ManageEngine
PAM360

Security specifications document

www.manageengine.com/pam360

Introduction

ManageEngine crafts IT management solutions to help tens of millions of IT admins across the globe proactively address their IT challenges. Our customers turn to us to improve their security posture, and we give the highest priority to keeping our customer data secure and private, which is reflected in our products, internal culture, and processes. This document explores our security processes at the organizational and product levels. Click here to view our detailed security policy.

Skip to product security >>

Organization security

We have an information security management system in place which takes into account our security objectives as well as the risks and mitigations concerning all the interested parties. We employ strict policies and procedures encompassing the security, availability, processing, integrity, and confidentiality of customer data.

- ## Employee background checks

  Each employee undergoes a process of background verification. We hire reputed external agencies to perform this check on our behalf. We do this to verify their criminal records, previous employment records, if any, and educational background. Until this check is performed, the employee is not assigned tasks that may pose risks to users.

- ## Security awareness

  Each employee, when inducted, signs a confidentiality agreement and acceptable use policy, after which they undergo training in information security, privacy, and compliance. Furthermore, we evaluate their understanding through tests and quizzes to determine which topics they need further training in. We provide training on specific aspects of security that they may require based on their roles. We educate our employees continually on information security, privacy, and compliance in our internal community, where our employees check in regularly, to keep them updated regarding the security practices of the organization. We also host internal events to raise awareness and drive innovation in security and privacy.

- ## Dedicated security and privacy teams

We have dedicated security and privacy teams that implement and manage our security and privacy programs. They regulate and maintain defense systems, develop review processes for security, and constantly monitor our networks to detect suspicious activity. They provide domain-specific consulting services and guidance to our engineering teams.

- ## Internal audit and compliance

We have a dedicated compliance team to review procedures and policies in ManageEngine to align them with standards, and to determine what controls, processes, and systems are needed to meet the standards. This team also does periodic internal audits and facilitates independent audits and assessments by third parties. For more details, check out our compliance portfolio.

- ## Endpoint security

All workstations issued to ManageEngine employees run up-to-date OS versions and are configured with antivirus software. They are configured such that they comply with our standards for security, which require all workstations to be properly configured, patched, and be tracked and monitored by ManageEngine’s endpoint management solutions. These workstations are secure by default as they are configured to encrypt data at rest, have strong passwords, and get locked when they are idle. Mobile devices used for business purposes are enrolled in the mobile device management system to ensure they meet our security standards.

Strict adherence to security hygiene

Our security, network operations centre, and privacy teams are dedicated to developing and implementing a rigorous security framework, which includes periodic employee education and training, building and maintaining our defence systems, streamlining security review processes across internal teams and departments, and constantly monitoring our corporate networks to detect and mitigate suspicious activities.

Incident response and management process

At ManageEngine, we have a dedicated incident management team to monitor, track, and respond to incidents in real time. Our team aims to detect and respond to incidents with appropriate corrective measures whenever applicable.

In the event of an incident, we provide our customers with an extensive report, which answers the what, who, how, and when of the security incident accompanied by essential information surrounding our response process. Furthermore, we provide details on the measures we will implement to prevent the recurrence of the incident.

To report any security and privacy incidents, you can write to us at incidents@zohocorp.com, and we will address them immediately.

Breach notification

As a data controller, we will notify all concerned data protection bodies of a data breach within 72 hours of it coming to our notice, as required by the General Data Protection Regulation (GDPR). We also duly notify our customers as and when required, depending on specific requirements. As a data processor, we will notify the concerned data controllers of the incidents as soon as possible. For incidents about a specific user or organization, we will notify the concerned party through their business email. As for general incidents, we will notify our users through emails, blogs, forums, and social media informing them of the incident and, if required, the next course of remedial action.

Vulnerability management: Security fixes, builds, and patching processes

To ensure tight security, the ManageEngine Security Response Center (MESRC) uses a combination of in-house and third-party tools to identify security vulnerabilities or bugs (listed in CVE or reported on social media) across our products, corporate networks, endpoints, databases, and other assets. Identified and reported vulnerabilities that require timely remediation are logged and prioritized according to their severity. Furthermore, we run extensive risk assessments and vulnerability proofing tests, and mitigate all the vulnerable systems by providing appropriate fixes and patch builds in our security releases. More info.

Responsible disclosure

We practice proactive and collaborative IT security

Aside from reinforcing our security routine, we appreciate our customers, partners, and security enthusiasts bringing their security concerns to us, which helps us stay on top of security threats. We constantly work with industry specialists and researchers to keep ourselves abreast with recent security developments, leveraging this collective expertise to build foolproof IT security products.

Our vulnerability reporting program, Bug Bounty, is committed to working with the security community to identify, verify, and implement appropriate controls and patches to reported vulnerabilities. If you have discovered a potential security issue with our line of products, please report it to https://bugbounty.zoho.com/, or write to us directly at security@zohocorp.com.

Once a vulnerability is reported, the MESRC, along with product experts, investigates the validity, risks, and severity associated with the reported vulnerabilities and implements remediation to our users in the form of bug fixes, upgrade packs, and security patches.

ManageEngine PAM360: Overview

ManageEngine PAM360 is a unified enterprise privileged access management solution that provides tight access control options to privileged users to manage and secure administrative access to corporate assets and sensitive corporate identities. Therefore, we've designed PAM360 to offer maximum security, including during application installation, user authentication, data transmission, storage, and regular use.

Secure by design

Our software development life cycle model mandates our PAM360 engineering team to strictly adhere to our secure coding standards, which includes the following security assessment framework and steps to identify and circumvent any potential security flaws:

Software development lifecycle

Security framework

Analysis and design	Development	QA/release
Gather and analyze the requirements to identify any security flaws and loopholes. Prepare a vulnerability assessment plan to address security concerns posed by users and security analysts in the previous releases/versions. Develop a product or feature prototype including the changes, and subject them to the change management authority for approval.	Continuous unit testing of newly developed features and modules to ensure they are aligned with user requirements and core business logic. Subject third-party code dependencies and libraries to vulnerability tests before use to ensure they are secure.	Perform integration, automation, and penetration tests to ensure that the new features or modules are secure from potential vulnerabilities/flaws. Continuous smoke testing to ensure that the core functionality of the product remains intact without opening new security loopholes. Generate security assessment reports to identify further areas of improvement. Run continuous vulnerability scans post release for timely identification and patching of vulnerabilities.

- Our repository and build infrastructure are secured with SSH and HTTPS protocols and are placed in a secure segmented network with stricter authentication and access controls.

- Our security and code frameworks are Open Worldwide Application Security Project (OWASP) compliant and implemented at the application layer.

- Every update and new feature in PAM360 is subject to internal change management policies and regular vulnerability assessments, and changes are implemented into production only if approved by the concerned change and security management authorities.

- All code changes, third-party dependencies, release bundles, and upgrade packs are subject to multiple levels of internal security review, automation and penetration testing efforts, and vulnerability scans to ensure they are well secured from logical bugs and security issues.

- The binaries are signed with a code-signing certificate, and the private key is securely stored in the segmented network with limited access.

- Every update and new feature in PAM360 is subject to and governed by an internal change management policy, which authorizes the requested change before implementing it into production.

- The PAM360 engineering team works closely with internal security teams to obtain their feedback and identify areas of improvement in terms of strengthening our security posture.

Besides the aforementioned security measures, we continuously strive to make the application more secure. The following section provides comprehensive details about the security specifications of ManageEngine Password Manger Pro.

PAM360: Security specifications

PAM360 protects data at various levels and is classified into the following categories:

Security specifications	
1. Vaulting and encryption mechanism	• AES-256 encryption • Dual encryption—first at the application and then at the database level • Encryption key and encrypted data cannot reside together • SafeNet Luna PCIe HSM, Entrust nShield HSM • Custom cryptography • Multi-tenant architecture (MSP edition)
2. Identification and authentication	**Application-level authentication** • Integration with identity stores like Microsoft AD, Azure AD, any LDAP-compliant directory service, and RADIUS • Local authentication mechanism using the SHA2 (SHA512) algorithm • Enforced password resets for local authentication • Smart card authentication • SAML 2.0 single sign-on **Two-factor authentication** • RSA SecurID • One-time unique password sent by email • Google Authenticator • Microsoft Authenticator • Okta Verify • Duo Security • YubiKey

	• Oracle Mobile Authenticator • Any RADIUS-compliant TFA solution • Zoho OneAuth Authentication • Any TOTP TFA authenticator
3. Data security and integrity	**Data transmission** • EEncrypted and over HTTPS • SSL mode for client connections **Remote password resets** • Automatic, scheduled remote password reset for over 70 resource types • Remote password reset using agents • Windows service account password reset • Windows scheduled tasks password reset • IIS AppPool account reset • Password reset listener • Password reset plugins for custom resource types • Password resets through SSH command sets • PAM360 one-way agents for network segments not directly reachable **Data storage and management** • Dual AES-256 encryption • SSH key management • SSL/TLS certificate management **Application-to-application password management** • HTTPS connections for inter-app communications • Verification through SSL certificate • Request source validation

	• Unique Auth Token validation **DevSecOps credential security** • Password management for CI/CD platforms: Jenkins, Ansible, Chef, and Puppet • Container platform: Kubernetes • RPA tools: Automation Anywhere, Cortex XSOAR **Web GUI input validation** • Protection against SQL injections, cross-site scripting, buffer overflow, and other attacks • OWASP-compliant input validation process **IP restrictions** • Allow or block IP address or IP range for web UI access • Allow or block mobile app and browser extension usage per user
4. Access control measures	**Data access control** • Granular access control mechanism • Request-release workflow for password access • Ticketing system integration **Just-in-time privilege elevation** • Local group elevation • AD domain group elevation **Self-service privilege elevation** • Application allow-listing and control • SSH command allow-listing and control

	Policy-based access control • Dynamic trust scores for users and resources • Application control and command filtering
5. Secure remote access	**One-click remote connections** • Windows Remote Desktop Protocol (RDP), SSH, SQL, and VNC sessions from any HTML5-compatible browser • No need for additional plug-in or agent software • Remote connections are tunnelled through the PAM360 server • Users don't need passwords (stored in their browsers) to launch remote sessions with target machines • No direct connectivity between user device and remote host • Secure file transfer to target machines • Landing server or jump server configuration to access data centers, servers, and other critical resources • Native thick client support for Windows devices **Automatic connection to websites and applications** • **Browser extensions:** Firefox, Edge, and Chrome • Content security policy (CSP) best practices • Prevention of inline JavaScript execution • AJAX requests
6. Privileged session management	• Privileged session recording and playback • Session shadowing and termination • Secure access to web applications through a dedicated HTTPS gateway server

7. Audit, accountability control, and real-time alerts	**Detection capabilities and non-repudiation measures** • Real-time alerts for password, user, and access events • In-depth audit trails • SIEM support • SNMP traps and syslog messages
8. Comprehensive reports	• Out-of-the-box compliance reports for ISO27001, HIPAA, PCI, NERC-CIP, and the GDPR • Password usage, expiry, out of sync and policy violation reports • User and access reports • Custom and query reports
9. Availability mechanisms	**High availability** • Redundant PAM360 server and database instances • Direct TCP connection with latency for database replication • Application scaling option to have distributed instances deployed in multiple sites or networks • Cluster support and application scaling using MSSQL • Read-only server with PostgreSQL database • Application scaling using PostgreSQL Cluster **Offline access** • Export passwords as an encrypted HTML file • Additional passphrase for AES-256 encryption • Export passwords to mobile devices through Box, DropBox, and AWS S3

	Mobile access • Native apps for iOS and Android • Passphrase as encryption key • Offline access • Audit trails for data sync to mobile device **Secure cloud storage** • Cloud storage provisions to enable anytime, anywhere, secure access to passwords • Auto-synchronization of the encrypted password file (in HTML format) with authorized users' mobile devices via Dropbox, Amazon S3, and Box accounts
10. Disaster recovery	**Provision for backup** • Live and periodic database backup • Encrypted storage of backup files **Emergency access** • Super administrator accounts for fire-call or break-glass purposes • Option to prevent the creation of more than one super admin account • Read-only server with PostgreSQL database

Security features

1. Vaulting and encryption mechanism: Secure by design

1.1 Installation of master key

- PAM360 uses AES-256 encryption (the strongest known encryption that the US government has approved). The key used for encryption is auto-generated and is unique for every installation. This serves as the first-level encryption key.

- The first-level encryption key is not allowed to be kept with the PAM360 installation. This is done to ensure that the encryption key and the encrypted data, in both live and backed-up databases, do not reside together.

- The recommended setup is to store the key in a physically separate server or device and ensure that it is available to the server during application start-up. Subsequently, the key is held only in the server memory and never written anywhere.

- PAM360 also supports periodic rotation of the encryption key, where a new key is generated and applied to the existing data and then the old key is discarded. More info

1.2 Database key

- The PAM360 database is secured through a separate key, which is auto-generated and unique for every installation.

- The key for the database can be stored securely within PAM360.

- PAM360 also allows users to store the database key in any secured location, leaving the key accessible to only the server.

- The relational database management system (RDBMS) is always configured to accept only secure connections (forces SSL mode for client connections) and clients can connect only from the same local host. In cases where the web server and the RDBMS have to reside in separate servers, the configuration enforces connections only from configured IP addresses.

1.3 SafeNet Luna PCIe HSM

- PAM360 also provides support for SafeNet Luna PCIe HSM to give administrators the option to enable hardware data encryption.

- SafeNet HSM handles all the encryption and decryption methods, and stores the encrypted key and data directly in its hardware module, which is fitted to a computer or a network server.

1.4 Custom cryptography

- Apart from the default cryptography technique, PAM360 provides the option to use custom cryptography, i.e., customizable encryption and decryption methods, which allows admins to implement their own key and encryption logic.

1.5 Multi-tenant architecture (MSP Edition)

- PAM360 offers an MSP edition for secure data segmentation between departments, or in the case of MSP customers, between their customers. The segmentation is implemented at the level of database rows in the RDBMS.

- Each department or customer that requires data segmentation is provided a value range for the unique identity for each row. All database operations performed for that department or customer are automatically restricted to that value range. For more details, click here.

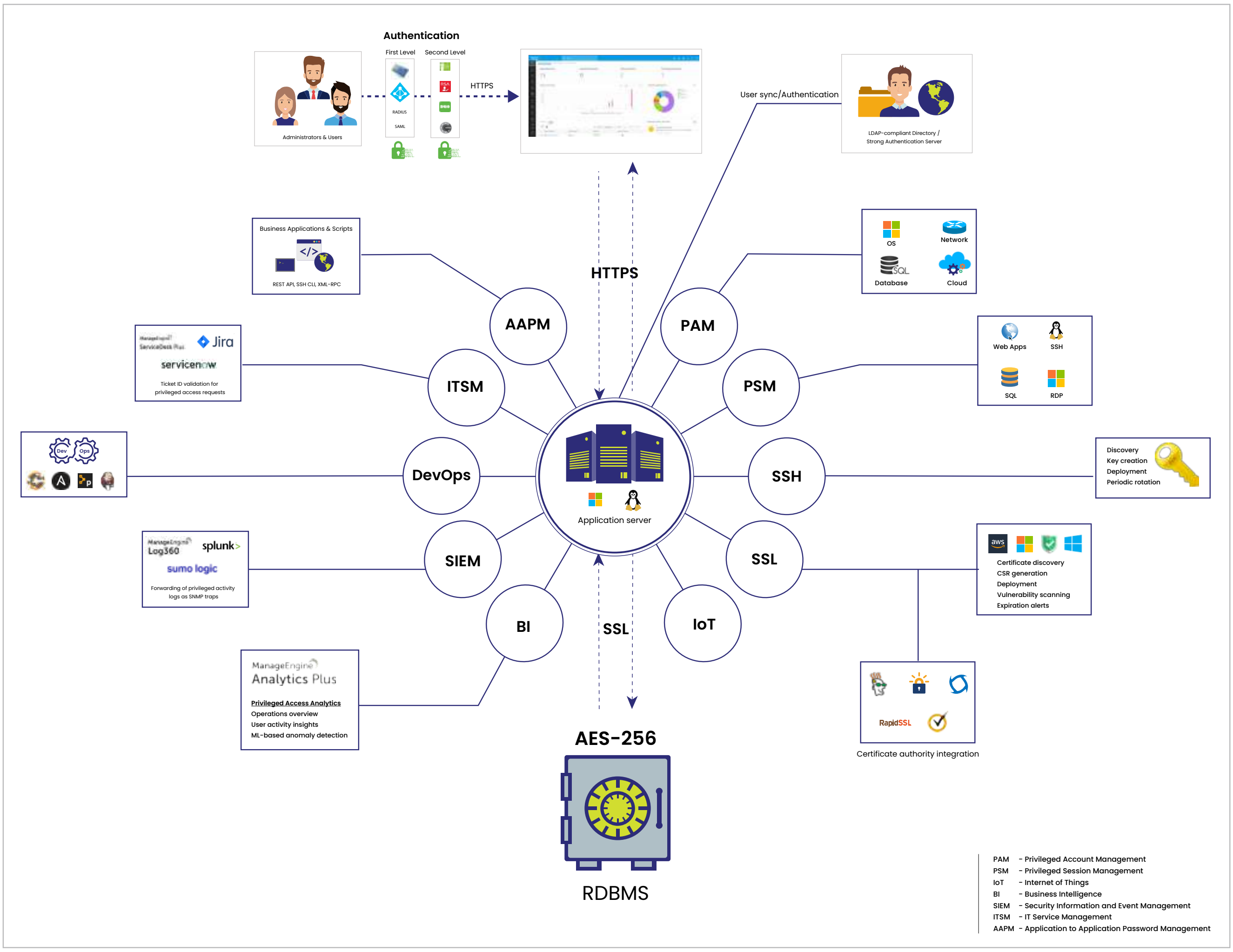

Authentication
First Level
Second Level
RADIUS
SAML
RSA
HTTPS
Administrators & Users
User sync/Authentication
LDAP-compliant Directory / Strong Authentication Server
Business Applications & Scripts
REST API, SSH CLI, XML-RPC
ManageEngine ServiceDesk Plus
Jira
servicenow
Ticket ID validation for privileged access requests
Dev
Ops
ManageEngine Log360
splunk>
sumo logic
Forwarding of privileged activity logs as SNMP traps
ManageEngine Analytics Plus
Privileged Access Analytics
Operations overview
User activity insights
ML-based anomaly detection
HTTPS
AAPM
ITSM
DevOps
SIEM
BI
PAM
PSM
SSH
SSL
IoT
Application server
SSL
AES-256
RDBMS
OS
Network
Database
Cloud
SQL
Web Apps
SSH
SQL
RDP
Discovery
Key creation
Deployment
Periodic rotation
aws
Certificate discovery
CSR generation
Deployment
Vulnerability scanning
Expiration alerts
RapidSSL
Certificate authority integration
PAM - Privileged Account Management
PSM - Privileged Session Management
IoT - Internet of Things
BI - Business Intelligence
SIEM - Security Information and Event Management
ITSM - IT Service Management
AAPM - Application to Application Password Management

Fig 1. Product architecture

2. Identification and authentication

2.1. Strong application-level authentication: Various options

PPAM360 provides four options for uniquely identifying the users who will be accessing the application. All the options are complemented by various two-factor authentication provisions, which provide an extra layer of security.

- **Integration with identity stores: PAM360** readily integrates with external identity stores like Microsoft AD, any LDAP-compliant directory service (Novell eDirectory and Oracle OID), and RADIUS. Users can be imported from identity stores and the respective authentication mechanism can be leveraged. Users will be uniquely identified through their respective accounts in the identity store. More info.

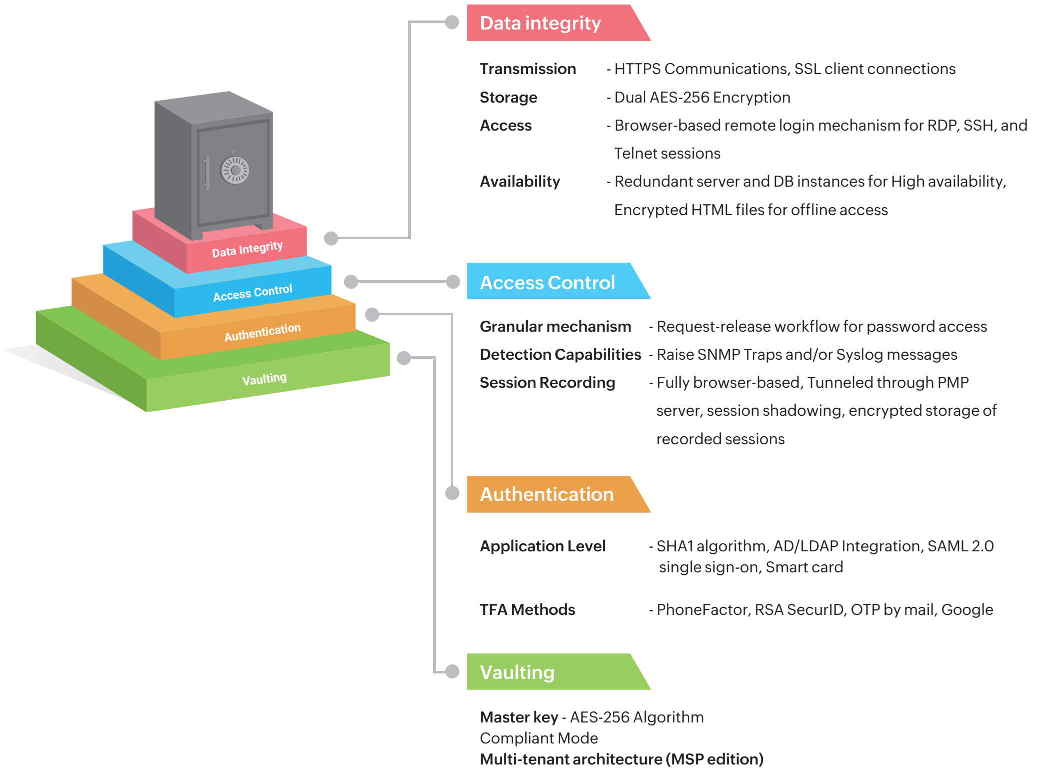
- **Unique accounts and strong local authentication:** PAM360 comes with a local authentication mechanism in which unique accounts are created for users. Users will be able to access the application with their credentials. PAM360 employs the SHA2 algorithm to generate passwords, which ensures that each login password is unique and irreversibly secured.

- **Common access card:** PAM360 supports smart card authentication. The user must possess the smart card and know the personal identification number (PIN) as well. For more details, click here.

- **Enforced password resets for local authentication:** As a security precaution, PAM360 requires the user to reset the local authentication password as a mandatory first step in the following scenarios:
  - User logs in for the first time using the default password
  - When the login password is the same as the username
  - When the user forgets the password and receives a new system-generated password by email

- In all these scenarios, the user will be allowed to proceed only after resetting the password.

- **SAML compliant service:** PAM360 offers support for SAML 2.0, which facilitates integration with federated identity management solutions for single sign-on. PAM360 acts as the service provider (SP) and it integrates with the identity provider (IdP) by using SAML 2.0. The integration basically involves supplying details about the SP to the IdP and vice versa. After you integrate PAM360 with an IdP, the logged-in users can log on from the respective identity provider's GUI without providing the credentials again. For more details, click here.



Data integrity

Transmission - HTTPS Communications, SSL client connections

Storage - Dual AES-256 Encryption

Access - Browser-based remote login mechanism for RDP, SSH, and Telnet sessions

Availability - Redundant server and DB instances for High availability, Encrypted HTML files for offline access

Access Control

Granular mechanism - Request-release workflow for password access

Detection Capabilities - Raise SNMP Traps and/or Syslog messages

Session Recording - Fully browser-based, Tunneled through PMP server, session shadowing, encrypted storage of recorded sessions

Authentication

Application Level - SHA1 algorithm, AD/LDAP Integration, SAML 2.0 single sign-on, Smart card

TFA Methods - PhoneFactor, RSA SecurID, OTP by mail, Google

Vaulting

Master key - AES-256 Algorithm
Compliant Mode
Multi-tenant architecture (MSP edition)

2.2. Assurance mechanism: Two-factor authentication (2FA)

To introduce an additional level of security, PAM360 provides two-factor authentication. Users will be required to authenticate through two successive stages to access the web interface. The second level of authentication can be done using one of the following:

- **RSA SecurID:** Integrate RSA SecurID with PAM360 to generate a one-time validation token that changes every 60 seconds.

- **Unique password through email:** Authenticate by emailing users unique passwords. The passwords validate the user for one login session and then expire.

- **Google Authenticator:** Time-based numeric tokens can be received by installing the Google Authenticator app on your smart phone or tablet.

- **RADIUS Authenticator:** Leverage the authentication mechanisms of any RADIUS-compliant system, like Vasco Digipass, Passley, etc., to create one-time passwords.

- **Microsoft Authenticator:** Provide the six-digit token on the Microsoft Authenticator app.

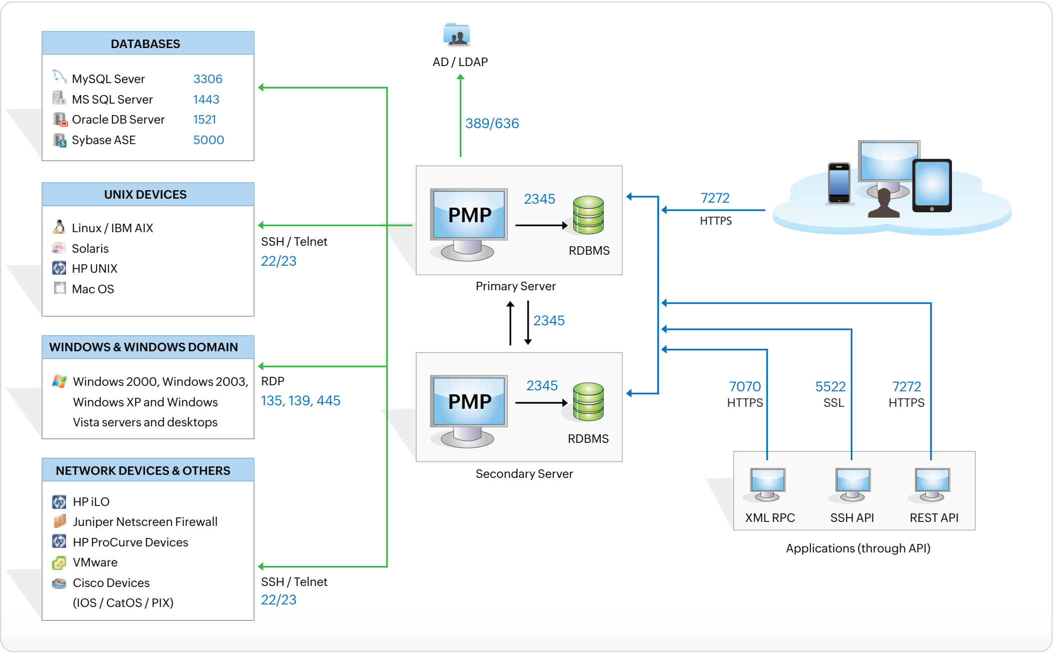
- **Okta Verify:** Use the six-digit token on the Okta Verify app.
- **Duo Security:** Leverage Duo security authentication.
- **YubiKey:** Generate one-time passwords with YubiKey.
- **Oracle Mobile Authenticator:** Use the six-digit token generated by Oracle Authenticator.
- **Zoho OneAuth:** Generate a six-digit number using Zoho OneAuth.
- Apart from these, PAM360 supports any TOTP-based authenticator.

For more details, click here.

3. Data security and integrity

3.1 Data transmission

- All data transmission between the PAM360 user interface and the server are encrypted and take place through HTTPS.



*RDBMS - PostgreSQL bundled. Option to use MySQL or MS SQL Server.

← - Inbound ← - outbound

Fig 3. Data flow diagram

- All data transmission between the PAM360 server and database occurs over SSL.

- For remote password reset actions, there is an option to transmit user passwords using SSH.

- **Communication between PAM360 and agents**: PAM360 allows agents to be deployed that can connect to the server. The communication is always one way—that is, the agent always initiates this connection. Therefore, only the server needs to be available for the agents, eliminating the need to punch firewall holes or create VPN paths for the server to reach all agents. The agent periodically pings the server through HTTPS to check whether any operation (password reset or verifying password) is pending for execution. The agent will then carry out the tasks and, after completing them, will notify the server with the results. More info.

- Communication between the primary and secondary servers is encrypted over HTTPS.

3.2 Remote password resets

- **Automatic, scheduled remote password reset:** PAM360 supports agentless remote password reset for over 70 resource types out of the box, the details of which can be found here.

- **Remote password reset using agents:** PAM360 agent automatically resets the password of remote resources that are not connected to the PAM360 server. Once the agent is deployed in the target machines, it will communicate with the application and carry out the password changes.

- **Windows service account password reset:** PAM360 identifies the services associated with a particular domain account. While resetting the password of a domain account managed in PAM360, it will find the services using that particular domain account as a service account and automatically reset its password.

- **IIS AppPool account reset:** While resetting domain account passwords, PAM360 will identify the IIS AppPools associated with that particular domain account and will automatically update their passwords.

- **Password reset listener:** The password reset listener is typically a PowerShell or Bash or Shell script, or any executable that can be invoked whenever the password of an account is being changed or reset in the PAM360 repository. The listener can be invoked even for local password changes and for resources for which remote password reset is not supported out of the box.

- **Password reset plugins for custom resource types:** The password reset plug-in allows admins to add their own implementation class and enforce automatic password resets for resources that are not supported by PAM360 out of the box, such as legacy resource types, in-house applications, and more. The plug-ins can also be designed to impose access controls for legacy accounts and enable automatic reset of passwords instantly upon use. This way, the passwords of these accounts will serve as one-time passwords that are reset after every use via the associated plug-in.

- **Password reset through SSH command sets:** For custom SSH-based resources, PAM360 allows admins to directly add the password reset SSH commands used in the resources to the PAM360 web interface, without the need for a CLI terminal. PAM360 offers a default set of basic commands along with an option to add custom commands, arrange them in the order of execution, and combine them into a new command set.

3.3 Data storage and management

- PAM360 is designed as a web application with a web server for business logic and an RDBMS for data storage.

- Upon applying appropriate initialization vectors and other standard good practices around encryption, the first-level encryption key with the AES-256 algorithm is generated in the web server.

- The encrypted data is pushed to the RDBMS for storage by using SQL queries. Next, PAM360 encrypts the data with built-in AES functions of the RDBMS for dual layers of encryption.

- Legacy SSH, Telnet, and SQL sessions are recorded in readable plaintext format, and the recording files are encrypted before storage. As for RDP, SSH, and VNC, the sessions are recorded in video format, and can be played only through a proprietary player.

- PAM360 also securely stores and manages SSH keys, SSL/TLS certificates, files, documents, images, and other digital identities.

3.4 Application-to-application password management

- In the case of application-to-application passwords, PAM360 exposes a web API, and the applications connect and interact through HTTPS. The application's identity is verified by forcing it to issue a valid SSL certificate, matching the details that have already been recorded in PAM360 about the application. More info.

3.5 DevSecOps credential security

- Password management for CI/CD and container platforms: PAM360 helps eliminate embedded credentials in the DevOps pipeline by providing integration capabilities with container platforms (Kubernetes); RPA tools like Automation Anywhere and Cortex XSOAR; and various CI/CD tools, like Jenkins, Ansible, Chef, and Puppet. The integration ensures that the required credentials are retrieved securely from PAM360's vault every time a task is executed, instead of being stored in plaintext within the script files.

3.6 Web GUI input validation

- PAM360 thoroughly validates all inputs in the GUI. Use of special characters and HTML code is filtered, and the application is guarded against common attacks like SQL injections, cross-site scripting, buffer overflows, and other attacks.

3.7 IP restrictions

- PAM360 allows administrators to limit inbound connections to the PAM360 server by enforcing IP-based restrictions to minimize unwanted traffic. It provides an added layer of security by letting the administrator choose exactly which systems should be allowed to or blocked from accessing and sending requests to the PAM360 server.

4. Access control measures

4.1 Data access control

- All data access in PAM360 is subjected to the granular access control mechanism. Password ownership and sharing practices are well defined, and users get access only to authorized passwords.

- For highly sensitive assets, an extra layer of security could be enforced by forcing the authorized users to go through a request-release mechanism. Whenever the password of a sensitive IT resource needs to be accessed, a request must be made, which goes to the administrator (persons who are designated to authorize access) for approval and is released for a limited time period. More info.

- All access to passwords (who accessed what password and when) and all operations performed by users on any resource are captured in audit trails, ensuring accountability for all users and actions.

- In addition, as part of policy enforcement, organizations can automatically randomize the passwords of sensitive IT resources periodically. PAM360 assigns strong, unique passwords to assets. It also analyzes the passwords of systems for required complexity and reports violations. These provisions help prevent unauthorized access to passwords, which prevents unauthorized access to systems and applications. More info.

- The Zero Trust approach in PAM360 is a micro-segment behavioral analysis of users and resources based on the predefined parameters for the trust score calculation. PAM360 offers access privileges to users by verifying their activities and state with the score-based access policy method instead of trusting them instinctively.

- **Ticketing system integration:** PAM360 also integrates with a wide range of ticketing systems to automatically validate service requests related to privileged access. The integration ensures that only users with a valid ticket ID can access the authorized privileged passwords. This integration also extends to the PAM360 workflow, which helps in granting approvals to password access requests upon automatic validation of corresponding service requests in the ticketing system.

5. Secure remote access

5.1 One-click remote connections

- **PAM360** allows users to launch highly secure, reliable, and completely emulated Windows RDP, SSH, SQL, and VNC sessions from any HTML5-compatible browser without the need for additional plug-ins or agent software.

- Remote connections to endpoints are tunnelled through the PAM360 server, requiring no direct connectivity between the user device and remote host.

- In addition to superior reliability, tunnelled connectivity provides extreme security, as passwords needed to establish remote sessions do not need to be available on the user's browser. More info.

- PAM360 lets users securely transfer files to target machines during remote sessions. For Windows, the files can be transferred to and from the target machine during an RDP session facilitated by RDP. For SSH sessions in Linux systems, file transfers are one-way, i.e., to the target machine only, using the Secure Copy Protocol.

5.2 Automatic connection to websites and applications with web browser extensions

- PAM360 provides browser extensions for Firefox, Edge, and Chrome. The extensions have been designed to ensure the highest level of data security and privacy.

- CSP best practices are enforced to combat content injection attacks effectively.

- Input validation and output encoding is done for all user inputs to prevent XSS attacks.

- The highest level of security has been ensured in all stages of data retrieval and transit, including when:

  i. Validating passphrases

  ii. Retrieving encrypted data from the server

  iii. Holding passwords and other sensitive data as JavaScript variables (which cannot be accessed by any external application or other extensions)

  iv. Storing other data in the background as local records

  v. Passing credentials to websites

  vi.The user logs out or remains idle for a specified time, after which local data gets completely erased.

6. Privileged session management

- All actions performed by users during a privileged session are video recorded and stored securely for future forensic analysis. More info.

- In addition to session recording, PAM360 allows administrators to monitor privileged sessions in real time through session shadowing. If any suspicious activity is found, the administrator can terminate the session immediately.

- PAM360 Remote Connect is an independent desktop client for Windows, designed to launch direct remote connections via passwordless login to Windows and SSH-based target resources without needing to install multiple remote clients or a web browser.

7. Audit, accountability control, and real-time alerts

7.1 Detection capabilities

- PAM360 provides real-time alerts and notifications on various password events, including access, modification, deletion, changes in share permissions, and other specific events. More info.

- The audit module, which records every user and system action, also lets administrators configure what events need to be sent to security information and event management (SIEM) systems. The event alerts can either be sent as standard syslog messages or SNMP traps. More info.

7.2 Non-repudiation measures

- Every action and scheduled task executed by users in the user interface is audited.

- The audit information, which contains details such as who did what operation, when, and from where, is stored in the same database. The audit logs are tamper-proof, ensuring non-repudiation.

- The RDBMS is always configured to accept only secure connections (forces SSL mode for client connections), and clients can connect only from the same local host. In cases where the web server and the RDBMS have to reside in separate servers, the configuration allows connections only from specific IP addresses.

8. Comprehensive reports

Information on all password and privileged access activities in your enterprise is presented in the form of comprehensive reports in PAM360. The status and summaries of the different activities such as password inventory, policy compliance, password expiration, user activity, and more are provided in the form of tables and graphs, which help IT administrators make well-informed decisions on password management.

- **Out-of-the-box compliance reports:** PAM360 makes it easy to meet security audits and compliance requirements stated in various regulations with the help of compliance reports on PCI DSS, ISO/IEC 27001, NERC-CIP, and the GDPR.

- **Canned reports:** PAM360 provides a range of canned reports on all password and user activities, various password and security policies, certificates, and SSH keys.

- **Custom reports:** PAM360 provides the option to create customized reports out of canned and audit reports by specifying certain criteria. Custom reports are designed to bring out specific information from the PAM360 database as per custom needs.

- **Query reports:** Admins can also create query reports to retrieve specific data from the PAM360 database by either writing their own SQL query or customizing an SQL query from the existing reports. PAM360 allows SQL statements to query the database directly, fetch information from provided tables, and format the data into a report.

For more information on reports, click here.

9. Availability mechanisms

9.1 High availability

- PAM360 provides high availability to ensure uninterrupted access to passwords, which is made possible through redundant server and database instances.

- One instance will be the primary instance to which all users stay connected, while the other will be a secondary or standby instance. Administrators and users can connect to the primary or secondary instance to access the GUI console through a desktop browser, smart phone, or tablet.

- The primary and secondary servers can be installed geographically apart, even across continents, as long as they have a direct TCP connection with latency good enough for database replication.

- The server can manage endpoints to which it has direct TCP connections. For managed systems that are in a DMZ or in network segments not directly reachable for the server, agents can be installed that can reach the server over standard HTTPS.

- At any point in time, data in both the primary and secondary instances will be in sync. Data replication happens through a secure, encrypted channel. More info.

- For continuous and uninterrupted workflow with a day-to-day growing user base, increased API workloads, user traffic, etc., an additional scalability function in PAM360 allows users to use their external PostgreSQL cluster as the backend database.

9.2 Offline access

- PAM360 facilitates secure export of passwords for offline access in the form of an encrypted HTML file and even synchronizes the file to the user's mobile device.

- Before export, the user is asked for a passphrase to secure the data with AES-256 encryption. The offline copy can be accessed only by providing the passphrase. Moreover, this passphrase is not stored anywhere in the server.

- Whenever the user makes an offline copy of the resources or passwords shared with them, the activity gets recorded in the audit trail.

- In addition, PAM360 allows auto-synchronization of the encrypted HTML file to users' mobile devices through integration with cloud storage services, like Dropbox, Box, and Amazon S3 services.

9.3 Mobile access

- PAM360 provides native apps for iOS, Android, and BlackBerry platforms. The mobile apps enable enterprise IT admins and users to securely retrieve passwords while on the go, without compromising on data security. The mobile app is as secure as the desktop installation and uses the same AES-256 encryption. All communication between PAM360 and the mobile app is secured by the HTTPS protocol over SSL.

- The apps are guarded by an additional passphrase entered by the user, which is used as the encryption key. So, even if the mobile device is stolen, passwords cannot be deciphered in plaintext.

- If two-factor authentication is configured for a user, they must adhere to it while using the mobile app too.

- The apps do not let users stay logged in, requiring them to authenticate every time they access the app.

- Whenever an offline copy of data is made on the web server, the native app syncs the file to the user's device and this activity is recorded in the audit trail. After the HTML file is deleted by the user, it is also erased from the user's device as part of the synchronization.

9.4 Secure cloud storage

- Apart from the option to export passwords to a spreadsheet in plaintext or an encrypted HTML file, PAM360 provides cloud storage provisions to enable anytime, anywhere access to passwords in a secure way. This can be done by enabling auto-synchronization of the encrypted HTML file to the authorized users' mobile devices via Dropbox, Amazon S3, and Box accounts.

10. Disaster recovery

10.1 Provision for backup

- PAM360 offers provisions for both live backup of the database and periodic backup through scheduled tasks.

- All sensitive data in the backup file is stored in the encrypted form in a ZIP file under the <PAM360_Home/backUp> directory or under the destination directory configured by the admin.

- The backup copy will not have the encryption master key because PAM360 does not allow both the encryption key and the encrypted data in both live and backed-up databases to reside together. Unless one presents the encryption key, sensitive data cannot be deciphered from the backup copy.

- While a database backup operation is in progress, no configuration change can be performed in PAM360. More info

10.2 System failure and recovery

- In the event of a disaster or data loss, users can quickly make a fresh install of the same version of PAM360 and restore the backed-up data to the database.

- Disaster recovery for PAM360 with MS SQL Server as the back-end database can be performed only with the master key initially used for encryption upon installation. More info.

10.3 Emergency access

- For break-glass purposes, one or a few administrators can be designated as super administrators who will have unconditional access to all information in the system, including all passwords added to the system by other administrators.

- Administrators cannot designate themselves as super administrators. This has to be approved and carried out by one or more other administrators.

- When the system has one or more super administrators configured, all the administrators will be notified about it.

- After an admin becomes a super admin, they can log on to PAM360 and enable the option to prevent the creation of additional super admin accounts.

- In case of a primary server failure, any read-only server can be configured as the primary server. The read-only server acts like a mirror server and synchronizes all the actions carried out by the primary server.

Operational security

Customer data security

The customer data resides only in their environment, as the product is an on-premises solution.

Note: If any customer requires help in resolving any issue, we may require the customer's logs. The customer uploads the logs through a secure portal owned by us, and the logs are stored in a centralized server that can be accessed only by authorized personnel. The logs will be deleted automatically after five days from the time of upload.

Logging and monitoring

The product logs certain data for debugging and to prevent any misuse.The log files generated by Password Manager Pro are stored in customer machines. A maximum of 30 log files can be stored with the size capped to 10MB for each file. Once this limit is reached, the log files are rolled over; the older files are removed from user machines.

Data access and masking logs are written and maintained in the customer machine. We do not have access to the log files unless the user shares it to avail support services. In this case, only the support staff and development team, limited by their roles, have access to the log files. After the issue is identified, the log files are deleted.

Vulnerability and patch management

We have a dedicated vulnerability management process that actively scans for security threats or vulnerabilities using a combination of certified third-party scanning tools and in-house tools. Subsequently, automated and manual testing is performed. Furthermore, the security team actively reviews inbound security reports and monitors public mailing lists, blog posts, and wikis to identify security incidents that might affect the company. Once we identify a vulnerability that requires remediation, it is logged, prioritized according to severity, and is assigned an owner. We further identify the associated risks and mitigate them by either patching the vulnerable systems or applying relevant controls. After assessing the severity of the vulnerability based on the impact analysis, we commit to resolve the issue within our defined SLA. Depending upon the severity, we send security advisories to all our customers describing the vulnerability, the patch, and the steps to be taken by the customer.

Business continuity

We have backup power, temperature control systems, and fire-suppression and fire-protection systems to ensure business continuity. Dedicated business continuity plans are present for major operations such as infrastructure management and technical support. We have a well-planned business continuity and disaster recovery plan in place to assist us in the event of extended service outages, thereby affecting the services provided to the customers by factors beyond our control, e.g., natural calamities, man-made disasters, etc., to resume endpoint management operations to the maximum possible extent within a minimal time frame. The plan encompasses all our internal operations to ensure continued services for our customers. We have three recovery teams, the emergency management team), the disaster recovery team, and the IT technical services team, in place for better coordination and support among various teams.

11. Build and patching process

- The PAM360 team works closely with the MESRC to run mandatory vulnerability scans and penetration tests before every major release to ensure that the latest builds are completely foolproof. In addition, the team also runs continuous vulnerability assessments on these builds to ensure that they are free from any new vulnerabilities.

- Users are notified immediately to upgrade to the latest version as and when there is a new security patch or update.

- In the event of a security concern or escalation, users are requested to submit a detailed report on the vulnerability or security bug. Meanwhile, the product team evaluates the validity and risks associated with the bug and prioritizes the release based on the severity.

- Hotfix builds are released within 24 to 72 hours of an issue being reported, depending on the severity of the issue, and the team will approve the builds for release only after they have been tested for further vulnerabilities or bugs.

www.manageengine.com/pam360

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.manageengine.com/pam360

ManageEngine
PAM360