ManageEngine
Password Manager Pro

Best Practices Guide

www.passwordmanagerpro.com

Table of Contents

1.0 Overview

1.1 About Password Manager Pro

Password Manager Pro is a web-based, privileged identity management solution that lets IT teams manage privileged identities—passwords, SSH keys, and SSL certificates—as well as control and monitor privileged access to critical information systems from a single, centralized console. It also helps prove compliance with regulations like PCI DSS, NERC CIP, and SOX that mandate privileged access control.

1.2 About the guide

This guide describes the best practices for setting up and using Password Manager Pro in an enterprise network environment. Coming from our experience of helping organizations around the world deploy Password Manager Pro successfully and streamline their privileged access management practices, this guide offers direction to IT administrators for quick and efficient software setup, as well as secure privileged account management implementation. The best practices can be adopted during all stages—product installation, configuration, deployment, and maintenance—and they are explained below with a special focus on data security, scalability, and performance.

2.0 Recommended system configuration

2.1 Minimum system requirements

Before installing Password Manager Pro, you need to decide on the system configuration. The minimum system requirements to run Password Manager Pro can be found here.

In general, the performance and scalability depends on the following factors:

- Number of users and groups.
- Number of resources and groups.
- Frequency of resource or password sharing.
- Number of scheduled tasks.

Based on the above factors, the following system settings are recommended for medium and large enterprises:

Medium enterprises

No. of users: 100-500

No. of resources/passwords: Up to 10,000

- Dual core processor or above
- 8 GB RAM
- 40 GB hard drive space

Large enterprises

No. of users: More than 500

No. of resources/passwords: More than 10,000

- Quad core processor or above
- 16 GB RAM
- 100 GB hard drive space

Note: We also recommend you install Password Manager Pro on a dedicated, hardened, high-end server for superior performance and security.

3.0 Installation

3.1 Windows vs Linux

Password Manager Pro can be installed on either Windows or Linux. Though the software runs equally on both the platforms, installing on Windows provides the following inherent advantages:

Active Directory (AD) integration: A Windows installation of Password Manager Pro can be directly integrated with Active Directory to import users and groups. Moreover, users who have logged into their Windows system with domain account credentials can use single sign-on (NTLM-SSO) to automatically log in to Password Manager Pro. With a Linux installation, you have to rely on LDAP-based authentication for Active Directory services.

Password resets for Windows resources: A Windows installation of Password Manager Pro can perform password resets in agentless mode for all supported target systems, as long as there is direct connectivity. On the other hand, Linux installation requires an agent to be deployed on all Windows resources and domain controllers to reset passwords of Windows domain accounts, service accounts, and local accounts.

Aside from the above, password resets for Windows service accounts, Scheduled Tasks, IIS Web.Config files and IIS app pool accounts are supported only from a Windows installation of Password Manager Pro.

3.2 Back-end database

Password Manager Pro provides back-end support for PostgreSQL database and MS SQL Server. By default, the product comes bundled with PostgreSQL database, which is ideal for small and medium businesses. Meanwhile, for large businesses, we highly recommend you use MS SQL Server as your back end for better scalability, performance, clustering, and disaster recovery.

If you're using MS SQL Server as your back end, we suggest the following practices:

- Password Manager Pro can communicate with MS SQL Server only over SSL, with a valid certificate configuration. Therefore, we recommend you have a dedicated SQL instance for Password Manager Pro to avoid any conflicts or disruptions with existing databases.

- While using MS SQL Server as your back end, a unique key is auto-generated for database-level encryption and by default, this key will be stored in the <PMP HOME/conf> directory, in a file named <masterkey.key>. We recommend you move the key file to a different location to protect it from unauthorized access. Since this key file is required for high availability configurations and during disaster recovery, its safety is paramount. Losing the key will lead to an MS SQL Server reconfiguration and may even result in data loss.

- Use Windows authentication while configuring MS SQL Server as your back end rather than using an SQL local account.

- We recommend you use the same domain account to run both Password Manager Pro server and MS SQL server, so that you can run SQL service and SQL agent services.

- The force encryption option should be enabled to allow all clients to connect to this SQL instance. When this is done, all client-to-server communication will be encrypted and clients that cannot support encryption will be denied access.

- Disable all protocols other than TCP/IP in the machine where MS SQL server is running.

- Hide this SQL instance to prevent it from being enumerated by other tools and disable access to this database for all other users except Password Manager Pro's service account.

- Set up firewall rules to allow access only for the required ports in the machine where MS SQL server is running.

3.3 Secure the installation master key

Password Manager Pro uses AES-256 encryption to secure passwords and other sensitive information. The key used for encryption (pmp_key.key) is auto-generated and unique for every installation. By default, this key will be stored in the <PMP HOME/conf> directory, in a file named <pmp_key.key>. The path of this key needs to be configured in the manage_key.conf file present in the PMP HOME/conf directory. Password Manager Pro requires this folder to be accessible with necessary permissions to read the pmp_key.key file when it starts up every time. After a successful start-up, it does not need access to the file anymore and so the device with the file can be taken offline. We highly recommend you move this key to a different secure location and lock it down by providing read access only to Password Manager Pro's service account. Also, update this remote path in the "manage_key.conf" file so that the product can read the encryption key during start up. You can also secure this key by storing it in a USB drive or disk drive. For extreme security, create script files to copy this key into a readable location and then destroy the copy upon service start up.

3.4 Take control of the database credential

Apart from AES encryption, the Password Manager Pro database is secured through a separate password, which is auto-generated and unique for every installation. This database password can be securely stored in Password Manager Pro itself. But we recommend you store the password in some other secure location accessible to the product server.

By default, the database information, such as the JDBC URL, log in credentials, and other parameters, will be stored in a file named database_params.conf, which is present in the <PMP HOME/conf> directory. Although the database is configured to not accept any remote connections, we recommend you move this file to a secure location, restrict access, and make it available only for Password Manager Pro's service account. If you place the database_params.conf file outside the PMP installation folder, you need to specify the location along with the filename in <PMP-Home>\conf\wrapper.conf file (for Windows) or <PMP-Home>\conf\"wrapper_lin.conf file (for Linux). Note that the service cannot be started if the entire location is not specified here.

- The path of this file is configured in the "wrapper.conf" file present in the <PMP HOME/conf> directory. Edit this file and look for the line `wrapper.java.additional.9=-Ddatabaseparams.file.`

- If you are using a Linux installation, then you will have to edit the file "wrapper_lin.conf" present in the <PMP HOME/conf> directory.

- The default path will be configured as `./../conf/database_params.conf.` Move the "database_params.conf" file to a secure location and specify its path in the above file. For example, `wrapper.java.additional.9=-Ddatabaseparams.file=\\remoteserver1\tapedrive\sharedfiles\database_params.conf.`

- Save the file and restart Password Manager Pro for the change to take effect.

Note: The above steps are applicable only for PostgreSQL and MySQL. If you are using MS SQL server as your back end, refer to section 3.2.

4.0 Server and environmental settings

4.1 Server hardening

By default, all components required for Password Manager Pro to function are stored in the installation directory (ManageEngine/PMP). Therefore, we highly recommend you harden the server in which Password Manager Pro is installed. Some of the basic steps you should carry out are as follows:

- Disable remote access to this server for all regular domain users in your organization using domain group policies. Restrict read permissions for all regular administrators, and provide write permissions to Password Manager Pro drive or directories for only one or two domain administrators.

- Set up inbound and outbound firewalls to protect against incoming and outgoing traffic, respectively. Using this setting, you can also specify which server ports must be opened and, ideally, used to carry out various password management operations such as remote password resets.

4.2 Use a dedicated service account

Create a separate service account for Password Manager Pro in your domain controller and use it in all areas of Password Manager Pro. The same account will be used to run Password Manager Pro. To begin using the service account created for Password Manager Pro, go to the service console ("services.msc") in the server where Password Manager Pro is installed and navigate to the properties of Password Manager Pro. Change the configured local system account with the service account created. This same service account can also be used for importing users and resources from Active Directory.

4.3 Configure a bound IP address for the web server

By default, Password Manager Pro's web-server will bind to all available IP addresses of the server in which the application is installed. Due to this, Password Manager Pro will be reachable on any or all IP address(es) with the configured port (7272). To restrict this, we recommend you configure the web server to bind to a single IP address and receive incoming communications from that IP address alone. The following steps can be used to configure the bound IP:

- Stop Password Manager Pro if it is running.
- Open the "server.xml" file present in the <PMP_HOME>\conf folder.
- Search for this line:

```
<Connector SSLEnabled="true" URIEncoding="UTF-8"
acceptCount="100" ciphers="TLS_RSA_WITH_AES_256_CBC_SHA,TLS_
RSA_WITH_AES_256_CBC_SHA256" clientAuth="false" debug="0"
disableUploadTimeout="true" enableLookups="false" keystore-
File="conf/server.keystore" keystorePass="passtrix" maxHttp-
HeaderSize="32768" maxSpareThreads="75" maxThreads="150"
minSpareThreads="25" port="7272" scheme="https" se-
cure="true" server="PMP" sslProtocol="TLS" truststoreFile="-
jre/lib/security/cacerts" truststorePass="changeit" trust-
storeType="JKS" useBodyEncodingForURI="true"/>
```

- In the above line, next to the value `port="7272"`, add the attribute `address="127.0.0.1"`. Replace `127.0.0.1` with the actual IP address of the server that you want to use for binding.

4.4 Restrict web-server access by black or white listing IP addresses

Password Manager Pro can be accessed from any client system, as long as there is connectivity. So, we recommend you restrict and provision only a limited number of client systems with access to Password Manager Pro. To configure IP based restrictions, navigate to **Admin >> Configuration >> IP Restrictions >> Web Access.** The IP restrictions can be set at various levels and combinations, such as defined IP ranges or individual IP addresses. You can choose to allow web access to specific IP ranges and addresses or alternatively, restrict access by adding them to the blocked IP address(es) field.

5.0 User onboarding and management

5.1 Leverage AD/LDAP integration for authentication and provisioning

Integrating Password Manager Pro with Active Directory or any LDAP-compliant directory can be very useful, as it provides the following benefits:

User provisioning or deprovisioning: With AD/LDAP integration, user addition in Password Manager Pro is quick and easy. Once integrated, you can directly import the user profiles and groups or OUs from your directory to Password Manager Pro. Moreover, user account provisioning in the product becomes a simple process. For instance, if you import an existing OU of "Database Administrators" from your directory to Password Manager Pro, you can easily allocate the database passwords to that imported group.

On top of this, you can enable synchronization while integrating Password Manager Pro with your directory so that any change, such as a user newly added or moved around between OUs in your directory, will automatically reflect in Password Manager Pro. Synchronizing Password Manager Pro with your directory will also keep you notified when a user is permanently deleted from the corresponding user directory. Password Manager Pro disables and locks such user accounts, notifies you of the same through an email and alert notification, upon which you can chose to either delete those accounts or reactivate them.

Active Directory authentication: Another benefit is that you can leverage your directory's respective authentication mechanism and provide your users with single sign-on (SSO) options. Once you activate this option, users will be automatically authenticated into Password Manager Pro (using NTLM-based authentication) as long as they have already logged in to the system with their directory credentials. Using AD credentials for Password Manager Pro authentication ensures that login passwords are not stored locally in Password Manager Pro, since users will be directly authenticated from your directory.

5.2 Disable local authentication

After integrating Password Manager Pro with your AD/LDAP-compliant directory, we advise you disable local authentication and let users log on to Password Manager Pro using their AD/LDAP credentials. To disable local authentication, navigate to **Admin >> Settings >> General Settings >> User Management.**

However, if you have configured a local Password Manager Pro account for break glass purposes, you cannot disable local authentication. In such cases, if you still want to have only AD/LDAP authentication, we recommend you disable the **"Forgot Password"** option in the same section (option used to reset the local authentication password for all users in Password Manager Pro). Disabling this option will ensure users can log in to Password Manager Pro using only their AD/LDAP credentials, even if local authentication is enabled.

5.3 Use two-factor authentication

An additional protective layer of user authentication ensures that only the right people have access to your sensitive resources. Password Manager Pro provides multiple options for configuring a second level of authentication before providing access to the product's web interface. The second factor options are: PhoneFactor, RSA SecurID tokens, Duo Security, Google Authenticator, unique passwords through email, any RADIUS-compliant two-factor authentication, Microsoft Authenticator, Okta Verify, and YubiKey. It is highly recommended to configure two-factor authentication for your users.

5.4 Assign user roles based on job responsibilities

After adding users, assign them proper roles. Password Manager Pro has four predefined user roles: administrator, password administrator, password auditor, and password user. To learn more about the privileges of each role, please refer to our help documentation. Administrator roles should be restricted only to the handful of people who need to perform

user management operations and product-level configurations in addition to password management.

Using the super administrator role: A super administrator in Password Manager Pro has access to all stored passwords. Ideally, this role is not required. However, if you would like to have a dedicated account for emergency purposes, you can create a super administrator for your organization. For security reasons, this role should always be limited to the top people in the organizational hierarchy. Also, the best practice approach in such cases is to create only one super administrator. Once an administrator has been promoted to a super administrator, they can prevent the creation of more super admins in the future as needed. This can be done by the super administrator navigating to **Admin >> Authentication >> Super Administrators,** and then enabling **Deny Creation of Super Admins by Admins.** For more information, refer to this documentation.

5.5 Create user groups

Organize your users into groups—for example, Windows administrators, Linux administrators, and so on. User grouping helps immensely while sharing resources and delegating passwords. If you've integrated Password Manager Pro with AD/LDAP, you can import user groups directly from the directory and use the same hierarchical structure.

5.6 Remove the default admin account

For security reasons, we highly recommend you delete the default admin and guest accounts in Password Manager Pro, after you've added one or more users with the administrator role.

5.7 Restrict access to mobile apps and browser extensions

By default, all users will be able to access Password Manager Pro's native mobile applications and browser extensions. If you would like your users to not be able to access any of the passwords from any device other than their workstation, disable access to mobile apps globally across your organization. If needed, you can enable access for required users or administrators alone. Similarly, you can also enable or disable access to browser extensions. These restrictions can be enforced by navigating to **Users >> More Actions** and selecting **Restrict Mobile Access/Restrict Browser Extension** from the drop-down menu.

6.0 Data population and organization

6.1 Adding resources: Choose a convenient method

The first step to getting started with password management in Password Manager Pro is adding resources. The quickest and most convenient way to do this is automated discovery of privileged accounts. The other ways are manual addition and CSV import. Use the import via CSV/TSV feature if you used another tool before switching to Password Manager Pro or have your credentials stored in spreadsheets.

6.2 Remember to specify resource types

While adding resources manually or via CSV import, check whether all resources have been properly sorted under a resource type. This is mandatory for using features such as password resets since Password Manager Pro uses different modes of communication for different resources, based on the applied resource type. Unless specified, resources will be sorted under "Unknown" and in that case, password resets will fail. Password Manager Pro provides 32 default resource types, listed under **Admin >> Resource Types.**

6.3 Remove unauthorized privileged accounts

When you use the auto-discovery feature to inventory the IT resources on your network and their respective privileged accounts, Password Manager Pro will, by default, fetch every single account associated with the resources detected on the network. Some accounts may be unauthorized, unwanted, or orphaned. For instance, when you add a Windows resource, all guest accounts will also be fetched.

From a security perspective, unauthorized accounts should be identified and deleted to avoid any unforeseen vulnerabilities in the future. Password management best practices demand that the number of privileged accounts should be kept at a minimum. Moreover, dumping unwanted accounts can also clutter the database and make data organization a daunting task. Therefore, we recommend you remove these unwanted accounts in the target machine itself before running auto-discovery in Password Manager Pro.

6.4 Randomize passwords after resource discovery

Once you have completed resource discovery and account enumeration, we highly recommend you randomize the passwords for all accounts. This practice is important because before deploying Password Manager Pro, your employees may have stored their passwords in different media such as spreadsheets and text files or may have even copied them down on paper. If the passwords are not changed, those employees can still access the resources directly, outside of Password Manager Pro. Therefore, passwords must be duly randomized after resource discovery to block all direct, unauthorized access to resources. In addition, randomization also gets rid of weak passwords and assigns strong, unique passwords for resources. Password randomization for the discovered accounts can be carried out from **Resources >> select the specific resource(s) >> Resource Actions** (at the top) **>> Configure Remote Password Reset.**

Note: In future, if you would like to preset password randomization for new accounts when they are discovered, you can configure the same from **Resources >> select the specific resource(s) >> Resource Actions** (at the top) **>> Discover Accounts,** and then enable **Randomize Passwords After Discovery** in the new window that opens.

6.5 Leverage the power of resource groups

Resource groups are quite powerful in Password Manager Pro. Most of the advanced password management operations, such as automated password delegation and scheduled password rotation, can be performed only at the resource group level. Among the two types of resource group creation, “Criteria-based” groups are highly recommended.

Criteria-based groups are basically dynamic groups. They provide you the flexibility to consolidate resources that satisfy certain criteria into a single group. Once you define the criteria, Password Manager Pro will automatically identify all matching resources and create the group, no manual intervention needed.

6.6 Use nested resource groups and order resources based on department

For ease of use and navigational convenience while retrieving a single resource from a huge database, you can leverage the explorer tree view setting in Password Manager Pro (i.e. create nested resource groups). By default, the tree displayed will be different for each user. Enable this tree view setting to globally display a uniform explorer tree across the organization. After enabling, change the name of the main node from 'Resource Groups' to your organization's name. Under this, create multiple sub-nodes based on the different teams or departments you have. Subsequently, you can designate the resource groups under the sub-nodes of the team or department they belong to.

By manipulating the explorer tree as mentioned above, you can create a clear hierarchy of resource groups that provides easy accessibility. To allow manipulation of the explorer tree, navigate to **Admin >> General Settings >> Password Retrieval, and enable "Allow all admin users to manipulate the entire explorer tree."**

6.7 Additional fields for easy reference and search

While adding resources, additional fields can be used to create custom columns and values. The fields will come in handy for creating criteria-based groups, searching specific resources or passwords, sharing resources, and more. For instance, assume you have three levels of IT administrators in your organization. So if you create an additional resource field titled **"Access Level",** you can easily sort resources under "Level I/II/III". With the **"Access Level"** field as a criterion, you can create three different resource groups. Similarly, you can create three user groups, each containing users belonging to different levels, and then assign "Level I" resources to "Level I" users and so on.

7.0 Password sharing and granular restrictions

7.1 Share passwords with varying access privileges

While sharing resources, password owners can grant different permission levels to users and groups by choosing one of the following privileges:

- **View Passwords:** Users can only access the password.
- **Modify Passwords:** Users can access and modify the shared password.
- **Full Access:** Users have complete management of a resource or group, and can re-share the resource, group, or individual account passwords.

We recommend you provide users only with "View Passwords" permissions as that will be mostly sufficient for various password-related operations. Exercise caution while providing "Full Access" permissions, because a user with "Full Access" permissions over a password is almost a co-owner and will be able to modify, delete, and even reshare the password with more users.

Note: Apart from these sharing privileges, you can also share resources without revealing the passwords in plain-text. This is possible when auto-logon is configured for the resource. To learn more about this feature, refer to section 10.1.

7.2 Use resource group to user group sharing

Though Password Manager Pro has provisions to share a single password or resource with a single user or a group, the best practice approach is sharing a resource group with a user group. This will work best for performing bulk operations efficiently and saving time. For instance, if you need to provide Windows administrators in your organization with access to all Windows resources, you can complete the operation in two simple steps:

- Create a criteria-based resource group (with "Windows" resource type as the matching criterion). That way, all existing Windows resources are added to the group and new resources created in the future will also the automatically added to the group.

- Create a user group for Windows administrators. If you have integrated AD/LDAP, you can import the group directly and enable auto-synchronization of the user database. That way, whenever a new Windows administrator joins the organization, their AD account will automatically be added to Password user group, and the new user will subsequently inherit the group's permissions to view Windows server passwords.

7.3 Make use of access control workflows

Access control in Password Manager Pro is a request-release mechanism that doesn't allow users to access passwords directly. Instead, users have to raise a request to the admin for access approval. The feature also helps you introduce various access restrictions for your resources such as time limited access, concurrency controls, and automated resets after the usage period. So we highly recommended you enable this release control for the credentials of your critical resources.

For better security, you can also configure dual approvals for critical resources, which mandates that two admins approve a request before the passwords are released for a temporary period. This setting comes in handy when an administrative credential is primarily owned by two different departments in your organization. Access controls can be configured by going to **Resources >> Resource Actions >> Configure Access Control.**

7.4 Require users to provide their reason for retrieving passwords

By default, all password-related operations are captured in Password Manager Pro's audit trails, complete with timestamp and IP address details. Optionally, you can require that users input a reason why they need access to a password. These reasons will also be recorded in the audit trails, which can be used for cross-verification and validation in forensic investigations. Therefore, whenever a user tries to retrieve the password of a resource, we

recommend you mandate that they provide a credible reason for requiring access, irrespective of whether or not access controls are configured. This option can be activated under **Admin >> Settings >> General Settings >> Password Retrieval.**

7.5 Integrate Password Manager Pro with enterprise ticketing systems

Password Manager Pro provides the option to integrate a range of ticketing systems to automatically validate service requests related to privileged access.The integration ensures that users can access authorized privileged passwords only with a valid ticket ID. In order to enable a stronger retrieval workflow for your critical resource passwords, we suggest you integrate Password Manager Pro with your enterprise ticketing system. Currently, Password Manager Pro readily integrates with ManageEngine ServiceDesk Plus On-Demand, ServiceDesk Plus MSP, ServiceDesk Plus, ServiceNow and JIRA. You can integrate Password Manager Pro with the aforementioned ticketing systems by navigating to **Admin >> Integration >> Ticketing System Integration.**

8.0 Password policies

8.1 Set separate password policies for critical resource groups

Primarily, password policies help you define password strength by specifying character complexities. Password Manager Pro allows you to customize and configure different password policies for different groups of resources. If you have a handful of resources that are ultra-sensitive in nature, organize them all into a resource group and configure a separate policy with very strict requirements. Policies for resource groups can be configured from **Groups >> Select the specific group(s) >> Bulk Configuration >> Associate Password Policy.**

8.2 Account-level password policies

Normally, each resource is provisioned with one or a few administrative accounts and other normal accounts. To protect these privileged accounts, we recommend you configure a strong password policy separately for sensitive accounts of important resources. Account-level password policies can be configured from **Resources >> Select the specific resource(s) >> Resource Actions** (at the top) **>> Associate Password Policy**

8.3 Define the age for your passwords while creating policies

While configuring a new password policy, always remember to set the maximum password age. Specifying an age lets Password Manager Pro automatically reset the password when the age expires. If you do not fill out the field, the passwords will not expire, which is **NOT** the recommended practice.

9.0 Password resets

9.1 Periodic password randomization

Secure management of privileged accounts requires the use of strong, unique passwords that are periodically reset. Ideally, passwords should be reset at least once every 90 days—the most common timeframe stated by IT regulations such as PCI-DSS. We recommend you configure regular password resets for resource groups in Password Manager Pro using the scheduled password reset feature. More importantly, configure passwords to be automatically reset during the following situations, as well:

- After a user is done using the password and checks it in.
- When share permissions are revoked for user(s) with whom the password was initially shared.
- When passwords expire, as set through password policies.

9.2 Choose the most suitable password reset mode

Password resets can be carried out in one of the two following modes in Password Manager Pro: agentless or agent-based.

For agentless mode, Password Manager Pro directly connects with the target system and changes the password. Administrative credentials have to be supplied to perform password changes. More specifically, to perform password resets for Linux resources from a Windows installation of Password Manager Pro, two accounts are required: one with root privileges and one with normal user privileges that can be used to log in remotely.

On the other hand, agent-based mode comes in handy when you have to reset passwords for resources without direct connectivity, such as those in DMZ locations or with firewall restrictions. To accomplish those password resets, Password Manager Pro deploys an agent to the remote host, which executes the task. All communication between the agent and the application server is one way and over HTTPS, so you don't have to open any firewall ports for in-bound traffic.

Basically, among both modes, the agentless mode is the most convenient and reliable way of changing passwords and we recommend you choose the same whenever resources can be directly reached. However, you have to choose the agent-based mode for the following use cases:

- When administrative credentials are unavailable in Password Manager Pro for a particular resource.
- When services required by Password Manager Pro for reset are not running on the target resource (Telnet/SSH for Linux, RPC for Windows)
- When Password Manager Pro is running on Linux and you need to make password changes to a Windows resource.
- When you have two different environments "A" and "B" with firewalls in between. During such cases, you can install Password Manager Pro in one environment, say A and use agentless mode for the machines in environment A. On the other hand, you can install agents in environment B's machines for password reset. That way, all passwords can be managed in both A and B without adding firewall port exceptions.

9.3 Restart services to achieve a complete management routine

With Password Manager Pro, Windows domain accounts that are used to run various services and IIS application pools can also be subject to periodic password resets, along with subsequent password propagation across all dependent services and application pools. To ensure that services, tasks, and app pools are properly updated with the password change, Password Manager Pro offers an option to automatically restart services after the password is reset, which we recommend.

10.0 Session management

10.1 Allow users to automatically log on to remote systems without revealing passwords in plain text

After you configure auto-logon options to remotely connect to resources, Password Manager Pro allows users to establish a direct connection to the resource with just a single click, eliminating the need to copy and paste passwords. In such cases, we recommend you prevent users from retrieving the passwords in plain text, since it is not required. Plain text retrieval of passwords can be disabled from **Admin >> Settings >> General Settings >> Password Retrieval.**

10.2 Monitor critical sessions in real time

Password Manager Pro offers session shadowing, which can be used to establish dual controls on privileged sessions. Use this feature to monitor remote sessions in real time and supervise user activity. Basically, dual controls are helpful to provide remote assistance and thwart malicious activities. If you are an admin, you can track critical sessions launched from the application by joining active sessions and observing concurrently, without affecting the end user. In case any suspicious activity is detected, you can terminate the session immediately to avoid any misuse of privileged access.

10.3 Regularly purge recorded sessions

By default, Password Manager Pro records all RDP, VNC, SSH, Telnet, and SQL sessions launched from the application. If your organization is large, with a comprehensive range of resources for which session recording is enabled, the recorded sessions will naturally grow at a faster rate. If you do not need recordings that are older than a specified number of days, we recommend you purge them to keep disk space free. You can also store these recordings in the local drive, so they can be moved elsewhere. On the other hand, if you want to delete a selective session or the chat history of a particular session, you can do so by navigating to **Audit >> Recorded Sessions,** and then clicking the **"Delete"** icon beside the selected session. Note that Password Manager Pro mandates the approval of at least two administrators to delete a particular session recording or a chat session.

11.0 Privileged access to third parties

11.1 Manage third party access to corporate systems

Most often, third parties such as contractors, consultants, and vendors require access to corporate IT resources for various contractual duties and other business needs. When you provide privileged access to a third party, we always recommend you provision them **only with temporary access, restricted with time stipulations and minimum necessary privileges**. On top of that, here are a few more suggested practices to follow while sharing critical information with third parties:

- Since contractors connect remotely to your resources, add all your third parties as users in Password Manager Pro and require them to establish direct sessions to target systems only through Password Manager Pro.

- After configuring auto-logon for the resource, the best practice approach is to share the login credentials without displaying the passwords in plain text.

- Also, configure access control workflows for such resources. This helps implement time limits for access to the passwords, including an automatic password reset at the end of the usage period.

- Shadow sessions regularly to detect any trace of malicious behavior and instantly adopt remediation measures.

- When you end a contract with a vendor, immediately execute password resets for all resources that the vendor had access to.

12.0 Data center remote access

12.1 Avoid circulating jump server credentials

Normally, connecting to remote data center resources is a lengthy process, since direct access is restricted from a security prespective. Instead, admins and users must hop through a series of jump servers before ultimately connecting to the target device, authenticating themselves manually at each stage. This process of multiple hops introduces separate credentials for each jump server, which the users require to launch a data center connection. For these cases, circulating all the credentials among users is not a secure practice. Instead, use the landing server configuration feature in Password Manager Pro to enforce your users to connect to data centers only through Password Manager Pro. The application provides secure, one-click automated access to the data center resources, eliminating the need for manual authentication at every hop. It also centralizes the management of jump server credentials.

12.2 Export passwords beforehand to keep them ready for offline access

If a data center environment does not allow internet connectivity, you will not be able to access Password Manager Pro from that network. In that case, export all required passwords as an encrypted HTML file beforehand and access passwords offline. If the export option is enabled, you can download the file from **Resources >> Resource Actions** (at the top) **>> Export Passwords.**

13.0 Auditing and reporting

13.1 Facilitate regular internal audits

Use Password Manager Pro's audit trails to instantly record all events around privileged account operations, user logon attempts, scheduled tasks, and completed tasks. By converting this information into well-presented reports, you can facilitate regular internal audits and forensic investigations, easily discovering who did what with a password, where, and when.

13.2 Keep a tab on select activities with instant alerts

Password Manager Pro also lets you send instant email notifications to chosen recipients when certain events take place. This option is very handy to stay constantly updated on what your users are doing. So we recommend you configure alerts for important operations such as new user addition, password deletion, password shares, and so on. Email alerts at the operational level can be enabled by going to **Audit >> Resource Audit** (for eg.) **>> Audit Actions >> Configure Resource Audit.** Password level alerts can be enabled from **Groups >> Actions >> Configure Notifications.**

13.3 Opt for daily digest emails to avoid inbox clutter

If you have enabled alerts and updates for a number of resources, your inbox may overflow with notification emails. In case this occurs, you can choose to receive a daily digest email at the end of each day with a consolidated list of notifications, if hourly updates are not a priority.

13.4 Configure email templates

By default, Password Manager Pro has specific content for email notifications. We recommend you configure the template to suit your needs and customize your own content. This can be done by going to **Admin >> Customization >> Email Templates.**

13.5 Generate syslog messages and SNMP traps to your management systems

If you use a third-party SIEM tool in your organization, you can integrate Password Manager Pro with the tool. This integration allows you to feed syslog messages to the tool whenever an activity takes place within Password Manager Pro. Optionally, you can also integrate your SNMP manager with the application and generate SNMP traps. This will help you acquire a holistic view of privileged access, along with overall network activity, from a central location.

13.6 Schedule periodic report generation

Password Manager Pro offers a variety of premade reports that provide information on password inventory, expiration status, user access frequencies, user activity, and more. Instead of generating these reports manually, we recommend you use the **Schedule Report** feature for the required reports to save time. Once scheduled, reports will automatically be generated during the specified interval and sent to your registered email.

13.7 Purge audit records

Naturally, when each and every operation is audited, the audit records grow at a faster rate. If you do not need audit records older than a specified number of days, you can purge them. This can be configured by navigating to **Audit >> User Audit** (for eg.) **>> Audit Actions >> Configure User Audit.** By default, the purge option will be disabled with the days set to zero (0).

14.0 Data redundancy and recovery

14.1 Set up disaster recovery

Data stored in Password Manager Pro's database is of critical importance. In the unlikely event of a production setup glitch, all data could be lost. So, disaster recovery is essential. The application provides provisions for both live data backup and automated periodic backups through scheduled tasks. Choose the method that suits your organization best. Also, ensure that the configured destination directory for the backup is in a secure remote location.

14.2 Deploy a secondary server with a high-availability architecture

High-availability architecture in Password Manager Pro is a recommended setup that helps you tackle downtime and assure continued access to passwords. This is achieved by installing another instance of Password Manager Pro on a secondary server, in addition to the primary application server. If you have different networks within your workplace (separate networks for each floor, for instance), we recommend you install primary and secondary application servers in different networks.

On the other hand, if you have offices in two different geographical locations, the best practice for a high-availability setup is to configure Password Manager Pro's primary server in your headquarters and deploy a secondary server in the other office. This way, employees in both locations will enjoy uninterrupted access to passwords in the event of server down-time. To set up high availability, go to **Admin >> Configuration >> High Availability,** and configure a standby server for Password Manager Pro.

15.0 Maintenance

15.1 Keep your installation updated

The team at Password Manager Pro constantly releases upgrade packs containing enhancements and fixes. Ideally, major upgrades are released once a quarter, while minor upgrades may be announced once every month or two. These upgrade packs will also contain updates for the Tomcat webserver, PostGresSQL database, and JRE that come bundled with the product. To keep your Password Manager Pro installation properly maintained for optimum performance, we recommend you download and apply upgrade packs for Password Manager Pro as and when they are released. Upgrade packs can be downloaded here.

Updating the Windows OS where Password Manager Pro is installed: When you have Windows patches to install in the Password Manager Pro server, follow the following steps:

1. Open Services console (services.msc) and stop Password Manager Pro service.
2. Take a copy of entire Password Manager Pro directory and store in any other machine as backup. Or if the server is a VM, just take a snapshot.
3. Now, update Windows OS.

15.2 Choose your maintenance window wisely

In order to apply upgrade packs, Password Manager Pro has to be temporarily stopped. If high availability is configured, both primary and secondary servers will be down. Moreover, the current design of Password Manager Pro requires high availability to be re-configured after every upgrade. Therefore, we highly recommend you schedule the maintenance window during weekends or non-business hours.

If you cannot avoid carrying out an upgrade during work hours, you can alert your users prior to the upcoming maintenance operation with Password Manager Pro's **Message Board.** The **Message Board** option can be found under **Admin >> Manage.** You can send the message that you type as an email or an online alert to all users.

15.3 Update your mobile apps and browser extensions periodically

Updates for Password Manager Pro's native mobile apps and browser plug-ins are released on a regular basis. We recommend you check for updates in the app and browser stores periodically .

15.4 Look for security advisories

If any security vulnerabilities are discovered in the product, fixes are immediately provided through upgrade packs. A security advisory is also sent to the customer email that you have registered with us. Keep an eye on that email to ensure you don't miss any advisories from us. Whenever you receive one, act as advised in the email.

15.5 Moving the Password Manager Pro installation from one machine to another

To move the Password Manager Pro installation from one machine to another, follow the procedure detailed below:

- Quit Password Manager Pro, if it's running.
- Simply copy the entire Password Manager Pro installation folder from one machine to another.
- Then, install it to run as service. In this option, you will not be able to uninstall the program through Windows or add or remove the programs console. If you want to re-install anytime, just delete the entire installation folder.

Caution: Do not remove the existing installation of Password Manager Pro until you've ensured the new installation works fine. This ensures you'll have a valid backup ready, in case you need to overcome disasters or data corruption during the move.

16.0 Emergency access provisions

16.1 Use a local Password Manager Pro account for emergency purposes

In the rare event that your Active Directory servers go down, users may be locked out. To deal with this, we recommend you have a local account in Password Manager Pro.

16.2 Export passwords as an encrypted HTML file for offline access

Usually, in controlled environments such as data centers, internet connectivity is not allowed on other devices. To ensure access to passwords in such places, Password Manager Pro provides offline access. This feature allows you to export all your passwords as an encrypted HTML file periodically, as desired, and store the file in a secure location. The file will be encrypted with a 16-digit passphrase provided by you. Only users who know the passphrase can unlock the offline file. You can also configure automatic logout for the file by specifying a time interval (for example, 15 minutes). These settings can be configured by navigating to **Admin >> Settings >> Export / Offline Access.** Apart from on-demand exports, you can also schedule export operations for the passwords of your resource groups by navigating to **Groups,** and selecting **Periodic Password Export** from the drop down menu under **Actions.** You can schedule the exports on a daily, weekly or monthly basis.

17.0 When an administrator leaves

There may come a time when one of your administrators leaves the organization. If this happens, make sure to do the following:

17.1 Prepare exit report

When an administrator leaves the organization, you need to first determine their privilege levels in the company and assess the associated vulnerabilities. This practice is critical, since they possess unrestricted access to your IT assets. In these cases, we recommend you generate a custom report in Password Manager Pro containing the complete list of passwords that the specific user had access to. To generate user-specific custom reports, navigate to **Users,** select specific user and then click on **'User Report'** icon under **Reports** column.

17.2 Transfer ownership of resources

After acquiring the list of resources created by the leaving administrator, transfer the ownership of all those resources to yourself or another administrator in Password Manager Pro. You cannot delete the administrator's account in the application until you do this. Transferring ownership of resources can be done by navigating to **Users,** selecting the leaving administrator, and then choosing **Transfer Ownership** from the drop down menu under **User Actions.**

17.3 Transfer approver privileges

If you have access controls configured, the leaving administrator may have been an approver for certain resource (i.e., they might have handled password access requests from other users in Password Manager Pro). We recommend you transfer their approver privileges to another administrator when they leave. Approver privileges can be transferred by clicking **Users,** selecting the leaving administrator, and clicking on **Transfer Approver Privileges** from the drop down menu under **User Actions.**

17.4 Reset passwords instantly

To rule out security breaches or unauthorized access attempts in the future, we highly recommend you reset the passwords of all the resources owned by the leaving administrator immediately after the ownership for those resources has been transferred to another user with admin-level permissions.

18.0 Security

18.1 Always choose SSL in all communications

Password Manager Pro offers both SSL and non-SSL modes for sensitive operations including password reset and resource addition or import. For obvious security advantages, we recommend you always opt for SSL communication.

18.2 Prudently execute scripts and prevent malicious inputs

By default, Password Manager Pro will be configured to identify harmful scripts or codes and prevent their execution. In addition, it also prohibits running scripts that contain HTML tags and attributes. Do not disable this option since it is a highly recommended best practice to enhance security. If you need to run a genuine script, temporarily disable this option and enable it immediately after completing the task.

18.3 Configure inactivity timeout

Allowing web-interface sessions to remain alive when users leave their workstations unattended is hazardous from a security point of view. By default, Password Manager Pro's web session auto-logout will be set to 30 minutes. We recommend you set it to 15 minutes or even fewer, just to be safe. To configure an inactivity timeout, navigate to **Admin >> Settings >> General Settings >>User Management.**

18.4 Configure auto-logout for browser extensions

You can choose how long your browser extension session should remain active. For maximum security, we recommend you set up automatic logout after a period of 15-30 minutes. Logout periods can be configured under **Settings** in the browser extension.

18.5 Offline access: Disable passwords export

Password Manager Pro provides multiple export options for secure offline access, such as plain text spreadsheet files and encrypted HTML files. We always recommend you allow users to export passwords only as encrypted HTML files. In case you've allowed users to export password information in CSV files, disable passwords from being exported as plain text. This can be done by navigating to **Admin >> Settings >> Export / Offline Access.**

18.6 Restrict API calls and Agent access by black or white listing IP addresses

Password Manager Pro allows you to enable IP based restrictions for API calls, communication from native mobile apps and browser extensions as well as agent communication from target machines to Password Manager Pro server. We recommend you restrict and provision only a limited number of client systems with access to Password Manager Pro. To configure IP based restrictions, navigate to **Admin >> Configuration >> IP Restrictions >> API Access** (or) **Agent Access.** The IP restrictions can be set at various levels and combinations, such as defined IP ranges or individual IP addresses.

19.0 Privacy

19.1 Privacy controls

To enhance privacy within the product, Password Manager Pro helps you customize and control the inclusion of personal data in canned reports' generation processes. You can decide whether each personal data input in Password Manager Pro should go as masked entries in the reports or be completely removed from them by navigating to **Admin >> Settings >> Privacy Settings >> Privacy Controls.** We recommend you to mask or remove highly confidential data while generating reports.

19.2 Encrypted exports

In order to have an additional layer of security for all the export operations across Password Manager Pro, we suggest you enable encryption of exported files by navigating to **Admin >> Settings >> Privacy Settings >> Encrypted Exports.** You can either set a global passphrase which will be uniformly used for all the export operations or allow users to define their own passphrase for their exported files. Users will then need to provide the passphrase for viewing the exported file.