ManageEngine

PAM360

DATASHEET

A complete privileged access security solution for enterprises

About PAM360

PAM360 is a web-based privileged access management **(PAM)** solution that defends enterprises against privilege misuse by regulating access to sensitive company information. Through powerful privileged access governance, smoother workflow automation, advanced analytics, and contextual integrations with various IT services, PAM360 enables enterprises to bring different avenues of their IT management system together, facilitating meaningful inferences and quicker remedies.

Key benefits

- Strict access governance
- Central control
- Regulatory compliance
- Smart workflow automation
- Greater visibility
- Online reputation management
- In-depth event correlation

PAM360 offerings


Privileged account management


SSH key management


SSL / TLS certificate management


DevOps and cloud security


Just-in-time privilege elevation*


Secure remote access provisioning


Privileged session monitoring


User behavior analytics*


Context-aware event log correlation*


Comprehensive auditing and reporting

*Capability requires licensed subscription of other ManageEngine products. Learn more.

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

manageengine.com/pam360

ManageEngine
PAM360
DATASHEET

Minimum system requirements

Processor	RAM	Hard disk
Dual core or above	4 GB or above	Application: > 200 MB Database: > 10 GB

Operating systems

Windows

- Windows Server 2019
- Windows Server 2016
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows 8
- Windows 10

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 flavor of Linux

Databases

- Azure MS SQL
- PostgreSQL 9.5.21
- MS SQL Server 2008 or above (SQL server should be installed in Windows 2008 Server or above)

Browsers

Any HTML-5 powered browser such as Google Chrome, Mozilla Firefox, 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
- VNC
- SSH
- SQL

Privileged account discovery

- Windows
- Linux
- Network devices
- VMware

SSL Vulnerability Detection

- Certificate revocation status—CRL, OCSP
- 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

API Support

- REST
- XML-RPC
- SSH CLI

Browser Extensions

- Chrome
- Firefox
- Internet Explorer
- Microsoft Edge

Encryption algorithms

- AES-256
- SafeNet Luna PCIe HSM
- FIPS 140-2 validated cryptography

Disaster recovery

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

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	JKS, PKCS12, PEM

Mobile applications

- iOS
- Android
- Windows

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
- Audiocode
- Brocade
- Brocade VDX
- Brocade SAN Switch
- Checkpoint Firewall
- Citrix Netscaler SDX
- Citrix Netscaler VPX
- Extreme Networks
- F5
- Fortinet
- Fortigate Firewall
- FortiMail
- 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

- AWS IAM
- Google Apps
- Microsoft Azure
- Rackspace
- Salesforce
- WebLogic

Others

- LDAP Server
- VMware ESXi
- IBM AS/40 0
- Oracle XSCF
- Oracle ALOM
- Oracle ILOM
- Aruba ATP
- Avaya-GW
- FortiManager-FortiAnalyzer
- Nortel

Remote password reset for custom resource types: For resources that don't 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 auditing for service requests (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	• PhoneFactor • RSA SecurID • Google Authenticator • Microsoft Authenticator • Okta Verify • RADIUS-based authenticators • Duo Security • YubiKey • Any TOTP-based authenticators

SIEM	ITSM	Certificate Authorities
• Log360 • Splunk • ArcSight • EventLog Analyzer • Sumo Logic • Any RFC 3164-compliant tool	• ServiceDesk Plus On-Demand • ServiceDesk Plus MSP • ServiceDesk Plus • ServiceNow • JIRA Service Desk	• Let's Encrypt • Microsoft CA • GoDaddy • Sectigo • Symantec • Thawte • GeoTrust • RapidSSL • DigiCert • GlobalSign SSL

CI/CD Platforms	Cloud Storage	Vulnerability Scanners	RPA Tools
• Jenkins • Ansible • Chef • Puppet	• Dropbox • Amazon S3 • Box	• InsightVM	• Automation Anywhere

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