ManageEngine
Password Manager Pro

La solución completa de gestión de cuentas privilegiadas

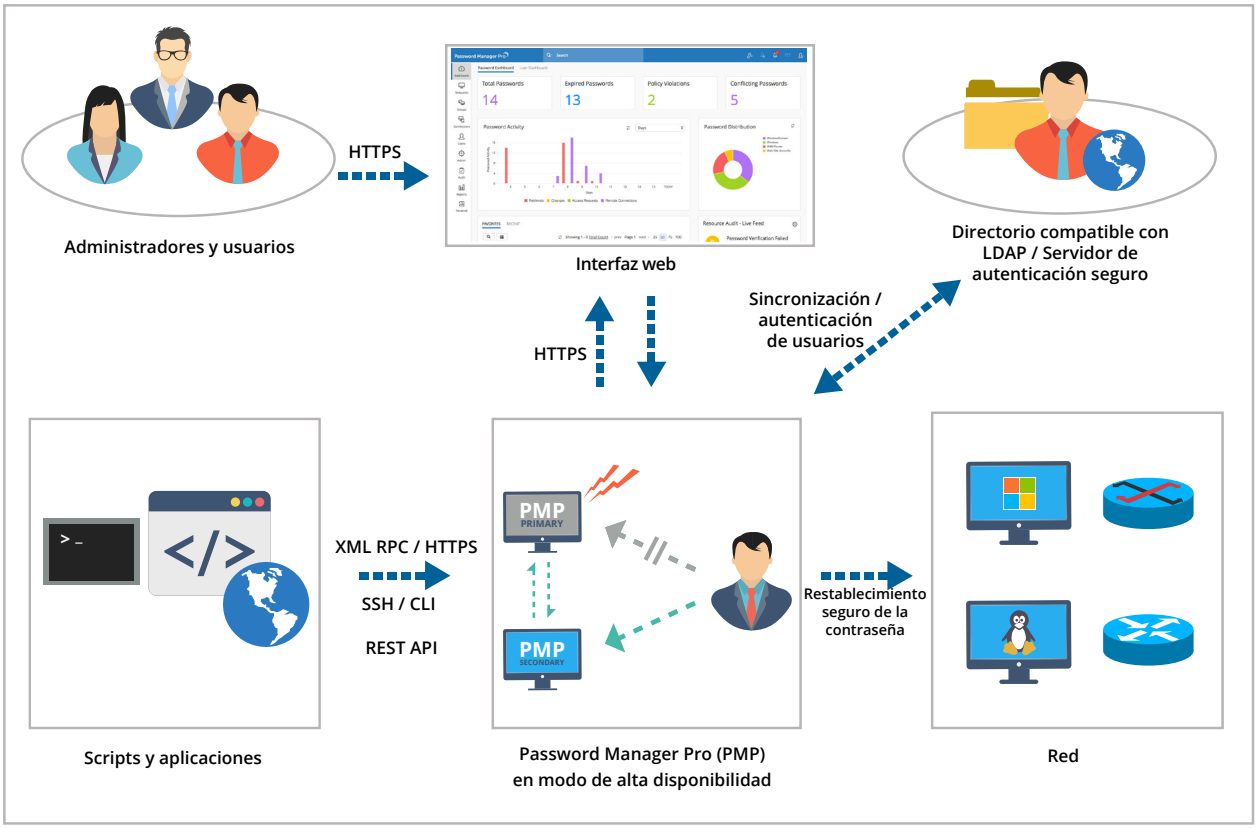
Introducción

Password Manager Pro es una solución integral de gestión de cuentas privilegiadas para controlar, monitorear y centralizar la gestión de credenciales privilegiadas e identidades digitales, como contraseñas, firmas digitales, documentos, imágenes, etc. La solución codifica completamente y consolida todas sus cuentas privilegiadas en una bóveda centralizada, reforzada con controles de acceso granulares. También mitiga los riesgos de seguridad relacionados con el acceso privilegiado y previene las violaciones de la seguridad y los problemas de cumplimiento.

Algunos de los beneficios de la implementación de Password Manager Pro incluyen:

- Eliminación de la fatiga de las contraseñas y de los fallos de seguridad mediante la implementación de una bóveda segura y centralizada para el almacenamiento y el acceso a las contraseñas
- Mejoramiento de la productividad de la TI al automatizar los cambios de contraseña frecuentes necesarios en los sistemas críticos
- Proporcionar controles de seguridad preventivos y detectivos mediante flujos de trabajo de aprobación y alertas en tiempo real sobre el acceso a las contraseñas
- Cumplimiento de las auditorías de seguridad y de la normativa, como SOX, HIPAA y PCI

> Password Manager Pro es un producto sencillo y fácil de implementar de ManageEngine. Permite a los administradores monitorear y auditar todos los accesos a través de una consola única, ofreciendo un gran conjunto de funciones a un coste muy razonable.
>
> ★★★★★
>
> **SC** MAGAZINE,
> Product Group Test
> (Gestión de accesos privilegiados)



01 Gestión de cuentas privilegiadas

Password Manager Pro ayuda a proteger las cuentas sensibles, las claves de sus recursos privilegiados, aplicando las mejores prácticas de gestión de contraseñas, como el almacenamiento centralizado de contraseñas, el uso de contraseñas seguras, el restablecimiento periódico de las contraseñas y el control del acceso de los usuarios a las contraseñas compartidas en toda la organización.

Descubrimiento

Automatice la detección de activos de TI en toda la red corporativa y consolide las cuentas privilegiadas y sus credenciales.

Bóveda de contraseñas segura

Almacene todas las contraseñas de su empresa, las cuentas privilegiadas, las cuentas compartidas, las cuentas firecall y otras en el repositorio seguro y centralizado.

Restablecimiento programado de la contraseña y aleatorización

Restablezca las contraseñas de los recursos remotos desde la interfaz web de Password Manager Pro como y cuando sea necesario o automáticamente a través de tareas programadas. Asigne automáticamente nuevas contraseñas a las cuentas descubiertas para eliminar cualquier vulnerabilidad

Aplique políticas de contraseñas

Imponga el uso de contraseñas seguras y el restablecimiento periódico de las mismas creando y aplicando su política de contraseñas.

Titularidad y uso compartido de contraseñas

Titularidad bien definida para las contraseñas almacenadas en la bóveda centralizada. Opción para compartir selectivamente las contraseñas en función de las necesidades.

Controles de acceso basados en roles

Restricciones detalladas en la gestión de recursos y contraseñas almacenadas en PMP. Las restricciones se aplican en función de los roles de usuario predefinidos.

Restablecimiento automático de contraseñas a distancia

Restablezca las contraseñas de los recursos remotos desde la interfaz web de Password Manager Pro como y cuando sea necesario o automáticamente a través de tareas programadas.

Controles periódicos de integridad

Automatice Password Manager Pro para realizar comprobaciones de integridad de las contraseñas periódicamente para verificar si las contraseñas registradas están sincronizadas con los recursos remotos.

Gestión de cuentas de servicio de Windows

Identifique y restablezca automáticamente las contraseñas de las cuentas de servicio asociadas a las cuentas de dominio.

Gestión de contraseñas entre aplicaciones

Cualquier aplicación o script puede consultar PMP y recuperar las contraseñas para conectarse con otras aplicaciones o bases de datos, eliminando las contraseñas codificadas.

Scripts posteriores al restablecimiento

Opción de ejecutar automáticamente scripts personalizados para llevar a cabo cualquier acción de seguimiento después de una acción de restablecimiento de contraseña.

Modo compatible con FIPS 140-2

Satisfaga los requisitos de conformidad con los módulos criptográficos validados por FIPS 140-2.

02 Gestión del acceso remoto

Password Manager Pro le ofrece un acceso seguro con un solo clic a todos los dispositivos remotos, incluidos los que se encuentran en centros de datos remotos que requieren conectarse primero a los servidores de salto y luego saltar a los dispositivos de destino. Password Manager Pro centraliza la gestión de todas esas credenciales y controles de acceso para que sus usuarios no tengan que autenticarse en cada etapa de un acceso remoto. Se encarga de todos los pasos de inicio de sesión y autenticación de forma automática, lo que le permite acceder a sus recursos remotos con un solo clic.

Acceso remoto de primera clase

Inicie sesiones RDP, SSH, Telnet y SQL altamente seguras, fiables y completamente emuladas con un solo clic desde cualquier navegador compatible con HTML5, sin necesidad de plug-ins adicionales ni software de agente.

Inicio de sesión automático a sitios web y aplicaciones

Inicie sesión automáticamente en los sistemas, sitios web y aplicaciones de destino directamente desde la interfaz web de PMP, sin necesidad de copiar y pegar las contraseñas. Proporcione acceso remoto a los empleados y a los contratistas autorizados sin revelar las contraseñas en texto plano.

Transmisión segura de datos

Consiga la integridad de los datos durante el tránsito con protocolos de comunicación seguros (HTTPS y SSL).

Configuración del servidor de salto

Conéctese directamente a los recursos de los centros de datos remotos sin necesidad de realizar saltos.

03 Gestión de sesiones privilegiadas

Password Manager Pro le ayuda a monitorear de cerca y a tomar el control completo de sus sesiones privilegiadas. Puede hacer un control continuo de lo que hacen sus usuarios con sus accesos privilegiados, para que nunca le sorprendan desprevenido.

Grabación de sesiones privilegiadas

Las sesiones privilegiadas lanzadas desde PMP pueden ser completamente grabadas en vídeo, almacenadas y reproducidas para auditorías forenses.

Controles dobles

Haga seguimiento de sesiones privilegiadas en tiempo real para monitorear la actividad de los usuarios y terminar si hay alguna actividad sospechosa.

Registros completos de auditoría

Reproduzca las grabaciones almacenadas en cualquier momento para escudriñar y responder a preguntas sobre el quién, el qué y el cuándo del acceso privilegiado.

> "Con múltiples formas de API seguras, Password Manager Pro nos ha ayudado a deshacernos de las contraseñas de conexión a bases de datos incrustadas en nuestros diversos servidores de aplicaciones. Ahora las contraseñas se aleatorizan automáticamente y se sincronizan a intervalos periódicos"

Ingeniero de Sistemas Senior de un proveedor de servicios tecnológicos líder en **Estados Unidos**

04 Auditoría, cumplimiento e informes

Pistas de auditoría exhaustivas

Registro completo de "quién", "qué" y "cuándo" del acceso a la contraseña. Informes intuitivos sobre todo el escenario de gestión de contraseñas en su empresa.

Informes de cumplimiento de PCI DSS

Informes sobre las infracciones con respecto al uso y la gestión de contraseñas privilegiadas con base a los requisitos de PCI-DSS.

Alertas en tiempo real

Envíe a su solución SIEM alertas en tiempo real para todas las operaciones auditadas, incluyendo el acceso, la modificación, la eliminación, los cambios en los permisos de uso compartido y otros eventos diversos. Genere traps SNMP y mensajes Syslog a los sistemas de gestión para detectar rápidamente las anomalías.

> "Con Password Manager Pro, la gestión de la creciente lista de contraseñas del sistema es ahora mucho más sencilla. Hemos eliminado la práctica insegura de guardar las contraseñas en copias impresas. Password Manager Pro ha mejorado el rendimiento y la seguridad general de los sistemas que gestionamos a diario."

Mark Laffan,
Jefe de equipo,
Sistemas de redes y comunicaciones,
Universidad Católica Australiana

05 Seguro y preparado para la empresa

Integración de SIEM

Password Manager Pro viene con funciones de integración SIEM para alimentar los datos de acceso privilegiado a cualquier herramienta de gestión de eventos. Las soluciones SIEM pueden entonces consolidar esta información con otros eventos del resto de la empresa y proporcionar consejos inteligibles sobre actividades inusuales.

Integración del sistema de generación de tickets

Automatice los flujos de trabajo de control de acceso a las contraseñas basándose en la validación de los tickets. Integración con numerosos sistemas de tickets, incluida la integración out-of-the-box con ManageEngine ServiceDesk Plus On-Demand, ServiceDesk Plus MSP, ServiceDesk Plus y ServiceNow.

Integración de AD/LDAP

Integración con Active Directory para importar, autenticar y aprovisionar usuarios. Las funciones de autenticación e inicio de sesión único de Active Directory pueden ampliarse a Password Manager Pro, permitiendo a los usuarios iniciar sesión con sus credenciales AD o LDAP.

> “ManageEngine Password Manager Pro es una bendición para nosotros. Es un producto maravilloso”

Sherry Horeanopoulos,
Universidad Estatal de Fitchburg, Estados Unidos

Cifrado avanzado de contraseñas

Todas las contraseñas y los datos confidenciales se cifran mediante un cifrado AES de 256 bits. Doble cifrado para mayor seguridad. Puede configurarse para funcionar en modo compatible con FIPS 140-2.

Autenticación de dos factores

Imponer dos etapas sucesivas de autenticación para iniciar la sesión en PMP. La autentificación habitual es la primera etapa. Se ofrecen varias opciones para la segunda etapa.

Acceso móvil

Recupere las contraseñas y apruebe las solicitudes desde cualquier lugar utilizando nuestra aplicación móvil (disponible en Android, iPhone y Windows). Opción de acceso seguro sin conexión.

> Password Manager Pro cubre todas las funciones que necesitamos. En particular, la capacidad de lanzar, grabar y reproducir sesiones RDP y SSH con recursos remotos es muy agradable. En general, estamos muy contentos con el producto. Está funcionando muy bien para el equipo.

Vinh Nguyen,
Ingeniero de seguridad de TI,
TiVo Inc.

06 Recuperación ante desastres y alta disponibilidad

Arquitectura de alta disponibilidad

Acceso ininterrumpido a las contraseñas de la empresa mediante la implementación de instancias redundantes de servidores y bases de datos.

Acceso seguro sin conexión

Recupere las contraseñas incluso cuando no hay conexión a Internet. La copia offline es tan segura como la versión online. El acceso sin conexión está disponible también en la aplicación móvil.

Copias de seguridad en tiempo real

Opción de copias de seguridad programadas y en tiempo real de toda la base de datos para la recuperación de desastres.

> "Utilizamos Password Manager Pro desde hace casi cinco años. Nos ha ayudado a eliminar la gestión manual de contraseñas, a reducir los gastos administrativos y a mejorar la eficiencia operativa. También cubre nuestra necesidad de gestión de identidades privilegiadas con funciones de descubrimiento y registro de sesiones. En general, Password Manager Pro es una muy buena solución para aumentar la productividad"

Muhamed Noufal,
Subdirector
Seguridad de bases de datos y sistemas
Banco Islámico de Dubai

Especificaciones del producto

Integraciones

Autenticación de usuarios

AD
Azure AD
LDAP
RADIUS
Smart Card

SAML SSO

Azure AD
Microsoft ADFS
Okta
OneLogin

Autenticación de dos factores

PhoneFactor
RSA SecurID
Google Authenticator
Microsoft Authenticator
Okta Verify
RADIUS-based authenticators
Duo Security
YubiKey

ITSM

ServiceDesk Plus On-Demand
ServiceDesk Plus MSP
ServiceDesk Plus
ServiceNow
JIRA Service Desk

SIEM

Herramientas compatibles con RFC 3164 como Splunk, Arcsight, EventLog Analyzer

Plataformas CI/CD

Jenkins
Ansible
Chef
Puppet

Almacenamiento en la nube

Dropbox,
Amazon S3
Box

Requisitos mínimos del sistema

Procesador	RAM	Disco duro
Dual Core o superior	4 GB o más	Aplicación: > 200 MB Base de datos: > 10 GB

Sistemas operativos

Windows

- 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 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 distribución de Linux

Bases de datos

- PostgreSQL 9.5.3, incluido en el producto
- MS SQL Server 2008 o versiones posteriores (el servidor SQL debe estar instalado en Windows 2008 Server o en versiones posteriores)

Navegadores

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

Virtualización

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

Descubrimiento de cuentas privilegiadas

- Windows
- Linux
- Network devices
- VMware

Protocolos de sesión compatibles

RDP, VNC, SSH, SQL

Plataformas compatibles con el restablecimiento remoto de la contraseña

Sistemas operativos

1. Windows (cuentas locales, de dominio y de servicio)
2. Linux
3. Mac
4. Solaris
5. HP Unix
6. IBM AIX
7. HP-UX
8. Junos OS

Dispositivos Cisco

1. Cisco Integrated Management Controller
2. Cisco Catalyst
3. Cisco SG300
4. Cisco UCS
5. Cisco Wireless LAN Controller
6. Cisco IOS
7. Cisco PIX
8. Cisco CatOS

Servidores de bases de datos

1. MS SSQL
2. MySQL
3. Sybase ASE
4. Oracle DB server
5. PostgreSQL

Dispositivos de red

1. ASA Firewall
2. Audiocode
3. Brocade
4. Brocade VDX
5. Brocade SAN Switch
6. Checkpoint Firewall
7. Citrix Netscaler SDX
8. Citrix Netscaler VPX
9. Extreme Networks
10. F5
11. Fortinet
12. Fortigate Firewall
13. FortiMail
14. Fujitsu Switch
15. Gigamon
16. H3C
17. HMC
18. HP Printer
19. HP Onboard Administrator
20. HP Virtual Connect
21. Huawei
22. HP ProCurve
23. Juniper
24. Juniper Netscreen ScreenOS
25. HP iLO
26. Magento
27. MikroTik
28. NetApp 7-Mode
29. NetApp cDOT
30. Opengear
31. Orange Firewall
32. Palo Alto Networks
33. pfSense
34. Routerboard
35. Ruijie Networks
36. SonicWall
37. TP-Link
38. VMware vCenter

Almacén de archivos

1. HPE StoreOnce
2. File Store
3. Key Store
4. License Store
5. Nimble Storage
6. Certificate Store

Servicios en la nube

1. AWS IAM
2. Google Apps
3. Microsoft Azure
4. Rackspace
5. Salesforce
6. WebLogic

Otros

1. Cuentas de sitios web
2. LDAP Server
3. VMware ESXi
4. IBM AS/400
5. Oracle XSCF
6. Oracle ALOM
7. Oracle ILOM
8. Aruba ATP
9. Avaya-GW
10. FortiManager-FortiAnalyzer
11. Nortel

Integración con ManageEngine Key Manager Plus

Password Manager Pro se integra fácilmente con la solución interna de gestión de certificados y claves de ManageEngine — **Key Manager Plus** — para formar un conjunto completo de gestión de identidades privilegiadas.

Consiga todo lo que necesita para proteger su entorno de cifrado con la oferta de gestión de claves SSH y certificados SSL de Key Manager Plus.

ManageEngine
Key Manager Plus

Gestión de certificados SSL

Descubrimiento

1. Certificados de usuario AD
2. Certificados emitidos por la CA local
3. Certificados emitidos por Microsoft Certificate Stores
4. Certificados del servidor SMTP
5. Certificados autofirmados

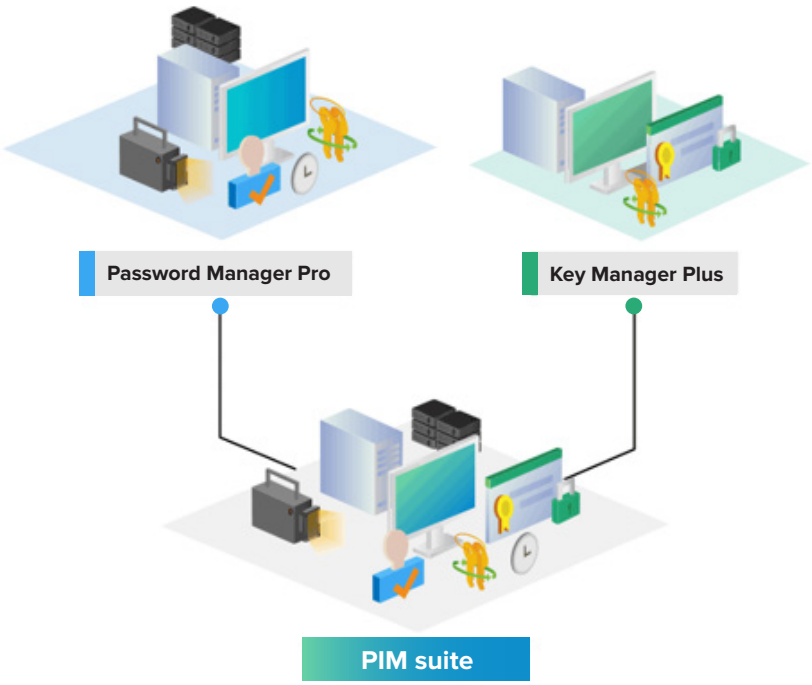
Integración de la autoridad de certificación

1. Let's Encrypt
2. GoDaddy
3. Microsoft CA
4. Symantec
5. Thwate
6. RapidSSL
7. Geotrust
8. Sectigo

Especificaciones de la clave privada del certificado

Algoritmos de la clave	Tamaño de la clave (en bits)
RSA	4096
DSA	2048
EC	1024
Funciones de Hash	**Tipos de almacén de claves**
SHA256	JKS
SHA384	PKCS12
SHA512	

La suite PIM integrada



Otras especificaciones del producto

Algoritmos de cifrado
Criptografía validada AES-256, SafeNet Luna PCIe HSM FIPS 140-2

Compatibilidad con API
REST, XML-RPC, SSH CLI

Recuperación ante desastres
Alta disponibilidad con configuración secundaria en tiempo real.
Múltiples instancias del servidor de aplicaciones.
Failover cluster del servidor SQL

Aplicaciones móviles
iOS, Android

Extensiones del navegador
Chrome, Firefox, IE

Idiomas
Alemán, francés, inglés, japonés, polaco, chino simplificado, español, chino tradicional, turco

Descargar una prueba gratuita de 30 días

Solicitar una demo personalizada

Más de 180.000
empresas de todo el mundo confían en
ManageEngine

G2 CROWD REVIEWS

¡Gran producto, equipo de asistencia técnica de clase mundial!

★★★★★

El modelo de precios del producto es muy bueno, el mejor que he visto. El producto funciona muy bien y en caso de problemas puedes contar con el equipo de asistencia técnica de ManageEngine. Conocen su producto y le ayudan en todo lo que puedan. Incluso nos corrigieron un parche personalizado en un día. Nunca antes había visto este tipo de compromiso con un cliente. ¡Soy un cliente feliz y satisfecho!

Martijn Dirkx,
Administrador de sistemas,
SeaChange International, Países Bajos.

Excelente recurso. Fácil de usar y de mantener.

★★★★★

Es muy bueno para mantener las contraseñas de todos los dispositivos, sitios externos y cuentas de aplicaciones internas en un servidor centralizado. Incluso tenemos este servidor como parte de nuestra recuperación ante desastres

Steven.R.McEvoy,
Analista de sistemas senior,
Christie Digital Systems, Canadá.

Potente aplicación para la gestión de contraseñas empresariales.

★★★★☆

Con Password Manager Pro, solucionamos los problemas que giraban en torno al uso de las cuentas administrativas. La gestión centralizada de contraseñas, el restablecimiento automático de contraseñas y los informes son algunas de las características que más nos gustan.

Said Youssef,
Oficial de seguridad senior,
Chisholm Institute, Australia.

www.passwordmanagerpro.com

Asistencia técnica

Teléfono: +1 408 454 4014

Email: support@passwordmanagerpro.com

Síganos en

ManageEngine

Password Manager Pro

Para consultas: hello@passwordmanagerpro.com

Para la demo: demo.passwordmanagerpro.com