Securden

Unified PAM

Securely store, protect, and automate the management of all high privileged account passwords. Monitor administrator access to critical IT assets, gain centralized control and complete visibility over privileged access across the enterprise.

Protect Privileged Accounts

Prevent Breaches

Achieve Compliance

Discover and Consolidate Accounts

Discover privileged accounts on Windows, Linux, and Mac systems, devices, databases and applications.

Manage Shared Admin Passwords

Share admin and firecall accounts with complete control and auditing. Link access and actions to individuals.

Protect SSH Keys

Securely store SSH keys, track usage, and associate them with UNIX devices for authentication and remote access.

Windows Accounts Management

Manage Windows domain, service, and local accounts. Manage the dependencies of service accounts.

Manage Application Passwords

Eliminate hard-coded passwords embedded in configuration files, scripts, and code through APIs.

Randomize Passwords Automatically

Automatically randomize passwords of administrative, service, and application accounts periodically.

Secure Remote Access

Launch secure, remote sessions in a single click without copying and pasting the login credentials.

Access without Revealing Passwords

Grant remote access to devices and applications without showing the passwords to users and third-parties.

Privileged Session Recording

Record the entire remote privileged sessions. Playback as videos. Continuously monitor activities.

Active Directory Integration

Integrate with Active Directory for user authentication, onboarding, and automatic offboarding.

Approval Workflows

Enforce password request-release approvals for IT staff. Automate reset after time-limited access.

Audit and Compliance Reporting

Track which individual IT staff has access to which account. Monitor and report privileged access activity.

Technical Specifications

Product Installation	Windows Server 2019 (OR) Windows Server 2008 R2 and later
Deployment Model	On-prem, VMs (or) private cloud (AWS/Azure)
Web-interface	IE, Chrome, Safari, Edge, Firefox
Backend Database	PostgreSQL (bundled) or MS SQL server
Primary Authentication	Active Directory, RADIUS, SAML, Native
MFA	Any TOTP authenticator (Google authenticator or Microsoft authenticator), any RADIUS-based authentication mechanism (RSA SecurID, Digipass, and others), Duo Security, Yubikey, Email to SMS gateway, and OTP through email
Data Encryption	AES-256
Data Transmission	SSL over HTTPS
Privileged Accounts Discovery	Agentless

Remote Connections	Web-based and native client applications RDP, SSH, SQL, and web applications
Session Management	Through the secure remote gateway
Password Resets	Agentless
Platforms Supported for Remote Password Reset	Flavors of servers, databases, network devices, VMs, cloud, and on-prem applications
Integrations	Active Directory, SIEM Solutions, ticketing systems, enterprise single sign-on applications
High Availability	Redundant servers pointing to the same database, MS SQL clusters
Disaster Recovery	Periodic database backup and recovery

Securden | support@securden.com | www.securden.com

Trusted by hundreds of SMBs and Enterprises across the globe

Securden, Inc.
2035 Sunset Lake Road,
Suite B-2, Newark,
Delaware, 19702