



Sun™ Identity Manager

The proven, scalable provisioning and compliance solution

Highlights

Cost-effective provisioning and compliance in one streamlined, scalable identity management solution.

- Comprehensive provisioning and identity auditing capabilities
- Seamless integration with role management capabilities that further streamline the provisioning and auditing processes
- Data export capabilities, allowing robust reporting and entitlements management
- Proven scalability in environments with millions of users
- Specifically designed to reduce operational costs with automation, self-service, and delegated administration capabilities
- Non-invasive architecture for fast, easy, cost-effective implementation
- Capabilities to address regulatory mandates as well as internal privacy and policy initiatives
- Repeatable processes for ongoing, sustainable compliance



Years after the adoption of the Sarbanes-Oxley Act of 2002, organizations continue to be challenged by the issue of complying with an ever-growing number of government regulations affecting the integrity of financial and other data and the privacy of sensitive personal information. Identity management has become a cornerstone of their efforts, especially considering identity controls are so often a priority for auditors. The challenge is finding a solution that provides provisioning and auditing capabilities that can be managed in an automated fashion at the business role level.

For most organizations, the first step in incorporating identity management into compliance processes is deploying a user provisioning solution to manage the identity lifecycle. This process is streamlined through the use of a role management solution, where provisioning is done at the business role level. However, traditional provisioning solutions offer little in the way of identity auditing and do nothing to ensure that identity controls are consistently applied across both provisioning and auditing processes. In addition, role management is commonly an afterthought to the initial provisioning project, rather than being an integral part of the provisioning solution.

Complicating matters further is the growing momentum toward collaboration with other organizations, including partners that can help develop competitive new products and services. This means that compliance requirements will ultimately extend beyond enterprise boundaries, and that provisioning solutions must be able to scale to include extranet environments. Without a complete solution that can scale, organizations resort to using

multiple products, building provisioning and auditing into each individual extranet project. However, this approach becomes financially and operationally untenable as the number of projects grows.

Sun™ Identity Manager

Sun Identity Manager is the first provisioning solution to fully address compliance challenges. Identity Manager integrates automated identity lifecycle management with identity auditing capabilities, and makes it possible to manage these processes at the business role level. By applying the same business rules, roles, and audit policies, it ensures consistent enforcement of identity based controls and reduces ongoing operational and compliance costs. It's also easily scalable to the extranet, with proven performance in environments with millions of users. With a large base of installed users, Sun Identity Manager's track record and proven performance have earned it widespread recognition as a leading provisioning solution by top industry analysts and observers.

Comprehensive Role Management

Sun™ Identity Manager leverages business roles to improve both provisioning and identity auditing. Business roles allow managers to grant and approve access to resources and applications in a meaningful business context. Granting and approving access using business roles adds another level of control to the provisioning and auditing processes, ensuring compliance with regulatory requirements.

Industry-leading user provisioning and synchronization

Identity Manager delivers automated provisioning and synchronization services to provision users quickly and accurately and to automatically synchronize user identity data across applications, directories, and data stores. It is designed to reduce costs for both initial deployment and ongoing operations.

Sun Identity Manager is the first provisioning solution to fully address identity auditing challenges.

Identity Manager's provisioning architecture is non-invasive, enabling organizations to implement it with little impact on existing IT infrastructures and enjoy a lower cost of ownership. The solution features simplified connections that use agentless adapters to speed deployment across multiple platforms, applications, directories, and databases. Identity Manager has been shown to enable improvements on internal rate of return (IRR) targets of up to 20%.

A data-sparse architectural approach is an important aspect of being non-invasive. The data-sparse approach collects some personal attributes centrally (such as name, email address, manager, etc.), but only stores a minimal set of the account data necessary to manage each resource. By eliminating the need to set up and maintain complex replication infrastructures for duplication of all account data back to a centralized repository, Identity Manager provides centralized management without the difficulty and delay associated with traditional redundant repository deployments. As more data is needed centrally, Identity Manager has the flexibility to optionally extend the data model to replicate other account attributes.

Once deployed, Identity Manager uses capabilities such as policy-based automation, delegated administration, and self-service to control ongoing provisioning and auditing costs. By automating processes that have been done manually in the past, it speeds provisioning and deprovisioning while ensuring consistently accurate processes. Administrative activities and everyday tasks such as password management are delegated to administrators and users throughout the organization. The results include lower operational costs and workload reductions of up to 80% for administrative and help desk personnel.

Auditing that goes beyond mere logging and reporting

Identity Manager provides policy based integration of the identity lifecycle management and identity auditing processes. This integrated approach is the only way to consistently apply identity based controls across provisioning and auditing processes. By making it possible to

use a single solution to handle essential tasks — such as stopping the improper aggregation of access privileges and detecting excessive access by any user — Identity Manager greatly simplifies compliance.

Identity Manager's identity auditing capabilities include automated reviews and proactive scanning to ensure consistent policy enforcement and repeatable processes. Automated reviews and scanning also enable early detection of and notification about policy violations, helping to reduce their impact.

Reports are key deliverables for audits, and Identity Manager provides compliance reports for major legislative mandates as well as the ability to easily build custom reports. But, Identity Manager goes far beyond simple reporting to provide ongoing policy violation tracking and automated remediation of violations. For example, if a violation is detected during an automated review, the account is automatically disabled pending investigation, and the entire incident is fully documented and reported for auditing purposes.

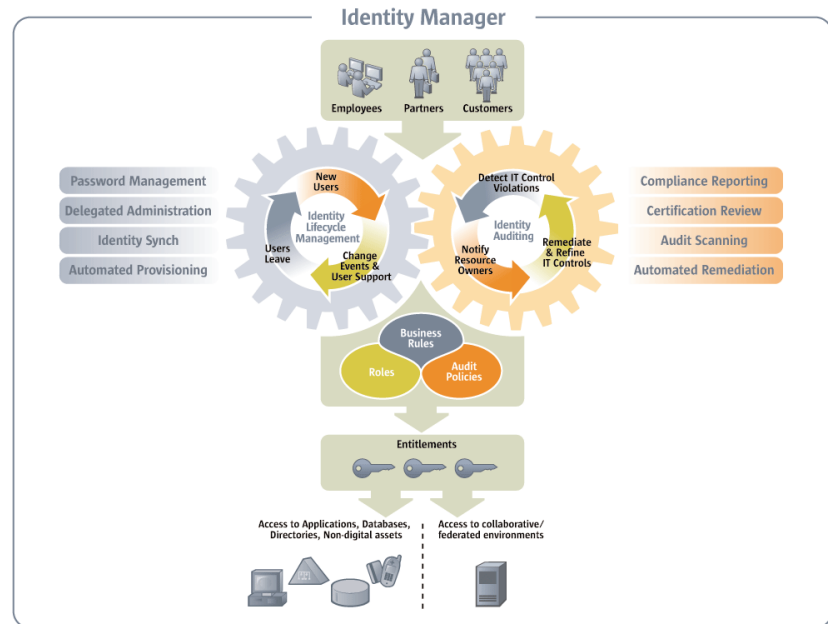
By offering extensive identity auditing capabilities and making identity auditing processes repeatable and sustainable, Identity Manager enables organizations to reduce their cost of compliance through streamlined operations and more efficient use of resources.

Scalable to millions of users, including extranet users

Identity Manager is the first provisioning solution to allow organizations to easily extend identity controls to unlimited extranet environments and to scale accordingly. It meets the toughest scalability requirements, delivering provisioning and auditing to environments with tens of millions of users, performing thousands of new account creations and account updates per minute, and meeting extreme availability requirements (99.9%+) to ensure the highest possible quality of service.

The same non-invasive architecture that speeds deployment across multiple platforms, applications, databases, and directories within an organization extends to quickly deploy the solution to extranet environments as well. This architecture allows data to be managed centrally yet stored locally.

Federated identity administration allows identities to be managed across domains, making it as easy to manage extranet identities as it is to manage internal identities. A key enabler of outsourced application projects, federation allows partnering organizations to trust and share digital identities and attributes of users across domains, vastly simplifying the process of enabling secure interaction among organizations.



Identity Manager brings together complete capabilities for identity lifecycle management and identity auditing to reduce costs and mitigate risks.

Another first from a pioneering leader in identity management solutions

Sun was the first to market with extranet provisioning and identity auditing capabilities — and is now the first to effectively integrate role management into its suite of identity management products. The company has a large installed base including thousands of customers, many in the Fortune 100.

Identity Manager is a key component of Sun's complete identity management portfolio, which also includes products for access management, directory services, role management, and identity federation. Identity Manager has been singled out as a leading provisioning solution in both the Gartner Magic Quadrant and the Forrester Wave.

Identity Manager is also a part of several joint solutions with Sun partners, extending the product's value by integrating it with technology for:

- Business roles management
- ERP compliance
- Enterprise single sign-on
- Converged physical and logical security

Choosing a solution that combines identity management with another key business function enables customers to pursue a comprehensive security and compliance strategy without the cost and effort associated with installing and integrating separate solutions.

Capabilities at a glance — Identity Manager provides all the capabilities to control the cost of managing identities while reducing compliance risk.

Feature	Function	Benefit
Audit Policy Engine	<ul style="list-style-type: none"> Enables IT controls to be translated into digital policies Allows enforcement of controls during both provisioning and periodic auditing 	<ul style="list-style-type: none"> Helps simplify compliance through policy-based integration of identity lifecycle management and identity auditing processes
Policy-Based Provisioning and Workflow	<ul style="list-style-type: none"> Enables complete and automated identity lifecycle management Flags potential violations before committing entitlements to target systems 	<ul style="list-style-type: none"> Prevents compliance violations during identity administration
Identity Audit Scanning	<ul style="list-style-type: none"> Checks for violations in identity data in target applications Automatically detects policy violations 	<ul style="list-style-type: none"> Provides automated, early warning about violations to reduce compliance risk later
Automated Certification Review	<ul style="list-style-type: none"> Provides for scheduled reviews of access privileges and policy violations with delegated managers and compliance owners Automatically initiates remediation processes and documents exceptions 	<ul style="list-style-type: none"> Reduces the cost and effort of compliance by streamlining and automating the ongoing access privilege review process
Compliance Dashboard	<ul style="list-style-type: none"> Displays a summary view of compliance metrics Displays violations, exceptions, and anomalies 	<ul style="list-style-type: none"> Ensures executives have complete and current visibility into security and compliance exposures for timely decision-making
Strong Security Services	<ul style="list-style-type: none"> Enables signing of approvals using digital certificates Detects tampering of audit log records 	<ul style="list-style-type: none"> Eliminates the need to manually write up documented remediations and exceptions approvals for auditors
Compliance Reporting	<ul style="list-style-type: none"> Issues preconfigured reports for common identity audit data Reports on policy violations, remediations, and exceptions Enables custom reports of identity and audit data 	<ul style="list-style-type: none"> Reduces need to gather data manually and accelerates compliance audit process
Extranet and Federated Identity Administration	<ul style="list-style-type: none"> Provides scalable option for secure identity administration and federated provisioning in extranet-facing applications and portals Delivers tested support in 10 million+ user environments 	<ul style="list-style-type: none"> Helps accelerate the introduction of new, revenue-generating applications and services without compromising security or compliance controls
Non-Invasive Architecture	<ul style="list-style-type: none"> Manages data where it natively resides using virtual identities Eliminates need for a centralized repository of all account data Connects to target systems with standard remote protocols 	<ul style="list-style-type: none"> Facilitates rapid deployment by eliminating the technical and political challenges surrounding data ownership and system maintenance
Business Process Editor	<ul style="list-style-type: none"> Provides a powerful NetBeans™ Integrated Development Environment (IDE) Includes comprehensive library of built-in identity business process templates 	<ul style="list-style-type: none"> Reduces time and cost of deployment and maintenance Allows for seamless integration with existing controls and processes
Support for Business Roles	<ul style="list-style-type: none"> Enables import of predefined business roles Enables automated provisioning and auditing at the business role level Integration with Sun Role Manager 	<ul style="list-style-type: none"> Provides additional efficiencies and greater controls over the provisioning and auditing processes
Data Export	<ul style="list-style-type: none"> Offers ability to export Identity Manager data and events to an external data warehouse Makes it possible to query a data warehouse from Identity Manager via SQL 	<ul style="list-style-type: none"> Delivers robust reporting capabilities and entitlements management

Sun™ Identity Manager

Supported Standards

- SPML v2.0 integration interface support

Sun Identity Manager supports out-of-the-box provisioning and auditing to the following resources:

Operating systems

- Solaris™ Operating System
- Red Hat Linux
- HP OpenVMS
- HP-UX
- IBM AIX
- IBM OS/400
- Microsoft Windows
- SuSE Enterprise Linux

Applications

- Oracle E-Business Suite
- PeopleSoft HRMS
- SAP R/3 Enterprise
- SAP Enterprise Portal
- Siebel CRM
- SAP Access Enforcer

Directory servers

- Sun Java System Directory Server
- Lightweight Directory Access Protocol (LDAP) v3
- Microsoft Active Directory
- Microsoft ADAM
- Novell eDirectory
- OpenLDAP

Databases

- IBM DB2 Universal Database for Linux, UNIX®, and Microsoft Windows
- Microsoft SQL Server
- Microsoft Identity Integration Server (MIIS)
- MySQL
- Oracle
- Sybase Adaptive Server

Help Desk

- Remedy Help Desk

Message platforms

- Lotus Notes
- Microsoft Exchange
- Novell GroupWise
- Blackberry RIM Enterprise Server
- Sun Java System Messaging and Calendar Service
- Java Message Service (JMS) Message Queue

Security managers

- CA-ACF2
- CA-Top Secret
- IBM RACF
- RSA SecurID
- ActivIdentity
- Natural
- INISafe Nexess
- Passlogix v-GO

Join Identity Insights

Stay connected to Identity Management news and trends by joining the Sun Identity Insights Program. As a member you will receive an e-newsletter, exclusive invitations to Net talk events, and expert exchanges, plus information on upcoming events and special offers. Join now at sun.com/identityinsights.

Web access control platforms

- Sun Java System Access Manager
- IBM Tivoli Access Manager
- CA eTrust SiteMinder
- RSA ClearTrust

Rapid connectivity for custom applications

- Generic Database Table Wizard
- Generic Database Script Adapter
- Generic UNIX/Linux Script Adapter
- Generic Windows Script Adapter
- Generic Host Access (Mainframe) Script Adapter

Standards

- Service Provisioning Markup Language (SPML)

For more information

To learn more about Sun Identity Manager, please visit sun.com/identity.