ManageEngine

PAM360

DATASHEET

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
- DevSecOps secrets management
- ML- &AI- based privileged user behaviour 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

Minimum system requirements

Processor	RAM	Hard disk
Dual core or above	8 GB or above	Application: > 200 MB Database: > 10 GB

Operating systems

Windows

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Linux

- Ubuntu 9.x or above
- CentOS 4.4 or above
- Red Hat Linux 9.0
- Red Hat Enterprise Linux 7.x
- Red Hat Enterprise Linux 6.x
- Red Hat Enterprise Linux 5.x
- Normally works well with any flavour of Linux.

Databases

- PostgreSQL 10.18, bundled with the product
- MS SQL Server 2012 or above
- Azure MS SQL
- AWS RDS - PgSQL and MSSQL

Browsers

Any HTML-5 powered browser such as Google Chrome, Mozilla Firefox, Microsoft Edge, Safari, and Internet Explorer 10 or above.

Other Specifications

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

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

Browser Extensions

- Chrome
- Firefox
- Microsoft Edge

Encryption algorithms

- AES-256

Disaster recovery

- High availability with live secondary setup
- Application scaling
- Multiple application server instances
- SQL server failover cluster
- Read-only server with PostgreSQL Database

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 specs

Algorithm	RSA, DSA, EC
Hash functions	SHA256, SHA384, SHA512
Key size (in bits)	4096, 2048, 1024
Keystore type	KS, PKC512, PEM

Mobile applications

- iOS
- Android

Platforms supported for remote password reset

Operating systems

- Windows (local, domain, and service accounts)
- Linux
- Mac
- Solaris
- HP Unix
- IBM AIX
- HP-UX
- Junos OS

Cisco devices

- Cisco Integrated Management Controller
- Cisco Catalyst
- Cisco SG300
- Cisco UCS
- Cisco Wireless LAN Controller
- Cisco IOS
- Cisco PIX
- Cisco CatOS

Database servers

- MS SQL
- MySQL
- Sybase ASE
- Oracle DB server
- PostgreSQL
- Azure MS SQL

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

Cloud services	Others
• AWS IAM	• LDAP Server
• Google Apps	• VMware ESXi
• Microsoft Azure	• IBM AS/40 0
• Rackspace	• Oracle XSCF
• Salesforce	• Oracle ALOM
• WebLogic	• 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 • Azure AD • LDAP • RADIUS • Smart Card	• Azure AD • Microsoft ADFS • Okta • Any SAML-based authenticators	• Azure MFA • RSA SecurID • Google Authenticator • Microsoft Authenticator • Okta Verify • RADIUS-based authenticators • Duo Security • YubiKey • Zoho OneAuth Authenticator • Oracle Mobile Authenticator • Any TOTP-based authenticators

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 Remedy-force	• 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

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.

manageengine.com/pam360

180,000+
companies around the world trust

ManageEngine

Technical support

Telephone: +1 408 454 4014
Email: pam360-support@manageengine.com

ManageEngine
PAM360