ManageEngine
Password Manager Pro

The complete privileged account management solution

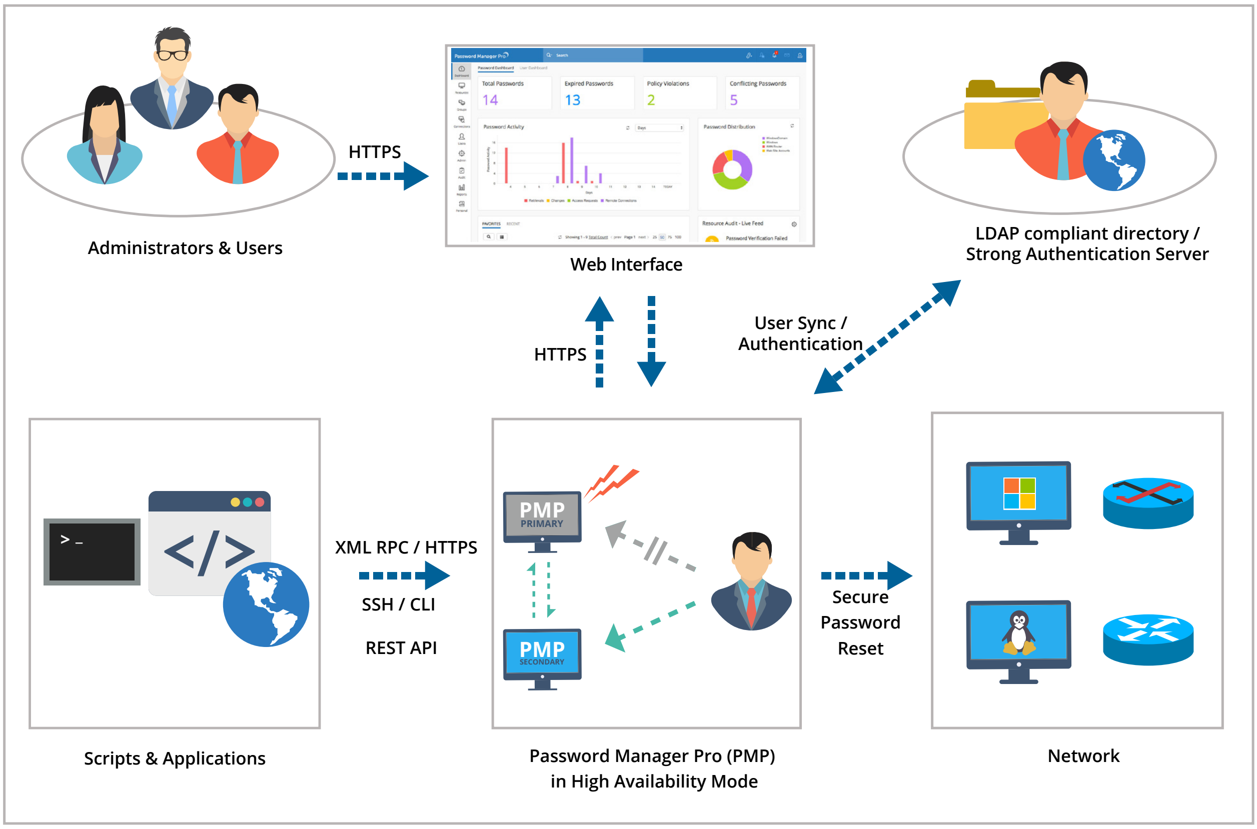
Introduction

Password Manager Pro is a comprehensive privileged account management solution to control, monitor, and centralize the management of privileged credentials and digital identities, such as passwords, digital signatures, documents, images and so on. The solution fully encrypts and consolidates all your privileged accounts in one centralized vault, reinforced with granular access controls. It also mitigates security risks related to privileged access and pre-empts security breaches and compliance issues.

Some of the benefits of deploying Password Manager Pro include:

- Eliminating password fatigue and security lapses by deploying a secure, centralized vault for password storage and access
- Improving IT productivity many times by automating frequent password changes required in critical systems
- Providing preventive & detective security controls through approval workflows & real-time alerts on password access
- Meeting security audits and regulatory compliance such as SOX, HIPAA and PCI

> Password Manager Pro is a simple and easy-to-deploy product from ManageEngine. It allows administrators to monitor and audit all access through a single pane of glass, by offering a great feature set at a very reasonable cost.
>
> ★★★★★
>
> **SC** MAGAZINE,
> Product Group Test
> (Privileged access management)



01 Privileged account management

Password Manager Pro helps secure sensitive accounts, the keys to your privileged resources by enforcing password management best practices such as centralized password storage, use of strong passwords, regular password resets, and controlling user access to shared passwords across your organization.

Discovery

Automate discovery of IT assets across your corporate network and consolidate privileged accounts and their credentials.

Secure password vault

Store all your enterprise passwords, privileged accounts, shared accounts, firecall accounts and others in the secure, centralized repository

Scheduled password resets and randomization

Reset the passwords of remote resources from Password Manager Pro web-interface as and when required or automatically through scheduled tasks. Assign new passwords for discovered accounts automatically to eliminate any vulnerabilities

Enforce password policies

Mandate usage of strong passwords and periodic resets by creating and enforcing your password policy.

Password ownership and sharing

Well-defined ownership for the passwords stored in the centralized vault. Provision for selective sharing of passwords on requirement basis.

Role-based access controls

Fine-grained restrictions on managing resources and passwords stored in PMP. Restrictions are enforced based on predefined user roles.

Automated remote password resets

Reset the passwords of remote resources from Password Manager Pro web-interface as and when required or automatically through scheduled tasks.

Periodic integrity checks

Automate Password Manager Pro to conduct password integrity checks periodically to verify whether the passwords on record are in sync with remote resources.

Windows service account management

Automatically identify and reset the passwords of service accounts associated with domain accounts.

Application-to-Application password management

Any application or script can query PMP and retrieve passwords to connect with other applications or databases, eliminating hard-coded passwords.

Post-reset scripts

Option to automatically execute custom scripts to carry out any follow-up action after a password reset action.

FIPS 140-2 compliant mode

Satisfy compliance requirements with FIPS 140-2 validated cryptographic modules.

02 Remote access management

Password Manager Pro gives you secure, one-click access to all remote devices, including those in remote data centers that require connecting to jump servers first and then hopping to the target devices. Password Manager Pro centralizes the management of all those credentials and access controls so your users don’t have to authenticate themselves at each stage of a remote access. It handles all login and authentication steps automatically, giving you one-click access to your remote resources.

First-in-class remote access

Launch highly secure, reliable, and completely emulated RDP, SSH, Telnet, and SQL sessions with a single click from any HTML5-compatible browser, without any additional plug-ins or agent software.

Automatic login to websites and applications

Automatically log on to the target systems, websites and applications directly from the PMP web interface without copying and pasting of passwords. Provide remote access to employees and authorized third-party contractors without disclosing the passwords in plain-text.

Secure data transmission

Achieve data integrity during transit with secure communication protocols (HTTPS and SSL).

Jump server configuration

Connect directly to remote data center resources without anyhops or jumps.

03 Privileged session management

Password Manager Pro helps you closely monitor and take complete control over your privileged sessions. You can continuously track what your users are doing with their privileged access, so you're never caught unaware.

Privileged session recording

Privileged sessions launched from PMP can be completely video recorded, archived and played back for forensic audits.

Dual controls

Shadow privileged sessions in real time to monitor user activity and terminate if there's any suspicious activity.

Complete audit records

Play back the archived recordings at any time to scrutinize and answer questions on the who, what, and when of privileged access.

> "With multiple forms of secure APIs, Password Manager Pro has helped us get rid of embedded database connection passwords in our various application servers. Passwords are now automatically randomized and synchronized at periodic intervals."

Senior Systems Engineer with a leading technology service provider in **USA**.

04 Audit, compliance & reports

Comprehensive audit trails

Complete record of 'who', 'what' and 'when' of password access. Intuitive reports on entire password management scenario in your enterprise.

PCI DSS compliance reporting

Reports on the violations with respect to the use and management of privileged passwords based on the requirements of PCI-DSS.

Real-time alerts

Send real-time alerts for all audited operations, including access, modification, deletion, changes in share permissions, and various other events, to your SIEM solution. Generate SNMP traps and Syslog messages to management systems to detect anomalies quickly.

> "With Password Manager Pro, managing the growing list of system passwords has become much simpler. We have done away with the insecure practice of keeping the passwords in print-outs. Password Manager Pro has improved the performance and overall security of the systems we manage on a daily basis."

Mark Laffan,
Team Leader,
Network & Communication Systems,
Australian Catholic University

05 Secure and enterprise-ready

SIEM integration

Password Manager Pro comes with SIEM integration capabilities to feed privileged access data to any event management tool. SIEM solutions can then consolidate this information with other events from the rest of the enterprise and provide intelligible tips about unusual activities.

Ticketing system integration

Automate password access control workflows based on ticket validation. Integration with numerous ticketing systems, including out-of-the-box integration with ManageEngine ServiceDesk Plus On-Demand, ServiceDesk Plus MSP, ServiceDesk Plus, and ServiceNow.

AD/LDAP integration

Integration with Active Directory to import, authenticate, and provision users. Active Directory's authentication and single sign-on capabilities can be extended to Password Manager Pro, letting users log on with their AD or LDAP credentials.

> ManageEngine Password Manager Pro is a Godsend for us.
> It is a wonderful product.
>
> **Sherry Horeanopoulos,**
> Fitchburg State University, USA

Advanced password encryption

All passwords and sensitive data are encrypted using AES 256-bit encryption. Dual encryption for extra security. Can be configured to run in FIPS 140-2 compliant mode.

Two-factor authentication

Enforcing two successive stages of authentication for logging in to PMP. Usual authentication is the first stage. Various options provided for the second stage.

Mobile access

Retrieve passwords and approve requests on the go using our mobile app (available on Android, iPhone and Windows). Provision for secure offline access.

> “Password Manager Pro covers all the features we need. Particularly, the ability to launch, record and playback RDP and SSH sessions with remote resources is very nice. Overall, we are very happy with the product. It’s working out very well for the team.”
>
> **Vinh Nguyen,**
> IT Security Engineer,
> TiVo Inc.

06 Disaster recovery & high availability

High availability architecture

Uninterrupted access to enterprise passwords through the deployment of redundant server and database instances.

Secure offline access

Retrieve passwords even when there is no internet connectivity. The offline copy is as secure as the online version. Offline access is available in mobile app too.

Live backups

Provision for both scheduled and live backup of entire database for disaster recovery.

> “We are using Password Manager Pro for nearly five years. It has helped us do away with manual password management, reduce administrative overheads, and improve operational efficiency. It also covers our need for privileged identity management with discovery and session recording capabilities. Overall, Password Manager Pro is a very good solution to boost productivity.”

Muhamed Noufal,
Assistant Manager
Database & Systems Security
Dubai Islamic Bank

Product specification

Integrations

User authentication

AD
Azure AD
LDAP
RADIUS
Smart Card

SAML SSO

Azure AD
Microsoft ADFS
Okta
OneLogin

Two-factor authentication

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

RFC 3164-compliant tools such as Splunk, Arcsight, EventLog Analyzer

CI/CD platforms

Jenkins
Ansible
Chef
Puppet

Cloud storage

Dropbox,
Amazon S3
Box

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 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

- PostgreSQL 9.5.3, bundled with the product
- 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.

Virtualization

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

Privileged account discovery

- Windows
- Linux
- Network devices
- VMware

Session protocols supported

RDP, VNC, SSH, SQL

Platforms supported for remote password reset

Operating systems

1. Windows (local, domain, and service accounts)
2. Linux
3. Mac
4. Solaris
5. HP Unix
6. IBM AIX
7. HP-UX
8. Junos OS

Cisco devices

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

Database servers

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

Network devices

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

File store

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

Cloud services

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

Others

1. Website accounts
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

Integration with ManageEngine Key Manager Plus

Password Manager Pro readily integrates with ManageEngine's in-house certificate and key management solution—**Key Manager Plus**—to form a comprehensive privileged identity management suite.

Achieve all that you need to protect your crypto-environment with Key Manager Plus' SSH key and SSL certificate management offering.

ManageEngine Key Manager Plus

SSL certificate management

Discovery

1. AD user certificates
2. Certificates issued by local CA
3. Certificates issued by Microsoft certificate store
4. SMTP server certificates
5. Self-signed certificates

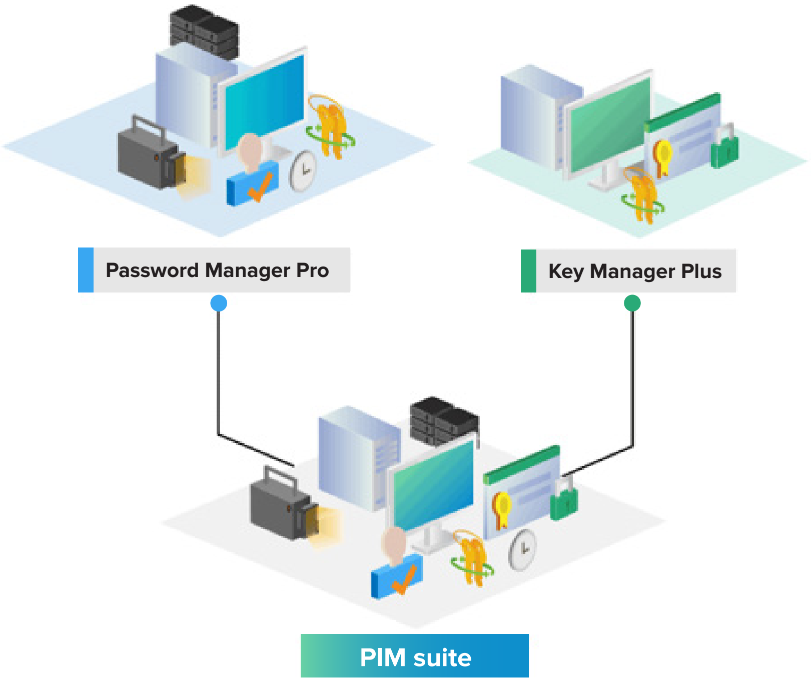
Certificate authority integration

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

Certificate private key specifications

Key algorithms	Key size (in bits)
RSA DSA EC	4096 2048 1024
Hash functions	**Keystore types**
SHA256 SHA384 SHA512	JKS PKCS12

The integrated PIM suite



Other product specifications

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

API support
REST, XML-RPC, SSH CLI

Disaster recovery
High availability with live secondary setup
Multiple application server instances
SQL server failover cluster

Mobile applications
iOS, Android

Browser extensions
Chrome, Firefox, IE

Languages
English, French, Portuguese, German, Japanese, Polish, Simplified Chinese, Spanish, Traditional Chinese, Turkish

Download a 30-day free trial

Request a personalized demo

180,000+
companies around the world trust
ManageEngine

G2 CROWD REVIEWS

Great product, World Class Support Team!

★★★★★

The pricing model of the product is very good, the best I've seen. The product works great and with issues you can count on the support team of ManageEngine. They know their product and help you in every way they can. We even had a custom patch fixed for us in a day. Never seen this kind of commitment to a customer ever before.I am one happy and satisfied customer!

Martijn Dirkx,
System Administrator,
SeaChange International, Netherlands.

Excellent resource. Easy to use and maintain.

★★★★★

It is great to keep passwords for all devices, external sites, and internal application accounts in one centralized server. We even have this server as part of our disaster recovery.

Steven.R.McEvoy,
Senior Systems Analyst,
Christie Digital Systems, Canada.

Powerful application for managing enterprise passwords.

★★★★☆

With Password Manager Pro, we solved problems revolving around the use of administrative accounts. Centralized password management, automated password resets, and reporting are some features that we like best.

Said Youssef,
Senior Security Officer,
Chisholm Institute, Australia.

www.passwordmanagerpro.com

Technical support

Telephone: +1 408 454 4014

Email: support@passwordmanagerpro.com

Follow us on f 🐦

ManageEngine

Password Manager Pro

For queries: hello@passwordmanagerpro.com
For demo: demo.passwordmanagerpro.com