

Product Overview



Every IT team needs to use many user IDs and passwords for managing hardware devices, servers and applications. These accounts should be accessible among all members of the IT team. **Privileged accounts allow unlimited access** to programs and data. If they are not properly secured and maintained, they **represent a very high risk** to an organization. Sometimes passwords are left as the default or are assigned well-known values and are generally not properly kept. With hundreds of systems and devices, management of shared accounts can become a real challenge. Routine control, updates, and reporting may require significant efforts and productivity tradeoffs.

Shared Identity Manager (SIM) **maintains and protects privileged shared accounts** of all types, from Active Directory and servers to routers and database systems. The product provides a secure facility for **provisioning, accessing, automatic updating, and de-provisioning of shared administrative accounts**, to enable centralized control and auditing of all shared accounts in your organization.

Product Benefits

- **Protection of Privileged Accounts**

All devices, servers, and workstations have powerful built-in accounts with unlimited rights, such as *enable* on Cisco, *Administrator* on Windows, and *root* on UNIX. Shared Identity Manager (SIM) provides a secure storage for all privileged accounts and their passwords within your organization.

- **Centralized Management**

The product stores all privileged accounts in a central location, enabling designated members of your IT team to access them according to established role-based security policies. SIM provides one unified workflow for creating, accessing, and updating all shared accounts in your organization.

- **Regulatory Compliance**

The product controls and audits the use of privileged shared accounts to enable security and compliance with Sarbanes-Oxley, GLBA, HIPAA, PCI, and others. At every single point, you can determine who knows an account password today and who knew it, for example, a month ago. SIM includes audit reports on operations with shared accounts.

- **Automated Password Management**

SIM automatically updates account passwords according to password expiration policies defined in your organization. It not only changes the account itself, it also updates all affected services and applications that use this account.

- **Enterprise Class Scalability**

SIM can effectively manage tens of thousands of privileged accounts and systems without performance degradation. All automated operations can be scheduled during non-business hours to ensure minimum impact on your production environment.

For more information and pricing, call 888-638-9749, or visit www.netwrix.com

Product Features

- **Account Checkout Concept**

To ensure maximum protection and to prevent the hiding of true user identities, SIM introduces “checkout” the operation, which must be done by every user who wants to gain access to the password. Once the password has been used, the person “checks in” the password, and the system creates a new random password to prevent further use until the next person checks it out again.

- **Automatic Discovery**

The product provides an automatic scanning engine to import your current set of shared accounts into the system during initial setup. Scheduled re-discovery ensures that no shared privileged accounts are used bypassing centralized auditing and control.

- **Shared Account Provisioning**

SIM provides a central facility to create, maintain, and recycle shared accounts according to organization policies. When someone creates a new account for service or application, the system creates it and enforces the appropriate security settings (group membership, permissions, password policies, etc.).

- **Automated Password Resets**

SIM automates routine password maintenance according to effective password policies. The system changes the password and updates all associated services, scheduled tasks, etc. - everything that uses the password being updated - preventing service disruptions, account lockouts, and related issues.

- **Encrypted Information Storage**

All passwords are stored and transmitted in encrypted form to prevent unauthorized disclosure. The product uses AES encryption and SHA-1 algorithm to ensure maximum protection.

- **Web-based Access**

SIM includes one central web-based console for management of all shared accounts. The console has a simple and intuitive user interface and requires minimum learning.

- **Role-based Entitlement Management**

SIM has flexible security rules to define the systems and accounts to which an employee can have access. As soon as a specific person moves to another department or retires, the product makes sure that he or she may no longer access specific accounts and systems.

- **Extensive Auditing**

All operations performed with accounts and systems are logged into the audit database - and optionally, to the event log, - to enable creation of detailed reports and real-time alerting. Audit records track the times, user identities and changes made to shared accounts.

- **Supported Systems**

The product supports major operating systems (Windows, UNIX, mainframes, etc.), databases (Oracle, MS SQL Server, and more), firewalls, routers, and identity frameworks such as Active Directory, NIS, NDS, and more. More systems and types of accounts can be added easily by using flexible plug-in architecture. Contact us to see if your system is supported.

- **Ease of Use**

SIM has a very simple and intuitive user interface, and requires no complex installation and configuration, and works almost completely right out of the box.

Product Licensing

Shared Identity Manager is licensed by the number of managed shared accounts.

Contact Information:	Contact Postal Address:
Phone: 1-888-638-9749 (toll-free)	140 E. Ridgewood Ave.
Phone: 1-201-490-8840 (international)	Suite 415 South Tower
Fax: 201-490-8838	Paramus, NJ 07652
Web: www.netwrix.com	