

ManageEngine PAM360 DATASHEET

Solución PAM de pila
completa para
empresas digitales

Acerca de PAM360

PAM360, la suite PAM empresarial de ManageEngine, es una completa solución de seguridad de acceso privilegiado que ayuda a los equipos de TI a aplicar una estricta gobernanza sobre las vías de acceso a los activos corporativos críticos. Con un enfoque integral de la seguridad de los accesos privilegiados, PAM360 satisface los requisitos básicos de PAM y facilita la integración contextual con otras múltiples herramientas de gestión de TI, lo que da lugar a una información más profunda, inferencias significativas y soluciones más rápidas. Más de 5.000 organizaciones globales y más de 1 millón de administradores confían sus necesidades de PAM a PAM360. Para obtener más información sobre PAM360 y sus funciones de nivel empresarial, visite <https://mnge.it/9K8>

Principales ventajas

- Establezca un control central y una propiedad clara de todas las entidades privilegiadas
- Aproveche el acceso de mínimo privilegio y regule el aprovisionamiento de acceso
- Correlacione los datos de acceso privilegiado en todos los segmentos de su red de TI
- Consiga la máxima visibilidad de las actividades privilegiadas
- Demuestre el cumplimiento de los estándares reglamentarios y de seguridad
- Refuerce los flujos de trabajo empresariales con funciones de nivel empresarial

**Potente protección de 360 grados para la
ciberresiliencia en la era digital.**

**[manageengine.com/latam/privileged-access-
management/](https://manageengine.com/latam/privileged-access-management/)**

Ofertas de PAM360

- Descubrimiento de cuentas privilegiadas
-

- Aprovisionamiento de acceso remoto seguro
-

- Gestión de sesiones privilegiadas
-

- Acceso seguro a las aplicaciones web a través de un servidor del gateway dedicado
-

- Seguimiento y grabación de sesiones
-

- Elevación de privilegios por autoservicio
-

- Aplicación y control de comandos SSH
-

- Acceso privilegiado justo a tiempo

- Gestión de secretos de DevSecOps
-

- Análisis del comportamiento de usuarios privilegiados basado en IA y ML
-

- Correlación exhaustiva de eventos y logs
-

- Auditoría e informes exhaustivos
-

- Gestión de certificados SSL/TLS
-

- Integración contextual con herramientas ITSM y aplicaciones empresariales
-

- Privilegio de confianza cero
-

*La función requiere la suscripción con licencia de otros productos ManageEngine. [Más información.](#)

Versiones, precios y disponibilidad*

Enterprise	10 administradores, 500 usuarios de conexión y 25 claves.
MSP Enterprise	10 administradores, 500 usuarios de conexión y 25 claves.
Prueba gratuita de 30 días	(Totalmente funcional) 5 administradores, 500 usuarios de conexión y 25 claves.

* Opciones de licencia perpetua disponibles

Requisitos mínimos del sistema

Procesador	RAM	Disco duro
Doble núcleo o superior	8 GB o superior	Aplicación: > 200 MB Base de datos: > 10 GB

Sistemas operativos

Windows	Linux
• Windows Server 2022 • Windows Server 2019 • Windows Server 2016	• Ubuntu 9.x o versiones posteriores • CentOS 4.4 o versiones posteriores • Red Hat Linux 9.0 • Red Hat Enterprise Linux 7.x • Red Hat Enterprise Linux 6.x • Red Hat Enterprise Linux 5.x • Normalmente funciona bien con cualquier variante de Linux.

Bases de datos

- PostgreSQL 10.18, incluido con el producto
- MS SQL Server 2012 o versiones posteriores
- Azure MS SQL
- AWS RDS - PostgreSQL and MSSQL

Navegadores

Cualquier navegador con HTML-5 como Google Chrome, Mozilla Firefox, Microsoft Edge, Safari e Internet Explorer 10 o versiones posteriores.

Otras especificaciones

Plataformas de virtualización

- Hyper V
- VMware ESXi
- Microsoft Azure VM
- AWS - Amazon EC2 VM

Protocolos de sesión

- RDP
- SSH
- VNC
- SQL
- HTTPS

Descubrimiento de cuentas privilegiadas

- Windows
- Linux
- Dispositivos de red
- VMware

Detección de vulnerabilidades SSL

- Estado de revocación de certificados - CRL, OCS
- Heartbleed
- POODLE
- Suites de cifrado débiles (Weak cipher suites)

Versiones SSH, SSL/TLS

- SSH-2
- SSL 3.0
- TLS 1.0
- TLS 1.1
- TLS 1.2

Idiomas

- Inglés
- Francés
- Alemán
- Japonés
- Polaco
- Chino simplificado
- Español
- Chino tradicional
- Turco
- Holandés
- Italiano
- Ruso

Compatibilidad API

- REST
- SSH CLI

Extensiones para navegadores

- Chrome
- Firefox
- Microsoft Edge

Algoritmos de cifrado

- AES-256

Recuperación en caso de desastres

- Alta disponibilidad con configuración secundaria en tiempo real
- Escalamiento de aplicaciones
- Múltiples instancias del servidor de aplicaciones
- Failover cluster del SQL server
- Servidor de solo lectura con base de datos PostgreSQL

SSL / TLS certificate discovery

- Certificados de servidor web
- Certificados de usuario AD
- Certificados alojados en AWS-ACM e IAM
- Certificados emitidos por CA local
- Certificados en Microsoft Certificate Store
- Certificados del balanceador de carga
- Certificados del servidor SMTP
- Certificados autofirmados

Especificaciones de la clave privada del certificado

Algoritmo	RSA, DSA, EC
Funciones hash	SHA256, SHA384, SHA512
Tamaño de la clave (en bits)	4096, 2048, 1024
Tipo de almacén de claves	KS, PKCS12, PEM

Aplicaciones móviles

- iOS
- Android

Plataformas compatibles para el restablecimiento remoto de la contraseña

Sistemas operativos

- Windows (cuentas locales, de dominio y de servicio)
- Linux
- Mac
- Solaris
- HP Unix
- IBM AIX
- HP-UX
- Junos OS

Dispositivos Cisco

- Cisco Integrated Management Controller (Controlador de gestión integrado Cisco)
- Cisco Catalyst
- Cisco SG300
- Cisco UCS
- Cisco Wireless LAN Controller (Controlador LAN inalámbrico Cisco)
- Cisco IOS
- Cisco PIX
- Cisco CatOS

Servidores de bases de datos

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

Dispositivos de red

- | | | |
|------------------------|------------------------------|----------------------|
| • ASA Firewall | • Fujitsu Switch | • MikroTik |
| • Audiocode | • Gigamon | • NetApp 7-Mode |
| • Brocade | • H3C | • NetApp cDOT |
| • Brocade VDX | • HMC | • Opendear |
| • 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 | |

Servicios en la nube

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

Otros

- LDAP Server
- VMware ESXi
- IBM AS/400
- Oracle XSCF
- Oracle ALOM
- Oracle ILOM
- Aruba ATP
- Avaya-GW
- FortiManager-FortiAnalyzer
- Nortel

Restablecimiento remoto de la contraseña para tipos de recursos personalizados:

remoto de contraseñas a través de plugins personalizados que pueden desarrollarse mediante cualquier lenguaje de código o script como Java, C, Rust, PowerShell, Bash, etc. Estos plugins pueden ejecutarse desde la interfaz de PAM360 para llevar a cabo el restablecimiento de contraseñas. También puede formular un conjunto de comandos SSH para restablecer la contraseña de cualquier recurso basado en SSH cuando se ejecuta desde la interfaz PAM360.

Combinación de diferentes módulos de seguridad de TI en una única consola

Para reforzar aún más su plan PAM, las empresas pueden incorporar funciones cruciales de varias otras soluciones de seguridad de TI de ManageEngine en una instancia de PAM360 a través de integraciones contextuales. Sin embargo, esta función requiere actualmente que los usuarios dispongan de licencias individuales para las soluciones puntuales correspondientes.

Ofertas clave a través de integraciones con otras soluciones de ManageEngine:

- Análisis del comportamiento de usuarios privilegiados (ManageEngine Analytics Plus)
- Flujos de trabajo de control de acceso privilegiado (ManageEngine ServiceDesk Plus)
- Funciones de elevación de privilegios justo a tiempo (ManageEngine ADManager Plus)
- Correlación de logs de endpoints para auditorías de sesiones privilegiadas (ManageEngine EventLog Analyzer)
- Análisis del comportamiento de usuarios y entidades basado en ML (ManageEngine Log360 UEBA)
- Gestión de contraseñas de autoservicio y funciones de inicio de sesión único (ManageEngine ADSelfService Plus)

Haga clic [aquí](#) para obtener más información sobre las integraciones.

Otras integraciones

Autenticación de usuarios • AD • Azure AD • LDAP • RADIUS • Smart Card	Inicio de sesión único • Azure AD • Microsoft ADFS • Okta • Cualquier autenticador basado en SAML	Autenticación de dos factores • Azure MFA • RSA SecurID • Google Authenticator • Microsoft Authenticator • Okta Verify • Autenticadores basados en RADIUS • Duo Security • YubiKey • Zoho OneAuth Authenticator • Oracle Mobile Authenticator • Cualquier autenticador basado en TOTP
SIEM • Log360 • Splunk • ArcSight • EventLog Analyzer • Sumo Logic • Microsoft Sentinel • Cualquier herramienta compatible con RFC 3164	ITSM • ServiceDesk Plus On-Demand • ServiceDesk Plus MSP • ServiceDesk Plus • ServiceNow • JIRA Service Desk • BMC Helix Remedy-force	Autoridades de certificación • Let's Encrypt • Microsoft CA • GoDaddy • Sectigo • Symantec • Thawte • GeoTrust • RapidSSL • DigiCert • GlobalSign SSL
Plataformas de CI/CD • Jenkins • Ansible • Chef • Puppet	Plataformas de contenedores • Kubernetes	Herramientas RPA • Automation Anywhere • Cortex XSOAR

Almacenamiento en la nube

- Dropbox
- Amazon S3
- Box

Analizadores de vulnerabilidades

- InsightVM

HSM

- Entrust nShield HSM
- SafeNet Luna PCIe HSM

Acerca de ManageEngine

ManageEngine es la división de gestión de TI empresarial de [Zoho Corporation](https://www.zoho.com). Las empresas establecidas y emergentes, incluidas 9 de cada 10 organizaciones de la lista Fortune 100, confían en nuestras [herramientas de gestión de TI en tiempo real](#) para garantizar el rendimiento óptimo de su infraestructura de TI, incluidas las redes, los servidores, las aplicaciones, los desktops y mucho más. Tenemos oficinas en todo el mundo, incluidos Estados Unidos, Países Bajos, India, Singapur, Japón, China y Australia, así como una red de más de 200 socios globales para ayudar a las organizaciones a alinear estrechamente sus negocios y TI.

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

manageengine.com/latam/pam360

Más de **180,000+**
empresas de todo el mundo confían en

ManageEngine

Asistencia técnica

Teléfono: +1 408 454 4014

Correo electrónico: pam360-support@manageengine.com

ManageEngine
PAM360