

Novell Privileged User Manager

Deliver Superuser Privilege Management for all UNIX/Linux Environments

Many organizations needlessly expose their superuser or root account credentials to users who are required to run commands that need elevated privileges, and passwords are often not changed when administrative staff change jobs—leaving potential back doors into systems and increasing the likelihood of a security breach.

Novell Privileged User Manager helps IT administrators manage identity and access of superuser and root accounts by providing controlled superuser access to administrators, allowing them to perform jobs without needlessly exposing root account credentials. It also provides a centralized activity log across multiple platforms. Privileged user management is a key component of any compliance solution. The introduction of Novell Privileged User Manager enriches the Novell Identity and Access Management and Compliance Management solutions by adding auditing and tracking capabilities for privileged user activity across the organization.

While securely managing UNIX and Linux systems has long been a challenge for administrators, Novell delivers unique technology that simplifies management, tracking and auditing to continuously prove compliance.

Novell Privileged User Manager limits corporate susceptibility to unauthorized transactions and information access by helping organizations rapidly deploy super user management and tracking across all UNIX/Linux environments. The result: organizations can reduce the cost, complexity and risk associated with managing superusers across the enterprise.

Novell Privileged User Manager works by delegating privileged access, which is authorized via a centralized database. The end result is that a user is authorized to run the privileged command and all activity is logged. The centralized database provides for easier administration. Compared to competitive solutions in the marketplace, Novell Privileged User Manager is deployed more quickly, provides faster response time, better logging and auditing and improved administration, leading to a more secure system and a fast return on investment.

A Single Solution Protects all UNIX/Linux Environments

Novell Privileged User Manager integrates seamlessly with all Unix and Linux platforms, allowing you to lock down user privileges and provide centralized logging of activity across your mixed environment. It also supports select Microsoft Windows and XP systems. Supported platforms include:

- AIX 4.2, 4.3.x & 5.x
- HP-UX (PA-RISC) 10.20, 11, 11i v1, v2, v3
- HP-UX (Itanium) 11i v1, v2, v3
- Linux kernel 2.4 — SUSE 9.x, 10, Red Hat 9, Ent Srv v3, v4 & Fedora
- Solaris (Sparc) 2.6, 2.7, 8, 9 & 10
- Solaris (Intel) 8, 9 & 10
- Tru64 4.x & 5.x
- Microsoft Windows 200, 2003 and XP

Rapidly Deploy Super User Management and Tracking

Novell Privileged User Manager provides a UNIX Super User Privilege Management (SUPM) system that minimizes exposure to unauthorized transactions and information access by delegating access to the root account, and providing centralized activity logging across mixed UNIX/Linux environments. This enables administrators to lock down user privileges by easily configuring rules based on the command executed, the user who executed it and the location. The account delegation feature removes the need to grant common access to the root account on any system. The importance of managing the access of privileged users is demonstrated by an increasing number of attacks on important systems, such as the attack at Fannie Mae that was narrowly prevented. According to a report from FBI and PricewaterhouseCoopers, 80 percent of security breaches are accidental, while 20 percent are malicious. Similarly, the average cost of an internal security breach is US\$2.7m compared to US\$50K for an external breach. Additionally, the fact that 70 percent of the breaches are internal makes Novell Privileged User Manager a necessary component to safeguard your enterprise.

Figure 1



[Click image for large view](#)

The Compliance Auditor component of Novell Privileged User Manager provides a comprehensive interface that pulls filtered audit events at hourly, daily, weekly or monthly intervals. This enables auditors to view pre-filtered security transactions, play back recordings of user activity and record notes for compliance purposes. In an era of increasing regulatory compliance, the ability to provide demonstrable audit compliance at any time provides a more secure system and reduces audit risk.

In addition to the Command Controls and Compliance Auditor, several out-of-the-box tools simplify the deployment and administration of user management and tracking. These include:

- An intuitive drag-and-drop visual interface for creating rules, reducing the need for manual scripting.
- Tools for dragging rules into nested hierarchies which, when used in conjunction with scripting, provide granular control for the most demanding environments.
- Unlike other similar systems, all rules and policies are maintained, updated and edited in a central fashion, thus reducing deployment time and the possibility of mistakes.
- An integrated test suite that allows administrators to model and test rule combinations before pushing new rules into a production environment.
- Tools for creating account groups that include user accounts and hosts, simplifying rule creation and maintenance, and reducing administration.

Figure 1



[Click image for large view](#)