure Identity Management solutions to meet each enterprise's unique needs, while training and educating staff to further optimize return on investment. Ngage brings together Novell partners and the world-class experience of three proven groups within Novell—Novell Consulting®, Novell Training and Novell Technical Services℠—to maximize the potential for IT solutions to result in strategic business success.

SUMMARY & CONCLUSION

While many of today's Identity Management products offer limited breadth and only solve small pieces of a business problem that must be addressed as an integrated whole, the Novell vision provides an innovative new foundation for creating a wide variety of Secure Identity Management solutions that fully integrate to comprehensively meet enterprise secure access management needs. By providing a thorough set of Secure Identity Management components and a uniquely flexible underlying architecture in the form of the Identity Automation Framework, the Novell goal is to deliver a superior customer experience:

- The Novell uniquely capable Integrated Identity enables a comprehensive set of Secure Identity Management solutions, therefore offering a superior return on investment through reduced cost of ownership.
- Novell empowers enterprises with new Identity Management capabilities enabling top-down policy definition, management and enforcement.
- Novell provides a powerful, complete solution for scalably managing large user populations and all types of resource access privileges.
- Novell extends the Identity Management paradigm with new levels of security and flexibility to thoroughly meet the unique needs of every enterprise customer.

The Novell Identity Automation Framework is designed to support Integrated Identity, a feature required for successful implementation of a single Secure Identity Management solution across all systems. Integrated Identity is a virtual aggregation and distribution of Identity from a multitude of Authoritative Sources. Integrated Identity lowers the barriers created by Identity silos by enabling application-specific Identity to be equally utilized by other systems or applications as authorized. Integrated Identity also supports distributed ownership of Identity information by accommodating the organizational, political and security boundaries that exist within many corporations, thus removing these often intractable problems associated with attempting to implement centralized Identity Management.

The Novell Identity Automation Framework is designed to support all features necessary to achieve effective Identity Management. Workflow and Self Service enable the automation of IT processes to speed efforts, automate process execution, augment security and increase employee satisfaction through enhanced quality of service. Role-based Administration and Delegation reduce operational costs by introducing innovative efficiencies and balancing workload. Triggers, Scheduling and systems integration further automate Identity Management processes by accommodating data and systems throughout the enterprise. Finally, Policy Lifecycle Management ensures that Policies and Integrated Identity can be scalably developed and maintained in a distributed manner.

The Novell Identity Automation Framework is also designed to provide features necessary to facilitate the security of Identity Management solutions. Federated Authentication enables

centralized management of authentication services, including support for strong, graded and multi-factor authentication. Secure Logging provides a repository for information regarding end user and administrator actions, thus enabling auditing for corporate and governmental compliance purposes. Account Restrictions ensure that resources can only be accessed as appropriate, and Notifications and Monitoring enable proactive response to security-related events.

The Novell Identity Automation Framework, through its uniquely flexible event-driven architecture, is designed to provide the full benefits of the comprehensive suite of Novell Security Identity Management technologies regardless of the nature of the systems being integrated, the location of those systems, the platforms on which they run, or the type of Identity-based solution being implemented through the framework. The Identity Automation Framework is also designed to support Identity Automation Rules that will enable the use of Identity Management-specific business logic to simplify the creation of highly customized solutions, allowing them to be implemented faster and with fewer resources. Furthermore, the uniquely modular nature of the Identity Automation Framework lends itself to future extension and innovation as the needs of Secure Identity Management customers continue to evolve.

Secure Identity Management is all about providing a scalable, cost effective solution for Identity, Identity Management and the security of corporate systems and data. Its distinctive approach to Integrated Identity, comprehensive Identity Management services, robust security components and innovative architectural vision uniquely positions Novell to satisfy customer needs. Novell Secure Identity Management solutions empower system administrators, employees, customers, partners and suppliers alike, reducing costs and enhancing security. These highly tangible value propositions should encourage enterprises to begin today to consider what Secure Identity Management can do to vitally enhance the effectiveness of their information technology efforts as a strategic component of overall business success.

GLOSSARY

TERM	DEFINITION
Account Restrictions	enable administrators to control the creation and usage of user accounts and passwords through password construction Policies, limitations on time and duration of access, etc.
Agents	components (sometimes called "drivers" or "connectors") of a Policy enforcement application that enforce Policy upon a specific system or Principal
Application-Specific Policy	a Policy that expresses the exact manner by which a Corporate Policy is implemented on a specific managed system or Principal
Authoritative Source	a system or application that acts as a primary provider of a given set of Identity information wherein other systems or applications can consume the Identity if authorized, but are prevented from modifying it
Corporate Policy	a Policy that expresses the desired state of some aspect of a managed system or Principal, but does not detail the exact manner by which that desired state is to be achieved
Delegated Administration	facilitates scalability of management by allowing system administrators to share their responsibilities, or a subset of their responsibilities, with other administrators
Directory Services	a distributed service that maintains Identity information regarding users, systems, applications and other Principals throughout the enterprise, and that generally serves as the foundation for Secure Identity Management
Dynamic Membership Inclusion Rules	rules that allow the membership of a Group or Role to be defined by common criteria, such as one or more LDAP queries
Dynamic Membership Exclusion Rules	rules that allow the membership to a Group or Role to exclude a set of Principals as defined by common criteria, such as one or more LDAP queries
Events	messages produced by system components that contain any type of information, such as indication of a specific occurrence, warning of a threshold being reached, notification of a Policy being changed by an administrator, etc.
Event Driven Architecture	an architecture in which integrated components can react to events produced by other components according to rules established by system administrators and integrators
Federated Authentication	the supported use of any type of authentication technique, including simple, strong, graded and chained authentication, to protect access to resources
Group	an organizational grouping of Principals to facilitate scalability of management and enforcement of Policy
Identity	information and attributes that define aspects of a managed Principal, and that can be acted upon to enforce Policy
Identity Management	the scalable administration of Identity, enabling a small number of system administrators to manage the Policies associated with a large number of users and other Principals throughout the myriad Authoritative Sources in the enterprise
Identity Automation Framework	The Novell technical foundation for its Secure Identity Management solutions in which Integrated Identity, Identity Management and security technologies are fully integrated and can be applied equally to any Policy Decision Point and Policy Enforcement Point
Identity Automation Rules	Identity Management-oriented business logic that allows solution providers to easily customize Novell Secure Identity Management solutions
Integrated Identity	provides systems that enforce Policy with a unified view of all available Identity information anywhere within the enterprise by supporting Authoritative Sources, distributed availability of aggregated Identity, and authorization
JMS (Java Message Service)	an industry-standard API enabling applications written in the Java programming language to flexibly send and receive events

continued on next page

TERM	DEFINITION
LAN	Local Area Network
Monitoring	real-time views of the status, configuration and resource utilization of a system or component
Notifications	real-time alerts delivered via a variety of possible methods such as events, e-mail, SNMP, etc.
Policy	a rule that formalizes the desired state of some aspect of a managed system or Principal
Policy Decision Point (PDP)	an application that makes Policy-based decisions, such as access control decisions, using Identity and other information
Policy Enforcement Point (PEP)	an application component that enforces the Policy decisions made by a corresponding PDP
Policy Lifecycle Management	the use of versioning, testing, ownership, evaluation and reconciliation technologies to facilitate scalable distributed development and management of Policies
Principals	manageable entities that have Identity within a system, such as users, Groups, Roles, workstations, servers, network devices, operating systems, applications, etc.
Provisioning	a solution to the administrative problems caused by frequent workforce changes by combining the end user self service components of Secure Identity Management with Policy-based synchronization of user accounts and passwords across all enterprise platforms and applications to ensure that end users have timely access to the resources they require
ROI	Return On Investment
Role	a functional grouping of Principals to facilitate scalability of management and enforcement of Policy
Role-Based Administration	enables scalable management of users and other Principals by grouping them together so that administrative actions can be applied to all members of the Role at one time
SAML (Security Assertion Markup Language)	an open standard created by the OASIS consortium that specifies mechanisms allowing a compliant application to trust the authentication, authorization and attribute assertions produced by another trusted compliant application
Scheduling	allows any action of a component of the Novell Secure Identity Management solution to be scheduled to occur on a time and date basis
Secure Identity Management	the combination of security-related technologies with the efficiency-oriented features of Identity Management to ensure the confidentiality, integrity and availability of business system resources
Secure Logging	the secure capture and storage of system activities to facilitate management, auditing and regulatory compliance
Self Service	a solution that provides facilities for end users to perform password resets, account registration, Identity profile updates, self subscription to Group or Roles, and request access to protected resources without IT administrator or Help Desk involvement
SIM	Secure Identity Management
Single Sign-On	a feature of Secure Identity Management solutions enabling end users to authenticate once and subsequently leverage that authentication to access additional protected systems without answering additional login prompts
Triggers	provide the ability to accommodate input other than Integrated Identity into the Policy-based management process
WAN	Wide Area Network
Web Access Control	a solution that provides centralized authentication and authorization, in combination with Integrated Identity, Self Service and single sign-on, to facilitate the security of Web-based applications and increase employee productivity

continued on next page

TERM	DEFINITION
Web services	standards-based reusable application components that can be combined to create distributed intranet, Internet and extranet solutions
Workflow	formalizes, documents and automates business processes by allowing the definition of processes as a series of sequential and parallel tasks whose assignment and execution are managed by a Workflow engine
XML	Extensible Markup Language, a structured, text-based method of representing data so that it can be easily interpreted and utilized by multiple applications

Novell Product Training and Support Services

For more information about Novell's worldwide product training, certification programs, consulting and technical support services, please visit:
www.novell.com/ngage

For More Information

Contact your local Novell Solutions Provider, or visit the Novell Web site at:
www.novell.com/nsure

You may also call Novell at:

1 888 321 4272 US/Canada
1 801 861 4272 Worldwide
1 801 861 8473 Facsimile

Novell, Inc.
1800 South Novell Place
Provo, Utah 84606 USA

www.novell.com

Novell

462-001346-001