



ManageEngine
PAM360



DATASHEET

www.manageengine.com/pam360



Full-stack PAM solution for digital enterprises

About PAM360

PAM360, ManageEngine's enterprise PAM suite, is a complete privileged access security solution that helps IT teams enforce strict governance on access pathways to critical corporate assets. With a holistic approach to privileged access security, PAM360 caters to core PAM requirements and facilitates contextual integration with multiple other IT management tools, resulting in deeper insights, meaningful inferences and quicker remedies. More than 5,000 global organizations and over 1 million administrators trust PAM360 with their PAM needs. To learn more about PAM360 and its enterprise-grade capabilities, please visit <https://mnge.it/pam360>

Key Benefits

- Establish central control and clear ownership of all privileged entities.
- Leverage least privilege access and regulate access provisioning.
- Correlate privileged access data across all segments of your IT network
- Achieve maximum visibility into privileged activities
- Prove compliance with security and regulatory standards
- Bolster business workflows with enterprise-grade features

Powerful 360-degree protection for cyber resiliency in the digital age.

manageengine.com/pam360

PAM360 Offerings

- Privileged account discovery
- Secure remote access provisioning
- Privileged session management
- Secure access to web applications through dedicated gateway server
- Session shadowing and recording
- Self-service privilege elevation
- Application and SSH command control
- Just-in-time privileged access
- Ephemeral access provisioning
- DevSecOps secrets management
- ML & AI based privileged user behavior analytics
- In-depth event and log correlation
- Comprehensive auditing and reporting
- SSL/TLS certificate management
- Contextual integration with ITSM tools and business apps
- Zero trust privilege

**Capability requires licensed subscription of other ManageEngine products. [Learn more.](#)*

Editions, Pricing, and Availability*

Enterprise	\$7,995 annually for 10 administrators, 500 connection users and 25 keys.
MSP Enterprise	\$11,995 annually for 10 administrators, 500 connection users and 25 keys.
30-day free trial	(Fully functional) 5 administrators, 500 connection users and 25 keys.

**Perpetual licensing options available *Price as of August 2026*

Minimum System Requirements

Processor	RAM	Hard Disk
4 Cores or More	16 GB or More	Application: > 4 GB Database: > 10 GB

Operating Systems

Windows	Linux
• Windows Server 2025 • Windows Server 2022 • Windows Server 2019	• Ubuntu 20.04 or above • CentOS Stream 9 or above • Red Hat Linux 9.0 • Red Hat Enterprise Linux 8.x or above • AlmaLinux 9.x and Above Note: PAM360 goes well with any flavor of Linux and also on VMs of the above operating systems.

Databases

- PostgreSQL 15.8, bundled with the product
- MS SQL Server 2019 or above
- Azure MS SQL
- AWS RDS - PgSQL and MSSQL

Browsers

Any HTML-5 powered browser such as Ulaa, Google Chrome, Mozilla Firefox, Microsoft Edge, and Safari.

Note: PAM360 is optimized for 1280 x 800 resolution and above.

Other Specifications

Specifications	Details
Encryption Algorithms	• AES-256
Virtualization Platforms	• Hyper V • VMware ESXi • Microsoft Azure VM • AWS - Amazon EC2 VM
Session Protocols	• RDP • SSH • VNC • SQL • HTTPS
Privileged Account Discovery	• Windows • Linux • Network devices • VMware

Specifications	Details
	• AWS devices
Ssl Vulnerability Detection	• Certificate revocation • status - CRL, OCS • Heartbleed • POODLE • Weak cipher suites
Ssh, Ssl/tls Versions	• SSH-2 • SSL 3.0 • TLS 1.0 • TLS 1.1 • TLS 1.2
Languages	• English, French, German, Japanese, Polish, Simplified Chinese, Spanish, Traditional Chinese, Turkish, Dutch • Italian • Russian
API Support	• REST • SSH CLI • SDK • OpenAPI
Browser Extensions	• Chrome • Firefox • Microsoft Edge
Disaster Recovery	• Application scaling • Multiple application server instances • SQL server failover cluster

Specifications	Details	
	• Read-only server with PostgreSQL Database • Secondary server model with read-only continuity	
SSL / TLS Certificate Discovery	• Webserver certificates • AD user certificates • Certificates hosted in AWS—ACM and IAM • Certificates issued by local CA • Certificates in Microsoft Certificate Store • Load balancer certificates • SMTP server certificates • Self-signed certificates	
Certificate Private Key Specifications	Algorithm	RSA, DSA, EC
	• Hash functions • Key size (in bits) • Keystore type	• SHA256, SHA384, SHA512 • 4096, 2048, 1024 • KS, PKC512, PEM
Mobile Applications	• Android • iOS	

Platforms Supported For Remote Password Reset

Operating Systems	Cisco Devices	Database Servers
- Windows (local, domain, and service accounts) - Linux - Mac - Solaris - HP Unix - IBM AIX - HP-UX - Junos OS	- Cisco Integrated Management Controller - Cisco Catalyst - Cisco SG300 - Cisco UCS - Cisco Wireless LAN Controller - Cisco IOS - Cisco PIX - Cisco CatOS	- MS SQL - MySQL - Sybase ASE - Oracle DB server - PostgreSQL - Azure MS SQL

Network Devices		
- ASA Firewall - Audiocode - Brocade - Brocade VDX - Brocade SAN Switch - Checkpoint Firewall - Citrix Netscaler SDX - Citrix Netscaler VPX - Extreme Networks - F5 - Fujitsu Switch - Gigamon - H3C	- HMC - HP iLO - HP Onboard Administrator - HP Printer - HP ProCurve - HP Virtual Connect - Huawei - Juniper - Juniper Netscreen - ScreenOS - Magento - MikroTik	- NetApp 7-Mode - NetApp cDOT - Opengear - Orange Firewall - Palo Alto Networks - pfSense - Routerboard - Ruijie Networks - SonicWall - TP-Link - VMware vCenter

Cloud Services	Others
• AWS IAM • Google Apps • Microsoft Azure • Rackspace • Salesforce • WebLogic	• LDAP Server • VMware ESXi • IBM AS/400 • Oracle XSCF • Oracle ALOM • Oracle ILOM • Aruba ATP • Avaya-GW • FortiManager-FortiAnalyzer • Nortel

Remote password reset for custom resource types:

For resources that do not belong to the above resource types, PAM360 facilitates remote password reset via custom plugins that can be developed through any language code or script like Java, C, Rust, PowerShell, Bash, etc. These plugins can be run from PAM360's interface to carry out password resets. You can also formulate a set of SSH commands to reset the password of any SSH-based resource when executed from the PAM360 interface.

Combining different IT security modules into a single console

To further fortify their PAM plan, enterprises can incorporate crucial features of various other ManageEngine IT security solutions into a PAM360 instance through contextual integrations. However, this capability currently requires users to have individual licenses for the corresponding point solutions.

Key offerings through integrations with other ManageEngine solutions:

- Privileged user behavior analytics (ManageEngine Analytics Plus)
- Privileged access control workflows (ManageEngine ServiceDesk Plus)
- Just-in-time privilege elevation capabilities (ManageEngine ADManager Plus)
- Endpoint log correlation for privileged session audits (ManageEngine EventLog Analyzer)
- ML-based user and entity behavior analytics (ManageEngine Log360 UEBA)
- Self-service password management and single sign-on capabilities (ManageEngine ADSelfService Plus)

Click [here](#) to learn more about the integrations.

Other Integrations

User Authentication	Single Sign-On	Two-Factor Authentication
• AD • Entra ID • LDAP • RADIUS • Smart Card	• Entra AD • Microsoft ADFS • Okta • Any SAML-based authenticators	• RSA SecurID • Okta Verify • RADIUS-based authenticators • Duo MFA • YubiKey • Google Authenticator • Microsoft Authenticator • Zoho OneAuth Authenticator • Oracle Mobile Authenticator

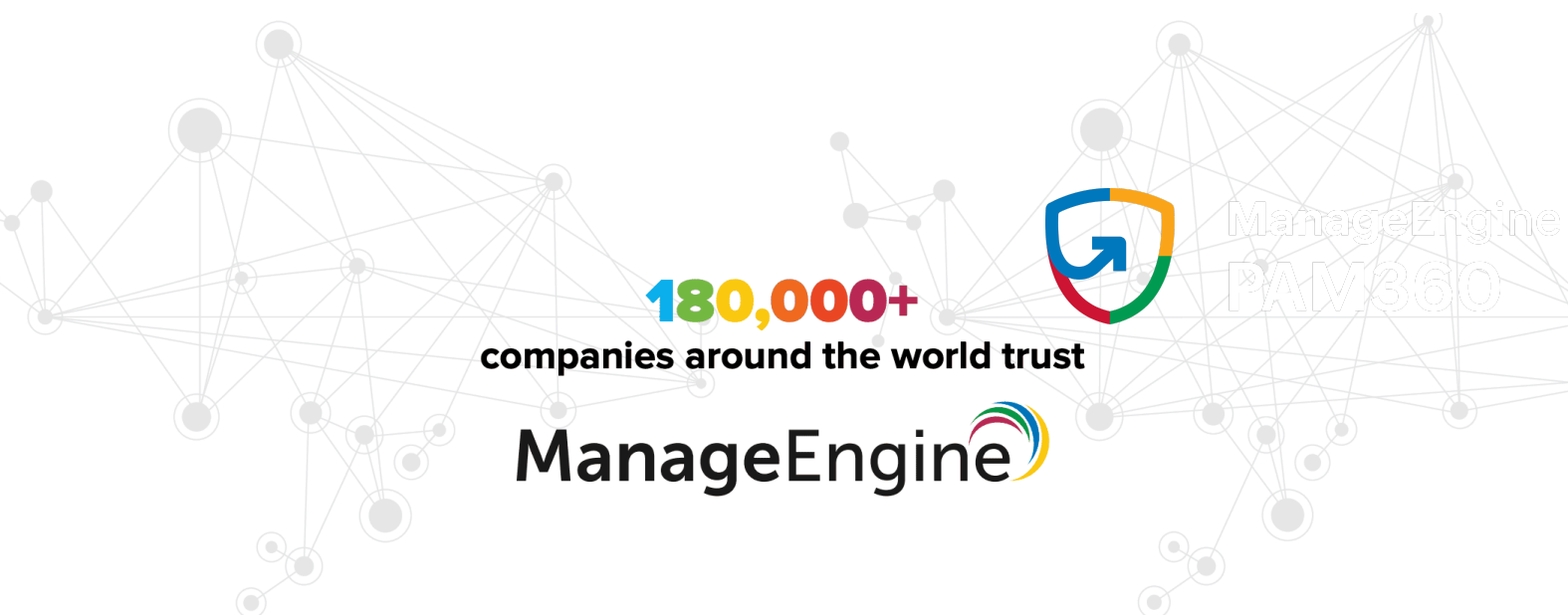
SIEM	ITSM	Certificate Authorities
• Log360 • Splunk • ArcSight • EventLog Analyzer • Sumo Logic • Microsoft Sentinel • Any RFC 3164-compliant tool	• ServiceDesk Plus On-Demand • ServiceDesk Plus MSP • ServiceDesk Plus • ServiceNow • JIRA Service Desk • BMC Helix Remedyforce	• Let's Encrypt • Microsoft CA • GoDaddy • Sectigo • Symantec • Thawte • GeoTrust • RapidSSL • DigiCert • GlobalSign SSL
CI/CD Platforms	Container Platforms	RPA Tools
• Jenkins • Ansible • Chef • Puppet	• Kubernetes	• Automation Anywhere • Cortex XSOAR
Cloud Storage	Vulnerability Scanners	HSM
• Dropbox • Amazon S3 • Box	• InsightVM	• Entrust nShield HSM • SafeNet Luna PCIe HSM • Trident HSM

About ManageEngine

ManageEngine is the enterprise IT management division of Zoho Corporation. Established and emerging enterprises — including 9 of every 10 Fortune 100 organizations — rely on our real-time IT management tools to ensure optimal performance of their IT infrastructure, including networks, servers, applications, desktops and more. We have offices worldwide, including the United States, the Netherlands, India, Singapore, Japan, China, and Australia as well as a network of 200+ global partners to help organizations tightly align their businesses and IT.

For more information, please visit www.manageengine.com; follow the company blog at blogs.manageengine.com and on LinkedIn at www.linkedin.com/company/manageengine, Facebook at www.facebook.com/ManageEngine and Twitter [@ManageEngine](https://twitter.com/ManageEngine).

manageengine.com/pam360



Technical support

Telephone: +1 408 454 4014

Email: pam360-support@manageengine.com



ManageEngine
PAM360