ManageEngine Password Manager Pro

BEST PRACTICES GUIDE

ZOHO Corp

Password Manager Pro - Best Practices Guide

1.0 Overview

This document describes the best practices in setting up and using Password Manager Pro in an enterprise network environment. It is intended to offer guidance to IT administrators when they set up the software for use in their production environment. Best practices during all stages - product installation, configuration, setup and deployment have been explained with special focus on data security.

2.0 Installation

2.1 System Configuration

Before installing PMP, you need to decide on the configuration of the system where you would install PMP. The following table provides information on the **minimum** hardware and software configuration required by PMP.

Minimum Requirements

Hardware	Operating systems	Web-Client & Database
Processor • 1.8 GHz Pentium processor **RAM** • 1 GB **Hard Disk** • 200 MB for product • 10 GB for database	**Windows** • Windows 2000 Server / Professional • Windows Server 2003 • Windows XP Professional • Windows Vista • Windows Server 2008 • Windows Server 2008 R2 **Linux** • Red Hat Linux 8.0 • Red Hat Linux 9.0 • CentOS 4.4 • Suse Linux 10.1 • Mandrake Linux 10.0 **Note:** Password Manager Pro can be run on VMs of the above operating systems	HTML client requires one of the following browsers** to be installed in the system: • IE 7 and above (on Windows) • Firefox 2.0 and above (on Windows and Linux) ** PMP is optimized for 1024 x 768 resolution and above. **Database** • MySQL 5.1.50, bundled with the product. • Supports MS SQL Server 2005 and above also. SQL server should be installed in Windows 2003 Server and above.

2.2 Recommended Configuration for Better Performance, Scalability & Security

For better performance and security, it is recommended to install PMP in a **dedicated, hardened, high-end server**. Also, the performance of PMP depends a lot on the following factors:

- Number of Users & User Groups
- Number of Resources & Resource Groups
- Number of Resources/Passwords Shared
- Number of Scheduled Tasks

Though PMP will very well run in the systems having the minimum configuration, you may have to choose a higher configuration if the above factors weigh high at your end.

We can roughly say that if the above factors are very high of the order of hundreds of users and user groups with a few thousands of resources and resource groups and shares, you may choose a high-end configuration as below:

- Single / Dual processor
- 4 GB RAM
- 40 GB hard disk space

2.3 Installing PMP in Windows Vs Linux

PMP can be installed in Windows and Linux. Though PMP will run equally fine in both the platforms, installation in Windows has some inherent advantages.

- Active Directory Synchronization (for resource & user import) can be leveraged only in Windows installation
- Single Sign-on (users who have logged into the Windows system using their domain account need not separately sign in to PMP) is possible only in Windows installation
- If you have installed PMP in Linux, agentless mode of password reset cannot be leveraged for Windows resources. You will have to use agent mode for resetting the passwords of Windows resources. Same is the case with Windows domain account password reset, Service Account and Scheduled Task password reset and Password reset for Services & Scheduled Tasks which are using local accounts

2.4 Using MS SQL Server as Backend Database

- SQL Server encrypts data with a hierarchical encryption and key management infrastructure. Each layer encrypts the layer below it by using a combination of certificates and symmetric keys. One among them is the Database Master Key, which in turn is created by Service Master Key and a password. This password is stored in PMP under **<Password Manager Pro Installation Folder>/conf** directory in a file named **master_key.key**. It is not secure to leave this file here, unless the server is sufficiently hardened to protect any illegal access of this file. It

is highly recommended to move this file out of its default location. **Take care to keep this key safe.** You will require it while performing High Availability and Disaster Recovery. If you lose this key, you will have to configure MS SQL server setup all over again. For more details, refer to the following section of our help documentation.

- Since PMP connects to MSSQL only in SSL mode, it is recommended that you create a dedicated database instance running in a specific port for PMP.
- **Rename 'sa' account:** Renaming the 'sa' account is a good security measure to be adopted on SQL Servers running in mixed authentication mode
- Remove all sample databases
- Use Windows Authentication logins instead of SQL Server logins
- If you are not using High Availability
    - Create a service account and map it to **dbcreator** role
- If you are using High Availability
    - Create a service account and map it to **sysadmin** role
- To ensure high level of security, PMP has been configured to connect to SQL server only through SSL. So, SSL encryption should be enabled in SQL server. PMP will start only if SSL connection is enabled
- ForceEncryption option should be enabled for the clients to connect to this SQL instance. When this is done, all client/server communication will be encrypted and clients that cannot support encryption will be denied access
- Disable all protocols other than TCP/IP in SQL server
- Hide this SQL instance to prevent it from being enumerated by other tools
- If the SQL Server resides in a different server than PMP installation, enable firewall rule in such a way that the IP **<SQL-Instance>:Port** is accessible only from the PMP Server
- If you have chosen to use a different database for PMP other than the default database created by PMP, make sure the service account used is the dbowner of the database
- Ensure that the users other than those with the role 'sa' and 'sysadmin' are not able to access the PMP database though they could have physical access to the database
- It is quite possible for the 'sa' accounts and "sysadmin" privileged users to access the PMP database and access the passwords present there. So, take necessary precautions
- By default, symmetric key is created using AES 256 algorithm during PMP Installation. You can also create your own symmetric key, which PMP can use for encryption
- Certain user defined functions and stored procedures are installed in the PMP database during installation. Those user defined functions and stored procedures are in encryption format, which can be run by the dbowner and sa/sysadmin privileged accounts.

3.0 Key Settings after Installation

3.1 Secure the Installation Master Key (MySQL)

PMP uses AES-256 encryption to secure the passwords and other sensitive information in the password database. The key used for encryption is auto-generated and is unique for every installation. By default, this encryption key is stored in a file named **pmp_key.key** under

<PMP_HOME>/conf folder. For production instances, PMP does not allow the encryption key to be stored within its installation folder. This is done to ensure that the encryption key and the encrypted data, in both live and backed-up database, do not reside together.

We strongly recommend that you move and store this encryption key outside of the machine in which PMP is installed - in another machine or an external drive. You can supply the full path of the folder where you want to move the **pmp_key.key** file and manually move the file to that location and delete any reference within PMP server installation folder. The path can be a mapped network drive or external USB (hard drive / thumb drive) device.

PMP will store the location of the **pmp_key.key** in a configuration file named **manage_key.conf** present under **<PMP_HOME>/conf** folder. You can also edit that file directly to change the key file location. After configuring the folder location, move the pmp_key.key file to that location and ensure the file or the key value is not stored anywhere within the PMP installation folder. PMP requires the **pmp_key.key** folder 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.

Important Note: You need to take care of sufficiently protecting the key with layers of encryption (like using Windows File Encryption for example) and access control. Only the PMP application needs access to this key, so make sure no other software, script or person has access to this key under any circumstance. You also need to take care of securely backing up the pmp_key.key file yourself. You can recover from PMP backups only if you supply this key. If you misplace the key or lose it, PMP will not start.

3.2 Take Control of Database Key (MySQL)

Apart from the AES encryption, the PMP database is secured through a separate key, which is auto - generated and unique for every installation. The key for the database can be stored securely in the PMP itself. There is also option to store it at some other secure location accessible to the PMP server.

It is better to store the database key outside PMP. For more details, refer to the following section of our help documentation.

4.0 Integration

4.1 Integration with Directory Services/Identity Stores

Password Manager Pro can be integrated with third party identity stores such as Active Directory / LDAP. If you have AD or LDAP in place, it is recommended to integrate them with PMP. You can import users from AD / LDAP and also leverage their authentication mechanism. Users get the advantage of logging into PMP using the AD / Credentials. Additionally, PMP user database can be synchronized with AD / LDAP database at specified, periodic intervals.

5.0 User Management

5.1 Use Local PMP Accounts for 'Fire-Call' Purposes Only

By default, PMP allows local authentication along with AD or LDAP authentication. The best practice approach is to use local PMP account only for 'fire call' purposes and all other user accounts should be from a directory service to leverage good user management practices.

5.2 Decide about Email notification on user creation

By default, whenever a new user account is added in PMP, an email is triggered to the respective user with information about the login password in the case of new user addition. When you integrate AD/LDAP, decide beforehand if you wish PMP to send email notification. Particularly, when you are evaluating the product, it is recommended that you disable email notification. It can be done from General Settings option.

5.3 Create User Groups

Organize the PMP users into groups - for example, Windows Administrators, Linux Administrators and so on. The grouping of users will immensely help in sharing resources. In case, you have integrated AD/LDAP, you can automatically have the same hierarchical structure in PMP just as in AD/LDAP, including the user groups.

5.4 Assign User Roles Properly

After adding users, assign proper roles to them - Administrator, Password Administrator, Password Auditor or Password User. Also, decide if your organization requires any administrator or password administrator to act as a '**Super Administrator**', who will have the privilege to view all the passwords in the system.

5.5 Use Two Factor Authentication

To access the PMP web-interface, there is provision to enforce users to authenticate through two successive stages. While the first authentication is through the usual native authentication or AD / LDAP, the second level of authentication could be either through a one-time, randomly generated unique password sent by PMP to the user by Email or by leveraging RSA SecurID authentication as the second level of authentication. From security standpoint, it is recommended to make use of the Two Factor Authentication.

5.6 Remove the Default 'admin' Account

For security reasons, it is highly recommended that the default 'admin' account of PMP be removed once you add another user with 'administrator' role.

6.0 Data Population & Organization

6.1 Prepare Inventory of Administrative Accounts

The first step prior to actual Password Management using Password Manager Pro is identifying all the administrative accounts in your organization. This can be done by first preparing the inventory of all servers, databases, network devices and other sensitive applications. If you are using other ManageEngine products such as Asset Explorer, OpManager, DeviceExpert etc, you can easily build an inventory of your resources. You can export the inventory as a CSV and then import them in PMP.

In addition, each resource might contain more than one administrative account. You need to identify all such accounts. These are the accounts that are to be managed by PMP.

6.2 Leverage the Power of Resource Groups

After adding resources, organize your resources into resource groups. Resource Groups are quite powerful in PMP. Most of the enterprise-class password management operations in PMP can be performed only at resource group level. Among the two types of resource group creation, "Criteria-based" resource groups are highly recommended.

Criteria-based groups act as dynamic groups providing the flexibility to automatically make a resource, which satisfies certain criteria to become part of specific groups, without any manual intervention. For example, if you create a criteria-based resource group based on the condition "Resource Type Contains Windows", all Windows resources could be made part of the Windows group automatically after resource addition.

Apart from the dynamic nature, the criteria-based resource groups allow you to create resource groups matching any required criteria - like department, location, type, name and even based on custom criteria. You can make use of a combination of criteria too. For example, you can create a group of resources belonging to type 'Linux' and location 'Second Floor' of the building.

Moreover, if you have thousands of resources in your environment, picking resources individually to make them a resource group, would be a laborious task. So, making use of the criteria-based resource group is the best practice approach.

6.3 'Resource Group - User Group' Sharing: The Best Approach

Though PMP has provision for sharing a single password or a single resource, the best practice approach here is sharing a resource group with a user group. This will come in handy when performing several bulk operations. For instance, assume there is a user group named "Windows Administrators" and there is a resource group named "Windows Servers" and all Windows Administrators should have access to all the Windows Resources.

In this case, the best practice approach is:

- creating a criteria-based resource group (matching all resources of type "Windows") so that if you add a new "Windows Server", it will automatically become a part of the group
- sharing this criteria group to the "Windows Administrators" user group
- if a new Windows Administrator joins the organization and gets an account in the AD/LDAP, the user will be automatically added to PMP; that too directly to the corresponding user group (if you have integrated AD/LDAP)
- the user will automatically inherit the permissions of the group to view the passwords of Windows servers

Another example to bring out the benefit of Resource Group – User Group Sharing:

Consider that you have integrated Active Directory and you want to manage the passwords of the Windows resources belonging to a certain OU. Also, assume that you have an IT administrator group, which is also part of that OU. In this case, you can import the resources from the domain and create a criteria-based resource group.

Similarly, you may import the users from the domain belonging to the OU and create that as a user group. In both the cases above, you can specify certain synchronization interval to keep the resources / users in PMP in sync with the ones in the Active Directory. You can then share the resource group with the user group. Once you do this, if any new resource/user is added to the OU, they will be automatically imported to PMP with the same share permissions.

6.4 Additional Fields for Easy Reference & Search

Make use of the "**Additional Field**" creation feature to create customized columns at resource and accounts view. The additional fields will come in handy in creating criteria-based groups, searching specific resources or passwords and in sharing the resources etc.

Assume the scenario that you have three levels of IT administrators in your organization. While creating resources, if you have an additional field specifying the level to which that particular resource belongs, it will be very convenient to share those resources to the respective level of users.

That is, you will have an additional field titled "Access Level" for resources. Each resource will then have a level associated - Level I / Level II / Level III. You can then create a criteria-based resource group based on the level. Similarly, you can create three levels of user groups - all users belonging to Level I as a group and so on. You can then assign 'Level I' resources to 'Level I' users.

6.5 Make Use of Access Control Workflow

If you have stored certain sensitive passwords, it is strongly recommended to enable 'Access Control Workflow' for that particular resource. When access control is enabled, users will have to go through a request-release flow for password access. It also helps in granting time-limited, exclusive privilege to passwords to select users.

6.6 Force Users to Provide Reason while Retrieving the Passwords

By default, when a user tries to retrieve the password of a resource, on clicking the asterisks, the passwords appear in plain text. It is better to force the users to provide a reason why access to the password is needed. You can achieve this through an option in General Settings.

6.7 Agentless Mode for Password Reset

One of the basic doubts that arise in the minds of PMP users is whether to use agentless mode or agent mode for password reset. Before recommending an option, let us first look at the requisites for both the modes:

The **agent mode** requires the agent to be installed as a service and run with administrative privileges to perform password changes. The agent could be used in target machines, which will communicate with the PMP server and effect password changes. All password related communication is over HTTPS and is secure. The communication is always one way - that is, the agent alone will contact the server. The PMP server will not communicate with the agent. So, there is no need to keep any port open in the host where the agent has been installed.

For the **agentless mode**, you must supply administrative credentials to perform the password changes. For Linux you must specify two accounts, one with root privileges and one with normal user privileges that can be used to login from remote. Telnet or SSH service must be running on the resources. For Windows domain, you must supply the domain administrator credentials. For Windows and Windows domain, PMP uses remote calls and relevant ports must be open on the resource.

Based on this you can choose which mode you want for your environment, indicated by the following tips:

Choose agent mode when,

- you do not have administrative credentials stored for a particular resource in PMP
- you do not have the required services running on the resource (Telnet / SSH for Linux, RPC for Windows)
- you run PMP in Linux and want to make password changes to a Windows resource

Choose agentless mode in all other cases as it is a more convenient and reliable way of doing password changes.

6.8 Do Not Perform Password Resets Across Untrusted Domains

By design, PMP is capable of resetting even foreign domain passwords without a trust. It is **strictly NOT** recommended to perform password resets across untrusted domains, as the setup could be exploited for malpractices.

6.9 Keep Tab on Activities Using Password Action Notification

PMP offers provision to send email notifications upon certain password events like a password access or modification or changing the share permission or when the password expires or when password policy is violated. Enabling 'Password Action Notification' helps achieve this.

6.10 Randomize Passwords Periodically

Foremost among the 'Password Management Best Practices' is to periodically reset the administrative passwords. PMP provides option to automatically reset the passwords at pre-determined intervals. Making use of the 'Scheduled Password Reset' feature you can achieve this.

7.0 Performance & Maintenance

7.1 MySQL Tuning

PMP comes with an inbuilt MYSQL database, in which passwords and other sensitive information are stored in encrypted form. You can carry out the following MySQL tuning procedure to enhance the performance of PMP.

- Stop PMP server, if running
- Go to **PMP_HOME\bin** folder and open **startDB.bat** (in Windows) or **startDB.sh** (in Linux) in an editor
- Search for the line starting with **@start "MySQL" /B** (Windows) and **$DB_HOME/bin/mysqld** (Linux) as shown below

Windows (startDB.bat)

```
@start "MySQL" /B "%DB_HOME%\bin\mysqld-nt" --no-defaults --standalone  --
default-character-set=utf8  --basedir="%DB_HOME%" --port=%DB_PORT% --
datadir="%DB_HOME%\data" --tmpdir="%DB_HOME%\tmp" --user=root --server-
id=%TSTAMP1% --log-bin=mysql-bin --log-slave-updates --master-connect-
retry=30 --slave-net-timeout=30 --expire_logs_days=7 --log-slave-updates --
log-slave-updates  --max_allowed_packet=32000000000 --
max_binlog_cache_size=4294967295 --binlog-do-db=passtrix  --
binlog_cache_size=32768 --max_binlog_size=52428800 --max_relay_log_size=0 --
relay_log_purge=1 --ssl-ca=..\conf\CAcert.pem --ssl-
cert=..\conf\ServerCer.cer --ssl-key=..\conf\ServerKey.key
```

Linux (startDB.sh)

```
$DB_HOME/bin/mysqld --no-defaults --default-character-set=utf8 --
basedir=$DB_HOME --tmpdir=$TMP_HOME --port=$DB_PORT --
socket=$TMP_HOME/mysql.sock --user=root --server-id=$ID --log-bin=mysql-bin -
-log-slave-updates --master-connect-retry=30 --slave-net-timeout=30 --
expire_logs_days=7 --log-slave-updates --log-slave-updates --
max_allowed_packet=32000000000 --max_binlog_cache_size=4294967295 --binlog-
do-db=PassTrix --binlog_cache_size=32768 --max_binlog_size=52428800 --
max_relay_log_size=0 --relay_log_purge=1 --ssl-ca=$PWD/../conf/CAcert.pem --
ssl-cert=$PWD/../conf/ServerCer.cer --ssl-key=$PWD/../conf/ServerKey.key --
log=mysql.log 2&gt;&gt;$TMP_HOME/mysql.out 1&gt;&gt;$TMP_HOME/mysql.out
```

Two parameters - ***key buffer size*** and ***innodb buffer pool size*** are to be tuned to make sure it makes the most of the dedicated RAM.

If the parameters are already present in the above line, just change the values as shown below. If they are not present, just add the parameters after the entry `max_binlog_cache_size` entry

For 1 GB RAM, you can try values

-- innodb_buffer_pool_size=350000000

(or)

-- innodb_buffer_pool_size=400000000

For 3 GB RAM, you can try values

-- key_buffer_size=200000000
-- innodb_buffer_pool_size=950000000

- Stop and start the PMP server and see if there is any difference in performance

Important Note:

(1) In the above lines, any of the existing parameters should not be removed
(2) Similarly, other than the suggested changes, no other new parameter be introduced

7.2 Purge Audit Records

All operations performed in PMP are comprehensively audited and the trails are stored in the database. Naturally, the audit records grow at a faster rate. If you do not need the audit records that are older than a specified number of days, you can purge them. However, if regulatory compliance requirements demand retention of the audit records for longer period of time, you may have to retain the trails.

7.3 Configure Email Templates

Password Manager Pro facilitates sending email notifications on the occurrence of various password actions. By default, PMP has a specific content for the email notification. It is recommended that you configure the template to suit your needs and have your own content.

7.4 Setup Disaster Recovery

Data stored in PMP database are of critical importance. In the unlikely event of something going wrong with the production setup, all passwords would be lost. Disaster recovery provision is highly essential. PMP provides two options - live backup and scheduled backup. Choose any convenient method and backup your data. You can always rely on the backup data.

7.5 Moving PMP Installation from one Machine to Another

If you want to move the PMP installed in one machine to another, follow the procedure detailed below:

Caution

Do not remove existing installation of PMP until the new installation works fine. This is to ensure having a valid backup setup to overcome disasters/data corruption during the movement.

Procedure

- Stop PMP server / service, if running
- Simply copy the entire PMP 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 Add/Remove programs console. If you want to uninstall anytime, just delete the entire installation folder.

8.0 Security

8.1 Always Choose SSL in all Communication

PMP offers both SSL mode and non-SSL mode for sensitive operations like password reset, resource addition/import etc. For obvious security advantages, it is recommended that you use SSL communication is used always.

8.2 Restrict plain-text password access for password users and auditors when auto logon is configured

Through the auto logon feature, PMP provides the option to establish direct connection to the resource eliminating the need for copy-paste of passwords. By default, password users and auditors will be able to retrieve the passwords that are shared with them. If auto logon is configured, they might not need access to the passwords. In such cases, it is recommended to restrict access to passwords through an option in General Settings.

8.3 Configure Inactivity Timeout

As PMP users are dealing with sensitive passwords, from the information security point of view, it would be hazardous to allow the web-interface session to remain alive if users leave their workstation unattended. Inactivity timeout could be configured by specifying the time limit in minutes through an option in General Settings.

8.4 Mask Passwords when Exporting Resources to CSV

When you export PMP resources to a CSV file, by default, password of the accounts are included in plain text. From security standpoint, it is better to mask the password in the report. You can achieve this through an option in General Settings.

8.5 Make Use of Auto-Reset Provisions

PMP provides options to carry out automatic password resets upon the completion of various activities such as changing password shares, password expiry, policy violation and when the password stored in PMP is not in sync with the one in the actual resource. From security standpoint, it is recommended that you make use of all the auto password reset options.

8.6 Audit Filters for Fine-Grained Tracking

PMP has provision for granular recording of audit events and also to send notifications on the occurrence of each event. From security standpoint, it is highly recommended that you register for specific events or to the daily notification digest to achieve granular tracking of events.

8.7 Carry Out User Deprovisioning Promptly

When an administrator leaves the organization, it is important that the passwords owned by the administrator are transferred to some other administrator. Otherwise, system lockout issues will occur. Also, it is quite possible that the administrator might have copied some / all the passwords. To rule out security breaches, it is recommended to reset all the passwords owned by the outgoing administrator before transferring the ownership.