Table of Contents

Getting Started

Introduction

Contents

Overview

In this age of IT revolution, most business applications deal with sensitive intellectual property and strategic information that are critical to the success and even survival of the enterprise. User access control systems are in place almost everywhere to protect the intellectual property.

Over a period of time at work, even a normal user acquires an amazing number of user accounts. Still more complex is the work of Network Administrators and System Administrators who deal with hundreds of passwords at various levels. Consequently, it becomes a daunting task for anyone to keep track of all the passwords. Users tend to store the user name and password information somewhere in their system locally or in a central location when multiple administrators need to use the information.

As System and Network Administrators mostly deal with sensitive administrative passwords, also known as privileged passwords, which provide complete access to all sensitive applications and data, any mismanagement of such passwords would result in a huge security risk exposing the applications to misuse and attacks by identity thieves.

The way out is the use of a secure password management solution that enables secure storage of administrative passwords offering the flexibility to share them among multiple users based on fine-grained user authorization.

Password Manager Pro - where passwords reside in safe custody

ManageEngine Password Manager Pro (PMP) is a Password Management Solution for Enterprises to manage the administrative/privileged passwords. It serves as a centralized repository for storing user names and passwords of any 'network resource' such as a network device, a desktop server, an application et al.

PMP serves not just as a secure password repository, but offers a complete Password Management solution. Using PMP, one can store all passwords in encrypted form in the database and achieve role-based access control for users. That is, administrators can centrally create users, assign them with specific roles and define access levels. Only authorized users will get access to view, edit or manage the permitted 'resources' (the resources assigned to them) based on their role. Thus, PMP facilitates encrypted storage and secure sharing of passwords in enterprises where multiple users will have access to multiple resources. The user account information and passwords can be accessed from a central web interface.

PMP helps in achieving password reset too. Existing passwords of remote resources can be changed from PMP itself and the changed passwords are stored in the repository. The comprehensive auditing mechanism of PMP helps in tracking who changed what and when, thereby ensuring accountability in multi-member environment.

Highlights

- Centralized, administrative password management
- Manage shared administrative passwords
- A-to-A, A-to-DB password management
- Password encryption using AES algorithm
- Provision for importing users from AD, LDAP and leveraging AD/LDAP authentication
- Provision for smart card authentication
- Role-based access control for users
- Password access control workflow
- Super administrator Support
- Remote password reset
- Windows service account reset
- Post password reset script execution
- Privileged Session Management
- Automatically connecting to servers and applications from PMP GUI
- Setting password expiry dates
- Real-time notifications for password events
- Two-factor Authentication for enhanced security
- High availability
- Password generator that helps in generating hard-to-guess passwords
- Password policy definition and enforcement
- Comprehensive audit mechanism recording all user operations for all resources
- Informative reports. Provision for creating custom reports, which helps in meeting regulatory compliance requirements

- Tools for scheduled backup of database and disaster recovery
- Provision for storing the passwords for personal use such as Email account information, Credit Card Numbers, PIN etc.
- Access from anywhere through web browser
- Anytime, anywhere access through mobile app

How secure are your passwords in Password Manager Pro?

Ensuring the secure storage of passwords and offering high defense against intrusion are the mandatory requirements of PMP. The following measures ensure the high level security for the passwords:

- Passwords entered are encrypted using the Advanced Encryption Standard (AES) and stored in the Database. So, hacking of passwords from the database, is highly improbable. AES has been adopted as an encryption standard by the U.S. Government
- Role-based, fine-grained user authentication mechanism ensures that the users are allowed to view the passwords based on the authorization provided
- All transactions through the PMP browser take place through HTTPS

Refer to Security Specifications document for more details.

Documentation Structure

This Help Documentation contains two parts:

- Installation & Getting Started provides information on how to install PMP, how to connect Web Interface and start working with the solution
- Working with Password Manager Pro provides information about the workflow in PMP. The subsequent topics provide information on the arrangement of the various tabs in PMP Web Interface through which various Password Management operations could be performed. This also deals with the pre-requisite browser settings and important terminologies used in the product.

Installation & Getting Started

Contents

Overview

Welcome to ManageEngine Password Manager Pro!

This section provides information on how to install Password Manager Pro (PMP) in your system. This section also deals with the system requirements for PMP, how to install the solution, how to start and shutdown and how to connect web interface after successfully starting the server.

Prerequisite Software

There is no prerequisite software installation required to use PMP. The standard system (hardware and software) requirements as mentioned below plus an external mail server (SMTP server) are essential for the functioning of PMP server and to send various notifications to users.

System Requirements

Following table provides the minimum hardware and software configuration required by PMP:

Hardware

Processor

- 1.8 GHz Pentium® processor

RAM

- 2 GB

Hard Disk

- 200 MB for product
- 10 GB for database

Operating systems

Windows

- Windows 2000 Server / Professional
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows XP Professional
- Windows Vista
- Windows 7
- Windows 8

Linux

- Ubuntu 9.x and above
- CentOS 4.4 & above
- Red Hat Linux 9.0
- Red Hat Enterprise Linux 5.3, 5.4, 5.5
- PMP normally works well with any flavor of Linux

Note: Password Manager Pro can be run on VMs of the above operating systems

Web Interface

HTML client requires one of the following browsers** to be installed in the system:

- IE 7 and above (on Windows)
- Chrome, Firefox, and Safari (on Windows, Linux and Mac)

** PMP is optimized for 1280 x 800 resolution and above.

Database

- PostgreSQL 9.2.4, bundled with the product.
- Supports MySQL and MS SQL Server 2005 and above also. SQL server should be installed in Windows 2003 Server and above.

Components of PMP

PMP consists of the following components:

- The PMP server
- PMP agent that helps in connecting to remote resources
- PostgreSQL 9.2.1 bundled with PMP. It runs as a separate process. It accepts connections only from the host in which it is running and is not visible externally

Installing PMP

In Windows

- Download and execute ManageEngine_PMP.exe
- The installation wizard will guide you through the installation process
- Choose an installation directory - by default, it will be installed in C:/ManageEngine/PMP; Henceforth, this installation directory path shall be referred as "PMP_Home"
- In the final step, you will see two check-boxes - one for viewing ReadMe file and the other one for starting the server immediately after installation; if you choose to start the server immediately, it will get started in the background.
- If you choose to start the server later, after installation, you can start it from the Start >> Programs >> ManageEngine Password Manager Promenu
- From the Start Menu, you can perform other actions such as stopping the server and uninstalling the product

In Linux

- Download ManageEngine_PMP.bin for linux
- Assign executable permission using command chmod a+x <file-name>
- Execute the following command: ./<file_name>
- Follow the instructions as they appear on the screen
- PMP is installed in your machine in the desired location. Henceforth, this installation directory path shall be referred as "PMP_Home".

Starting & Shutting Down PMP

In Windows

Using Start Menu	Using Tray Icon
From Start >> Programs >> Password Manager Pro menu, you can do the following: Start PMP service Stop PMP service Launch Tray Icon View Help Documentation Uninstall the product	Once you installed PMP, in the windows tray area on the far right end of your task bar, you will find the  for PMP. Right click the tray icon and click the desired operation Start PMP Service Stop PMP Service PMP web console

In Linux

Installing as Startup Service	Starting & Stopping the Server as Service
Login as root user Open a console and navigate to<PMP_Home>/bin directory Execute "sh pmp.sh install" (In Ubuntu, execute as "bash pmp.sh install") To uninstall, execute the script "sh pmp.sh remove"	*To Start PMP as a service in Linux* Login as root user Execute /etc/rc.d/init.d/pmp-service start PMP server runs in the background as service *To Stop PMP Server started as service in Linux* Execute /etc/rc.d/init.d/pmp-service stop(as root user)

Connecting Web Interface

Automatic Browser Launch

Once the server is started successfully, a browser is automatically launched with the PMP login screen. As the connection is through HTTPS, you will be prompted to accept security certificate. Hit 'Yes' and then type the user name and password in the login screen and press Enter. For an unconfigured setup, the default user name and password will be admin

and admin respectively. Every time you start the server, the browser will be automatically launched.

Launching the Web Client Manually

In the case of windows, you can also launch the web client manually from the Windows Tray. Right-click the PMP tray icon and click "PMP Web Console". A browser would be launched with the PMP login screen. As the connection is through HTTPS, you will be prompted to accept security certificate. Hit 'Yes' and then type the user name and password in the login screen and press Enter. For an unconfigured setup, the default user name and password will be admin and admin respectively. Every time you start the server, the browser will be automatically launched.

In the case of Linux, open a browser and connect to the URL
https://<hostname>:portnumber/
where hostname - host where Password Manager Pro Server is running; Default port - 7272
Example: https://localhost:7272

Connecting the Web Client in Remote Hosts

If you want to connect web clients in a different machine than the one in which PMP is running, open a browser and connect to the URL

https://<hostname>:port

As the connection is through HTTPS, you will be prompted to accept security certificate. Hit 'Yes' and then type the user name and password in the login screen and press Enter. For an unconfigured setup, the default user name and password will be admin and admin respectively. Every time you start the server, the browser will be automatically launched.

Using MS SQL Server as Backend

(Feature available only in Enterprise Edition)

PMP supports PostgreSQL, MySQL and MSSQL databases as backend. PostgreSQL database is bundled with the product and by default, it is configured to run with PostgreSQL. In case, you wish to use MSSQL databases, follow the steps detailed below:

Important Note

MS SQL server as backend is supported from PMP version 6400 only. Earlier versions do not have provision to run with MS SQL server.

If you are using an earlier version of PMP with MySQL as the backend database, data migration is supported.

Steps to Use MS SQL Server

To ensure high level of security, PMP has been configured to connect to SQL server only through SSL.

Summary of Steps:

1. Create SSL certificate and install it in Windows Certificate Store (where SQL server is running)
   - Get the certificate signed by a third-party CA or use self-signed certificate
2. Import the SSL certificate to PMP
3. Enable SSL Encryption in SQL Server
4. Configure PMP to Connect to SQL Server

Step 1 & 2: Create SSL certificate and install it in Windows Certificate Store (in the machine where SQL server is running)

Prior to trying to connect PMP with SQL server, you need to enable SSL encryption in SQL Server. Here, you may create an SSL Certificate and get it signed by a Certificate Authority (CA) or it could be self-signed.

Option 1:

Generating the certificate and getting it signed by a third-party CA:

You can create the certificate using openssl and it involves two steps - generating private key and generating certificate. Use the following commands to create the certificate.

Generate private key

openssl genrsa -des3 -out server.key 2048

Generate a certificate request

Use the server private key to create a certificate request. Enter the passphrase for the key, Common Name, hostname or IP address, when prompted:

openssl req -new -key server.key -out server.csr

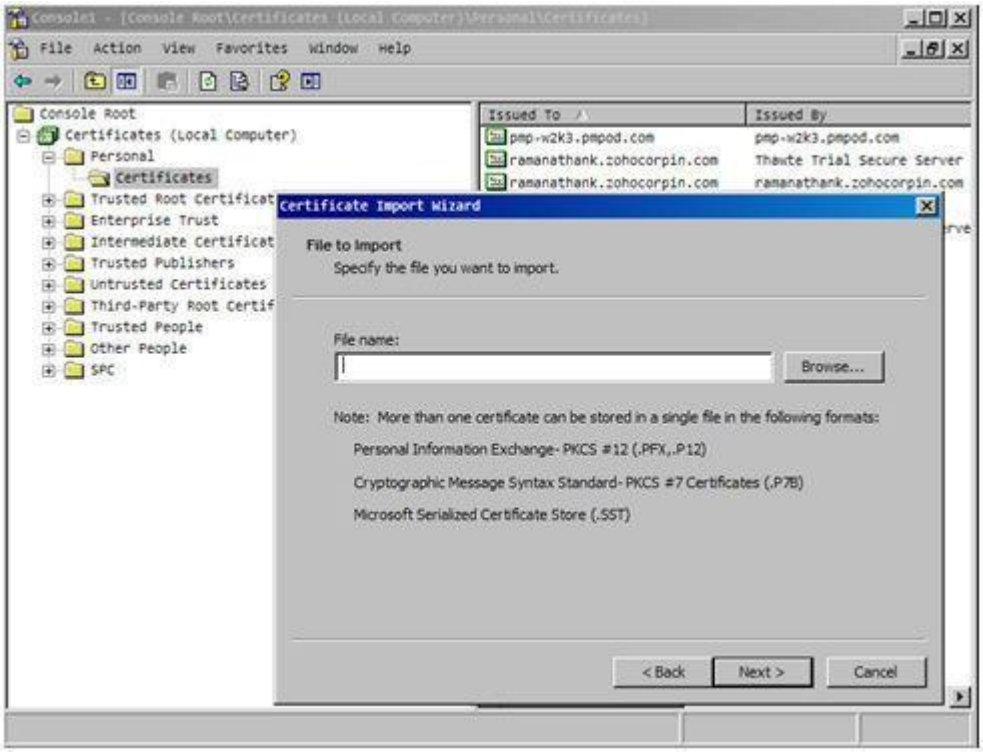
Here, for Common Name, specify the FQDN of the SQL Server.

- After generating the certificate, you need to get it signed by a third-party CA such as VeriSign, Thawte, RapidSSL etc or you may self-sign the certificate. Procedure for both have been explained below. Choose one based on your environment:
- Some of the prominent CAs are Verisign (http://verisign.com), Thawte (http://www.thawte.com), RapidSSL (http://www.rapidssl.com). Check their documentation / website for details on submitting CSRs and this will involve a cost to be paid to the CA
- This process usually takes a few days time and you will be returned your signed server SSL certificate and the CA's root certificate as .cer files

- The server certificate has to be installed in the machine where SQL server is running. The CA root certificate has to be installed in PMP server.

Install the server certificate in the machine where SQL server is running. You may use MMC to do this as shown below

- Open the MMC console by clicking Start >>> Run (in the machine where SQL server is running). In the Run dialog box type: MMC
- On the Console menu, click Add/Remove Snap-in. Click Add and then click Certificates. Click Add again.You will be prompted to open the snap-in for the current user account, the service account, or for the computer account. Select the Computer Account.
- Select Certificates (Local Computer) >> Personal >> Certificates
- Right-click Certificates >> Click All Tasks >> Import
- Browse select the certificate to be installed



Install the CA's root certificate in PMP

- Copy the CA's root certificate and paste it under <Password Manager Pro Installation Folder >/bin directory
- From <Password Manager Pro Installation Folder>/bin directory, execute the following command:
  importCert.bat <name of the root certificate pasted as explained above>

- This adds the certificate to the PMP certificate store.

Option 2:

Creating a self-signed certificate

If you want to create a self-signed certificate and use it, you need to carry out the following steps in the machine where SQL server is installed:

Create a self signed certificate using the certificate creation tool makecert.exe and install it in the machine where SQL Server is running

- Execute the following command from the machine where SQL server is installed

  makecert.exe -r -pe -n "CN=pmptestlab.manageengine.com" -b 01/01/2011 -e 01/01/2036 -eku 1.3.6.1.5.5.7.3.1 -ss my -sr localMachine -sky exchange pmptestlab.manageengine.com.cer

  Here, for CN, enter the FQDN of the SQL server replacing the example entry pmptestlab.manageengine.com.

- The above command will install a self signed certificate in your local store. It will also store the certificate in the file pmptestlab.manageengine.com.cer

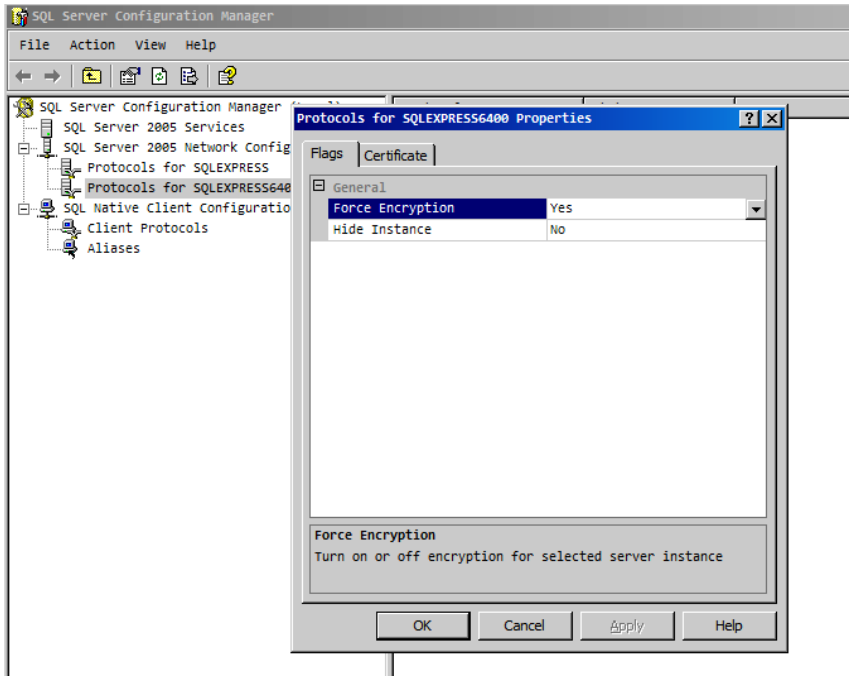
Install the server certificate in PMP

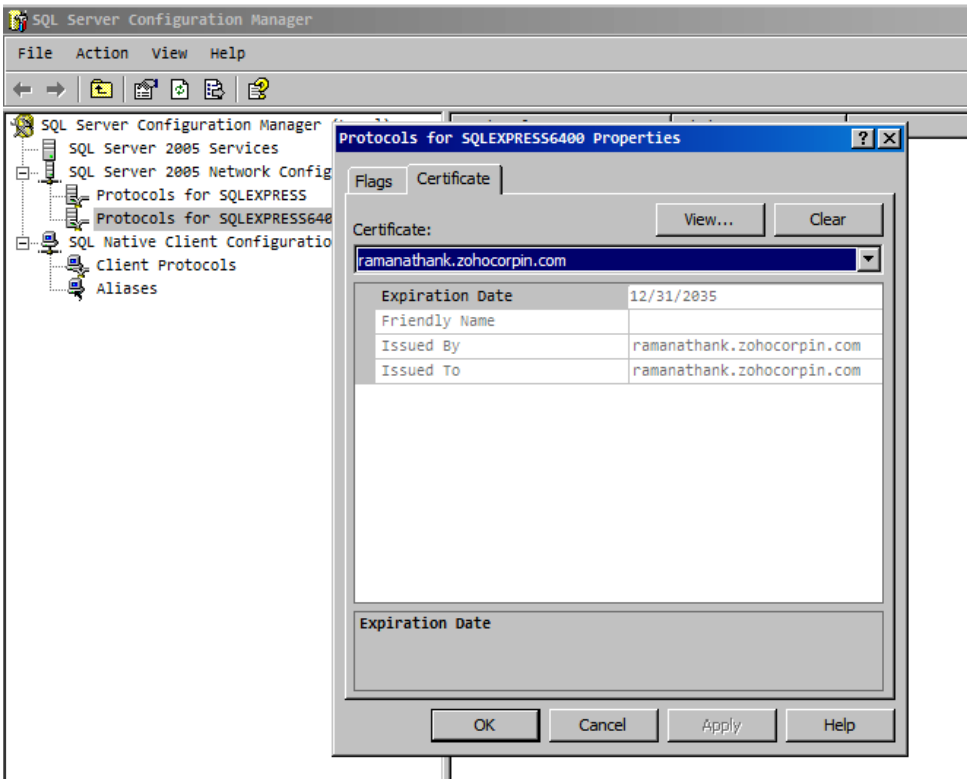
- Copy the server certificate and paste it under <Password Manager Pro Installation Folder>/bin directory
- From <Password Manager Pro Installation Folder>/bin directory, execute the following command:
  importCert.bat <name of the server certificate>
- This adds the certificate to the PMP certificate store.

Step 3: Enable SSL Encryption in SQL Server

To enable SSL for SQL Server,

- In the machine where SQL server is running, click Start, in the Microsoft SQL Server program group, click Configuration Tools, and then click SQL Server Configuration Manager.
- Expand SQL Server Network Configuration, right-click the protocols for the server you want, and then click Properties. (This is the Protocols for section in the left pane of the tool, not a specific protocol in the right pane.)
- On the Certificate tab, configure the Database Engine to use the certificate.
- When the ForceEncryption option for the Database Engine is set to Yes, all client/server communication is encrypted and clients that cannot support encryption are denied access.
- When the ForceEncryption option for the Database Engine is set to No, encryption can be requested by the client application but is not required.
- SQL Server must be restarted after you change the ForceEncryption setting.





For more details, refer to the section "Configuring SSL for SQL Server" in Microsoft's knowledge base article available at http://msdn.microsoft.com/en-us/library/ms189067.aspx

Step 4: Execute ChangeDB.bat in PMP

(Important Note: If you are already using PMP with MySQL and wish to migrate data to MS SQL Server, skip this step and proceed to the next section)

Now, you need to provide the details about the SQL server to PMP by editing the file ChangeDB.bat (Windows) or ChangeDB.sh (Linux)

- Navigate to<Password Manager Pro Installation Folder>/bin folder and execute ChangeDB.bat (Windows) or sh ChangeDB.sh (Linux)
- Select 'Server Type' as SQL Server and enter other values

1. Host Name: The name or the IP address of the machine where MSSQL server is installed.
2. Port: The port number in which PMP must connect with the database. Default is 1433. 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.
3. Database Name: Name of the PMP database. Default is "PassTrix". If you want to have a different database name, you may specify here. PMP will take care of creating the Master Key, Symmetric Key etc.
4. Authentication: The way in which you would like to connect to the SQL server. If you are connecting to the SQL server from Windows, you have the option to make use of the Windows Single Sign On facility provided PMP service is running with a service account, which has the privilege to connect to SQL server. In that case, choose the option "Windows". Otherwise, select the option "SQL". It is recommended to choose the option 'Windows' as the username and password used for authentication are not stored anywhere.
5. User Name and Password: If you have selected the option "SQL", specify the user name and password with which PMP needs to connect to the database. The username and password entered here will be stored in database_params.conf file in PMP. So, you need to take care of hardening the host.
6. Here, you have the option to use even your Windows login credentials, if you are connecting to the database from Windows. In this case, you need to enter the username as <domain-name>\<username>
7. Encryption Key: The key with which your data is to be encrypted and stored in the SQL server. You may either leave it "Default" making PMP to generate a key. If you want to have your custom key, select the option "Custom".
8. If you have selected the option "Custom:" If you have chosen the option 'Custom', you need to create a new database, create Master Key, create Certificate (this will be certificate name) and Create the Symmetric Key using AES 256 encryption.

You need to do the following steps:

Create Database -> For details, refer to http://msdn.microsoft.com/en-us/library/aa258257(v=sql.80).aspx

Create Master Key -> For details, refer to http://technet.microsoft.com/en-us/library/ms174382.aspx

Create Certificate -> For details, refer to http://msdn.microsoft.com/en-us/library/ms187798.aspx

Create Symmetric Key -> For details, refer to http://msdn.microsoft.com/en-us/library/ms188357.aspx

After doing the above, you need to provide certificate name and symmetric key name in the GUI.

- Finally, click "Test" to ensure that the connection settings are proper and then click "Save"

Important Note:

After performing the above steps, navigate to <Password Manager Pro Installation Folder>/conf directory and move the masterkey.key file to a secure location. 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, asymmetric keys, 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 masterkey.key. It is highly recommended that you move the masterkey.key file to a secure location. This is to ensure data security.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 on encryption and key management in MS SQL, refer to this MSDN document http://msdn.microsoft.com/en-us/library/ms189586.aspx

Migrating Data from MySQL/PostgreSQL to MS SQL Server (applicable only for PMP builds 6401 and later)

If you are already using PMP with MySQL/PostgreSQL and wish to use MS SQL as backend database, you may follow the steps below to migrate the data. (These steps are only migrating the data from MySQL to MS SQL server. You should have already completed steps 1, 2 and 3 above to use MS SQL as backend database)

Important Note:

Before trying database migration, please take necessary precautions with regard to the following aspects:

1. Personal Password Management

- In case, you / other users in your organization have used 'Personal Password Management' in PMP with the option of specifying own encryption key, which is NOT stored in PMP, the above migration procedure will NOT take care of migrating the personal passwords. Users will have to be advised to use the 'Export Passwords' option in the personal passwords section before this migration is attempted.

2. Bundled Database Only

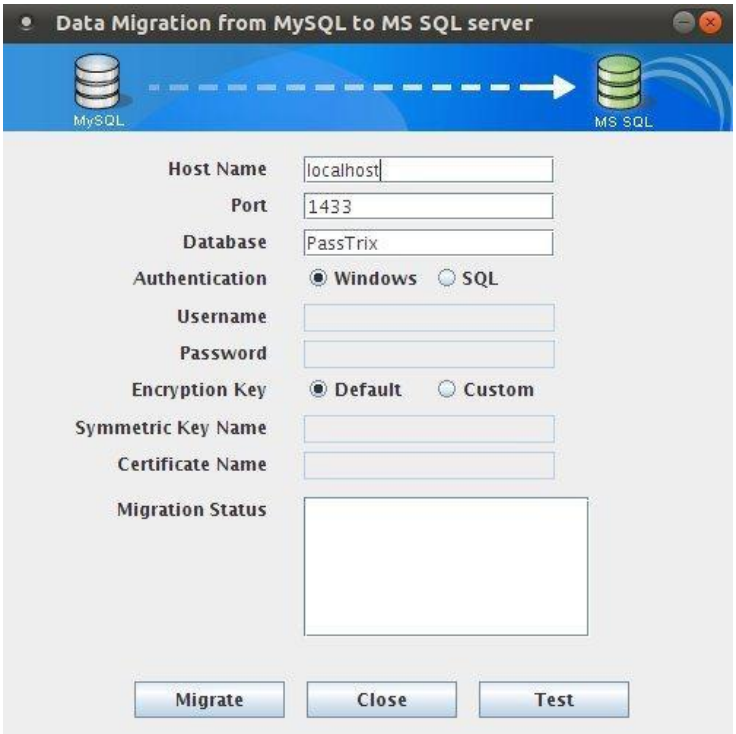
- PMP provides the migration option only if your current PMP installation uses the database bundled with the prooduct. In case, you are using an external database, this procedure does NOT apply.

Step 1

- Take a copy of the entire Password Manager Pro Installation folder and keep it somewhere. If something goes wrong with data migration, this will serve as a backup copy.
- Shutdown PMP server. Also, make sure that the mysqld / postgres process is not running

Step 2

- Navigate to <Password Manager Pro Installation Folder>/bin folder and execute MigrateDB.bat (Windows) or sh MigrateDB.sh (Linux). In the pop-up, select to read the "Best Practices Guide" first and later choose the option "Go to Migration Set Up".



In the window that opens up, enter the details:

1. Host Name: The name or the IP address of the machine where MSSQL server is installed.
2. Port: The port number in which PMP must connect with the database. Default is 1433. 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.
3. Database Name: Name of the PMP database. Default is "PassTrix". If you want to have a different database name, you may specify here. PMP will take care of creating the Master Key, Symmetric Key etc.
4. Authentication: The way in which you would like to connect to the SQL server. If you are connecting to the SQL server from Windows, you have the option to make use of the Windows Single Sign On facility provided PMP service is running with a service account, which has the privilege to connect to SQL server. In that case, choose the option "Windows". Otherwise, select the option "SQL". It is recommended to choose the option 'Windows' as the username and password used for authentication are not stored anywhere.
5. User Name and Password: If you have selected the option "SQL", specify the user name and password with which PMP needs to connect to the database. The username and password entered here will be stored in database_params.conf file in PMP. So, you need to take care of hardening the host. Here, you have the option to use even your Windows login credentials, if you are connecting to the database from Windows. In this case, you need to enter the username as <domain-name>\<username>
6. Encryption Key: The key with which your data is to be encrypted and stored in the SQL server. You may either leave it "Default" making PMP to generate a key. If you want to have your custom key, select the option "Custom".
7. If you have selected the option "Custom:" If you have chosen the option 'Custom', you need to create a new database, create Master Key, create Certificate (this will be certificate name) and Create the Symmetric Key using AES 256 encryption. You need to do the following steps:

   Create Database -> For details, refer to http://msdn.microsoft.com/en-us/library/aa258257(v=sql.80).aspx

   Create Master Key -> For details, refer to http://technet.microsoft.com/en-us/library/ms174382.aspx

   Create Certificate -> For details, refer to http://msdn.microsoft.com/en-us/library/ms187798.aspx

   Create Symmetric Key -> For details, refer to http://msdn.microsoft.com/en-us/library/ms188357.aspx

   After doing the above, you need to provide certificate name and symmetric key name in the GUI

Step 3

- Finally, click "Test" to ensure that the connection settings are proper and then click "Migrate". The status of data migration will be displayed in the textbox
- After the end of data migration, start PMP server

Troubleshooting Tip

If database migration is attempted when PMP server is running, you will encounter this error in the DB Migration GUI: "Server seems to be running. Shutdown PMP server and try again" and the GUI will remain open. In case, you get this error even after shutting down the server, you need to delete the .lock file under <PMP-Installation-Folder>/bin folder and then try migration. If the issue persists, contact PMP support with the .lock file.

Important Note:

After completing the migration, start PMP server and navigate to "Admin >> Resource Additional Fields" and "Admin >> Accounts Additional Fields". Open the GUI and click "Save". This will take care of restoring the additional fields added you in the migrated instance too.

Migrating data from MySQL to PostgreSQL (applicable only for builds 6801 and later)

If you are already using PMP with MySQL and wish to use PostgreSQL as backend database, you may follow the steps below to migrate the data.

- Stop PMP server and make sure mysqld process is not running.
- Download PostgreSQL-9.2.1-Windows.zip (For Windows) / PostgreSQL-9.2.1-Linux.zip (For Linux) and extract the zip file under <Password Manager Pro Installation Folder>
- Open a command prompt and navigate to <Password Manager Pro Installation Folder>/bin directory
- Execute MigrateMySQLToPgSQL.bat (in Windows) or MigrateMySQLToPgSQL.sh (in Linux)
- Start PMP server. Now, PMP will run with PostgreSQL as backend database

Quick Start Guide

Refer to the "Work flow in PMP" section of help documentation.

For any assistance, please contact passwordmanagerpro-support@mnageengine.com / Toll Free: + 1 925 924 9500

Managing PMP Encryption Key (from PMP 6402 onwards)

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.

Rotating Encryption Key

(Feature available only in Enterprise Edition)

Though the encryption key is being securely managed outside of PMP, periodically changing the encryption key is one of the best practices. PMP provides an easy option to automatically rotate the encryption key.

How the key rotation process work?

PMP will look for the current encryption key present in pmp_key.key in the path specified in manage_key.conf present under <PMP_HOME>/conf folder. Only if it is present in the specified path, the rotation process will continue. Before rotating the encryption key, PMP will take a copy of the entire database. This is to avoid data loss, if anything goes wrong with the rotation process.

During the key rotation process, all passwords and sensitive data will be decrypted first using the current encryption key and subsequently encrypted with the new key. Later, the new key will be written in the pmp_key.key file present in the location as specified in the manage_key.conf file. If there occurs any error while writing the key, rotation process will not continue. At the end of successful rotation process, PMP will write the old encryption key in the same file that contains the new key.

To rotate the encryption key (if you are NOT using High Availability)

- The current encryption key (pmp_key.key file) should be present in the location as specified in the manage_key.conf file. Also, ensure that PMP gets read/write permission when accessing the pmp_key.key file.
- PMP server should be stopped
- Open a command prompt and navigate to <PMP-Installation-Folder>/bin directory and execute RotateKey.bat (in Windows) or sh RotateKey.sh (in Linux)
- Based on the number of passwords managed and other parameters, the rotation process will take a few minutes to complete
- Once you see the confirmation message about successful completion of the rotation process, you can start the PMP server.

To rotate the encryption key (if you are using High Availability setup)

- Go to Admin tab>>General>>High Availability in the web interface. Make sure high availability and replication status are alive.
- The current encryption key (pmp_key.key file) should be present in the location as specified in the manage_key.conf file. Also, ensure that PMP gets read/write permission when accessing the pmp_key.key file.
- PMP Primary server should be stopped and make sure PMP Secondary server is running.
- Open a command prompt in PMP Primary installation and navigate to /bin directory and execute RotateKey.bat (in Windows) or sh RotateKey.sh (in Linux)
- Based on the number of passwords managed and other parameters, the rotation process will take a few minutes to complete. You will see confirmation message upon successful completion of the rotation process
- You need to copy the new encryption key from Primary installation and put it in the location from where the standby looks for pmp_key.key file as specified in the manage_key.conf file. (That means, you need to copy the pmp_key.key file in Primary and put it in the location as specified in the manage_key.conf file). Then you can start primary and standby servers.

Managing PMP Database Password

- Apart from the AES encryption, the PMP database is secured through a separate password, which is auto-generated and unique for every installation
- The password 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

Leaving it to PMP

If you choose to leave it to PMP, you need not do anything. PMP will take care of it automatically

Storing it by yourself

- By default, the database password is present in the file <PMP Installation Folder>/conf/database_params.conf file
- If you choose to manage the database key by yourself, you need to store this configuration file somewhere securely and instruct the location of the file to PMP
- If you are starting PMP as service, go to <<PMP Installation Folder>/conf/wrapper.conf (in Windows) / <PMP Installation Folder>/conf/wrapper_lin.conf (in Linux) and edit the following entry under "Java Additional Parameters"
  wrapper.java.additional.9=-Ddatabaseparams.file=<full path of the database_params.conf file location>
- If you are starting PMP from command line or through Start >> Programs, you need to edit the file system_properties.conf present in <PMP Installation Folder>/conf directory. In this file, edit the following entry under "Splash Screen default Properties" databaseparams.file=<full path of database_params.conf file>

Note: If you misplace the conf file or lose it, PMP will not start. So, take care to save it in a secure location.

Ports Used by PMP

PMP uses the following two ports:

- PostgreSQL port : 2345
- Web client port : 7272

Licensing

There are three license types:

- Evaluation download valid for 30 days capable of supporting a maximum of 2 administrators
- Free Edition licensed software allows you to have 1 administrator and manage up to 10 resources. Valid forever.
- Registered Version - need to buy license based on the number of administrators required and the type of edition Standard/Premium/Enterprise:
    - Standard - If your requirement is to have a secure, password repository to store your passwords and selectively share them among enterprise users, Standard Edition would be ideal.
    - Premium - Apart from storing and sharing your passwords, if you wish to have enterprise-class password management features such as remote password reset, password alerts and notifications, application-to-application password management, reports, high-availability and others, Premium edition would be the best choice.
    - Enterprise - If you require more enterprise-class features like auto discovery of privileged accounts, integration with ticketing systems and SIEM solutions, jump server configuration, application-to-application password management, out-of-the-box compliance reports, SQL server / cluster as backend database, Enterprise edition will be ideal.

Password Management Features Matrix

Standard Edition	Premium Edition	Enterprise Edition
• User / User group Management • Password Repository • Password Policies • Password Sharing and Management • Audit / Audit Notifications • AD / LDAP Integration • Offline Access • Password Change Listener • Backup and Disaster Recovery • Auto Logon • TFA - Unique Password Generated Through Email • Rebranding • Mobile Access (Android, iOS, Windows) • Browser Extensions (Chrome, Firefox)	• All Features of Standard Edition • Auto Logon Helper • Password Alerts and Notifications • Bulk Configuration • Remote Password Reset (on demand, scheduled and rule based) - for Windows, Windows Domain, Windows Service Accounts, Windows Scheduled Accounts, Flavors of UNIX and Linux, Cisco, HP ProCurve and Juniper Netscreen Devices, MS SQL Server, MySQL Server, Oracle DB Server and Sybase ASE, LDAP Server • Instant Verification of Passwords for Synchronization with Remote Systems • Password Access Control Workflow • Privileged Session Recording • Reports • Password Management APIs for Application to Application Password Management • Two-Factor Authentication - RSA, PhoneFactor, Google Authenticator • High Availability Architecture	• All Features of Premium Edition • AD User Group / OU Sync • LDAP Sync Support • Encryption Key Rotation • Privileged Accounts Discovery • Ticketing System Integration • SNMP, Syslog Integration and Email Templates • Real Time Alerts & SIEM Integration • Jump Server Configuration • Federated Identity Management • TFA - Radius Based, Smart Card • Out of the Box Compliance Reports • SQL Server / Cluster as Backend Database • Privileged Session Shadowing and Termination • Custom Password Reset Listener • Custom Reports • Exporting Passwords as encrypted HTML • RESTful APIs for integration with third-party applications

- For more information and to get license, contact sales@manageengine.com

Moving PMP Installation Within Same Machine / From One Machine to Another

If you want to move the PMP installed in one machine to another or to a different location within the same machine, follow the procedure detailed below:

Prerequisite

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

Procedure

If you are using the PostgreSQL database bundled with PMP

- Take backup of the current database Install the same version of PMP (as the one you are currently running) in the new machine
- Restore the backup data in the new installation

If you are using MySQL as backend database

- Stop PMP server / service, if running
- If you have installed PMP to run as a startup service, remove it as service before proceeding further.
- See the table below for the procedure to remove it as service.
- Take a zip of the entire PMP installation folder; move the zip to a different machine or to a different location in the same machine as required Then, install it to run as service.

Installing as Startup Service in Windows	Installing as Startup Service in Linux
To install as service using batch file • Open a console and navigate to <PMP_Installation_Folder>/bin directory • Execute the command pmp.bat install To remove as service using batch file • Open a console and navigate to <PMP_Installation_Folder>/bin directory • Execute the command pmp.bat remove	• Login as root user • Open a console and navigate to /bin directory • Execute "sh pmp.sh install" • (In Ubuntu, execute as "bash pmp.sh install") • To remove as service, execute the script "sh pmp.sh remove" • (In Ubuntu, execute as "bash pmp.sh remove")

Note:

- 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.
- You need not reapply the license after moving the installation

MSP Edition

If you want to use the MSP edition of PMP, refer to this section of the help documentation.

PMP MSP Edition Getting Started

Overview

ManageEngine Password Manager Pro is now available in MSP edition, which has been specially designed taking into consideration the requirements of the Managed Service Providers. If you are an MSP wishing to manage the administrative passwords of your clients separately from a single management console or offer Password Management Service to them, you can now leverage the MSP edition.

Passwords can be securely shared between MSP administrators and their respective customers, making sure that users only get access to the passwords they own or ones that are shared with them. The solution offers the flexibility to entrust the control of the password vault to the MSP administrator, the end user or both, as desired.

The MSP edition also follows the basic password entitlement model of PMP – that means, at any time, one will be able to view only the passwords that are owned and shared. As MSP admin, while you will be able to view the names of the organizations you manage, you will be able to view the data pertaining to all your customers only if you add their resources or if they share the resources with. Your customers will be able to view the data belonging to their organization.

MSP Edition – Getting Started

Pre-requisite

- For testing the MSP edition, you need to deploy a separate machine. If you try to install the MSP edition in the same machine where PMP is running, it will uninstall the existing PMP instance.

Getting started

- Download and install the ManageEngine_PMP_MSP.exe

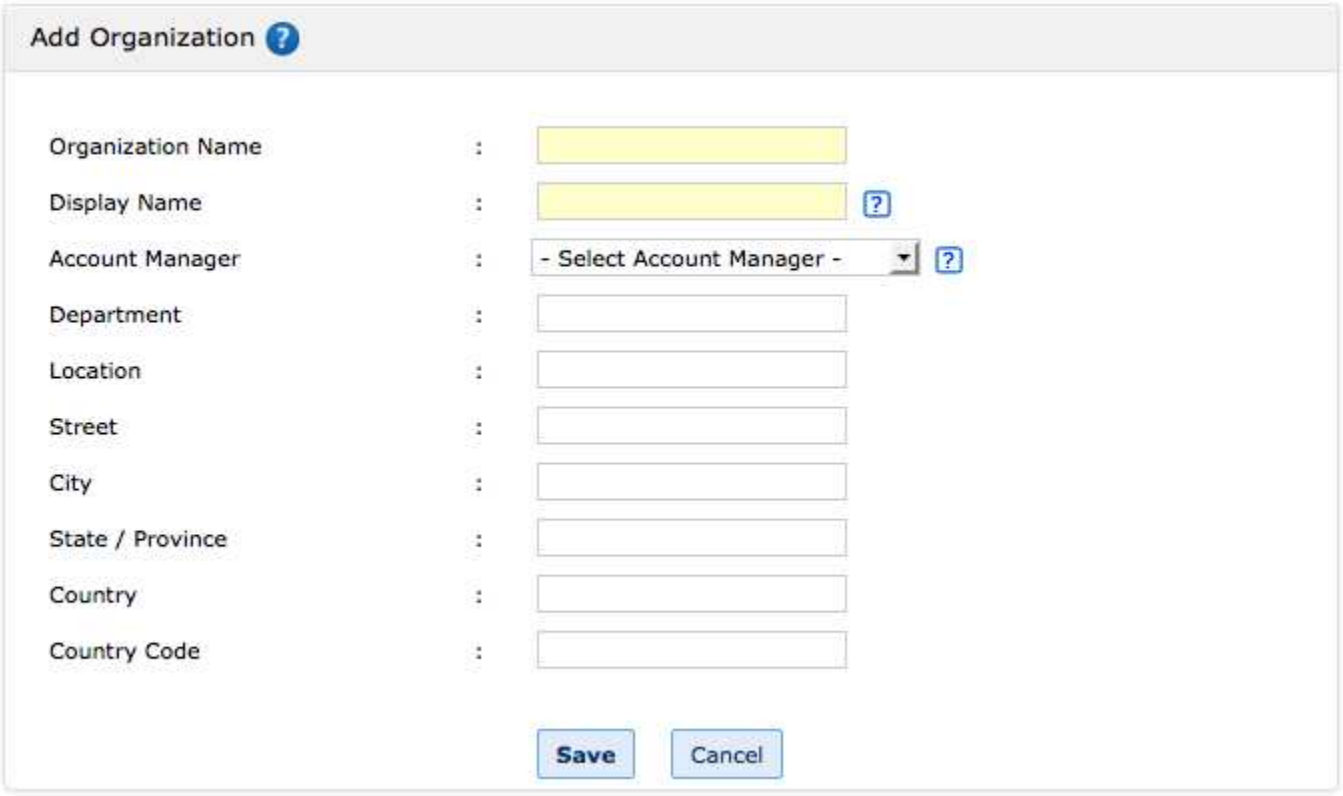
Step 1: Add users to the MSP org

The MSP administration process starts with User Management. The first step is to add users to your MSP organization. You should designate one administrator as „Account Manager“ for each of your clients. Proceed with adding users.

Step 2: Add your client organizations

After adding users, you need to add your client organizations. Navigate to Admin >> Customize section and you will find an icon named"Organizations". The organizations to be managed by the MSP should be registered with PMP here.

You can manually add the client organizations one-by-one or import all the organizations in bulk from a CSV file.



Manually adding organizations

- Navigate to Admin >> Customize section and you will find an icon named "Organizations"
- Click the button "Add Organization"
- In the UI that opens up, specify a name for the organization being added
- Display Name: The name with which you wish to identify the organization being added. Only alphanumeric characters without empty spaces are allowed here. The name should be a single word. The name that you enter here will appear in the drop-down at the top RHS of PMP GUI. In addition, the display name will appear in PMP login URL. For example, if you assign 'xyz' as the display name, the login URL for the organization will be https://:/xyz

- Account Manager: You can designate any administrator at your end (MSP) as the 'Account Manager' for the organization being added. As the name indicates, the account manager will be the point of contact for the organization being managed and will have privileges to add and manage resources on behalf of the organization. The Account Manager with the role 'Admin' in PMP will be able to manage the users of the organization too. You can designate only one account manager per organization being managed. The same administrator can be made the account manager for multiple client organizations.
- Fill-in other details like Department, Location etc. as required

Import Organizations from CSV

You can import multiple organizations from a CSV file using the import wizard. The CSV should have entries regarding organization name, display name and other details in comma separated form. The entry for each organization should be in a new line. All the lines in the CSV file should be consistent and have the same number of fields. CSV files having extensions .txt and .csv are allowed.To import organizations,

- Navigate to Admin >> Customize section and you will find an icon named "Organizations"
- Click the button "Import Organizations"
- In the UI that opens up, browse and select the CSV file containing the organizations
- Click "Next"
- In the UI that opens, you can choose which field in the CSV file maps to the corresponding attribute of the Organization.
- Finally, click "Finish"

The result of every line imported will be logged as an audit record.

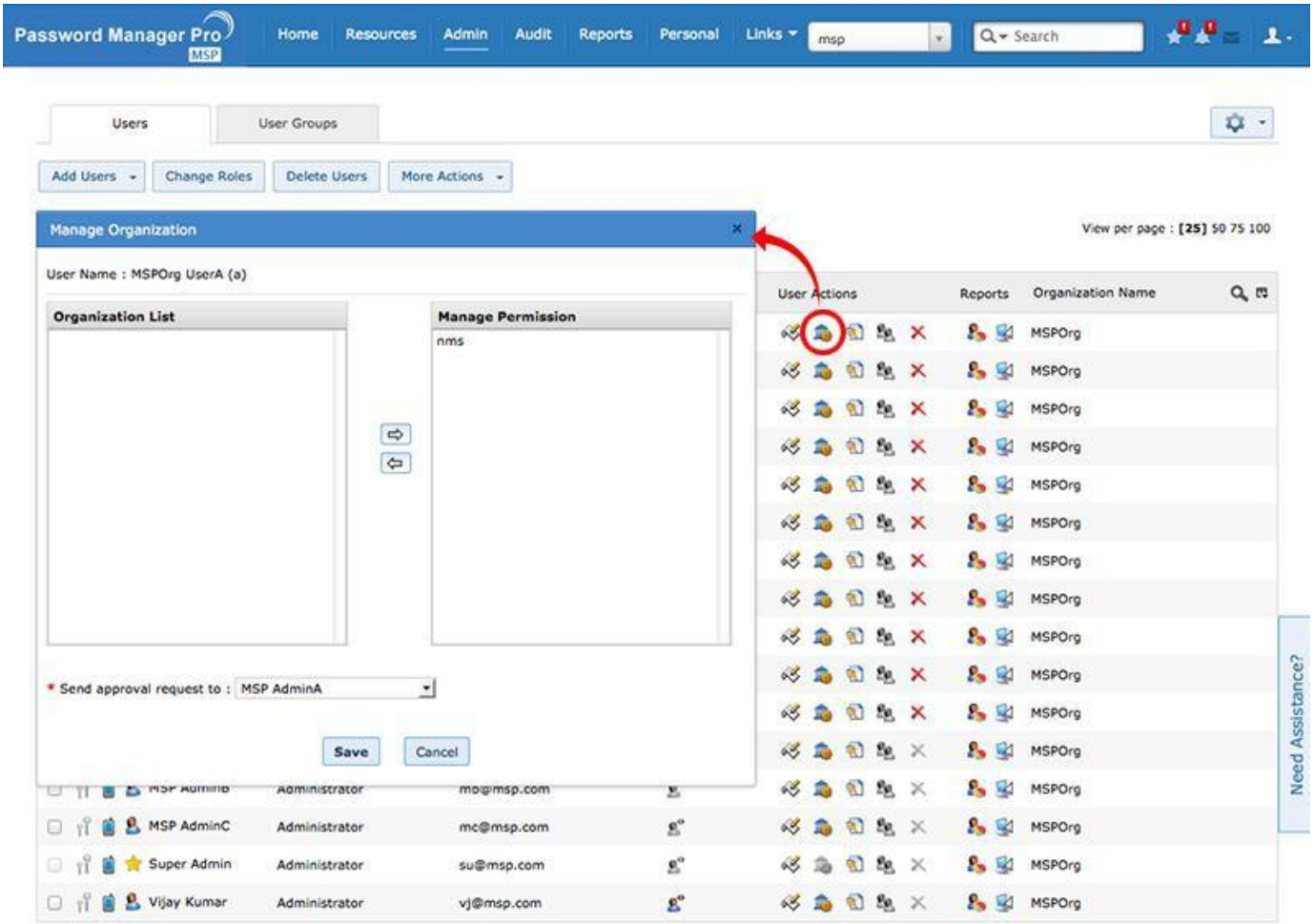
Granting Manage Organization Privilege

Apart from designating an administrator as „Account Manager", you have the option to grant „Manage Organization" privilege to any other member of your MSP org. When you grant this permission to an administrator, he will have admin privileges on the client org. Similarly, if the permission is granted to a password administrator or to a password user, they will have the respective privileges.

For security reasons, PMP enforces approval process for managing an organization. That means, while any administrator at the MSP can initiate manage permission to a user, it has to be approved by some other administrator at the MSP org. One who initiates the request and the one for whom the request is being initiated cannot approve. A third administrator

has to approve. This is to ensure that no administrator is able to acquire manage permission for himself or grant that privilege to anyone else without the approval of another admin. This essentially means that the MSP org should have a minimum of three administrators to carry out this process.

For example, assume the scenario when „Admin A“ wants to provide manage permission to „Admin B“ for the organization „ABC“. In this case, both Admin A (the proposer) and Admin B (the admin designate) cannot approve. Another admin, say, „Admin C“ will have to approve.

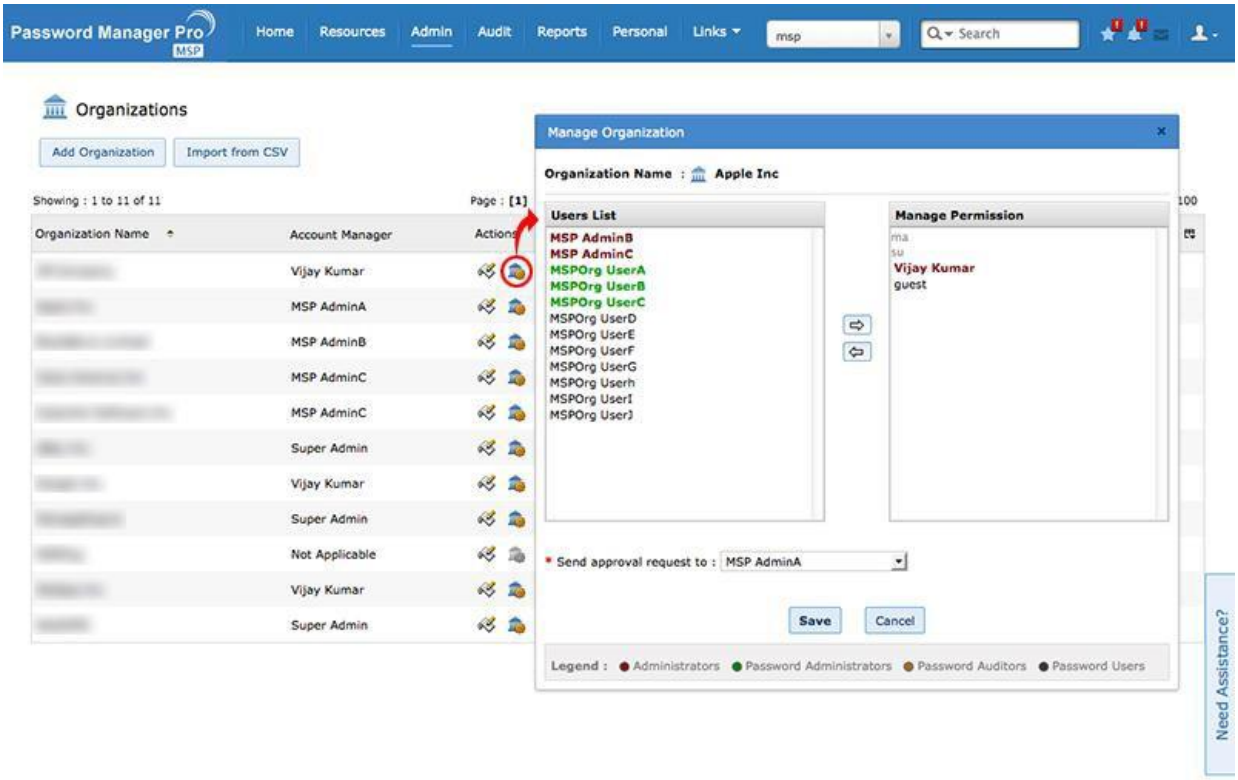


To grant manage permission for an organization,

- Login to your MSP account and navigate Admin >> Users
- Click the „Manage Organization“ icon under „User Actions“ column
- In the UI that opens up, select the required client organization and move it to right
- Select the name of the approver
- Click „Save“

The user will gain manage privilege once the approval is done.

Alternatively, you can grant manage permission from 'Organizations' page too by clicking the „Manage Organization“ icon under „User Actions“ column



MSPOrg – The default org

By default, one organization named “MSPOrg” would be available. This default org is basically your organization (MSP“s organization). The passwords that you add here will pertain to your own organization and not that of your clients.

Password Management for Client Organizations

Once the organization is added, you will see the list of organizations being managed by you (i.e for which you have manage permission or for which you are the account manager) on the top band of the PMP GUI “Select Organization”.

Select the required organization and proceed with resource addition. You can then share the passwords with your clients. On the other hand, if you are providing Password Management Service, you will ask your client to add passwords themselves.

How to access any specific client org?

You can access your MSP org as usual by accessing the URL https://<PMP-Host-Name>:7272/. You can select the required client organization from the top band of the PMP GUI.

How do your clients access PMP?

After creating an organization, you clients can connect to their organization and view/manage passwords by typing the URL as explained below:
https://<Host Name:<port>/<Name of the org>

For instance, assume that the name of the organization of your client is „abc“ and PMP is running on the host “pmphost”, then the URL to connect to an organization will be: https://pmphost:7272/abc

For information on how to perform various password management features, refer to the respective sections of the help documentation.

Important Terminologies

While working with Password Manager Pro, you will come across some terminologies having unique meanings. It is worthwhile to take a note of those terminologies before proceeding further:

Hardware	Operating systems
Resource	Denotes the server/application/device whose user accounts and passwords are to be managed by Password Manager Pro
Resource Group	Denotes the group to which a particular resource belongs. For example, if you have some Windows XP servers among a number of other windows servers, you can group all the XP servers as one resource group
User Account	Denotes the 'User Account' & 'Password' that are to be managed by Password Manager Pro
User	Denotes the Password Manager Pro user accounts created as part of Password Manager Pro User Management.
User Group	Group of Password Manager Pro Users
Password Policy	Refer to the explanation
PMP	Abbreviation for Password Manager Pro

Work flow in PMP

If you are an Administrator ...

If you are an administrator engaged in the job of setting up PMP in your environment and managing passwords, following is the ideal work flow:

- Setup Mail Server
- Add users who will use PMP
- Add resources whose passwords you want to manage
- Setup disaster recovery

User Addition work flow

- Prior to adding users, the important step to be done is configuring your mail server. Users will be notified of their PMP access details through email only, so ensure the mail server is setup properly. Click the link "Mail Server Setting" available in "Admin >> General" section. Enter your mail server name, its port and authentication credentials, the url that is to be displayed on the mail intimation to users to access PMP (access url). While providing authentication details, you have the option to specify the required username and password manually or you can make use of an user account already stored in PMP. When you choose the second option "Use an user account already stored in PMP", the resources and the accounts that appear on your resources tab, will be listed in the drop-down. You can choose the required details. After providing the authentication details, click "Save"
- Change the password of the default 'admin' user or delete the account after adding another administrator user
- Add users either manually or import user information from ActiveDirectory, LDAP or CSV file
- Specify appropriate access roles and password policies for the PMP users
- Group users together for the convenience of performing operations in bulk
- Enable authentication to any one of AD, LDAP or Local

Resource Addition work flow

The first step to actual Password Management in PMP starts with adding your "resource" to the PMP database. Here, resource denotes the server/application/device whose user accounts and passwords are to be managed by PMP.

- Add resources either manually or import from a CSV file along with their user account and password information
- Setup the password reset method to one of remote or agent-based, if you need
- Group resources together for the convenience of performing operations in bulk
- Create Nested Resource Groups: Maintaining resource groups in hierarchical structure (groups, sub-groups) for navigational convenience
- By default, the passwords added by you could be viewed and edited only by you. If required, share resource passwords with other PMP users or user groups
- Access and modify passwords that are owned by you and that are shared to you

Access Control work flow

After adding the resources, administrators can put in place access control work flow for extra level of security. After successful authentication into Password Manager Pro, users get access to the passwords that are owned by them or shared to them. In some cases, administrators wish to give temporary access to passwords for certain users for a specified period of time. In other instances, there would be requirements to give users exclusive privilege to passwords. That means, only one user should be allowed to use a particular password at any point of time. When more than one user is required to work on the same resource, problems of coordination arise. Access control on concurrent usage would help resolve such issues.

- Set up access control work flow as per the requirements of your organization

Setup Disaster Recovery

If you are a Password User ...

- Configure the database backup schedule to backup the entire contents of the Password Manager Pro database
- Export resource information in the format of your choice to have readable copies of resource information only

If you are a Password user engaged in the job of viewing the passwords allotted to you, there is no need to carry out any configuration. You may directly view the passwords of resources/accounts and edit passwords if you have that permission.

Important Terminologies

While working with Password Manager Pro, you will come across some terminologies having unique meanings. It is worthwhile to take a note of those terminologies before proceeding further:

Category	Feature	Explanation
User Management	*AD / LDAP support*	Integration with external directory server for user management, authentication
	Smart Card Authentication	If you have a smart card authentication system in your environment, you can configure PMP to authenticate users with their smart cards, bypassing other first factor authentication methods like AD, LDAP or Local Authentication.
	User Roles	Four different user roles providing fine-grained access control
	Super Administrator	Enabling an administrator to see all the resources in the system unconditionally
	User Groups	Create groups of users for carrying out operations in bulk
	Domain Single SignOn	Pass through authentication for PMP server, when integrated with AD
Resource Management	*Resource types*	Categorise resources based on their types (for e.g Windows Servers). Create and manage your own resource types, in addition to the default types
	Resource Groups	Create groups of resources / passwords and manage the groups. Carry out password management operations in bulk.
	Nested Resource Groups	Maintain resource groups in hierarchical structure (groups, sub-groups) for navigational convenience
	Share Resources/Groups	Share resources /resource groups with desired users/user groups
Password Management	*Resource Customization*	Add attributes to resources and accounts according to your needs
	Password Access Control Workflow	Helps enforce enhanced access control in the product. The user, who requires a password, will have to 'request the release' and one or more administrators will authorize the request. The password availability to the user is time limited. It will be automatically reset thereafter and the user will thereby forfeit the access.

Category	Feature	Explanation
	Password Policies	Create and manage your own password policies for enforcing their adoption through PMP
	Password Resets	Perform password resets to resources from PMP (Windows, Windows Domain, Linux, IBM AIX, HP UNIX, Solaris, Mac OS, MS SQL server, MySQL server, Oracle DB Server, Sybase ASE, HP ProCurve and Cisco Devices (IOS, CatOS, PIX)).
	Password Reset Schedules	Automate password resets
	Password Actions / Notifications	Generate alerts for various password events and specify action to be taken on password events
	Password Reset Listener	Invoke a custom script to initiate desired action on password changes
	Windows Service Account Management	Keep your windows service account and scheduled task passwords synchronized with the corresponding domain account
	Auto Logon Helper	Connect to target systems with a single click from PMP console without having to actually see the passwords
	Password Management API	Setup your applications to query PMP for A-to-A and A-to-DB passwords
Audit and Reports	*Audit*	Comprehensive audit of all operations done on resources, passwords and users. Export to pdf and email
	Audit Filters	Create Filters to view only those audit records that are of interest
	Audit Notification	Choose to send/receive notification on the occurrence of desired audit events
	Canned Reports, Custom Reports	Intuitive reports on password inventory, compliance, expiry, resource and user activity. Print reports, export to pdf and email Provision for generating various custom reports to suit specific business requirements
	Dashboard	Password and user dashboard providing a snapshot on password management activities
Non-functional Features	*Two-Factor Authentication*	Enforcing users to identify themselves with two unique factors before they are granted access to the web-interface
	Backup for Disaster Recovery	Setup backup of the PMP database for disaster recovery purposes

Category	Feature	Explanation
	High Availability	setup redundant PMP servers to provide high availability of PMP application
	Customize Email Notification Content	By default, PMP has a specific content for the email notification for various password actions. If you want, you can customize the content and have your own content.
	Re-brand	Use your own logo in the PMP user interface
	General Settings	Switch on and off various features on need basis
	Manage Encryption Key	Store PMP's encryption key in a desired location for additional security

User Management

User Management

As PMP serves as a repository for the sensitive passwords, fine-grained access restrictions are critical for the secure usage of the product. PMP provides role-based access control to achieve this.

In practical applications, information stored in PMP will have to be shared among multiple users. By default, PMP comes with four pre-defined roles –

- Administrators set up, configure and manage the PMP application and can perform all the resource and password related operations. However, they can view only those resources and passwords that were created by them and the ones shared to them by other users.
- Password Administrators can perform all resource and password related operations. However, they can view only those resources and passwords that were created by them and the ones shared to them by other users
- An administrator/Password Administrator can be made as a 'Super Administrator' by other administrators (and not by himself). Super Administrator will have the privilege to manage all the resources added in the system by all. (To know how to make an administrator or a password administrator as super administrator, click here)
- Password Users can only view passwords that are shared to them by the Administrators or Password Administrators. They can modify passwords if the sharing permission allows them to do so
- Password Auditors have the same privileges as Password Users and in addition they have access to audit records and reports

Role	*Operations*					
	Manage Users	*Manage Resources*	*Manage Passwords*	*View Passwords*	*Managing Personal Passwords*	*View Audit & Reports*
Administrator	✓	✓	✓	✓	✓	✓
Password Administrator	✗	✓	✓	✓	✓	✗
Password User	✗	✗	✗	✓	✓	✗
Password Auditor	✗	✗	✗	✓	✓	✓
Irrespective of the role, the personal passwords remain exclusive to the individual user and other users have no control over them.						

You can create as many users as you desire and define appropriate roles for the user. This section explains how to create users and assign roles for them.

Adding New Users

Note: User Addition can be done only by the Administrators.

From the Users tab, administrators can

- View all the existing PMP users
- Create new users
- Edit the access role of the user
- Enable two-factor authentication
- When RSA SecurID is used as the second authentication factor, you need to ensure that the user name in RSA Authentication Manager and the corresponding one in PMP are same. In case, for the already existing RSA users, if the user name in PMP and in RSA Authentication Manager are different, you can do a mapping of names in PMP instead of editing the name in RSA. This can be done from here through "RSA SecurID UserName". (Assume the scenario that in PMP you have imported a user from Active Directory, who has the username (say) ADVENTNET\rob inPMP. In RSA Authentication Manager, assume that the username is recorded as 'rob'. In normal case, there will be mismatch of usernames between PMP and RSA Authentication Manager. To avoid that, you can do a mapping in PMP - ADVENTNET\rob will be mapped to rob).

New users can be added in four ways

- Adding users manually
- Importing users from Active Directory
- Importing users from LDAP
- Importing users list from a CSV file

By default, PMP stores all user data in the MySQL database and performs authentication using database lookups. When you integrate AD/LDAP as the authentication system, the default authentication of PMP would be replaced by AD or LDAP to authenticate a user's identity. At any point of time, only one mode of authentication could be employed in PMP.

Denying Super-Administrator Creation by Administrators

Super-Administrators in PMP get the privilege to view all the passwords stored in the system. Organizations generally wish to keep the super-administrator role as a break-glass account for emergency access to passwords. At present, any administrator can change the role of another administrator (not himself) as super-administrator

PMP now provides the option to deny administrators from creating super-administrators. This can be done by any super-administrator from Admin >> Super Administrator >> Deny Administrators from Creating Super Administrators.

The Best Practice Approach

If your organization requires super-administrator only as a break-glass account, the following would be the best practice approach:

- Create a new administrator account in PMP
- Designate the new account as the Super-Administrator
- The new super-administrator will login and enforce the above option of denying other administrators from creating super-administrators
- The login credentials of this super-administrator will be sealed and kept in a safe to be opened only for emergency access

The Implications

- Once you enforce this option, no more super-administrators could be created by administrators
- The existing super-administrators (other than the break-glass account), if any, will not get affected. They will continue to have super-admin access as usual
- The existing super-administrators and the break-glass super-admin accounts will have the privilege to create new super-admins

Adding Users Manually

- Click "Add User" button in "Admin >> Users" tab
- In the "Add User" UI that opens up, enter the 'First Name' and 'Last Name' of the user to be added against the respective text fields. These entries are mandatory
- Enter the desired login name against the text filed "User Name". This entry is also mandatory and it should be unique
- Enter the E-Mail id of the user. It is to this id, the login password for that user will be mailed
- Select an appropriate access level - Administrator/Password Administrator/Password User
- If you are adding a user as "Administrator" or "Password Administrator", you can specify the 'Access Scope'. If you select the option, "Passwords Owned and Shared", the administrator/password administrator will be able to view the passwords owned by them and those shared to them by others. You can choose to make the administrator/password administrator a super administrator, you need to select the option "All Passwords in the System". When you do so, the administrator or the password administrator will be able to access all passwords in PMP without any restriction.
- Select the required password policy. Based on this policy, login password will be generated and sent to the user
- Enter the department to which the user belongs (optional)
- Enter the location of the user. This would be helpful for future reference (optional)
- Click "Save". The required user with desired access restriction has been created

Integrating Active Directory & Importing Users

(AD User Group / OU Sync - Feature available only in Enterprise Edition)

PMP provides the option to integrate with Active Directory in your environment and import users from there. Users who have logged into the Windows system using their domain account can be allowed to login to PMP directly (without separate PMP login).
There are four steps involved in completing the process of importing users from AD and assigning them necessary roles and permissions in PMP. Follow the three steps detailed below:

Step 1 - Importing Users

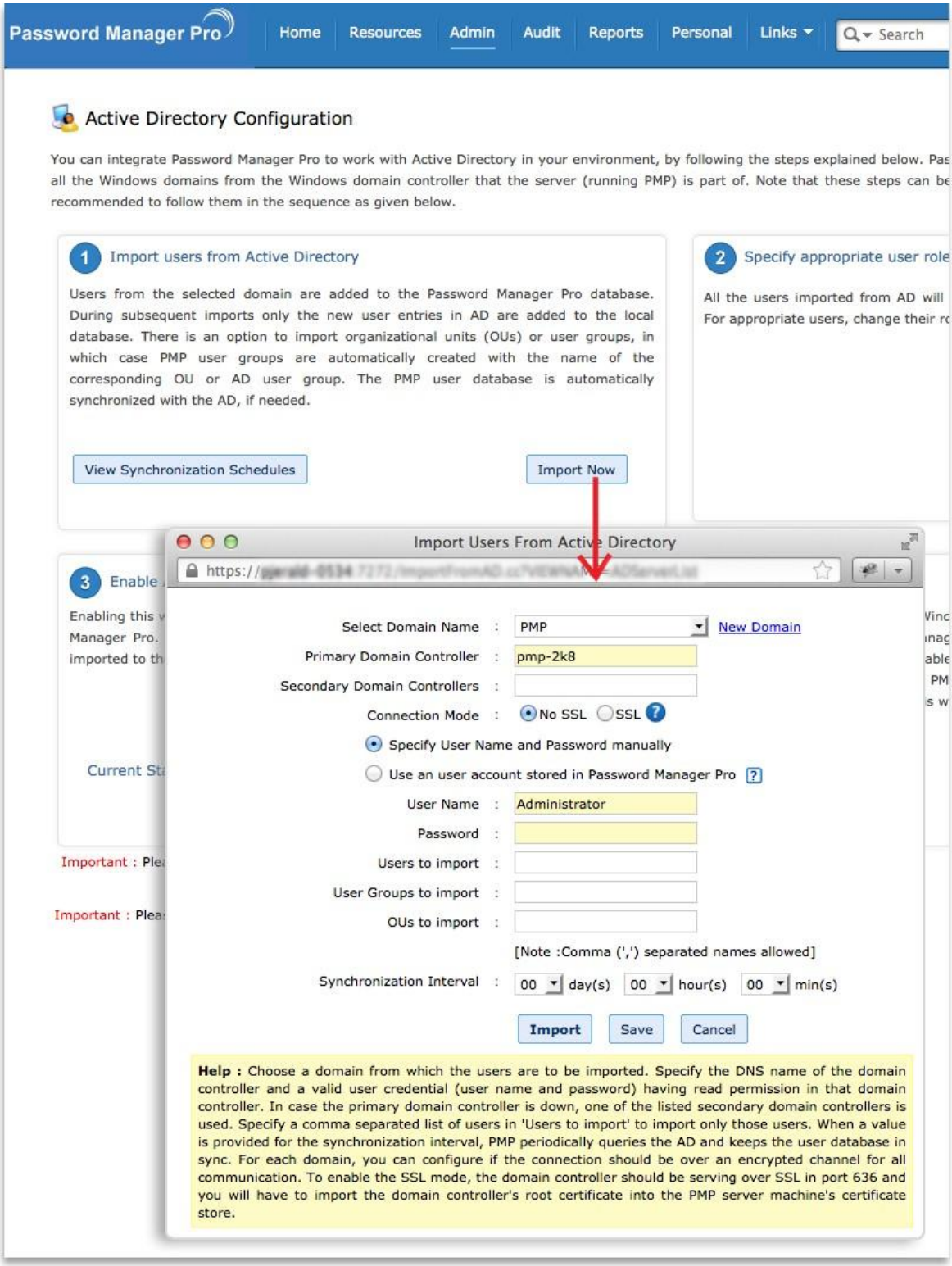
The first step is to provide credential details and importing users from AD. PMP automatically gets the list of the domains present under the "Microsoft Windows Network" folder of the server of which the running PMP is part of. You need to select the required domain and provide domain controller credentials.

To do this,

- Go to "Admin" tab and click "Active Directory"
- Go to Step 1 and click the button "Import Now"
- Alternatively, you can also access this from "Admin >> Users >> Import from AD" button

In the UI that pops-up,

- Select the required Domain Name, which forms part of the AD from the drop-down
- Specify the DNS name of the domain controller. This domain controller will be the primary domain controller



- In case, the primary domain controller is down, secondary domain controllers can be used. If you have secondary domain controllers, specify their DNS names in comma separated form. One of the available secondary domain controllers will be used. When

you use SSL mode make sure the DNS name specified here matches the CN (common name) specified in the SSL certificate for the domain controller

- Enter a valid user credential (user name and password) having read permission in the domain controller. (If you want to import users from multiple domains, you may enter the username as <DomainName>\<username>. For example, if you want to import DOMAIN A users by giving DOMAIN B username/password, you need to enter the username as <DOMAIN B>\username))
- For each domain, you can configure if the connection should be over an encrypted channel for all communication. To enable the SSL mode, the domain controller should be serving over SSL in port 636 and you will have to import the domain controller's root certificate into the PMP server machine's certificate.

As mentioned above, to enable SSL mode, the domain controller should be serving over SSL in port 636. If the certificate of the domain controller is not signed by a certified CA, you will have to manually import the certificate into the PMP server machine's certificate store. You need to import all the certificates that are present in the respective root certificate chain - that is the certificate of the PMP server machine and intermediate certificates, if any.

To import domain controller's certificate into PMP machine's certificate store: (you can use any procedure that you normally use to import the SSL certificates to the machine's certificate store. One example is given below)

- In the machine where PMP is installed, launch Internet Explorer and navigate to Tools >> Internet Options >> Content >> Certificates
- Click "Import"
- Browse and locate the root certificate issue by your CA
- Click "Next" and choose the option "Automatically select the certificate store based on the type of certificate" and install
- Again click "Import"
- Browse and locate the domain controller certificate
- Click "Next" and choose the option "Automatically select the certificate store based on the type of certificate" and install
- Apply the changes and close the wizard
- Repeat the procedure to install other certificates in the root chain

PMP server can now communicate with this particular domain controller over SSL. Repeat these steps for all domain controllers to which you want PMP to communicate over SSL. Note that the DNS name you specify for the domain controller should match the CN (common name) specified in the SSL certificate for the domain controller.

- By default, PMP will populate all the OUs and groups from AD. If you want to import only a particular user, enter the required user name(s) in comma separated form
- Similarly, you can choose to import only specific user groups or OUs from the domain. You can specify the names in the respective text fields in comma separated form
- Whenever new users get added to the AD, there is provision to automatically add them to PMP and keep the user database in sync. Enter the time interval at which PMP has to query the AD to keep the user database in sync. The time interval could be as low as a minute or it can be in the range of hours/days.
- Click "Save". Soon after hitting this "Save" button, PMP will start adding all users from the selected domain. During subsequent imports, only the new users entries in AD are added to the local database
- In the case of importing organizational units (OUs) and AD groups, user groups are automatically created with the name of the corresponding OU / AD group.
- During import, every user will be notified through email about their account, along with a password that will be used to login to PMP when AD authentication is disabled. If you do not want to send emails, select the option 'No'. You can also disable email notification, from General Settings. But, the option entered here ('YES' or 'NO' for email notification) will override the option chosen in 'General Settings'.

Important Note:
"Groups/OUs too large to display"

When you have a large number of groups or OUs in the domain controller, specifically when the number exceeds 2500, PMP will not display them in the GUI. In such cases, you will see the message "Groups too large to display" / "Organizational Units too large to display". When this happens, you have the following options:

Option 1: Specify only the specific groups / OUs to be imported
You may just specify the groups or OUs that are to be imported alone, instead of getting all the groups / OUs in the display.

Option 2: Increase the limit on the number of groups / OUs to be imported
The maximum number of groups / OUs to be displayed in the PMP GUI is indicated in system_properties.conf file present under <PMP_Installation_Folder>. You can increase the number through the following entries:
Navigate to <PMP_Installation_Folder>/conf directory and edit the following entries in system_properties.conf
domain.group.limit=2500
domain.ou.limit=2500
Replace the above entries with the required values.

- What will be role of the users imported from AD, in PMP?
  The users added to the PMP database will have the role as "Password Users". If you want to assign specific roles to specific users, proceed with Step 2 below.
- Can I handle both AD and non-AD permissions to login to PMP?
  Yes. You can use both your AD and local (non-AD) passwords to login to the application. The choice can be made in the GUI login screen itself.
- How to verify if user/user group synchronization had taken place in AD?
  The synchronization happens as a scheduled task. You can check Audit >> Task Audit for details. You can also choose to receive notifications whenever the synchronization happens. Refer to 'Task Audit' section for details. Alternatively, you can also click the button "View Synchronization Schedules" present in Step 1. The status of synchronization will be displayed there.

Step 2 - Assigning Roles

All the users imported from AD will be assigned the 'Password User' role by default. To assign specific roles to specific users,

- Go to Step 2 in the UI (Admin >> Active Directory) and click the button "Assign Roles Now"
- In the UI that opens, all the Users imported from AD are shown in the LHS under the column "Password Users"
- Select the users for whom you wish to change the role and use the appropriate arrow button to assign them the role of "Password Administrator" or "Password User"
- Click "Save" and the required roles are set for the users

Step 3 - Enabling Authentication

The third step is to enable AD authentication. This will allow your users to use their AD domain password to login to PMP. Note that this scheme will work only for users who have been already imported to the local database from AD.
Note: Make sure you have at least one user with the 'Administrator' role, among the users imported from AD.

Step 4 - Enabling Single SignOn

Users who have logged into the Windows system using their domain account need not separately sign in to Password Manager Pro, if this setting is enabled. For this to work, AD authentication should be enabled and the corresponding domain user account should have been imported into PMP.

For Single SignOn, PMP makes use of a third party library named 'Java Enterprise Security Provider Authority' (Jespa), which provides advanced integration between Microsoft Active Directory and Java applications. Jespa NTLM security provider validates credentials using the NETLOGON service just as a Windows server.

To facilitate this, a Computer account must be created with a specific password, which will be used as a service account to connect to the NETLOGON service on an Active Directory domain controller.

That means, PMP requires a computer account in the domain controller to perform the authentication (a computer account must be available/created - a regular User account will not work.

To Enable Single SignOn,

- Go to Step 4 in the UI (Admin >> Active Directory) and click the button "Enable Single SignOn"
- In the UI that opens, select the domain
- Enter the fully qualified DNS domain name in the text field against "Fully qualified DNS Domain Name" (For example, zohocorpin.com)
- Enter the Computer Account name created in the domain controller and specify the password
- If you want to create computer account afresh, select the checkbox "create this computer account in the domain". Jespa contains a script to set the password on a Computer account.
- Click "Save"

Note:
The IE browser supports NTLM authentication by default. Follow the instructions below to get this working in Firefox:

- Open a Firefox browser and enter the URL about:config and hit "Enter".
- You will see a big list of settings
- In the filter, type "ntlm" to look for the setting "network.automatic-ntlm-auth.trusted-uris". Double click that entry and enter PMP server url in the text field (https://<PMP Server Host Name>:<port>)
- Then look for the setting "network.ntlm.send-lm-response"
- Double click the entry to change it from its default setting of "False" to "True"

In MSP Edition, Single SignOn can be enabled only for one client organization at a time. This can be enabled/disabled by the MSP Administrator.

Integrating LDAP & Importing Users

You can make PMP to work with a LDAP compliant directory (like Active Directory) in your environment, by following the steps explained below. Note that these steps can be performed in any order, but on the first time it is recommended to follow them in the sequence as given below.

Step 1 - Import Users

The first step is to provide credential details and importing users from LDAP.

To do this,

- Go to "Admin" tab
- Click "LDAP"
- Go to Step 1 in the UI and click the button "Import Now"
- Alternatively, you can also access this from "Admin >> Users >> Import from LDAP" button

In the UI that pops-up,

1. You can configure the connection between LDAP Server and PMP to be over an encrypted channel (SSL) or Non-SSL. If you choose, SSL mode, do the following. Otherwise, proceed to Step 2.

To enable the SSL mode, the LDAP server should be serving over SSL in port 636 and you will have to import the LDAP server's root certificate, LDAP server's certificate and all other certificates that are present in the respective root certificate chain into the PMP server machine's certificate store.

To import certificates, open a command prompt and navigate to <PMP_SERVER_HOME>\bin directory and execute the following command:

```
For Windows
importCert.bat <Absolute Path of certificate>
For Linux
importCert.sh <Absolute Path of certificate>
```

Restart PMP server. Then continue with the following steps.

2. Enter the url of the LDAP provider in the format attribute://ldap server host:port (Example ldap://192.168.4.83 <:389/)
3. Enter the credentials of any one of the user already present in LDAP for authentication. It should be in the format exactly how the user would have submitted their username

when authenticating to your application. For example, a typical entry would look something like: cn=Eric,cn=Users,o=adventnet,c=com

4. Enter the password of the user
5. This is the 'base' or 'root' from where directory lookups should take place. Enter the LDAP base (top level of the LDAP directory tree). Enter it exactly in the format used in your LDAP. No spaces are allowed between the commas or the '=' equal symbol and that entries are case sensitive
6. If you want to add only specific users from your LDAP directory, just perform a search using the appropriate search filter. For example, for adding only those users who belong to the category "Managers", a typical search filter would be like: ou=Managers,ou=Groups,o=adventnet,c=com
7. Enter the group name. While importing users from LDAP, PMP will automatically create a user group with all the imported users. If you enable synchronization, the user group will get synchronized based on the search filter created by you.
8. Select your LDAP server type
   Microsoft Active Directory (or)
   Novell eDirectory (or)
   OpenLDAP (or)
   Others
9. If your LDAP server belongs to the type Microsoft Active Directory/Novell eDirectory/OpenLDAP, you can select that type and click "Save".

If your LDAP server belongs to types other than Microsoft Active Directory/Novell eDirectory/OpenLDAP

If your LDAP server belongs to types other than Microsoft Active Directory/Novell eDirectory/OpenLDAP, yon need to enter three more details to authenticate the users:

- Enter the user login attribute in your LDAP structure in the text field for "Login Attribute". For instance, for LDAP making use of AD, the entry would be "sAMAccountName" and for OpenLDAP, the entry would be "uid". If you are using any other LDAP, make this entry in accordance with your LDAP structure.
- Enter the e-mail attribute for the users in your LDAP structure in the text field for "Mail Attribute". For instance, for LDAP making use of AD, the entry would be "mail". If you are using any other LDAP, make this entry in accordance with your LDAP structure.
- Enter the distinguished name attribute - that is the LDAP attribute that uniquely defines this object. For instance, for LDAP making use of AD, the entry would be "distinguishedName" and for OpenLDAP, the entry would be "dn". If you are using any other LDAP, make this entry in accordance with your LDAP structure.
- Click "Import". Soon after hitting this "Save" button, PMP will start adding all users from LDAP. During subsequent imports only the new users entries in LDAP are added to the

local database. During import, every user will be notified through email about their account, along with a password that will be used to login to PMP when LDAP authentication is disabled.

Configure Synchronization and Manage LDAP Server Details

(Feature available only in Enterprise Edition)

Whenever new users get added to the LDAP, there is provision to automatically add them to PMP and keep the user database in sync. This can be done from the 'LDAP Server Details' page. Click the button 'LDAP Server Details' in Step 1 in the UI. This UI has been designed to serve as an one-stop place for managing all configurations pertaining to the LDAP servers integrated with PMP.

- In the 'LDAP Server Details' UI, you can view the list of LDAP servers already integrated, integrate new LDAP servers, delete existing ones, edit entries and manage the entries pertaining to the LDAP servers.
- In addition, from the "Actions" section of this page,
    - you can edit the existing LDAP server details
    - you can configure user database synchronization. Enter the time interval at which PMP has to query the LDAP server to keep the user database in sync. The time interval could be as low as a minute or it can be in the range of hours/days.

- The users added to the PMP database will have the role as "Password Users". If you want to assign specific roles to specific users, proceed with Step 2 below.

Step 2 - Assign Roles

All the users imported from LDAP will be assigned the 'Password User' role by default. To assign specific roles to specific users,

- Go to Step 2 in the UI (Admin >> LDAP) and click the button "Assign Roles Now"
- In the UI that opens, all the Users imported from LDAP are shown in the LHS under the column "Password Users"
- Select the users for whom you wish to change the role and use the appropriate arrow button to assign them the role of "Password Administrator"or "Password User"
- Click "Save" and the required roles are set for the users

Step 3 - Enable Authentication

The final step is to enable LDAP authentication. This will allow your users to use their LDAP directory password to login to PMP. Note that this scheme will work only for users who have been already imported to the local database from AD.

Note: Make sure you have at least one user with the 'Administrator' role, among the users imported from LDAP.

Importing Users from a CSV file

If you have the list of users in a text file, you can import the same to PMP database. All the lines in the CSV file should be consistent and have the same number of fields. The entries should be in comma separated form. Apart from standard details such as First Name, Last Name, User Name, Email Address, Department, Location etc. you can also enable or disable two-factor authentication for specific users. If you want to do that, you need to put the text enabled for enabling two-factor authentication and disabled for disabling it. CSV files having extensions .txt and .csv are allowed.

To import users from a CSV file,

- Go to "Admin" >> "Users" >> "Import from CSV"
- Browse and select the file and click "Next"
- The user inventory of PMP contains six fields by default - First Name, Last Name, User Name, Email Address, Department and Location. Of these six, the first four fields are mandatory. In your CSV file, the entries could be present in any order. You can choose which field in the CSV file maps to the corresponding attribute of the PMP user account
- Click "Finish"
- The result of every line imported will be logged as an audit record. For troubleshooting errors during import, refer to the log file in the location <PMP_Home>\logs\user_import_errors.txt

Editing Users

You can edit the details pertaining to existing list of users to change details such as email id, access level, password policy, department and location. Also, you can enable or disable two-factor authentication for any user, anytime.

To edit users,

- Go to "Admin" tab and click "Users"
- The list of users will be displayed
- Click the "Edit" button present against the user. In the UI that pops-up, you can edit the first name, last name, mail id, access level, password policy, department and location of the user
- You can also enable/disable 'two-factor authentication' for the particular user
- When RSA SecurID is used as the second authentication factor, you need to ensure that the user name in RSA Authentication Manager and the corresponding one in PMP are same. In case, for the already existing RSA users, if the user name in PMP and in RSA Authentication Manager are different, you can do a mapping of names in PMP instead of editing the name in RSA. This can be done from here through "RSA SecurID UserName". (Assume the scenario that in PMP you have imported a user from Active Directory, who has the username (say) ADVENTNET\rob in PMP. In RSA Authentication Manager, assume that the username is recorded as 'rob'. In normal case, there will be mismatch of usernames between PMP and RSA Authentication Manager. To avoid that, you can do a mapping in PMP - ADVENTNET\rob will be mapped to rob).
- You can change 'Access Scope' to make an administrator/password administrator, a super administrator by choosing the option "All Passwords in the system". Conversely, a super administrator can be changed to his earlier role of administrator/password administrator by choosing the option"Passwords owned and shared".
- Click "Save" to give effect to the changes

Important Note: While changing the access levels/ access scope, the following rule would be applied:

If you are an Administrator, you will not be allowed to change your access level or scope (that means, the currently logged in administrator's access level cannot be changed). You will have to request another administrator to do the change.

Deleting Users

Administrators can delete those users who are no longer required. The delete operation is a permanent one and cannot be reverted.

Important Note:

(1) PMP will allow to delete users only if the user/users do not own any resource. If the user(s) own any resource, you need to first transfer the ownership of all the resources to some other Password Administrator.
(2) Currently logged-in user will not be permitted to delete himself/herself

To delete a user or users,

- Go to "Admin >> Users" tab
- Select the user/Users and click "Delete Users". The user will be deleted from the database once and for all
- Since the resources owned by the user have been transferred to other users prior to deletion, there will not be any loss of enterprise data. However, all the personal data stored by the user will be deleted once and for all. The audit trails will clearly capture all these changes and deletion. The audit trails depicting the activities of the user will remain unaffected in the database even after deleting the user. Audit trails will not be deleted.

How to delete the in-built 'admin' user?

Before proceeding to delete the admin user, check if the admin user owns any resources. If so, the resources should be transferred to another administrator/password administrator.

- Go to "Admin >> Users" tab
- Transfer all the resources owned by 'admin' to another administrator/password administrator
- If you have logged-in as the 'admin' user who has to be deleted, you will not be permitted to delete (currently logged-in user cannot be deleted)
- Place a request to some other administrator (other than the one to be deleted) to delete the 'admin' user.
- The above procedure holds good for deleting any user with the role administrator/password administrator

User Groups

Users can be grouped together for easier management. User grouping helps in carrying out operations in bulk on all the resources of the group. The resources added to PMP can be assigned to a user group.

To add user groups,

- Go to "Admin >> Users" tab in the web interface
- Click "User Groups" tab (alternatively, you can launch this page directly through the "User Groups" link in the "Links" tab)

In the Add User Group UI that opens,

- Enter a name for the user group
- Provide a description about the group being created. This would be helpful for future reference.
- From the list of users, search & select the ones to be added to the group. Click the icon to search for specific users
- Click "Save". The required group is created

What happens for a new user who gets added to an already existing group?

The new user will become part of that group and automatically inherit all the properties and permission levels of the group.

Importing User Groups from AD

You can import specific user groups and OUs from the active directory and retain the same user group structure in PMP. You can even choose to synchronize the user group structure in PMP with that of AD at periodic intervals. Refer to the section integrating active directory for more details.

Settings for User Groups

In order to achieve high level of security, PMP provides the option to configure the following settings for user groups:

Include passwords when resource details are exported to CSV format

When one exports PMP resources to a CSV file, by default, password of the accounts are included in plain text. In case, for security reasons, you wish not to allow the members of a user group to export passwords during resource import, you can do so from the group level setting:

- Go to Links >> Groups >> User Groups tab
- Click the icon "Settings" present against the required group
- Uncheck the checkbox against the field "Include passwords when resource details are exported to CSV format"
- Click "Save"

Allow to manage personal passwords

PMP provides personal password management feature as a value addition to individual users to manage their personal passwords such as credit card PIN numbers, bank accounts etc while using the software for enterprise password management. The personal password management belongs exclusively to the individual users. For security reasons, if you do not wish to allow personal password management for a group of PMP users, you can do so from the setting as explained below. Once you do this, the 'Personal' tab will not appear in the PMP GUI for all the members of that particular group.

- Go to "Links >> Groups >> User Groups" tab
- Click the icon "Settings" present against the required group
- Uncheck the checkbox against the field "Allow to manage personal passwords"
- Click "Save"

Allow to export personal passwords

PMP provides the option for users to export their personal passwords. For security reasons, if you do not wish to allow export of personal passwords for a group of PMP users, you can do so from the setting as explained below.

- Go to Links >> Groups >> User Groups tab
- Click the icon "Settings" present against the required group
- Uncheck the checkbox against the field "Allow to export personal passwords"
- Click "Save"

Permit group members to grant 'Manage Share' of their criteria-based resource groups to others

By default, 'Manage Share' for criteria-based resource groups is disabled. To enable it you need to carry out a configuration setting at the user group level.

The Reason

'Manage Share' for criteria-based resource groups is fraught with a risk of exploitation. There is a possibility that an administrator or password administrator could gain unauthorized manage permission for resources that are not allotted to them by intelligently creating a series of Resource Groups specifying certain matching criteria for the condition "Resource name contains".

How to Securely Enable it?

This can be enabled through a setting at the User Group level only. You need to do the following:

- Create a user group containing the administrators / password administrators who are to be permitted to do 'Manage Share' for criteria-based resource groups. (Links >> Groups >> User Groups tab)
- After creating the group, click the icon "Settings" present against that group
- Select the checkbox against the field "Permit group members to grant 'Manage Share' of their criteria-based resource groups to others" and click"Save"

Once you carry out the above setting, the members of that particular user group will be permitted to do "Manage Share" of their criteria-based resource groups. Thus, administrators can decide who can use 'manage' share and track the events.

Managing User Groups

Editing a User Group - Adding new users to the group, deleting existing users from the group

You can edit an existing user group to add more users to the group or remove existing users. To edit a user group,

- Go to Links >> Groups >> User Groups tab
- Click the icon "Edit" present against the required group
- All the users present in the system are listed in the GUI. The users who are already part of the group are shown selected (checkbox). If you want to add new users to the group, select the user. On the other hand, if you want to delete an existing user, uncheck the checkbox.
- Click "Save"

Deleting User Group

You can delete an existing user group in PMP. When you do so, the group will no longer exist. The group level settings done for that group will no longer apply for the users who were members of that group. Deletion of user group will not have any impact on the resources stored in PMP. The resource shares done for the group will vanish.

To delete a user group,

- Go to Links >> Groups >> User Groups tab
- Click the icon "Delete" present against the required group

Changing the PMP login password

Users having an account with the PMP, can change their own password and email ID. The "Edit Account settings" tab facilitates changing of password and email ID. Using this tab, the currently logged in user can change his/her password and email ID alone.

To Change Login Password,

- Go to "Admin" tab
- Go to "Change Password" in the "General" tab
- Enter the old password
- Enter new password. The new password you provide will have to be compliant to the password policy assigned to your account by your administrator. The password generator will generate passwords according to the assigned policy. The new password will NOT be emailed. Take care to remember your new password. If you forget your password, use the 'Forgot password' link available in the login page of PMP to reset your password.
- Confirm the new password
- Click "Save"
- Password is now reset

Note: If you do not want to display the 'Forgot Password' option, you can very well turn it off. See the section "General Optional Settings" for details.

Smartcard Authentication

(Feature available only in Enterprise Edition)

Overview

Since Password Manager Pro serves as the vault for sensitive passwords, it is essential to have a strong authentication mechanism to grant access to the software. PMP provides various authentication options and users can choose the ones that suit their environment better. Apart from PMP's local authentication, there is provision for leveraging the authentication of external identity stores such as Active Directory / LDAP.

To bolster the security further, PMP offers Smart Card Authentication, which makes the authentication stronger because, to get access to PMP, the user must possess the smart card and should know the personal identification number (PIN) as well.

Smart Card authentication in PMP serves as the Primary Authentication and it should not be confused with the Two Factor Authentication.

If you have a smart card authentication system in your environment, you can configure PMP to authenticate users with their smart cards, bypassing other first factor authentication methods like AD, LDAP or Local Authentication.

How Does Smart Card Authentication Work in PMP?

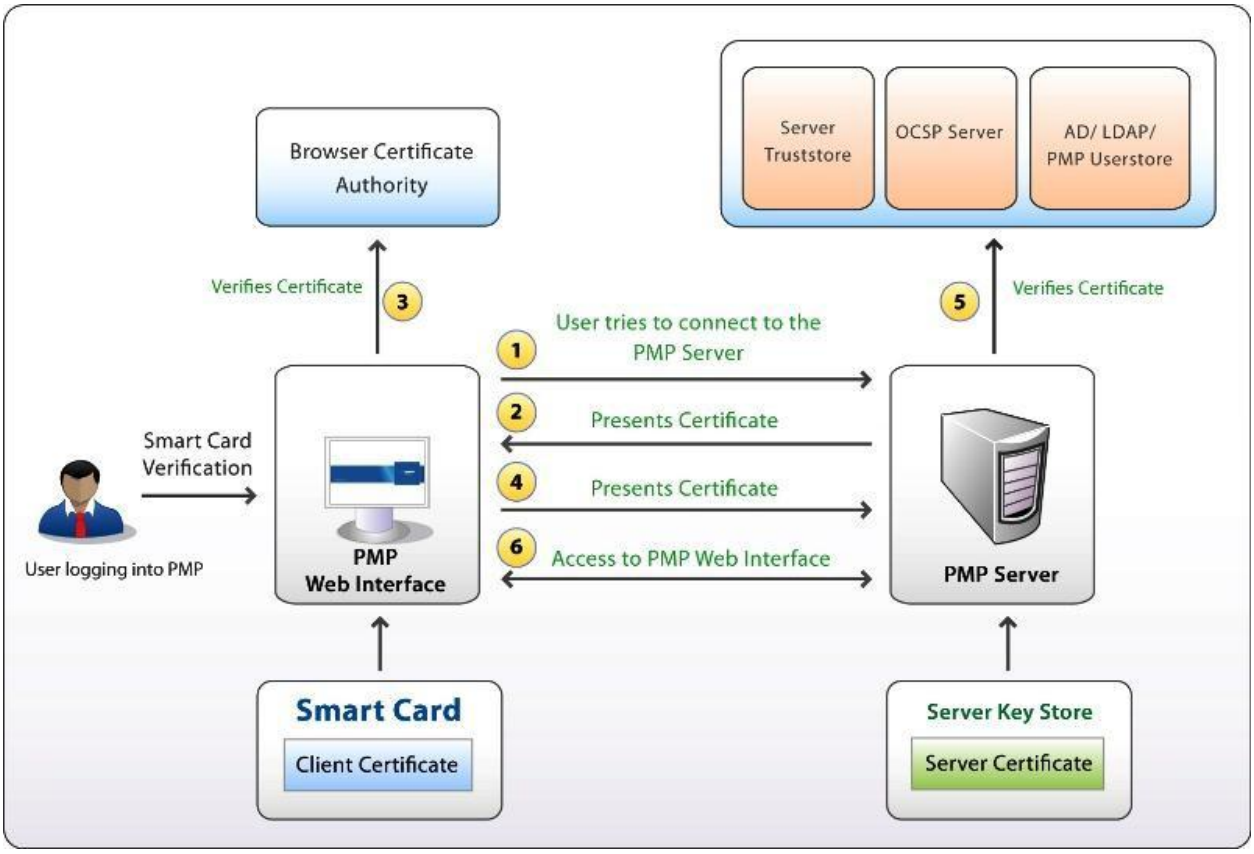
When the user attempts to access PMP web-interface, he would be allowed to proceed further only if he had already completed the smart card authentication in the machine by presenting the smart card and subsequently entering the PIN. PMP's web-interface supplements smart card technology with SSL communication. So, the user is prompted to specify their X.509 certificate for getting access.

The users can chose to provide the certificate from the smart card or the local certificate store, in which case PMP performs the steps to authenticate the user with the certificate.

The users can also choose to decline providing the certificate and PMP takes them to the usual login page for authentication.

Smartcard Authentication Workflow

- User tries to connect to the PMP server
- The PMP server presents its certificate to the client (web-inteface)
- The client verifies the server's certificate with that of the browser certificate authority
- If the above process is successful, the client sends the user's smartcard certificate to the server
- The server verifies the client certificate with the server's trustStore and then checks the revocation status with the OCSP server (if applicable); finally checks if the user certificate is same as the one in the AD/LDAP or PMP user store.
- If the above process also succeeds, the PMP server grants the user access to the web interface



Enabling Smart Card Authentication

Summary of Steps

- Importing the root of the CA in case of internal certificates (your own certificate). This is the certificate authority issuing the X.509 user certificates to the PMP users. If you are using a certificate signed by third-party CA, you may skip this step.
- Mapping user details between Smartcard Certificate and the PMP user store
- Configuring status check for user certificates
- User certificates verification for authentication
- Enabling Smart Card Authentication in PMP
- Restart PMP Server & Web Browser

Step 1 - Importing the Root of CA

In case, you are using an already available internal certificate (your own certificate), you need to specify the root of the CA. If you are using a certificate signed by third-party CA, you may skip this step.

To import the root of the CA,

1. Go to Admin >> Smart card / PKI / Certificate
2. In the UI that opens, click "Import Now" button in Step 1
3. Specify the path of the root of the CA
4. Restart PMP server

Once you execute the above, the root of the CA will be recorded in PMP. All the certificates signed by the particular CA will henceforth be automatically taken.

Step 2 - Mapping user details between smartcard certificate and PMP user store

The next step is to choose the mapping between the smartcard certificate and the PMP user database. That means, the attribute in the smartcard certificate that uniquely identifies the user should match with the corresponding value in the PMP user database.

This mapping involves two things:

1. Specifying which attribute in certificate should be taken up for comparison
2. Specifying the corresponding matching attribute in PMP user store

Specifying the certificate attribute

- PMP provides the flexibility to specify any attribute of the smartcard certificate that you feel uniquely identifies the user in your environment. You may choose any attribute among SAN.OtherName, SAN.RFC822Name, SAN.DirName, SAN.DNSName, SAN.URI and Common Name. During authentication, PMP reads the value corresponding to this attribute and compares it with the attribute in PMP user store.
- From the drop-down "Certificate Attribute", select the desired attribute.

Note: In case, in your environment, if any other attribute is used to uniquely identify the user, contact PMP support to add that attribute.

Specifying the matching PMP user name

After specifying the Certificate Attribute, you need to specify the mapping attribute in PMP user store. That means, you need to specify the particular attribute that uniquely identifies the user in PMP user store. This depends on how the user was added in PMP - whether by manual addition or imported from Active Directory / LDAP.

Users manually added

For the users manually added into PMP, username in PMP is probably the only attribute that could be taken up for comparison with the corresponding attribute in certificate. So, just leave this text field with the default value "username".

Users imported from Active Directory / LDAP

In the case of the users imported from Active Directory/LDAP, normally the attribute 'userPrincipalName' is used to uniquely identify the user. It is quite possible that in your environment, some other attribute like 'distinguishedName' might uniquely identify the user. So, specify the attribute accordingly.

Finally, Save the settings.

Step 3 - Configuring Status Check for User Certificates

During authentication, PMP checks for certificate revocation status against an Online Certificate Status Protocol (OCSP) server, with details available in the certificate itself. If some certificates do not have OCSP information, the information provided in the settings here will be used. This check can be disabled by changing the property ocsp.check to false in 'System Properties' file found in conf directory of PMP.

Also, authentication through OCSP will require access to the internet. In enterprise network setup, you might need to go through a proxy server to access the internet. You may specify proxy server settings if you have not specified it already.

Click the button "Configure Now" and enter OCSP server details such as OCSP server name, port and if required, the proxy server settings.

Step 4 - Comparing User Certificates for Verifying Authentication

Another step in the authentication process is comparison of the user certificates presented by the user and the ones stored in the system or Active Directory/LDAP. For the users who were added manually, the X.509 certificate stored in the PMP database will be compared with the one presented by the user.

Another step in the authentication process is comparison of the user certificates presented by the user and the ones stored in the system or Active Directory/LDAP. For the users who were added manually, the X.509 certificate stored in the PMP database will be compared with the one presented by the user.

Important Note:

In case, you do not have AD or LDAP in your environment, you need to manually put the x.509 format SSL certificate used for smartcard authentication into PMP.

- You can do this from Admin >> General >> Change Login Password GUI.
- Choose the option 'Change Certificate' to specify the path of the x.509 format SSL certificate

Step 5 - Enabling Smart Card Authentication

After carrying out the settings, you need to enable Smart Card Authentication. Before enabling this, you need to ensure that AD/LDAP authentication is disabled.

Click "Enable" to enable smart card authentication.

Step 6 - Restart PMP Server & Web Browser

After completing aforesaid steps, restart PMP server and the web server once to give effect to the settings. Whenever you enable or disable Smart Card authentication in PMP, you need to restart the server and the browser to give effect to the change.

Important Note:

- Once you enable Smart Card authentication, it will take effect globally - that means, Smart Card authentication will be applied to all the users. However, the users for whom Smart Card authentication is not applicable, will be prompted to use local authentication automatically. For those Smart Card authentication is applicable, they will be prompted to proceed with Smart Card authentication
- When Smart Card Authentication is enabled, AD or LDAP authentication will remain suspended for all users. So, you need to choose between AD, LDAP and Smart Card

Smart Card Authentication in PMP - Workflow

- User tries to access PMP web-interface
- The attribute that uniquely identifies the user in the smartcard certificate is compared with the corresponding attribute in PMP userstore.
- Then, the user certificate - the X.509 certificate stored in the PMP database in the case of users manually added will be compared with the one presented by the user.

In the case of users imported from Active Directory / LDAP, the certificate will be retrieved from AD/LDAP for comparison.

- If there is perfect matching, user is allowed access.

Smart Card Authentication in High Availability Scenario

If you have configured high availability and if you have enabled smart card authentication in Primary, the same has to be configured in the secondary server too.

To do this,

- Stop PMP primary server
- Connect to the PMP secondary server
- Go to Admin >> Users >> Smart Card Authentication
- In the UI that opens, perform Step 1 and Step 5 alone (for details, refer to the section 'enabling smart card authentication' above)
- Restart secondary after completing the above steps

Troubleshooting Tip

In case, you do not get the pop-up that prompts you to select the client certificate during authentication, try again after restarting the browser

Integrating RADIUS Server & Leveraging RADIUS Authentication

(Feature available only in Enterprise Edition)

You can integrate Password Manager Pro and RADIUS server in your environment and also leverage the RADIUS authentication for user access bypassing the local authentication provided by PMP. This section explains the configurations involved in integrating RADIUS server with PMP.

Step 1 - Providing Basic Details about RADIUS Server

To configure RADIUS server in PMP, provide the following basic details about RADIUS server and credentials to establish connection:

1. Go to "Admin" >> "Users" >> "RADIUS"
2. In the UI that opens, click the button "Configure" on step 1
3. In the UI that opens, provide the following details
4. Server Name/IP Address - enter the host name or IP address of the host where RADIUS server is running
5. Server Authentication Port - enter the port used for RADIUS server authentication. By default, RADIUS has been assigned the UDP port 1812 for RADIUS Authentication
6. Server Protocol - select the protocol that is used to authenticate users. Choose from four protocols - Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), Microsoft Challenge-Handshake Authentication Protocol (MSCHAP), Version 2 of Microsoft Challenge-Handshake Authentication Protocol (MSCHAP2)
7. Authentication Retries - select the number of times you wish to retry authentication in the event of an authentication failure
8. Server Secret - You have the option to enter the RADIUS server secret either manually in the text box or you can direct PMP to use the secret already stored in the product. In that case, you need to select the resource name and account name from the drop-down. The second option - storing the RADIUS password in PMP and selecting it from drop-down is the recommended approach.
9. Click "Save"

Step 2 - Enable RADIUS Authentication

After configuring the RADIUS server, the next step is to leverage the RADIUS server's authentication mechanism. To enable RADIUS authentication, click the button "Enable" in step 2. Once you do this, users would be able to login with their RADIUS credentials.

Important Note: The users who will be accessing PMP using their RADIUS server credentials, will have to be added as users in PMP first. When you do so, you need to ensure that the "user name" in PMP is exactly the same as the username used for accessing the RADIUS server. Here, PMP does not store the password used for RADIUS authentication.

Configuration for Single Sign-On using SAML

(Feature available only in Enterprise Edition)

ManageEngine Password Manager Pro (PMP) offers support for SAML 2.0, which facilitates integration with Federated Identity Management Solutions for Single Sign-On. PMP acts as the Service Provider (SP) and it integrates with Identity Providers (IdP) using SAML 2.0. The integration basically involves supplying details about SP to IdP and vice-versa. Once you integrate PMP with an IdP, the users have to just login to Okta and then, they can automatically login to PMP from the respective identity provider's GUI without having to provide credentials again. PMP supports out-of-the-box integration with Okta.

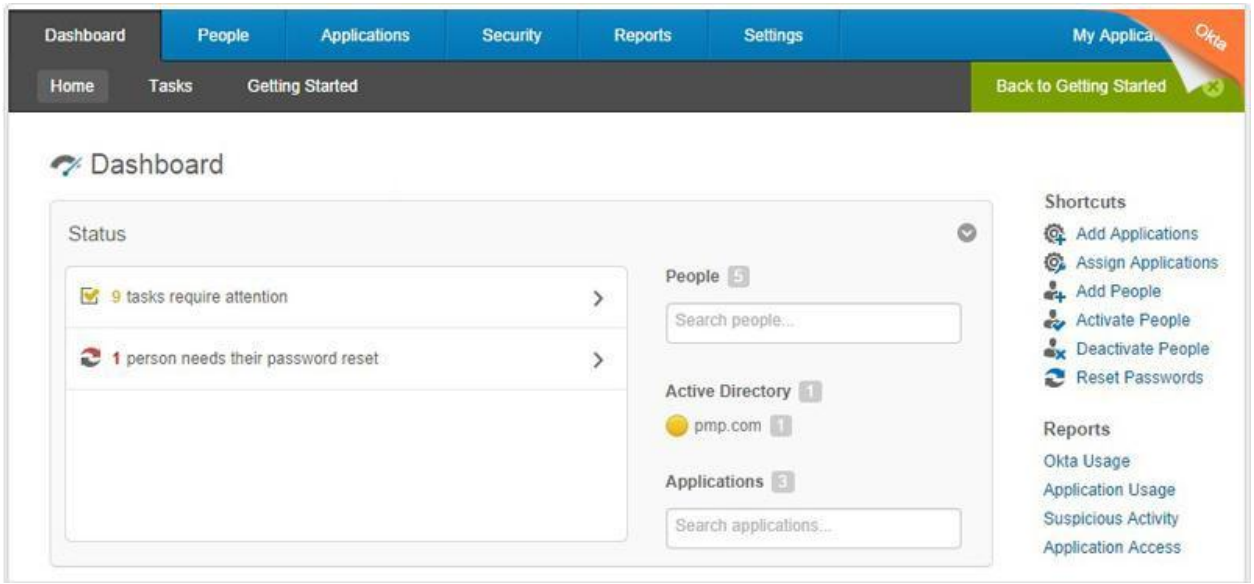
Steps to add PMP as an application in Okta:

Integrating PMP with Okta involves the following four steps:

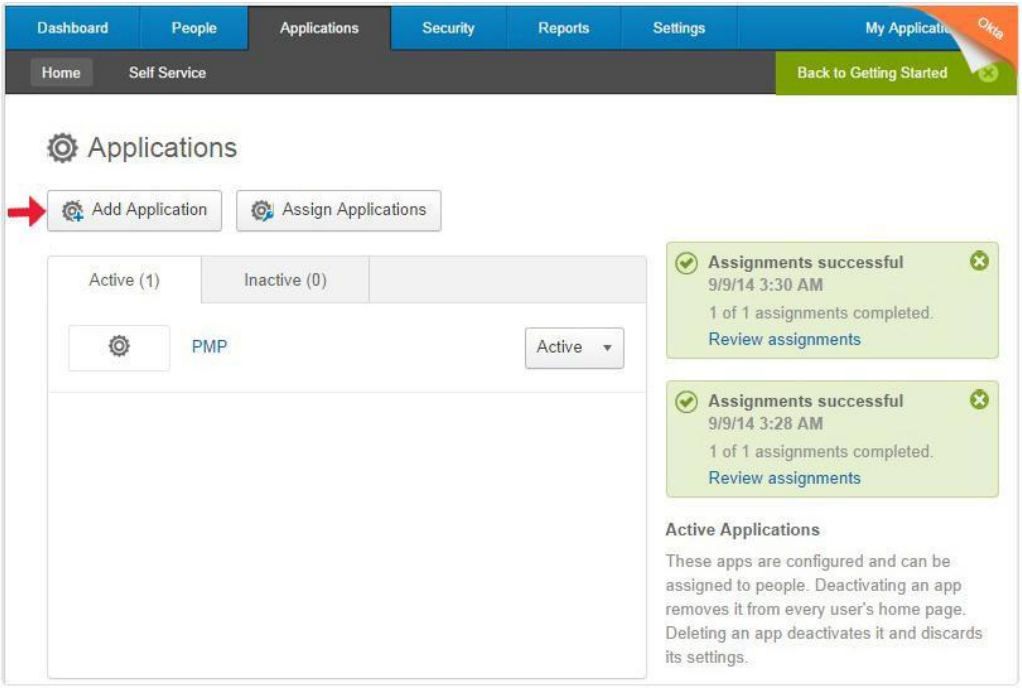
1. Adding Password Manager Pro as an application on the Okta dashboard
2. Configuring Okta details in Password Manager Pro
3. Assigning PMP Application to Users in Okta
4. Enabling SAML Sign On in Password Manager Pro

1) Adding Password Manager Pro as an application on the Okta dashboard.

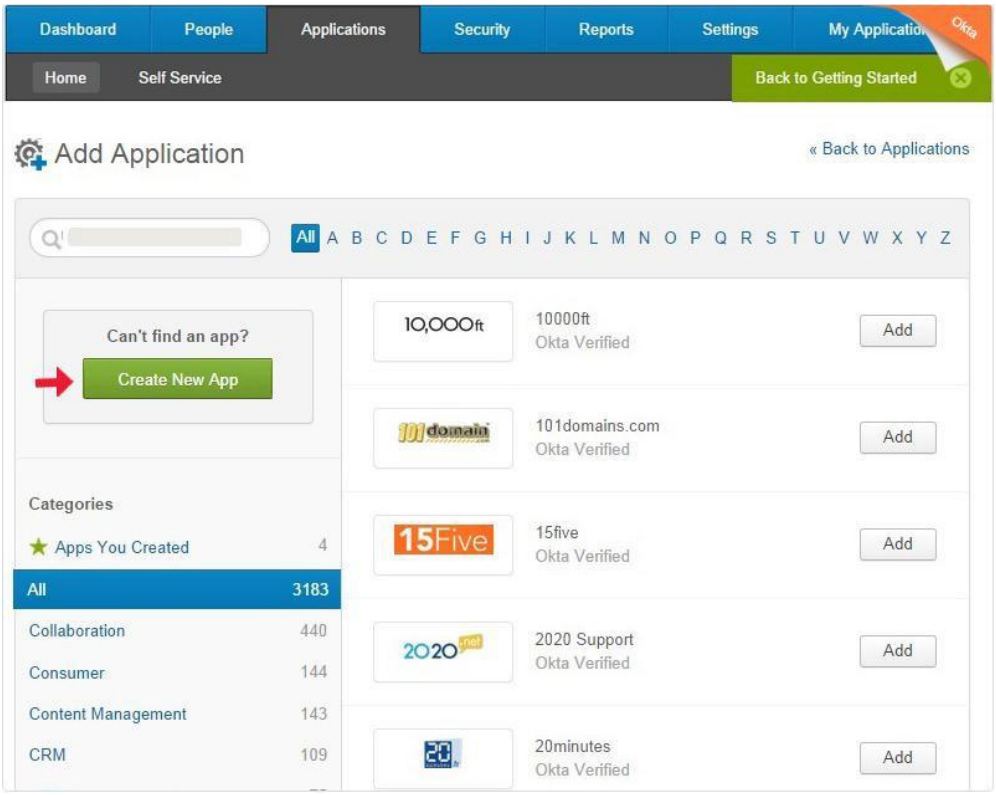
- Log in to your Okta Admin account and click 'Applications' tab.



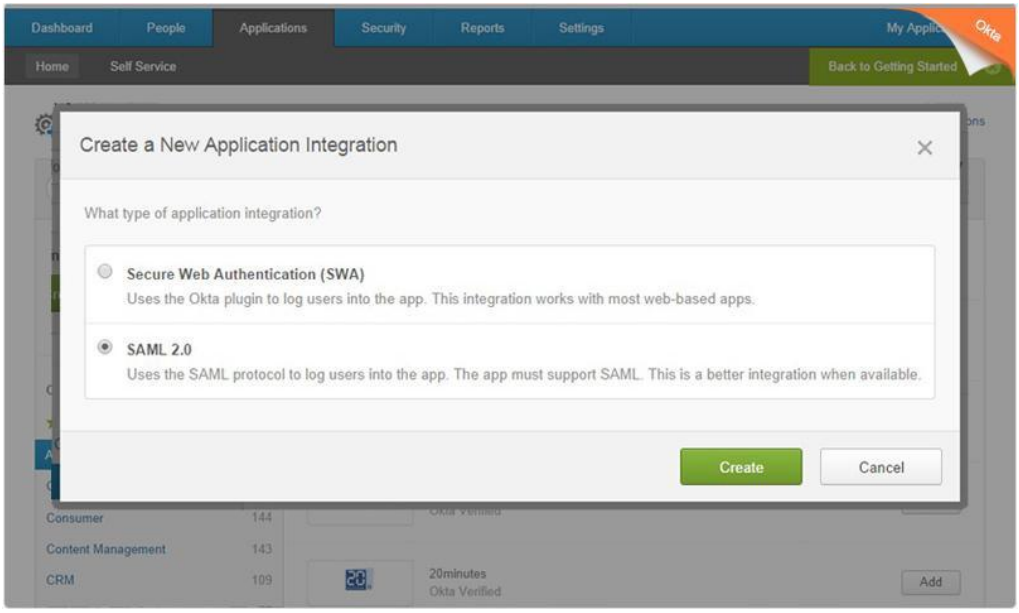
- In the new page that opens up, select 'Add Application'.



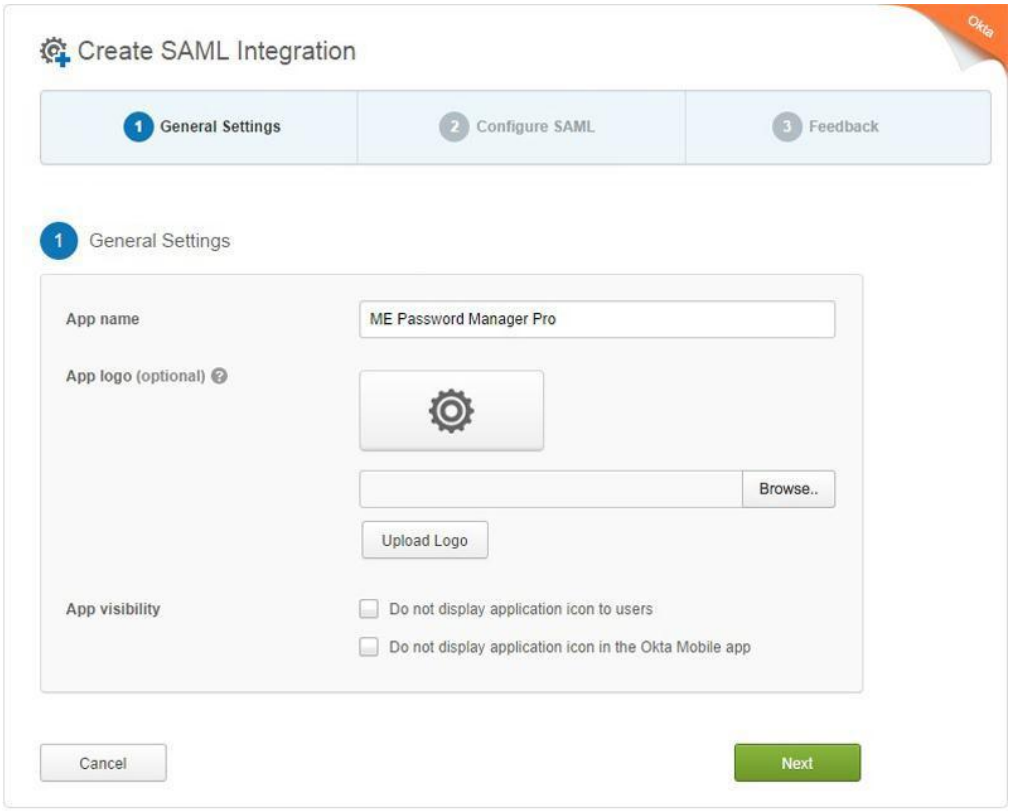
- As shown in the image below, click on 'Create New App'.



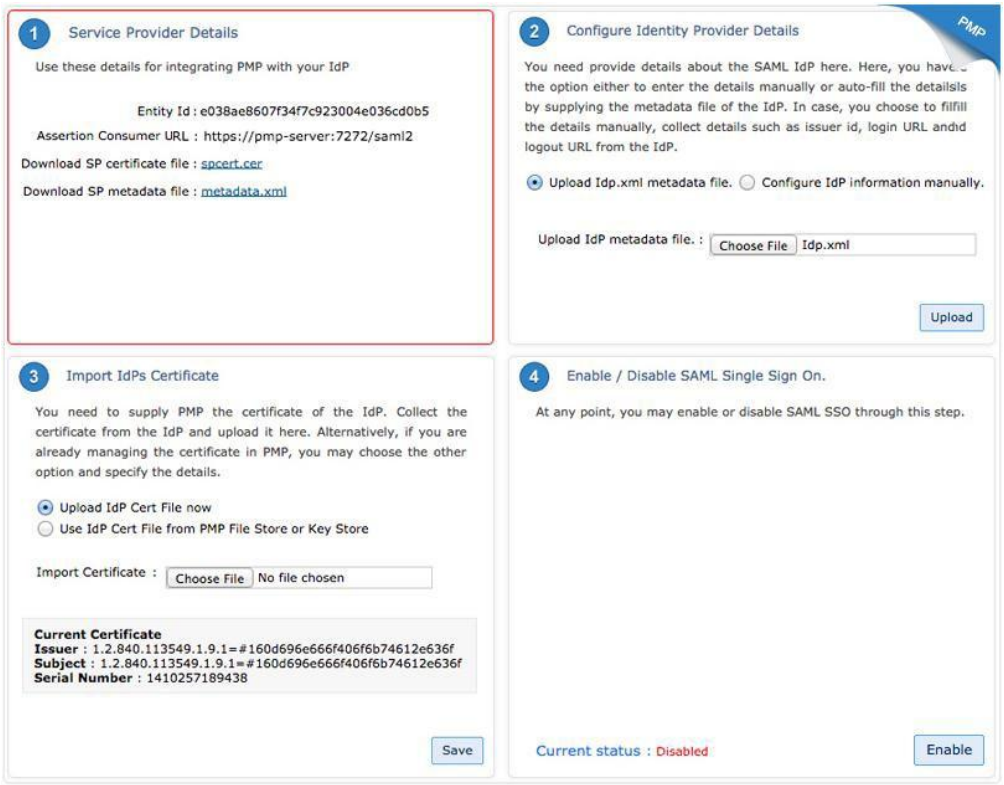
- Immediately, a window will pop-up asking information about the type of application integration. Choose ''SAML 2.0' and click 'Create'.



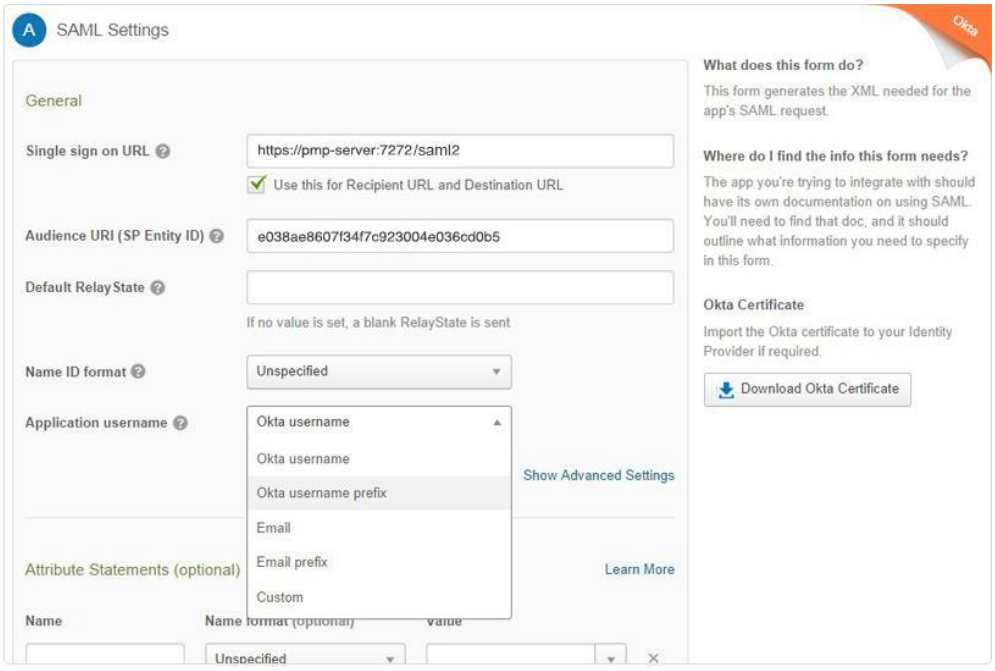
- Enter the name of the app being added (ME Password Manager Pro) as prompted under 'General Settings'. You can also optionally choose to upload a logo for the app. When you are done, click on 'Next'.



- The second step in configuring SAML integration consists of providing details about the Service Provider (ME PMP) to Okta. To access these details, go to PMP Homepage and select Admin >> SAML Single Sign On.



- The area highlighted in red contains the respective details titled as 'Service Provider Details'. Input these in the corresponding fields in Okta's SAML Settings page.

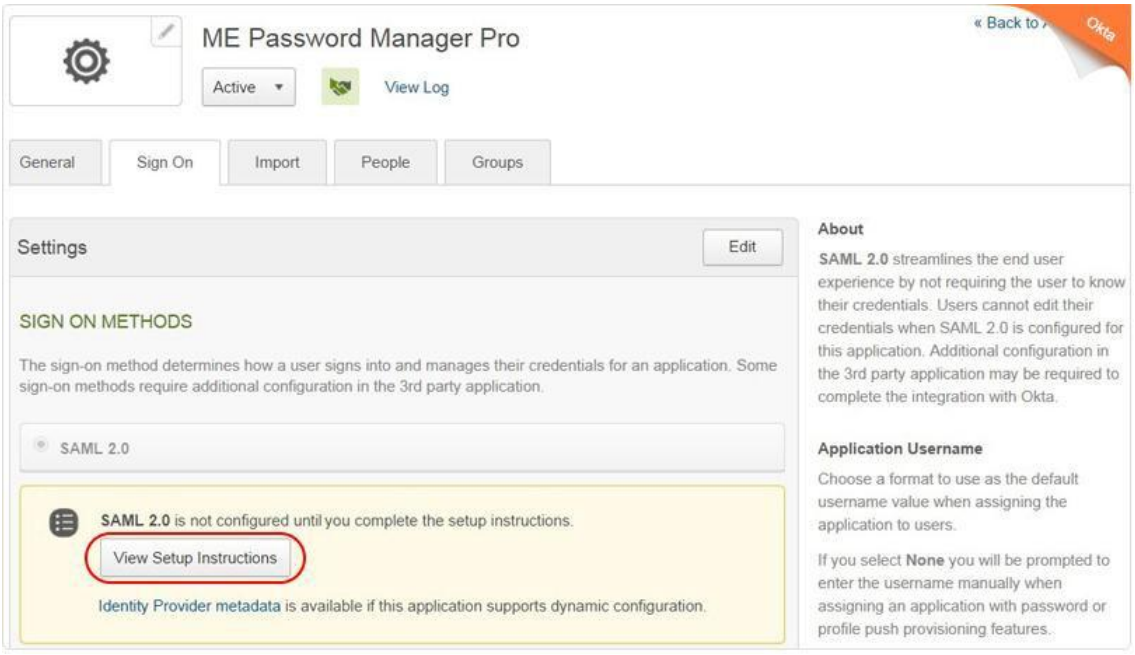


- After filling-in the Single Sign On URL and SP Entity ID (Audience URI) fields, you need to specify how you want Okta to recognize the names of your users in PMP. Since the way in which the usernames are displayed in Okta is different from how they are depicted in PMP, you have to specify the format. There are two scenarios here:

1. Scenario 1: If you have imported users from AD into PMP, they would have been imported in the format Domain\Username. For more help on integrating Okta with your on-premise AD, please check the help documentation of Okta available here. In Okta GUI, you need to choose the option "Custom" from the drop-down "Name ID format". Then, you should specify the custom format as given below:

```
${f:toUpperCase(f:substringBefore(f:substringAfter(user.login, "@"),
".")))}${"\\"}${f:substringBefore(user.login, "@")}
```

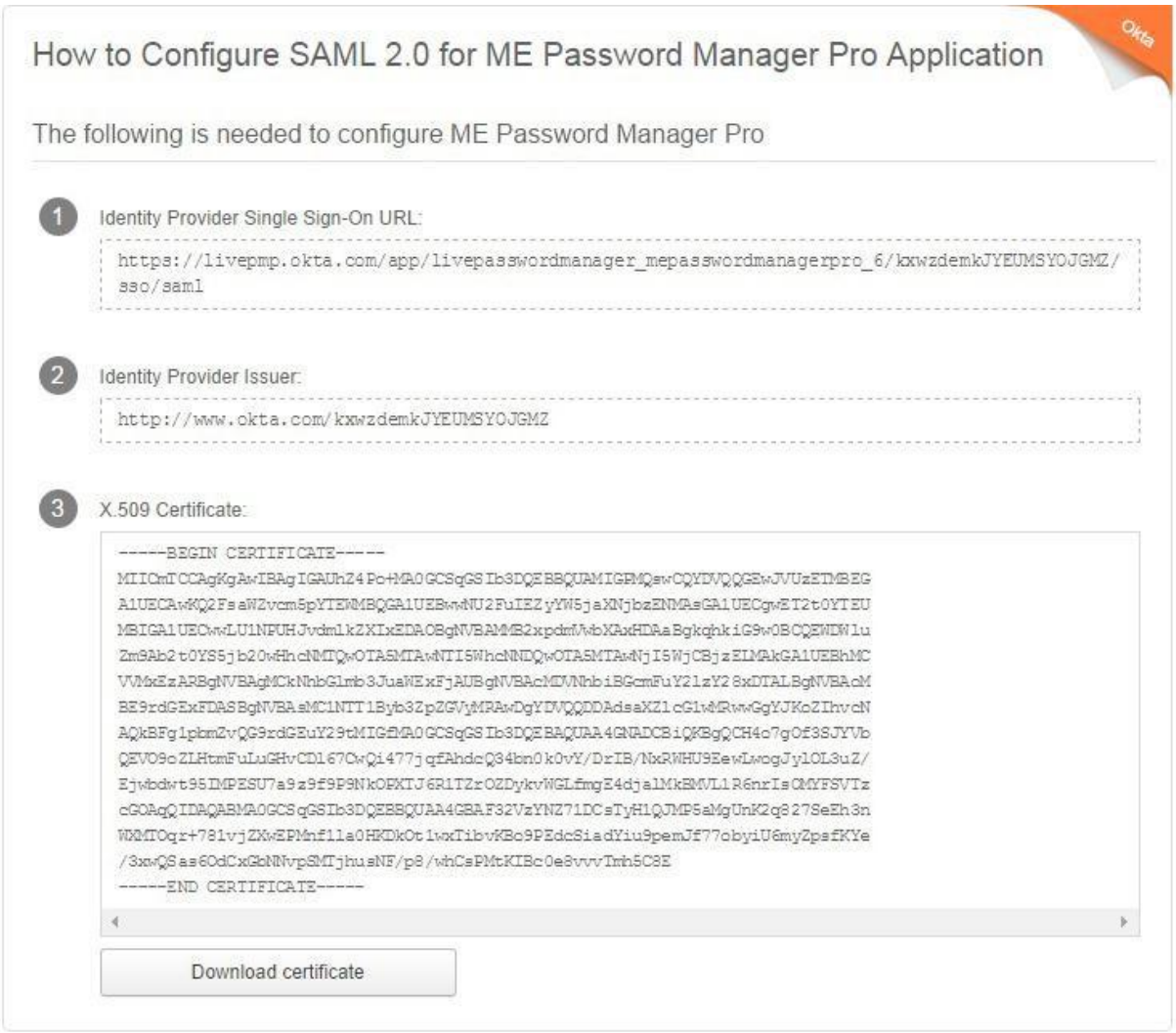
2. Scenario 2: If you have not used AD integration in PMP, you should select the option "Okta Username Prefix". This is because in Okta, user profiling is done in the format username@domain.com. But, in PMP, user names are depicted only as usernames. This step is crucial because, only if you specify the correct "Name ID format" in Okta, you will be able to assign the application (PMP) to other users in Okta.
   - Once you have filled in the required details as mentioned above, click 'Finish' to add the application. On addition, the application details will be displayed as shown in the image below. Click on 'Sign On' and then select 'View Setup instructions'. A new tab will open containing the details required to configure SAML 2.0 in PMP, which is discussed in the next step.

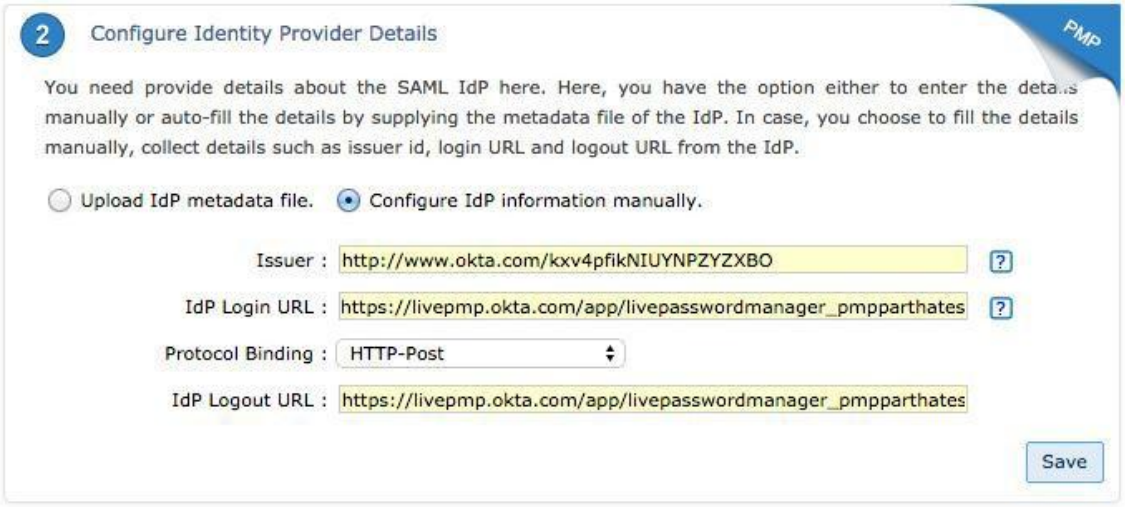


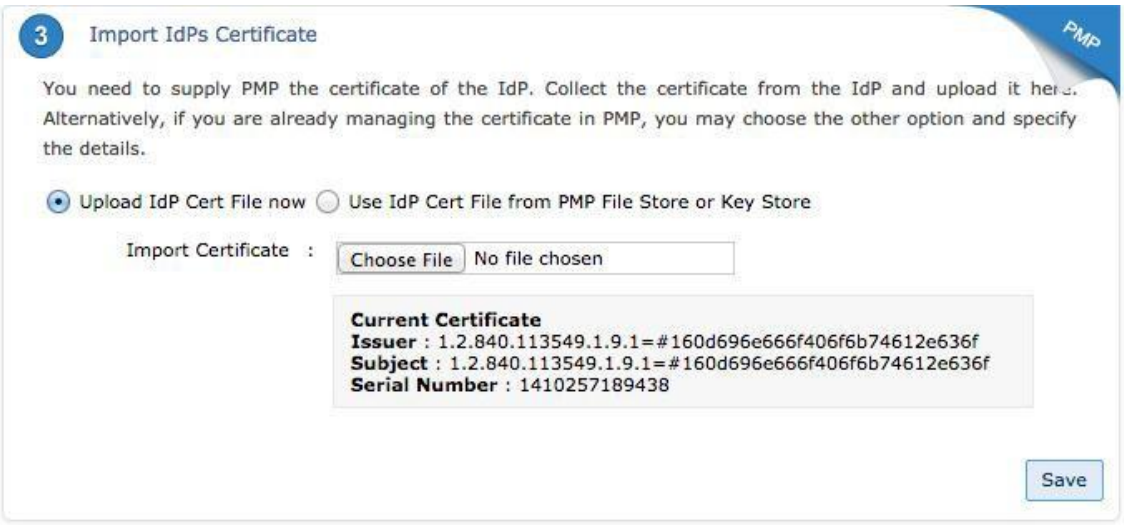
2) Configuring Okta details in Password Manager Pro

- You need to configure IdP details in PMP. This is done as part of the second step, 'Configure Identity Provider Details' in PMP's SAML Single Sign On page. Here, you have the option either to enter the details manually or auto-fill the same by supplying the metadata file from the IdP.

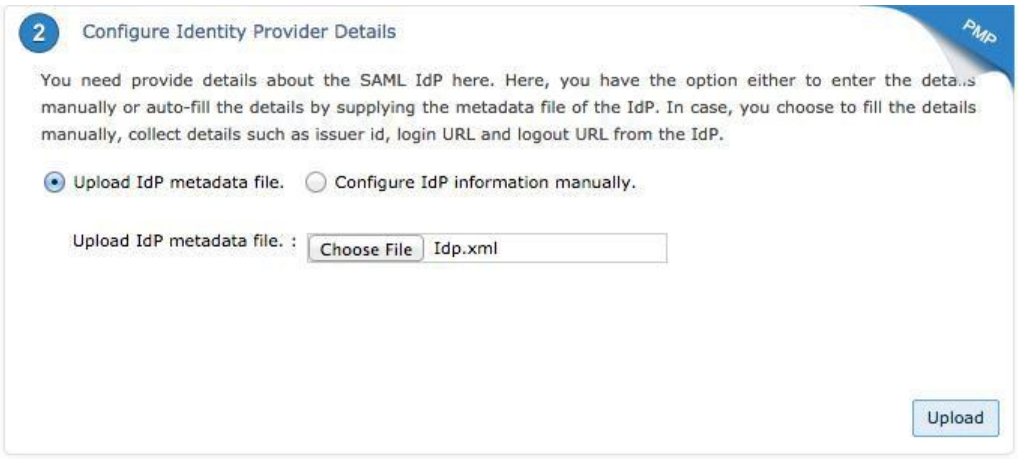
1. Manual Set-up: If you choose to fill the details manually, get the IdP details such as Issuer ID, Login URL, and Logout URL from the 'Setup Instructions' page of Okta. Configure the same in the step 2 given in PMP SAML Sign On configuration page. Enter the details in the corresponding fields and also download the Okta certificate and upload onto the PMP client (Listed as the 3rd step in the PMP GUI). Alternatively, you can also save the certificate file in the PMP File Store or Key Store and then use it here.





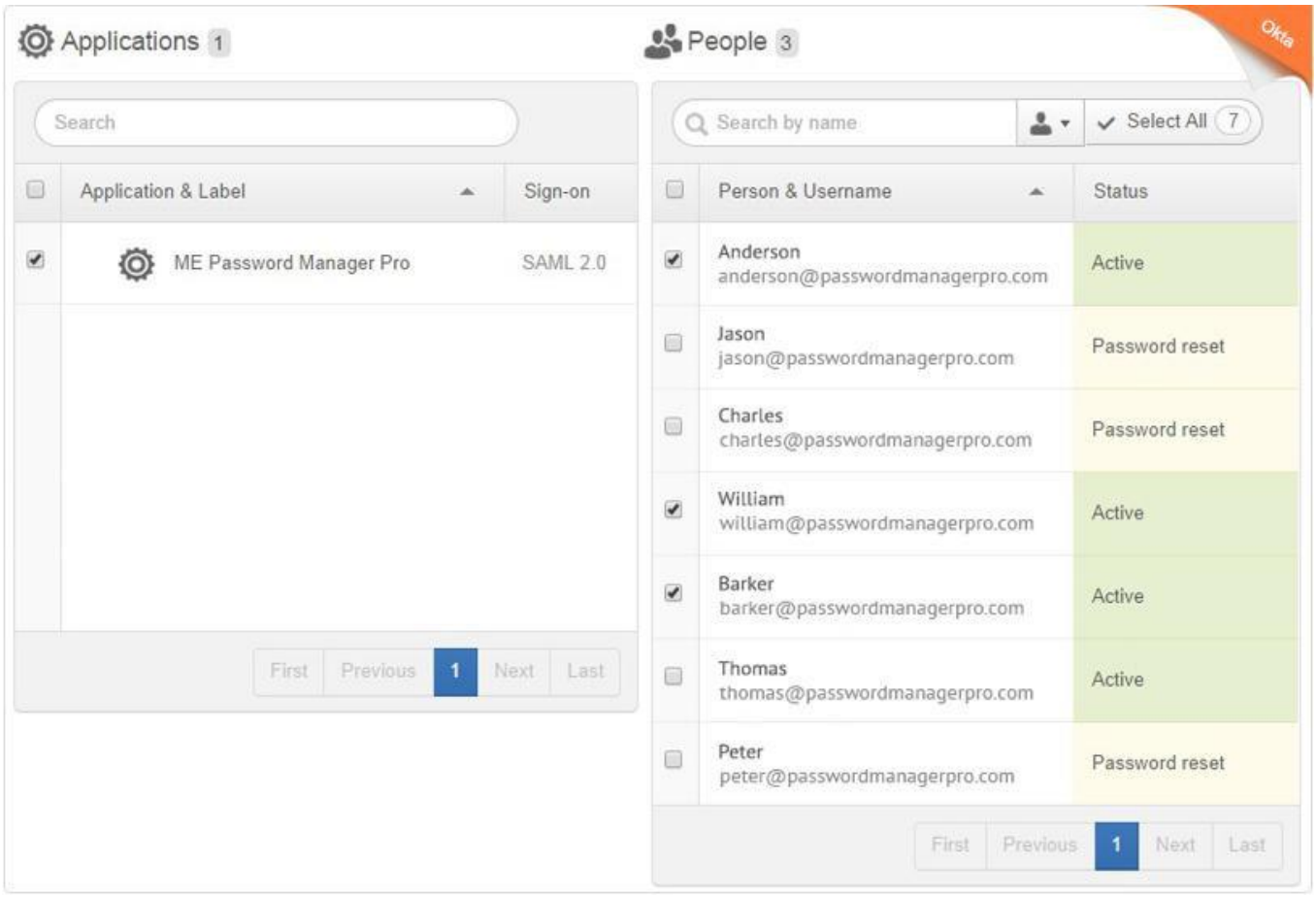


2. Auto-Filling with IdP Metadata File: Scroll down on the SAML 2.0 setup instructions page of Okta and you will find the IdP metadata under 'Optional'. Copy the text and save in a file with .xml extension. Now, upload the same .xml file onto the PMP client. In this case, you needn't import IdP certificate in PMP. It will be updated automatically.



3) Assigning Application to Users in Okta

After completing the configurations in PMP, go back to Okta to assign the newly added application to your users. Navigate to Applications --> Assign Applications and select the PMP app. Under People, select the desired users and confirm assignments.



4) Enabling SAML Sign On in Password Manager Pro:

The final step of this configuration is enabling SAML Single Sign On in Password Manager Pro. This would be shown as the 4th step in the SAML page in PMP GUI. Click 'Enable' shown at the bottom right to begin using this feature.

Two Factor Authentication

Overview

Password Manager Pro stores sensitive administrative passwords of enterprise resources in encrypted form in the database. Access to the data was earlier restricted by a single level of authentication - local authentication of PMP or the authentication of third party identity stores like ActiveDirectory or LDAP.

To introduce an extra level of security, PMP provides two factor authentication. Users will have to authenticate through two successive stages to access the PMP web-interface. While the first authentication will be through the usual native authentication or AD / LDAP, the second level of authentication could be one of the following:

- Leveraging PhoneFacotor - a phone-based authentication service
- Leveraging RSA SecurID authentication as the second level of authentication
- A one-time, randomly generated unique password sent by PMP to the user by Email
- Google Authenticator

This section explains how to enable two factor authentication in PMP.

Enabling Two Factor Authentication

Enabling two factor authentication in Password Manager Pro consists of two steps:

- Setting up two factor authentication
- Specifying the users for whom the two factor authentication is to be enforced

Note: Two factor authentication will take effect only if both the two steps are performed. Also, two factor authentication will be applicable only for the users for whom it is enforced through Step 2. All other users will be allowed to login to PMP through the usual way.

Two Factor Authentication - Various Options

Before enabling the two factor authentication, decide on the technology you wish to use. At present PMP supports TFA through the following four options:

- PhoneFactor Authentication
- RSA SecurID
- Unique password generated and sent through Email
- Google Authenticator

Click the respective links to know more and proceed setting up the required TFA technology.

PhoneFactor Authentication

(Feature available only in Premium and Enterprise Editions)

Overview

ManageEngine has partnered with PhoneFactor, the leading global provider of phone-based two-factor authentication, to enable simple, effective two-factor security for Password Manager Pro. ManageEngine is a PhoneFactor Alliance Partner and offers seamless integration with PhoneFactor's authentication services.

PhoneFactor works by placing a confirmation call to your phone during the login process. Upon completing your first authentication through usual means and when you go to the second authentication stage, you simply need to answer your phone and press # (or enter a PIN), which serves as the phone-based authentication.

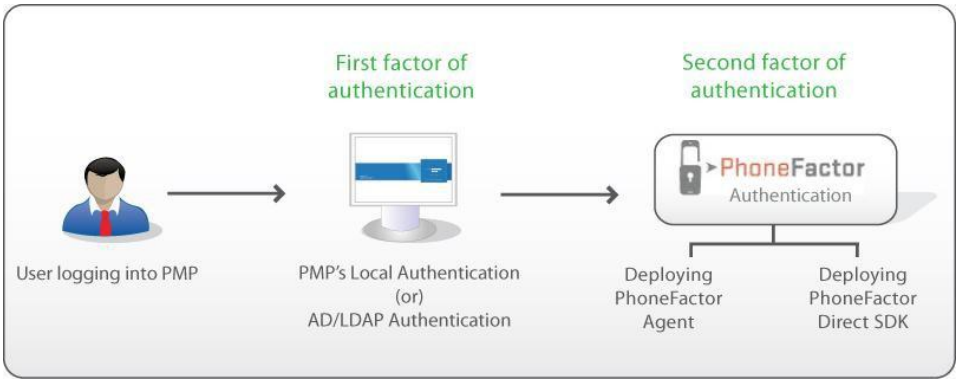
Following is the sequence of events involved in PhoneFactor Authentication:

1. A user tries to access PMP web-interface
2. PMP authenticates the user through Active Directory or LDAP or locally
3. PMP prompts for the second factor credential through PhoneFactor
4. PhoneFactor calls you. Answer the call and press # (or enter a PIN)
5. PMP grants the user access to the web-interface

Enabling PhoneFactor Authentication

Prerequsite

Prior to enabling PhoneFactor authentication, you need to buy PhoneFactor. Refer to PhoneFactor website for details. After getting PhoneFactor, you need to decide about the specific authentication method - whether you want to install PhoneFactor agent in your environment or deploy PhoneFactor Direct SDK.



How Does PhoneFactor Work with PMP?

You will be specifying the phone numbers for your users, which results in a mapping between the users and the corresponding phone numbers. In PhoneFactor agent mode, the details about the user, including the phone numbers are maintained at the agent. In Direct SDK mode, the phone numbers are maintained in PMP database itself. When a user tries to login to PMP, PhoneFactor finds out the phone number of the respective user and triggers a call.

To enable two-factor authentication using PhoneFactor, you need to follow the steps detailed below:

Summary of Steps

1. Setting up two factor authentication in PMP
2. Deciding the type of PhoneFactor authentication & associated configuration
3. Enforcing two factor authentication for required users in PMP

Step 1: Setting up Two Factor Authentication in PMP

The first step is to enable two factor authentication. To do that,

1. Go to "Admin" tab and click "Two Factor Authentication"
2. Choose the option "PhoneFactor"

Note: Before proceeding further, ensure that you have entered the phone numbers for all the users for whom you wish to enable two factor authentication through PhoneFactor in Password Manager Pro. You can enter a landline number or a mobile number as the primary contact number for PhoneFactor authentication.

Landline numbers should be entered in the following format:

<Country Code> <Phone Number with Area Code> <Extension Number, if any>
Example: 1 9259249500 292
Mobile numbers should be entered in the following format:
<Country Code> <Mobile Number>

Step 2: Choose the Authentication Method

You can choose to deploy PhoneFactor Agent or PhoneFactor Direct SDK.

PhoneFactor Agent

The PhoneFactor agent runs on a Windows server within your network. It includes a configuration wizard that guides you through the setup process for securing Password Manager Pro with PhoneFactor. The PhoneFactor agent can also integrate with your existing Active Directory or LDAP server for centralized user provisioning and management. All user data is stored within the corporate network for additional security. Extensive logging is available for reporting and auditing.

Direct SDK

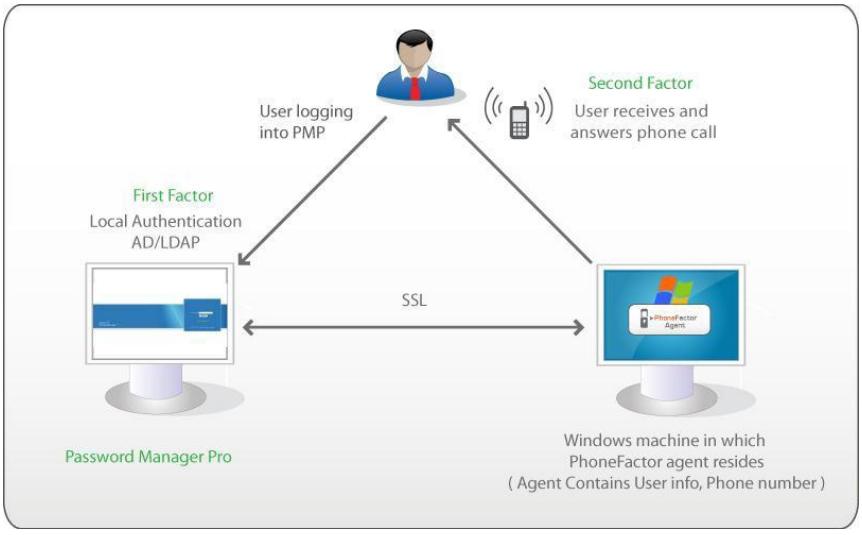
Instead of using the Agent, you can also use PhoneFactor Direct SDK, which can be used to integrate with Password Manager Pro and it leverages PMP's existing user database.

Note: Among the choices above, PhoneFactor agent supports entering a PIN for authentication while answering the phone call from PhoneFactor. In Direct SDK mode, users will just be prompted to enter the # key and not a PIN.

If you choose to deploy PhoneFactor agent

(Note: If you have already installed PhoneFactor agent, you may skip Step 1 below and directly proceed to Step 2).

Obtain and install the PhoneFactor Agent and Web Services SDK on a Windows server within your network. The wizard will guide you through the installation process.



Step 1: Configurations in PhoneFactor agent

- Since the phone numbers of the users are maintained in the PhoneFactor agent, after installing it, you need to add all the PMP users (for whom two factor authentication through PhoneFactor has been enabled in PMP) in the agent and enter their phone numbers too. You can also integrate Active Directory / LDAP with PhoneFactor agent and automatically import users. If you have users authenticated through PMP's local authentication, add them to PhoneFactor manually providing details about the phone number
- While adding users in the PhoneFactor agent, take care to provide the same username as available in PMP. (In PMP, you would have provided a 'PhoneFactor username' for the users who will be authenticated by PhoneFactor. Take care to enter the same username here in PhoneFactor agent configuration)
- After importing users, check if the phone numbers have been entered in the correct format

Important Note: User information and their phone numbers are maintained in PhoneFactor agent. That means, users will receive the call only at the phone numbers specified in the agent. Whenever, you want to modify the phone number, you need to carry out the change at the agent. Similarly, whenever you add new users to PMP and if TFA through PhoneFactor is enabled for them, you need to add the user in PhoneFactor agent too. Otherwise, TFA through PhoneFactor will not work.

Step 2: Configurations in PMP

- In the Two Factor Authentication GUI in PMP, select the Authentication Method as "PhoneFactor Agent"
- Enter the credentials to access the PhoneFactor. You need to enter the user name, password and the URL of the host where the PhoneFactor agent is running
- Communication between PMP and the host where the PhoneFactor agent is running takes place through SSL. So, you need to import (into PMP) the SSL certificate, which you specified while installing the Web Services SDK.

While installing the PhoneFactor agent/ Web Services SDK, you would have either created a self-signed SSL certificate or you would have used an already available internal certificate (your own certificate). Here, in PMP, you need import the root of the CA. If you are using a certificate signed by third-party CA, you may skip this step.

To import the root of the CA,

- Navigate to "PMP_Installation_Folder>/bin" directory
- Execute importPhoneFactorCert.bat (in Windows) orimportPhoneFactorCert.sh (in Linux) as follows

(In Windows)
In the case of Self-signed certificates
importPhoneFactorCert.bat <absolute path of the Self-signed certificate>

In the case of your own certificates or already available internal CAs
importPhoneFactorCert.bat <absolute path of the root of the CA>

(In Linux)
In the case of Self-signed certificates
sh importPhoneFactorCert.sh <absolute path of the Self-signed certificate>

In the case of your own certificates or already available internal CAs
sh importPhoneFactorCert.sh <absolute path of the root of the CA>

- Restart PMP server
- Once you execute the above, the root of the CA will be recorded in PMP. All the certificates signed by the particular CA will henceforth be automatically taken.
- Proceed to Step 3 - Enforcing Two Factor Authentication for required users in PMP.

Note: If your enterprise network setup requires connecting to the internet via a proxy server, you need to configure the proxy settings to enable PMP connect to PhoneFactor website. (PMP GUI >>> Admin >>> General >>> Proxy Server Settings)

If you have configured PMP High Availability: Configurations in PMP Secondary

(PhoneFactor Agent Mode)

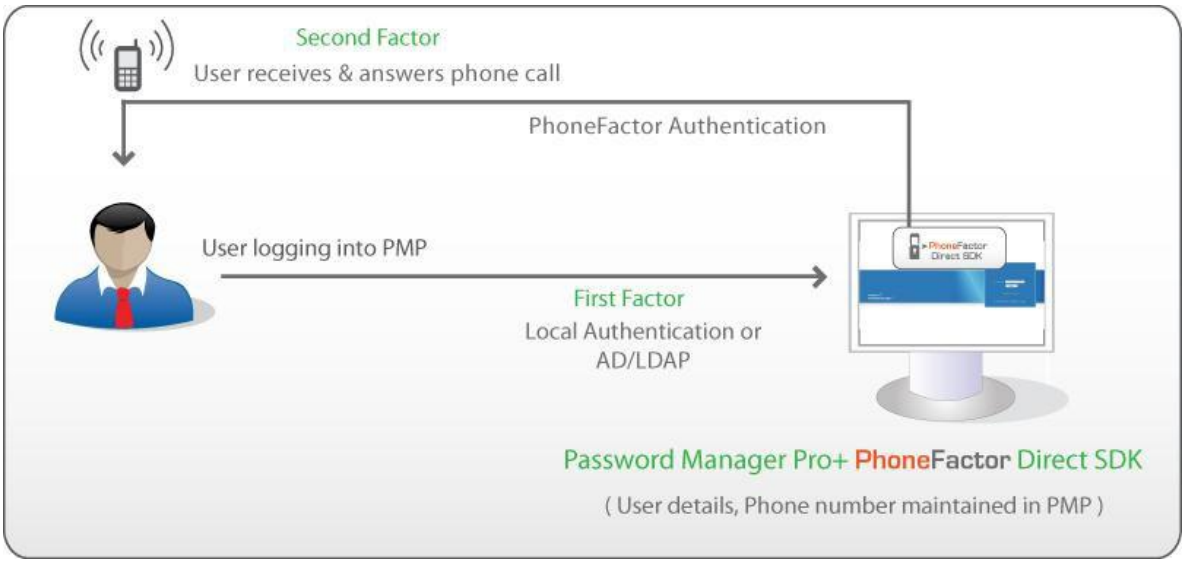
If you have configured High Availability in PMP and if you chosen to deploy PhoneFactor Agent, you need to carry out the following configuration in PMP Secondary server. Just as you imported the root of the CA as explained above, you need to do the same in the PMP secondary. If you are using a certificate signed by third-party CA, you may skip this step.

If you choose to deploy PhoneFactor Direct SDK

Step 1: Configurations in SDK

PhoneFactor jars have been bundled with Password Manager Pro. So, it is enough if you buy PhoneFactor and supply the license details as explained in Step 2 below.

Step 2: Configurations in PMP GUI



- Check the PMP users and ensure that you have entered phone numbers for all the users for whom you wish to enable two factor authentication through PhoneFactor in Password Manager Pro. The phone numbers should be entered in proper format. In sharp contrast to PhoneFactor agent where the phone numbers of the users are recorded and maintained at the agent, in the case of Direct SDK, phone numbers are maintained at PMP itself.
- In PhoneFactor GUI, you need to specify the path of PhoneFactor license file, PhoneFactor Certificate and Private Key password. (These files will be present under the PhoneFactor SDK folder.)
- Proceed to Step 3 - Enforcing Two Factor Authentication for required users in PMP.

Note: If your enterprise network setup requires connecting to the internet via a proxy server, you need to configure the proxy settings to enable PMP connect to PhoneFactor website. (PMP GUI >>> Admin >>> General >>> Proxy Server Settings)

If you have configured PMP High Availability: Configurations in PMP Secondary (PhoneFactor Direct SDK Mode)

If you have configured High Availability in PMP and if you chosen to PhoneFactor Direct SDK mode, you need to carry out the following configuration in PMP Secondary server.

- Go to <PMP-Primary-Installation>/licenses folder
- Copy the files license.xml and cert.p12
- Now go to <PMP-Secondary-Installation>/licenses folder
- Paste these two files

Step 3: Enforcing Two Factor Authentication for Required Users

In step 1&2 above, you have chosen PhoneFactor as the option for two factor authentication. After choosing this option, you need to apply two factor authentication for the required users.

To enforce two factor authentication for a user,

- Go to "Admin" >> "Users"
- Click the button "Set 2-factor authentication"
- In the UI that opens, select the users for whom two factor authentication is to be enforced
- Click "Save"

How to connect to PMP Web-Interface when TFA through PhoneFactor is Enabled?

The users for whom two factor authentication is enabled, will have to authenticate twice successively. As explained above, the first level of authentication will be through the usual authentication. That is, the users have to authenticate through PMP's local authentication or AD/LDAP authentication.

When TFA is enabled, the login screen will ask for the username alone in the first UI. The users will be prompted to enter the passwords only in the second step.

TFA using PhoneFactor - Workflow

If the administrator has chosen TFA throgh phoneFactor, the two factor authentication will happen as detailed below:

- Upon launching the PMP web-interface, the user has to enter the username to login to PMP and click "Login"

- Against the text field "Password", the user has to enter the local authentication password or AD/LDAP password as applicable

- Once the authentication through the first factor is successful, you need to await a call to your phone from the PhoneFactor
- Answer the call and press # key or enter the PIN as instructed. PhoneFactor will take care of authentication.

If you have configured High Availability

Whenever you enable TFA or when you change the TFA type (PhoneFactor or RSA SecurID or One-time password) AND if you have configured high availability, you need to restart the PMP secondary server once.

Setting up Two Factor Authentication - Unique Password Generated Through Email

Step 1: Enabling Two Factor Authentication

The first step is to enable two factor authentication. To do that,

- Go to "Admin" tab and click "Two Factor Authentication"
- Choose the option "Unique password generated and sent through Email"

Unique Password Generated Through Email

If you choose this option, after the first level of authentication through the usual way, Password Manager Pro will randomly generate a unique password and it will be emailed to the user. The user has to enter the second password sent by email to authenticate at the second level. The second level password generated and sent by PMP is applicable only for that particular session of the web-interface. If the user logs out and tries to login again, he will not be allowed to login with the same password sent by email earlier. The user has to fetch the password sent by email again and enter it for authentication.

Step 2: Enforcing Two Factor Authentication for Required Users

In Step 1 above, you have chosen the required option for two factor authentication. After choosing this option, you need to apply two factor authentication for the required users.

To enforce two factor authentication for a user,

1. Go to "Admin" >> "Users"
2. Click the button "Set 2-factor authentication"
3. In the UI that opens, select the users for whom two factor authentication is to be enforced
4. Click "Save"

How to connect to PMP Web-Interface when TFA is Enabled?

The users for whom two factor authentication is enabled, will have to authenticate twice successively. As explained above, the first level of authentication will be through the usual authentication. That is, the users have to authenticate through PMP's local authentication or AD/LDAP authentication. Depending on the type of TFA chosen by the administrator, the second level of authentication will differ as explained below:

Note: When TFA is enabled, the login screen will ask for the username alone in the first UI.

The users will be prompted to enter the passwords only in the second step.
If the administrator has chosen the TFA option "Unique password generated and sent through email", the two factor authentication will happen as detailed below:

1. Upon launching the PMP web-interface, the user has to enter the username to login to PMP and click "Login"
2. Then the user has to enter the local authentication password or AD/LDAP domain password as applicable
3. Once the first level of authentication succeeds, PMP will generate a random password and email it to the user
4. The user has to fetch email and copy the second password and enter it as the second password
5. If the second authentication succeeds, the user will be allowed to view the PMP web interface

Note: The second level password generated and sent by PMP is applicable only for that particular session of the web-interface. If the user logs out and tries to login again, he will not be allowed to login with the same password sent by email earlier. The user has to fetch the password sent by email again and enter it for authentication.

If you have configured High Availability

Whenever you enable TFA or when you change the TFA type (PhoneFactor or RSA SecurID or One-time password) AND if you have configured high availability, you need to restart the PMP secondary server once.

Setting up Two Factor Authentication - RSA SecurID

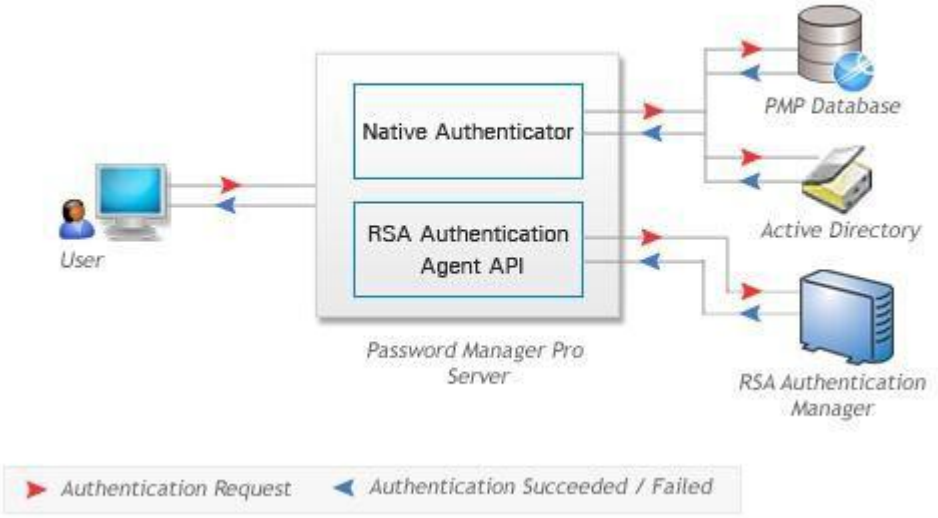
(Feature available only in Premium and Enterprise Editions)

Step 1: Setting up Two Factor Authentication
The first step is to enable two factor authentication. To do that,

1. Go to "Admin" tab and click "Two Factor Authentication"
2. Choose the option "RSA SecurID"

RSA SecurID
If you have RSA Authentication Manager and RSA SecurID Appliance in your environment, you can integrate them with PMP and leverage the RSA SecurID authentication as the second level of authentication.

For RSA SecurID authentication, PMP communicates with RSA Authentication Manager using the RSA APIs. PMP sends the user credential to RSA Authentication Manager, which validates and sends back the status to the PMP server.



PMP - RSA SecurID Integration

Following are the important steps involved in PMP-RSA SecurID Integration.

- Register the PMP server as an Agent Host in the RSA Authentication Manager
- Generate RSA Authentication Manager configuration file, or sdconf.rec in RSA manager. Copy and paste the sdconf.rec to the<PMP_Installation_Folder>/bin directory. In addition, if a node secret file (securid) exists, copy that as well

- Edit 'RSA_AGENT_HOST' property value as PMP server hostname or IP Address in the RSA Authentication API configuration file (rsa_api.properties) which is located in the default application directory (<PMP Home>\bin)

Important Note: If you are making use of PMP high availability feature, you need to carry out the above steps in the secondary server installation as well.

Two-factor Authentication using RSA SecurID - Flow of Events

Before authentication can take place, use the RSA Security Console to enter all desired PMP users into RSA Authentication Manager, assign tokens to them and activate them on the appropriate Agent Host. Ensure that the user name in RSA Authentication Manager and the corresponding one in PMP are same. In case, for the already existing RSA users, if the user name in PMP and in RSA Authentication Manager are different, you can do a mapping of names in PMP instead of editing the name in RSA. This can be done by editing the PMP user properties. (Assume the scenario that in PMP you have imported a user from Active Directory, who has the username (say) ADVENTNET\rob in PMP. In RSA Authentication Manager, assume that the username is recorded as 'rob'. In normal case, there will be mismatch of usernames between PMP and RSA Authentication Manager. To avoid that, you can do a mapping in PMP - ADVENTNET\rob will be mapped to rob).

The following sequence describes a typical PMP - RSA SecurID authentication process. Note that users must authenticate twice: first with their local LDAP or Active Directory passwords, and then with their RSA SecurID tokens.

1. A user tries to access PMP web-interface
2. PMP authenticates the user through ActiveDirectory or LDAP or locally
3. PMP prompts for the user for a username and RSA SecurID passcode and forwards the credentials to RSA Authentication Manager through the RSA Runtime API.
4. RSA Authentication Manager authenticates the user and returns a message to PMP.
5. PMP grants the user access to the requested resource.

Step 2: Enforcing Two Factor Authentication for Required Users

In Step 1 above, you have chosen RSA SecurID as the option for two factor authentication. After choosing this option, you need to apply two factor autentication for the required users.

To enforce two factor authentication for a user,

1. Go to "Admin" >> "Users"
2. Click the button "Set 2-factor authentication"
3. In the UI that opens, select the users for whom two factor authentication is to be enforced
4. Click "Save"

How to connect to PMP Web-Interface when TFA is Enabled?

The users for whom two factor authentication is enabled, will have to authenticate twice successively. As explained above, the first level of authentication will be through the usual authentication. That is, the users have to authenticate through PMP's local authentication or AD/LDAP authentication. Depending on the type of TFA chosen by the administrator, the second level of authentication will differ as explained below:

Note: When TFA is enabled, the login screen will ask for the username alone in the first UI. The users will be prompted to enter the passwords only in the second step.

TFA using RSA SecurID - Workflow

If the administrator has chosen TFA throgh RSA SecurID, the two factor authentication will happen as detailed below:

- Upon launching the PMP web-interface, the user has to enter the username to login to PMP and click "Login"

- Against the text field "Password", the user has to enter the local authentication password or AD/LDAP domain password as applicable
- Against the text filed "RSA Passcode", enter the RAS SecurID passcode. The passcode could be a combination of PIN and tokencode or just tokencode alone depending on the configuration done in RSA Authentication Manager

- Against the text field "Password", the user has to enter the local authentication password or AD/LDAP domain password as applicable

TFA using RSA SecurID: Different Scenarios in logging into PMP

Case 1: Entering user generated / system created PIN

As mentioned above, the RSA passcode could be a combination of PIN and tokencode or just tokencode alone or a password depending on the configuration done in RSA Authentication Manager. If the settings in RSA Security Console demands the users to create a PIN on their own or use a system generated PIN, the following screen would be shown to the users after step 2 (that is, after entering the first password & RSA tokencode to login to PMP).

User Created PIN

In the case of user created PIN, users will get the option to enter the PIN on their own. The PIN should contain numeric characters - minimum 4, maximum 8 characters. After entering the PIN, the user will have to wait for a while until the RSA tokencode changes to a new value. Then, in the next screen, enter the new PIN and the RSA tokencode to authenticate.

System Created PIN

In the case of system created PIN, PMP itself will randomly generate a PIN and it will be shown on the screen. Users will have to note down the new PIN and wait for a while until the RSA tokencode changes to a new value. Then, in the next screen, the users will have to enter the new PIN as generated by the system and the RSA tokencode to authenticate.

Case 2: New Tokencode Mode

If a user attempts to login to PMP using a random RSA passcode or by guesswork for a specified number of time, the RSA Authentication Manager will turn the screen to the next tokencode mode to verify whether the user possesses the token. In that case, PMP prompts for next tokencode during the login. That means, the user will have to wait until the RSA device shows a new tokencode and the new code to proceed with logging into PMP.

Note: If the new tokencode entered by the user is wrong, PMP will revert to the initial login screen. Users will have to start from entering the username again

If you have configured High Availability

Whenever you enable TFA or when you change the TFA type (PhoneFactor or RSA SecurID or One-time password) AND if you have configured high availability, you need to restart the PMP secondary server once.

Google Authenticator

(Feature available only in Premium and Enterprise Editions)

Overview

Google Authenticator is a software based authentication token developed by Google. The token provides an authenticator, which is a six digit number users must enter as the second factor of authentication.

You need to install the google authenticator app on your smart phone or tablet devices. It generates a six-digit number, which changes every 30 seconds. With the app, you don“t have to wait a few seconds to receive a text message. Here“s how to set up and use the Google Authenticator app with your Google account, along with a few other well-known sites.

Following is the sequence of events involved in using Google Authenticator as the second factor:

1. A user tries to access PMP web-interface
2. PMP authenticates the user through Active Directory or LDAP or locally (first factor)
3. PMP prompts for the second factor credential through Google Authenticator
4. Enter the six-digit token that you see on the Google Authenticator GUI
5. PMP grants the user access to the web-interface

Enabling Google Authenticator

PMP administrators can set up two factor authentication (with Google Authenticator as the second factor) as explained below:

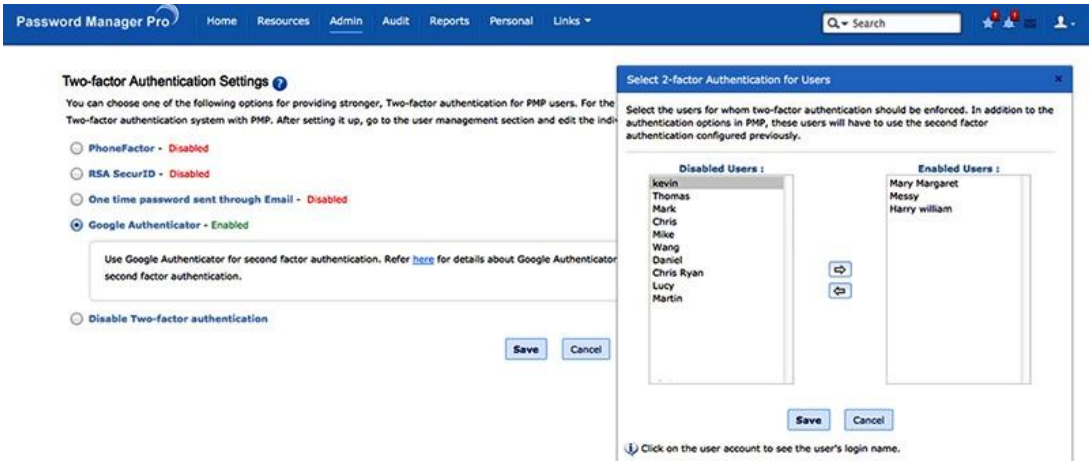
Summary of Steps

1. Setting up two factor authentication in PMP
2. Enforcing two factor authentication for required users in PMP

Step 1: Setting up Two Factor Authentication in PMP

The first step is to enable two factor authentication. To do that,

1. Go to "Admin" tab and click "Two Factor Authentication"
2. Choose the option "Google Authenticator"
3. Click "Save"



Step 2: Enforcing Two Factor Authentication for Required Users

In step 1 above, you have chosen Google Authenticator as the option for two factor authentication. After choosing this option, you need to apply two factor authentication for the required users. You can do this from the GUI that pops-up upon clicking "Save' button in step 1 above. Alternatively, you can do this as explained below:

To enforce two factor authentication for a user,

1. Go to "Admin" >> "Users"
2. Click the button "Set 2-factor authentication"
3. Click "Save"

How to connect to PMP Web-Interface when TFA through Google Authenticator is Enabled?

Pre-requisite

To make use of google authenticator as the second factor of authentication, you should first install Google Authenticator app in your smart phone or tablet. Google officially supports Android, iPhone, iPad, iPod Touch and BlackBerry devices. Detailed instructions to install the Google Authenticator app is available in Google's website.

Connecting PMP Web-Interface

The users for whom two factor authentication is enabled, will have to authenticate twice successively. As explained above, the first level of authentication will be through the usual authentication. That is, the users have to authenticate through PMP's local authentication or AD/LDAP authentication.

When TFA is enabled, the login screen will ask for the username alone in the first UI. The users will be prompted to enter the passwords only in the second step.

TFA using Google Authenticator - Workflow

If the administrator has chosen TFA throgh Google Authenticator, the two factor authentication will happen as detailed below:

- Upon launching the PMP web-interface, the user has to enter the username to login to PMP and click "Login"

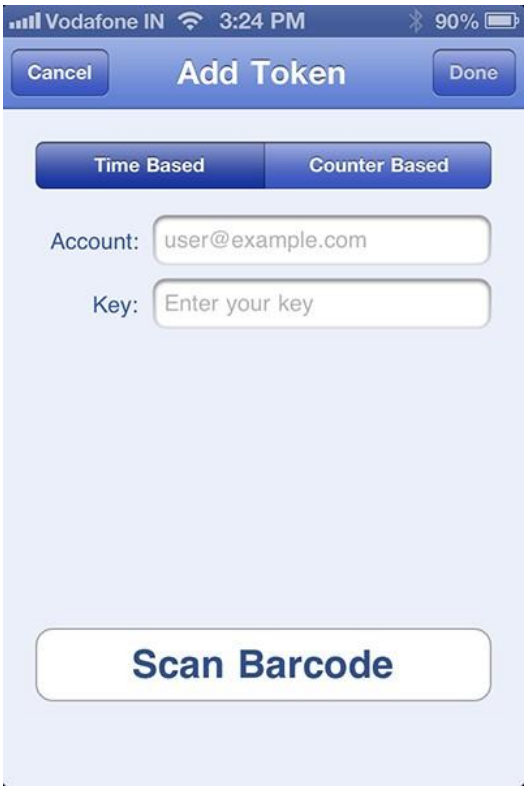
Associating Google Authenticator with your account in PMP

- When you are logging in for the first time after enabling TFA through Google Authenticator, you will be prompted to associate it with your account in PMP. You need to first launch the Google Authenticator app in your mobile device/tablet and choose the '+' button. Then select 'Scan Barcode' and point your device to the barcode shown below. This will automatically configure Google Authenticator to start generating authentication codes for PMP.
- After completing this, you can enter the current token for authentication in the text box

Google Authenticator Token – Sample

Important Note: If you had trouble scanning the barcode, the automatic setup will not work. Do the following manual steps in the Google Authenticator app in your device:

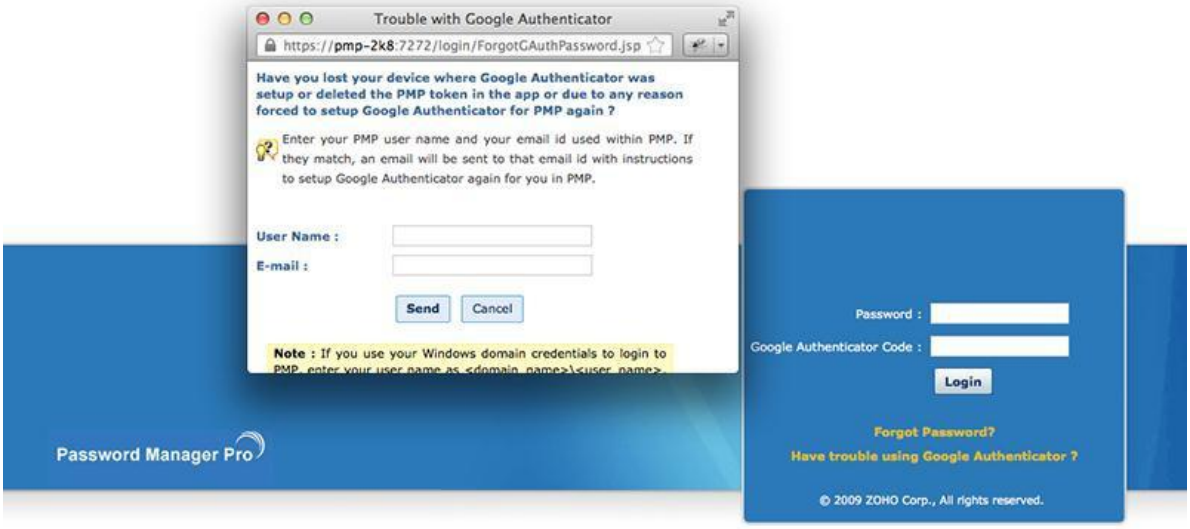
- Choose 'Time Based' for your token (this is the default selection in the app)
- Supply an identifier for your PMP account in this format - PMP:<your email id in PMP> (for ex. PMP:john@abc.com)
- Supply the alphanumeric string as the key and select 'Done'
- Google Authenticator is now setup and it will start generating codes periodically for <PMP:user@mailid>. Enter the current code to continue logging into PMP : _____ [Submit]



From the next time onwards, you will be prompted to enter the token alone as shown below:

Troubleshooting Tip

As mentioned earlier, the Google Authenticator is associated with your PMP account. If you ever lose your mobile device/tablet OR if you accidentally delete the Google Authenticator app on your device, you will be able to get tokens to login to PMP. In such scenarios, just click the link "Have trouble using Google Authenticator?" in the PMP login screen. You will be prompted to enter your PMP username and the email address associated with PMP. You will receive instructions to get Google Authenticator again.



If you have configured High Availability

Whenever you enable TFA or when you change the TFA type (PhoneFactor or RSA SecurID or One-time password or Google Authenticator) AND if you have configured high availability, you need to restart the PMP secondary server once.

RADIUS-Compliant Two Factor Authentication

(Feature available only in Enterprise Edition)

Overview

You can integrate RADIUS server or any RADIUS Compliant two Factor Authentication system (like Vasco Digipass) with PMP for the second factor authentication.
Following is the sequence of events involved in using RADIUS-based authentication system as the second factor:

- Provide basic details about RADIUS server
- Enable the RADIUS-based authentication system as the second factor

Steps to leverage any RADIUS based authentication as the second factor has been explained below.

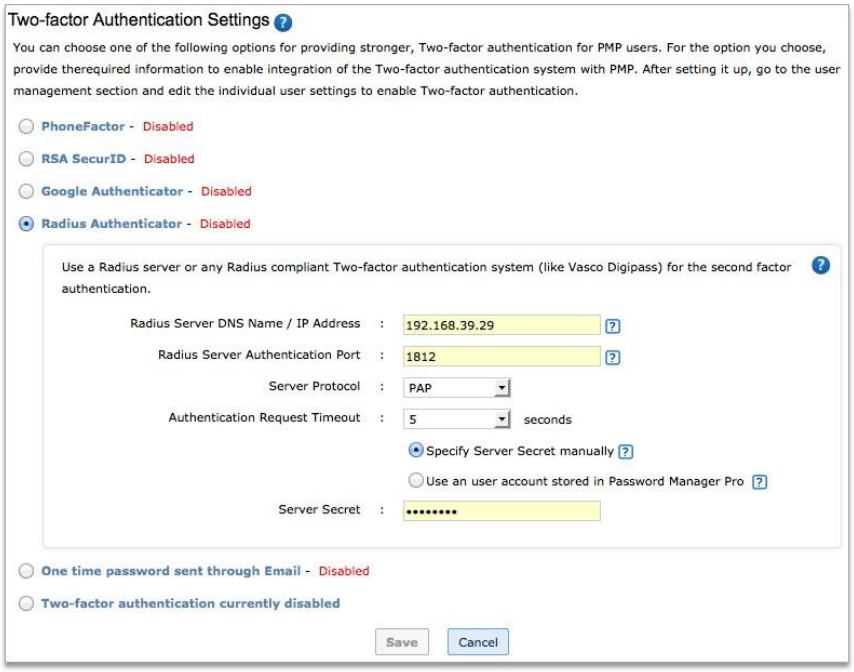
Enabling RADIUS Authenticator

Summary of Steps

1. Setting up two factor authentication in PMP
2. EEnforcing two factor authentication for required users in PMP

Step 1: Setting up Two Factor Authentication in PMP

The first step is to enable two factor authentication. To do that,



1. Go to "Admin" tab and click "Two Factor Authentication"
2. Choose the option "RADIUS Authenticator"
3. In the UI that opens, provide the following details:
   - Server Name/IP Address - enter the host name or IP address of the host where RADIUS server is running
   - Server Authentication Port - enter the port used for RADIUS server authentication. By default, RADIUS has been assigned the UDP port 1812 for RADIUS Authentication
   - Server Protocol - select the protocol that is used to authenticate users. Choose from four protocols - Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), Microsoft Challenge-Handshake Authentication Protocol (MSCHAP), Version 2 of Microsoft Challenge-Handshake Authentication Protocol (MSCHAP2)
   - Server Secret - You have the option to enter the RADIUS server secret either manually in the text box or you can direct PMP to use the secret already stored in the product. In that case, you need to select the resource name and account name from the drop-down. The second option - storing the RADIUS password in PMP and selecting it from drop-down is the recommended approach.
4. Click "Save"

Step 2: Enforcing Two Factor Authentication for Required Users

In step 1 above, you have chosen Google Authenticator as the option for two factor authentication. After choosing this option, you need to apply two factor authentication for the required users. You can do this from the GUI that pops-up upon clicking "Save' button in step 1 above. Alternatively, you can do this as explained below:

To enforce two factor authentication for a user,

- Go to "Admin" >> "Users"
- Click the button "Set 2-factor authentication"
- In the UI that opens, select the users for whom two factor authentication is to be enforced
- Click "Save"

How to connect to PMP Web-Interface when TFA through RADIUS Authenticator is Enabled?

Connecting PMP Web-Interface

The users for whom two factor authentication is enabled, will have to authenticate twice successively. As explained above, the first level of authentication will be through the usual

authentication. That is, the users have to authenticate through PMP's local authentication or AD/LDAP authentication.

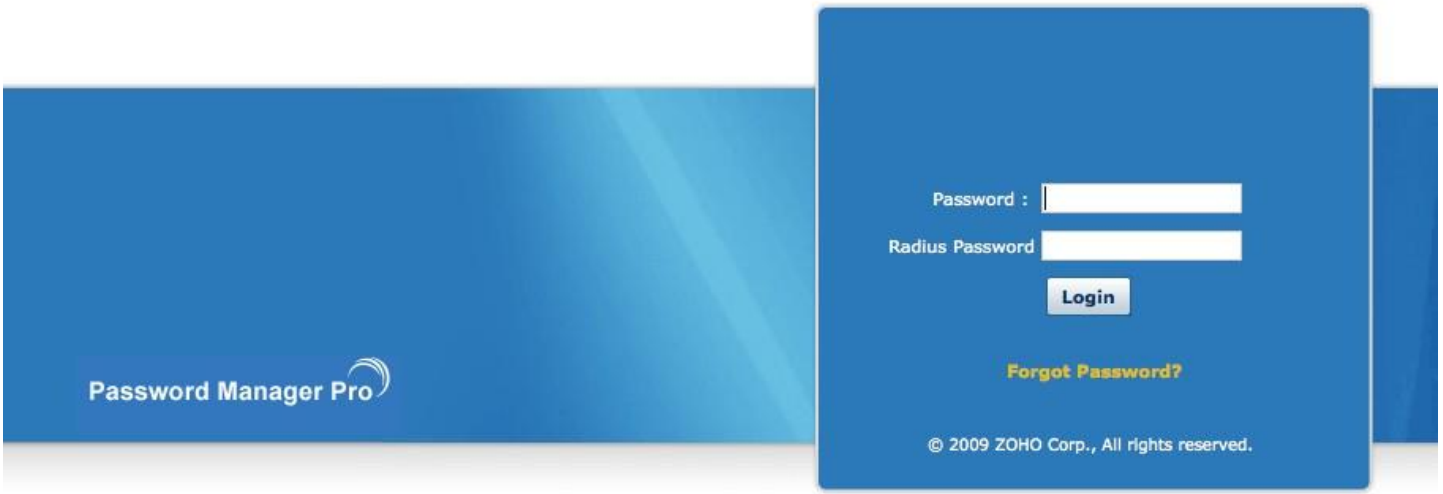
When TFA is enabled, the login screen will ask for the username alone in the first UI. The users will be prompted to enter the passwords only in the second step.

TFA using RADIUS Authenticator - Workflow

If the administrator has chosen TFA throgh RADIUS Authenticator, the two factor authentication will happen as detailed below:

- Upon launching the PMP web-interface, the user has to enter the username to login to PMP and click "Login"

In the next screen, you will be prompted to enter the RADIUS code:



Resource Management

Adding Resources

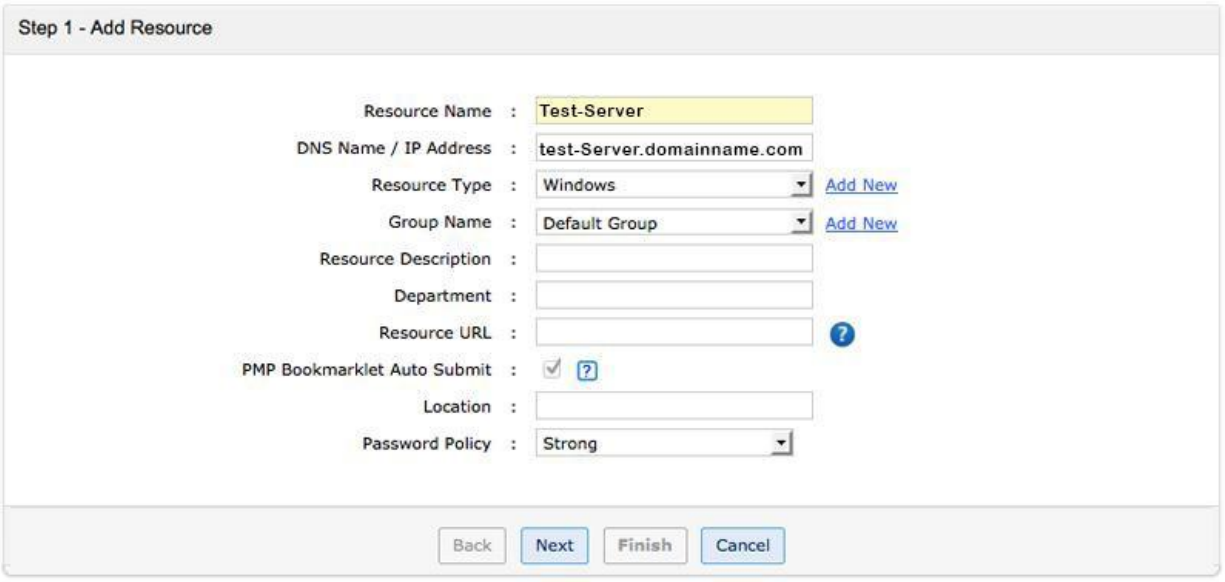
The first step to get started with Password Management in PMP is adding your "resource" to the PMP database.

To add your resource,

Addition of resources to be managed in your setup falls under three steps. The first steps involves entering details about the resource such as its name, its DNS Name/IP, type, location etc. The second step

Step 1: Adding Resource Details

- Go to "Resources" tab in the web interface
- Click the "Add Resource" link
- In the UI that opens, enter the name of the resource in the text field against "Resource Name". The resource name is the one that uniquely identifies the resource in the PMP database. This field is mandatory
- Enter the DNS Name/IP Address of the resource against "DNS Name/IP Address". The DNS name or the IP address is used during password changes made to the resource. This field is optional. However, if you want to enable remote password reset, this is mandatory.



- Select the type of the resource against the text field "Resource Type". For example, if you are adding a server, you can select its type - Windows/Windows Domain/Linux/Mac/Soalris/HP UNIX/IBM AIX/MS SQL Server/ MySQL server/ Oracle DB Server/ VMWare ESXi/ Sybase ASE/ LDAP Server / HP ProCurve/ HP iLO/ Cisco IOS/ Cisco CatOS/ Cisco PIX/ Juniper Netscreen/ File Store/ Key Store/ License Store/ Website Accounts. Based on your requirements and the nature of your resource, you can add any custom type by clicking the link "Add New". PMP provides the option to store digital files, certificates, images and documents too. In that case, you need to choose the Resource Type as explained below:

Storing Digital Certificates, Licence Keys, Files, Documents, Images etc.

Different file types could be securely stored in the PMP repository along with the passwords. To store a license key or a certificate or a document etc. you need to select the 'Resource Type' as explained below:

By default, PMP supports the following file stores:

Certificate store: to store any private / public keys, digital certificates and digital signature files
License key store: to store any software license keys
File store: to store any digital content (documents, pictures, executables etc)
You can create any new resource type as pert your requirements.

Resources of the above types are managed and shared the same way as other resources. During retrieval, a link to the file is provided for it to be saved locally to the disc.

- If you already have resource groups and if you wish to make the resource you are adding as part of a group, select the "Group Name". Otherwise, leave this column with default value
- Provide a description for the resource addition. This will be helpful for reference at a future point of time
- In case, the resource belongs to type 'Windows Domain', enter the domain name. This is needed if you wish to use Windows Service Account Reset feature
- Fill-in details such as "Department" and "Location" of the resource (if applicable)
- If you want to access the resource being added over the web, you can specify the URL for the same. You can even specify the user name and password in the URL to directly login to the resource. For security reasons, PMP provides the option for using place holders to avoid the usage of user name, password etc in plain text in the URL. At the

time of URL invocation, PMP replaces the respective data for the placeholders and submits the data by 'POST' method. Nowhere during the URL invocation, the password will be visible to the users. The following four place holders are allowed: %RESOURCE_NAME%, %DNS_NAME%, %ACCOUNT_NAME% and %PASSWORD%

Examples for using the place holders in the URL:

(1) Assume that you have a resource named 'abc' and on typing the resource name in the browser as http://abc you can access an application. In this case, you can enter the resource url with placeholder as shown below:
http://%RESOURCE_NAME%
(2) Assume you have an application running on port 7272 and you can access it through the DNS name of the host where it runs. You can make use of the placeholder and construct the URL as below:
https://%DNS_NAME%:7272

In case, you wish to supply the username and password for the application and directly login to the resource, you can construct the URL as below:

https://%DNS_NAME%:7272/j_security_check?j_username=%ACCOUNT_NAME%&j_password=%PASSWORD%&domainName=LOCAL

- Select the required 'Password Policy' - Strong, Medium or Low. Apart from the default policies, you can create more custom policies based on your needs. Selection of the required policy is crucial because, when administrators try to change the passwords of the accounts that are part of this resource, this policy would be enforced. The chosen password policy is applied to passwords of all the accounts of this resource by the password generator.
- What is the need for Password Policy field here?
  This question naturally arises when you are in the process of adding a resource. The following example would provide the answer: If your intention is to have accounts with strong passwords, others with admin privileges should not disturb this intention while changing the password. So, this step is crucial though it does not have a direct bearing on resource addition.

- Can I add my own custom fields for resources?
  Yes, you can. You can have up to 20 additional custom fields to resources. To add a custom field, go to "Resources" tab and click the button"Customize Resource" in the drop-down under "More Actions"
  - Character/list - for text inputs
  - Numeric - to store numeric inputs
  - Password - to store password inputs. The values entered here, will not be echoed in the GUI. Additionally, Password Generator icon will be present beside it to help generate
  - Date & Time - to store date and time inputs
  - File - to store file based inputes

Important Note:

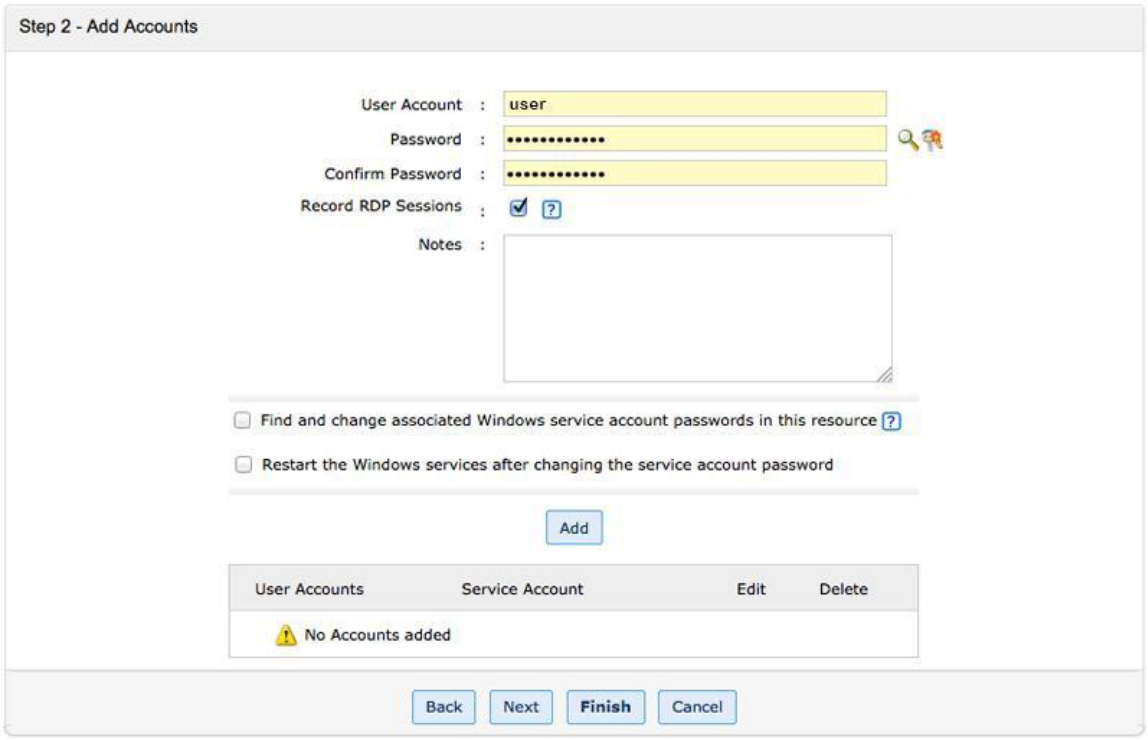
When you create a custom field of the type 'File', it does not take effect automatically. You need to specify for which resource types you would like to have this additional field. To do this, you need to navigate to "Admin >> Resource Types", then click "Edit" against the required resource type. In the GUI that opens, select the checkbox against the field "File".

- Can others see the resources added by me?
  Except super administrators (if configured in your PMP set up), no one, including admin users will be able to see the resources added by you. Apart from this, if you decide to share your resources with other administrators, they will be able to see them.

Step 2: Adding Account Details - (User Account & Password to be Managed)
The second step is to add the user accounts and their passwords of this resource that are to be shared between multiple users. Notes can be added to each account.

Important Note:

If you want to enable password reset in remote systems, make sure that the passwords you enter in this step and the ones in the actual target systems are the same. PMP uses these credentials to login to the target systems and do the password reset and if the passwords are wrong, the password reset will not happen.



- In the text field for "User Account", enter the user name of the particular account being added. This field is mandatory
- n the text field for "Password", enter the password of the account. This field is mandatory. If you have set a 'Password Policy' during the previous step, you need to enter your password only in accordance with the specified policy. For example, if you have set 'Strong' as the policy, the password entered here should comply to that. If you do not want to enforce the policy here, change the setting through "General Settings"
- Confirm the password
- Enter description about the account being added in the "Notes" column. This would help in properly identifying a particular account in future
- In case, the resource belongs to type 'Windows Domain', you can choose to use Windows Service Account Reset feature (refer to this link for more details on this)
- The account added until now are listed in the table below
- Within one resource, one might have many accounts - for example, consider managing the passwords of a linux server. There will be many user accounts for the server such as root, guest and so on. For a single resource, you can add as many accounts and passwords as present in the resource. If you have multiple accounts for the resource, repeat the above procedure
- If your resource type belongs to Windows, Linux, Windows Domain, IBM AIX, HP UNIX, Solaris, Mac OS, VMWare ESXi, MS SQL Server, MySQL server, Oracle DB Server, Sybase ASE, LDAP Server, HP ProCurve, HP iLO, Cisco IOS, Cisco CatOS, Cisco PIX, Juniper Netscreen and if you require remote password reset, click "Next";

- Otherwise, click "Finish" to complete the resource addition process
- Can I add my own custom fields for accounts?
  Yes, you can. You can have up to 20 additional custom fields to accounts. To add a custom field, traverse to "Admin >> Customize >> Accounts -Additional Fields". Your additional fields can be in any of the following five formats -
  Character/list - for text inputs
  Numeric - to store numeric inputs
  Password - to store password inputs. The values entered here, will not be echoed in the GUI. Additionally, Password Generator icon will be present beside it to help generate
  Date & Time - to store date and time inputs
  File - to store file based inputes <

Important Note: When you create a custom field of the type 'File', it does not take effect automatically. You need to specify for which resource types you would like to have this additional field. To do this, you need to navigate to "Admin >> Resource Types", then click "Edit" against the required resource type. In the GUI that opens, select the checkbox against the field "File".

The required user name and password have now been added to the PMP repository. Users who are authorized to access the resource, will be able to view the information.

Step 3: Remote Password Reset

(Feature available only in Premium and Enterprise Editions)

PMP provides the option to remotely change the password of select resources. As of now, this facility is available for changing the password of only those resources that belong to the type Windows, Windows Domain, Linux, IBM AIX, HP UNIX, Solaris, Mac OS, VMWare ESXi, MS SQL server, MySQL server, Oracle DB Server, Sybase ASE, HP ProCurve, HP iLO and Cisco Devices (IOS, CatOS, PIX), Juniper Netscreen. Using this utility, you can change the password of a server present in a remote location, from the PMP web interface itself.
You can avail this facility in two ways:

- By deploying PMP agents in the remote location
- Without deploying agents

If the remote resource has restrictions such as a firewall, you would require deployment of agents. Otherwise, you can do password reset without deploying agents.

You may proceed with Step 3 only if you intend to do password reset without deploying agents. You need to specify the credentials to be used to login to the resource and effect

the changes. For Windows domain controller, Linux, IBM AIX, HP UNIX, Solaris, Mac OS, VMWare ESXi, MS SQL server, MySQL server, Oracle DB Server, Sybase ASE, LDAP Server, HP ProCurve, HP iLO and Cisco Devices (IOS, CatOS, PIX), Juniper Netscreen specify the accounts that will be used to login from remote to perform password reset. For other type of resources this step is not applicable.

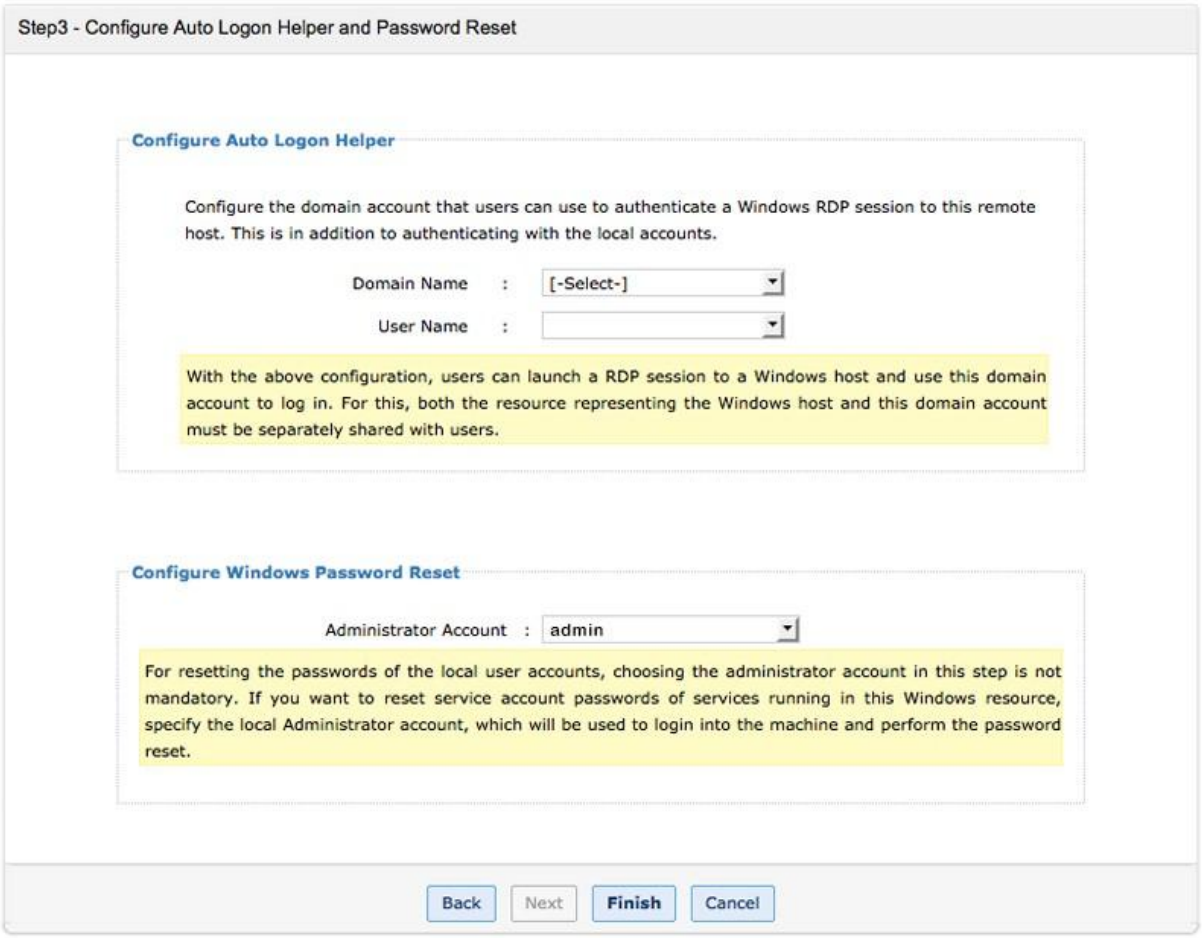
Specifying credentials & enabling remote reset for different resource types
Resource Type
Reset Credentials Requirement
Windows & Windows Domain

Configure Auto Logon

- PMP offers support to launch a secure direct connection to the resource from the web-interface. The configuration for the auto logon can be made here. For logging into a Windows resource, you need to configure the domain account that can be used by users to authenticate a Windows RDP session to this remote host. You can authenticate with local accounts also. This is just another option.

Configure Remote Password Reset

- For resetting the passwords of the local user accounts, choosing the administrator account in this step is not mandatory.
- If you want to reset service account passwords of services running in this Windows resource, specify the local Administrator account, which will be used to login into the machine and perform the password reset
- PMP has the ability to find and reset the local service account passwords of the resource being added. If you want to reset the local service account passwords, select the checkbox "Find and change associated Windows service account passwords in this resource" after adding the local administrator account. You also have the option to restart the Windows services after changing the passwords of local service accounts.
- If the PMP service is run with domain administrator privilege, PMP will be able to change the passwords of all the local accounts in the computer (present in the domain) without the need for supplying the old password
- Click "Finish"



Linux / IBM AIX, HP UNIX, Solaris, Mac OS

Configure Auto Logon

PMP offers support to launch a secure direct connection through SSH to the resource from the web-interface. The configuration for the auto logon has to be made here. To connect through SSH, you need to specify the port to connect, if it is different than the default 22.Configure Remote Password Reset

For remote password reset of Unix resources, PMP first uses the remote login account to login to the target system. Then, to carry out password reset, privilege elevation is needed. PMP can either 'su' as root or use 'sudo' to execute the remote password reset commands (if the target system supports execution of password reset commands through 'sudo)'.

In this process, the following steps are involved:

1. Selecting the protocol
2. Selecting the authentication method for remote login based on the protocol chosen and specifying the remote login account
3. Specifying the root account if PMP has to use 'su' / selecting 'sudo'

Step 1 - Selecting the Protocol

- Select the protocol for remote login - ssh or telnet and then select the remote login account and root account. If you have chosen telnet, you can go to step 3.

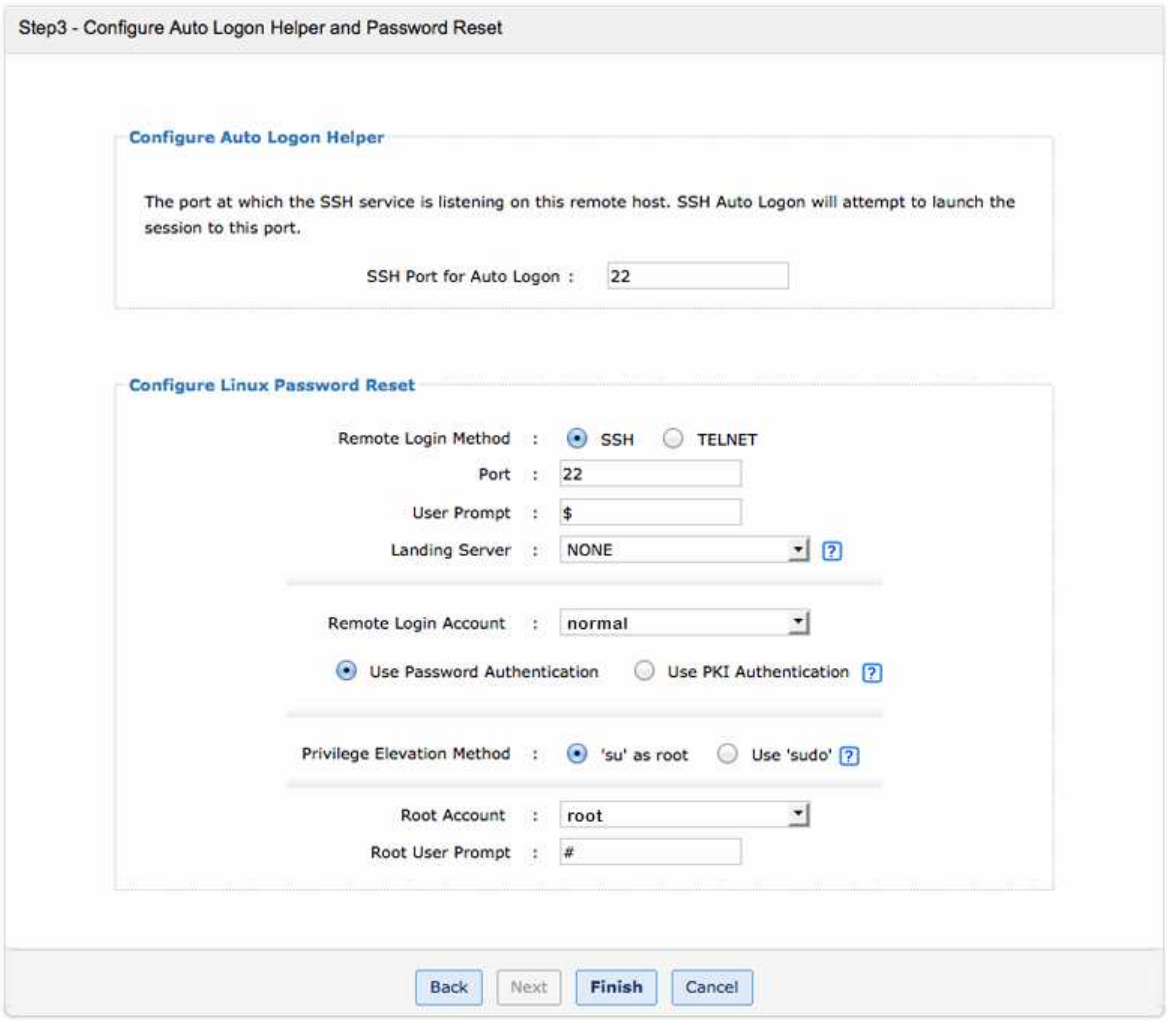
Step 2 - If you opt for SSH, specify the authentication method

- If you opt for SSH, you have the option to use either "Password Authentication" or "Public Key Infrastructure" (PKI) Authentication.

  If you choose PKI authentication, you need to select the remote login account as explained below:
  The public key would be present under the remote system under a specific remote login account. Typically, it would be available under $Home/.ssh folder. Select the remote login account for which the public key is present. Also, PMP supports SSH2 and above only.
  Then browse and supply the corresponding Private Key.

Step 3 - Specifying the root account / selecting 'sudo'

- As mentioned above, for executing remote password reset commands, PMP can either 'su' as root or use 'sudo', which allows the user to run the command with root privileges without having to switch to the root account.
- If you use the option, 'su' as root, you need to select the root account
- If the target system allows execution of password reset commands through 'sudo', you can select that option
- Click "Finish"



IBM AS400

No specific configuration in Step 3 required. The resource addition process ends with Step 2.
VMWare ESXi

Configure Auto Logon

PMP offers support to launch a secure direct connection through SSH to the resource from the web-interface. The configuration for the auto logon has to be made here. To connect through SSH, you need to specify the port to connect, if it is different than the default 22.

Configure Remote Password Reset

For remote password reset of VMWare ESXi resources, PMP first uses the remote login account to login to the target system. Then, to carry out password reset, privilege elevation is needed. PMP can either 'su' as root or use 'sudo' to execute the remote password reset commands (if the target system supports execution of password reset commands through 'sudo)'.

In this process, the following steps are involved:

1. Selecting the protocol
2. Selecting the authentication method for remote login based on the protocol chosen and specifying the remote login account
3. Specifying the root account if PMP has to use 'su' / selecting 'sudo'

Step 1 - Selecting the Protocol

- Select the protocol for remote login - ssh or telnet and then select the remote login account and root account. If you have chosen telnet, you can go to step 3.

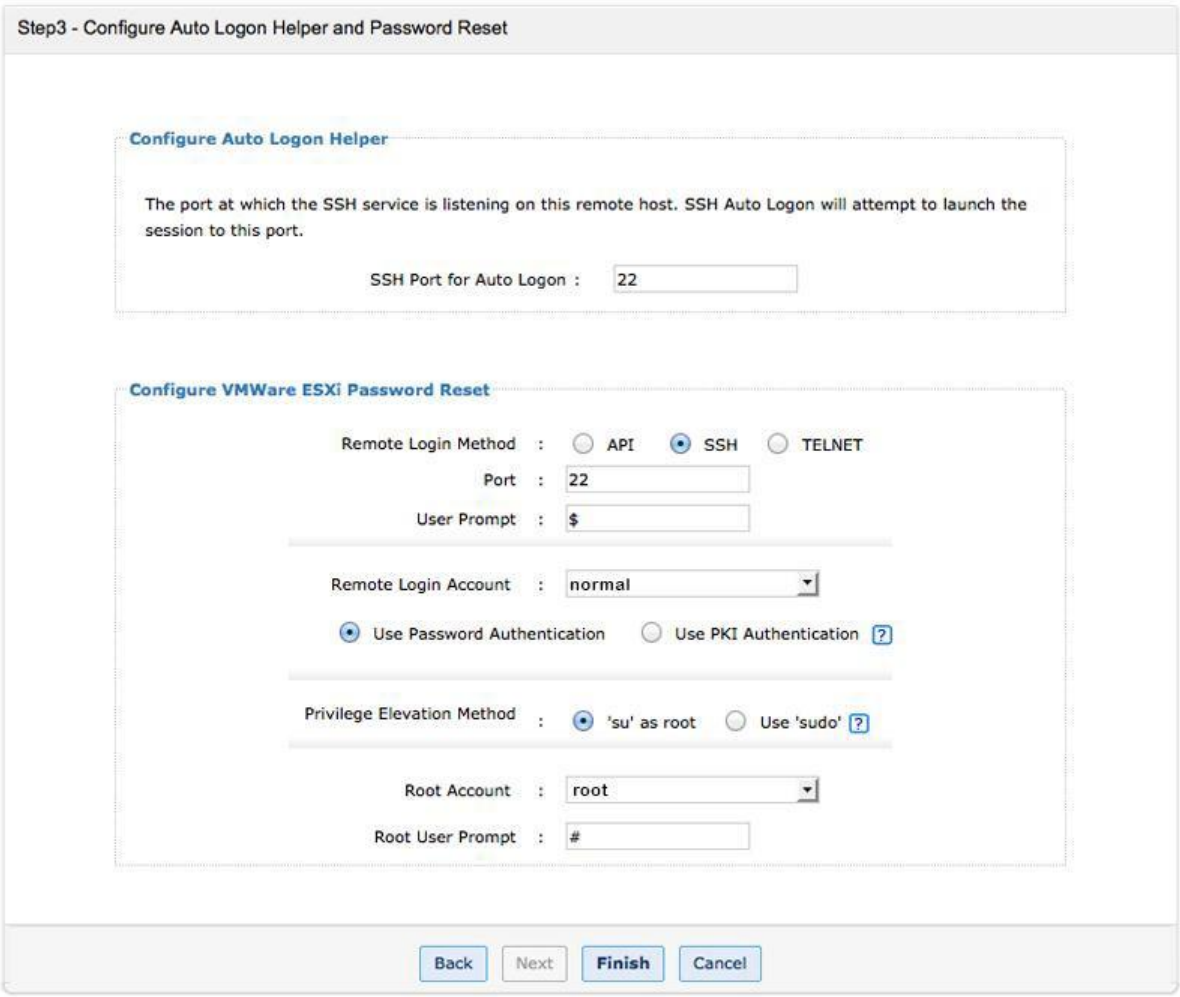
Step 2 - If you opt for SSH, specify the authentication method

- If you opt for SSH, you need to specify SSH port first and then specify the SSH User Prompt. You have the option to use either "Password Authentication" or "Public Key Infrastructure" (PKI) Authentication.
  If you choose PKI authentication, you need to select the remote login account as explained below:
  The public key would be present under the remote system under a specific remote login account. Typically, it would be available under $Home/.ssh folder. Select the remote login account for which the public key is present. Also, PMP supports SSH2 and above only.
  Then browse and supply the corresponding Private Key.

Step 3 - Specifying the root account / selecting 'sudo'

- As mentioned above, for executing remote password reset commands, PMP can either 'su' as root or use 'sudo', which allows the user to run the command with root privileges without having to switch to the root account.

- If you use the option, 'su' as root, you need to select the root account. You need to specify the 'Root User Prompt'.
- If the target system allows execution of password reset commands through 'sudo', you can select that option
- Click "Finish"



MySQL Server Resource Type

Password reset for server is done over JDBC. So, the MySQL Administrator credentials are required. You can enable remote reset of the password of MySQL server as below:

Specify the port where the MySQL server is running. By default, MySQL occupies the port 3306Specify the connection mode - you can configure the connection between MySQL Server and PMP to be over an encrypted channel (SSL) or Non-SSL. If you choose SSL mode, do the following. Otherwise, proceed to Step 3.

To enable the SSL mode, the MySQL server should be serving over SSL and you will have to import the MySQL server's root certificate into the PMP server machine's certificate store. You need to import all the certificates that are present in the respective root certificate chain - that is the certificate of the PMP server machine and intermediate certificates, if any.

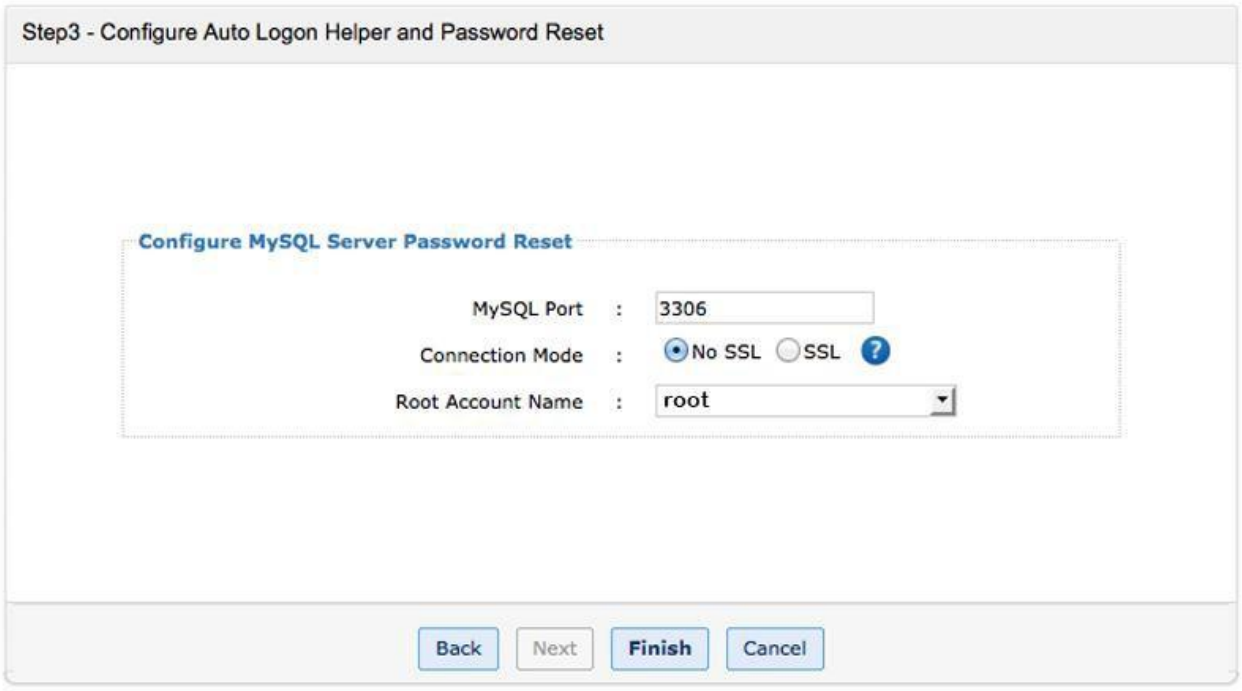
To import root certificate, open a command prompt and navigate to <PMP_SERVER_HOME>\bin directory and execute the following command:

For Windows
importCert.bat <Absolute Path of certificate>

For Linux
importCert.sh <Absolute Path of certificate>

Restart PMP server. Then continue with the following steps.

1. To enable PMP access the MySQL server, provide MySQL Root Account Name
2. Click "Finish"



MS SQL Server Resource Type

Password reset for MS SQL server is done over JDBC. So, either a domain account credential having enough privileges to modify SQL server passwords or the MS SQL Administrator credential are required. You can enable remote reset of the password of MS SQL server as below:

1. Specify the port where the MS SQL server is running. By default, MS SQL occupies the port 1433
2. Specify the connection mode - you can configure the connection between MS SQL Server and PMP to be over an encrypted channel (SSL) or Non-SSL. If you choose SSL mode, do the following. Otherwise, proceed to Step 3.

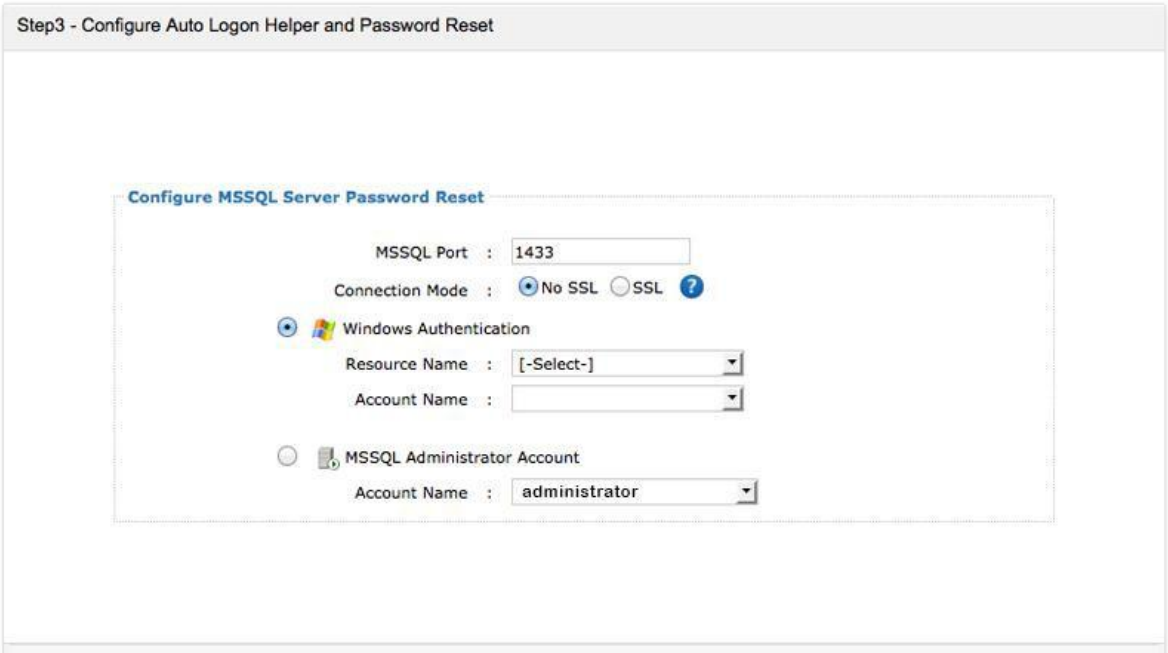
To enable the SSL mode, the MS SQL server should be serving over SSL and you will have to import the MS SQL server's root certificate into the PMP server machine's certificate store. You need to import all the certificates that are present in the respective root certificate chain - that is the certificate of the PMP server machine and intermediate certificates, if any.

To import root certificate, open a command prompt and navigate to <pmp_server_home>\bin directory and execute the following command:

```
For Windows
importCert.bat     <Absolute Path of certificate>
For Linux
importCert.sh      <Absolute Path of certificate>
```

Restart PMP server. Then continue with the following steps.

3. To enable PMP access the MS SQL server, provide any one of the following details -
    1. Windows Authentication details - that is specifying the domain name of which the MS SQL server is a part and then selecting any one user username present in the domain (OR)
    2. MS SQL Administrator Account
4. Click "Finish"



For Oracle DB Server

To carry out password reset for Oracle DB server, administrative privileges are required. So, an administrator account has to be specified. You can enable remote reset of the password of Oracle DB server as below:

1. Specify the Oracle DB Listener Port. By default, the Oracle DB server listens to the port 1521
2. Specify the connection mode - you can configure the connection between Oracle DB Server and PMP to be over an encrypted channel (AES 256). If you choose the option 'YES' (encrypted mode), do the following. Otherwise, proceed to Step 3.
   - Start Oracle Net Manager
   - In the Navigator window, select "Oracle Net Configuration".
   - Expand the option Local > Profile
   - From the list in the right side pane, select the option "Oracle Advanced Security"
   - In the tabbed window that appears thereafter, click the tab "Encryption"
   - In the drop-down list for Encryption, select the option "Server"
   - For "Encryption Type" list, select the option "Accepted"
   - In the text-filed for 'Encryption Seed', enter random characters numbering between 10 and 70. Or, it can even be left blank
   - Select the algorithm "AES 256"
   - Specify an Oracle administrator account
3. Specify the Oracle Service Name. By default, the service name is taken as ORCL

4. Click "Finish"

For Sun Oracle ALOM / ILOM / XSCF
No specific configuration in Step 3 required. The resource addition process ends with Step 2.

For Sybase ASE
Prerequisite:

- jConnect 6.0 JDBC driver is required for the password reset. The driver is a file named "jconn3.jar" will be available under<sybase_install_directory>\jConnect_6_0\classes folder (in Sybase ASE 15.0)
- Copy the jconn3.jar and save it under <pmp_install_directory>\lib folder (in the machine running PMP server)

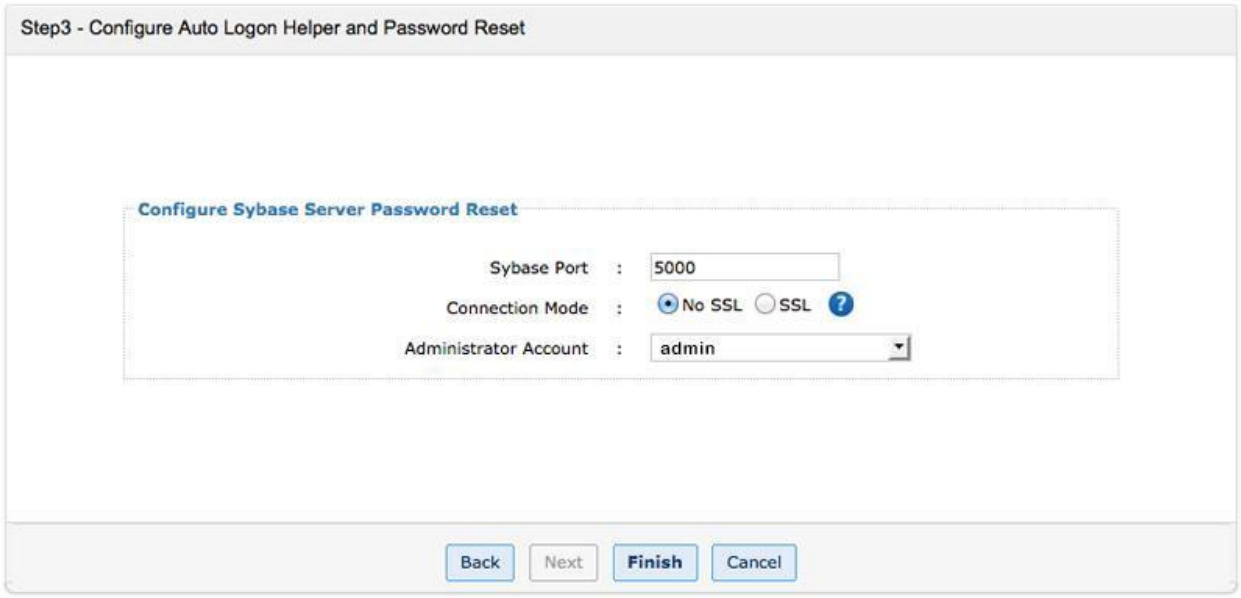
To carry out password reset for Sybase ASE, administrative privileges are required. So, an administrator account has to be specified. Steps for enabling remote password reset for Sybase ASE are explained below:

1. Specify the Sybase ASE Port. By default, it occupies the port 5000 (in SSL mode, default port is 2748)
2. Specify the connection mode - you can configure the connection between Sybase ASE and PMP to be over an encrypted channel (SSL) or Non-SSL. If you choose SSL mode, do the following. Otherwise, proceed to Step 3.
   - If you want to enable SSL communication from PMP to Sybase ASE
     - Copy and save the trust root certificate of the Sybase server present under <sybase_home>\ASE-15_0\certificates (in sybase ASE 15.0) to <pmp_install_directoty>\conf\ folder

- Run this command to import the certificate in PMP: '<pmp_home>\jre\bin\keytool.exe -import -v -alias sybase -file <rootcert.txt> -keystore server.keystore -keypass passtrix -storepass passtrix -noprompt'
- <rootcert.txt> is the root certificate of the Sybase ASE and usually named as <hostname>.txt

- Restart PMP server

3. Specify an administrator account of Sybase ASE
4. Click "Finish"



For LDAP Server

Prerequisite:

In Step 2 of 'Resource Addition', while adding accounts, you should have specified the Distinguished Name of the LDAP server account being added. Example: c=administator,cn=people,dc=test,dc=com.

LDAP server password reset

To carry out password reset for LDAP server, administrative privileges are required. So, an administrator account has to be specified. For remote reset, PMP supports Microsoft Active Directory, OpenLDAP, Oracle Internet Directory and Novell eDirectory. You can enable remote reset of the passwords of the above types of LDAP servers as below:

1. Specify the type of the LDAP Server being added

2. Specify the LDAP server Port. By default, it occupies the port 389 (in SSL mode, default port is 636)
3. Specify the connection mode - you can configure the connection between the LDAP server and PMP to be over an encrypted channel (SSL) or Non-SSL. If your LDAP server is of type Microsoft Active Directory, the connection has to be through SSL only. For other types, you may choose SSL or Non-SSL. If you choose SSL mode, do the following. Otherwise, proceed to Step 4.
   - To enable the SSL mode, the LDAP server should be serving over SSL and you will have to import the LDAP server's root certificate into the PMP server machine's certificate store. You need to import all the certificates that are present in the respective root certificate chain - that is the certificate of the PMP server machine and intermediate certificates, if any.

   To import root certificate, open a command prompt and navigate to <PMP_SERVER_HOME>\bin directory and execute the following command:

   For Windows
   importCert.bat <Absolute Path of certificate>

   For Linux
   importCert.sh <Absolute Path of certificate>

   Restart PMP server. Then continue with the following steps.
4. Specify an administrator account of LDAP server
5. Click "Finish"

For HP ProCurve Devices

Configure Auto Logon

PMP offers support to launch a secure direct connection through SSH to the resource from the web-interface. The configuration for the auto logon has to be made here. To connect through SSH, you need to specify the port to connect, if it is different than the default 22.

Configure Remote Password Reset

PMP requires Telnet or SSH service to be running in the resource. Manager Account and Prompts of Manager Mode and Configuration Mode are required for PMP to login to the resource. PMP will use the configuration mode to reset the passwords. You can enable remote reset of passwords of your HP Pro Curve devices by providing the following credentials:
Credential
Description

Remote Login Method

PMP supports SSH and TELNET protocols by which connection could be established with the device for password reset. Select the required protocol

Manager Account

Login account for establishing connection with the device. If the device is configured to prompt for the user name, then check on the option 'Account name required for login'. The account name associated will then be used with the user name prompt. If this option is unchecked, PMP will expect only the password prompt.

Manger Mode Prompt

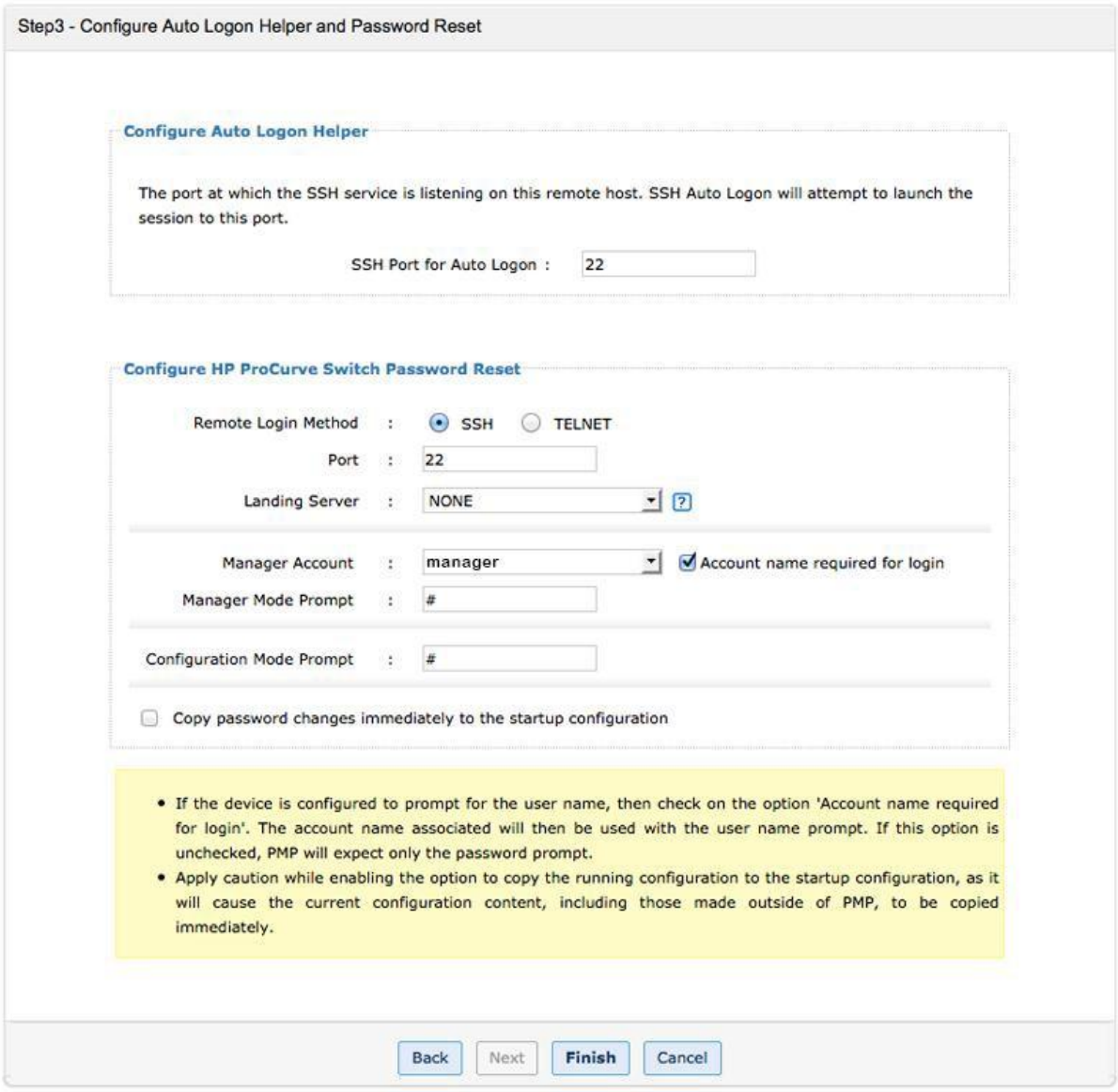
The prompt that appears after successful login

Configuration Mode Prompt

This is for entering into privileged mode to perform password reset.

Remote Login Method

If you want the password changes made to the running configuration from PMP to be applied to the startup configuration, select this checkbox. Exercise caution while enabling the option to copy the running configuration to the startup configuration, as it will cause the current configuration content, including those made outside of PMP, to be copied immediately.



For HP iLO

Configure Auto Logon

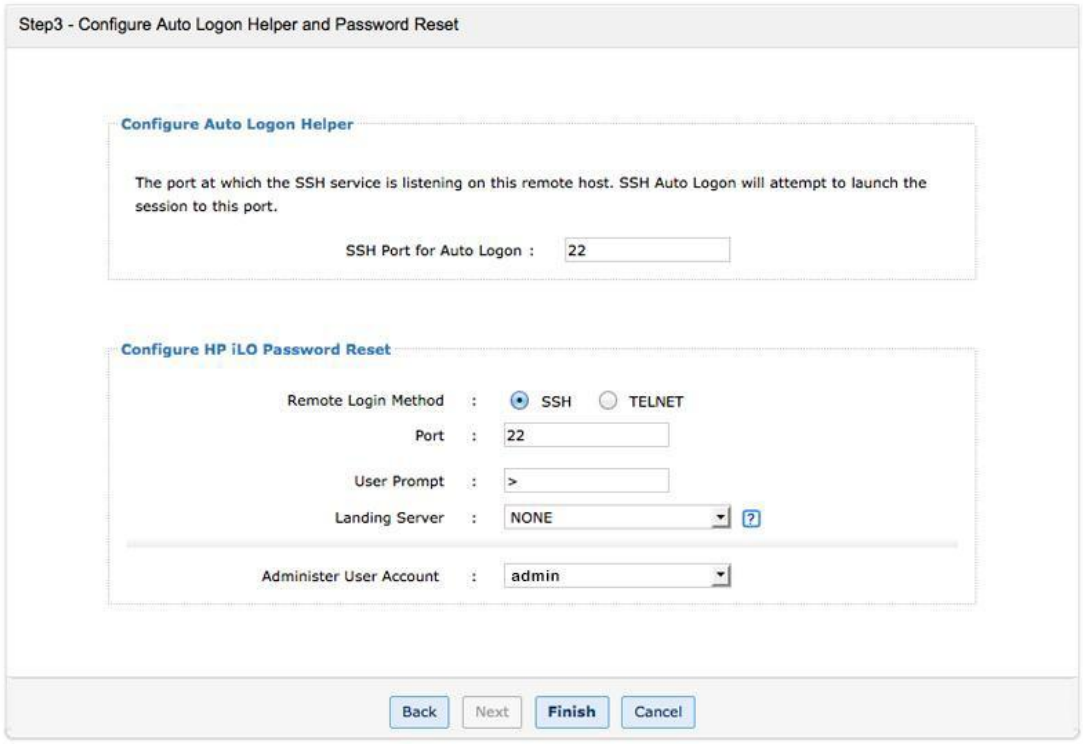
PMP offers support to launch a secure direct connection through SSH to the resource from the web-interface. The configuration for the auto logon has to be made here. To connect through SSH, you need to specify the port to connect, if it is different than the default 22.

Configure Remote Password Reset

Select the Remote Login Method

PMP supports SSH and TELNET protocols by which connection could be established with the device for password reset. Select the required protocol. Telnet or SSH service to be running in the resource.

Then, specify the prompt that appears upon successful user login. Also, specify the user account with administer privileges.



For Cisco Devices (IOS/CatOS/PIX)

Configure Auto Logon

PMP offers support to launch a secure direct connection through SSH to the resource from the web-interface. The configuration for the auto logon has to be made here. To connect through SSH, you need to specify the port to connect, if it is different than the default 22.

Configure Remote Password Reset

PMP requires Telnet or SSH service to be running in the resource. Passwords of the enable mode and a user account are required for PMP to login to the resource. PMP will use the configuration terminal mode to reset the passwords. You can enable remote reset of passwords of your cisco devices by providing the following credentials:

Credential
Description
Remote Login Method
PMP supports SSH and TELNET protocols by which connection could be established with the device for password reset. Select the required protocol

Remote Login Account

Login account for establishing connection with the device

User Mode Prompt

The prompt that appears after successful login

Enable Secret

This is for entering into privileged mode to perform password reset. If the remote login account has enough privileges to modify passwords, it is not necessary to specify enable secret

Enable Password

This is for entering into privileged mode to perform password reset. If the remote login account has enough privileges to modify passwords, it is not necessary to specify enable password

Enable Mode Prompt

This is the prompt that will appear after going into enable mode. For example, #

Account name required for login

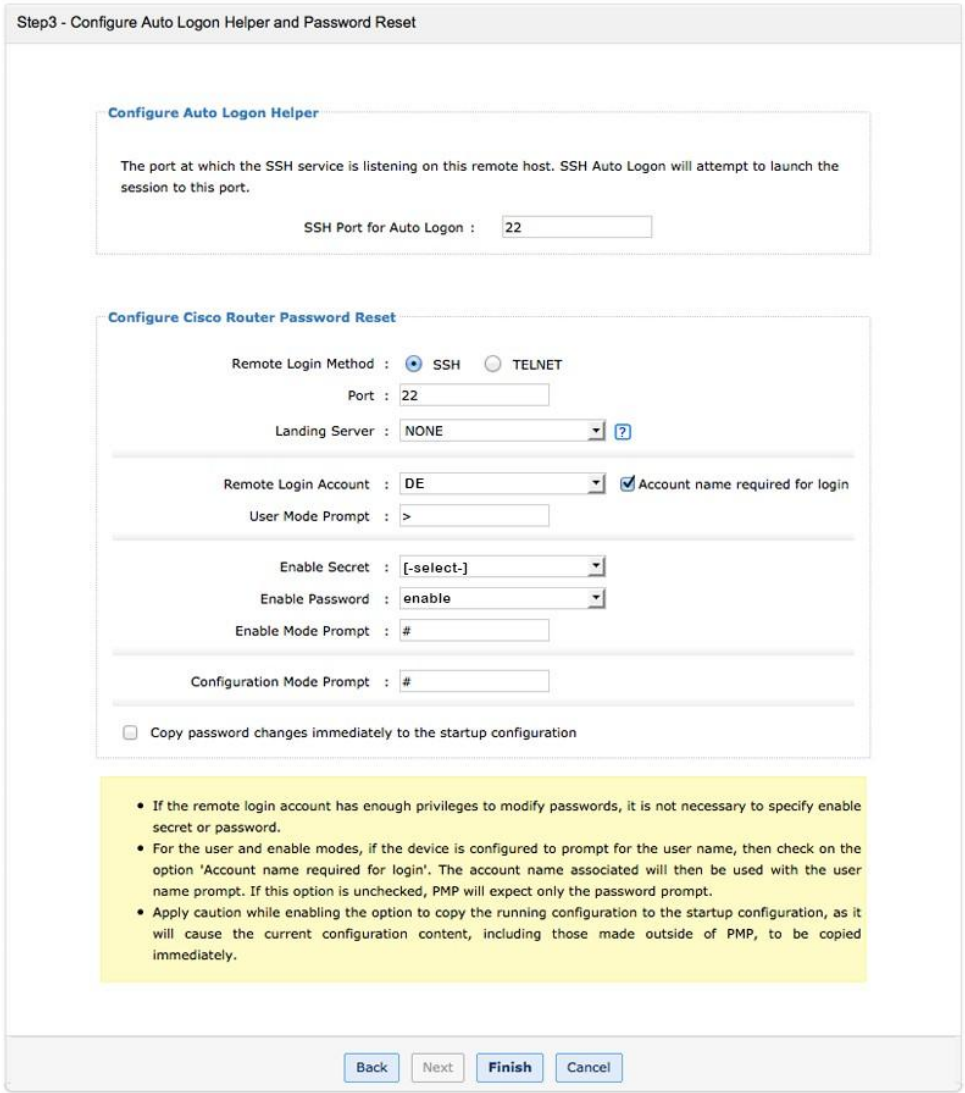
For the user and enable modes, if the device is configured to prompt for the user name, then check on the option 'Account name required for login'. The account name associated will then be used with the user name prompt. If this option is unchecked, PMP will expect only the password prompt.

Configuration Mode Prompt

To carry out any change to any feature/configuration of the device, you need to enter configuration mode. The prompt that will appear while going into configuration mode has to be entered here. For example, #" Primary Credentials

Copy Password Changes to Startup

If you want the password changes made to the running configuration from PMP to be applied to the startup configuration, select this checkbox. Exercise caution while enabling the option to copy the running configuration to the startup configuration, as it will cause the current configuration content, including those made outside of PMP, to be copied immediately.



For Juniper Netscreen Firewall Devices

Configure Auto Logon

PMP offers support to launch a secure direct connection through SSH to the resource from the web-interface. The configuration for the auto logon has to be made here. To connect through SSH, you need to specify the port to connect, if it is different than the default 22.

Configure Remote Password Reset

PMP requires Telnet or SSH service to be running in the resource. Admin Account and Prompt of Admin Account are required for PMP to login to the resource. You can enable remote reset of passwords of your Netscreen devices by providing the following credentials:

Credential

Description

Remote Login Method

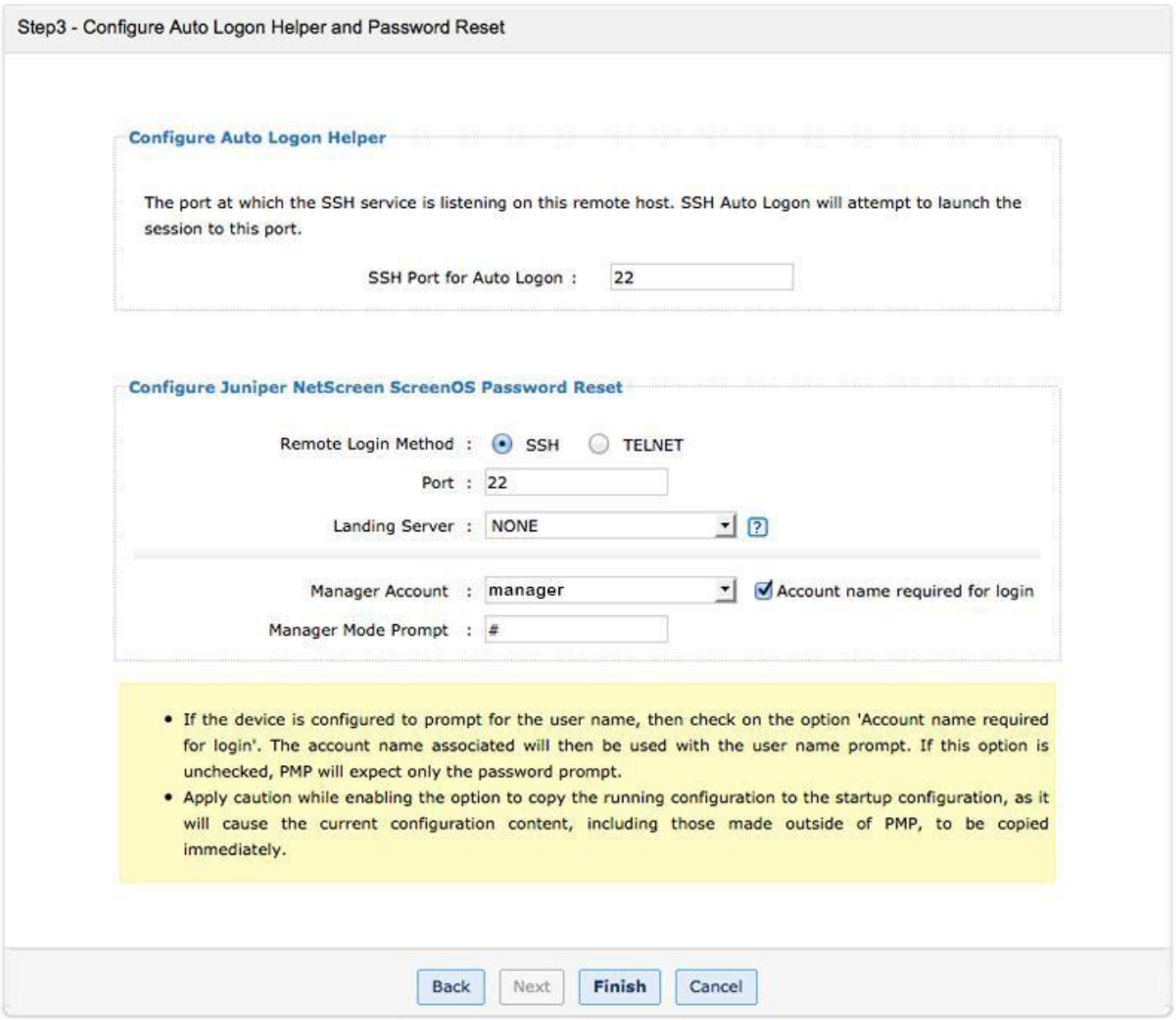
PMP supports SSH and TELNET protocols by which connection could be established with the device for password reset. Select the required protocol

Admin Account

Login account for establishing connection with the device. If the device is configured to prompt for the user name, then check on the option 'Account name required for login'. The account name associated will then be used with the user name prompt. If this option is unchecked, PMP will expect only the password prompt.

Admin Account Prompt

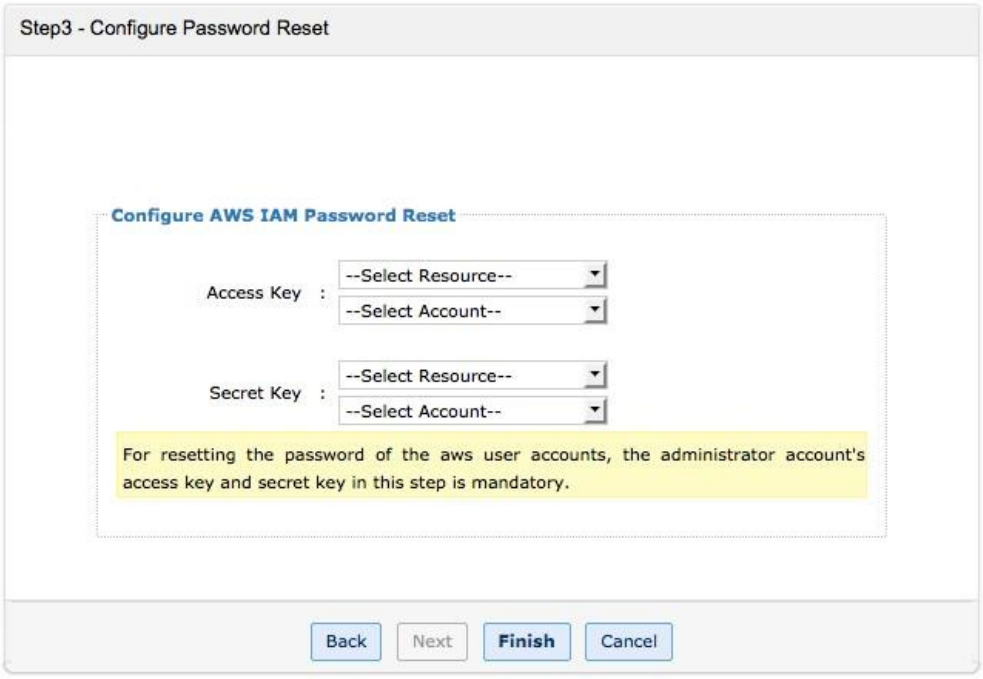
The prompt that appears after successful login



AWS IAM

Configure Remote Password Reset

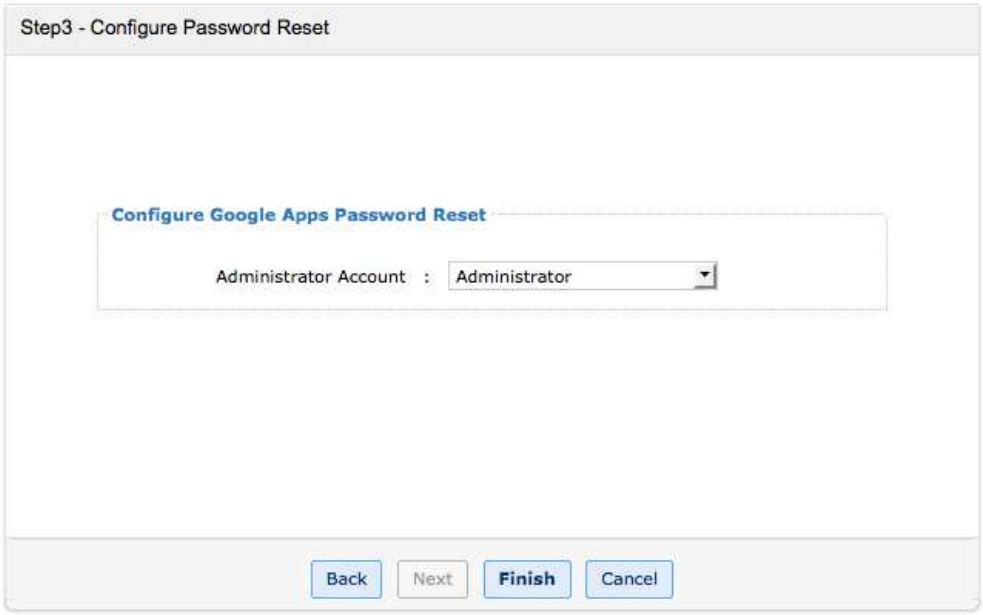
- Password reset for AWS IAM user accounts is done using AWS SDK.
- In order to proceed with the configuration in Step 3, the administrator account's access key and secret key are required.
- The access key and secret key should have been added as a password in Password Manager Pro. This password can be associated with an account of any resource type, which will eventually be used for remote synchronization.



Google Apps

Configure Remote Password Reset

- Password reset for Google Apps is done using Google Data APIs.
- To enable the Password reset option for GApps, an administrator account has to be selected so that it can be used to reset the passwords of other admin/user accounts.

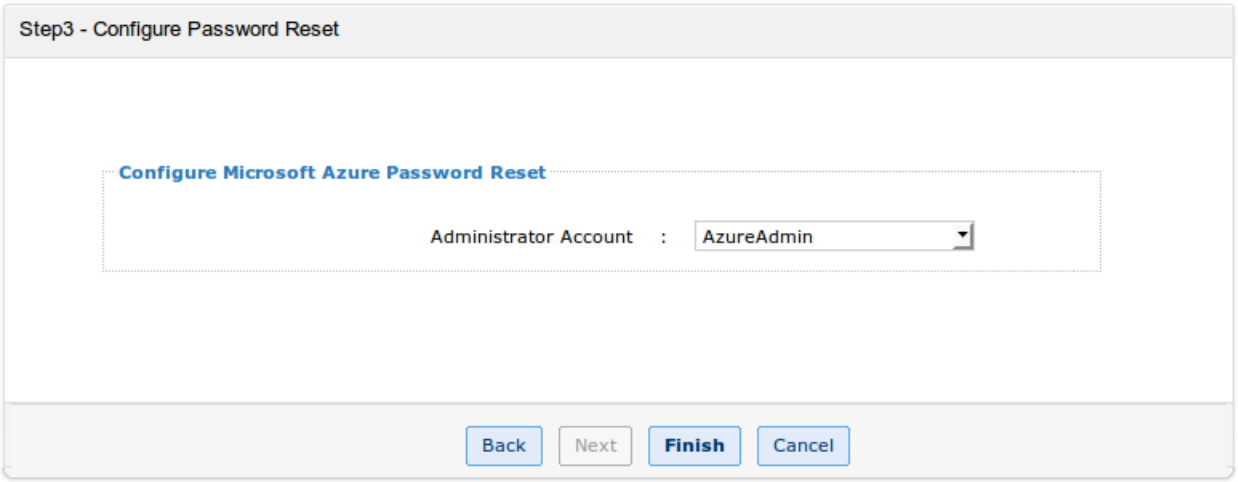


Microsoft Azure

Configure Remote Password Reset

- Password Reset for Microsoft Azure accounts is done using Powershell. Please note that Password Resets for Microsoft Azure Resources work only with Powershell 2.0 and above versions.
- For resetting the passwords of user accounts, an administrative account has to be selected to enable login from remote.

Note : Password Reset for Microsoft Azure user accounts can be carried out only if the product is installed on a Windows server/workstation as Microsoft Azure uses Powershell 2.0 and above versions. Also, the MSOnline module of Powershell needs to be installed.



Steps to download and install Windows Azure AD Module for Powershell

Before you can configure Microsoft Azure with Password Manager Pro for Password Synchronization, you have to install the appropriate version of the Windows Azure AD Module for Windows PowerShell for your operating system.

For 32-bit systems:

- Download and install the Microsoft Online Services Sign-In Assistant from here.
- Download and install the Windows Azure AD Module for Windows PowerShell from here.

or 64-bit systems:

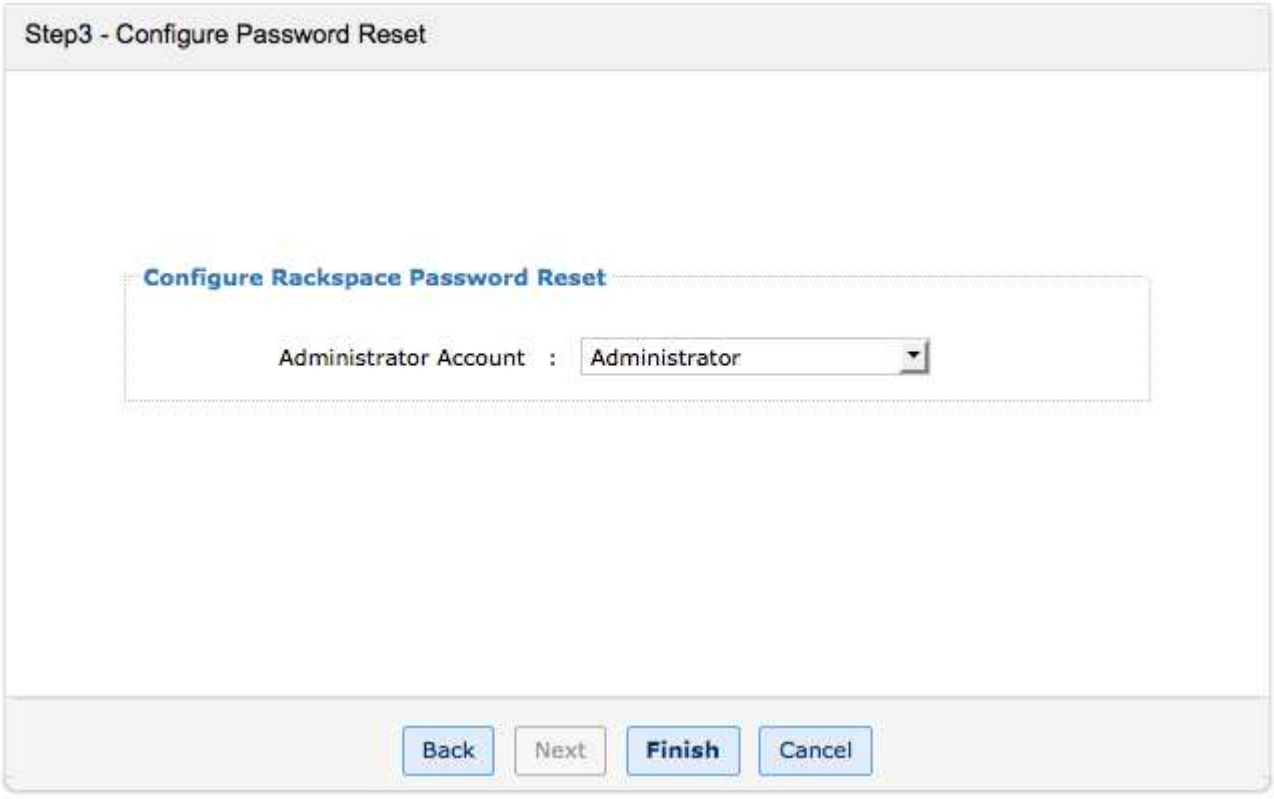
- Download and install the Microsoft Online Services Sign-In Assistant from here.
- Download and install the Windows Azure AD Module for Windows PowerShell from here.

- After installing the module, move MSOnline and MSOnlineExtended folders fromC:\Windows\System32\WindowsPowerShell\v1.0\Modules to C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules.

Rackspace

Configure Remote Password Reset

- Password Reset for Rackspace user accounts is done using Rackspace REST APIs.
- To carry out password resets, a Rackspace administrative credential is required which has to be selected as the admin account in Step 3.



Note : The following are the location-based Authentication End Points available for connection to the server.
US Based end point - https://identity.api.rackspacecloud.com/v2.0
UK Based end point - https://lon.identity.api.rackspacecloud.com/v2.0

Password reset using PMP agents

(Feature available only in Premium and Enterprise Editions. This procedure and document is applicable only for PMP versions 6400 and above. If you are using previous versions of PMP, click here for the document)

PMP provides the option to remotely change the password of select resources by deploying PMP agents. As of now, this facility is available for changing the password of servers - Windows, Windows Domain and Linux alone. Using this utility, you can change the password of a server present in a remote location, from the PMP web interface itself.
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 agent is useful in cases when,

- the PMP server runs in a Linux system and has to make password changes to Windows resources
- the required administrative credentials are not available in the PMP server to make the password changes from remote
- to change the password of domain accounts without the administrator credentials of the domain controller

Agent-Server One-way Communication

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.

The agent will periodically ping the PMP server through HTTPS to check if any operation (password reset or verify password) is pending for execution. The agent will then carry out the tasks and after completing them, it will notify back the PMP server with the results. So, when a task is to be executed by an agent, the PMP server will just trigger the task. The agent will get the list of tasks to be done at the remote host, when it contacts the server. That means, there will be some delay for execution of tasks depending on the time interval at which the agent contacts the server. By default, the agent pings the server once in 60 seconds. The interval is configurable.

Downloading the PMP Agent

The PMP agent package is dynamically created by the PMP server to include the SSL certificate of the PMP server, that is used for the HTTPS communication between the agent

and the agent. So, the only place to download the agent is from the 'Admin' tab of the PMP web GUI. The agent package is a zip file containing the necessary executables, configuration files and the SSL certificate. Download the agent based on the OS of the target and just unzip the package.

Installing the PMP Agent in Windows

The package has all the necessary configuration already created by the server. Make sure the account in the system in which the agent is installed has sufficient privileges required to modify passwords.

To install the PMP Agent as a Windows service,

- Open a command prompt and navigate to the PMP agent installation directory
- Execute the command 'AgentInstaller.exe start'

To stop the agent and uninstall the Windows service,

- Open a command prompt and navigate to the PMP agent installation directory
- Execute the command 'AgentInstaller.exe stop'

Configuring the time interval at which the agent should ping the PMP server

By default, the agent pings the server once in 60 seconds. The interval is configurable. To change this,

- Go to the PMP agent installation directory
- Open the file Agent.conf
- Modify the time interval value in seconds for the parameter ScheduleInterval to the value you require (in seconds)
- Restart the agent service

Installing the PMP Agent in Linux

The package has all the necessary configuration already created by the server. Make sure the account in the system in which the agent is installed has sufficient privileges required to modify passwords.

To install the agent as service

- Execute the command "sh installAgent-service.sh install" to install the agent as service

To install the agent as service

- Execute the command "sh installAgent-service.sh install" to install the agent as service

To start the agent

- Execute the command "sh installAgent-service.sh start"

To stop the agent

- Execute the command "sh installAgent-service.sh stop"

To uninstall the agent as service

- Use the command "sh installAgent-service.sh remove", in case you wish to remove PMP Agent as service

Configuring the time interval at which the agent should ping the PMP server

By default, the agent pings the server once in 60 seconds. The interval is configurable. To change this,

1. Go to the PMP agent installation directory
2. Open the file Agent.conf
3. Modify the time interval value in seconds for the parameter ScheduleInterval to the value you require (in seconds)
4. Restart the agent service

To remotely change the password,

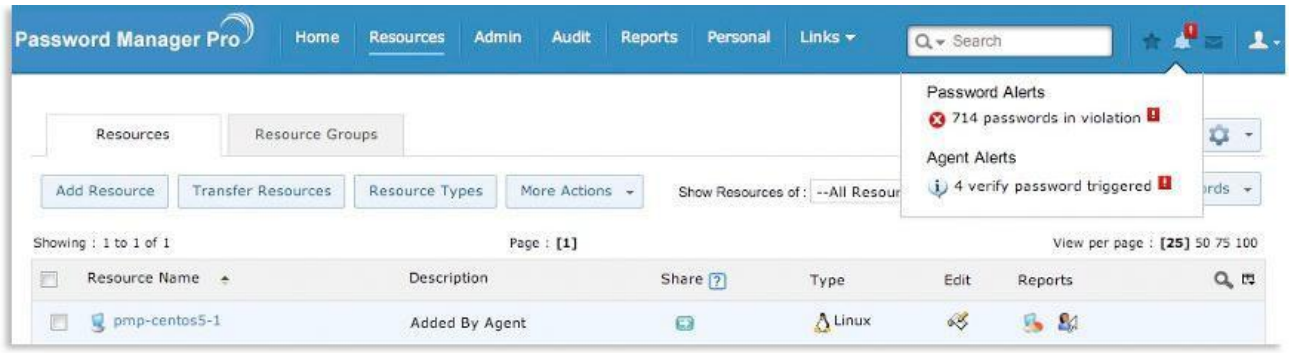
- Go to 'Resources' Tab
- Click the name of the resource whose password has to be changed remotely
- Click the "Change Password" icon

To find if any tasks are pending for execution by the agents,

The remote password reset and other tasks triggered by the user in PMP and awaiting execution by the agents, can be found from by clicking the icon on the top pane of the GUI. The status of the previously triggered tasks can also be known from here.
The notification icon will provide the following information:

- Number of password reset actions triggered
- Number of password verify actions triggered
- Status of password reset action triggered earlier
- Status of verify password action triggered earlier

This listing will be use-specific - that means, users get to know the status of only those tasks triggered by them.



Troubleshooting

If the password changes do not take effect in the target systems, check

- if the account in which the agent is installed has sufficient privileges to make password changes
- by default, the agent tries to communicate with the PMP server through the port 7272. If you have configured the default PMP port, you need to make the agent communicate with the new address.

Configuring Remote Password Reset for Resources in Bulk

(Feature available only in Premium and Enterprise Editions)

Overview

Remote password reset is one of the most useful features of Password Manager Pro. As you may be aware, to carry out remote password reset, you need to provide root account/administrator credentials while adding the resource. When you import resources in bulk, you might have to manually edit the resources one by one to enter the credentials, which would be cumbersome. To enable editing of the resources in bulk for entering the credentials, PMP provides the bulk edit option.

You can choose a set of resources and configure remote password reset for the chosen resources in bulk. For every resource type that is part of the chosen list, you can input details that are required to perform remote password resets.

This document explains how to edit the resources in bulk.

How to Edit the Resources in Bulk?

The basic design of the bulk resource edit feature is such that the same configuration will be applied to all the resources of a particular resource type. For example, assume that you want to configure remote password reset for 50 resources - 25 Linux resources and 25 Oracle database resources. Assume that you have chosen all the 50 resources and provide the credentials for Oracle database, the credentials will be applied only to the 25 Oracle database resources. It will not be applied to the remaining 25 resources. However, after applying the credentials for the Oracle resources, if you apply the credentials for Linux resources, it will be updated for the remaining 25 Linux resources.

So, you must ensure that you choose only the resources that have similar configuration. This operation will simply overwrite the current password reset configuration, if any, of the chosen resources.

To edit the resources in bulk for configuring remote password reset:

1. Go to Resources tab
2. Select the resources for which you wish to configure remote password reset
3. Click the link Configure Password Reset from More Options listing

In the UI that opens up,

1. Select the required 'Resource Type' from the LHS
2. Enter the credentials based on the resource type chosen
3. Click Save

Once you do this, the credentials entered by you will be updated for all the chosen resources that were of the same type as the one selected by you in the 'Configure Password Reset' UI.

Note:

- The above operation will simply overwrite the current password reset configuration, if any, of the chosen resources.

Importing Resources

Importing Resources from Text File

You can import resource details from a CSV file using the import wizard. All the lines in the CSV file should be consistent and have the same number of fields. CSV files having extensions .txt and .csv are allowed.

To import users from a CSV file,

- Go to "Resources" >> "More Actions" >> "Import Resources"
- Browse and select the file and click "Next"
- In your CSV file, the entries could be present in any order. You can choose which field in the CSV file maps to the corresponding attribute of the PMP resource & account. Both the default and the user defined attributes will be listed in the wizard and the user defined attributes have been defined before the import operation. If a resource contains multiple user accounts, then the resource fields will have to be repeated for each user account in the CSV file
- If you have resources with attributes that can not be placed in the CSV file (like files for the File Store resource type), you can leave those entries blank in the CSV file and later edit the resource and update the attribute value
- If the list of resources imported by you contains any of the already existing resources, they will not be added to PMP by default. If you it to be overridden, you need to select the option "Overwrite existing resources".
- Click "Finish"
- The result of every line imported will be logged as an audit record. For troubleshooting errors during import, refer to the log file in the location\logs\pmp0.txt
- Important Note: After importing resources, if you to configure password reset with the target systems, you need to do it by editing resources.
- Importing Resources takes time ...
  When you try to import a large number of resources, it would take a while to import all of them to PMP inventory. When the importing process is in progress, you will notice the rotating gif at the RHS end. Once, it is done, you will notice the message "Resources Imported Successfully".
- My resources have additional fields ..
  You can import the additional fields too. But, prior to importing the resources, you need to add those custom fields to PMP.
- I do not have some of the fields that are listed mandatory for PMP in my CSV file..
  That is not a problem. Only 'Resource Name' and 'Account Name' fields are mandatory. So, you can import whatever you have.

Importing Resources from Active Directory

You can import the computers in your domain and the user accounts part of those computers as resources in PMP.

To import resources from domain,

- Go to "Resources" tab in the web interface
- Click the link "Import from Domain" present in the drop-down of "More Actions" button
- 'Import Resources from Active Directory' UI will open

The first step is to provide credential details and importing resources from AD. PMP automatically discovers and lists all the Windows domains from the Windows domain controller of which the running PMP is part of. You need to select the required domain and provide domain controller credentials.

In the UI,

- Select the required Domain Name from which the resources (computers) are to be imported
- Specify the DNS name of the domain controller. This domain controller will be the primary domain controller.
- In case, the primary domain controller is down, a secondary domain controllers can be used. If you have secondary domain controllers, specify their DNS names in comma separated form. One of the listed secondary domain controllers will be used. When you use SSL mode make sure the DNS name specified here matches the CN (common name) specified in the SSL certificate for the domain controller
- Enter a valid user credential (user name and password) having admin privilege or the name of the user present in Domain Admins group
- For each domain, you can configure if the connection should be over an encrypted channel for all communication. To enable the SSL mode, the domain controller should be serving over SSL in port 636 and you will have to import the domain controller's root certificate into the PMP server machine's certificate.

As mentioned above, to enable SSL mode, the domain controller should be serving over SSL in port 636. If the certificate of the domain controller is not signed by a certified CA, you will have to manually import the certificate into the PMP server machine's certificate store. You need to import all the certificates that are present in the respective root certificate chain - that is the certificate of the PMP server machine and intermediate certificates, if any.

To import domain controller's certificate into PMP machine's certificate store: (you can use any procedure that you normally use to import the SSL certificates to the machine's certificate store. One example is given below)

- In the machine where PMP is installed, launch Internet Explorer and navigate to Tools >> Internet Options >> Content >> Certificates
- Click "Import"

- Browse and locate the root certificate issue by your CA
- Click "Next" and choose the option "Automatically select the certificate store based on the type of certificate" and install
- Again click "Import"
- Browse and locate the domain controller certificate
- Click "Next" and choose the option "Automatically select the certificate store based on the type of certificate" and install
- Apply the changes and close the wizard
- Repeat the procedure to install other certificates in the root chain

PMP server can now communicate with this particular domain controller over SSL. Repeat these steps for all domain controllers to which you want PMP to communicate over SSL. Note that the DNS name you specify for the domain controller should match the CN (common name) specified in the SSL certificate for the domain controller.

- If you want to import only a particular computer, enter the required user name(s) in comma separated form
- Similarly, you can choose to import only specific resource groups (i.e. computer groups) or OUs from the domain. You can specify the names in the respective text fields in comma separated form. PMP resource groups will be created with the name of the corresponding AD computer groups, prefixed by the domain name.
- Whenever new computers get added to the AD, there is provision to automatically add them to PMP and keep the resource database in sync. Enter the time interval at which PMP has to query the AD to keep the resource database in sync. The time interval could be as low as minutes or it can be in the range of hours and days
- Click "Import". Soon after hitting this "Import" button, PMP will start adding all computers

Important Note: After importing resources, if you want to configure remote password reset for the target systems, you can do it from Resources > More Option > Configure Password Reset.

Editing Resources

At any point of time, you can edit any of properties of the resource added by you. To edit a resource, go to the "Resources" tab and click the "Edit" icon present against the resource name. In the UI that pops-up, edit the required property and click "Save". The required change will get reflected in the view.

Note: When you edit a resource, the account details that are part of the resource will remain unaffected.

Adding a new account to an existing Resource

You can add any number of user accounts to an already existing resource. To add an account,

- Go to "Resources" tab in the web interface
- Click the particular resource to which you wish to add another account
- Click the button "Add"
- In the GUI that opens, enter details about the account to be added
- Click "Add". If you want to add more accounts, add them too
- Click "Save"

Deleting Resources

You can delete those resources that are no longer required from the PMP's resources list. If you delete a resource, all the accounts and passwords that were part of that resource would also be deleted permanently. The entries would be removed from the database once and for all.

To delete a resource,

- Go to "Resources" tab in the web interface
- Select the particular resource(s) that is to be deleted
- Click the button "Delete Resources"

Copying Resources

If you have many resources with identical properties, you may just add one resource and get multiple copies of the same in PMP. This simplifies the resource addition process in such scenarios.

You can copy a single resource or multiple resources and duplicate them as separate resources in PMP. The duplicated resources could then be edited to suit your requirements.

To copy resources,

- Select the specific resource or resources to be copied
- Go to "Resources" >> "More Actions" >> "Copy Resources"

In the UI that opens, you need to select the specific properties, which you want the copied resources to inherit:

- Resource(s) level and account(s) level sharing can be inherited. When you select this, all the sharing permissions of the original resource will be inherited by the copy or copies
- Access control settings - if you select this option, the access control setting configured for the original resource, will be inherited by the copy or copies
- You can also copy all the accounts that are part of the resource(s) being copied
- Password history of account(s) that are part of the resource(s) being copied
- You can also add the resultant copy resource to all the resource group(s) to which the original resource(s) belong(s)
- You can also specify the number of copies you want
- Click "Save"

You will now see the required copy or copies in "Resources" tab.

Important Note:The copying operation does not affect the original resource in anyway.

Viewing Account Details

To view the accounts that are part of a resource, go to the "Resources" tab and click the particular resource name. The accounts would be displayed.

Viewing Passwords

By default, passwords are shown in hidden form behind asterisks. Just click the asterisks to view the password in plain text. The passwords are shown for 10 seconds only. After that, they will be automatically hidden. If you want to view, you need to click again. If you want to modify the default 10 seconds, you can do so from General Settings.

Enforcing Users to Provide a Reason for Viewing Passwords

By default, when a user tries to retrieve the password of a resource, on clicking the asterisks, the passwords appear in plain text. If you want to force your users to provide a reason why access to the password was needed, you can enable the option "Force users to provide reason while retrieving the passwords" in General Settings.

Allowing password users and auditors to retrieve passwords for which 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, you can take a decision on allowing/restricting access to passwords and implement the same through the option "Allow password users and auditors to retrieve passwords for which auto logon is configured" in General Settings.

Copying Passwords

PMP leverages clipboard utility of browsers to copy passwords when you intend to copy and paste passwords. Click the copy icon present by the side of the passwords to copy them. The copied passwords will be available for pasting for 30 seconds.

Changing Passwords

To change the passwords of user accounts, click the "Change Password" icon against the account name. In the UI that pops-up, enter the new password and confirm the same and then click "Save". Here, password policy set by the administrator for this resource would get

enforced. For example, if the administrator has set "Strong" as the password policy, you would be allowed to change the password only if you enter a password which is strong enough in accordance with the PMP settings.

If your account belongs to any of the types - Windows, Windows Domain, Linux, IBM AIX, HP UNIX, Solaris, Mac OS, MS SQL server and Cisco Devices (IOS, CatOS, PIX), you have the option to synchronize the new password in the remote resource too. In this case, if there is a failure in updating the password in the resource, password changes will not be saved locally also.

Verifying the Integrity of Passwords with actual Resource
(Feature available only in Premium and Enterprise Editions)

Passwords of resources such as servers, databases, network devices and other applications are stored in PMP. It is quite possible that someone who have administrative access to these resources could access the resource directly and change the password of the administrative account. In such cases, the password stored in PMP would be outdated and will not be of use to the users who access PMP for the password. PMP provides option for checking the validity of passwords at any point of time on demand and also at periodic intervals.

On demand verification for password validity could be performed for a single account or for all the resources/accounts stored in the PMP application.

To verify the integrity of the password of a single account,

- Go to "Resources" or "Home" tab
- Select the account whose password has to be verified for synchronization
- Click the verify password icon present next the 'change password' icon
- PMP will try to establish connection with the target system. Once the connection is established, it tries to login with the credentials stores in PMP. If login does not succeed, PMP concludes that the password is out of sync. In case, PMP is not even able to establish connection with the system due to some network problem, it will not be taken as password out of sync.

Note: Password Verification will work only for the accounts for which 'Remote password reset' has been enabled.

To verify all the passwords stored in PMP,

- Go to "Reports" tab >> "Password Integrity" report
- Click the link "Run Integrity Check"
- PMP will try to establish connection with the target systems for all the accounts for which remote password reset has been enabled. Once the connection is established, it tries to login with the credentials stores in PMP. If login does not succeed, PMP concludes that the password is out of sync. In case, PMP is not even able to establish connection with the system due to some network problem, it will not be taken as password out of sync. A consolidated notification would be emailed to all the administrators and auditors.

Editing Account Details

At any point of time, you can edit the details of any of the accounts. To edit an account, go to the "Resources" tab, click the resource of which the account is a part and the click the "Edit" icon present against the account name. In the UI that pops-up, edit the required property and click "Save". The required change will get reflected in the view.

Copy Accounts

A single account or multiple accounts could be copied and added under one or more resources. The replicated accounts could then be edited to suit your requirements. When you want to have the same identical accounts under many resources, this will help in adding the accounts with ease. The copying operation does not affect the account being copied in anyway.

To copy one or more accounts, go to the "Resources" tab, click the resource of which the account is a part and select the account or accounts to be copied. Then click the "Copy" button. In the UI that pops-up, you can choose to inherit the share permissions also (the new account will also be shared with all those who had permission to view the parent account). You can also specify the number of copies required. The account(s) will appear under the selected resource(s).

Move Accounts

A single account or multiple accounts part of this resource could be moved under another resource. When you do so, the selected account(s) will be removed from the present resource.

To move one or more accounts, go to the "Resources" tab, click the resource of which the account is a part and select the account or accounts to be moved. Then click the "Move" button. In the UI that pops-up, you can choose to Move the share permissions also (the new account will also be shared with all those who had permission to view the account being moved). The account(s) will be removed from the present resource and it will appear under the selected resource(s).

Viewing Password History

The history of changes done to the passwords are captured in the form of password history. Information such as the old password, modified by whom, from which machine and the time at which it was modified are all captured in history. To view password history of an account, go to the "Resources"tab, click the resource of which the account is a part and the click the icon  present beside the "Last Modified" column. In the UI that pops-up, password history would be displayed.

Resource Groups

Resources can be grouped together for easier management. The grouping can be done either by specifying a set of criteria or by specifying individual resources. When you provide a criteria, whenever a new resource is added that matches the criteria, it also becomes part of that group.

Resource groups created by the administrator users can be shared with other users or user groups. Whenever resources get added or deleted from a group, it affects the password access shared through the group. That is, users who are shared with the group can see passwords of only the resources that are part of the group at that point in time.

Password Manager Pro provides the option to maintain resource groups in hierarchical structure providing a tree view for navigational convenience. From the "Home" tab of PMP web-interface, you can view the hierarchical structure of the resource groups in tree form. You can also navigate to any desired group or sub-group directly and view the resources within. Password policy can be specified for the resource groups, which will be used for password generation for resources of that group. Note that a password policy specified for a resource will override the group-level setting.

The resource grouping helps in carrying out operations in bulk on all the resources of the group.

To add resource groups,

- Go to "Resources" tab in the web interface
- Click "Resource Groups" tab (alternatively, you can launch this page directly through the "Add Resource Group" link under the "Links" tab)

In the Add Resource Group UI that opens,

- Choose your option for creating a resource group. Either you can create a group based on certain matching criteria or you can pick resources from the list of resources and assign them to the group.

Creating groups based on matching criteria,

- Select the option "Based on Criteria"
- Enter the name for the group against the text field "Group Name"
- Provide a "Description" for the group. It will be helpful for future reference
- Select a "Password Policy" for the group

- Nested Groups: If you want to make the resource group being added as the sub-group of an already existing resource group, select the required group from the drop-down against the field "Sub Group of". The group selected by you will become the parent group for the resource group being added
- Specify the exact criteria based on which you want to create the group. Here, you have many options to choose from - you can search for resources based on resource name, resource type, resource description and user accounts and filter the search in fine-grained manner based on the criteria such as "contains", "does not contain", "equals" "not equal", "starts with" and "ends with".
- Once you specify the criteria, click "Search" if you want to view the list of resources that will become part of this group
- Click "Add" to add your resource group

Creating groups based on resources,

- Select the option "Based on Resources"
- Enter the name for the group against the text field "Group Name"
- Provide a "Description" for the group. It will be helpful for future reference
- Select a "Password Policy" for the group. If you select "Strong" (say), it would be applicable to all the members of this resource group
- Nested Groups: If you want to make the resource group being added as the sub-group of an already existing resource group, select the required group from the drop-down against the field "Sub Group of". The group selected by you will become the parent group for the resource group being added
- Select the required resources to be added to this group
- Click "Save" to add your resource group

How do I view the resources belonging to a particular resource group?

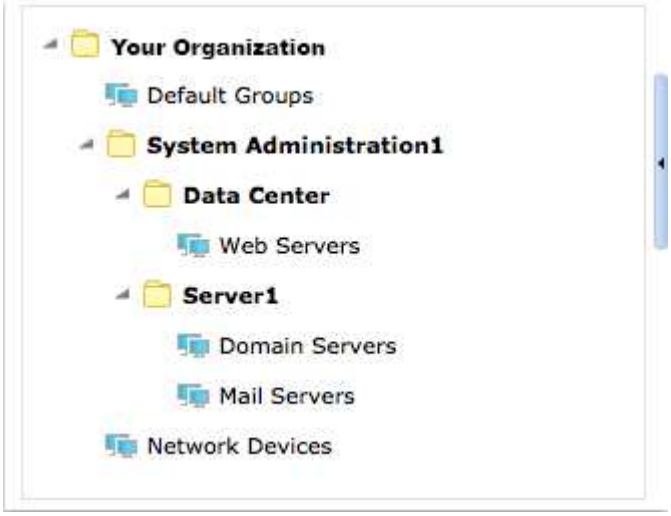
- To view the resources belonging to a particular Resource Group,
- go to "Resources" tab
- select the required Resource Group (whose resources you want see) from the drop-down "Show Resources of"
- all the resources belonging to that group will be displayed
- How do I view the hierarchical order of resource groups?
- To view the hierarchical order of the resource groups as well the resources that are part of the respective group,
- go to "Home" tab
- on the LHS, the resource groups are displayed in tree view. Select the required Resource Group (whose resources you want see)

- all the resources belonging to that group will be displayed
- To view the hierarchical order alone,
- go to "Resources" >>> "Resource Groups" tab
- click "Show Tree View"
- Is it possible to edit the name of the root node of the nested resource group tree?
- Yes, the name of the root node can be edited. To edit it.
- go to "Resources" >>> "Resource Groups" tab
- click "Show Tree View"
- in the UI that opens, click the "Edit" button present near the filed "Root Node Name" and click "Update"

Nested Resource Groups

Tree View / Hierarchical Arrangement of Resource Groups

Password Manager Pro provides the option to maintain resource groups in hierarchical structure providing a tree view. For example, assume that your organization contains some departments/sections in the following hierarchy. Resource Groups pertaining to the departments could be arranged in the following order:



That means, you can group the resources belonging to the respective sections and create sub-groups as required. From the "Home" tab of PMP web-interface, you can view the hierarchical structure of the resource groups in tree form. You can also navigate to any desired group or sub-group directly and view the resources and passwords within.

Important Note:

1. Every administrator and password administrator can create his/her own tree with the resource groups they own and manage.
2. When you create a nested resource group, by default, the name of the root node of the tree will have your login name. For example, if you are logging into PMP as "admin", the name of the root node will be "admin's Group". If you want to have a different name for the root node, you can edit it as explained below.

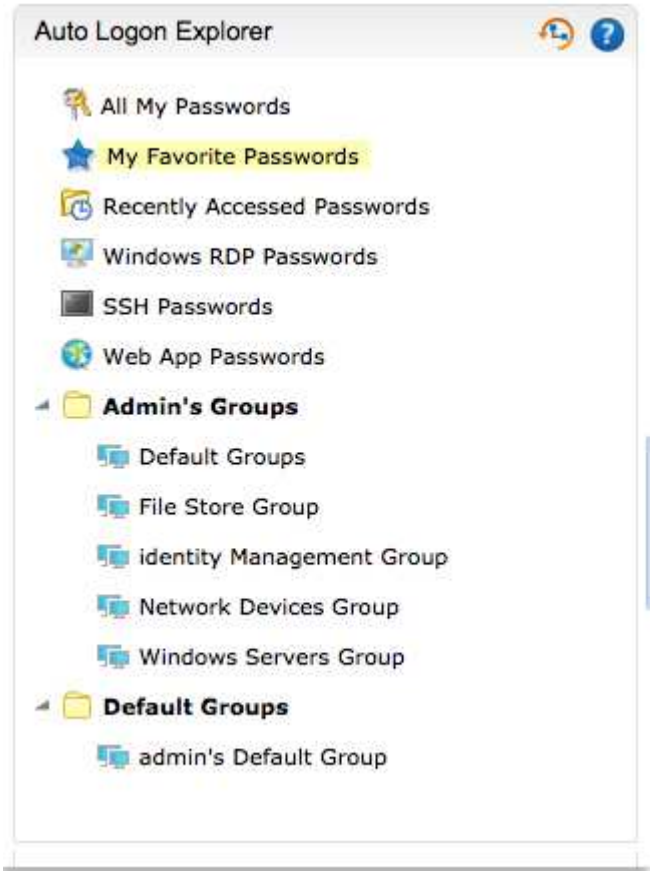
Nested Resource Groups are purely for navigational convenience only. You can just view the passwords belonging to the respective resource groups directly. The sub-groups will not inherit sharing and other configurations like scheduled password reset, password action

notification and other events from their parents.

Components of Nested Resource Group Tree

Nested Group Tree, depicted as "Password Explorer" as present in the LHS of the "Home" tab of PMP web-interface, has the following components:

- All My Passwords
- My Recent Passwords
- My Favourite Passwords
- Nested Resource Group Tree

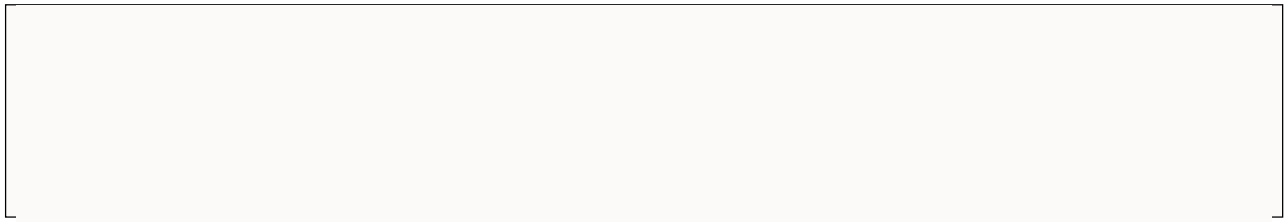


All My Passwords View (To view all the passwords owned by you and the ones shared to you)

All the passwords that are owned by you and the ones shared to you will be displayed. If you own resources or some resources had been shared to you, the resources will be displayed.

To access this,

- Go to the "Home" >> "My Passwords"
- On the LHS, you will find "Password Explorer" >> Click the link "All My Passwords"



My Recent Passwords

The passwords that were accessed by you most recently will be displayed under this section to facilitate easy access to a recently used password. The recently accessed passwords will be shown on top of other available passwords.

To access this,

- Go to the "Home" tab >> "My Passwords"
- On the LHS, you will find "Password Explorer" >> Click the link "My Recent Passwords"

My Favourite Passwords

PMP provides the option to retrieve your favourite passwords with ease. You need not have to search for the resources to locate your favourite passwords. In front of all the accounts, you will find a greyed out 'star' icon. When you click the star, it will turn blue and the respective password will be marked as your favourite password. By clicking the link "My Favourite Passwords", you will be able to retrieve your favourite passwords immediately. At any point of time, you may remove any password from the 'favourites' list by unmarking the star icon from either "All My Passwords" view (Home Tab) or from the "Resources" tab.

Important Note: Assume that you have marked a password that was shared by an admin to you as favourite. The admin revokes the share permission for that particular password. When you click the 'My Favourite Passwords' link, you will see the resource still listed there. However, if you try to retrieve the password, you will not be permitted to view the password. Also, the resource would be removed from the 'My favourites'. By default, you will land up in "My Favourite Passwords" section only.

Nested Resource Group Tree

This tree consists of the following components:

1. Resource group tree created by you. In this tree, all the resource groups and sub-groups owned by you will be depicted. As mentioned above, by default, the root node of your tree will be named as - 's Group. If you want, you can edit the name of the root node to make it more meaningful or to make it reflect your organizational structure. For example, if you are a Database Administrator, you can name the root node as "Database Passwords". Click here to know how to edit/rename the root node. You can click any desired group or sub-group to view the resources and passwords therein.
2. Resource group trees shared to you by other admins. Note that only the groups that the other admins has shared to you will appear in the tree under his/her root node. For example, if an admins has created a tree with 10 groups but had shared only 3 groups with you, you will only see those 3 groups under his/her tree.

Important Note:

1. The resources and passwords that are individually shared and not through groups, which are also not part of any of the shared resource groups, will not be found under the tree. They will listed under "All My Passwords" only.
2. Super administrators will see the entire tree of all other administrators and password administrators under their 'Password Explorer' in the 'Home' tab
3. Password users will not be able to create nested resource groups, but they can see the groups that have been shared to them in tree form.

Constructing Nested Resource Groups

Creating groups based on matching criteria,

See the section "Creating Resource Groups" section of the help documentation.

Creating groups based on resources,

See the section "Creating Resource Groups" section of the help documentation.
Guidelines on Nested Resource Group Construction (for admins & password admins)
Though the nested resource groups are mainly intended for navigational convenience, by properly creating the tree, you can leverage a lot of benefits, mainly ease of use.
Assume that you are a Database Administrator responsible for managing the passwords of various databases. In this case, you can construct the resource group tree as explained below:

- By default, the root node of your resource group tree will have your login name
- Rename it as "Database Passwords"

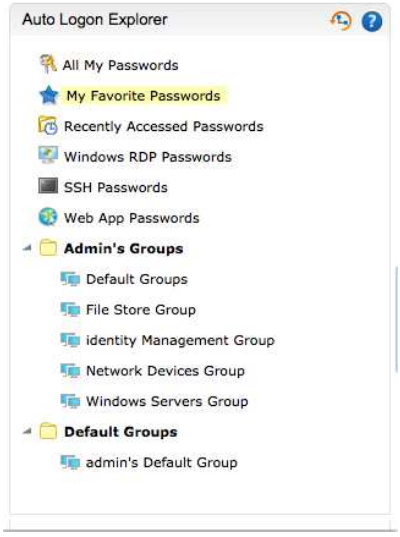
- Create a resource group for each database that you own - say, My SQL Passwords, MS SQL Passwords, Oracle Passwords, Sybase Passwords etc
- All these resource groups could be made as the sub-groups of the root node - Database Passwords

Once you do this, you will see your resource group tree as shown below in the "Home" tab of PMP web-interface:

Some More Examples:

A Network Administrator's Tree Structure

In case, you are a Network Administrator is managing Network Devices of his organization. You may name your root node as "All Network Devices" and have the tree as shown below:



Applications Management team

Assume that you belong to the Applications Management team and responsible for

managing various IT applications. You may name your root node as"All Applications". The hierarchical resource group could look like:

- How do I view the resources belonging to a particular resource group?
  To view the resources belonging to a particular Resource Group,
  - go to "Resources" tab
  - select the required Resource Group (whose resources you want see) from the drop-down "Show Resources of"
  - all the resources belonging to that group will be displayed

- How do I view the hierarchical order of resource groups?
  To view the hierarchical order of the resource groups as well the resources that are part of the respective group,
  - go to "Home" tab
  - on the LHS, the resource groups are displayed in tree view. Select the required Resource Group (whose resources you want see)
  - all the resources belonging to that group will be displayed

  To view the hierarchical order alone,
- go to "Resources" >>> "Resource Groups" tab
- click "Show Tree View"
- Is it possible to edit the name of the root node of the nested resource group tree?
  Yes, the name of the root node can be edited. To edit it.

- go to "Resources" >>> "Resource Groups" tab
- click "Show Tree View"
- in the UI that opens, click the "Edit" button present near the filed "Root Node Name" and click "Update"

Allowing Administrators to Manipulate the Nested Resource Group Explorer Tree

PMP offers provision to allow admin users to manipulate the entire explorer tree structure as they wish. Through a configuration setting in "General Settings", PMP administrator can enable this option. Once this is enabled, PMP creates an organization wide, global explorer tree structure containing the names of resource groups under a root node. Any administrator in PMP would be able to create/edit the explorer tree structure of resource groups. The tree structure will be accessible to all admins, password admins and end users. Admins and password admins can add their resource groups anywhere into the global tree and the whole structure will be available for view to all the end users.

This feature allows depicting resource groups of your organization in the form of a global tree for easy access, identification and navigation. Users can view the resource groups in the same structure as that of the internal grouping structure in your organization. Externally the tree structure depiction will be the same for all the members of the organization (that means all the users will see the entire structure). But, the users will be allowed to view only the resources that are owned by them and the ones shared to them. The resource groups that are not related to them will be shown as empty sub-nodes (without any resources inside) in the explorer tree.

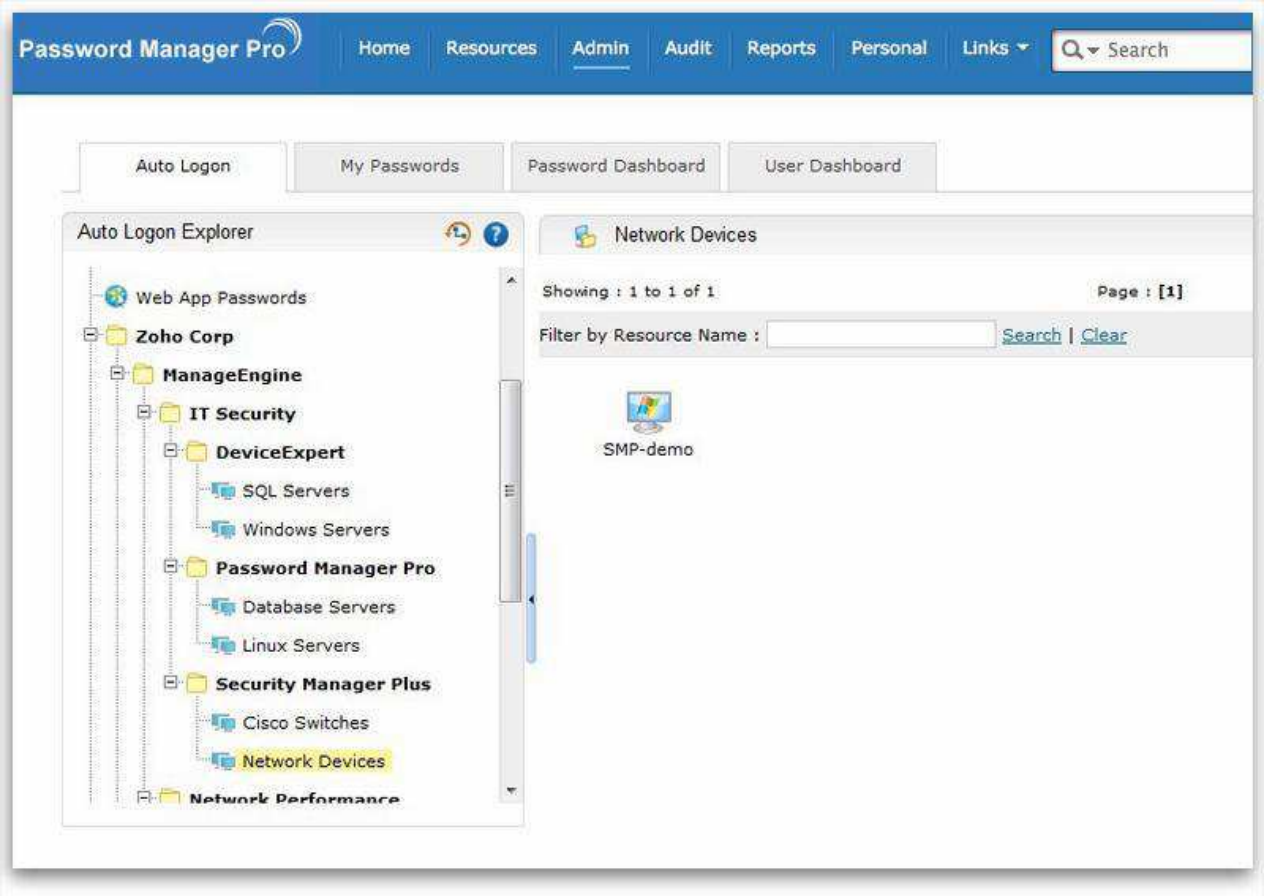
How to Enable this Option?

- Navigate to "Admin" >> "General" and click "General Settings"
- Select the option "Password Retrieval"
- Select the check box "Allow all admin users to manipulate the entire explorer tree" and click "Save"

How to Manipulate the Tree Structure?

- Navigate to the "Home" tab and click "My Passwords" or "Auto Logon"
- You will see the Resource Groups of your organization as a tree structure under a root node
- Just right-click the name of any node or sub-node to edit, modify or delete. You can manipulate the structure in any manner you want. The "delete" operation here just deletes the particular structure in the tree. It does not delete the resource.

- If you have committed an error in manipulation, you can 'undo' the operation immediately
- In addition, the admin users have the privilege to view the history of the manipulations done on the tree structure. They can revert to any former structure anytime just by a click.



Sharing Resources / Resource Groups Among Users

You can share your resources and passwords / resource groups with other users and user groups. When you share a resource, all the passwords of that resource are shared. Similarly, when a resource group is shared, all the resources part of that group will be shared. While sharing the resources / resource groups, you can set privileges for the user(s) who get the share:

View only privilege	Modify Privilege	Manage privilege
User can only access the password	User can both access and modify the password(s) that are shared. The Modify privilege does not allow the other users to change any other attribute of the resource.	You can delegate complete management of a resource group and the associated resources. This includes providing share permissions to other users also.

You can share

- an individual account within a resource to a user or a user group
- a resource to a user or a user group
- a resource group to a user or user group

Note: Manage privilege can be assigned only at resource & resource group levels. Not available for individual accounts.

You can perform the sharing operation in any combination from the above list.

Case 1: Share a particular account(s) to a User or User Group

- Go to "Resources" Tab
- Search/select the particular user account to be shared
- If you want to share the account with a user/users, click the icon  present under the column "Share" against the particular account. In the UI that opens search/select the user(s) to whom the account is to be shared. Decide about the permissions "View" or "Edit" and then move the user to the respective box (i.e view or edit). Click "Save". The account is shared.

- If you want to share the account with a usergroup(s), click the icon  present under the column "Share" against the particular account. In the UI that opens search/select the user group(s) to which the account is to be shared. Decide about the permissions "View" or "Edit" and then move the user group(s) to the respective box (i.e view or edit). Click "Save". The account is shared.

Note: When you share a particular account to a user group, the account will be visible to all the members of the group. Also, the permissions granted to the user group (view/edit) will be applicable for all the members.

Case 2: Share a resource to a User or User Group

- Go to "Resources" Tab
- Search/select the particular resource to be shared
- If you want to share the resource with a user/users, click the arrow mark against the particular resource present under the column "Share". Select the option "Share with Users" and in the UI that opens search/select the user(s) to whom the resource is to be shared. Decide about the permissions "View" or "Edit" or "Manage" and then move the user to the respective box (i.e view or edit or manage). Click "Save". The resource is shared.
- If you want to share the resource with a usergroup(s), click the arrow mark against the particular resource present under the column "Share". Select the option "Share with User Groups" and in the UI that opens search/select the user group(s) to which the resource is to be shared. Decide about the permissions "View" or "Edit" or "Manage" and then move the user group to the respective box (i.e view or edit or manage). Click "Save". The resource is shared.

Note: When you share a particular resource to a user group, the resource and all its accounts will be visible to all the members of the group. Also, the permissions granted to the user group (view/edit) will be applicable for all the members.

Case 3: Share a Resource Group to a User or User Group

- Go to "Resources >> Resource Group" Tab
- Search/select the particular Resource Group to be shared
- If you want to share the Resource Group with a user/users, click the icon  present under the column "Share" against the particular Resource Group. In the UI that opens search/select the user(s) to whom the Resource Group is to be shared. Decide about the permissions "View" or "Edit"or "Manage" and then

move the user to the respective box (i.e view or edit or manage). Click "Save". The Resource Group is shared.

- If you want to share the Resource Group with a usergroup(s), click the icon  present under the column "Share" against the particular Resource Group. In the UI that opens search/select the user group(s) to which the account is to be shared. Decide about the permissions "View" or "Edit" or"Manage" and then move the user group to the respective box (i.e view or edit or manage). Click "Save". The Resource Group is shared.

Note:
(1) When you share a particular Resource Group to a user group, the Resource Group will be visible to all the members of the user group. That means, all the resources with their respective accounts would be visible to all the members of the user group. Also, the permissions granted to the user group (view/edit) will be applicable for all the members.
(2) Precedence for Share Permissions: The share permission ('view' or 'view & modify') set for a password overrides that of its resource, which in turn overrides that of the resource groups which the resource is part of. (Lowest level takes highest precedence). Similarly, the share permission provided to an user overrides that of a user group the user is part of.

Transferring Ownership of Resources / Resource Group

You can transfer the resources that you own to other administrator users. With a 'transfer' you no longer have any access to that resource unless the new owner shares the password access to you. The shares that you enabled before to other users will remain intact.

To Transfer the ownership of Resources

- Go to "Resources" Tab
- Search/select the particular resource whose ownership has to be transferred to someone else with admin privileges
- Click the arrow mark against the particular resource present under the column "Share". Select the option "Transfer Ownership" and in the pop-up that opens select the user to whom the ownership has to be transferred. Click "Save". The ownership will be transferred

To Transfer the ownership of Resource Groups

- Go to "Resources >> Resource Group" Tab
- Search/select the particular resource group whose ownership has to be transferred to someone else with admin privileges
- Click the arrow mark against the particular resource present under the column "Share". Select the option "Transfer Ownership" and in the pop-up that opens select the user to whom the ownership has to be transferred. Click "Save". The ownership will be transferred

Note: The ownership of default resource group and the criteria-based resource groups (the resource groups that were created based on some criteria) cannot be transferred.

Managing Resource Types

You can add as many resource types as you require and manage such resource types from the "Admin" tab. Apart from adding custom resource types, you can provide your own icons for the types, edit the existing types and delete resource types from the database.
PMP provides the option to store digital files, certificates, images and documents too. By default, PMP comes with the following resource types:

Operating Systems

1. Windows
2. Windows Domain
3. Linux
4. Mac
5. Solaris
6. HP UNIX
7. IBM AIX

Cisco Devices

1. Cisco IOS
2. Cisco CatOS
3. Cisco PIX

Other Network Devices

1. HP Procurve
2. Juniper Netscreen
3. HP iLO

Database Servers

1. MS SQL Server
2. MYSQL Server
3. Oracle DB Server
4. Sybase ASE

Digital Files/Keys/Licences

1. File Store
2. Key Store
3. License Store

Cloud Services

1. AWS IAM
2. Microsoft Azure
3. Google Apps
4. Rackspace

Others

1. LDAP Servers
2. VMware ESXi
3. Oracle ALOM
4. Oracle ILOM
5. Oracle XSCF
6. IBM AS400
7. VMware ESXi

You cannot delete/edit the above default resource types.

To add a new resource type,

- Go to "Admin >> Customize" section and click the icon "Resource Types"
- Click "Add Type"
- Provide a name for the new resource type
- If you have a custom icon for the new resource type, click 'Browse' and choose the image. If you do not have a custom image, the default icon  will be displayed
- If you wish to enable "Remote Password Reset" for this resource type, select the checkbox "Remote Password Reset Required". Then select a reset type that is similar to the one being added. For example, if you are adding a new resource type that is similar in behaviour to Linux, select accordingly

- For new resource types, you have the option to customize the attributes appearing in the 'Resource Addition' and 'Edit Resource' forms. You can choose not to have certain attributes - for example, if your new resource type does not require the attributes 'Department' and 'Location', just leave the checkboxes for the two entries blank. After doing this, when you invoke "Add Resource" or "Edit Resource" form of a resource belonging to this type, the two fields "Department" and "Location" will not appear
- Click "Save" to add the new resource type

To edit a resource type,

- Go to "Admin >> Customize" section and click the icon "Resource Types"
- Click the "Edit" icon present against the resource to be edited
- You can change the resource name and/or the icon
- Click "Save" to give effect to the changes
- The changed name and/or icons will get displayed wherever the particular resource type had been referred

Exporting Passwords for Secure Offline Access

PMP provides multiple export options for secure offline access and safekeeping of password information.

- The basic option is to export the resource name, account name and passwords in plain-text in a spreadsheet
- The more secure option is to export the passwords to an encrypted HTML file
- There is also provision to automatically synchronize the exported HTML file to users' mobile devices through Dropbox. Typical use case scenarios for this option include:
    - A managed service provider (MSP) using PMP to store shared passwords of their clients and technicians visiting clients with no access to PMP installed in their network
    - Technicians working in DMZs with no access to PMP web interface

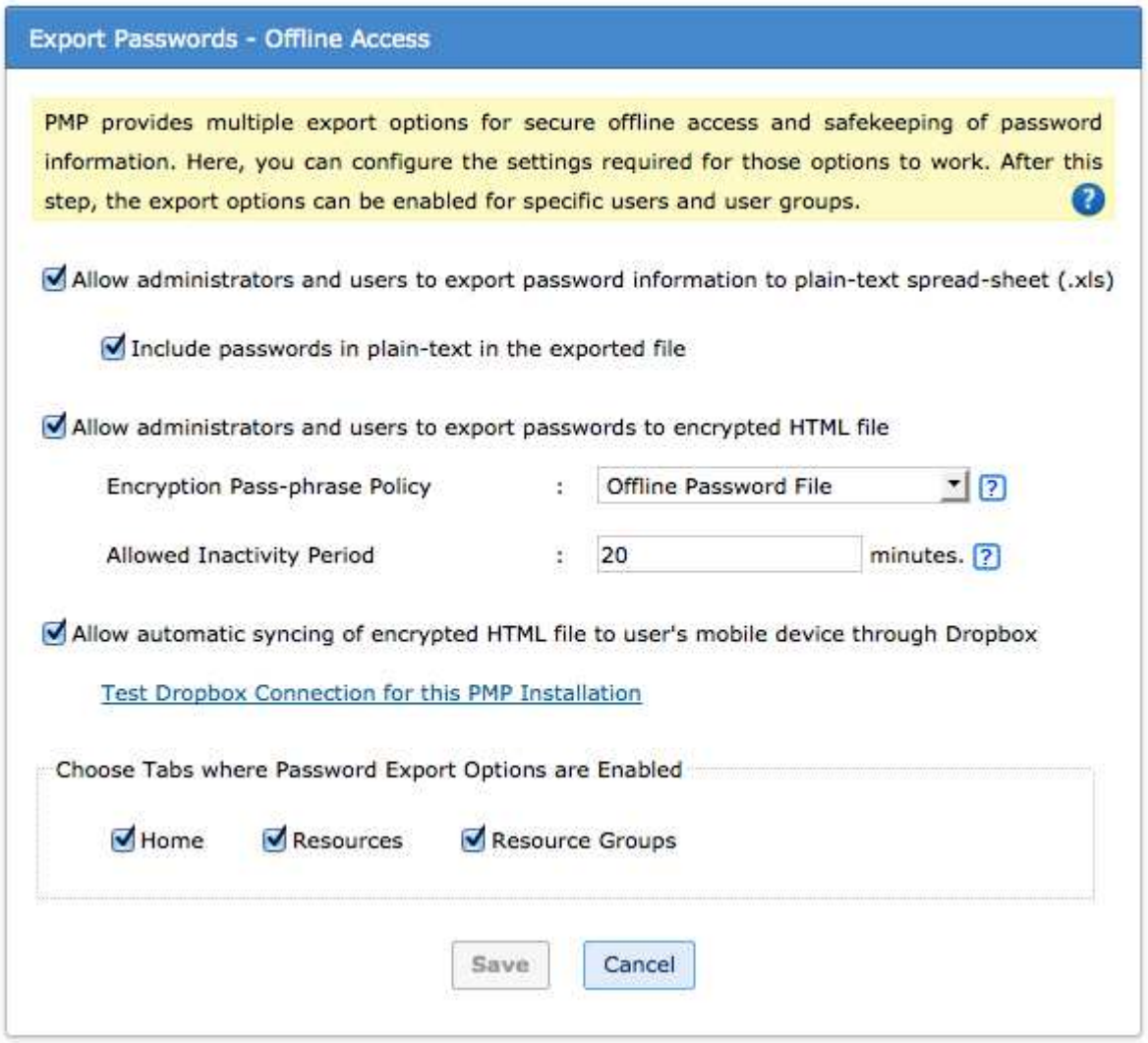
Administrators can decide which option (encrypted HTML or auto-sync to mobile devices) to be used in their organization. In addition, the export can be enabled or disabled to specific users or user groups based on requirements.

In all the options above, you can export the resources, accounts and passwords for offline access.

Administrative Setting for Exporting of Passwords

Administrators have to determine whether to allow the users in their organization to export passwords using any of the three options. Administrators can change this setting anytime on need basis. The settings done here take effect globally for all users and administrators.

This can be done from Admin >> Customize >> Export Passwords - Offline Access GUI.



By default, the first two options - exporting passwords in plain-text to .xls and exporting passwords to an encrypted HTML file have been enabled to all users and administrators. You can disable this permission by deselecting the respective check-box. The third option to allow the users to export the passwords to encrypted HTML file and automatically sync it users' mobile devices through Dropbox has to be enabled if you want this option.

Settings for exporting resources in plain-text to a .xls file

While allowing the users and administrators to export the passwords, you have the option to just export the resource and account details alone and prevent the passwords from being printed in plain-text in the .xls file. This can be done by deselecting the check-box "Include passwords in plain-text in the exported file".

Settings for exporting passwords in encrypted HTML file

Password Policy for offline copy

You can export passwords to an encrypted HTML file so as to view the passwords even when there is no internet connection. This offline option is very secure. The contents of the file for offline access will be encrypted using AES-256 bit algorithm with the passphrase supplied by the users when exporting the passwords. PMP will not store this passphrase anywhere.

As the name itself indicates, the passphrase is different from the usual passwords. Since these phrases are not stored anywhere, it is necessary that you should be able to remember them. A weak passphrase is not desirable from the standpoint of security. Your passphrase could be up to 32 characters long, including blank spaces.

Administrators can enforce standard policies for specifying the passphrases. The required policy can be selected from the three default password policies of PMP or the custom policies created by you, if any. You can select the desired policy here in the "Encryption Passphrase Policy". PMP has created a policy named "Offline Password File" and this policy is enforced by default.

Inactivity Logout

You can also specify the inactivity log out time period in minutes, after which the user will be automatically logged out from the offline file while viewing the passwords in the browser. You can specify the timeout against the textfield "Allowed Inactivity Period".

Settings for syncing encrypted HTML to mobile devices through Dropbox

If you want to enable this option for the users in your organization, select the checkbox "Allow automatic syncing of encrypted HTML file to users' mobile device through Dropbox". Then, press the link "Test Dropbox connection for this PMP installation". This operation does the necessary background processes to enable users upload the encrypted HTML file to their Dropbox account. This basically checks the proxy settings (if applicable in your environment) and tries to connect to the Dropbox app named "ManageEngine Password Manager Pro" created by PMP for this purpose.

Also, you can specify the places where the export option should be shown. By default, the options would be displayed at three places - Home Tab, Resources Tab and Resource Groups Tab at the extreme right corner. You select or de-select any location anytime.

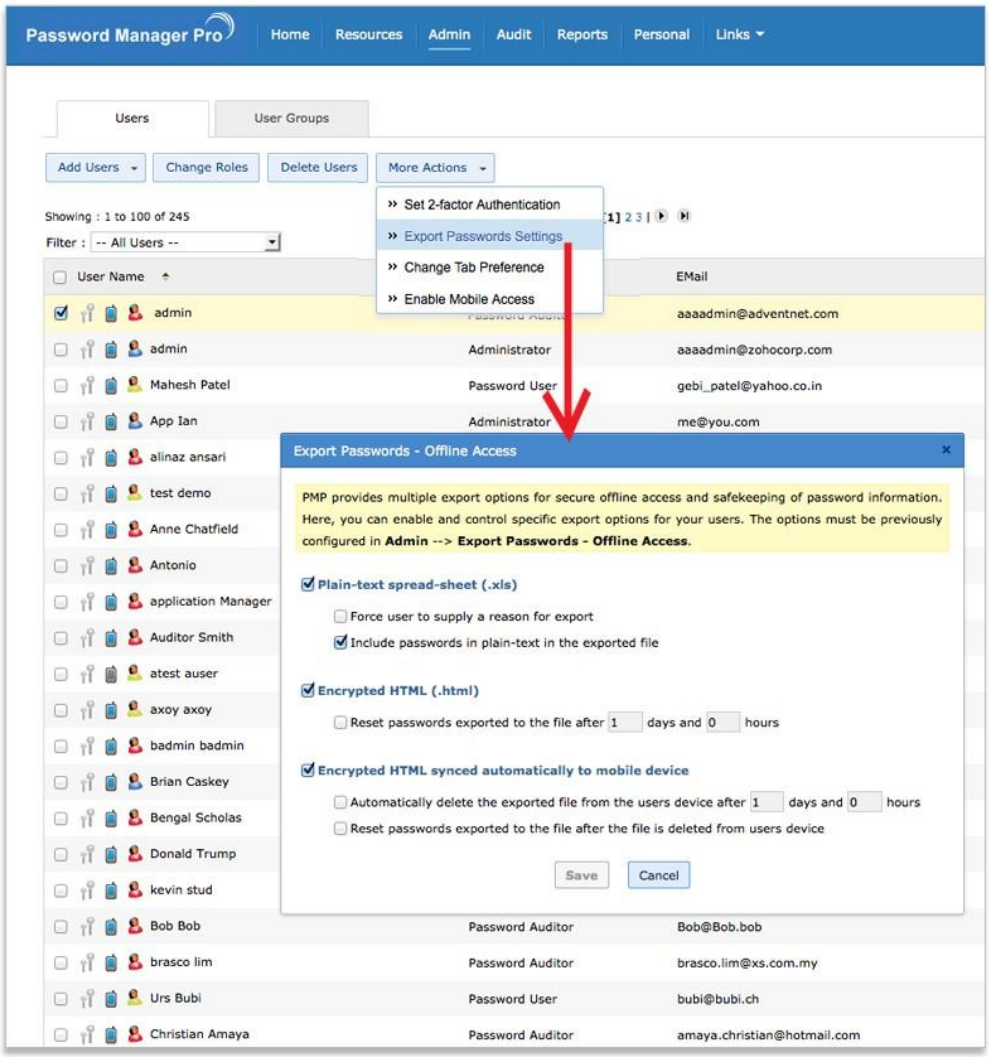
Important Note: All the above options take effect globally for all users and administrators in

the organization. In case, you want enable or disable specific options for specific users, follow the 'User-specific settings' procedure as explained below.

User-specific settings

If you want to restrict certain users from having one or all the options of exporting passwords or if you want to allow only specific users to have this permission, you need to do user specific setting from the Admin >> Users >> Export Passwords Settings.

You may select or deselect the check-box against any of the three options to enable or disable specific option. User-specific settings are subject to the global administrative setting as described above. That means, if any of the options had been disabled globally, it cannot be enabled for a specific user alone. Conversely, if the option had been enabled globally, it can be enabled or disabled at will for specific users.



Imposing restrictions for users

You can also impose fine-grained restrictions for the users when enabling/disabling options to export passwords.

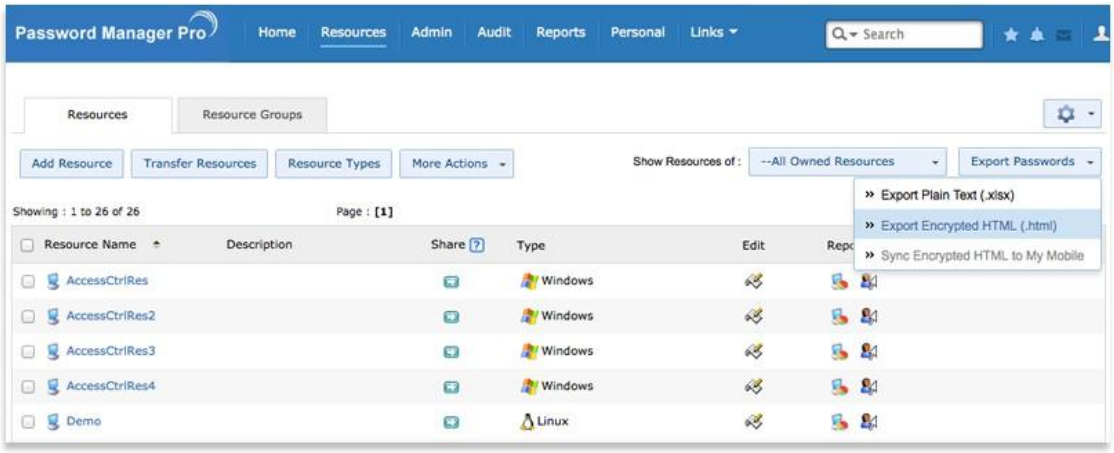
- When allowing users to export passwords in plain-text, you can enforce them to specify a reason for exporting. The reason entered here will be recorded as an audit trail. In addition, you can just allow the users to export the resource name and user account details alone, but prevent them from exporting the passwords in plain-text.
- In the case of exporting passwords as an encrypted HTML, for security reasons, administrators can enforce automatic reset of the exported passwords after a specific time period (in days and hours).
- In the case of syncing offline copy to users' mobile devices, administrators can enforce automatic deletion of the offline copy from the users' device after a specific time period (in days and hours). There is also option to automatically reset the exported passwords immediately after deletion of the offline copy from users' devices

Least privilege model for security reasons

For ensuring security, PMP adopts the 'lest privilege' model for users. For example, assume that a particular user is part of three user groups. Also, assume that there is group level restriction for one of the groups - the members of that group are not allowed to export passwords in plain-text. In the above scenario, even if the user has permission to export passwords in plain-text at the individual level, the restriction imposed on one of the groups in which the user is part of, will take precedence. The above rule applies for all types of restrictions as explained above.

Exporting Resources

The passwords can be exported by users and administrators as per the settings done by the PMP administrator. If you have the permission to export the passwords through any or all of the export options, you will see the "Export Passwords" button in 'Home Tab' or 'Resources Tab' or 'Resource Groups' or in all these tabs at the right hand corner in the GUI (if you are an administrator/password administrator). If your role is 'Password User', you will see this option in the RHS corner of 'Enterprise' tab.



Option 1: Exporting resources in plain-text in a spreadsheet

- Click the link "Export Plain Text (.xls)" of "Export Passwords" button
- The resources are exported to a file and it is shown as a pop-up
- Save the file in a secure location (in .xls format)

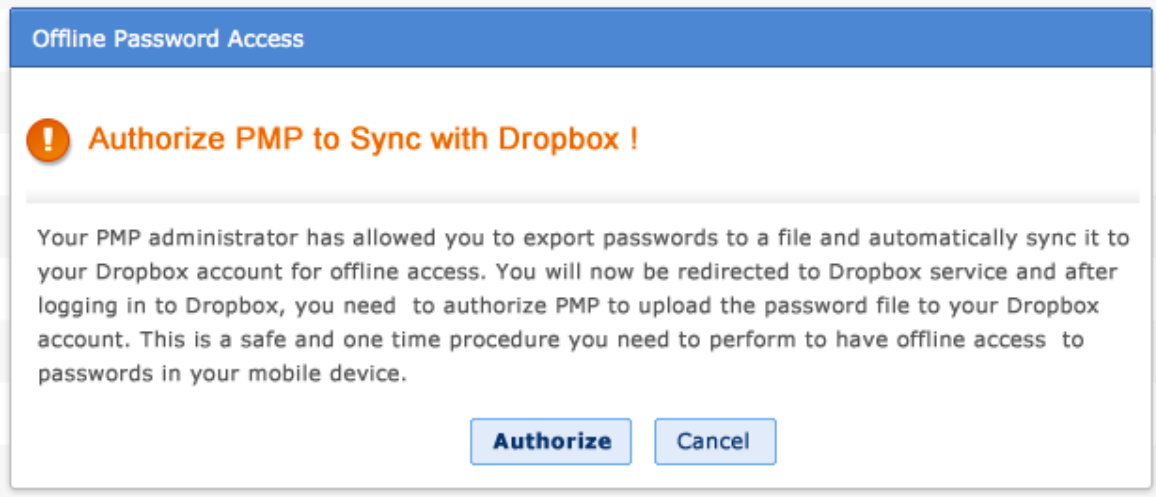
Note: If the resources/accounts/passwords contain non-English characters, the application in which you open the exported resources, should support UTF-8 encoding.

Option 2: Exporting passwords as encrypted HTML

- Click the link "Export Encrypted HTML (.html)" of "Export Passwords" button
- In the UI that pops-up, you need to specify a passphrase that will be used for encryting (AES-256) the HTML file for offline access. You will have to specify the passphrase in accordance with the password policy as enforced by your administrator. PMP will not store this passphrase anywhere and we recommend you not to store or write it down anywhere either . The contents cannot be read if you forget the passphrase, but you can create another offline file with a different passphrase. You can open this file in any web browser, supply the same passphrase and access the contents.
- Confirm the passphrase and also enter a reason for exporting the passwords
- The resources will be exported as a HTML file. It will take some time for exporting the resources and the offline copy will be displayed in a pop-up in the GUI.
- Save the file in a secure location (in .html format)

Option 3: Automatically syncing the encrypted HTML to users' mobile devices through Dropbox

- Click the link "Sync Encrypted HTML to my Mobile" of "Export Passwords" button
- When you attempt this option for the first time, you will be prompted to authorize PMP to sync with Dropbox. Upon clicking the "Authorize" button, you will be redirected to Dropbox service and after logging in to Dropbox, you will have to authorize PMP to upload the password file to your Dropbox account. This is a safe and one time procedure to be done to have offline access to passwords in your mobile device.



Access Control Workflow

(Feature available only in Premium and Enterprise Editions)

Overview

After successful authentication into Password Manager Pro, users get access to the passwords that are owned by them or shared to them. While storing very sensitive passwords, quite often administrators wish to have an extra level of security. In some other cases, administrators wish to give temporary access to passwords for certain users for a specified period of time.

There are also requirements to give users exclusive privilege to passwords. That means, only one user should be allowed to use a particular password at any point of time. When more than one user is required to work on the same resource, problems of coordination arise. Access control on concurrent usage would help resolve such issues.

To achieve all the above requirements, PMP provides the Password Access Control Workflow. This document explains how to implement the access control workflow in PMP.

How does Password Access Workflow work?

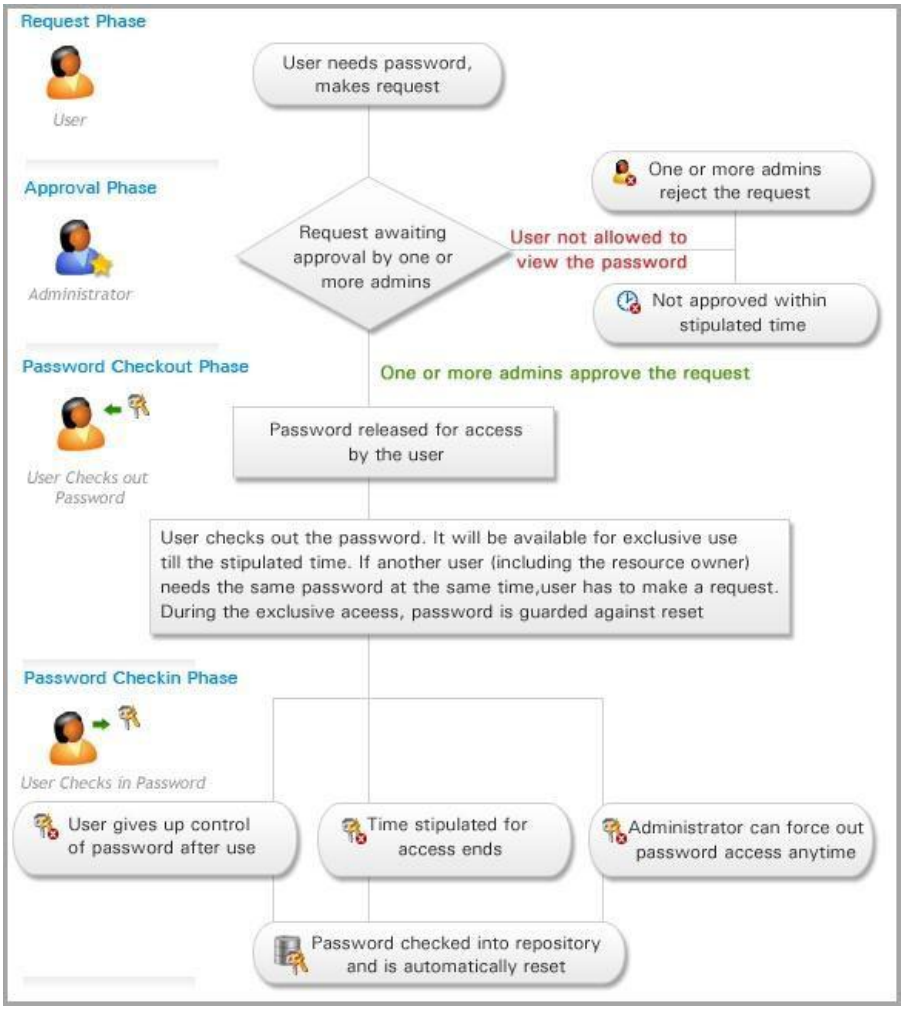
Once password access control is enforced, the password access attempt by the users will follow the work flow as detailed below:

1. User needs access to a password that is shared to him/her
2. Makes a request for accessing the password
3. Request goes to administrator(s) for approval. If more users require access to the same password, all the requests will be queued up for approval
4. If the administrator(s) does not approve the request within the stipulated time, it becomes void
5. If the administrator rejects the request, it becomes void
6. If the administrator(s) approves the request, user will be allowed to check out the password. In case, two administrators have to approve a password, user will be allowed to check only after the approval by both the administrators
7. Once the user checks out a password, it will be available exclusively for his/her use till the stipulated time
8. If any other user requires access to the same password at the same time, he will be provided access only after the previous user checks in the password. This rule applies to all, including administrators, password administrators and owner of the password

9. Administrator can force out password access anytime. In such cases, the password will be forcefully checked-in denying access to the user
10. Once the user finishes his work, the password will be reset
11. While giving the exclusive access to a user temporarily, PMP provides the flexibility to enable administrators view the password concurrently. Through a simple administrative setting from "General Settings", users will be able to do that, if required.

Important Note: The access control workflow does not override the password ownership and sharing mechanism of PMP. That means, it is only an enhanced access control mechanism. Normally, when a password is shared to a user, the user will be able to directly view the password. When the access control is enabled, the user will have to request the release of the password that he is already allowed access.

The following diagram illustrates the typical access control workflow:

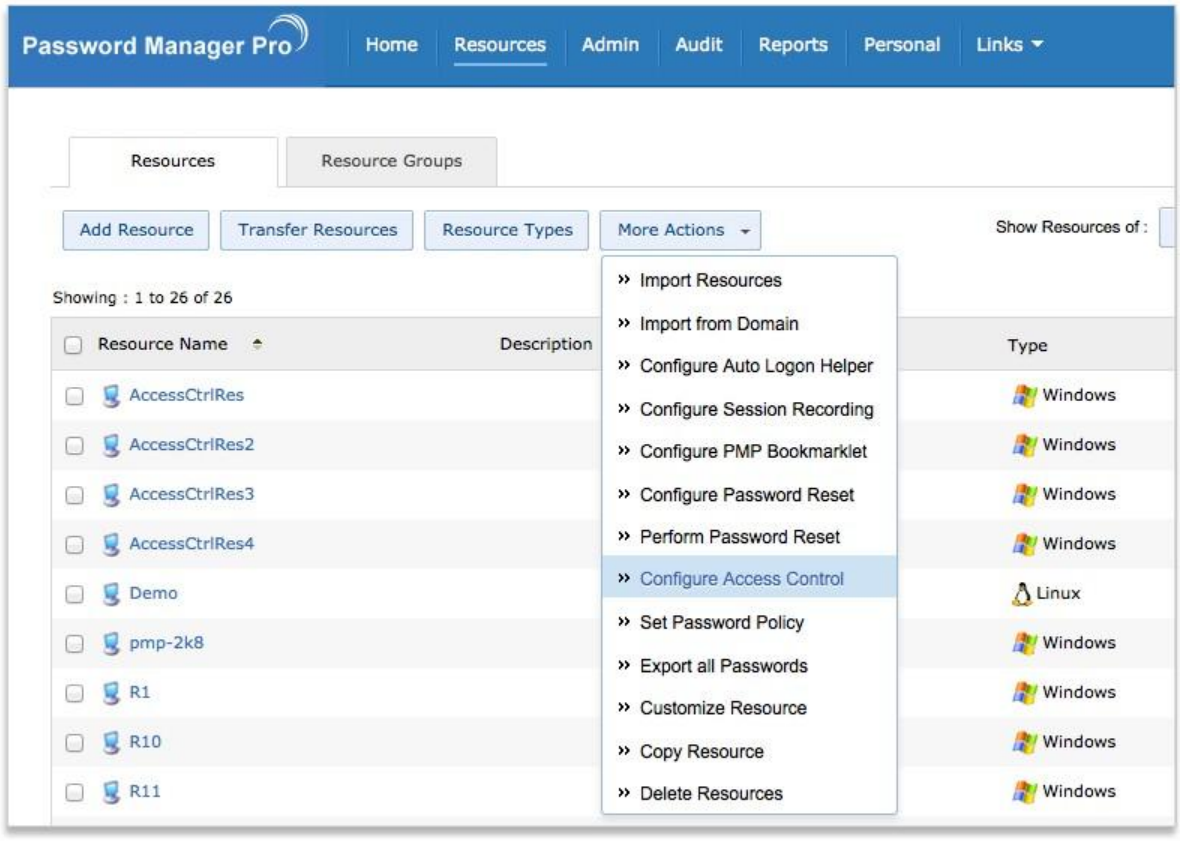


How to Implement Access Control Workflow?

To implement access control, administrators need to carry out the following administrative settings:

Administrative Settings

1. Go to "Resources" tab
2. Select the resources for which you wish to enforce access control
3. Click the link "Configure Access Control" from "More Options" listing



In the UI that opens up,

1. Designate the administrator(s) who could approve password release requests. The list of all administrators and password administrators in the system are listed in the LHS. You can designate as many administrators as you wish. Anyone from the list of 'authorizers' could approve the requests. Optionally, you can enforce dual approval by designating two administrators. In that case, select the check box "Require at least

two administrators to approve password access" present at the end of the page and select two administrators.

2. List down the users to be excluded from the request process. When you exclude a user from approval, he/she would be able to retrieve the password without administrator approval. That means, the user need not have to go through the 'Request-Release' process
3. If you have chosen dual approval in Step 1, select the checkbox "Require at least two administrators to approve password access"
4. Specify the maximum time period in hours after which a password request would go void, if administrator(s) does not approve
5. Concurrency Controls: You can also enforce concurrency controls for password access. That is, the password could be made available for the exclusive use of a particular user for a specified time period during which no one else, including the owner of the resource would be allowed to view the password. You can specify the time period in hours up to which the released password would remain valid and be available exclusively for the user. For Example, if you specify the time period as two hours, the password would be made available exclusively for that user for two hours. Others cannot view the password during that period. After the specified time period, the password would become void and will not be available to the user. Other users will now be able to view the passwords.

   Note: By default, the password will remain exclusive for 8 hours. You can modify it to the desired value. If you specify the value as '0' hours, the password will remain exclusive for unlimited hours.

6. You can also enforce automatic reset of password once the user gives up password access. To do this, select the option "Reset password after check-in"

   Important Note: For automatic password reset to take effect, you need to ensure that all required credentials have been supplied to the resource for remote password reset OR you should have installed PMP agents in the resource. Otherwise, the automatic password reset will not take effect.

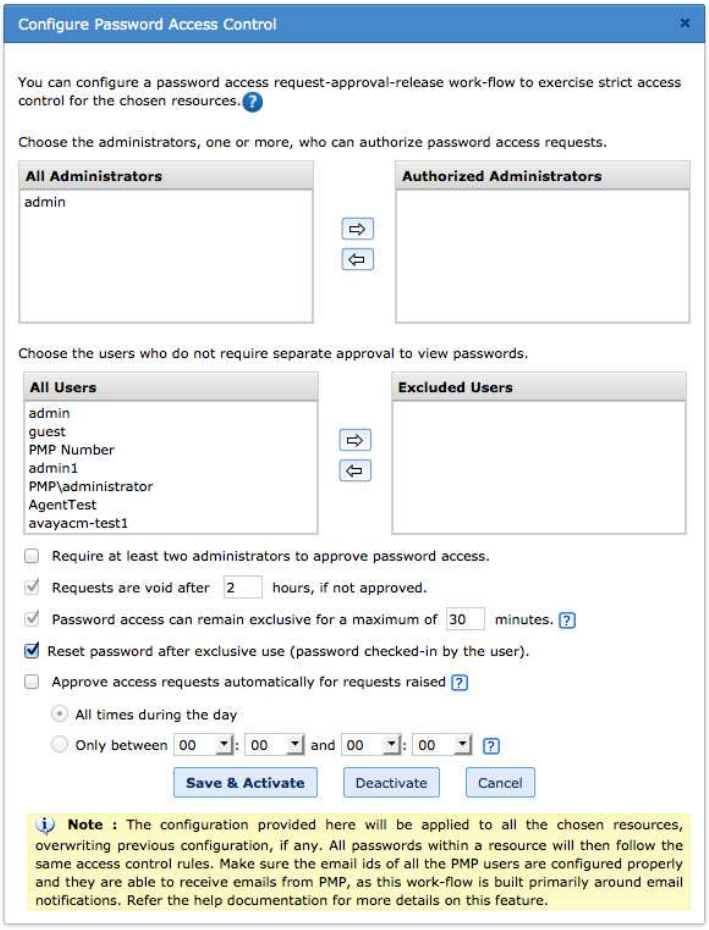
7. Approve access requests automatically: Password Manager Pro provides the option for automatic approval of password access requests. That means users need not have to wait for approval by authorized administrators while going through the access control workflow. The requests will be automatically approved and notifications will be sent to the authorized administrators. When the password is released after automatic approval, it will be reserved for exclusive use of the requester for the specified time period.

You have the option to automatically approve the requests raised during a specific time period in the day - for example, all the requests raised between 2 p.m to 3 p.m. Alternatively, you can even set automatic approval to take place anytime of the day.

This automatic approval feature has been provided to serve the users when administrator is not available to approve. Except the automatic nature of approval, all other aspects of this feature remains the same as access control workflow.

8. Click "Save & Activate"

With the above steps, access control workflow would be enabled for the required resources.



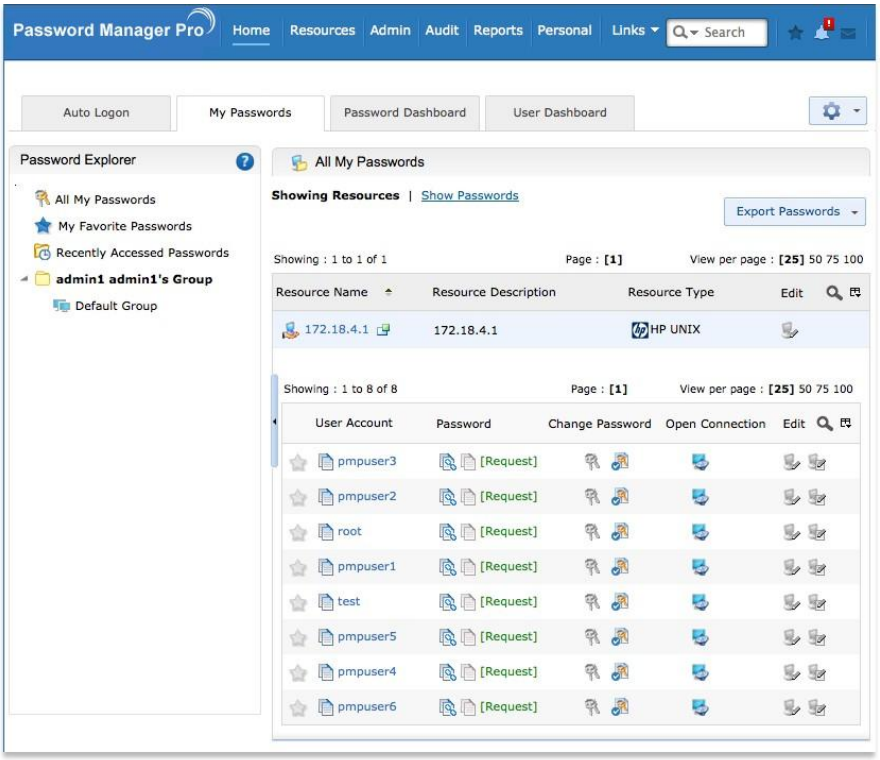
Use Cases

Following are some of the use case scenarios of the access control workflow:

Case 1: User Requiring Access to a Password
A user who requires access to a password, which is safeguarded by the access control mechanism will have to make a request to the administrator to grant permission to view the password.

To make a request

1. Go to the "Home" tab
2. In the drop-down "Show Passwords of" you select the option "All" to view all the passwords; select "Resource Group" to view the passwords that are owned by you; select "Shared Groups" to view the passwords that are shared to you
3. Once you select your option, all the passwords falling under your selection will be listed in the table below
4. Each entry in the table is a link and when you click that, you can view the corresponding resource details
5. Click the link "Request" and in the UI that opens, enter your request as a comment to retrieve the password and the request will be sent to the administrator for approval.
6. Once the administrator approves your request, you will be allowed to view the password. Till then, you will see the status as "Waiting for approval"
7. Once the administrator approves, users will see the status as "Check Out". To view the password, click the link "Check Out" and in the UI that opens up, enter a reason to view the password and click "Save".
8. Now, you will be allowed to view the password

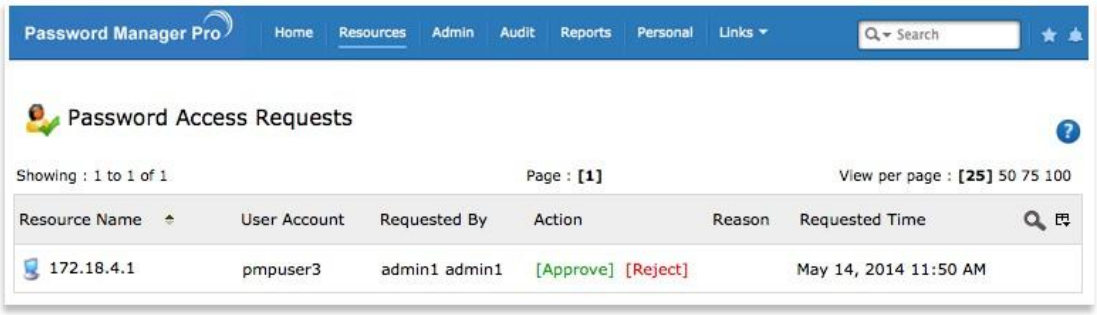


Case 2: Administrator approving a password request

When a user has requested your approval to view a password, you will receive email notification about the request. You can view all the requests pending your approval from the 'Admin' tab.

To approve a request,

1. Go to "Admin" >> "Password Access Requests"
2. Click the link "Approve" against a request to allow the user to view the password. Once you do this, user will be allowed to view the password. (You can also "Reject" the request, in which case, the request will be removed from the queue).
3. Immediately after you approve the request, the status of the link will change to "Yet Use" indicating that use is yet to check out the password. Once the user has viewed the password, the status will change to "In use"

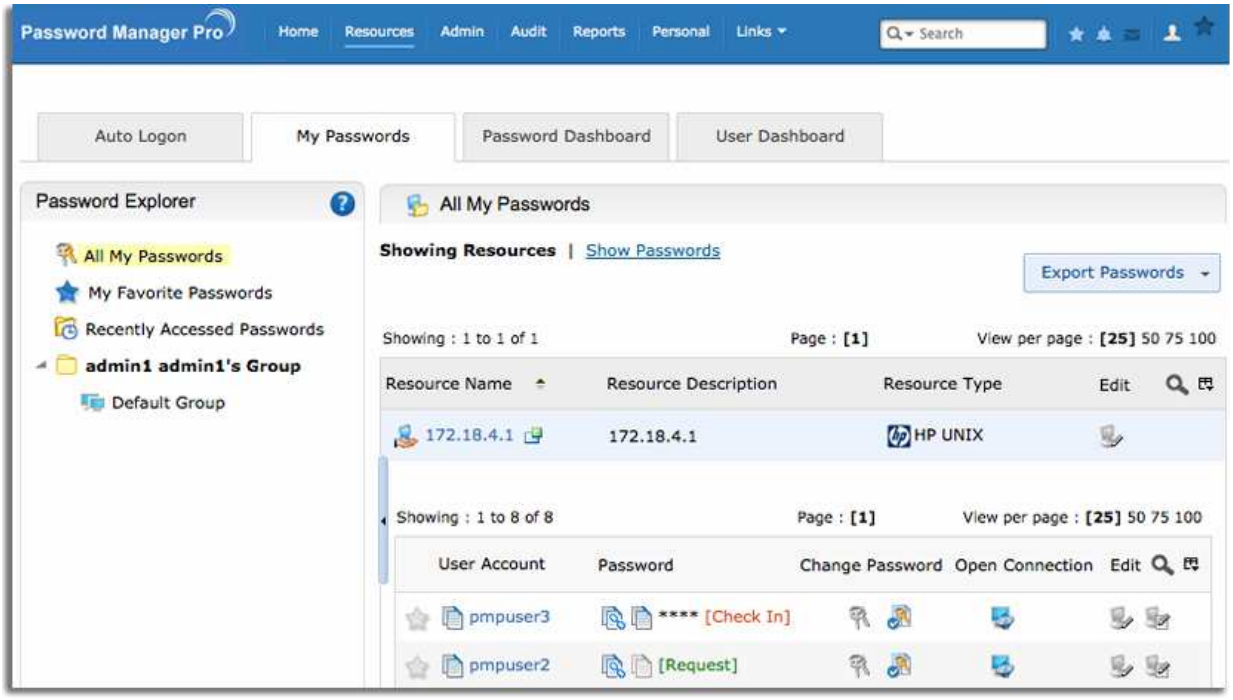


Case 3: User completes his password usage

The crux of the access control mechanism is that user will be allowed only temporary access to passwords. So, once the user finishes his work, he can give up the password.

To give up access to the password,

1. Click the link "Check In" present near the password. Once you do this, the password will be checked in and the status will change as "Request" again.
2. You will no longer be able to view the password. In case, you require access again, you will have to go through the "Request-Release" process again.



Case 4: Administrator forcefully checking in the password

The essence of the access control mechanism is to provide exclusive access privilege to a user for a specified time period. During this period, no one will be allowed to view the password, including the owner. In case, an emergency need arises to revoke the exclusive permission to the user, administrator can forcefully check in the password at any point of time.

To forcefully checkin a password,

1. Go to "Admin" >> "Password Access Requests"
2. Click the link "Check in" against the specific request to revoke permission to the user. Once you do this, user will not be allowed to view the password. Also, the request will vanish from the list

Case 5: Allowing administrators to have concurrent view of a password when access control is enabled

As mentioned in Case 4 above, when a user is viewing the password, no one else would be allowed concurrent view by default. While giving the exclusive access to a user temporarily, PMP provides the flexibility to enable administrators view the password concurrently.

Through a simple administrative setting from "General Settings", users will be able to do that, if required.

To enable this,

1. Go to "Admin" >> "General Settings"
2. In the UI that opens up, select the check box "When access control is enabled and a password has been released to a 'password user', allow admins to view the password" and click "Save"
3. Once you do this, the user who makes a request for a password, will not have the exclusive privilege. All PMP administrators will be able to view the password concurrently.

Case 6: What happens if automatic password reset (if enabled) during password check in fails?

Once a password is checked out by a user, it will be checked in due to any of the following three reasons:

1. User checks-in on his own after using the password
2. System automatically revokes access after the stipulated time and checks in
3. Administrator forcefully checks-in

When password is checked in, if the admin settings require automatic password reset, PMP will try to reset the password. In case, PMP is not able to reset the password in the actual resource, PMP will immediately trigger email notifications to the administrators who approved the password access request of the user. They can troubleshoot and set things right. The password reset failure will also reflect in the audit trails.

Case 7: When a user has checked out a password, what happens if an already configured password reset scheduled task runs?

PMP provides option for creating scheduled tasks for automatically resetting the passwords periodically. It is quite possible that a scheduled task start executing the reset of a password that is being used by a user. If that reset task is allowed to get executed successfully, the user will be working with an outdated password. To avoid such issues, PMP will not allow reset of that password alone. (All other passwords of other resources that are part of the scheduled task will be reset). The failure of scheduled reset of the particular password will reflect in the audit trails.

Case 8: Disabling Access Control

If you want to disable access control for any of the resources, you (administrator) may do so at anytime as explained below:

1. Go to "Resources" tab
2. Select the resources for which you wish to disable access control
3. Click the link "Configure Access Control" from "More Options" listing
4. Select the option "Deactivate"

Access Control for the selected resource will be deactivated. That means, any user who has permission to view the password (owned/shared) will be able to view the password without going through the Access Control process for that particular resource.

Summary of Terminologies

Term	What it Signifies
Request	The user has to make a request to view the password
Waiting for Approval	The password release request made by the user is pending administrator's approval
Check Out	Administrator has approved the request and the user could view the password
Approve/Reject	The administrator can either approve or reject a password request
Yet to Use	Indicates that the user is yet to view the password released by the administrator
In use	Password is being used exclusively by a user
Check in	Giving up/revoking password access

Integrating PMP with Enterprise Ticketing Systems

(Feature available only in Enterprise Edition)

Overview

PMP 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. This integration also extends to PMP workflow, which helps in granting approvals to access requests against automatic validation of corresponding service requests in the ticketing system.

How does this integration work?

Once you integrate PMP with an enterprise ticketing system, users would be required to enter ticket ID for password retrieval or reset. PMP will verify the following before granting access:

- Validate that the ticket ID entered by the user exists in the ticketing system
- Verify that the incident connected with the ticket is NOT in 'Closed' state
- If the user is authorized to view that password and thereby access the IT resource
- In the case of password reset attempts, verification for appropriate permissions

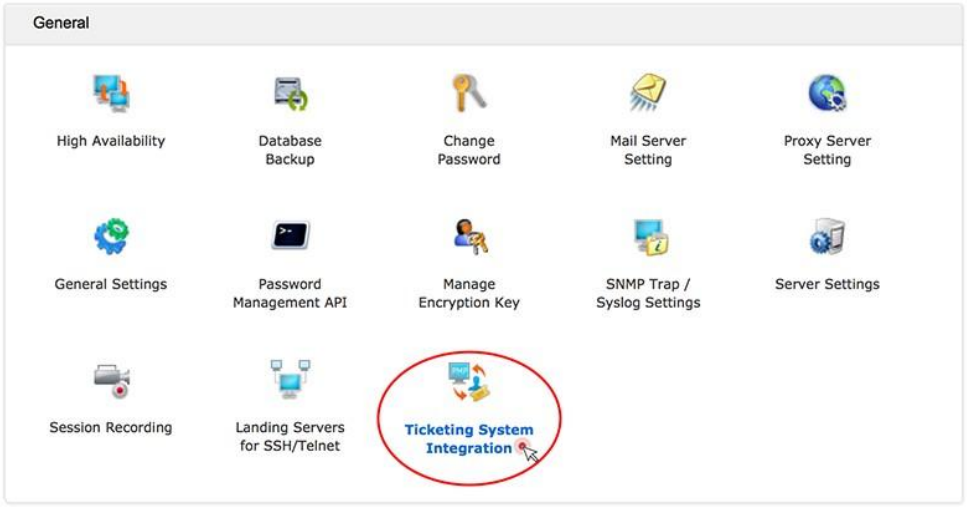
In addition to verifying the above by default, PMP also lets you define custom criteria and validate them with the ticketing system before granting access to passwords. The entire process is completely audited - that means, privileged actions can be traced to ticket IDs. Password access could be traced with ticket numbers in the ticketing system. In addition, you can generate a custom reports on privileged access scenario through ticket IDs.

How to integrate?

Integrating PMP with your ticketing system is a simple process. PMP readily integrates with ManageEngine ServiceDesk Plus On-Demand, ServiceDesk Plus MSP, ServiceDesk Plus and ServiceNow. You can also integrate with any other enterprise ticketing system.

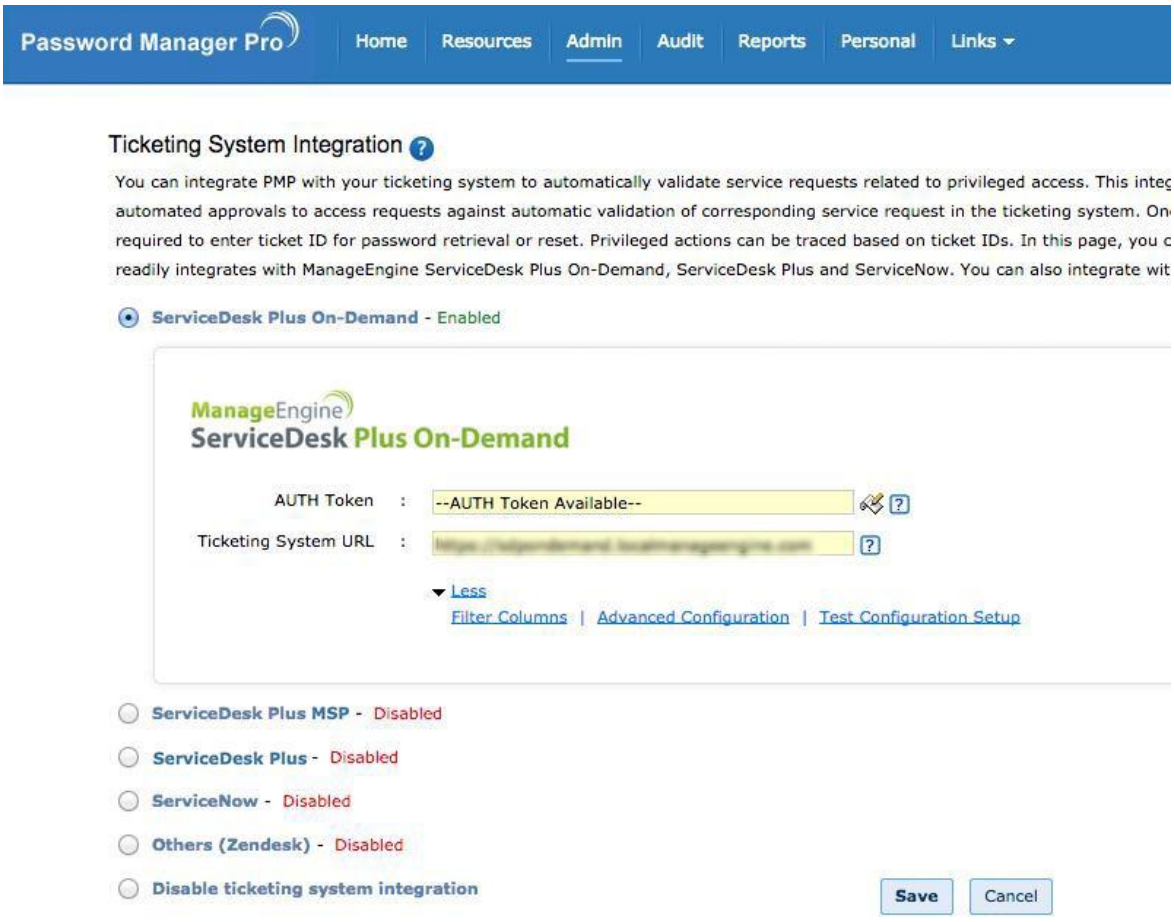
To integrate your ticketing system,

- Navigate to Admin >> General and click Ticketing System Integration
- In the GUI that opens, you can select the ticketing system you wish to integrate (from the list of ticketing systems that are supported. If the ticketing system that you use is not found in the list, select 'Other')



To integrate with the ticketing systems readily supported:

Integration with the ticketing systems that are readily supported is straightforward. You just need to provide the details necessary to establish connection with the ticketing system.



Settings to Establish Connection

- Basically, the integration is achieved leveraging the REST APIs provided by the respective ticketing systems. So, all that you need to do is to specify/generate the Authentication Token and Ticketing System's application URL. You can generate and obtain the the Auth Token from the respective websites - ManageEngine ServiceDesk Plus On-Demand or ServiceDesk Plus MSP or ServiceDesk Plus and ServiceNow.
- By default, PMP validates if the ticket ID entered by the user exists in the ticketing system and also verifies if the incident connected with the ticket is NOT in 'Closed' state. If your requirement is satisfied with these, ticketing system integration is complete.

Optional Advanced Configurations

In case, you want to validate some other criteria (in addition to ticket number and ticket status), you have the option to configure advanced settings. For example, you can choose to check if the PMP user who is raising the password access request matches with the 'REQUESTER' column in the ticketing system. Similarly, you can check for certain specific conditions related to the ticket - for instance, 'PRIORITY' of the ticket as 'HIGH'. PMP offers the total flexibility to check for any parameter in the ticketing system, including additional fields.

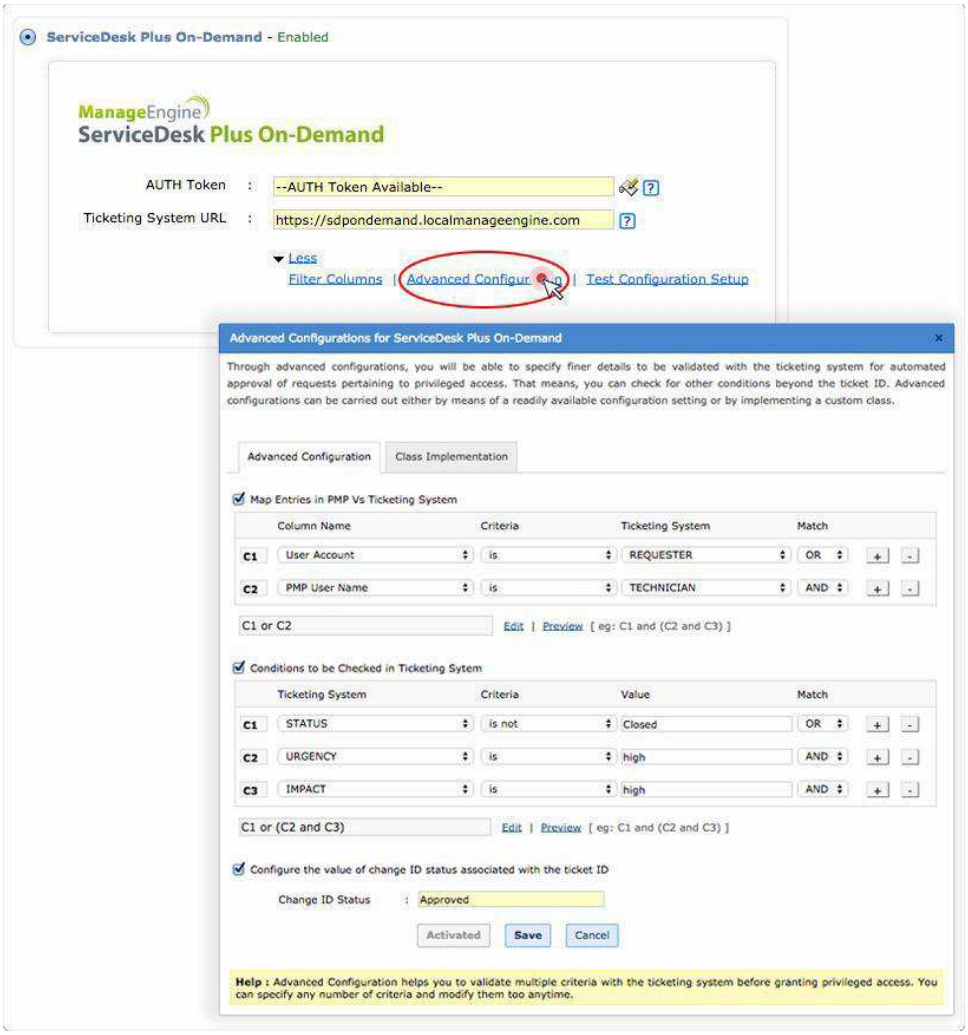
To carry out advanced configurations, click the "More" >> "Advanced Configuration" link. In the GUI that opens, you can carry out advanced configurations. Advanced configurations can be carried out either by means of a readily available configuration setting or by implementing a custom class.

Options in Advanced Configurations

1. Validating if specific columns in PMP match with the ones you specify in the ticketing system
   - To validate if specific columns in PMP match with the ones you specify in the ticketing system, you need to select the option "Map Entries in PMP Vs Ticketing System".
   - The column name drop-down lists down the column names as available in PMP - Resource Name, Resource Type, Account Name, PMP User Name, DNS Name etc. The custom fields created in PMP are also included.
   - Through the criteria column, you can specify what you want to check

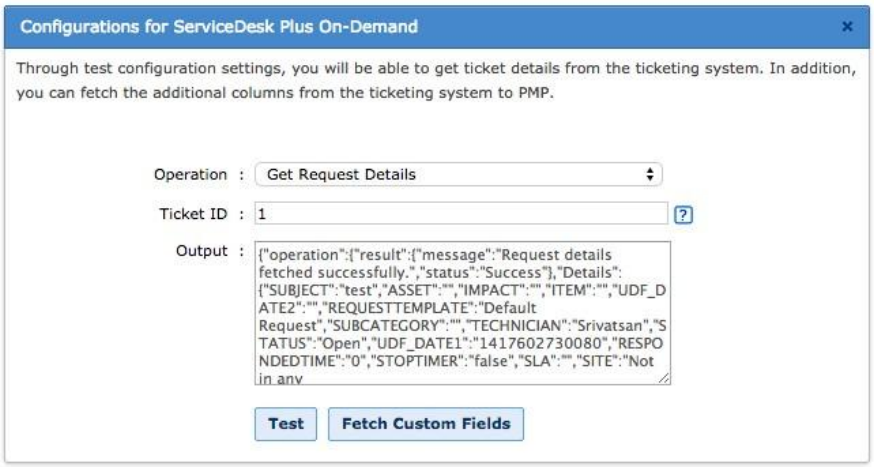
- The 'Ticketing System' column lists down the fields (including custom fields) available in the ticketing system. You need to choose the field, which you has to be mapped with the corresponding field in PMP. For example, you can choose to map RESOURCE NAME in PMP with ASSET in the ticketing system. Once you specify such a mapping, before granting access to the password, PMP will check if the RESOURCE NAME as specified in PMP matches with the ASSET name in the ticketing system. Only if the validation succeeds, access will be granted.

2. Validating specific conditions related to the ticket in the ticketing system
   - To validate if specific conditions related to the ticket are met, you need to select the option 'Conditions to be checked in the ticketing system'. By default PMP checks if the ticket STATUS is not in CLOSED state.
   - You can select any number of additional conditions and PMP will validate all of them with the ticketing system. By default, PMP lists down all the fields available in the ticketing system, including the custom fields. You can specify the value, which PMP has to validate.



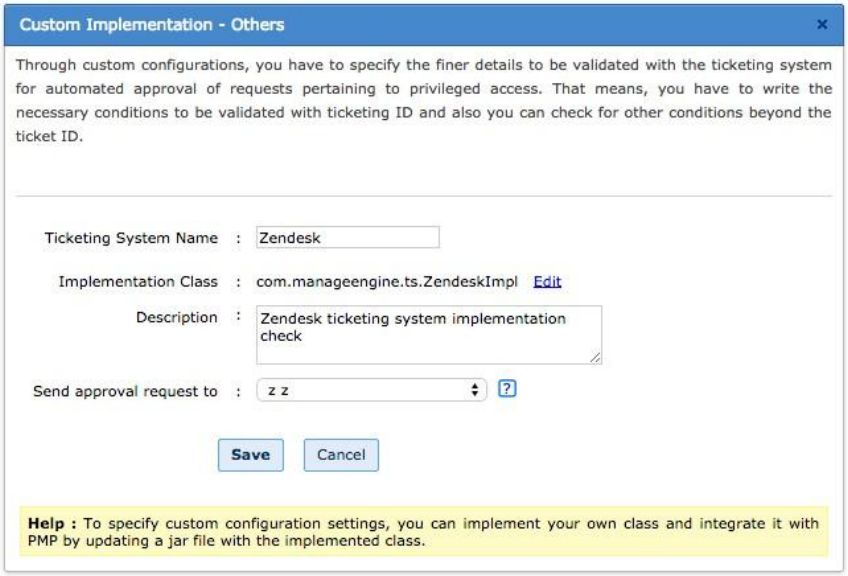
Test Ticketing System Configuration Setup

After completing the integration, you can do a testing to ensure if PMP is able to establish communication with the ticketing system properly. Click the link "Test Configuration Setup" link in Advanced Configuration to do this. As part of this testing, you can also fetch the custom fields available in PMP to the advanced configuration setup.



Custom Implementation

In case, the advanced configuration does not satisfy your requirements, you can provide your own custom implementation and integrate it with PMP by updating a jar file with the implemented class. For more details, refer to 'Integrating Other Ticketing Systems' section below. The steps outlined there hold good here too.



Ticketing System Validation Enforcement and Exceptions

Once you complete ticketing system integration, it takes immediate effect globally and users will have to produce valid ticket IDs to access passwords. By design, super administrators are exempted from ticket ID enforcement. In addition, as part of access control workflow, users could be enforced to produce ticket IDs and access can be auomatically granted after validating the IDs.

From 'General Settings', you can selectively allow/restrict users through the options "Allow users to retrieve password without ticket ID" and "Allow users to reset passwords without ticket ID".

In addition, you can have user group-specific settings too, which can be done from the respective settings icon in Admin >> User Groups.

Disabling Ticketing System Integration

You can disable the integration with the ticketing system anytime, if required. Just select the option 'Disable Ticketing System' in Ticketing System Integration page.

Integrating Other Ticketing Systems

If you are using any other ticketing system, you can integrate it with PMP by having your own custom implementation. To guide you through the process, we have taken integrating Zendesk as example and explaining below the steps involved.

Step 1: Create your implementation class

Refer to the sample implementation class created for integrating Zendesk. The important aspects of the implementation class have been explained below:

Generate Authentication Token

The first step is to generate authentication token of the ticketing system to enable PMP establish connection. When generating the AUTH TOKEN, ensure that you provide the credentials of an administrator who has full access to the ticketing system. You can do this either by providing the credentials directly in the implementation class or by generating the token and putting the token.

The snippet below shows how to generate Base64 Authstring belonging to a privileged account of the ticketing system. This will come in handy when the REST API is based on Base64 Authorization header. Some ticketing systems offer AUTH-Token with inbuilt GUI. In such cases, you can directly use the authentication parameters. In addition, instead of hardcoding username and password in the implementation class, you can very well skip this part and make REST API call with direct Base64 token that are generated through Java or through any online editors.

Refer to the code snippet below:

```
// Constructing Authstring from Zendesk login credentials
String username = "username@example.com"; //Zendesk username
String password = "zendeskpassword"; //Zendesk password
Base64 encoder = new Base64();
byte[] encodedPassword = (username + ":" + password).getBytes();
byte[] encodedString = encoder.encodeBase64(encodedPassword);
String authStr = new String(encodedString);
```

Step 2: Check connection with ticketing system

Using REST APIs, PMP can be made to get the information about tickets from the ticketing system. Each ticketing system follows its own procedure to disseminate ticket details. Refer to the respective documentation to identify the procedure. After obtaining the ticket details, you need to validate the details.

Refer to the code snippet below:

```
String sUrl = "https://<zendesk-instance>.zendesk.com/api/v2/tickets/"; //REST API call Zendesk
sUrl = sUrl + ticketId +".json"; //This is the ticket ID that will be validated against the one supplied by the user in PMP
URL url = new URL(sUrl);
HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
connection.setRequestProperty("Authorization","Basic "+authStr); //Setting Authstring in the header
```

Step 3: Validating if specific columns in PMP match with the ones you specify in the ticketing system (optional configuraion)

Refer to the code snippet below to validate if specific columns in PMP match with the ones you specify in the ticketing system (For example, you can choose to map RESOURCE NAME in PMP with the SUBJECT in the ticketing system. Once you specify such a mapping, before granting access to the password, PMP will check if the RESOURCE NAME as specified in PMP matches with the SUBJECT name (if the subject contains the resource name) in the ticketing system. Only if the validation succeeds, access will be granted):

```
String assetName = (String)pmpColumns.get("Resource Name");//PMP Asset Name for which password related operation done
String subject = (String)ticket.get("subject");//Getting the ticket subject
boolean descriptionCheck = subject.toLowerCase().contains(assetName.toLowerCase()); //Checking the description of the ticket contains the resource name of user account
```

Step 4: Validating specific conditions related to the ticket in the ticketing system (optional configuraion)

You can validate if specific conditions related to the ticket are met - by default PMP checks if the ticket STATUS is not in CLOSED state. You can select any number of additional conditions and PMP will validate all of them with the ticketing system. By default, PMP lists down all the fields available in the ticketing system, including the custom fields. You can specify the value, which PMP has to validate. Refer to the code snippet below for this implementation:

```
JSONObject ticket = (JSONObject)ticketingOuput.get("ticket");
String status = (String)ticket.get("status");
boolean statusCheck = "open".equalsIgnoreCase(status); //Checking whether the status of the ticket is in open state
```

Step 5: Compilation

While compiling keep the following jars in the classpath (the jars are available under <PMP_HOME>\lib folder)
AdventNetPassTrix.jar;
json_simple-1.1.jar;
commons-codec-1.4.jar
For Example,

javac -d . -cp AdventNetPassTrix.jar;json_simple-1.1.jar;commons-codec-1.4.jar ZendeskImpl.java - (For Windows)
javac -d . -cp AdventNetPassTrix.jar:json_simple-1.1.jar:commons-codec-1.4.jar ZendeskImpl.java - (For Linux)

Step 6: Configurations in PMP installation

- Make the implemented class files as a single jar and place that jar in PMP_HOME\lib folder
- Restart the PMP Service so that PMP will make use of the implemented class.
- Navigate to Admin >> General and click Ticketing System Integration
- In the GUI that opens, select the option 'Other' (to integrate any ticketing system) OR the 'Class Implementation' section of 'Advanced Configuration' of the already integrated ticketing system (if you want to extend the functionality)
- Specify the name of your implementation class
- Your implementation has to be approved by another administrator. All other administrators (other than those who made the request) will receive an alert regarding the request for approval
- Once an admin approves the implementation, it will be made available for use.
- After enabling, ticketing system workflow will be made mandatory for password retrieval and password reset

For further information, refer to the sample implementation class created for integrating Zendesk.
Implementation Tips

For steps 3 and 4 above, you might require additional information for implementation. Refer to the tips below for details:

Columns in PMP

List of data related to the user account for which ticketing request is raised through

pmpColumns parameters from PMP side:
PMP User Name - Logged in user name
Resource Name - Name of the resource
DNS Name - IP Address of the resource
User Account - Account name
Resource Type - Type of the resource being accessed (Windows/ WindowsDomain/ Linux etc.)
Resource Description - Description about the resource

Department - Department to which the resource belongs
Location - Resource location
Domain Name - Domain name of the resource
Request Type - Request Type for which ticketing system call is made. It can be

RETRIEVAL - Password access
REQUEST - Password access request raised through Access-Control workflow
RESET - Password reset
AUTOLOGON - 'Open Connection' request

User Organization Name - Organization name of the user who made the request
User Current Organization Name - Name of the organization where the requested account is present
Other than this, all additional columns will be sent as shown below:
Resource additional field - Resource@<field_name>
Account additional field - Account@<field_name>

Credentials to Access Ticketing System

AUTHTOKEN - Authentication token value given in the integration GUI
TICKETINGSYSTEMURL - URL given in the integration GUI

Advanced Configuration Details

ISPMPTICKETCRITERIA - To check if PMP vs Ticketing system is configured or not

(Boolean - true or false)

PMPTICKETCRITERIACOLUMNS - Mapping details between PMP and ticketing system. Each element in the array represents a criteria. For example, the column 'User Account' in PMP has to be validated against Ticketing system column 'REQUESTER' with match parameter 'EQUAL' in criteria 'C1'

JSONArray - [["C1","User Account","REQUESTER","EQUAL"],
["C2","PMP User Name","TECHNICIAN","EQUAL"]]

PMPTICKETCRITERIA - Specifies the relationship between different criteria.Each element of 'PMPTICKETCRITERIACOLUMNS' contains the first parameter as criteria name. It gives the relationship between criteria

(String - Example: C1 or C2)

ISTICKETVALUECRITERIA - To check if the validation for ticketing system values is configured or not

(Boolean - true or false)

TICKETVALUECRITERIACOLUMNS - Mapping details that ticket should satisfy. Each element in the array represents an criteria. For example, ticket column 'STATUS' has to be validated against value other than 'Closed' in criteria 'C1'

JSONArray - [["C1","STATUS","Closed","NOT_EQUAL"],
["C2","URGENCY","high","EQUAL"],
["C3","IMPACT","high","EQUAL"]]

TICKETVALUECRITERIA - Specifies the relationship between different criteria. Each element of 'TICKETVALUECRITERIACOLUMNS' contains the first parameter as criteria name. It gives the relationship between criteria

(String - Example: C1 or (C2 and C3)

ISTICKETCHANGEIDSTATUS - To check if the validation for system change status check is configured or not (true or false)

TICKETCHANGEIDSTATUS - Associated 'change ID status' of the ticket ID value

Match Parameters can be

EQUAL - Values of two parameters should be same
NOT_EQUAL - Values of two parameters should not be same
CONTAINS - First parameter value should contain the value of second parameter
NOT_CONTAINS - First parameter value should not contain the value of second parameter,
STARTS_WITH - First parameter must start with value of second parameter,
ENDS_WITH - First parameter must end with value of second parameter,
(Date based comparison parameters)
LESS_THAN - First parameter date value should be less than the second one,
GREATER_THAN - First parameter date value should be greater than the second one,
LESS_THAN_EQUAL - First parameter date value should be less than or equal to the second one,
GREATER_THAN_EQUAL - First parameter date value should be greater than or equal to the

second one
Depending on the match parameters, the criteria should get validated.

Code Snippet For ServiceNow Custom Implementation

If the advanced configuration does not satisfy your requirements, you can have a custom implementation. You can extend the default implementation provided by PMP and have the additional functionalities. The following example shows how the default implementation created for ServiceNow, can be extended to serve as the custom implementation.

```
package com.manageengine.ts;
import java.util.Properties;
import org.json.simple.JSONObject;
import com.adventnet.passtrix.helpdesk.ServiceNowImpl;

//ServiceNow custom implementation
public class ServiceNowCustomImpl extends ServiceNowImpl
{
  public boolean checkViewHelpDeskRequest(String ticketId, Properties pmpColumns,
Properties credentialDetails, JSONObject criteriaDetails)
   throws Exception
  {
        boolean result = super.checkViewHelpDeskRequest(ticketId, pmpColumns,
credentialDetails, criteriaDetails);
        //Your own implementation
        return result;
  }
}
```

The table below lists down default functionality processing classes for the ticketing systems that readily integrate with PMP:

ServiceDesk Plus On-Demand	com.adventnet.passtrix.helpdesk.ServiceDeskPlusOnDemandImpl
ServiceDesk Plus MSP	com.adventnet.passtrix.helpdesk.ServiceDeskPlusMSPImpl
ServiceDesk Plus	com.adventnet.passtrix.helpdesk.ServiceDeskPlusOnPremiseImpl
ServiceNow	com.adventnet.passtrix.helpdesk.ServiceNowImpl

Interface Description

The interface for ticketing system integration:

```
package com.manageengine.ts;

import java.util.Properties;
import org.json.simple.JSONObject;

// This class provides the methods to implement ticketing system integration. You need to implement this interface
public interface TicketingSystemInterface
{
  /**
   * Used to display the error message while doing the ticketing system related operations. The output gets reflected in audit trails.
   * @return Error message, if the ticketing system accessible, return null. Otherwise, return a proper error message.
   */
  public String getErrorMsg();
  /**
   * Used to return the properties related to the ticketing system operation
   * @return Comments and needed message
   */
  public Properties getRequestProperties();
  /**
   * Used for testing configuration setup. While testing, administrator will be able to get ticket details from the ticketing system.
   * @param tsName Ticketing system Name
   * @param tsUrl Ticketing system Web URL
   * @param authToken Authentication Token assigned to a technician of ticketing system (Base64 authorization string constructed using login credentials in the case of ServiceNow ticketing system)
   * @param ticketId Ticket ID given as the input ((Ticket ID/Sys ID in the case of ServiceNow ticketing system)
   * @param Ticketing System operation type
   *      {@value 0} Ticketing Operation
   *      {@value 1} Change Related Operation
   * @return the output from ticketing side
   * @throws Exception
   */
  public JSONObject helpdeskCheck(String tsName, String tsUrl, String authToken, String
```

```
ticketId, String operation) throws Exception;
  /**
   * Actual function that will be called upon whenever a ticketing system related operation is done from PMP GUI
   * @param ticketId Ticket ID (Ticket ID/Sys ID in the case of ServiceNow ticketing system)
   * @param pmpColumns Details of the PMP account for which ticketing system query is raised
   * @param credentialDetails Key details of ticketing system (Authentication token or Base64 authorization string and web URL of ticketing system)
   * @param criteriaDetails Criteria mapping done as part of advanced configuration
   * @return Final output that will be sent to PMP server
   *     {@value true} Success case - Allows the operation to proceed
   *     {@value false} Failure case - Denies the operation to proceed
   * @throws Exception
   */
  public boolean checkViewHelpDeskRequest(String ticketId, Properties pmpColumns, Properties credentialDetails, JSONObject criteriaDetails)
   throws Exception;
}
```

Exporting Resource Groups

PMP provides three options to export all the passwords that are part of any specific resource group for secure offline access.

- The basic option is to export the resources belonging to the resource group in plain-text in a spreadsheet
- The more secure option is to export them to an encrypted HTML file
- There is also provision to create a scheduled task to export the resources belonging to any resource group as an encrypted HTML file

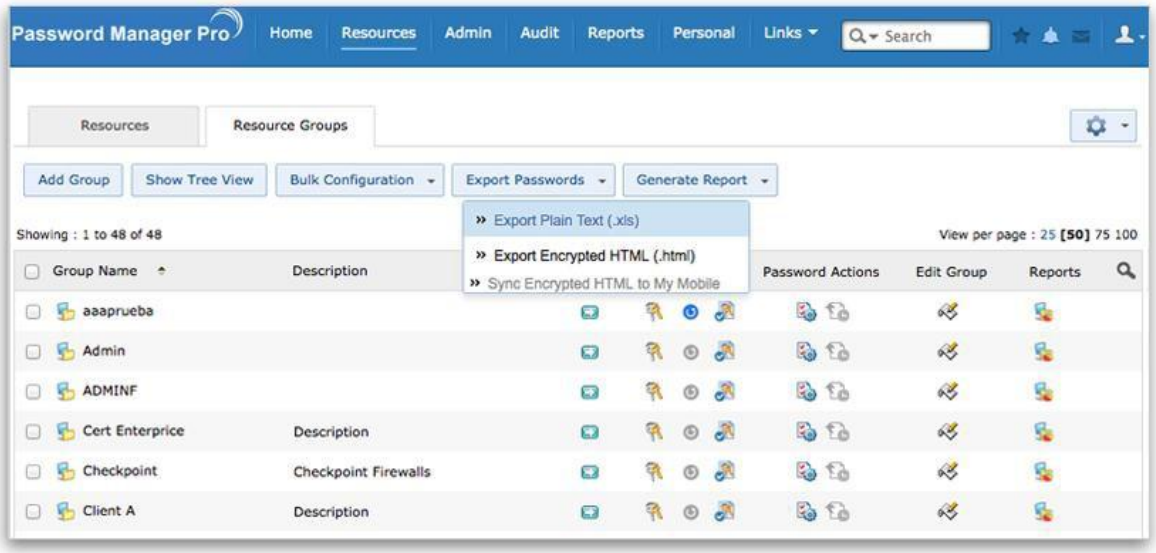
In all the options above, you can export the resources, accounts and passwords that are part of specific resource groups for offline access.

Option 1: Exporting resource groups in plain-text (.xls)

The passwords belonging to specific resource groups can be exported by administrators and password administrators in plain-text in .xls format.

To export any resource group,

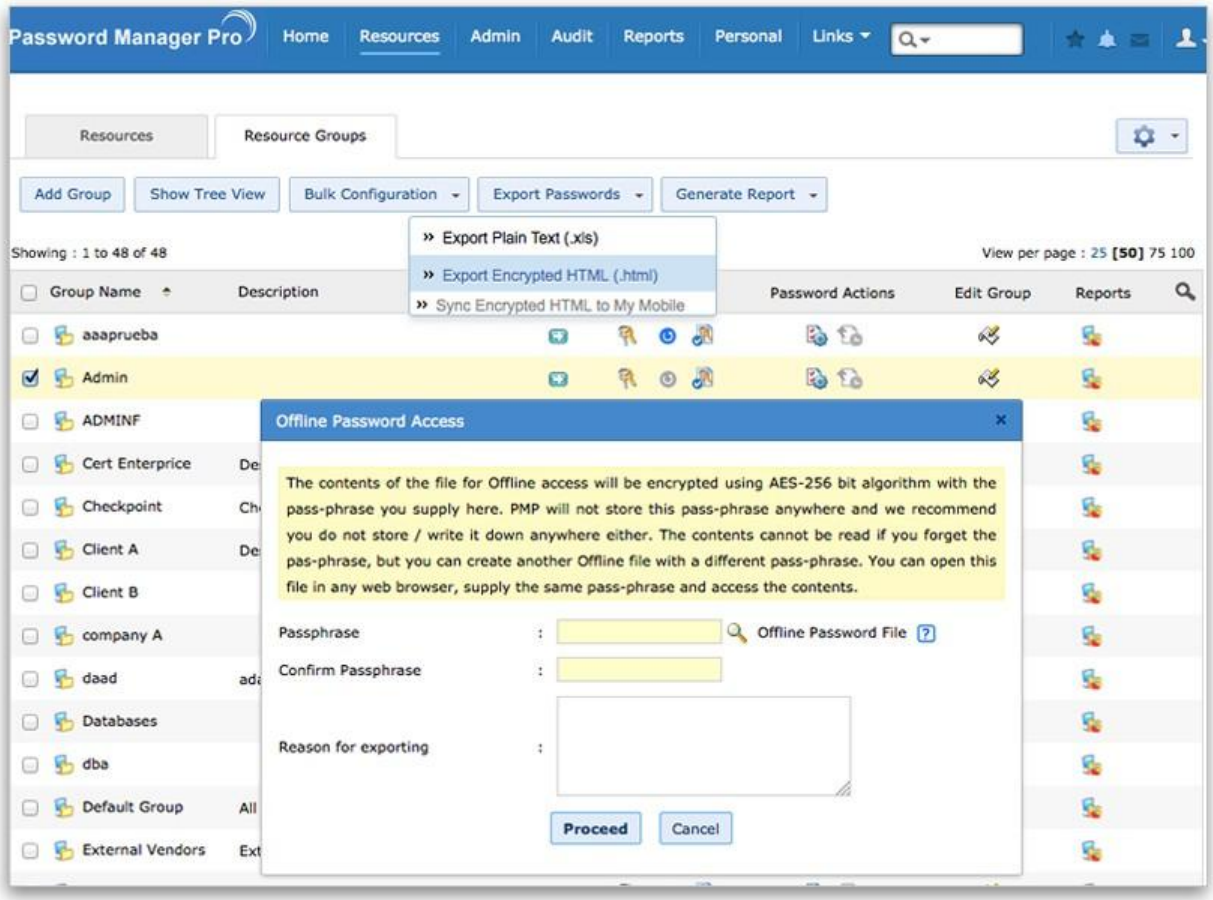
- Navigate to Resource Groups tab in GUI
- Select the required resource group(s)
- Click the option "Export Plain Text" in "Export Passwords" button
- The resources that are part of the selected resource groups will be exported to a file and it is shown as a pop-up
- Save the file in a secure location (in .xls format)



Option 2: Exporting passwords as encrypted HTML

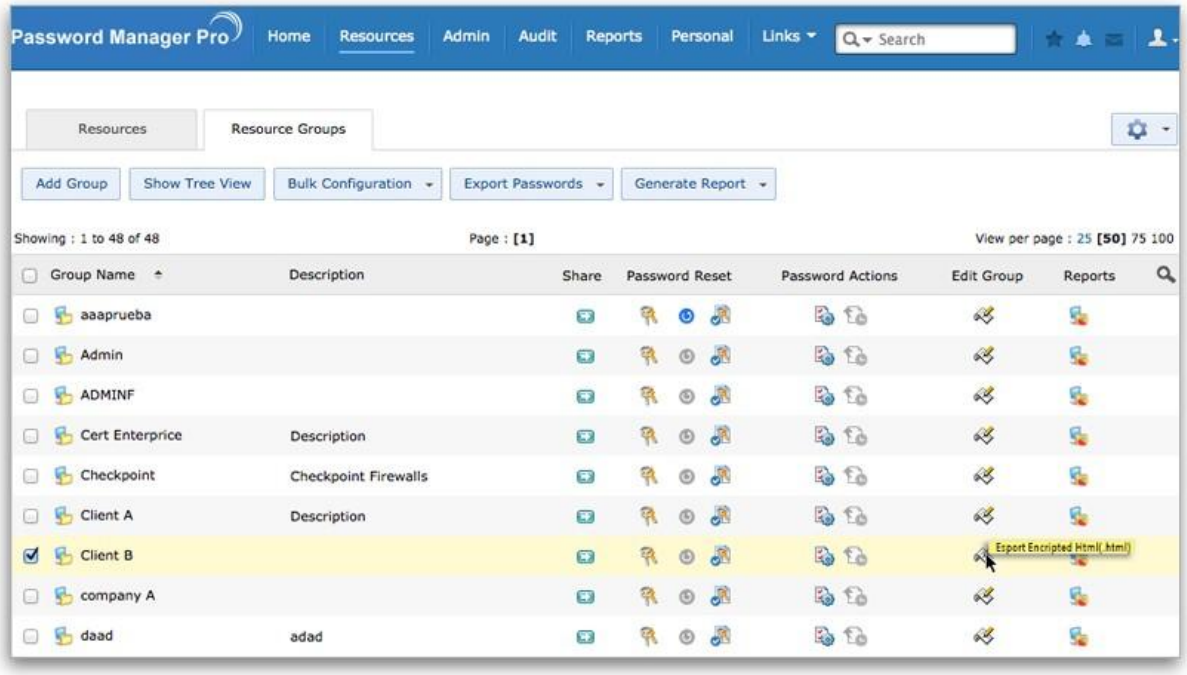
To export any resource group,

- Navigate to Resource Groups tab in GUI
- Select the required resource group(s)
- Click the link "Export Encrypted HTML (.html)" of "Export Passwords" button
- In the UI that pops-up, you need to specify a passphrase that will be used for encryting (AES-256) the HTML file for offline access. You will have to specify the passphrase in accordance with the password policy as enforced by your administrator. PMP will not store this passphrase anywhere and we recommend you not to store or write it down anywhere either. The contents cannot be read if you forget the passphrase, but you can create another offline file with a different passphrase. You can open this file in any web browser, supply the same passphrase and access the contents.
- Confirm the passphrase and also enter a reason for exporting the passwords
- The resources will be exported as a HTML file. It will take some time for exporting the resources and the offline copy will be displayed in a pop-up in the GUI.
- Save the file in a secure location (in .html format)



Option 2: Exporting passwords as encrypted HTML
(Feature available only in Enterprise Edition)

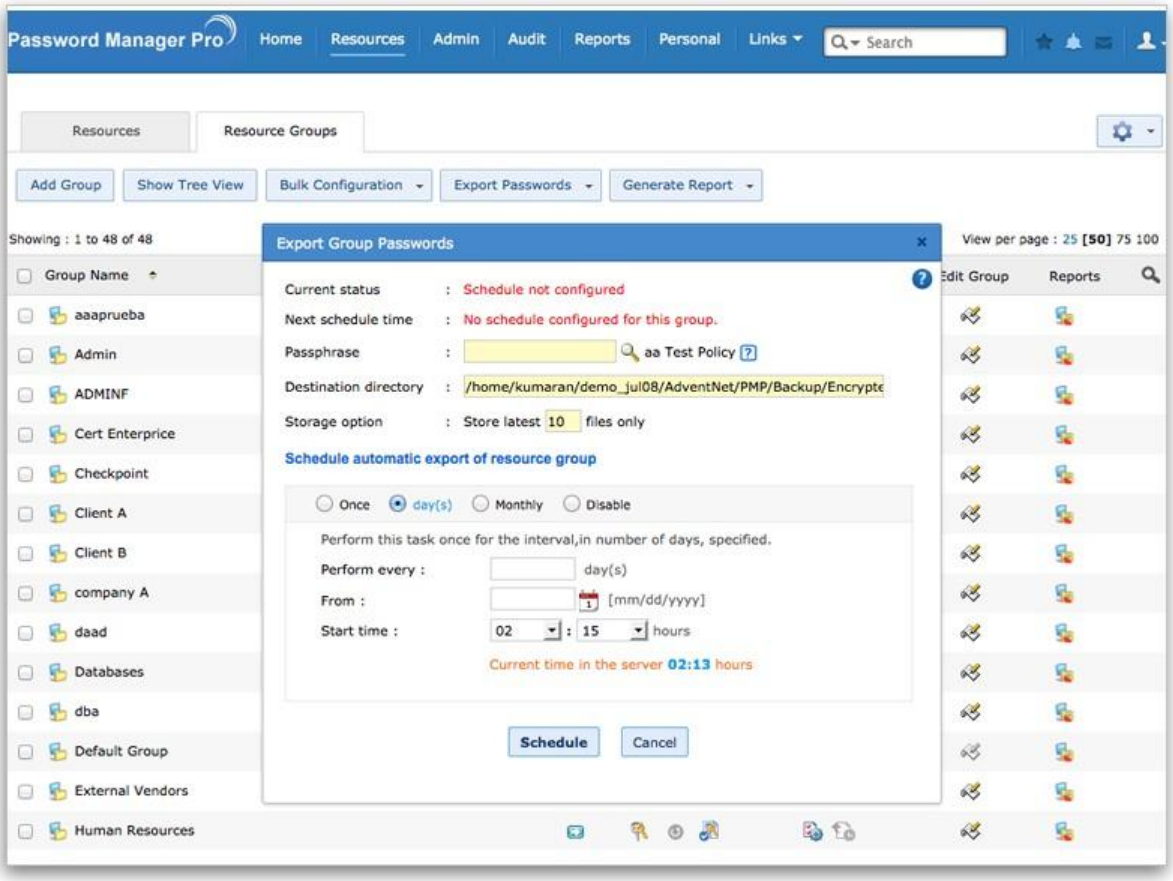
- Navigate to "Resource Groups" tab in the GUI
- Click the icon for scheduled export present along the required resource group under "Password Actions" column



In the GUI that opens,

- you need to specify a passphrase that will be used for encrypting (AES-256) the HTML file for offline access. You will have to specify the passphrase in accordance with the resource group's password policy. You can open this file in any web browser, supply the same passphrase and access the contents.
- specify the destination where the exported HTML file has to be stored. You may specify any location accessible to PMP for the write operation. By default, the files are stored under <PMP-Installation-Folder>/Backup/EncryptedFiles
- specify the number of files to be stored. By default, only the latest 10 files will be kept. Others will be deleted
- specify the schedule for resource group export. The schedule can be for one-time rotation or it could be for a recurring one at periodic intervals. Depending on your requirements, choose any one among the options - Once / Days / Monthly / Never. After selecting the option, specify other details as required and click "Schedule"

The required schedule will be created and resources belonging the selected resource groups will be exported as encrypted HTML.



Scheduled Password Rotation

(Feature available only in Premium and Enterprise Editions)

Shared administrative passwords are prone to misuse even in a very secure environment and periodic rotation of passwords is very much needed. Manually changing the passwords one-by-one would prove to be laborious. PMP helps in automating the process of changing the passwords periodically for which remote password reset is supported in PMP. Scheduled Password Rotation can be done only at the resource group level.

The prerequisite for using this feature is the proper configuration of password reset either by agentless mode or by deploying agents in the remote resource.
Multiple options are available to set the periodicity of password rotation. Notifications are generated both before and after the password reset task is run, with a consolidated report of the results for each password.

To add a schedule for rotating passwords of the resources of a group,

- Go to "Resources" tab in the web interface
- Click "Resource Groups" tab (alternatively, you can launch this page directly through the "Add Resource Group" link under the "Links" drop-down)
- Click the icon present against the resource group for whose resources password rotation is to be enabled
- In the UI that opens up, the required schedule can be created through the following four-step process

Step 1 Settings for sending notification prior to password rotation,

When a password is scheduled to be rotated at a specified time, the users who have access to the present password(s) are to be informed about the rotation operation beforehand - say for example, a day prior to the rotation. Apart from the users directly connected with the passwords to be rotated, any other user could also be informed of the scheduled rotation on need basis.

Pre-Notification Timing

- You can choose to send the notification anytime a week prior to the actual rotation schedule. The notification could be sent even a minute prior to the rotation. Select the number of days and/or hours and/or minutes prior to which the notification is to be sent.
- Specify the recipients of the notification -
  - Users having access to the passwords - users who possess any one of the share permissions (read only, read and write, manage) for the password, at the time when notification is generated
  - Other Users/ User Groups - any other specific user(s) (to be selected from the list)
  - Email ids - to generate notifications to specified list of email aliases or email addresses
  - Click "Next"

Step 2 Specify the new password to be used

- You have the option to specify the new password(s) to be used for resources after rotation.
- You can either choose to allot randomly generated, unique passwords to the accounts based on the password policy set for the group or you can allot a new, common password to all the resources (in accordance with the password policy already specified for the group)
- You can also assign the same password to all user accounts, with the condition that the password should be changed during every schedule
- Select the required choice and click "Next"

Step 3 Specify the rotation schedule

Actual creation of the schedule for password rotation is done in this step. The schedule can be for one-time rotation or it could be for a recurring one at periodic intervals. Depending on your requirements, choose any one among the options - Once / Days / Monthly / Never. After selecting the option, specify other details as required and click "Next"

Step 4 Settings for sending notification after password rotation

Immediately after the completion of password rotation process, notification could be sent to all those who have access to the passwords regarding the completion of the rotation. Apart from the users directly connected with the passwords to be rotated, any other user could also be informed of the rotation on need basis.

- Specify the recipients of the notification -
    - Users having access to the passwords - users who possess any one of the share permission (read only, read and write, manage) for the password, at the time when notification is generated
    - Other Users/ User Groups - any other specific user(s) as selected from the list
    - Email ids - to generate notifications to specified list of email aliases or email addresses
    - Click "Finish"
    - The required password rotation schedule has been created. The setting could be saved as a template for use with configuring password reset schedule for another resource group.

Windows Service Account Password Reset

(Feature available only in Premium and Enterprise Editions)

Windows Service Accounts, used by the system programs to run application software services or processes often possess higher or even excessive privileges than normal user accounts. These are indeed very powerful accounts that run critical business processes and services. Many third-party services or scheduled tasks or processes might make use of the same service account, resulting in a complex interconnection.

Typically, specific windows domain accounts are used as service accounts in services running in Windows servers, that need network access. Password Manager Pro has the ability to identify the service accounts associated with a particular domain account. While resetting the password of a domain account managed in Password Manager Pro, it will find out the services which use that particular domain account as service account. It will automatically reset the service account password when the domain password is changed.

In certain cases, you will require to restart the services for the service account password reset to take effect. The windows service account password reset feature of PMP helps achieve this precisely, fully automated.

How does windows service account reset work?

For every Windows domain account for which the service account reset is enabled, PMP will find out the services which use that particular domain account as service account, and automatically reset the service account password if this domain password is changed.

How to setup Windows Service Account Password Reset?

Prerequisite: Before enabling windows service account reset, ensure if the following services are enabled in the servers where the dependent services are running:
(1) Windows RPC service should have been enabled
(2) Windows Management Instrumentation (WMI) service should have been enabled

Work flow Summary: Setting up Windows Service Account Password & Scheduled Task Password Reset
Consider that

- You have a Service Account SA1
- You have four servers Win1, Win2, Win3 & Win4 that make use of SA1
- Your domain name is MyDomain and the SA1 is present in this domain

- Your domain administrator account is DomainAdmin

For enabling Windows Service Account Reset, you need to do the following:

- Create Windows resources for each of the servers that use service accounts. In the above example, you need to create Win1, Win2, Win3 & Win4 as four separate resources (with resource type 'Windows'). (In the case of service accounts spread across multiple domains, PMP uses the local administrator account to login. So, if you wish to have service account password reset for multiple domains, ensure that you have entered local administrator account while creating the resource).
- Create a resource group consisting of these resources - say RG1
- Create a Windows Domain resource. In the above example, it will be MyDomain with resource type Windows Domain
- Inside the domain account, add the individual domain account. In the above example, add SA1 as domain account
- Specify the Resource Group (the group that contains the resources that use the domain account as the service account) that are associated with the domain account. In the above example, associate SA1 with RG1
- Specify the domain administrator account. In this example, it is DomainAdmin. This is required for resetting the service account

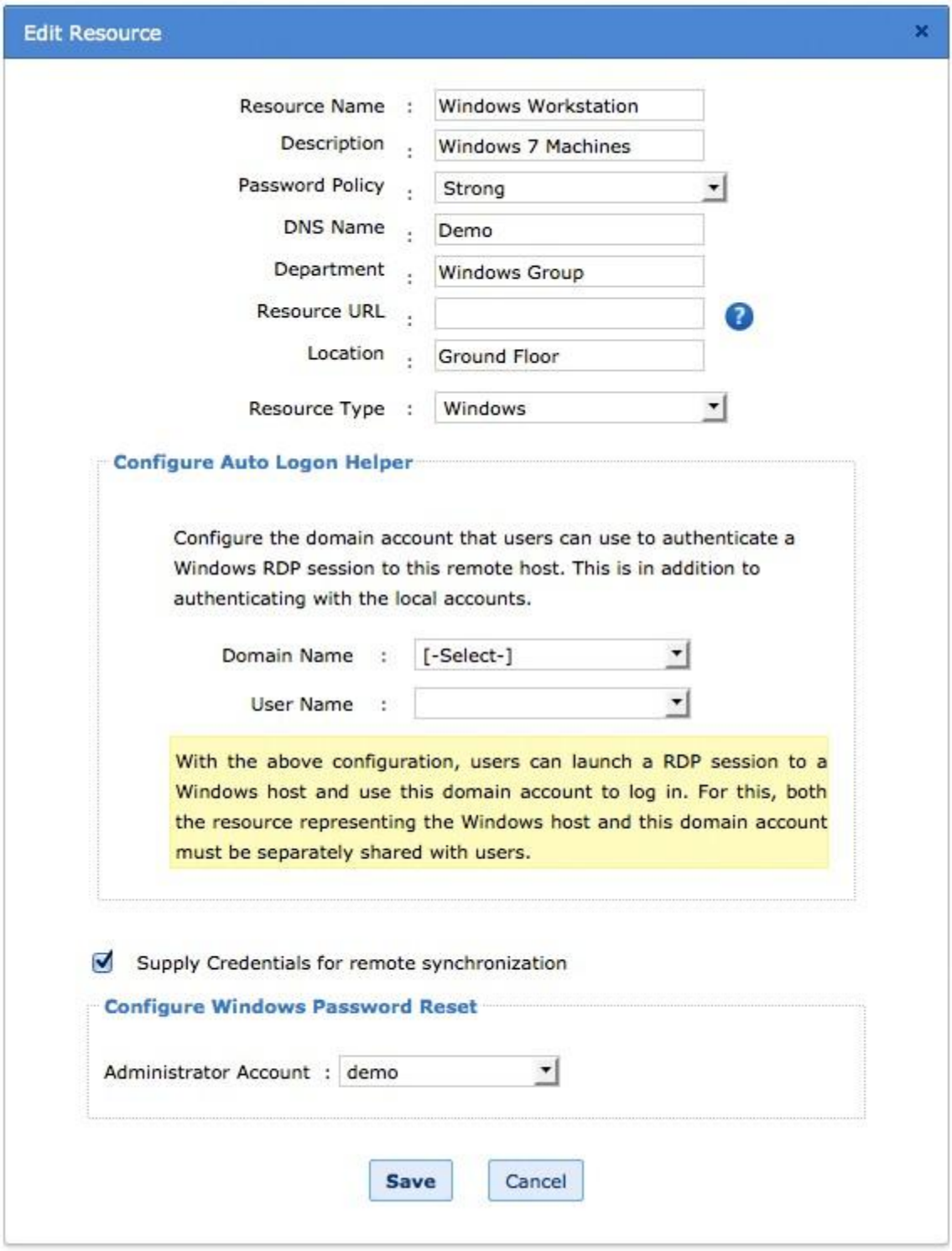
Now, when the domain account password is reset

- It is modified immediately in the domain
- PMP iterates through the associated resource group and for each resource find the list of services and scheduled tasks which use this domain account as their service account
- PMP uses the domain administrator credentials to login to the servers and forcefully modify the service account password and schedules task passwords too and restart the services.

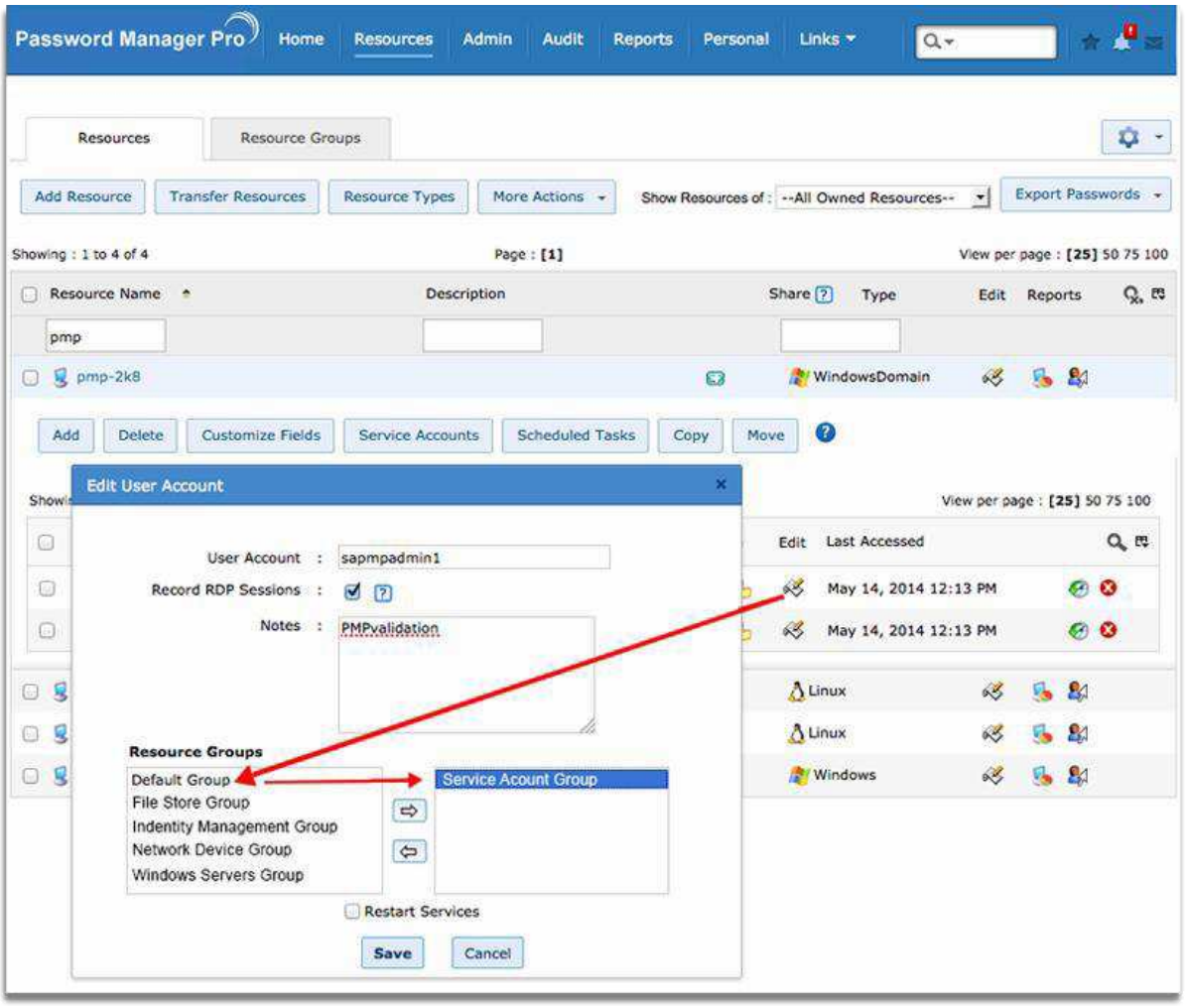
Steps to configure Windows Service Account Password Reset

- Add the Domain controller as 'Windows Domain' resource type. Make sure that you specify the DNS name and Domain name.
- Add the domain administrator account to this 'Windows Domain' resource.
- Add the service account which is used as logon account to this 'Windows Domain' resource./li>
- Add each machine in which services are running as individual resource with resource type 'Windows'.

- Create a resource group which contains all these windows machines. For example: Service Account group.
- Click "edit" button of the 'Windows Domain' resource and select the domain administrator account which you added in the 'Supply credentials for remote synchronization' section. Refer to the screenshot below:



- Click "edit" of the service account and move the resource group which you created to the box on the right side and save. Refer to the screenshot below:



  - Check the checkbox for service account which you added in the 'Windows Domain' resource and click on the service account tab-> select Supported service accounts tab. Services which uses this service account as log on account will be listed. When you reset the password, it will be reset in the service running in the remote machine as well.

Important Note :
In certain cases, there would be requirements for stopping and starting the services during domain account reset. In such cases, through "General Settings" you can configure PMP to wait for a specified time period (in seconds) between stopping and starting the services. By default, PMP waits for 60 seconds. You may configure it in accordance with your needs.

Viewing Service Account Status

For any windows domain account (for which you have enabled Windows service account reset), you can view the list of associated service accounts, scheduled tasks and information on whether the service accounts and scheduled tasks were reset upon the corresponding domain account reset.

To view this information,

- Go to "Resources" tab click the name of the resource
- Select the domain account of the resource for which you wish to know the status of service account reset
- Click "Service Account Status"

Important Note
(1) Whenever the password of the domain account is changed, the windows service account associated with it will also be changed. In case, you have created schedules for rotating domain accounts, the service account reset will also follow the schedule.
(2) Once you create Windows Service Account Reset, the passwords of the Windows scheduled tasks associated with the service accounts will also be reset.

Password Action Notification

(Feature available only in Premium and Enterprise Editions)

Any action performed on a password, be it just a password access or modification or changing the share permission or when the password expires or when password policy is violated, notifications are to be sent to the password owners and/or to those who have access to the passwords or to any other users as desired by the administrators. The 'Password Action Notification' feature helps in achieving this.

You can configure E-mail notification on the occurrence of specific events as mentioned above. When password shares are changed and when passwords expire, in addition to notifications, there is option for password reset action to be performed by the PMP server. When a password belongs to multiple groups and each group has different actions configured, every distinct action will be performed once.

To add a schedule for rotating passwords of the resources of a group

- Go to "Resources" tab in the web interface
- Click "Resource Groups" tab (alternatively, you can launch this page directly through the "Add Resource Group" link under the "Links" tab)
- Click the icon present against the resource group for which password action notification is to be enabled
- In the UI that opens up, select the condition upon which you wish to send notifications and click the button at the end

When passwords are accessed

As mentioned earlier, when a user views a password, email notification (informing the access) could be sent to desired recipients.

If you want to make use of this action,

- Specify the recipients of the notification -
    - Owner - the owner of the password
    - Users having access to the passwords - users who possess any one of the share permission (read only, read and write, manage) for the password, at the time when notification is generated
    - Other Users/ User Groups - any other specific user(s) as selected from the list

    - Email ids - to generate notifications to specified list of email aliases or email addresses. If you want to enter multiple ids, you may do so by separating each address with a comma
    - Click "Save"
    - You can also generate a SNMP Trap and/or Syslog Message to your network management system. Before selecting an option here, make sure you have carried out SNMP Trap/Syslog settings.

When passwords are changed

As mentioned above, when a password is changed, notification (informing the change) could be sent to desired recipients.

If you want to make use of this action,

- Specify the recipients of the notification -
    - Owner - the owner of the password
    - Users having access to the passwords - users who possess any one of the share permission (read only, read and write, manage) for the password, at the time when notification is generated
    - Other Users/ User Groups - any other specific user(s) as selected from the list
    - Email ids - to generate notifications to specified list of email aliases or email addresses. If you want to enter multiple ids, you may do so by separating each address with a comma
    - Click "Save"
    - You can also generate a SNMP Trap and/or Syslog Message to your network management system. Before selecting an option here, make sure you have carried out SNMP Trap/Syslog settings.

When password share is changed

In multi-user environments, passwords are shared among multiple persons. In such a scenario, when a password permission of a password is changed, notification (informing the change) could be sent to desired recipients.

If you want to make use of this action,

- Specify the recipients of the notification -
    - Owner - the owner of the password
    - Users having access to the passwords - users who possess any one of the share permission (read only, read and write, manage) for the password, at the time when notification is generated
    - Other Users/ User Groups - any other specific user(s) as selected from the list
    - Email ids - to generate notifications to specified list of email aliases or email addresses. If you want to enter multiple ids, you may do so by separating each address with a comma
    - You have the option to reset passwords in addition to sending notifications. For example, when the share for a password is removed, if you wish to automatically reset the password, you may do so by selecting the checkbox 'Reset the password when a share is removed'. Password reset action is applicable and performed only for passwords for which it is currently supported and correctly configured, using one of remote or agent modes
    - Click "Save"
    - You can also generate a SNMP Trap and/or Syslog Message to your network management system. Before selecting an option here, make sure you have carried out SNMP Trap/Syslog settings.

When passwords expire

To enhance password security, passwords of sensitive accounts would be rotated periodically. In such a scenario, validity period is set for a password. When the validity ends, the password expires and a notification (informing the expiry) could be sent to desired recipients.

How do I set Password Expiry for a resource?

Password Validity Period could be set through password policies. After the validity period, the password would expire and it has to be reset.

If you want to make use of this action,

- Specify the recipients of the notification -
    - Owner - the owner of the password
    - Users having access to the passwords - users who possess any one of the share permission (read only, read and write, manage) for the password, at the time when notification is generated
    - Other Users/ User Groups - any other specific user(s) as selected from the list
    - Email ids - to generate notifications to specified list of email aliases or email addresses. If you want to enter multiple ids, you may do so by separating each address with a comma
    - You have the option to reset passwords in addition to sending notifications. For example, when the share for a password is removed, if you wish to automatically reset the password, you may do so by selecting the checkbox 'Reset the password when a share is removed'. Password reset action is applicable and performed only for passwords for which it is currently supported and correctly configured, using one of remote or agent modes
    - Click "Save"
    - You can also generate a SNMP Trap and/or Syslog Message to your network management system. Before selecting an option here, make sure you have carried out SNMP Trap/Syslog settings.

When password policy is violated

If you have defined a password policy and if the passwords are in violation to the policy defined, notifications (informing the violation) could be sent to desired recipients. The notification would be sent everyday.

If you want to make use of this action,

- Specify the recipients of the notification -
    - Owner - the owner of the password
    - Users having access to the passwords - users who possess any one of the share permission (read only, read and write, manage) for the password, at the time when notification is generated
    - Other Users/ User Groups - any other specific user(s) as selected from the list
    - Email ids - to generate notifications to specified list of email aliases or email addresses. If you want to enter multiple ids, you may do so by separating each address with a comma

    - You have the option to reset passwords in addition to sending notifications. For example, when the share for a password is removed, if you wish to automatically reset the password, you may do so by selecting the checkbox 'Reset the password when a share is removed'. Password reset action is applicable and performed only for passwords for which it is currently supported and correctly configured, using one of remote or agent modes
    - Click "Save"
    - You can also generate a SNMP Trap and/or Syslog Message to your network management system. Before selecting an option here, make sure you have carried out SNMP Trap/Syslog settings.

When passwords in PMP go out of sync with those in the resource

When the passwords stored in PMP differ with those in the resource, notifications (informing the out of sync) could be sent to desired recipients. Every night at 1 AM, PMP tries to establish connection with the target systems for which remote password sync has been enabled. Once the connection is established, it tries to login with the credentials stores in PMP. If login does not succeed, PMP concludes that the password is out of sync. In case, PMP is not even able to establish connection with the system due to some network problem, it will not be taken as password out of sync.

The out of sync notification would be sent everyday.

If you want to make use of this action,

- Specify the recipients of the notification -
    - Owner - the owner of the password
    - Users having access to the passwords - users who possess any one of the share permission (read only, read and write, manage) for the password, at the time when notification is generated
    - Other Users/ User Groups - any other specific user(s) as selected from the list
    - Email ids - to generate notifications to specified list of email aliases or email addresses. If you want to enter multiple ids, you may do so by separating each address with a comma
    - Click "Save"
    - You can also generate a SNMP Trap and/or Syslog Message to your network management system. Before selecting an option here, make sure you have carried out SNMP Trap/Syslog settings.

See also "Running Integrity Check on demand".

Changing the Email Notification Content

In all the above cases, email notifications are sent to the specified recipients. PMP provides the option to customize the email content. Refer to the"Email Templates" section for complete details.

Password Reset Listener

Password Reset is one of the important operations performed by the PMP. After resetting the password of resources/accounts in PMP, there might be requirements to carry out some follow-up action automatically. This could be done using the Password Reset Listeners.

For Example:

- restarting the dependent services immediately after password reset
- if there is a windows service that makes use of the account whose password is being changed in PMP. You can use the listener mechanism to change the 'stored credentials' (i.e the credentials specified in the 'Logon' property) of the windows service
- if you have added the accounts of network devices as resources/accounts in PMP, you can first reset the passwords of such accounts locally and then invoke a custom script to connect to the device and carry out the change in the device too
- reset the passwords of windows scheduled tasks and other associated processes

How does Password Reset Listener work?

Whenever the password of an account is modified in the PMP repository, you can configure PMP to invoke a script or executable supplied by you. The script or the executable is called the Password Reset Listener. The listener will be invoked even for local password changes and for resources for which remote password reset is not supported. It can be configured for each resource type, including the user defined resource types. Thus, the password reset listener mechanism is very helpful for resource types for which PMP does not support remote password reset by default.

- The password reset listener script will be invoked in a similar fashion as it will be from the command prompt of the operating system from which it is invoked
- In case, the script needs another program to invoke it from the command prompt, it could be provided as the 'Pre-Command' for that script (for example 'cscript c:\scripts\changepassword.vbs old_password new_password)
- PMP will pass these arguments, in this order, when the script is invoked: resource name, dns name, account name, old password, new password.
- You can add additional arguments that will also be supplied at the time of invoking the script, in the order specified

The script runs with the same privileges as the user account running the PMP server. To guard against potential risks associated with invoking arbitrary scripts, a dual control mechanism is implemented, which will ensure two administrators see and approve the script

before it is invoked by PMP. When an administrator adds a password reset listener, PMP does not invoke it unless it has been approved by another administrator. The same process if followed when the password reset listener details are edited by an administrator. These operations can be performed by any two administrators and are audited.

The password reset listener is invoked from a separate thread so that it does not impact the password reset process of PMP. The password reset listener script supplied will be stored in the same database as the other information, which provides security as well as backup, if it is configured for the PMP database.

How to setup Password Reset Listener?

Prerequisite
Before setting up the password, keep your custom script/executable ready. PMP has no control over the script other than invoking it and also does not process the result of the script. So, take care of all your requirements while creating the script.

To set up Password Reset Listener,

- Go to "Admin" >> "Customize" >> and click "Password Reset Listener"
- In the UI that opens, click the button "Add Listener"
- As mentioned above, the password reset listener script will be invoked in a similar fashion as it will be from the command prompt of the operating system from which it is invoked. In case, the script needs another program to invoke it from the command prompt, it could be provided as the'Pre-Command' for that script (for example 'cscript c:\scripts\changepassword.vbs old_password new_password)
- Provide a name for the listener to be created. This would uniquely identify the listener
- Browse and locate the listener script
- By default, the parameters resource name, dns name, account name, old password, new password are passed as arguments to the script. In case, you require to pass additional arguments, specify them against the text field "Additional Parameters". The additional parameters supplied here will be passed to the script as they are
- Specify the Resource Types for which the changes are to be applied

Approval for Listeners

As explained above, the listener script runs with the same privileges as the user account running the PMP server. To guard against potential risks associated with invoking arbitrary scripts, a dual control mechanism is implemented, which will ensure two administrators see and approve the script before it is invoked by PMP.

The listeners can be added only by PMP administrators. The listeners thus added have to be approved by some other administrator. So, the listener created will remain pending for approval. Select an administrator from the drop-down to send approval request. A mail will be sent to that administrator intimating the approval request.

If you are an administrator and requested by another admin to approve a listener, you need to navigate to "Admin" >> "Customize" >> and click"Password Reset Listener" and click the link present under "Approval Status". Once it is approved, the listener will take effect.

- Click "Save". The required listener has been created

The listener creation and approval events are all audited in PMP.

Custom Listener

(Feature available only in Enterprise Edition)

Password Manager Pro allows you to provide your own implementation for Password Reset Listener through "custom listener". The custom listener basically lets you provide your own listener implementation class, instead of just letting PMP execute the listener script provided by you. It offers you complete flexibility to execute any post password reset follow-up action.

How to Create Custom Listener?

Summary of steps involved in custom Listener creation:

Step 1: Write your own implementation class

Implement PMPListenerInterface (more details in the reference implementation below)

Step 2: Configuration in PMP GUI

Add entries for the implementation class in PMP GUI

Step 3: Archive your implementation class as .jar and put it into PMP

Step 4: Restart PMP

Reference Implementation

To explain how you can have your own implementation for listener in PMP, we are providing a reference implementation below. This implementation is for executing PowerShell scripts with reset listener.

Step 1: Write your own implementation class

You need to write your own class implementing PMPListenerInterface.java as explained below.

```
public interface PMPListenerInterface {
static final Logger LOG =
Logger.getLogger(PMPListenerInterface.class.getName());
public String executeListener(Properties resourceProps, Properties accountProps,
String listenerFilePath, String oldPassword) throws Exception;
}
```

You can implement your class in such a way that properties of resources (resources and accounts in PMP) are obtained as arguments. For example, if you need 'Resource Name', you may have to do it as below:

```
resourceProps.get("RESOURCENAME")
```

You may obtain the value of any propery from the list of keys listed below.

Resource Properties (resourceProps)

RESOURCENAME - Name of the Resource added in Password Manager Pro
IPADDRESS - DNSName or IPAddress of the Resource
RESOURCEURL - Resource URL configured for the resource
DOMAINNAME - Domain Name if the Resource is of type WindowsDomain
SSHPORT - SSH Port if the device can be connected over SSH
RESOURCEDESC - Description of the resource
LOCATION - Location of the Resource
DEPARTMENT - Department to which the resource belongs to
ALL RESOURCE CUSTOM COLUMN NAMES (Label name will be the key)

Resource Properties (resourceProps)

DESCRIPTION - Account's description
LOGINNAME - Login Name of the userAccount added into PMP
PASSWORD - Password for this user account
DOMAINNAME - Domain Name if the account added is a domain account
COMPLIANTSTATUS - Provides a status whether the password is in compliant with the Password Policy configured in PMP
COMPLIANTREASON - Reason, if the password is not compliant with the Password Policy
EXPIRYSTATUS - Status of expiry of the account's password
PASSWRDSYNCSTATUS - Provides information if the password is in sync with the password that is set on the remote resource
ALL ACCOUNT CUSTOM COLUMN NAMES (Label name will be the key)

Other Arguments

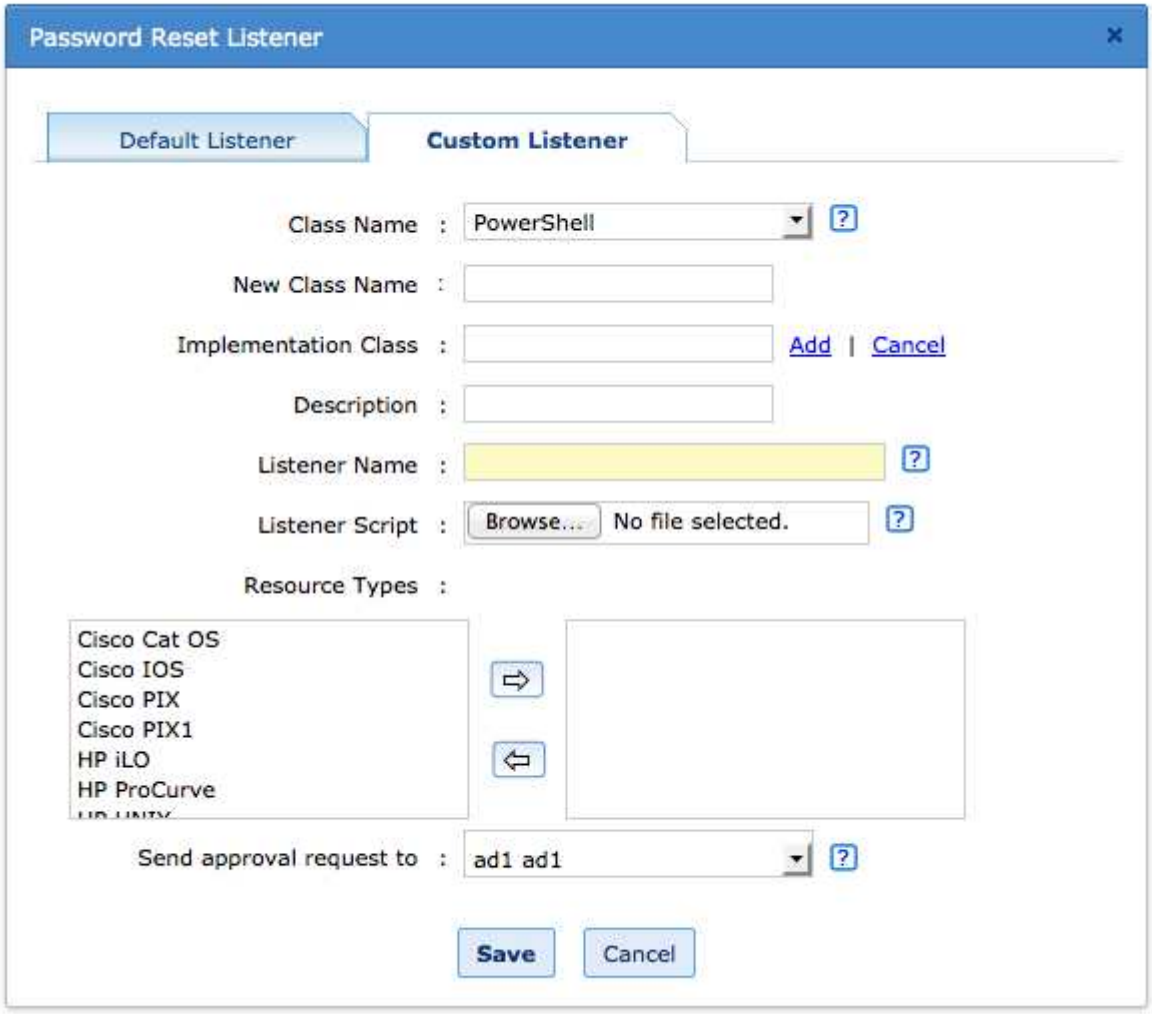
- listenerFilePath - The path of the script/file that you want to invoke as listener. You also have the option to provide the script/file while configuring the listener in PMP in Step 5.
- oldPassword - Passing the old password to the implementation class to carry out password reset

Sample implementation to execute PowerShell script

```
public class PowerShellListener implements PMPListenerInterface {
public String executeListener(Properties resourceProps, Properties accountProps, String listenerFilePath, String oldPassword) throws Exception {
String message = "Executed Successfully";// used for audit reason
// got the properties
// call the powershell script
}
}
```

Step 2: Configuration in PMP GUI

Add entries for your implementation class in PMP GUI. To do this, navigate to Admin >> Password Reset Listener >> Add Listener and in the GUI that opens, click the tab "Custom Listener" and then click the link "Add New". Enter the following details:



- Class Name - This lists down the already existing listener implementation classes
- New Class Name - The name of the new implementation class that provides the workflow for the custom listener
- Implementation Class - Full name of the implementation class with package details. For example: com.adventnet.passtrix.listener.PowerShellListener
- Description - Information about the implementation class
- Listener Name - Specify the name of the custom listener script with the appropriate extension. The label provided here will be invoked from the command line.
- Listener Script - Browse and locate the listener script. If you have provided the file/script path of the listener in your implementation class OR if you are making use of APIs to do password reset, you may skip this step. When you browse and submit the script in this step, it will be persisted in PMP database in fully encrypted form. The script will be invoked at runtime.
- Resource Types - Select the resource types to which the custom listener script will have to be applied

- Send Approval Request to - The listener script runs with the same privileges as the user account running the PMP server. To guard against potential risks associated with invoking arbitrary scripts, a dual control mechanism is implemented, which will ensure two administrators see and approve the script before it is invoked by PMP.The listeners can be added only by PMP administrators. The listeners thus added have to be approved by some other administrator. So, the listener created will remain pending for approval. Select an administrator from the drop-down to send approval request. A mail will be sent to that administrator intimating the approval request.If you are an administrator and requested by another admin to approve a listener, you need to navigate to "Admin" >> "Customize" >> and click "Password Reset Listener" and click the link present under "Approval Status". Once it is approved, the listener will take effect.
- Click "Save"
- The listener creation and approval events are all audited in PMP.

Step 3: Archive your implementation class as .jar and put it into PMP

You need to convert your implementation class as .jar and put it into <PMP-Installation Folder>/lib directory.

Step 4: Restart PMP

After completing the above steps, you need to restart PMP to give effect to this implementation.

Password Policies

Password policies help you define the characteristics of passwords of various strengths, which can then be used to enforce strong passwords on resources. Apart from the default policies, you can create your own based on your requirements. The built-in password generator can generate passwords compliant to the defined policies.

Password Generator randomly generates password based on the rule set by the administrator - for example, minimum number of characters, alphanumeric characters, mixed case, special characters etc. Every password input field in PMP has the password generator along-side and the policy that is set as system default will be used to generate passwords, unless directed otherwise.

Password policy for PMP can be centrally managed from the "Admin" tab:

- Go to "Admin >> Customize >> Password Policies"
- By default, three policies - Low, Medium and Strong are available in PMP indicating the relative strength of the passwords. Low represents the passwords with less strict constraints, medium with a few strict conditions and strong with very strict conditions. The three default policies cannot be edited or deleted
- You can set any one of the policy as the default policy -that is, when the user tries to change the password of a resource/account, the default policy would be enforced and the user would be forced to enter a password as per the policy. To set a policy as the default policy, just click the"set as default" icon present against the policy

You can create you own password policy based on your requirements. To create a password policy,

- Click "Add Policy"
- In the form that pops-up, provide a name for your policy, enter a description, specify the minimum and maximum password lengths, specify if mixed-cases, special characters are to be enforced and how many such special characters, specify if the password has to start with an alphabet, if login name could be used as password, how many old passwords are to kept in archives and the Password Age - i.e. the time limit (in days) up to which the password is valid. After the validity period, the password would expire
- Click "Save"

- How does a Password Policy get enforced in PMP?
  This question naturally arises when you are in the process of adding a resource. The following example would provide the answer: If your intention is to have accounts with strong passwords, others with admin privileges should not disturb this intention while changing the password. So, this step is crucial. If you want to enforce policy at time of resource addition itself, see "General Optional Settings" for details.

Applying Password Policies to Resources in Bulk

You can apply any password policy to many resources in bulk at one go.

- Go to "Resources" tab
- Select the resources for which you wish to apply the same password policy
- Click the link "Set Password Policy" from "More Options"
- Listing

In the UI that opens up,

- Select the required policy from the drop-down
- Click "Save"

Once you do this, the chosen password policy would be applied to all the selected resources in bulk. In case, any of the chosen resources were associated with a password policy already, this action would simply overwrite the previous policy.

High Availablility

High Availability (with PostgreSQL database)

(Feature available only in Premium and Enterprise Editions. Procedure applicable only for builds 6800 and later)

In mission-critical environments, one of the crucial requirements is to provide un-interrupted access to passwords. PMP provides the 'High Availability' feature just to ensure this.

How does High Availability work?

- There will be redundant PMP server and database instances
- One instance will be the Primary providing read/write access to the users. All users will be connected with primary only
- The other instance will act as Secondary/Standby
- At any point of time data in both Primary and Secondary will be in sync with each other. The data replication happens through a secure, encrypted channel
- When Primary server goes down, the Secondary will offer emergency access to the users, until the fully-functional primary server is brought back to service. The changes made in the database in the intervening period will be automatically synchronized upon connection restoration

Example Scenarios

Scenario 1 - Primary & Secondary in different geographical locations and WAN Link failure happens between the locations

Assume that the Primary Server is in one geographical location 'A' and Secondary is deployed in another location 'B'. The users in both the locations will be connected to the Primary and will be carrying out password management activities. At any point of time data in both Primary and Secondary will be sync with each other. Assume there happens loss of network connectivity between the two locations. In such a scenario, users in location 'A' will continue to remain connected with the primary and will be doing all operations. Users in location 'B' will be able to get emergency access to the passwords from Secondary. Once the network between the two locations is up again, data in both the locations will be synchronized.

Scenario 2 - Primary & Secondary within the same network & Primary goes down

In case, the Primary crashes or goes down, the users in location 'A' & 'B' can rely upon the emergency access to the passwords from the Secondary.

How to set up High Availability?

Setting up high availability in PMP consists of the following four simple steps:

Step 1: Primary & Secondary Setup

You can use your current PMP installation as primary server and install another instance of PMP as secondary server in a separate workstation. To install PMP as secondary, during installation process, you need to choose the option "Configure this server as High availability secondary server". After installation, the PMP Secondary server should not be started.

Step 2: Create Data Replication Pack for High Availability in Primary

1. Stop Primary and Secondary Servers, if running. Ensure that the postgres process of PMP is NOT running
2. Open a command prompt and navigate to <PMP_Primary_Installation_Folder>/bin directory
3. Run the script HASetup.bat <FQDN of PMP Primary Server> <FQDN OF PMP Secondary Server > (Windows) / HASetup.sh <FQDN of PMP Primary Server> <FQDN OF PMP Secondary Server >
   To run this script, you need to pass the fully qualified domain names of the host where PMP primary and secondary servers are installed as commandline arguments. For Example, if the primary server is running at (say) primary-server in the domain zohocorpin.com and thesecondary server is running at (say) secondary-server in the domain zohocorpin.com , you need to execute the above script as follows:
   In Windows: HASetup.bat primary-server.zohocorpin.com secondary-server.zohocorpin.com
   In Linux: sh HASetup.sh primary-server.zohocorpin.com secondary-server.zohocorpin.com
4. This will create a replication package named 'HAPack.zip' under <PMP_Primary_Installation_Folder>/replication folder. This zip contains the database package for secondary
5. Copy the HAPack.zip. This has to be put in the PMP Secondary installation machine as detailed in Step 3 below.

6. Start PMP primary server

Step 3: Put the HA Data Replication Pack in Secondary

Put the HAPack.zip file copied from the PRIMARY Installation (as detailed in the previous step) in to the <PMP_Secondary_Installation_Folder> and unzip it. Take care to extract the files under <PMP_Secondary_Installation_Folder> only. It will overwrite the existing data files.

Step 4: Specify the Location of Encryption Master Key

After extracting HAPack.zip in PMP Secondary Server, navigate to /conf folder, edit manage_key.conf and specify the location of pmp_key.key (encryption master key). PMP requires the pmp_key.key file accessible with its full path when it starts up every time. After a successful start-up, it does not need the key anymore and so the device with the key file can be taken offline.

The High Availability configuration is ready now. To get it up and running, start PMP Secondary server.

Important Note: By default, PMP comes with self-signed SSL certificate. In case, you have overwritten it with a certificate signed by an internal CA (other than the prominent CAs like Verisign (http://verisign.com), Thawte (http://www.thawte.com), RapidSSL (http://www.rapidssl.com) etc) at the secondary installation, you need to carry out the following additional step to install the root certificate in PMP primary server:

- Stop Primary Server, if running
- Open a command prompt and navigate to <PMP_Primary_Installation_Folder>/bin directory
- Copy the secondary server certificate and paste it under <PMP_Primary_Installation_Folder>/bin directory
- From <PMP_Primary_Installation_Folder>/bin directory, execute the following command:
  importCert.bat <name of the server certificate>
- This adds the certificate to the PMP certificate store.
  Now start the PMP Primary server.

Verify High Availability Setup

After carrying out the above steps, you can verify if the High Availability setup is working properly by looking at the message in "Admin General >> High Availability" page of Primary or Secondary server. If the setup is proper, you will see the following:

High Availability Status: Alive

It indicates that high availability is working fine. In case, if the status turns 'Failed', it indicates failure of the setup.

If you have configured TFA

- Whenever you enable TFA or when you change the TFA type (PhoneFactor or RSA SecurID or One-time password) AND if you have configured high availability, you need to restart the PMP secondary server once.

High Availability (with MySQL database)

(Feature available only in Premium and Enterprise Editions. Procedure applicable only for builds 6302 and later. For earlier versions, click here)

In mission-critical environments, one of the crucial requirements is to provide un-interrupted access to passwords. PMP provides the 'High Availability' feature just to ensure this.

PMP has provision to use either MySQL or MS SQL Server as backend. By default, PMP uses the MySQL database, which comes bundled with the product. This document is applicable for configuring High Availability with MySQL. If you are using MS SQL and wish to configure High Availability, refer to this document.

How does High Availability work?

- There will be redundant PMP server and database instances
- One instance will be the Primary providing read/write access to the users. All users will be connected with primary only
- The other instance will act as Secondary
- At any point of time data in both Primary and Secondary will be in sync with each other. PMP leverages MySQL's database replication technique for data synchronization. The data replication happens through a secure, encrypted channel
- When Primary server goes down, the Secondary will offer 'Read Only' access to the users, until the fully-functional primary server is brought back to service. The changes made in the database in the intervening period will be automatically synchronized upon connection restoration

Example Scenarios

Scenario 1 - Primary & Secondary in different geographical locations and WAN Link failure happens between the locations

Assume that the Primary Server is in one geographical location 'A' and Secondary is deployed in another location 'B'. The users in both the locations will be connected to the Primary and will be carrying out password management activities. At any point of time data in both Primary and Secondary will be sync with each other. Assume there happens loss of network connectivity between the two locations. In such a scenario, users in location 'A' will continue to remain connected with the primary and will be doing all operations. Users in location 'B' will be able to get emergency read-only access to the passwords from

Secondary. Once the network between the two locations is up again, data in both the locations will be synchronized.

Scenario 2 - Primary & Secondary within the same network & Primary goes down

In case, the Primary crashes or goes down, the users in location 'A' & 'B' can rely upon the emergency read-only access to the passwords from the Secondary.

What happens to Audit Trails?

In the high availability scenarios mentioned above, audit trails will be recorded as usual. In scenario 1, as long as there is network connectivity between the two locations, the audit trails will be printed by the primary. When users connect to the Secondary, it will print operations such as 'password retrieval', 'login' and 'logout'. When the two locations get back network connectivity, the audit data will be synchronized. In scenario 2, when the primary crashes, the 'password retrieval', 'login' and 'logout' done by the users in secondary will be audited. Other audit records will already be in sync at the Standby.

How to set up High Availability?

Setting up high availability in PMP consists of the following four simple steps:

Step 1: Primary & Secondary Setup

You can use your current PMP installation as primary server and install another instance of PMP as secondary server in a separate workstation. To install PMP as secondary, during installation process, you need to choose the option "Configure this server as High availability secondary server (Read Only)". After installation, the PMP Secondary server should not be started.

Step 2: Create Data Replication Pack for High Availability in Primary

- Stop Primary and Secondary Servers, if running. Ensure that the mysqld process of PMP is NOT running
- Open a command prompt and navigate to <PMP_Primary_Installation_Folder>/bin directory
- Run the script HASetup.bat <FQDN of PMP Primary Server> <FQDN OF PMP Secondary Server > (Windows) / HASetup.sh <FQDN of PMP Primary Server> <FQDN OF PMP Secondary Server >(Linux)

To run this script, you need to pass the fully qualified domain names of the host where PMP primary and secondary servers are installed as commandline arguments. For Example, if the primary server is running at (say) primary-server in the domain zohocorpin.com and the secondary server is running at (say) secondary-server in the domain zohocorpin.com, you need to execute the above script as follows:

In Windows: HASetup.bat primary-server.zohocorpin.com secondary-server.zohocorpin.com

In Linux: sh HASetup.sh primary-server.zohocorpin.com secondary-server.zohocorpin.com

- This will create a replication package named 'HAPack.zip' under <PMP_Primary_Installation_Folder>/replication folder. This zip contains the database package for secondary
- Copy the HAPack.zip. This has to be put in the PMP Secondary installation machine as detailed in Step 3 below.

Step 3: Put the HA Data Replication Pack in Secondary

Put the HAPack.zip file copied from the PRIMARY Installation (as detailed in the previous step) in to the <PMP_Secondary_Installation_Folder> and unzip it. Take care to extract the files under <PMP_Secondary_Installation_Folder> only. It will overwrite the existing data files.

Step 4: Specify the Location of Encryption Master Key

After extracting HAPack.zip in PMP Secondary Server, navigate to <PMP_Secondary_Installation_Folder>/conf folder, edit manage_key.conf and specify the location of pmp_key.key (encryption master key). PMP requires the pmp_key.key file accessible with its full path when it starts up every time. After a successful start-up, it does not need the key anymore and so the device with the key file can be taken offline.

The High Availability configuration is ready now. To get it up and running, start PMP Secondary server.

Verify High Availability setup

After carrying out the above steps, you can verify if the High Availability setup is working properly by looking at the message in "Admin >> General >> High Availability" page of Primary server. If the setup is proper, you will see the following:

High Availability Status: Alive

Replication Status: Alive

If both the above messages show "Alive", it indicates that high availability is working fine. In case, if the status turns 'Failed', it indicates failure of the setup.

What does 'High Availability Status' Indicate (Alive/Failed)?

Constant replication of data between Primary and Standby server is the technology underlying high availability. The status 'Alive' indicates perfect data replication and data synchronization. If there happens any disruption like network problems between Primary and Standby (in turn between the databases), the status will get changed to 'Failed'.
This may happen when there is no communication/connection between the database of primary server and that of the standby server. When the connection gets reestablished, data synchronization will happen and both databases will be in sync with each other. During the intervening period, those who have connected to the primary and standby will not face any disruption in service.

In short, this status is only an indication of the connection/communication between databases and does not warrant any troubleshooting.

What does 'Replication Status' Indicate (Alive/Failed)?

As mentioned above, high availability leverages the MySQL replication feature. The database of Primary server acts as the Master and the one with Standby acts as the 'Slave'. When the data gets replicated properly, the status will be 'Alive'. In case, there happens any error in updating the data or query failure, the replication status become 'Failed'.
Once the status becomes failed, PMP High Availability setup also breaks down. That means, you will have to configure high availability setup all over again.

If you find the status marked as 'Failed' even after re-configuring High Availability, you may have to contact PMP support with the following log files:

PMP In Windows: <PMP Installation Folder>/mysql/data/<hostname>.err file

PMP In Linux: <PMP Installation Folder>/mysql/data/tmp/ .out file

Alerting Mechanism for Status Failure

Since the above two conditions assume importance in high availability setup, it is important to receive real-time alerts when the status turns Alive to Failed and vice-versa. To configure alerts, go to Audit >> Resource Audit >> Configure User Audit >> General Operations and select the mode of alert (email/SNMP trap/Syslog message) for the events 'High Availability Alive' and 'High Availability Failed'.

Note 1 : In case, the Primary Server crashes, when carrying out disaster recovery, please ensure the following:

- Go to the <PMP_Home>/mysql/data of secondary server and copy the files ibdata1, passtrix
- Install another instance of PMP afresh (same version as that of the PMP secondary from which you copied the above files)
- In the new installation, go to <PMP_Home>/mysql/data and overwrite the ibdata1, passtrix files
- Start the new PMP installation

Note 2:

- After configuring high availability, if you change the port of the Primary PMP server, the high availability setup will not work. It has to be re-configured with suitable changes.

Note 3:

If you have configured TFA

- Whenever you enable TFA or when you change the TFA type (PhoneFactor or RSA SecurID or One-time password) AND if you have configured high availability, you need to restart the PMP secondary server once.

High Availability (with MS SQL server)

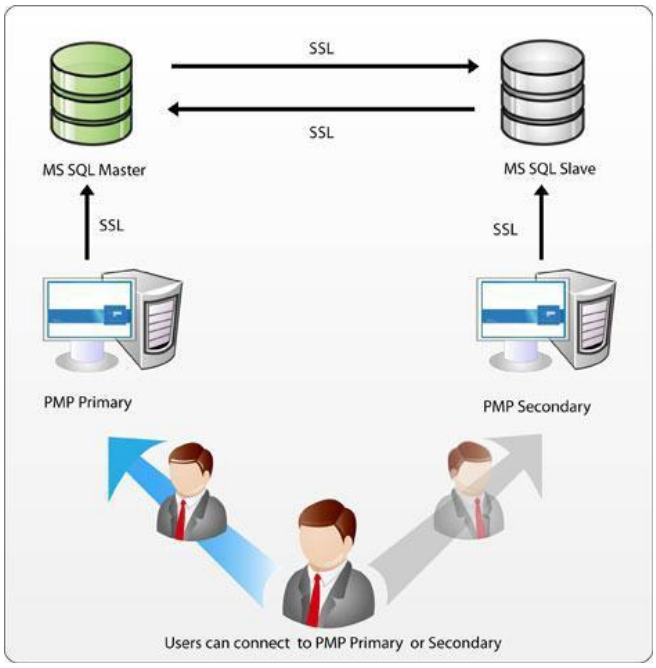
(Feature available only in Enterprise Edition. Procedure applicable only for builds 6400 and later)

In mission-critical environments, one of the crucial requirements is to provide un-interrupted access to passwords. PMP provides the 'High Availability' feature just to ensure this.

How does High Availability work?

- There will be redundant PMP server and database instances
- One PMP instance will be the Primary providing read/write access to the users. All users will be connected with primary only
- The other instance will act as Secondary
- At any point of time data in both Primary and Secondary will be in sync with each other. PMP leverages SQL server's replication technique for data synchronization. The data replication happens through a secure, encrypted channel
- When Primary server goes down, the Secondary will offer 'Read/Write' access to the users (except password reset), until the fully-functional primary server is brought back to service. The changes made in the database in the intervening period will be automatically synchronized upon connection restoration
- At any point, users can connect to Primary or Secondary

High Availability Architecture



Example Scenarios

Scenario 1 - Primary & Secondary in different geographical locations and WAN Link failure happens between the locations

Assume that the Primary Server is in one geographical location 'A' and Secondary is deployed in another location 'B'. The users in both the locations will be connected to the Primary and will be carrying out password management activities. At any point of time data in both Primary and Secondary will be sync with each other. Assume there happens loss of network connectivity between the two locations. In such a scenario, users in location 'A' will continue to remain connected with the primary and will be doing all operations. Users in location 'B' will be able to get emergency read/write access to the passwords from Secondary (except password reset actions). Once the network between the two locations is up again, data in both the locations will be synchronized.

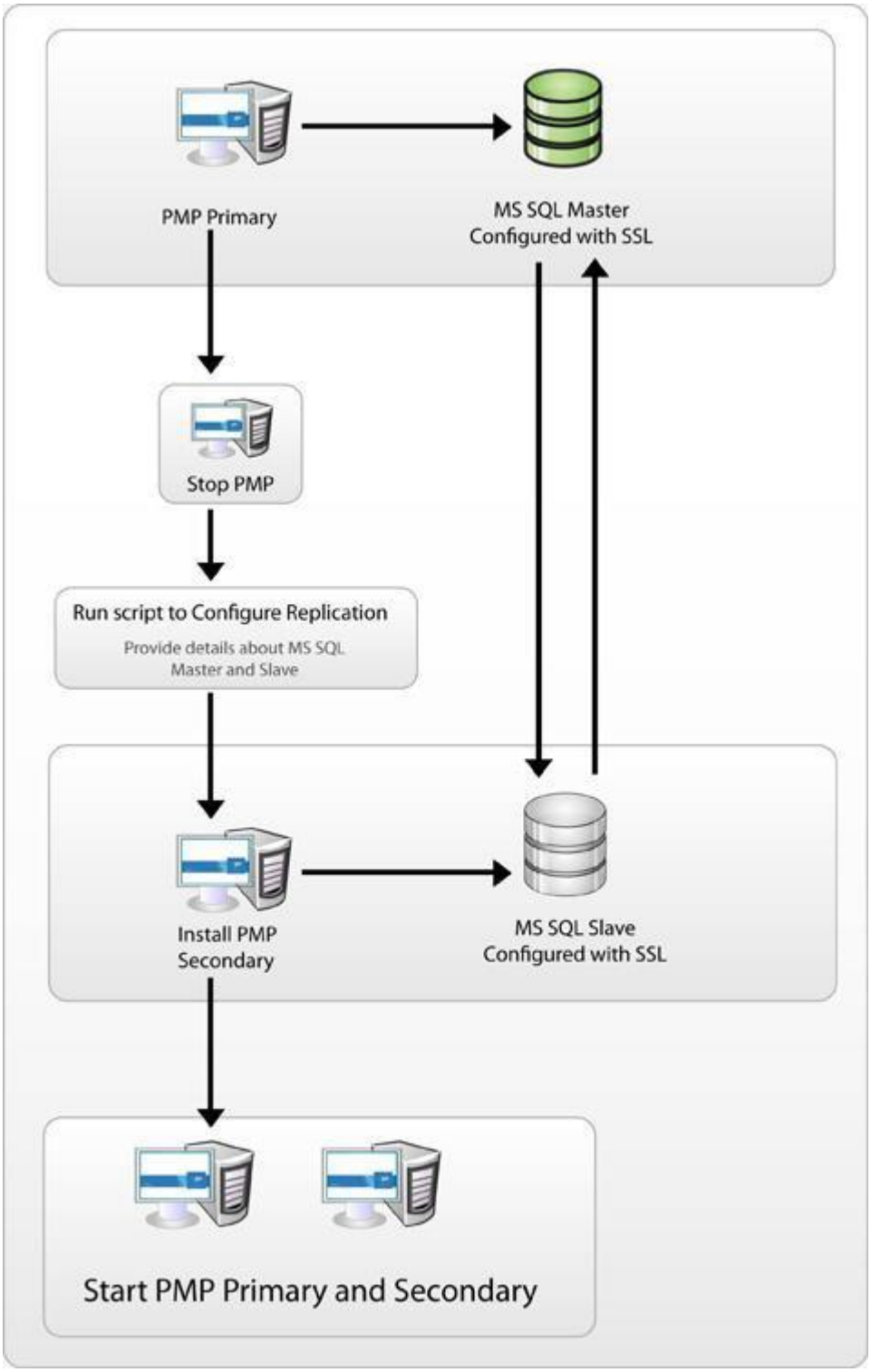
Scenario 2 - Primary & Secondary within the same network & Primary goes down

In case, the Primary crashes or goes down, the users in location 'A' & 'B' can rely upon the emergency access to the passwords from the Secondary (except password reset actions).

What happens to Audit Trails?

In the high availability scenarios mentioned above, audit trails will be recorded as usual. In scenario 1, as long as there is network connectivity between the two locations, the audit trails will be printed by the primary. When users connect to the Secondary, it will print operations such as 'password retrieval', 'login' and 'logout'. When the two locations get back network connectivity, the audit data will be synchronized. In scenario 2, when the primary crashes, the 'password retrieval', 'login' and 'logout' done by the users in secondary will be audited. Other audit records will already be in sync at the Standby.

How to set up High Availability?



Step 1:

- Stop primary server, if running

Step 2:

- The MS SQL server, which is used by the PMP primary server, will act as the Master database. You should now specify another instance of MSSQL as slave database. Then, you need to import the SSL certificate of MS SQL server slave database into PMP Primary server. Before proceeding with this step, ensure that the MS SQL slave server is also configured with SSL. You can do this by carrying out Steps 1, 2, 3 in this document.

To import the SSL certificate of slave SQL server into PMP Primary:

- Navigate to <Password Manager Pro Primary Installation Folder>/bin directory and execute the command importCert.bat <slavecert.cer >

Step 3:

- Navigate to <Password Manager Pro Primary Installation Folder>/conf directory, open the file masterkey.key and copy the SQL Master Key. You will use this in the next step. (In case, you have moved this key to a secure location as recommended while integration SQL server, keep the key ready for use in the next step).

Step 4:

You need to configure MS SQL server replication between master and slave MS SQL databases.

- Navigate to <Password Manager Pro Primary Installation Folder>/bin directory and execute the command ConfigureReplication.bat (in Windows) or sh ConfigureReplication.sh (Linux)
- Specify the details about Master and Slave databases and other details as required

Under Master Database details, provide the following details:

1. Master Host Name:The name or the IP address of the machine where MS SQL server is installed.
2. Port: The port number in which PMP must connect with the SQL server. Default is 1433. Since PMP connects to SQL server only in SSL mode, it is recommended that you create a dedicated database instance running in a specific port for PMP.
3. User Name and Password: Specify the user name and password with which PMP needs to connect to the database. (You need to specify the username having SQL role as sysadmin. PMP does not store this username and password anywhere. It is just used for carrying out some queries while configuring replication between MS SQL master and slave servers).
   Here, you have the option to use even your Windows login credentials, if you are connecting to the database from Windows. In this case, you need to enter the username as <domain-name>\<username>
4. Master Database Name: Name of the PMP database.
5. Master Key: Paste the master key copies in Step 3 above.

Under Slave Database details, provide the following details:

1. Slave Host Name: The name or the IP address of the machine where MS SQL server is installed.
2. Port: The port number in which PMP must connect with the database. Default is 1433.
3. User Name and Password: Specify the user name and password with which PMP needs to connect to the database. (You need to specify the username having SQL role as sysadmin. PMP does not store this username and password anywhere. It is just used for carrying out some queries while configuring replication between MS SQL master and slave servers).
   Here, you have the option to use even your Windows login credentials, if you are connecting to the database from Windows. In this case, you need to enter the username as <domain-name>\<username>
4. Slave Database Name: Name of the PMP database. Default is "pmpstandby". (If you have chosen the option 'Custom' for "Encryption Key"while configuring ChangeDB.bat for Primary server, you need to create a new database for slave, create Master Key, create Certificate and Create the Symmetric Key using AES 256 encryption. You need to mention the slave database name here.)
5. Click "Test & Configure" to complete replication. This process will take about 30 minutes or more.

Step 5:

Start the primary server

Step 6:

Install another instance of PMP as secondary server in a separate workstation. To install PMP as secondary, during installation process, you need to choose the option "Configure this server as High availability secondary server (Read Only)". After installation, the PMP Secondary server should not be started.

Step 7:

After installing the PMP secondary server, you need to change it to run with MS SQL by carrying out the following:

Execute ChangeDB.bat

Now, you need to provide the details about the SQL server to PMP by editing the file <Password Manager Pro Standby Installation Folder>/bin ChangeDB.bat (Windows) or <Password Manager Pro Standby Installation Folder>/bin sh ChangeDB.sh (Linux)

Select SQL Server and enter other values

1. Host Name of Slave Database: The name or the IP address of the machine where MS SQL server is installed.
2. Port: The port number in which PMP must connect with the database. Default is 1433.
3. Database Name: Name of the Slave database. Here, take care to specify the name of the slave database exactly as done in Step 4 above.
4. Authentication: The way in which you would like to connect to the SQL server. If you are connecting to the SQL server from Windows, you have the option to make use of the Windows Single Sign On facility provided PMP service is running with a service account, which has the privilege to connect to SQL server. In that case, choose the option "Windows". Otherwise, select the option "SQL". It is recommended to choose the option 'Windows' as the username and password used for authentication are not stored anywhere.
5. User Name and Password: If you have selected the option "SQL", specify the user name and password with which PMP needs to connect to the database. The username and password entered here will be stored in PMP. So, you need to take care of hardening the host.

Here, you have the option to use even your Windows login credentials, if you are connecting to the database from Windows. In this case, you need to enter the username as <domain-name>\<username>

6. Encryption Key: The key with which your data is to be encrypted and stored in the SQL server. You may either leave it "Default" making PMP to generate a key. If you have configured Master database with custom key, you need to choose 'Custom' here also.
7. If you have selected the option "Custom:" After doing the above, you need to provide certificate name and symmetric key name in the GUI as mentioned in Master database
8. Click Test and then Save.

Step 8:

To carry PMP license, custom icons and rebranding settings, if any, from Primary to Secondary, go to \replication directory and copySQLServerHAPack.zip. Put the this zip file copied from the PRIMARY Installation to the <PMP_Secondary_Installation_Folder>and unzip it. Take care to extract the files under <PMP_Secondary_Installation_Folder> only. It will overwrite the existing files. This SHOULD NOT be unzipped under <PMP_Secondary_Installation_Folder>/SQLServerHAPack directory.

Step 9:

After extracting SQLServerHAPack.zip in PMP Secondary Server, navigate to <PMP_Secondary_Installation_Folder>/conf folder, edit manage_key.confand specify the location of pmp_key.key (encryption master key). Then, start PMP Secondary Server. PMP requires the pmp_key.key file accessible with its full path when it starts up every time. After a successful start up, it does not need the key anymore and so the device with the key file can be taken offline.

Verify High Availability setup

After carrying out the above steps, you can verify if the High Availability setup is working properly by looking at the message in "Admin >> General >> High Availability" page of Primary or Secondary server. If the setup is proper, you will see the following:

High Availability Status: Alive

It indicates that high availability is working fine. In case, if the status turns 'Failed', it indicates failure of the setup.

Database Backup (for PMP with MySQL)

(Procedure applicable only for builds 6302 and later. For earlier versions, click here)

Data stored in PMP database are of critical importance and in any production environment, there would be constant requirements for backing up the data for reference purposes or for disaster recovery. To achieve this, PMP provides two features:

1. Live Backup of PMP database
2. Scheduled Backup

Live Backup

Whenever there happens an addition or modification of the entries in the PMP database, the data gets immediately backedup. PMP achieves this live backup by leveraging the database replication feature offered by MySQL.

A live 'slave' database could be configured in a remote location and it will get instantaneously updated whenever the 'master' database running with PMP undergoes a change. At any point of time, the data in both the databases will be in synchronization with each other. In the unlikely event of any disaster to the primary database, you can rely on the slave database and recover the data.

To enable Live Backup,

Prerequisite

After installation, the PMP server should have been started and stopped at least once. If PMP server is already running, stop it before proceeding further. Ensure that the mysqld process of PMP is NOT running

Step 1: Setup master and slave databases

- Go to <PMP_Installation_Folder>/bin directory and run the script replicationPack.bat <FQDN of PMP Primary Server> <FQDN OF Remote Host where slave database is running> (in Windows) / replicationPack.sh <FQDN of PMP Primary Server><FQDN OF Remote Host where slave database is running>(in Linux)
  To run this script, you need to pass the fully qualified domain names of (1) the host where PMP primary server is running and (2) the host where slave

database is to be put, as commandline arguments. For Example, if the primary server is running at say testserver in the domainzohocorpin.com and the slave database is to be put in the host (say) testserver1 in the domain zohocorpin.com , you need to execute the above script as follows:
In Windows
replicationPack.bat testserver.zohocorpin.com testserver1.zohocorpin.com
In Linux
sh replicationPack.sh testserver.zohocorpin.com testserver1.zohocorpin.com

- This will create the data replication package "LiveBackup.zip" under <PMP_Home>/replication folder.
- Move this zip file from <PMP_Home>/replication folder to the remote host where you wish to keep the slave database for live backup
- Unzip the zip file in the remote host
- The slave database is now setup
- The database that is bundled with PMP acts as the master database. No separate setup is required for that

Step 2: Start PMP server and slave database

- Now, start the PMP server. This in turn starts the master database.
- Go to the remote machine, open a command prompt with administrator privilege and navigate to the /bin folder and run the script startSlaveDB.bat (Windows) / startSlaveDB.sh (Linux). This will start the slave database.

Verify Live Backup Setup

After carrying out the above steps, you can verify if the Live Backup setup is working properly by looking at the message in "Admin >> General >> Database Backup" page. If the setup is proper, you will see the following:
Connection Status: Alive and Live Backup is in progress now
Slave database is running in host: <Host Name>
Recovering data from slave when master database crashes

In the rare event of master database crash, you can recover data from the slave database.
To recover the data,

- In the remote machine where slave DB is running, navigate to <MySQL>/data folder and create a zip of the following:
  - "passtrix" directory
  - "ibdata1" file
- Copy the zip created as above

- Go to the machine where PMP was running
- Get a fresh PMP installation in the machine where the master database was running
- Navigate to /mysql/data folder and unzip the zip created from the slave database. Once you do this, the data is safely recovered in the new PMP version
- After extracting the zip, navigate to <PMP_Installation_Folder>/conf folder, edit manage_key.conf and specify the location of pmp_key.key(encryption master key). PMP requires the pmp_key.key file accessible with its full path when it starts up every time. After a successful start-up, it does not need the key anymore and so the device with the key file can be taken offline.
- Now, start the PMP server

Note: Once you recover the data from the slave and give life to the master database, the slave database will no longer be valid. Just delete the mysql folder in the remote machine. If you want to have the Live Backup enabled again, you need to follow the steps once again.

Scheduled Backup

You can schedule database backup to be executed at any specific point of time.

To schedule database backup,

- Go to "Admin" tab
- Click "Database Backup" icon under "General" section

In the UI that opens up,

- Select the schedule option - day, weekly or monthly.

To schedule database backup,

1. If your requirement is to backup the database contents in specific day intervals - say, once in three days, this option would come in handy. You can choose any interval between 1 and 28 and also specify the time at which backup has to be taken.
2. To enable this option, click the radio button "Day"
3. Select the day interval
4. Select the time at which backup has to be taken
5. Backed up data are stored as a .zip file under <PMP_Home>/backUp directory by default. If you want, you can specify the destination directory where you wish to store the backedup contents.

6. Every time backup is executed, one backup file will be created. You can specify the maximum number of such backup files to be kept in this directory. For example, if you choose "10" in the drop-down against the field "Maintain latest --- backups only", only the latest 10 backup files would be kept under this directory
7. Click "Save". The required backup schedule is created.

- Where does the backup data get stored? Is it encrypted?
  All sensitive data in the backup file are stored in encrypted form in a .zip file under <PMP_Home/backUp> directory or under the directory specified by you. It is recommended that you backup this file in your secure, secondary storage for disaster recovery.

- What is the best option for database backup schedule?
  Database backup operation is both time and resource consuming. Hence, it is recommended to schedule it to run during off-peak traffic timings. While the operation is in progress, no configuration change could be performed in PMP.

- Can I replicate the data to another server and have the permissions stay intact?
  Yes. PMP application is stateless and all the data are stored in the database and just replicating the database against a fresh installation of the application gets you all the data intact.

To schedule backup on a specific day every week,

1. If your requirement is to backup the database contents on a specific day every week - say, on Mondays, this option would come in handy. You can choose any day from Sunday to Saturday and also specify the time at which backup has to be taken. To enable this option,
2. click the radio button "Weekly"
3. select the day of the week
4. select the time at which backup has to be taken
5. Backed up data are stored as a .zip file under <PMP_Home>/backUp directory by default. If you want, you can specify the destination directory where you wish to store the backedup contents.
6. Every time backup is executed, one backup file will be created. You can specify the maximum number of such backup files to be kept in this directory. For example, if you choose "10" in the drop-down against the field "Maintain latest --- backups only", only the latest 10 backup files would be kept under this directory
7. Click "Save". The required backup schedule is created

To schedule backup on a specific day every month,

1. If your requirement is to backup the database contents on a specific date every month - say, on 13th, this option would come in handy. You can choose any date from 1st to 31st and also specify the time at which backup has to be taken. To enable this option,
2. Click the radio button "Monthly"
3. Select the date of the month
4. Select the time at which backup has to be taken
5. Backed up data are stored as a .zip file under <PMP_Home>/backUp directory by default. If you want, you can specify the destination directory where you wish to store the backedup contents.
6. Everytime backup is executed, one backup file will be created. You can specify the maximum number of such backup files to be kept in this directory. For example, if you choose "10" in the drop-down against the field "Maintain latest --- backups only", only the latest 10 backup files would be kept under this directory
7. Click "Save". The required backup schedule is created

Database Backup (for PMP with MS SQL Server)

(Procedure applicable only for builds 6400 and later)

Data stored in PMP database are of critical importance and in any production environment, there would be constant requirements for backing up the data for reference purposes or for disaster recovery.

A task could be scheduled to backup the database contents periodically. The backup will be stored as a .zip file by default in the host where SQL server is running. All sensitive data will remain encrypted in that file.
Scheduled Backup

You can schedule database backup to be executed at any specific point of time.

To schedule database backup,

- Go to "Admin" tab
- Click "Database Backup" icon under "General" section In the UI that opens up,
- Select the schedule option - day, weekly or monthly
- Select the time at which backup has to be taken
- The backup will be stored as a .bak file by default in the <MSSQL_installation_folder>\Backup directory in the host where SQL server is running. All sensitive data will remain encrypted in that file. It is recommended that you backup this file to a secure, secondary storage.
- The backup file will have the file name structure as pmpbackup_pmpversion_YYMMDD-time.bak
- Click "Save". The required backup schedule is created

Instant Backup

You can take one-time backup anytime on-demand by clicking the button "Backup Now" available in the GUI explained above.

Disaster Recovery

In the event of a disaster or data loss, you can restore the backed up data to the PMP database. To restore the data, PMP provides scripts.

Disaster Recovery Steps for PMP with PostgreSQL (OR) MySQL as Backend Database

Restoring the data

Important Note:

1. Stop PMP server before trying to restore data. If restoration is done while the server is running, it may lead to data corruption
2. Data backed up from PMP running on Windows can be restored only in Windows

For Windows

- Navigate to <PMP_Installation_Directory>/bin folder
- Execute the script "restoreDB.bat <backup file name>" (enter your backup file name in .zip format)
- The backed up contents would be restored to the PMP DB
- Navigate to <PMP_Installation_Folder>/conf folder, edit manage_key.conf and specify the location of pmp_key.key (AES 256 encryption master key). PMP requires the pmp_key.key file accessible with its full path when it starts up every time. After a successful start-up, it does not need the key anymore and so the device with the key file can be taken offline.

For Linux

- Navigate to <PMP_Installation_Directory>/bin folder
- Execute the script "sh restoreDB.sh <backup file name>" (enter your backup file name in .zip format)
- The backed up contents would be restored to the PMP DB
- Navigate to <PMP_Installation_Folder>/conf folder, edit manage_key.conf and specify the location of pmp_key.key (AES 256 encryption master key). PMP requires the pmp_key.key file accessible with its full path when it starts up every time. After a successful start-up, it does not need the key anymore and so the device with the key file can be taken offline.

Note:

If you are using PostgreSQL as backend database:

PMP database is secured through a password, which is auto-generated and unique for every installation. The database password can be stored securely in the PMP installation itself. However, for additional security, there is an option to store it at some other secure location accessible to the PMP server. While backup, if you have not selected the option "Securely Store database password in PMP backup data", the database password will not be available with the backup copy. You need to manually copy the database_params.conf file available under the <PMP-Installation-Folder>/conf directory.

Disaster Recovery Steps for PMP with MS SQL Server

Prerequisite

PMP uses SQL server's encryption mechanism to encrypt the data. The encryption master key will be stored under <Password Manager Pro Installation Folder>/conf directory with the name masterkey.key. For security reasons, during installation of MS SQL, we recommend moving the encryption key from the default location to a secure location. For performing disaster recovery, the master key is required.

Step 1

Install another instance of PMP. Follow the steps for using MS SQL server as the backend (specifying a new instance of MS SQL server where the backup has to be restored). The new instance of MS SQL server should have been configured with SSL. You can do this by carrying out Steps 1, 2, 3 in this document.

Step 2

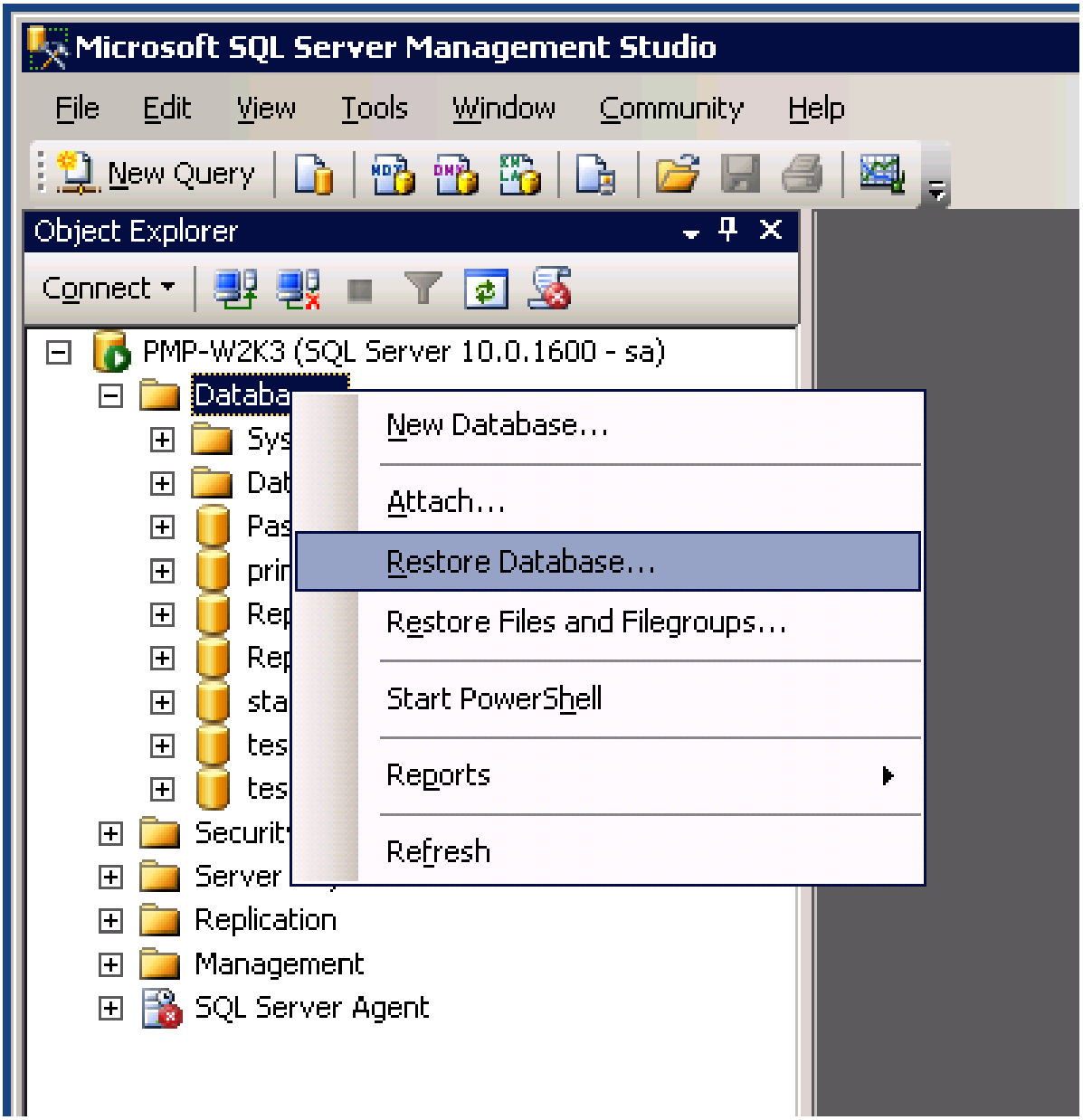
Copy the PMP backup file from the SQL server. By default, it will be present under /Backup folder and have the name something likepmpbackup_pmpversion_backupdate-time.bak (For example, pmpbackup_6400_110721-1159.bak)

Step 3

Launch "Microsoft SQL Server Management Studio" (in the machine where the backedup data are to be restored - that is, another instance of SQL server) and connect to the Database Engine.

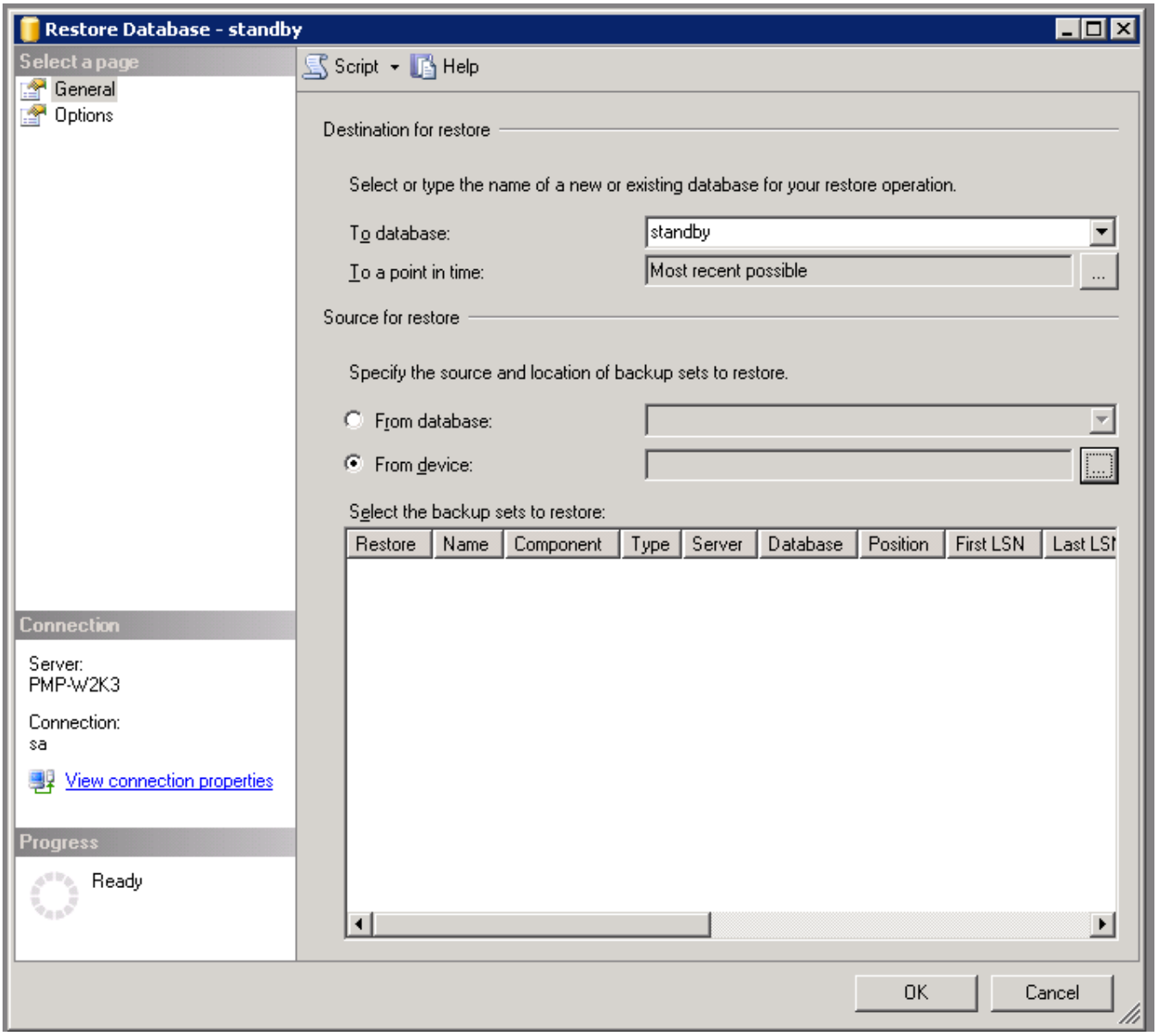
Step 4

Right-click on "Databases" and the click "Restore Database" from the displayed menu.



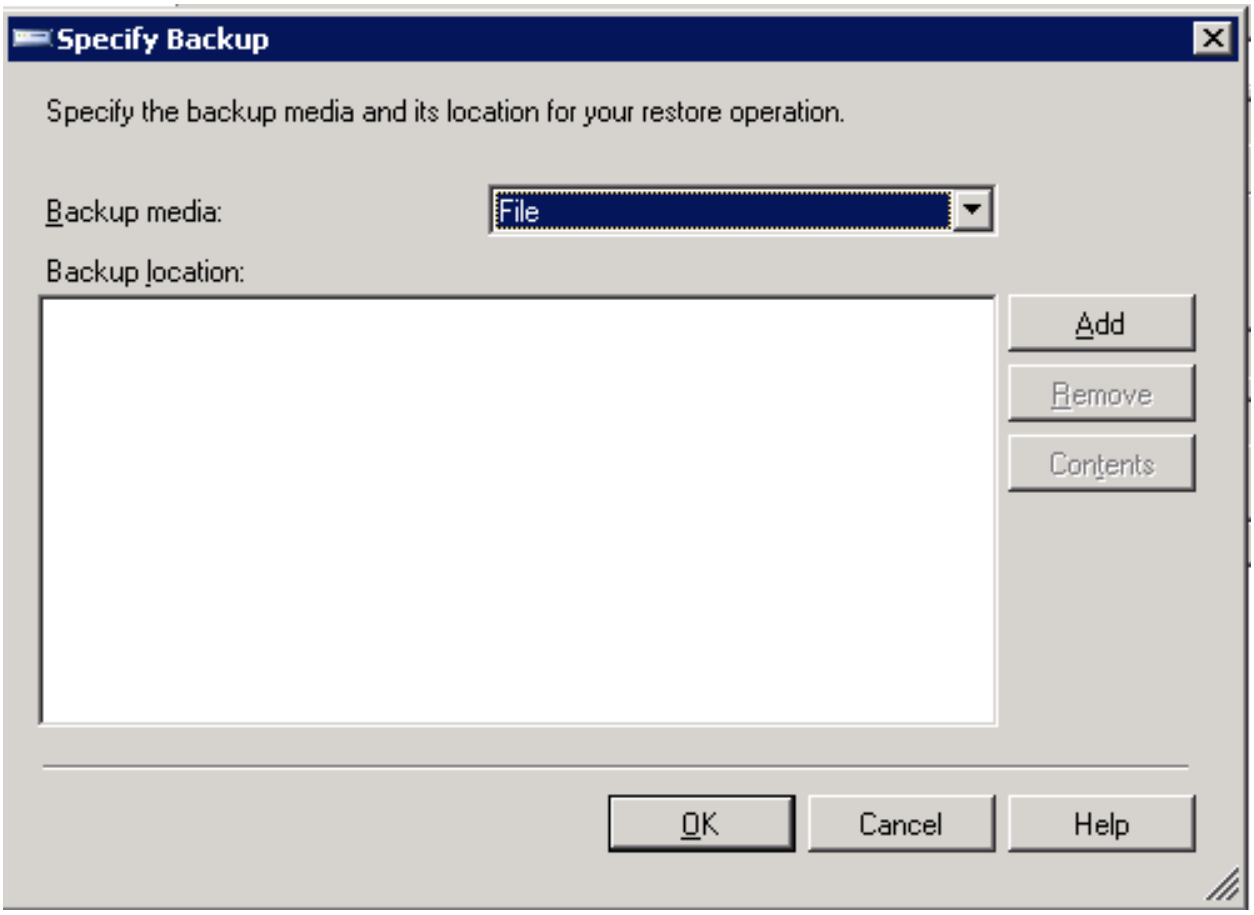
Step 5

In the "Restore Database" window, choose the option "From device" and click [...] button to browse the PMP backup file



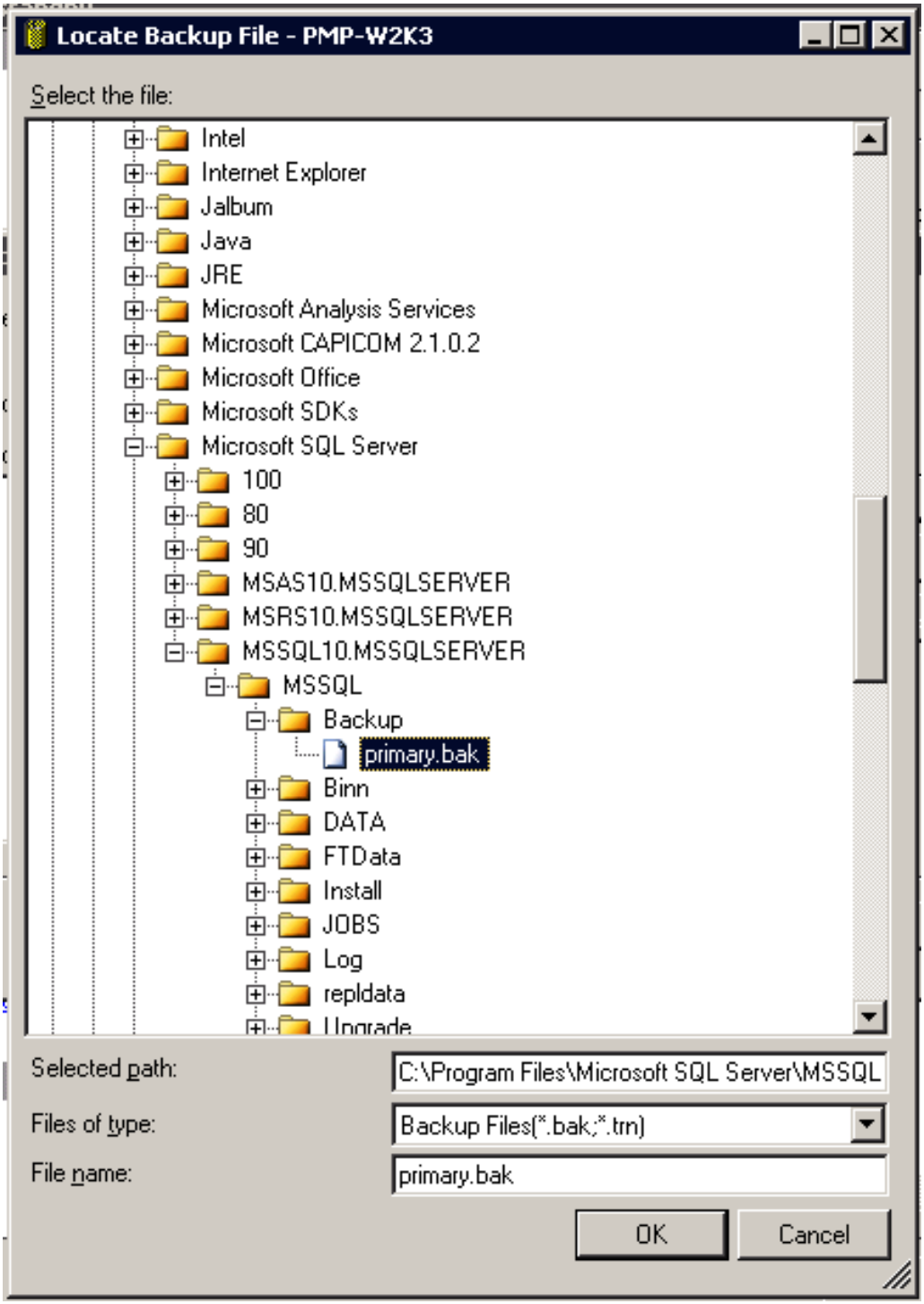
Step 6

In the "Specify Backup" window that opens up, choose the option "File" as the Backup media and click "Add".



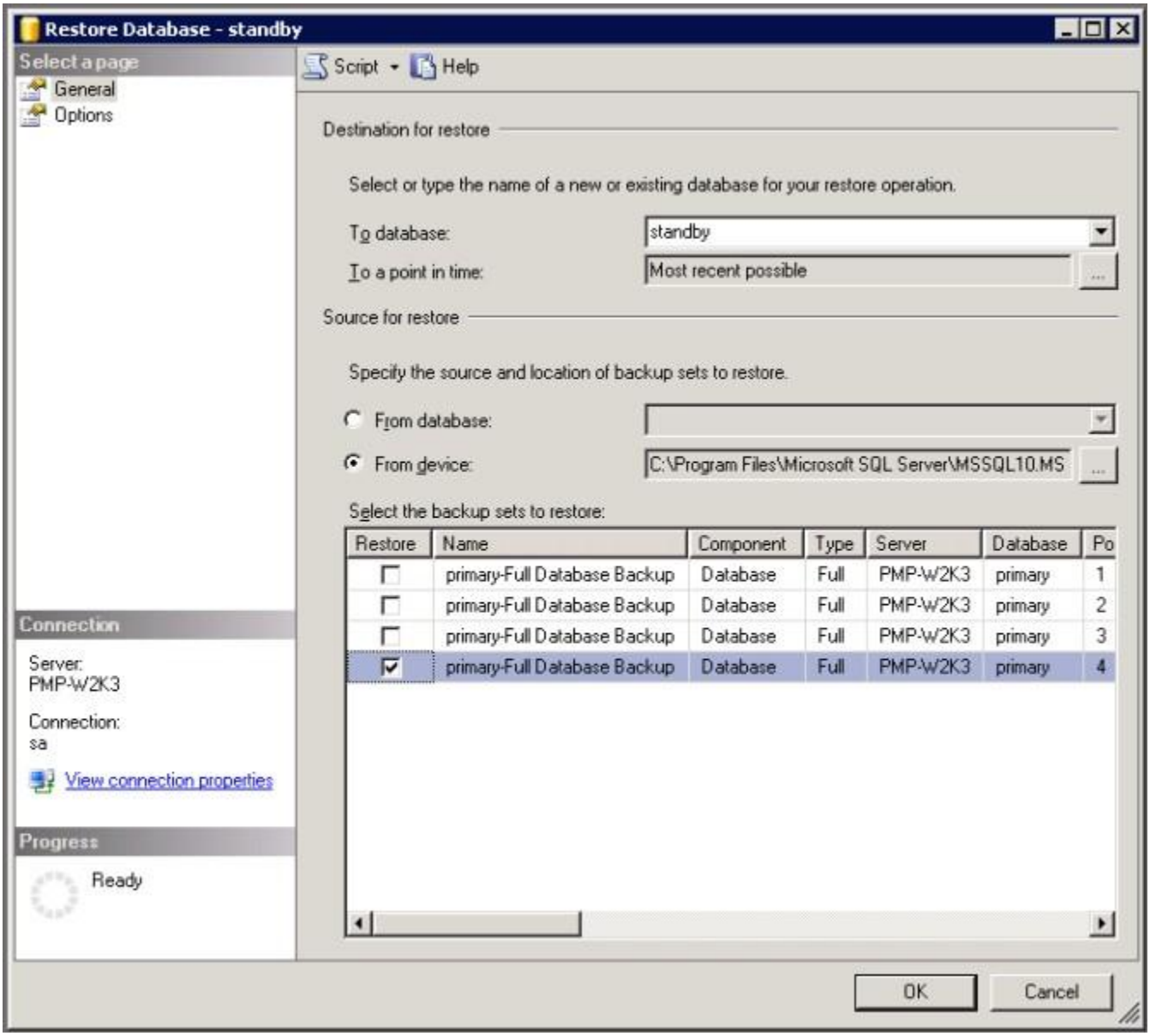
Step 7

In the "Locate Backup File" window, select the PMP backup file and click "OK".



Step 8

- Now, in the "Restore Database" window, select the database where the backup is to be restored and specify it in the "To database" field.
- Under "Select the backup sets to restore", select the required "Restore column".
- Click OK to start the restoring the database.
- Upon completion of the restoration, a status window pops-up.



Step 9

Now, you need to restore the Master Key. As mentioned in the prerequisite section above, by default, the encryption master key will be stored under<Password Manager Pro Installation Folder>/conf directory in the file named masterkey.key. For security reasons, if you have moved the file to some other secure location, identify that. Open the masterkey.key file and copy the password.

Step 10

Connect to the SQL server in which you have restored the PMP backup file.
Open "Microsoft SQL Server Management Studio" and connect the database engine.
Execute the following queries:
use write_the_name_of the restored_database;
OPEN MASTER KEY DECRYPTION BY PASSWORD = 'type_the_master_key_password';
alter master key regenerate with encryption by password =
'type_the_master_key_password';
Example:
use passtrix;
OPEN MASTER KEY DECRYPTION BY PASSWORD = 'secret';
alter master key regenerate with encryption by password = 'secret';
Execution of the above queries will help decrypt the data.

Step 11

Navigate to <PMP_Installation_Folder>/conf folder, edit manage_key.conf and specify the location of pmp_key.key (encryption master key). PMP requires the pmp_key.key file accessible with its full path when it starts up every time. After a successful start-up, it does not need the key anymore and so the device with the key file can be taken offline.

Session Management

Auto Logon Helper

(Feature available only in Premium and Enterprise Editions)

Automatically Logging in to Remote Systems & Applications

Passwords of remote systems and applications are stored in PMP. Normally, to login to the systems and applications, you need to copy the password from PMP and paste it in the target system. PMP provides an option for automatically logging in to the target systems and applications directly from the PMP web interface eliminating the need for copying and pasting of passwords.

From version 6500 onwards, PMP provides two kinds of Auto Logon Mechanisms :

- Auto Logon Gateway for launching Windows RDP, SSH and Telnet sessions
- Auto Logon Helper Scripts for launching custom programs from the user's browser

How does this auto logon feature work?

Auto Logon Gateway

From version 6500, PMP comes bundled with RDP, SSH and Telnet session gateways. This allows the users to launch remote terminal sessions from their browser that are tunneled through the PMP server. The remote terminal sessions are emulated in the browser screen itself and hence there is no need for installing any plug-in or agent in any end-points. The only requirement is the browser should be HTML 5 compatible (For example IE 9 or above, FF 3.5 or above, Safari 4 or above, Chrome).

As soon as an administrator adds a resource that supports one of these remote terminal session types, the feature becomes available to all users in the system who have access to that resource, with no further configuration anywhere. In addition, the 'Auto Logon' sub tab under the 'Home' tab will allow users to easily locate remote accounts and launch a session with a single click.

The entries in the 'Auto Logon' page with the names 'Windows Remote Desktop', 'SSH' and 'Telnet' belong to this type and come out-of-the-box. No additional configuration or management is required for these types other than modifying their names for your convenience. Resource level configuration like port to connect for SSH (if different than the

default 22) and logging into a Windows machine using a domain service account can be performed in a specific resource or for a set of resources.

Auto Logon Helper Scripts

This can be enabled by configuring helper scripts which will be invoked by the browser, in the user's machine. The script is nothing but a command specific to the operating system, which the users normally use to connect to the target systems (for exampls telnet, rdp, putty etc). Due to inherent security restrictions in the browsers, users have to download and install browser specific plug-ins one time to be able to invoke operating system commands.

Example 1

Assume you have 10 resources - Windows servers. You have stored the login accounts and passwords of these 10 resources in PMP. You want to directly login to these resources from PMP web-interface. You will connect the PMP web-interface from both Windows and Linux systems. For auto logon, you need to do the following:

Create a 'helper script' by providing the command to establish connection to the target system. The command has to be written specific to the operating system from where the PMP web-interface will be connected. That is, if you would connect the PMP web-interface in Windows, the command has to be Windows specific - enter the command that would normally use to invoke a MSTSC session in Windows. If you would connect the web interface from Linux, enter the command to invoke Remote Desktop (RDP) connection. By doing so, whether you connect the PMP web-interface from Windows or Linux, you will be able to establish the connection automatically.

Example 2

Assume you have 10 resources - Cisco devices and Unix servers. You have stored the login accounts and passwords of these 10 resources in PMP. You want to directly login to these resources from PMP web-interface. You will connect the PMP web-interface from Windows. For auto logon, you need to do the following:

Create a 'helper script' by providing the command to establish connection to the target system. The command has to be written specific to the operating system from where the PMP web-interface will be connected. That is, if you would connect the PMP web-interface in Windows, the command has to be Windows specific - enter the command that would

normally use to invoke a PuTTY session in Windows. Instead of PuTTY, you can also enter the command for TELNET.

PMP will have no control over the command other than invoking it and also does not process the result of the command. The helper script supplied will be stored in the same database as the other information, which provides security as well as backup, if it is configured for the PMP database. The command is invoked with the same privileges as the user account running the browser that is accessing the PMP application.

Difference Between Gateway and Helper Script Methods - When to Use, What?

Description	Auto Logon Gateway	Auto Logon Helper Scripts
Supported for	Windows RDP, SSH and Telnet	No restrictions. Any program can be invoked from the user machine
Requisites	The user's browser should be HTML 5 compatible. No other requisite	Should install browser version specific plug-ins. The program to execute should be available in all machines that the end users will use
When to use	When you are sure that the remote systems support one of Windows RDP, SSH or Telnet	When you are not sure of the type of remote connection, you can configure multiple options and let the users choose
Benefits	Very reliable. Connections are tunneled through the PMP server, so the user needs connectivity only to the PMP server and can still launch remote sessions to multiple end points	No apparent benefit other than the flexibility of multiple options
Security	Extremely secure as the passwords for remote sessions do not even come to the browser. Traffic encryption at every hop is ensured by PMP	Not very secure after the control is transferred to the launched program. Installing browser plug-ins is not a secure practice
PMP Recommendation	Recommended	Not recommended unless you understand the implications and left with no choice

How to set up auto logon?

Configuring Auto Logon Gateway

As mentioned above, PMP comes bundled with RDP, SSH and Telnet session gateways. This allows the users to launch remote terminal sessions from their browser that are tunneled through the PMP server. The remote terminal sessions are emulated in the browser screen itself and hence there is no need for installing any plug-in or agent in any end-points. The only requirement is the browser should be HTML 5 compatible (For example IE 9 or above, FF 3.5 or above, Safari 4 or above, Chrome).

Auto Logon configuration while adding resources

When administrators add a resource that supports one of these remote terminal session types, the configuration for Auto Logon has to be made in Step 3 of the resource addition process.

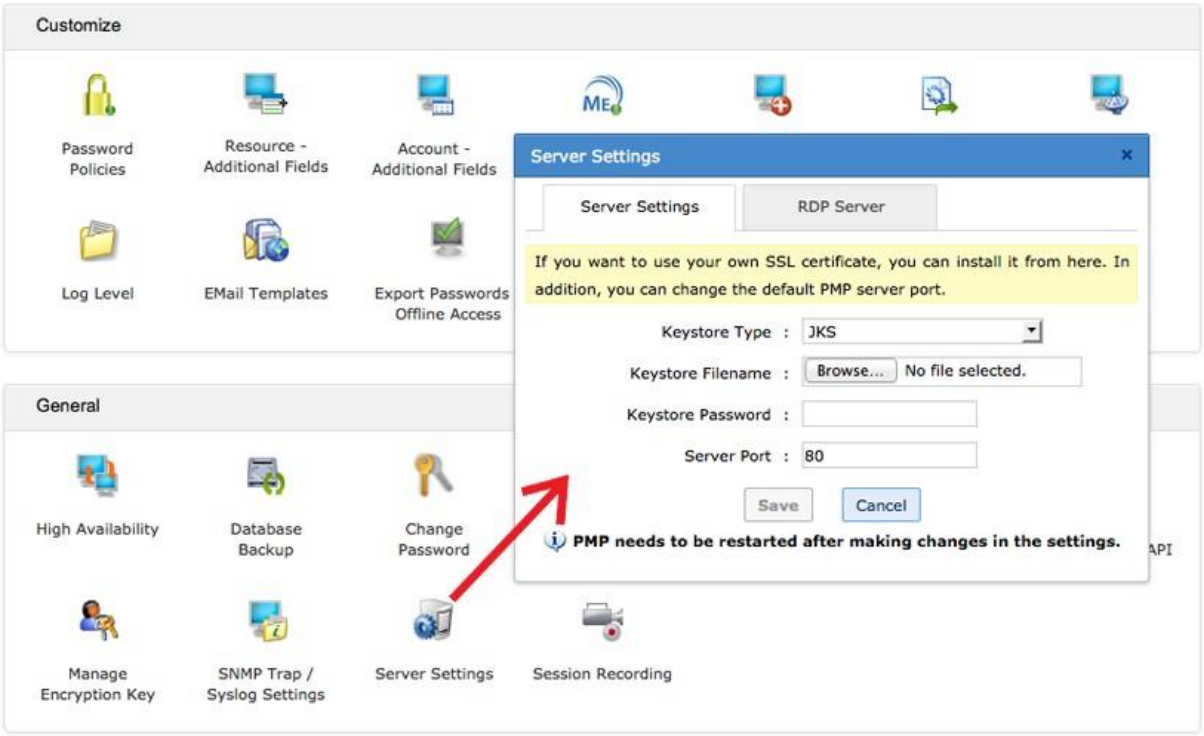
- For logging into a Windows resource, you need to configure the domain account that can be used by users to authenticate a Windows RDP session to this remote host. (You can authenticate with local accounts also. This is just another option).
- To connect through SSH, you need to specify the port to connect, if it is different than the default 22.

Port Requirements

The Windows RDP Auto Logon Gateway listens at port 7273 by default. This is a secure web socket port (wss://) and you should allow traffic to this port from the end user machines for this to work. You can change this port from Admin >> General >> Server Settings >> Remote Desktop Gateway Port.PMP web server (7272 by default) and this gateway should open and listen at different ports.

Important Note: When PMP is installed, it generates a self-signed SSL certificate for the instance which is also used by the Auto Logon Gateway to encrypt the traffic. It is recommended that you apply a CA signed certificate to the PMP instance before opening it out for end users. With a self-signed certificate, connecting to the gateway is not possible unless users explicitly mention the gateway port in the URL, accept the warning and install the self-signed certificate. (For steps to generate unique SSL certificare, refer to this section of our site).

The SSH and Telnet Gateways have no such requirement as they use the same PMP web server port for all communication.



Configuring Auto Logon Script

Step 1: Add 'Helper' Script

- Go to "Admin" >> "Customize" >> and click "Auto Logon Helper"
- In the UI that opens, click the button "Add Helper"

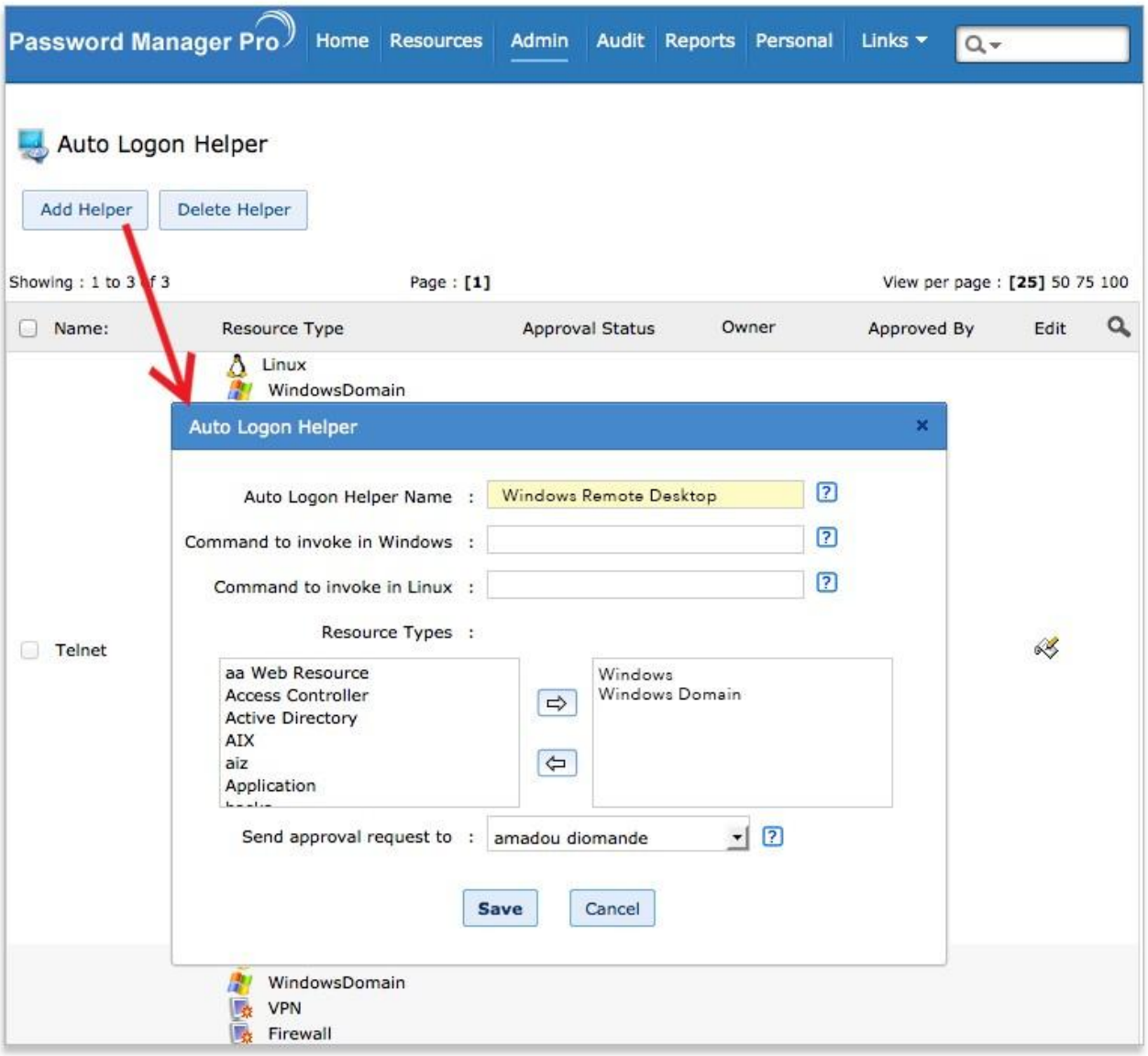
In the UI that pops-up, provide the details as detailed in the steps below.

Steps 2 & 3: Entering 'Name' & Commands for the Helper Script

As mentined above, auto logon can be enabled by configuring helper scripts which will be invoked by the browser, in the user's machine. The script is nothing but a command specific to the operating system, which the users normally use to connect to the target systems (for example telnet, rdp, putty etc). Due to inherent security restrictions in the browsers, users have to download and install browser specific plug-ins one time to be able to invoke operating system commands.

You can configure the individual commands required for Windows and Linux systems respectively and map the relevant target system type. For a particular target system type, there can be more than one method to connect and hence you can map any number of commands to a single target system type.

You need to provide a 'Name' (a label or an alias) for the command, which the users will click against a password to login to the remote system. When there are multiple commands configured for a target system type, all the command names will be listed in a menu for the user to choose.



In addition, if the 'Resource URL' attribute is set for the resource, the menu will also include a label 'Open URL' which will open the URL in a new browser window. If the attribute has

the usual placeholders, they will be substituted in the URL query string appropriately. (Refer to the section below to configure the Resource URL attribute).

The following example will make you understand this step with ease:

Assume that your requirement is to connect to a remote system automatically from PMP by establishing a telnet connection, you need to do the following:

You need to write the command for establishing telnet connection to the target system. The command has to be written specific to the operating system from where the PMP web-interface will be connected. That is, if you would connect the PMP web-interface in Windows, the command has to be Windows specific - enter the command that would normally use to invoke a telnet session in Windows. However, it is advisable to enter the commands for establishing the connection from both Windows and from Linux separately. By doing so, whether you connect the PMP web-interface from Windows or Linux, you will be able to establish the connection automatically.

It is pertinent to take note of the following before creating your commands:

You can use the following place holders in your command string:
%RESOURCE_NAME%
%DNS_NAME%
%ACCOUNT_NAME%
%PASSWORD%

These place holders will be replaced with respective values at the time of invoking of the commands.

Also, the command configured will be invoked as is on the user machines and hence it is recommended to ensure that the PATH environment variable is properly set or the command be located in the same execution path in all the user machines.

Invoking Direct Connection to URLs

If you want to open connection to a URL automatically in a browser window, you can specify the URL for the same through 'Resource URL' field while adding the resource or by editing a resource. You can even specify the user name and password in the URL to directly login to the resource. For security reasons, PMP provides the option for using place holders to avoid the usage of user name, password etc in plain text in the URL. At the time of URL invocation, PMP replaces the respective data for the placeholders and submits the data by

'POST' method. Nowhere during the URL invocation, the password will be visible to the users.

The following four place holders are allowed: %RESOURCE_NAME%, %DNS_NAME%, %ACCOUNT_NAME% and %PASSWORD%
Examples for using the place holders in the URL:

(1) Assume that you have a resource named 'abc' and on typing the resource name in the browser as http://abc you can access an application. In this case, you can enter the resource url with placeholder as shown below:
http://%RESOURCE_NAME%

(2) Assume you have an application running on port 7272 and you can access it through the DNS name of the host where it runs. You can make use of the placeholder and construct the URL as below:
https://%DNS_NAME%:7272

In case, you wish to supply the username and password for the application and directly login to the resource, you can construct the URL as below:

https://%DNS_NAME%:7272/j_security_check?j_username=%ACCOUNT_NAME%&j_password=%PASSWORD%&domainName=LOCAL

In the text field against "Command to invoke in Windows", enter the command for invoking auto logon from PMP web interface connected in Windows. For example, to establish telnet connection to a remote system automatically from the PMP web interface connected in Windows, enter the command as follows:
telnet %DNS_NAME% -l %ACCOUNT_NAME%

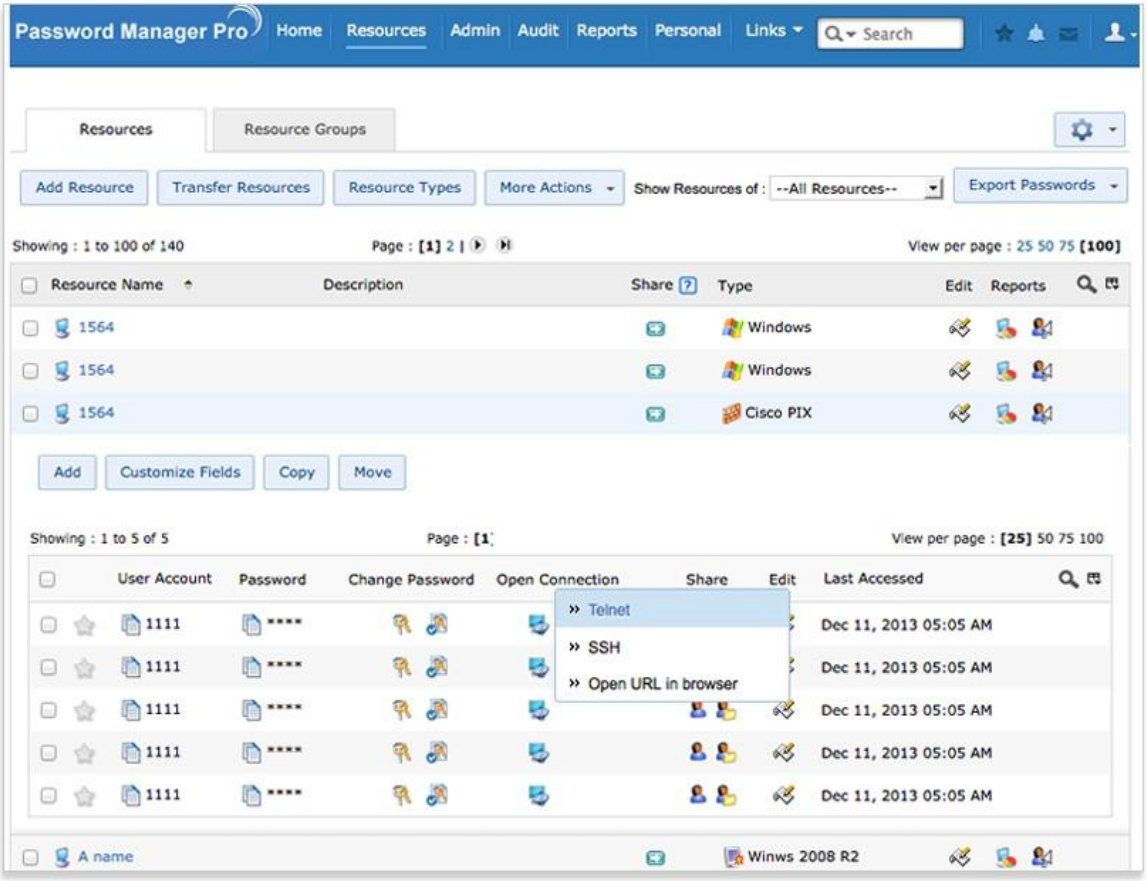
PMP will take care of replacing the values of the respective place holders.
Similarly, in the text field against "Command to invoke in Linux", enter the command for invoking auto logon from PMP web interface connected in Linux. For example, to establish telnet connection to a remote system automatically from the PMP web interface connected in Linux, enter the command as follows:
konsole -e telnet %DNS_NAME% -l %ACCOUNT_NAME%

Step 4: Map Commands with the Resource Types

After creating the required commands as detailed above, you need to select the 'Resource Types' for which you wish to map the helper commands.

For example, assume you have created helper script for connecting to remote systems via PuTTY (from PMP web-interface), you can map the command to the following resource types: All UNIX resources and Cisco devices.

If you do so, the auto logon to remote systems via PuTTY will be enabled for all the resources belonging to the above three resource types. When you view those resources, you will find "Connect To" icon as shown below. The command names associated by you to that resource type will be visible in the list. (Complete Step 6 below before trying to check this step in your setup, otherwise the data entered in this UI till now will not be saved).
For a particular target system, there can be more than one method to connect (telnet, PuTTY, RDP etc.,) and hence you can map any number of commands to a single target system type. All the command names associated with the resource type will be displayed on "Connect To" icon.



Step 5: Request for Approval

As explained above, the helper script is invoked with the same privileges as the user account running the PMP server. To guard against potential risks associated with invoking arbitrary scripts/commands, a dual control mechanism is implemented, which will ensure two administrators see and approve the script before it is invoked by PMP. When an administrator adds a helper script, PMP does not invoke it unless it has been approved by

another administrator. The same process is followed when the helper script details are edited by an administrator. These operations can be performed by any two administrators and are audited.

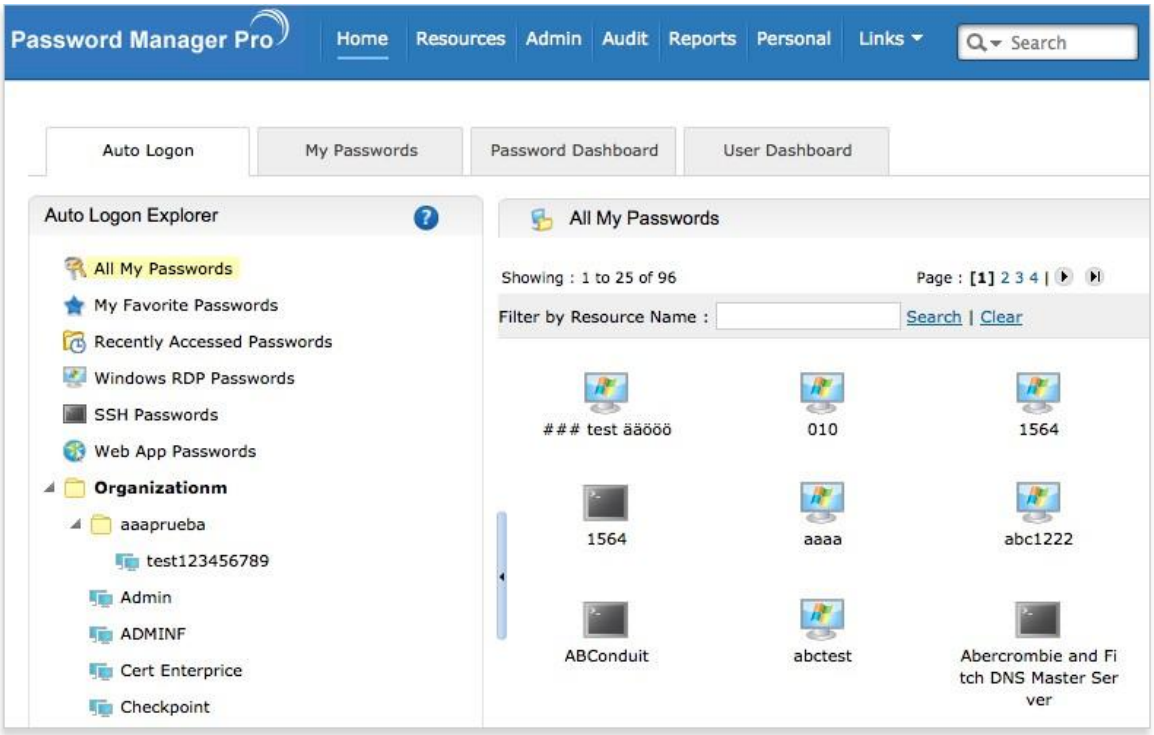
The helper scripts can be added only by PMP administrators. The scripts thus added have to be approved by some other administrator. So, the helper script created will remain pending for approval. Select an administrator from the drop-down to send approval request. A mail will be sent to that administrator intimating the approval request.

If you are an administrator and requested by another admin to approve a script, you need to navigate to "Admin" >> "Customize" >> and click "Auto Logon" and click the link present under "Approval Status". Once it is approved, the helper script will take effect.
Click "Save". The required auto logon helper has been created. The helper script creation and approval events are all audited in PMP.

Invoking Auto Logon

Through Auto Logon Gateway

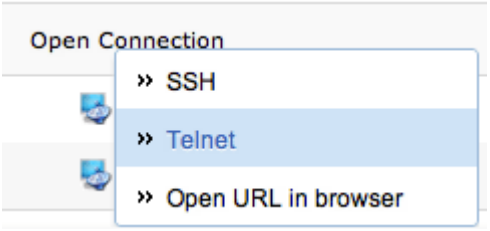
As soon as an administrator adds a resource that supports one of the three remote terminal session types (Windows RDP, SSH and Telnet sessions), the feature becomes available to all users in the system who have access to that resource, with no further configuration anywhere. You will see the'Auto Logon' sub tab under the 'Home' tab will allow users to easily locate remote accounts and launch a session with a single click.



Through Auto Logon Helper Script

To automatically connect to a particular resource, navigate to the 'Resources' tab and click the required resource. Click the

"Connect To" icon present against the required user account. A list containing the list of commands supported for that resource will be displayed. Click the required command.



The command configured will be invoked as is on the user machines and hence it is recommended to ensure that the PATH environment variable is properly set or the command be located in the same execution path in all the user machines. The command string will have these place holders%RESOURCE_NAME%, %DNS_NAME%, %ACCOUNT_NAME% and %PASSWORD% which will be replaced with respective values at the time of invocation.

PMP has no control over the command other than invoking it and also does not process the result of the command. The helper script supplied will be stored in the same database as the other information, which provides security as well as backup, if it is configured for the PMP database.

For the first time of invocation alone, you will have to install browser plug-ins as explained below:

Due to inherent security restrictions in the browsers, as a one-time activity, you need to download and install browser specific plug-ins to invoke operating system commands.

To install plug-in for Internet Explorer

When you click the 'Connect To' icon of a resource, you will get a security warning pop-up. The pop-up will ask if you want to install that plug-in with publisher name as ZOHO Corp. Click 'Install'. The plug-in would be installed.

To install plug-in for Firefox

- Go to Admin >>> General and click the icon "Plug-in for Firefox"
- You will see an yellow band on top of the browser with the following wordings: "Firefox prevented this site () from asking you to install a software in your computer". At the end of that you will find "Edit Options". Click that.
- Click Admin >>> General >> "Plug-in for Firefox" again
- Click "Download Software"
- Click "Install"
- Click the option "Restart Firefox"

Once you do this, you will be able to login automatically.

Privileged Session Recording

(Feature available only in Premium and Enterprise Editions)

Overview

Privileged sessions launched from Password Manager Pro can be recorded, archived and played back to support forensic audits and let enterprises monitor all actions performed by privileged accounts during privileged sessions. Session recording caters to the audit and compliance requirements of organizations that mandate proactive monitoring of activities. Administrators can readily answer questions regarding the „who," „what" and „when" of privileged access.

Password Manager Pro enables recording of Windows RDP, SSH and Telnet sessions launched from the product.

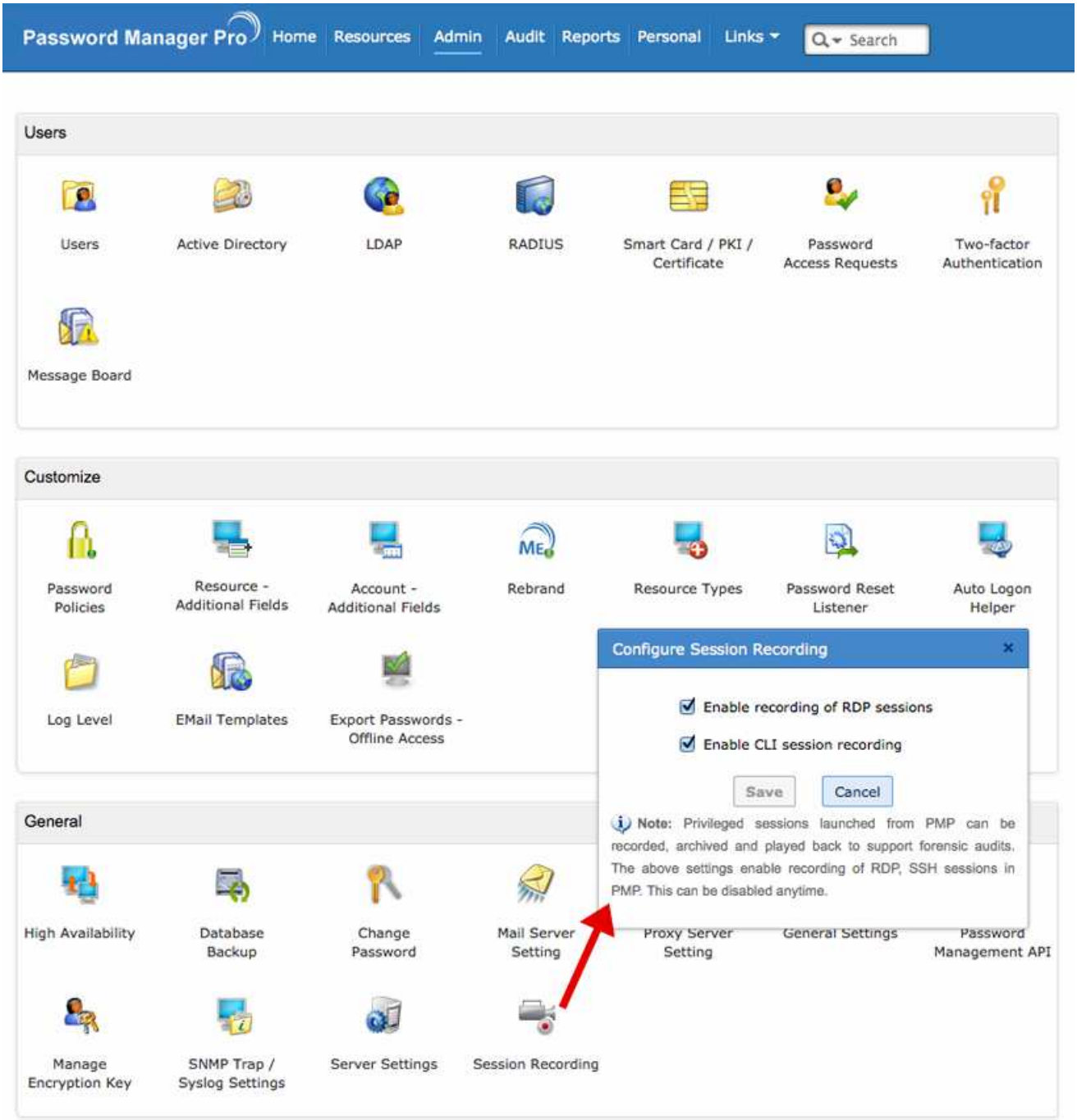
How secure is session recording?

Password Manager Pro employs first-in-class, browser-based remote login mechanism for the session recording process. From any HTML5-compatible browser, users can launch highly secure, reliable and completely emulated Windows RDP, SSH and Telnet sessions with a single click, without the need for additional plug-in or agent software. Remote connections are tunneled through the Password Manager Pro server, requiring no direct connectivity between the user device and remote host. In addition to superior reliability, the tunneled connectivity provides extreme security as passwords needed to establish remote sessions do not need to be available at the user"s browser. The new session recording capability is an extension of the robust remote login mechanism.

From version 6500, PMP comes bundled with RDP, SSH and Telnet session gateways. This allows the users to launch remote terminal sessions from their browser that are tunneled through the PMP server. The remote terminal sessions are emulated in the browser screen itself and hence there is no need for installing any plug-in or agent in any end-points. The only requirement is the browser should be HTML 5 compatible (For example IE 9 or above, FF 3.5 or above, Safari 4 or above, Chrome).

How to enable session recording?

Session recording can be enabled through a simple administrative setting. Navigate to Admin >> General and click "Session Recording".



In the GUI that opens up, select the text boxes "Enable recording of RDP sessions" and/or "Enable recording of CLI sessions" as required. Once this is done, as soon as an administrator adds a resource that supports one of these remote terminal session types (RDP, SSH, Telnet), the session recording feature becomes available.
Whenever a user launches a recomote connection, whatever they do afterwards gets recorded.

How to view/playback the recorded sessions?

The recorded sessions are available for view under "Audit" tab. Along with Resource Audit, User Audit and Task Audit, "Recorded Sessions" has been added as a separate tab. You can trace the required session through the name of the resource, user who launched the session, time at which the session was launched etc. Just click "Play" at the end of each entry to view the recorded session.

Shadow Sessions in Real-Time

(Feature available only in Enterprise Edition)

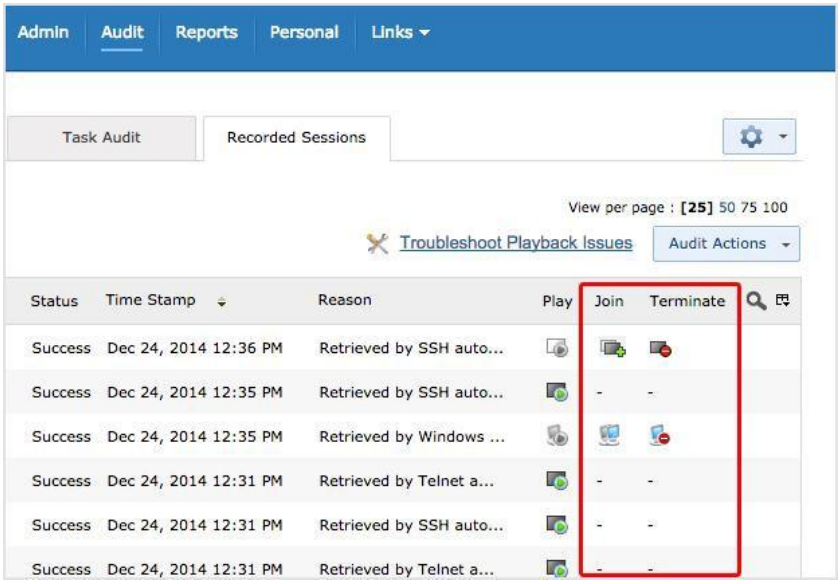
PMP lets administrators closely monitor the privileged sessions on highly-sensitive IT resources. Admins can view the sessions in parallel and terminate suspicious activities. Similarly, admins can offer assistance to users while monitoring the users" activities during troubleshooting sessions.

To monitor sessions in parallel,

- Navigate to Audit >> Recorded Sessions
- Trace the session to be monitored through the name of the resource
- Click the link available under the column "Join"
- You will be able to view the session in parallel

To terminate a suspicious session,

- Navigate to Audit >> Recorded Sessions
- Trace the session to be monitored through the name of the resource
- Click the link available under the column "Terminate"
- The session with the remote resource will be terminated. The user will lose connection with the remote resource



Purging Recorded Sessions

The recorded sessions occupy only very little space in the database. However, if you have a large number of resources with session recording enabled, you need to have a few GBs available in the DB.

- If you do not need the session recordings that are older than a specified number of days, you can purge them
- Navigate to "Resource Audit" section and go to the end of the page. To purge the records that are older than a specified number of days, specify the number in the text-box against the field "Purge Audit Records".
- Click "Save". The Session Recordings that are older than the number of days specified by you, will be purged

Configuring Landing Servers for Data Center Remote Access

(Feature available only in Enterprise Edition)

Overview

Typically, data centers limit direct access to remote devices via SSH and Telnet connections. Instead, data center admins working remotely must first connect to a landing server and then "hop" to the target system. In some cases, admins must make multiple hops before ultimately connecting to the target devices. At each step of the remote access process - from the initial landing server to each subsequent hop and the target device - the admin must provide the username and password as well as know the IP address of the landing server.

Password Manager Pro has simplified this entire data center remote access management. You can use Password Manager Pro to effectively launch direct connections (TELNET, SSH) to IT equipment in the data center, overcoming access barriers created by network segmentation while adhering to data center access protocols. Password Manager Pro also supports full password management of those remote devices.

You can configure any number of landing servers to remotely access the IT equipment in your data centers. You need to associate the landing servers with the resources being managed in the product. Once the configuration is done, you can launch a direct connection with the remote resources in a single click without worrying about the intermediate hops. PMP takes care of establishing connection with the landing server(s) and finally with the remote resources, in fully automated fashion.

Configuring Landing Servers - Summary of Steps

Following are the steps involved in configuring landing servers:

1. Add the required landing servers as resources in PMP
2. Create identities for landing servers by providing them names
3. Associate resources with landing servers

Step 1: Add the required landing servers as resources in PMP

Landing servers are also basically resources in PMP. Data center remote access starts with establishing connection with the landing servers first. So, the first step is to add the

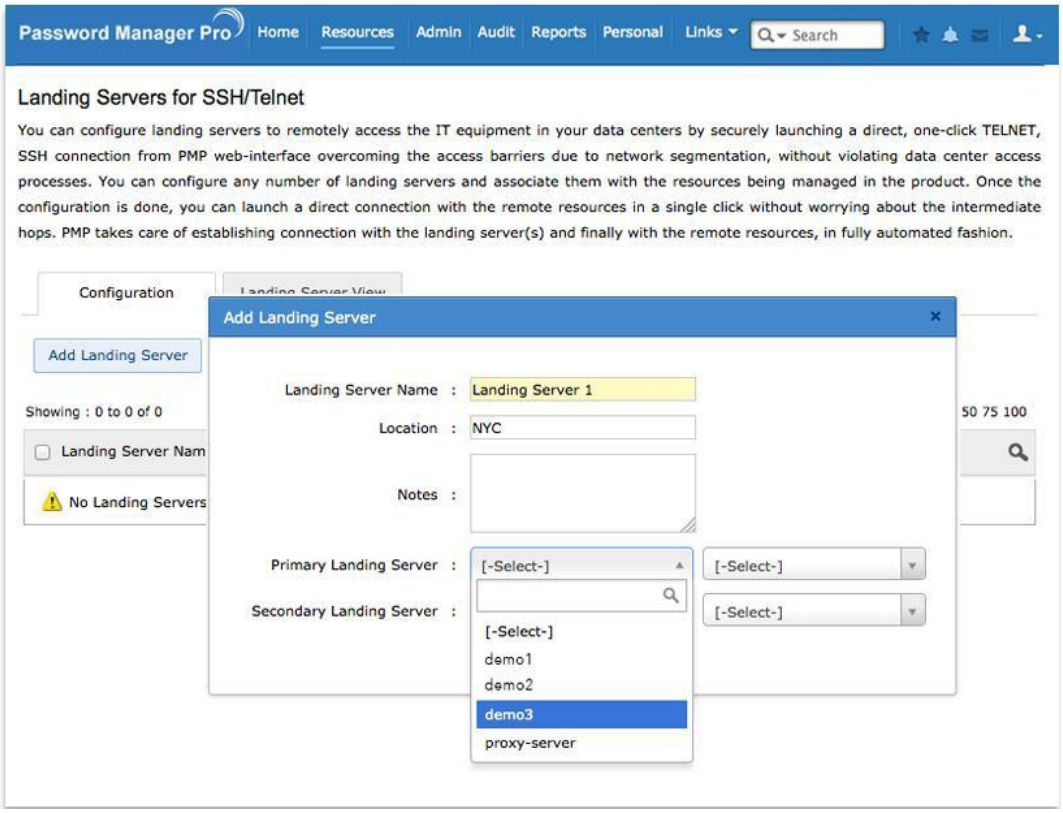
required landing servers as resources in PMP through the usual resource addition process. Landing servers typically have primary and secondary setup. Add both primary and secondary servers as resources.

Step 2: Create identities for landing servers by providing them names

After adding the required landing servers as resources in PMP, you need to establish an identity for each landing server. You can do this by providing a name for each landing server.

- To do this, navigate to Admin >> General >> Landing Servers for SSH/Telnet
- In the GUI that pops-up, enter a name for the landing server. This will help you uniquely identify it
- Enter other details like location, description notes
- If you have primary and secondary instances for your landing server, select the respective resources from the drop-down (these resources were added by you in step 1 above)
- Also, select the account that is used to login to the landing server

Repeat the above steps and create identities for as many landing server as needed.



Step 3: Associate resources with landing servers

After adding the landing servers, you need to associate resources with the respective landing servers. This is a crucial step as this is where you are connecting the resources with the landing servers. Also, this is where you will be defining the direct connection launching path.

For example, assume that you want to connect to your corporate mail server, which runs on a Linux host in the database and you need to hop to 'Landing Server A' first. Now, you will have to associate the mail server with Landing Server A.

You can associate as many resources with a landing server as needed - different resources have different landing servers and different connecting paths. Quite often, there could be multiple landing servers (or multiple hops) to connect to a resource. In that case, you should be associating resources as explained below:

Assume the scenario:

PMP Server ----> Landing Server 1 -----> Landing Server 2 ----> Proxy Server in Data Center

To connect to your proxy server in data center from PMP, you need to connect to Landing Server 1 first, then to Landing Server 2 and finally the actual resource. You should associate landing server with resources as explained below.

All the three entities - landing server 1, landing server 2 and the proxy server are resources in PMP.

- You should associate Landing Server 1 with Landing Server 2
- Then, you need to associate Landing Server 2 with Proxy Server

Once you establish the association this way, PMP will take care of finding the connection path automatically and establish direct connection with the resource.

To associate resources with a landing server:

- Navigate to Admin >> General >> Landing Servers for SSH/Telnet
- Click the "Associate Resources" icon against the respective landing server
- In the GUI that opens up, select the required resources
- Click "Associate Resources"

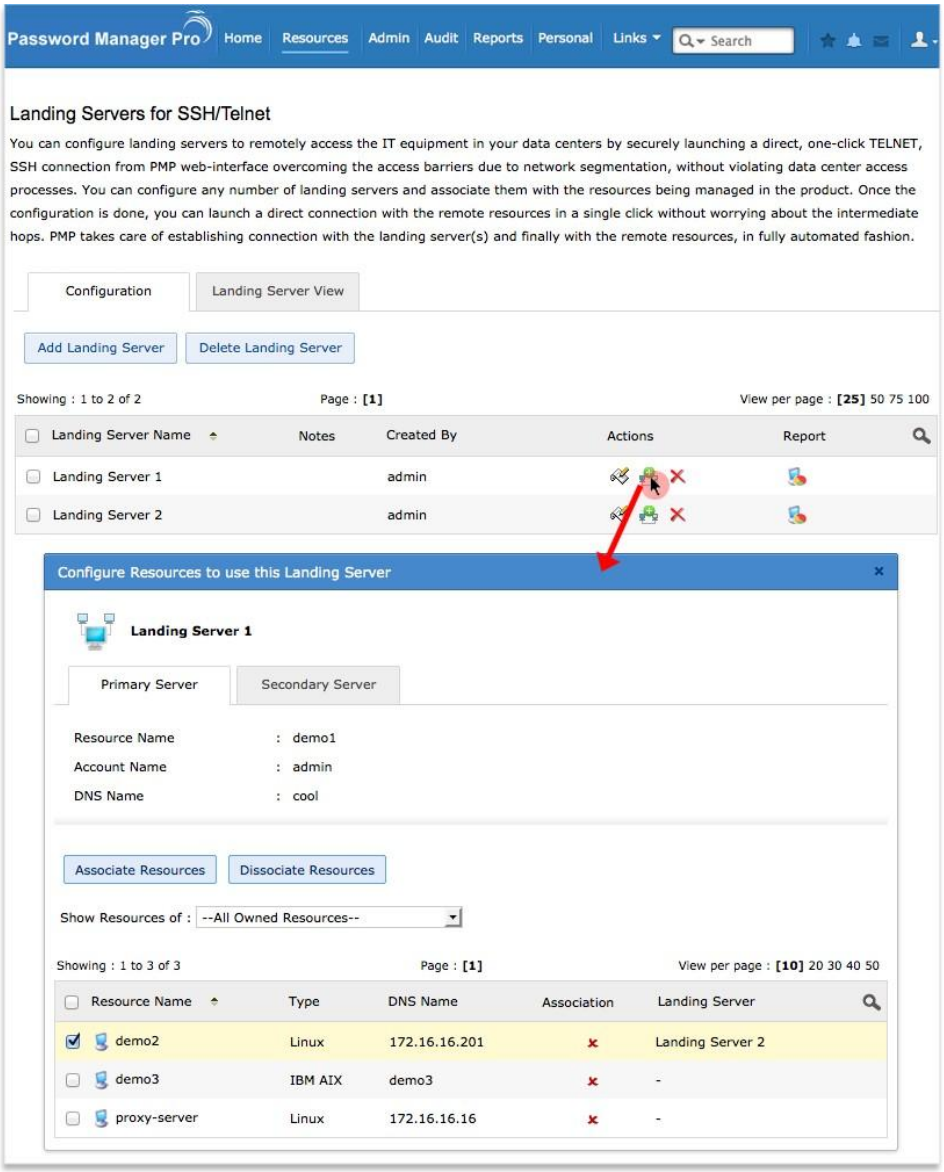
Example

For estalishing connection to the Proxy Server in the data center as per the set up below, you need to make associations as shown below.

PMP Server ----> Landing Server 1 -----> Landing Server 2 ----> Proxy Server in Data Center

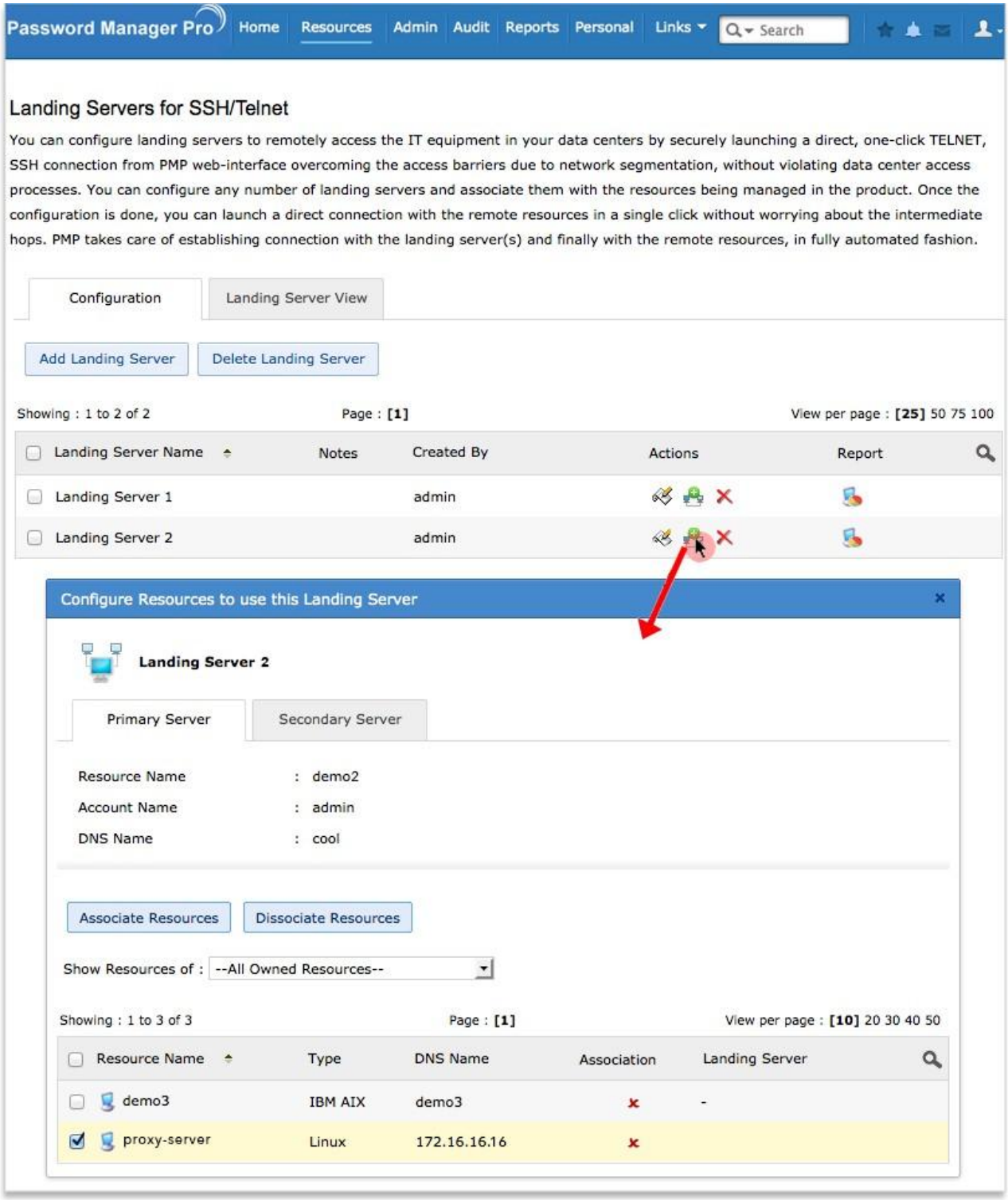
Associating Landing Server 1 with Landing Server 2

As you see in the screen capture below, Landing Server 2 has been added as a resource with the name 'demo2' in PMP. So, that resource is being associated with Landing Server 1.



Associating Landing Server 2 with the Resource Proxy-Server

The actual resource proxy-server is connected through Landing Server 2. So, Landing Server 2 is associated with the resource Proxy-Server as shown below:



Providing landing server details during resource addition

If you have added landing servers and created identities for them (step 1 and 2 above), the association part (step 3) could be done during resource addition process. In step 3 of resource addition, you can select the landing server.

Alternatively, as part of editing resource details too, you can associate landing servers with resources.

Auto Logon for Web Apps

One-click Log in to Web Applications

You can setup PMP to auto-fill the login page of web applications with appropriate username/password information, to allow users to login to those apps with just a few clicks, instead of manually entering the information. This is achieved by the users installing the PMP bookmarklet in their browsers.

What is a bookmarklet?

Every browser allows users to create bookmarks for URLs. A browser bookmark typically contains a static URL and clicking the bookmark opens the URL. A bookmarklet is similar to a browser bookmark, but additionally it contains a piece of unobtrusive script. Clicking on the bookmarklet not only opens the URL, but executes the script which can be used to perform a few tasks on the opened URL. A bookmarklet is a secure mechanism to bring dynamism to browser bookmarks.

How does PMP use bookmarklet for auto logon?

As a requisite step, the PMP user must install the PMP bookmarklet in his/her browser's bookmarks bar. To use auto logon, the user clicks the right resource-name/account-name pair and then the PMP bookmarklet in the bookmarks bar. This bookmarklet first opens the URL of the web app and then executes a script that accesses the PMP web server, retrieves the username/password for the requested web app, populates the fields in the login page of the web app and finally submits the page for authentication. The script works only when the user is logged into PMP and is on the right login page of the application.

How to use the PMP bookmarklet for auto login?

One-time setup

- Navigate to Home >> Auto Logon tab in the web-interface
- Click "Web App Passwords"
- Drag this button 

bookmarklet-button to the bookmarks bar to install it. This is a one time action required for every browser you use to access PMP.

One-click Auto Login

- This can be initiated either from "Auto Logon" tab or "My Passwords" tab in PMP Home
- Locate the right resource-name/account-name that you want to login to
- Invoke the 'Open URL' against the appropriate credential. This will open the URL in a new browser window or tab
- Now click the PMP bookmarklet in the browser's bookmarks bar
  If you have permission to access more than one credential for this URL, the choices will be shown as a pick list. Choose one
  This will populate and submit the login information and if the authentication is successful, you will be allowed access to the web app

Security Tip

When using public or shared computer to access PMP and subsequently bookmarklet based auto logon, make sure to remove the PMP bookmarklet from the bookmarks bar after you are done using PMP. Though the bookmarklet does not work when there is no valid PMP session in the browser, the script may be used to obtain information about PMP server's DNS name etc., which can be avoided. The bookmarklet can be installed/removed easily as required.

High Availability Scenario

If you have configured High Availability, in the event of failover, when you connect to the PMP secondary server, the bookmarlet installed for the Primary server will not work for the secondary. You need to install bookmarklet for secondary separately.

Misc

Password Management API for Application-to-Application Password Management

(Feature available only in Premium and Enterprise Editions. Procedure applicable only for PMP Builds 6200 onwards)

Overview

For applications and scripts in your infrastructure that communicate with other applications using a password, you no longer have to hard-code the password in a configuration file or a script. They can securely query PMP to retrieve the password whenever they need, so that administrators are free to apply good practices like periodic rotation to such passwords as well, without worrying about having to update them manually in many places.
Password Management APIs

Note: The mechanism used to configure and use the API till version 6.1 stands deprecated and will eventually be removed.

From version 6.2 onwards, PMP provides two flavors of the API:

- a comprehensive application API based on XML-RPC over HTTPS and
- a command line interface for scripts over secure shell (SSH)

Both the forms use PKI authentication for allowing access to the PMP application through the API. The XML-RPC API also comes with a Java Wrapper API to make it easy for integrating it with Java applications.

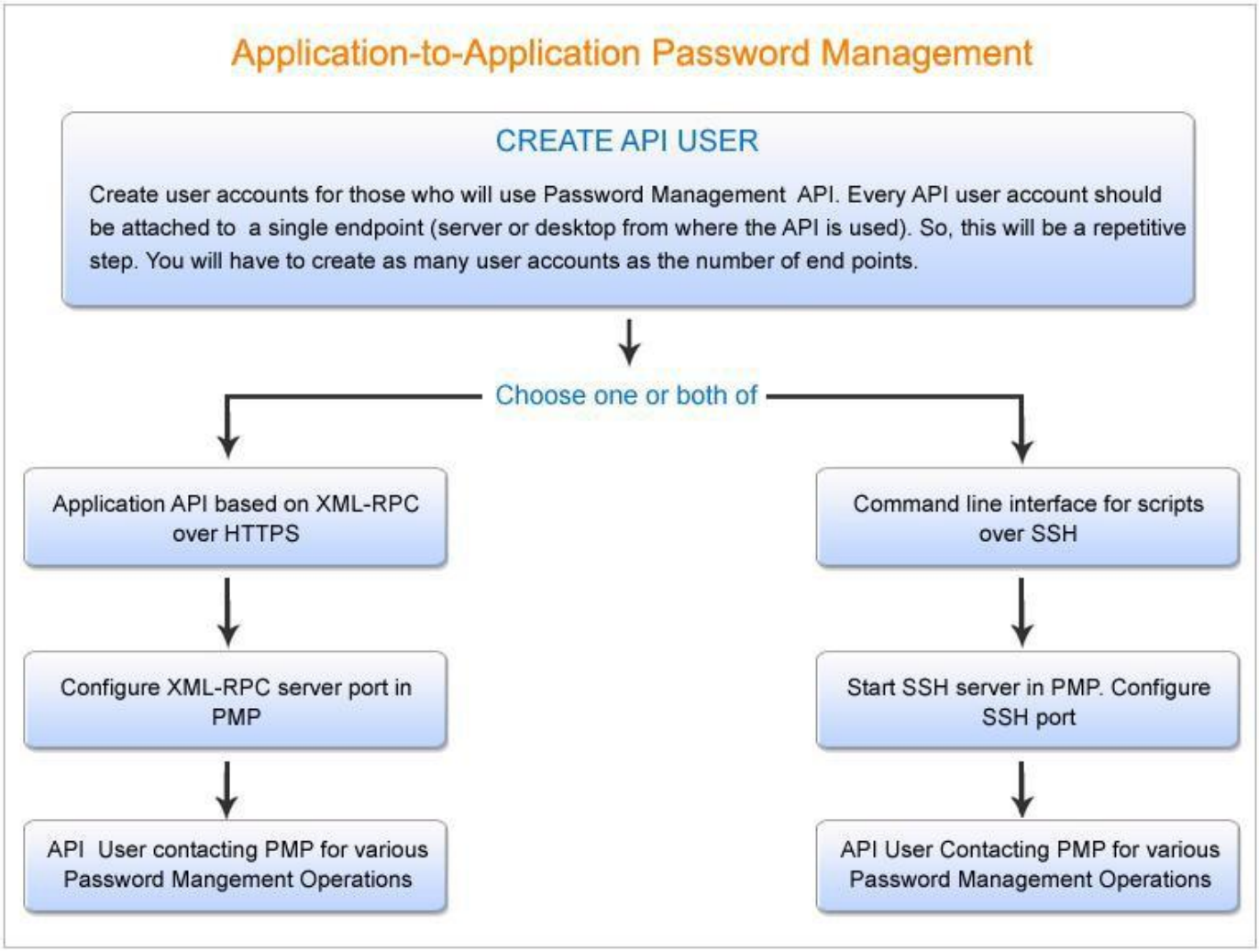
Configuring Password Management APIs - Summary of Activities

The following is the summary of the activities involved on configuring and use the API from version 6.2

- User accounts have to be created in PMP that will use only the PMP API. Every API user account should be attached to a single endpoint (server or desktop from where the API is used, so the user accounts are uniquely identified as user@hostname)
- An API user can use both the forms of the API, that is, XML-RPC and SSH CLI

- The API users are authenticated using PKI authentication. So, for each user, depending on the type of API used, the following should be supplied:
    - a X.509 format SSL certificate that has the user name as the common name for using XML-RPC API
    - an OpenSSH format public key, corresponding to the private key of user@host, for using SSH CLI
- PMP has built in XML-RPC and SSH servers and they can be configured to run on specific ports
- After API users are created and the respective servers (XML-RPC and/or SSH) are enabled, PMP is ready to serve the API users
- Administrators can provide access to passwords to API users in the same way as it is done for other users. API users can only access passwords that they have permission to, through the API
- Currently the API allows password retrieve, modify and create operations

The following diagram better illustrates the summary of steps involved in Application-to-Application Password Management:



Step-by-step Procedure

Prerequisites

1. Create API User Accounts in PMP

This is the first step in the process to configure and use Password Management APIs for Application-to-Application Password Management. As mentioned above, user accounts have to be created in PMP to those who will use only the Password Management API. Every API user account should be attached to a single endpoint (server or desktop from where the API is used, so the user accounts are uniquely identified as user@hostname)

To create an API user account,

1. Click "Add API User" button in "Admin >> Users" tab
2. In the "Add API User" UI that opens up, enter the 'User Name' in the respective text field. This name identifies the API user. It is important that the same name should be used as the 'Common Name' (CN) in the corresponding SSL certificate. In MSP edition, in addition to the 'Common Name'(CN), the Organization Name (O) in the certificate should be same as the organization display name in PMP
3. Enter the name of the host from where the API user would access PMP for password management operations. Internally, the user name and the host together is used to uniquely identify the API user. For example, a user with the name 'test' from the host 'test-server' will be considered as 'test@test-server' to uniquely identify the API user
4. 'Full Name' refers to the name with which the API user would be identified in the external world. That means, in reports, audit trails and such other places where activities are traced to users. By default, the 'User Name' - 'Host Name' combination with the suffix "API User" is used as 'Full Name'. In the above example, it will be test@test-server - API User. However, if you want to have a different name, you are free to define that.
5. Select an appropriate access level for the API user being added - Administrator/Password Administrator/Password User
6. If you are adding a user as "Administrator" or "Password Administrator", you can specify the 'Access Scope'. If you select the option,"Passwords Owned and Shared", the administrator/password administrator will be able to view the passwords owned by them and those shared to them by others. You can choose to make the administrator/password administrator a super administrator, you need to select the option "All Passwords in the System". When you do so, the administrator or the password administrator will be able to access all passwords in PMP without any restriction.
7. SSH connects and logs into the specified host with user name specified above. The user must prove his identity to the remote machine using public key authentication. If you wish to make use of the SSH CLI access, browse and select the open SSH format public key of the CLI user.

   If you want to create SSH format private-public key afresh,

   - Open a command prompt and run the command ssh-keygen
   - By default, the private key is stored in id_rsa file. The public key is stored in id_rsa.pub. These two files are stored under the directory specified in the command prompt by default

- If you want, you can store them under a different location. You need to import the id_rsa.pub. It will be stored in PMP under<PMP_HOME>/<user name>/.ssh/authorized_keys]
- If you want to have an extra layer of security, you can use passphrase on the SSH key. Once you enter and confirm a passphrase, the passphrase is added to the key. You will have to enter the passphrase everytime when you use the SSH key
- Once you generate the key, specify the location of the public key (browse and locate in the user addition GUI)
- The following snapshot explains the above sequence:

```
Generating public/private rsa key pair.
Enter file in which to save the key (/home/xyz/.ssh/identity):
/home/xyz/.ssh/pmp_identity
Enter passphrase (empty for no passphrase): *enter your passphrase here*
Enter same passphrase again: *repeat your passphrase*
Your identification has been saved in /home/xyz/.ssh/pmp_identity.
Your public key has been saved in /home/xyz/.ssh/pmp_identity.pub.
The key fingerprint is:
22:71:3c:ff:7e:df:59:ad:72:47:d1:16:bd:e2:e9:2d xyz@xyz
```

The above example shows how to generate the key pair using open SSH. You may use any other standard tool to generate the keys as you wish.

8. If you wish to make use of XML-RPC API access, enter the X.509 format SSL certificate of the XML-RPC API user
    - Certificate can be created using OpenSSL and it can either be signed by a Certificate Authority (CA) or it could be self-signed.

Step 1: Generating Certificate

Creating a certificate using openssl involves two steps - generating private key and generating certificate. Use the following commands to create the certificate.

Generate private key

```
openssl genrsa -des3 -out server.key 2048
```

Generate a certificate request

Use the server private key to create a certificate request. Enter the passphrase for the key, Common Name, hostname or IP address, when prompted:

```
openssl req -new -key server.key -out server.csr
```

- After generating the certificate, you need to get it signed by a CA. Here, you have the option to get it signed by a third-party CA such as VeriSign, Thawte, RapidSSL etc or you may self-sign the certificate. Procedure for both have been explained below. Choose one based on your environment:

Step 2: Getting the certificate signed by third-party (like Verisign) CA

- Some of the prominent CAs are Verisign (http://verisign.com), Thawte (http://www.thawte.com), RapidSSL (http://www.rapidssl.com). Check their documentation / website for details on submitting CSRs and this will involve a cost to be paid to the CA
- This process usually takes a few days time and you will be returned your signed SSL certificate and the CA's root certificate as .cer files
- Save them both in the same working folder where files from steps 1 and 2 are stored

-OR-

Self-Signing the certificate

The procedure for self-signing the certificate involves the following steps:

Creating Private Key

Use the following command to create private key:

openssl genrsa -des3 -out server.key 2048
This command generates output like this:
Generating RSA private key, 2048 bit long modulus
.....++++++
.....
.++++++
e is 65537 (0x10001)
Enter pass phrase for ca.key: password
Verifying - Enter pass phrase for ca.key: confirm_password

Creating Public Key Without CA:

Use the following command to create public key without using CA:

openssl req -new -x509 -key server.key -out server.crt -days 1095
The output from this command looks like this:
Enter pass phrase for ca.key: password
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:Pleasanton
Organization Name (eg, company :Zoho Corporation
Organizational Unit Name (eg, section) []:Manage Engine Password Manager Pro
Common Name (eg, YOUR name) []:localhost
Email Address []:
Note: If you enter '.', the field will be left blank.

Generate PKCS12 certificate file

The procedure for self-signing the certificate ends with the above step. However, you require to generate PKCS12 file for use in the calling application in A-to-A password management. Use OpenSSL to convert an x509 certificate and/or RSA key to a Public-Key Cryptography Standard #12 (PKCS#12) format:
openssl pkcs12 -export -clcerts -in server.crt -inkey server.key -out server_cert.p12 -name "PMP"

1. Enter the department to which the user belongs (optional)
2. Enter the location of the user. This would be helpful for future reference (optional)
3. Click "Save". The required API user with desired access restriction has been created

Important Note:

- You can make use of either or both XML-RPC API & SSH CLI API. The API user creation process is the same for both
- The API User creation is specific to the host from where the application would contact PMP for passwords. That means, user and host are tied with other. If you want to make use of Password Management API from more than one host, you need to create as many API users as the number of hosts. Conversely, if you wish to have many users on a single host, then again you need to create as many API users as needed.

Steps to Configure SSH CLI Access

Summary of Steps Involved

1. Create API user (as explained in the Pre-requisite above)
2. Configurations on the server-side
3. Starting SSH server
4. Configurations on the client-side to enable applications access PMP

Configurations on the server-side

PMP comes with an inbuilt SSH server. By default, it occupies 5522. You may configure it to run on any other desired port, if you wish to do so. You need to start the SSH server.
To configure the SSH server port and to start it,

1. Go to "Admin >> General >> Password Management API >> SSH CLI"
2. Change the SSH-CLI server port, if you want to
3. Click "Start SSHD Server"

Accessing PMP from the Application

Once you have created API users and also started SSH server in PMP, API users can access PMP for the passwords that are allotted to them. Note that the ownership and sharing mechanism of PMP applies in the case of API users too. That means, the API users will be able to access only those passwords that are allotted to them. Using Password Management APIs, users can retrieve, modify and create accounts.

Password access workflow on the client-side: How does it work?

Each user creates SSH public-private key pair for authentication purposes. The server knows the public key and the user knows the private key. The file <PMP_HOME>/<user name>/.ssh/authorized_keys lists the public keys that are permitted for logging in. When the user logs in, the SSH program tells the server which key pair it would like to use for authentication. The server checks if this key is permitted, and if so, sends the user a challenge, a random number, encrypted by the user's public key. The challenge can only be decrypted using the proper private key. The user's client then decrypts the challenge using the private key, proving that user knows the private key but without disclosing it to the server. Once the authentication is successful, the user is permitted to do password management operations.

API User Contacting PMP for various password operations

As explained above, the API users will be allowed to access PMP for password retrieval and other operations only from the host in which they were configured to function. That is, during user creation, you would have entered the name of the host from where the API user would access PMP for password management operations. The API user will be allowed to access PMP only from the specified host.

To retrieve passwords or to do any other password management operation, the applications running in the host should access the SSH server that runs with PMP. The SSH server, in turn, connects to PMP for password operations.

The SSH server can be accessed using any standard openSSH command. As explained below, along with the command, you need to append PMP-specific commands to carry out the required password management operations.

ssh -q [-p port] user@hostname [-i private_key] [PMP specific command]
For Example: ssh -q -p 5522 test@test-server -i /home/guest/id_rsa [PMP specific command]

For MSP Edition use the below command

ssh -q [-p port] ORGNAME/user@hostname [-i private_key] [PMP specific command]
For Example: ssh -q -p 5522 MANAGEENGINE/test@test-server -i /home/guest/id_rsa [PMP specific command]
PMP-specific commands to be included in your application for application-to-application password management
For automatic A-to-A password management, you need to use the following commands in your application invoking the API.

For Password Retrieval

ssh -q [-p port] user@hostname [-i private_key] RETRIEVE --resource=<RESOURCE NAME As present in PMP> --account=<ACCOUNT NAME As Present in PMP> --reason=<REASON For Password Access> --ticketid=<TICKET ID For Password Access>

Example:

ssh -q -p 5522 test@test-server -i /home/guest/id_rsa RETRIEVE --resource=test-server --account=root --reason=Testing password retrieval using ssh client API --ticketid=7

For Password Reset

For Local Password Reset
ssh -q [-p port] user@hostname [-i private_key] RESET_LOCAL --resource=<RESOURCE NAME AS PRESENT IN PMP> --account=<ACCOUNT_NAME As Present in PMP> --newpassword=<NEW PASSWORD> --reason=<Reason for Password Reset> --ticketid=<TICKET ID For Password Reset>

Example:

ssh -q -p 5522 test@test-server -i /home/guest/id_rsa RESET_LOCAL --resource=test-server --account=root--newpassword=rootnew --reason=Rotating Password --ticketid=7

For Remote Password Reset

ssh -q [-p port] user@hostname [-i private_key] RESET_REMOTE --resource=<RESOURCE NAME AS PRESENT IN PMP> --account=<ACCOUNT_NAME As Present in PMP> --newpassword=<NEW PASSWORD> --reason=<Reason for Password Reset> --ticketid=<TICKET ID For Password Reset>

Example:

ssh -q -p 5522 test@test-server -i /home/guest/id_rsa RESET_REMOTE --resource=test-server --account=root --newpassword=rootnew --reason=Rotating Password --ticketid=7

For Creating a New Resource and a User Account

ssh -q [-p port] user@hostname [-i private_key] CREATE --resource=<RESOURCE NAME To Be Created> --account=<ACCOUNT NAME to be created>--newpassword=<PASSWORD of the Account being added> --resourcetype=<Type of the Resource Being Added> --notes=<Reference Notes>

Example:

ssh -q -p 5522 test@test-server -i /home/guest/id_rsa CREATE --resource=testresource --account=testaccount --newpassword=test password--resourcetype=Windows --notes=A New resource is added

Refer this document for more details.

Troubleshooting Tips

When I executed the above command, I did not get any response from PMP.
Solution
Remove the -q option in the above commands. You will receive warning/error messages on the screen. For example, to retrieve password, execute the command as:
ssh [-p port] user@hostname [-i private_key] RETRIEVE --resource= --account= --reason=

Contact PMP support with the message you see on the screen.
When I try to retrieve a password from PMP Secondary Server in High Availability mode, I do not get the required password

Solution

Every time after adding a new API user, the entire sshd folder available under has to be copied and pasted under . If this is done, you will be able to access the passwords from PMP Secondary.

Accessing PMP Secondary for A-to-A Password Management (HA Mode - SSH CLI)

If you have configured high availability setup in PMP, when the Primary Server goes down, applications can seamlessly connect to the Secondary for A-to-A Password Management. For this to work, you need to make the following simple configuration:

- Go to and copy the 'sshd' directory
- Paste it under

Important Note: The sshd folder has to be copied and pasted as explained above every time you create a new API user.

As mentioned earlier, PMP comes with an inbuilt SSH server. It has to be started in the PMP secondary installation as explained below:

If you have configured high availability setup in PMP, when the Primary Server goes down, applications can seamlessly connect to the Secondary for A-to-A Password Management. For this to work, you need to make the following simple configuration:

1. Stop PMP Primary Server

2. Connect to PMP Secondary's Web-Inteface
3. Go to "Admin >> General >> Password Management API >> SSH CLI"
4. Change the SSH-CLI server port, if you want to (by default it occupies 5522)
5. Click "Start SSHD Server"

Commands for accessing PMP Secondary Server

For automatic A-to-A password management, you need to use the following commands in your application:

For Password Retrieval
ssh -q [-p port] user@PMP_Secondary_hostname [-i private_key] RETRIEVE --resource= --account= --reason=

Example:
ssh -q -p 5522 test@test-secondary-server -i /home/guest/id_rsa RETRIEVE --resource=test-server --account=root --reason=Testing password retrieval using ssh client API

Once the above configuration is done, password access in high availability mode will be seamless. However, as write operations are not permitted when Primary Server is down, applications would only be able to RETRIEVE passwords. They will not be allowed to carry out password reset and resource/account creation.

Steps to Configure XML-RPC API

Summary of Steps Involved

1. Create API user (as explained in the Pre-requisite above)
2. Configurations on the server-side
3. Configurations on the client-side to enable applications access PMP
   - Option to use Java Wrapper provided by PMP in the calling application (OR) you may make use of XML-RPC client (using other programming languages as existing in your environment)
     - If you decide to use the Java Wrapper provided by PMP, download API jars and place them on the hosts from where applications would connect to PMP
       - Edit entries in configuration file that is bundled with the jar
       - Include the PMP-specific commands in the calling application
     - If you decide to use XML-RPC client with other programming languages as existing in your environment, include PMP-specific commands in the calling application

Configurations on the server-side

Step 1

Configure XML-RPC Server Port

PMP comes with an inbuilt XML-RPC server. By default, it occupies 7070. You may configure it to run on any other desired port, if you wish to do so.

To configure the XML-RPC server port,

1. Go to "Admin >> General >> Password Management API >> XML-RPC"
2. Change the XML-RPC server port, if you want to
3. Click "Save"
4. Restart PMP server to give effect to this setting

Step 2: (If you have self-signed the certificate or using your own certificate, carry out the following configuration; if you are using a certificate signed by third-party CA, skip this step)

While creating the API user, in case, you have self-signed SSL certificate (step 8 in pre-requisite above) or if you have used an already available internal certificate (your own certificate), you need to specify the root of the CA:

To specify the SSL root certificate,

1. Navigate to "PMP_Installation_Folder>/bin directory
2. Execute importCert.bat (in Windows) or importCert.sh (in Linux) as follows
   (In Windows)
   In the case of Self-signed certificates
   importCert.bat <absolute path of the Self-signed certificate>
   In the case of your own certificates or already available internal CAs
   importCert.bat<absolute path of the root of the CA>
   (In Linux)
   In the case of Self-signed certificates
   sh importCert.sh <absolute path of the Self-signed certificate>
   In the case of your own certificates or already available internal CAs
   sh importCert.sh<absolute path of the root of the CA>
3. Restart PMP server

Once you execute the above, the root of the CA will be recorded in PMP. All the certificates signed by the particular CA will henceforth be automatically taken.

Note:

- The root of the CA is recorded in server.xml file present under <PMP_Installation_Folder>/conf directory. For some reason, if you want to change it or if you want to enter a specific root directory, you may edit the file as explained below:

  In server.xml file, look for the following line (hint: you need to look for the line containing the entry clientAuth="true")
  <Connector URIEncoding="UTF-8" useBodyEncodingForURI="true" acceptCount="100" clientAuth="true" port="7070"connectionTimeout="-1" debug="0" disableUploadTimeout="true" enableLookups="false" keystoreFile="conf/server.keystore" keystorePass="passtrix" truststoreFile="jre/lib/security/cacerts" maxSpareThreads="75" maxThreads="150" minSpareThreads="25" port="7070" scheme="https" secure="true" sslProtocol="TLS"/>
- By default, the root of the CA will be jre/lib/security/cacerts. If you want to edit this, you need to change value for the entry truststoreFile as shown above.
- If Online Certificate Status Protocol (OCSP) is enabled in your client certificate, PMP will carry out authentication through it. Authentication through OCSP will require access to the internet. In enterprise network setup, you might need to go through a proxy server to access the internet. You may specify proxy server settings through Admin >> General >> Proxy Server Setting.

Step 3: Configurations on the client-side

Once you have created API users and also started XML-RPC server in PMP, API users can access PMP for the passwords that are allotted to them. Note that the ownership and sharing mechanism of PMP applies in the case of API users too. That means, the API users will be able to access only those passwords that are allotted to them. Using Password Management APIs, users can retrieve, modify and create accounts.

Password Management API is XML-RPC based. You have two options here:

- PMP provides a Java wrapper over XML-RPC. You may use it in the calling application

  OR
- You may make use of XML-RPC client (using other programming languages)

Option 1: Using the Java Wrapper Provided by PMP

Step 1: Download Java Wrapper Jar from PMP

1. Go to "Admin >> General >> Password Management API >> XML-RPC"
2. Download "Java PMP API Package" in the form of a zip named 'JavaWrapper.zip'
3. Put the zip in the host from where the application would contact PMP. Unzip JavaWrapper.zip
4. You will get two folders named 'docs' and 'lib' inside the main folder 'JavaWrapper'

Step 2: Edit Entries in the Configuration File

- Inside the 'lib' folder of JavaWrapper, you will find a configuration file named 'JAVA_API.conf'
- Edit the entries in the configuration file as per the details below:

ServerName=<The name of the host where the XML-RPC server is running. This will be same as the host where PMP is running. The value is entered by default and hence there is no need to edit this value >
ServerPort=<By default, the XML-RPC server occupies 7070 >
SecondaryServerName=<The name of the host where the PMP Secondary server is running. If high availability had been configured prior to setting up A-to-A Password Management, secondary server name is taken by default. In case, you configure high availability afterwards, you need to manually specify the PMP Secondary Server's host name here. If you do not intend to use high availability, leave this field blank>
SecondaryServerPort= <This represents XML-RPC server's port in PMP Secondary installation. By default, it occupies 7070>
KeyStorePath=
KeyStorePassword=

Example:
ServerName=testserver
ServerPort=7070
SecondaryServerName=test_workstation_secondary
SecondaryServerPort=7070
KeyStorePath=C:\\openssl\\bin\\file.p12
KeyStorePassword=passtrix
The calling application should present a SSL certificate when using the Password Management API. The jar provided by PMP contains the required certificates.

Step 3: Include PMP-specific commands in the calling application

Commands to be included (Refer to Javadocs for details)

For Password Retrieval

If password retrieval does not require a reason to be entered

To retrieve the password of a resource, enter the respective name of the resource and the account name exactly as present in PMP.
retrievePassword (String resourceName, String accountName)

Example:

```
import com.manageengine.pmp.PasswordManagerPro;
import com.manageengine.pmp.PMPException;

class Sample
{
   public static void main(String args[])
   {
      try
      {
      System.out.println(PasswordManagerPro.getInstance().retrievePassword("test-
server","administrator"));          }
      catch (PMPException pmpEx)
      {
      }
   }
}
```

If password retrieval requires reason to be entered

In case, the PMP settings in your environment mandate entering a reason for password retrieval, you need to enter the respective name of the resource and the account name exactly as present in PMP. Also, you must provide 'reason' for password retrieval.
retrievePassword (String resourceName, String accountName, String reason)

Example:

```
import com.manageengine.pmp.PasswordManagerPro;
import com.manageengine.pmp.PMPException;

class Sample
{
```

```
   public static void main(String args[])
   {
      try
      {
      System.out.println(PasswordManagerPro.getInstance().retrievePassword("test-
server","administrator","testing"));          }
      catch (PMPException pmpEx)
      {
      }
   }
}
```

If password retrieval requires ticket ID to be entered

In case, the PMP settings in your environment mandate entering a ticket ID for password retrieval, you need to enter the respective name of the resource and the account name exactly as present in PMP. Also, you must provide 'ticketId' for password retrieval.

retrievePassword (String resourceName, String accountName, String reason,
String ticketId)

Example:

```
import com.manageengine.pmp.PasswordManagerPro;
import com.manageengine.pmp.PMPException;

class Sample
{
   public static void main(String args[])
   {
      try
      {
      System.out.println(PasswordManagerPro.getInstance().retrievePassword("test-
server","administrator","testing","7"));          }
      catch (PMPException pmpEx)
      {
      }
   }
}
```

For Password Reset

Local Password Reset

To reset the password of a resource locally, enter the respective name of the resource and the account name exactly as present in PMP. Providing 'reason' for password reset is optional. For resetting the password locally, specify 'false' for the boolean updateRemote.
changePassword (String accountName, String reason, String updateRemote) (This will assign a new, random password)

OR

changePassword (String accountName, String reason, String newPassword, String updateRemote) (This will assign the new password specified by you)

Example:

```
import com.manageengine.pmp.PasswordManagerPro;
import com.manageengine.pmp.PMPException;

class Sample
{
   public static void main(String args[])
   {
      try
      {
      PasswordManagerPro.getInstance().changePassword("test-
server","administrator","testing","false" );
      }
      catch (PMPException pmpEx)
      {
      }
   }
}
```

Remote Password Reset

To carry out remote password reset, enter the respective name of the resource and the account name exactly as present in PMP. Specify 'true' as the value for the boolean updateRemote to indicate remote password reset. Optionally, you may include the reason for password reset as a string.

changePassword (String accountName, String reason, String updateRemote) (This will assign a new, random password)

OR

changePassword (String accountName, String reason, String newPassword, String updateRemote) (This will assign the new password specified by you)

Example:

```
import com.manageengine.pmp.PasswordManagerPro;
import com.manageengine.pmp.PMPException;

class Sample
{
   public static void main(String args[])
   {
      try
      {
      PasswordManagerPro.getInstance().changePassword("test-
server","administrator","testing","true");
      }
      catch (PMPException pmpEx)
      {
      }
   }
}
```

If password reset requires ticket ID to be entered

Local Password Reset

To reset the password of a resource locally, enter the respective name of the resource and the account name exactly as present in PMP. Providing 'reason' and 'ticketId' for password reset is optional. For resetting the password locally, specify 'false' for the boolean updateRemote.

changePassword (String accountName, String reason, String updateRemote, String ticketId) (This will assign a new, random password)

OR

changePassword (String accountName, String reason, String newPassword, String updateRemote, String ticketId) (This will assign the new password specified by you)

Example:

```
import com.manageengine.pmp.PasswordManagerPro;
import com.manageengine.pmp.PMPException;

class Sample
{
```

```
   public static void main(String args[])
   {
      try
      {
      PasswordManagerPro.getInstance().changePassword("test-
server","administrator","testing","false","7");
      }
      catch (PMPException pmpEx)
      {
      }
   }
}
```

Remote Password Reset

To carry out remote password reset, enter the respective name of the resource and the account name exactly as present in PMP. Specify 'true' as the value for the boolean updateRemote to indicate remote password reset. Optionally, you may include the reason and ticket ID for password reset as a string.

changePassword (String accountName, String reason, String updateRemote, String ticketId) (This will assign a new, random password)

OR

changePassword (String accountName, String reason, String newPassword, String updateRemote, String ticketId) (This will assign the new password specified by you)

Example:

```
import com.manageengine.pmp.PasswordManagerPro;
import com.manageengine.pmp.PMPException;

class Sample
{
   public static void main(String args[])
   {
      try
      {
      PasswordManagerPro.getInstance().changePassword("test-
server","administrator","testing","true","7");
      }
      catch (PMPException pmpEx)
      {
      }
```

```
   }
}
```

Creating New Resource & User Account

To create a new resource and a user account, enter the name of the resource and the account to be added and the account name exactly as present in PMP. Specify 'true' as the value for the boolean updateRemote to indicate remote password reset. Optionally, you may include the notes to serve as reference.

createResource (String resourceName, String resourceType, String accountName, String notes) (This will assign a new, random password for the account being created)

OR

createResource (String resourceName, String resourceType, String accountName, String newPassword, String notes) (This will assign the specific password for the account being created)

Example:

```
import com.manageengine.pmp.PasswordManagerPro;
import com.manageengine.pmp.PMPException;

class Sample
{
   public static void main(String args[])
   {
      try
      {
      PasswordManagerPro.getInstance().createResource("Mail-
Server","Windows","administrator","testing");
      }
      catch (PMPException pmpEx)
      {
      }
   }
}
```

Option 2 Making use of XML-RPC client (using other programming languages)
Refer to this document for details.

Accessing PMP in High Availability Mode (XML-RPC)

If you have configured high availability setup in PMP, when the Primary Server goes down, applications can seamlessly connect to the Secondary for A-to-A Password Management.
Case (1): If you have configured High Availability setup prior to configuring A-to-A password management through XML-RPC

If you are using a certificate signed by a third-party CA, you need not carry out any specific configuration for accessing secondary server when primary is down. Everything is automatically taken care of.
If you are using self-signed certificate or using your own certificate, you need to import the SSL root certificate in PMP Secondary Server by following the steps as explained in one of the sections above .
As mentioned earlier, PMP comes with an inbuilt XML-RPC server. By default, it occupies the port 7070 in PMP Secondary installation. If you want to change it to some other desired value, you may do so as explained below:

1. Stop PMP Primary Server
2. Connect to PMP Secondary's Web-Inteface
3. Go to "Admin >> General >> Password Management API >> XML-RPC"
4. Change the XML-RPC port, if you want to (by default it occupies 7070)
5. Click "Save"
6. Restart PMP Secondary Server for this change to take effect
   Once the above configuration is done, password access in high availability mode will be seamless. However, as write operations are not permitted when Primary Server is down, applications would only be able to RETRIEVE passwords. They will not be allowed to carry out password reset and resource/account creation.

Case (2): If you configure High Availability setup AFTER configuring A-to-A password management through XML-RPC

In this case, you need to make the following configurations:
Step 1

Inside the 'lib' folder of JavaWrapper, you will find a configuration file named 'JAVA_API.conf'. You will find an entry named"SecondaryServerName". Against that, specify the host name of the secondary server.
SecondaryServerName=<The name of the host where the PMP Secondary server is running>
As mentioned earlier, PMP comes with an inbuilt XML-RPC server. By default, it occupies the port 7070 in PMP Secondary installation. If you want to change it to some other desired value, you may do so as explained below:

1. Stop PMP Primary Server
2. Connect to PMP Secondary's Web-Inteface
3. Go to "Admin >> General >> Password Management API >> XML-RPC"
4. Change the XML-RPC port, if you want to (by default it occupies 7070)

5. Click "Save"
6. Restart PMP Secondary Server for this change to take effect

Also, specify the new port in 'JAVA_API.conf' against the textfield "SecondaryServerPort".

SecondaryServerPort=<This represents XML-RPC server's port in PMP Secondary installation. By default, it occupies 7070>

Step 2

If you are using self-signed certificate or using your own certificate, you need to import the SSL root certificate in PMP Secondary Server by following the steps as explained in one of the sections above. (If you are using a certificate signed by a third-party CA, you need not carry out any specific configuration for accessing secondary server when primary is down. Everything is automatically taken care of).

Once the above configuration is done, password access in high availability mode will be seamless. However, as write operations are not permitted when Primary Server is down, applications would only be able to RETRIEVE passwords. They will not be allowed to carry out password reset and resource/account creation.

RESTful API

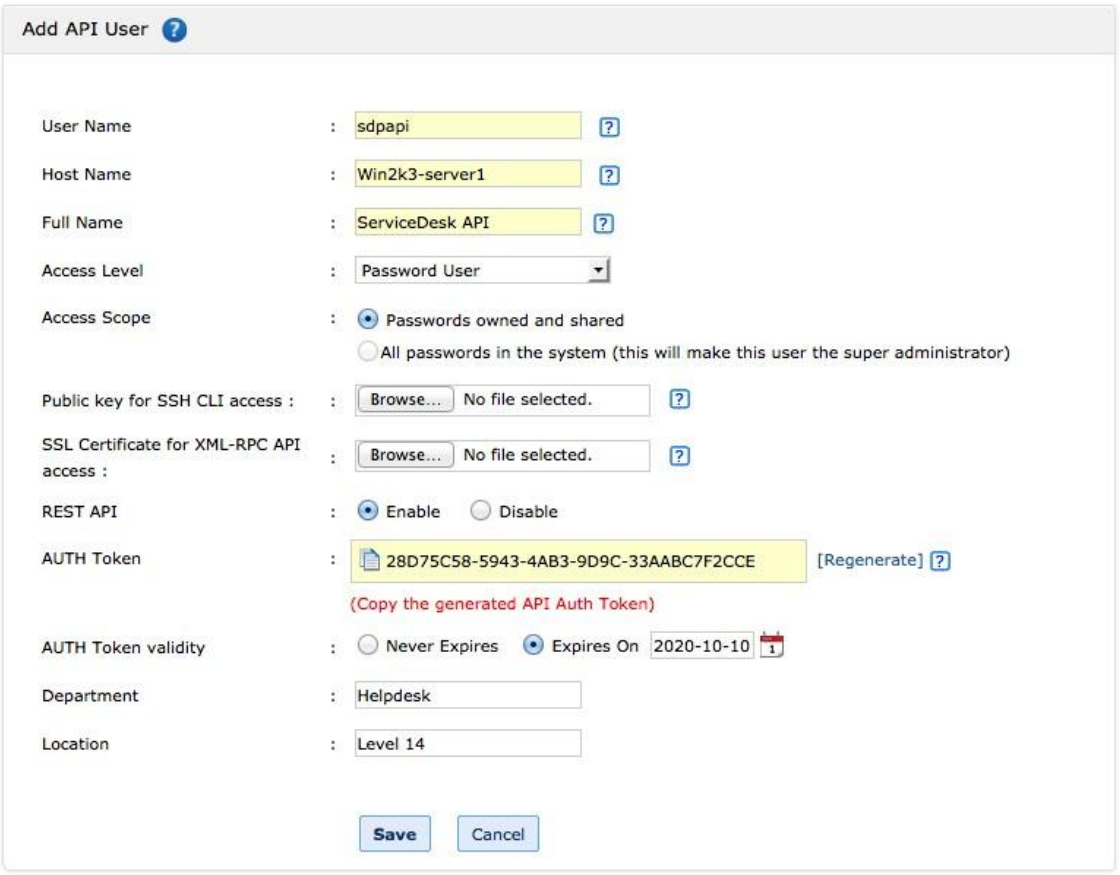
(Feature available only in Enterprise Edition)

PMP APIs allow any application to connect, interact and integrate with Password Manager Pro directly. The APIs belong to the REpresentational State Transfer (REST) category and allow you to add resources, accounts, retrieve passwords, retrieve resource/account details and update passwords programmatically.

Prerequisites

Create API User Accounts in PMP

This is the first step in the process to configure and use Password Management APIs for Application-to-Application Password Management. As mentioned above, user accounts have to be created in PMP to those who will use only the Password Management API. Every API user account should be attached to a single endpoint (server or desktop from where the API is used, so the user accounts are uniquely identified – for example, as user@hostname)



1. Click "Add API User" button in "Admin >> Users" tab
2. In the "Add API User" UI that opens up, enter the 'User Name' in the respective text field.
3. Enter the name of the host from where the API user would access PMP for password management operations.
4. 'Full Name' refers to the name with which the API user would be identified in the external world. That means, in reports, audit trails and such other places where activities are traced to users.
5. Select an appropriate access level for the API user being added - Administrator/Password Administrator/Password User
6. If you are adding a user as "Administrator" or "Password Administrator", you can specify the 'Access Scope'. If you select the option, "Passwords Owned and Shared", the administrator/password administrator will be able to view the passwords owned by them and those shared to them by others. You can choose to make the administrator/password administrator a super administrator, you need to select the option "All Passwords in the System". When you do so, the administrator or the password administrator will be able to access all passwords in PMP without any restriction.
7. Leave the options "Public key for SSH CLI access" and "SSL Certificate for XML-RPC API access"
8. Enable REST API by clicking the button "Enable" beside REST API
9. Once you do this, you will see a text box for the API key. Click "Generate" to generate the API key. The API key is the Auth Token for your access purposes. Copy down this key and store it in some secure location for your future reference. This key will be displayed in the GUI only once and it will not be shown. If you ever lose this key, you need to come back to this GUI and regenerate the key.
10. You can set validity period for the API key - you can choose the option "Never Expires" if you want the key to be valid for ever. Otherwise, specify a validity date.

Important Note

The API User creation is specific to the host from where the application would contact PMP for passwords. That means, user and host are tied with other. If you want to make use of Password Management API from more than one host, you need to create as many API users as the number of hosts. Conversely, if you wish to have many users on a single host, then again you need to create as many API users as needed.

APIs summary

PMP provides a total of seven APIs:

1. To GET the resources owned and shared to a user
2. To GET the accounts that are part of a resource
3. To GET details of an account
4. To GET the password of an account that is part of a resource
5. To change the password of an account
6. To create a new resource
7. To GET the ID of an account of a resource
8. To DELETE a Resource in PMP
9. To GET the list of Password Requests
10. To Request Password Approval by the Admin
11. To Reject a Password Request
12. To Approve a Password Request
13. To Check-in Password Approved by Admin
14. To Checkout the Password approved by the Admin
15. To create a new User

GET
To fetch resources, accounts, passwords, account/resource details

PUT
To change a password

POST
To create new resource and accounts

How to make use of the APIs?

Invoking the APIs

The APIs can be via HTTP POST, GET and PUT requests. All parameters in the request should be form-urlencoded. For all the APIs you need to pass AUTH token, which is mandatory.

Supported Format

PMP supports JSON format and the URL structure for would be as below:
https://<Host-Name-of-PMP-Server OR IP address>:7272/restapi/json/v1/resources/<Resource ID>/accounts/<Account ID>?AUTHTOKEN=(The token you have generated and copied from the GUI)
1.To GET the resources owned and shared to a user

Description:
Used to get the list of resources which are owned/shared to an API user

URL
https://<Host-Name-of-PMP-Server OR IP address>:7272/restapi/json/v1/resources?AUTHTOKEN=(The token you have generated and copied from the GUI)

HTTP METHOD:
GET

Input Data:
None

Sample Requests
curl -k https://192.168.xx.xx:7272/restapi/json/v1/resources?AUTHTOKEN=B9A1809A-5BF7-4459-9ED2-8D4F499CB902

Sample Output
In the output (as shown in the sample below), you will get all the resources owned and shared by the specific API user.


```
{
 "operation":{
  "name":"GET RESOURCES",
  "result":{
   "status":"Success",
   "message":"Resources fetched successfully"
  },
  "totalRows":3,
  "Details":[
   {
    "RESOURCE DESCRIPTION":"CentOS Machine",
    "RESOURCE NAME":"CentOS Machine",
    "RESOURCE ID":"301",
    "RESOURCE TYPE":"Linux",
    "NOOFACCOUNTS":"3"
   },
   {
    "RESOURCE DESCRIPTION":"Cisco IOS Device",
    "RESOURCE NAME":"Cisco IOS Device",
    "RESOURCE ID":"302",
    "RESOURCE TYPE":"Cisco IOS",
    "NOOFACCOUNTS":"2"
   },
   {
    "RESOURCE DESCRIPTION":"Weblogic Data Source Password",
    "RESOURCE NAME":"MSSQL Server",
    "RESOURCE ID":"303",
    "RESOURCE TYPE":"MS SQL Server",
    "NOOFACCOUNTS":"2"
   }
  ]
 }
}
```

2.To GET the accounts that are part of a resource

Description

To get the list of accounts and resource details present in the resource. Resource ID can be obtained from the GET RESOURCES API (explained above).
URL

```
https://<Host-Name-of-PMP-Server OR IP address>:7272/restapi/json
/v1/resources/<Resource ID>/accounts?AUTHTOKEN=(The token you have generated and
copied from the GUI)
```

HTTP METHOD:

GET

Input Data:

None

Sample Requests

```
curl -k
https://192.168.xx.xx:7272/restapi/json/v1/resources/303/accounts?AUTHTOKEN=B9A180 9A-
5BF7-4459-9ED2-8D4F499CB902
```

Sample Output

In the output (as shown in the sample below), you will get all the resources owned and shared by the specific API user.

```
{
 "operation":{
  "name":"GET RESOURCE ACCOUNTLIST",
  "result":{
   "status":"Success",
   "message":"Resource details with account list fetched successfully"
  },
  "Details":{
   "RESOURCE ID":"303",
   "RESOURCE NAME":"MSSQL Server",
   "RESOURCE DESCRIPTION":"Weblogic Data Source Password",
   "RESOURCE TYPE":"MS SQL Server",
   "DNS NAME":"sqlserver-1",
   "PASSWORD POLICY":"Strong",
   "DEPARTMENT":"SQL Server DBA",
   "LOCATION":"Level 10",
   "RESOURCE URL":"http://sqlserver-1/",
   "RESOURCE OWNER":"admin",
   "CUSTOM FIELD":[
    {
     "CUSTOMFIELDVALUE":"78736298",
     "CUSTOMFIELDTYPE":"Numeric",
     "CUSTOMFIELDLABEL":"License No",
     "CUSTOMFIELDCOLUMNNAME":"COLUMN_LONG1"
    },
    {
     "CUSTOMFIELDVALUE":"Sep 10, 2013",
     "CUSTOMFIELDTYPE":"Date",
     "CUSTOMFIELDLABEL":"Installed Date",
     "CUSTOMFIELDCOLUMNNAME":"COLUMN_DATE1"
    },
    {
     "CUSTOMFIELDVALUE":"Test123$%^%",
     "CUSTOMFIELDTYPE":"Password",
     "CUSTOMFIELDLABEL":"Resource Password",
     "CUSTOMFIELDCOLUMNNAME":"COLUMN_SCHAR1"
    },
    {
     "CUSTOMFIELDVALUE":"YES",
     "CUSTOMFIELDTYPE":"Character",
     "CUSTOMFIELDLABEL":"Secure Resource",
     "CUSTOMFIELDCOLUMNNAME":"COLUMN_CHAR1"
    }
   ],
   "ACCOUNT LIST":[
    {
     "ISFAVPASS":"false",
     "ACCOUNT NAME":"sysdba",
     "PASSWDID":"308",
     "PASSWORD STATUS":"[In Use]",
     "ACCOUNT ID":"308"
    },
    {
     "ISFAVPASS":"false",
     "ACCOUNT NAME":"system",
     "PASSWDID":"307",
     "PASSWORD STATUS":"****",
     "ACCOUNT ID":"307"
    }
   ]
  }
 }
}
```

Note: If password access control had been enabled AND If the password status is 'IN USE', you will see the output as [In use].

3.To GET details of an account

Description

To get the details of an account that is part of a resource. You need to pass both Resource ID and Account ID to fetch the required details.

URL

https://<Host-Name-of-PMP-Server OR IP address>:7272/restapi/json/v1/resources/<Resource ID>/accounts/<Account ID>?AUTHTOKEN=(The token you have generated and copied from the GUI)

HTTP METHOD:

GET

Input Data:

None

Sample Requests

```
curl -k
https://192.168.xx.xx:7272/restapi/json/v1/resources/303/accounts/307?AUTHTOKEN=B9A1809A-5BF7-4459-9ED2-8D4F499CB902
```

Sample Output


```
{
 "operation":{
  "name":"GET RESOURCE ACCOUNT DETAILS",
  "result":{
   "status":"Success",
   "message":"Account details fetched successfully"
  },
  "Details":{
   "DESCRIPTION":"",
   "LAST ACCESSED TIME":"N/A",
   "LAST MODIFIED TIME":"Sep 10, 2013 03:33 PM",
   "PASSWORD STATUS":"****",
   "PASSWDID":"307",
   "CUSTOM FIELD":[
    {
     "CUSTOMFIELDVALUE":"5645567",
     "CUSTOMFIELDTYPE":"Numeric",
     "CUSTOMFIELDLABEL":"Account Lic Number",
     "CUSTOMFIELDCOLUMNNAME":"COLUMN_LONG1"
    },
    {
     "CUSTOMFIELDVALUE":"Sep 10, 2013",
     "CUSTOMFIELDTYPE":"Date",
     "CUSTOMFIELDLABEL":"Acc Creation Date",
     "CUSTOMFIELDCOLUMNNAME":"COLUMN_DATE1"
    },
    {
     "CUSTOMFIELDVALUE":"Test12345",
     "CUSTOMFIELDTYPE":"Password",
     "CUSTOMFIELDLABEL":"Secondary Password",
     "CUSTOMFIELDCOLUMNNAME":"COLUMN_SCHAR1"
    },
    {
     "CUSTOMFIELDVALUE":"YES",
     "CUSTOMFIELDTYPE":"Character",
     "CUSTOMFIELDLABEL":"Secure Account",
     "CUSTOMFIELDCOLUMNNAME":"COLUMN_CHAR1"
    }
   ]
  }
 }
}
```


4.To GET the password of an account that is part of a resource

Description

To get the password of an account that is part of a resource. You need to pass both Resource ID and Account ID to fetch the required details.

URL

```
https://<Host-Name-of-PMP-Server OR IP address>:7272/restapi/json/v1/resources/<Resource ID>/accounts/<Account ID>/password?AUTHTOKEN=(The token you have generated and copied from the GUI)
```

HTTP METHOD:

GET

Input Data:

In case, the setting at your end demands a reason to be supplied for retrieving a password, you need to pass the following details as input. If the ticketing system is enabled, you need to pass ticket ID for validation

```
INPUT_DATA={"operation":{"Details":{"REASON":"Need the password to Login Windows Server","TICKETID":"7"}}}
```

Sample Requests

```
curl -k https://192.168.xx.xx:7272/restapi/json/v1/resources/303/accounts/307/password?AUTHTOKEN=B9A1809A-5BF7-4459-9ED2-8D4F499CB902
```

```
curl -X GET -k -H "Content-Type: text/json" --url 'https://192.168.xx.xx:7272/restapi/json/v1/resources/303/accounts/307/password?AUTHTOKEN=B9A1809A-5BF7-4459-9ED2-8D4F499CB902&INPUT_DATA=\{"operation":\{"Details":\{"REASON":"Need the password to Login Windows Server","TICKETID":"7"\}\}\}'
```

Sample Output

```
{
 "operation":{
"name":"GET PASSWORD",
  "result":{
   "status":"Success",
   "message":"Password fetched successfully"
  },
  "Details":{
   "PASSWORD":"fqxdB7^)4"
  }
 }
}
```

Note :If there occurs any problem on retrieving password, the reason will be displayed as part of message.

5.To change the password of an account

Description

To change the password of an account that is part of a resource. You need to pass both Resource ID and Account ID to fetch the required details. If the ticketing system is enabled, you need to pass ticket ID for validation

URL

https://<Host-Name-of-PMP-Server OR IP address>:7272/restapi/json/v1/resources/<Resource ID>/accounts/<Account ID>/password?AUTHTOKEN=(The token you have generated and copied from the GUI)

HTTP METHOD:

PUT

Input Data:

You need to pass input data such as new password, reset type and reason. Reset type should be either LOCAL or REMOTE.

```
      INPUT_DATA={
  "operation":{
    "Details":{
      "NEWPASSWORD":"Test@12345$",
      "RESETTYPE":"LOCAL",
      "REASON":"Password Expired"
      "TICKETID":"7"
    }
  }
}
```

Sample Requests

```
curl -X PUT -k -H "Content-Type: text/json" --url
https://192.168.xx.xx:7272/restapi/json/v1/resources/303/accounts/307/password?AUTHT
OKEN=B9A1809A-5BF7-4459-9ED2-8D4F499CB902 -d
INPUT_DATA=\{"operation":\{"Details":\{"NEWPASSWORD":"Test12345$","RESETTYPE":"L
OCAL","REASON":"test","TICKETID":"7"\}\}\}
```

Sample Output

```
{
 "operation":{
  "name":"CHANGE PASSWORD",
  "result":{
   "status":"Success",
   "message":"Password changed successfully"
  }
 }
}
```

Note :If there occurs any problem on changing password, the reason will be displayed as part of message.

6.To create a new resource

Description

To create a new resource in PMP

Input Data:

You need to pass input data such as name of the resource, account name, resource type, password, URL, description, notes and any other additional fields at the resource and account levels. You can add as many as 40 custom fields (20 each at resource and account levels). Of these, resource name, account name, resource type and password are mandatory.

```
      INPUT_DATA={
  "operation":{
    "Details":{
```

```
        "RESOURCENAME":"Windows Server",
        "ACCOUNTNAME":"Administrator",
        "RESOURCETYPE":"Windows",
        "PASSWORD":"Test123#@!",
        "NOTES":"Testing API",
        "RESOURCEURL":"http://windowsserver/adminconsole",
        "RESOURCECUSTOMFIELD":[
          {
            "CUSTOMLABEL":"Secure Resource",
            "CUSTOMVALUE":"YES"
          }
        ]
      }
    }
}
```

URL

```
https://<Host-Name-of-PMP-Server OR IP address>:7272/restapi/json/v1/resources?AUTHTOKEN=(The token you have generated and copied from the GUI)
```

HTTP METHOD:

POST

Sample Requests

```
curl -X POST -k -H "Content-Type: text/json" 'https://192.168.39.29:7272/restapi/json/v1/resources?AUTHTOKEN=B9A1809A-5BF 7-4459-9ED2-8D4F499CB902' -d 'INPUT_DATA={"operation":{"Details":{"RESOURCENAME":"Windows Server","ACCOUNTNAME":"Administrator","RESOURCETYPE":"Windows","PASSWORD" :"Test123#@!","NOTES":"Testing API","RESOURCEURL":"http://windowsserver/adminconsole","RESOURCECUSTOMFIEL D":[{"CUSTOMLABEL":"Secure Resource","CUSTOMVALUE":"YES"}]}}}'
```

Sample Output

```
{
 "operation":{
  "name":"CREATE RESOURCE",
  "result":{
   "status":"Success",
   "message":"Resource Windows Server has been added successfully"
  }
 }
```

7.To GET the ID of an account of a resource

Description

To get the ID of an account of a resource in PMP. You need to pass the name of the resource and account in the URL/

URL

```
https://<Host-Name-of-PMP-Server OR IP address>:7272/restapi/json/v1/resources/resourcename/<Resource Name>/accounts/accountname/<Account Name>?AUTHTOKEN=(The token you have generated and copied from the GUI)
```

HTTP METHOD:

GET

Input Data:

None

Sample Requests

```
curl -k https://192.168.xx.xx:7272/restapi/json/v1/resources/resourcename/MSSQLServer/accounts/accountname/system?AUTHTOKEN=B9A1809A-5BF7-4459-9ED2-8D4F499CB902
```

Sample Output

```
{
 "operation":{
  "name":"GET_RESOURCEACCOUNTNAME",
  "result":{
   "status":"Success",
   "message":"Resource id and account id fetched successfully for the given resource
name"
  },
  "Details":{
   "RESOURCEID":"303",
   "ACCOUNTID":"307"
  }
 }
}
```

8.To DELETE a Resource in PMP:

Description

To delete a resource for the given resource ID. Resource ID can be obtained from the GET RESOURCES API (explained above).

URL

```
https://<Host-Name-of-PMP-Server OR IP
address>:7272/restapi/json/v1/resources/{resourceid}?AUTHTOKEN=(The token you have
generated and copied from the GUI)
```

HTTP METHOD:

DELETE

Input Data :

None

Sample Requests

```
curl -X POST -k -H "Content-Type: text/json"
https://192.168.xx.xx:7272/restapi/json/v1/resources/307?AUTHTOKEN=iddPyMeUOnv9hu
R%2BzLfan1GbB4VYZ4%2F7UDHfbpY8socCJ7C1%2BVUyhjtcRHlysShHeLf9va63EEkt%0A4x
%2FG42EYLQ%3D%3D
```

Sample Output

```
{
"operation":{
"name":"DELETE RESOURCE"
"result":{"status":"Success"
"message":"Resources deleted successfully."}
}
}
```

9.To GET the list of Password Requests

Description

Method to get the list of password requests to be approved/rejected by the admin logged in.

URL

```
https://<Host-Name-of-PMP-Server OR IP
address>:7272/restapi/json/v1/accounts/passwordaccessrequests?AUTHTOKEN=(The token
you have generated and copied from the GUI)
```

HTTP METHOD:

GET

Input Data :

None

Sample Requests

```
curl -k
https://192.168.xx.xx:7272/restapi/json/v1/accounts/passwordaccessrequests?AUTHTOKE
```

```
N=iddPyMeUOnv9huR%2BzLfan1GbB4VYZ4%2F7UDHfbpY8socCJ7C1%2BVUyhjtcRHlysShHe
Lf9va63EEkt%0A4x%2FG42EYLQ%3D%3D
```

Sample Output

```
{
"operation":{
            "name":"GET_PASSWORDREQUEST"

            "result":{
                    "status"    :   "Success"
                    "message" : "Password Request fetched successfully"
                   }

             "Details":{
                       "REQUESTER USERID" : "2"
                       "REQUESTED BY" : "guest"
                       "REQUESTED BY FULLNAME" : "Guest guest"
                       "PASSWORDREQUESTLIST" : [

                          {
                           "ACCOUNT ID"  :  "1"
                           "ACCOUNT NAME" : "ACCOUNT1"
                           "RESOURCE ID":"1"
                           "RESOURCE NAME":"apt-server1"
                           "PASSWD ID" : "1"
                           "STATUS":""
                           "REQUESTED TIME":"Nov 27
                           "REASON" : "For connecting the machine and update the pmp
server".
                          }

                                 {
                                  "ACCOUNT ID"  :  "2"
                                  "ACCOUNT NAME" : "ACCOUNT2"
                                  "RESOURCE ID":"2"
                                  "RESOURCE NAME":"apt-server2"
                                  "PASSWD ID" : "2"
                                  "STATUS":""
                                  "REQUESTED TIME":"Nov 28
```

```
                                "REASON" : "For connecting the machine and update the pmp
server".
                            }

                        ]

                }

            }

}
```

10.To Request Password Approval by the Admin:

Description

Method to request the admin for password access approval. The account id has to be passed for the same in the URL.

URL

```
https://<Host-Name-of-PMP-Server OR IP
address>:7272/restapi/json/v1/accounts/{accountid}/requestpassword?AUTHTOKEN=(The
token you have generated and copied from the GUI)
```

HTTP METHOD:

POST

Input Data:

In case the setting at your end demands a reason to be supplied for requesting a password, you need to pass the following details as input. If the ticketing system is enabled, you need to pass ticket ID for validation

Sample Input

```
INPUT_DATA= { "operation" : { "Details" : { "REASON" : "Testing", "TICKETID" : "7"}}}
```

Sample Requests

```
curl -X POST -k -H "Content-Type: text/json"
https://192.168.xx.xx:7272/restapi/json/v1/accounts/7/requestpassword?INPUT_DATA= {
"operation" : { "Details" : { "REASON" : "Testing", "TICKETID" :
"7"}}}&AUTHTOKEN=iddPyMeUOnv9huR%2BzLfan1GbB4VYZ4%2F7UDHfbpY8socCJ7C1%2
BVUyhjtcRHlysShHeLf9va63EEkt%0A4x%2FG42EYLQ%3D%3D
```

Sample Output

```
{
"operation":{

        "name":"REQUEST_PASSWORD"  ,

        "result":{
                "status": "Success"    ,
                "message":"Request to view password have been raised successfully"
               },

        "Details":{
                 "STATUS" : "WAITING FOR APPROVAL / CHECKOUT" ;
                 }

      }

}
```

11.To Reject a Password Request

Description

Method for the admin to reject the password requests. This requires the account ID and requester ID to be passed in the URL.

URL

```
https://<Host-Name-of-PMP-Server OR IP
address>:7272/restapi/json/v1/accounts/{accountid}/requester/{requesterid}/reject?AUTH
TOKEN=(Theoken you have generated and copied from the GUI)
```

HTTP METHOD:

POST

Input Data :

None

Note: Requester ID is the same as the ID of the user who has requested the password. REQUESTEDID can be obtained from the GET PASSWORDREQUEST API(REQUESTER USERID).

Sample Requests

```
curl -X POST -k -H "Content-Type: text/json"
https://192.168.xx.xx:7272/restapi/json/v1/accounts/7/requester/34/reject?AUTHTOKEN=i
ddPyMeUOnv9huR%2BzLfan1GbB4VYZ4%2F7UDHfbpY8socCJ7C1%2BVUyhjtcRHlysShHeLf9
va63EEkt%0A4x%2FG42EYLQ%3D%3D
```

Sample Output

```
{
"operation":{
            "name" : "ADMIN_REQUEST_REJECT"
            "result" : {

                        "status"    :     "Success"
                        "message" : "Password Rejected successfully"
                       }

          }

}
```

12.To Approve a Password Request

Description

Method for the admin to approve the password requests. Here, the account ID and the Requester ID are required to be passed in the URL.

URL

```
https://<Host-Name-of-PMP-Server OR IP address>:7272/restapi/json/v1/accounts/{accountid}/requester/{requesterid}/approve?AUTHTOKEN=(The token you have generated and copied from the GUI)
```

HTTP METHOD:

POST

Input Data :

None

Note : Requester ID is the same as the ID of the user who has requested the password. REQUESTEDID can be obtained from the GET PASSWORDREQUEST API(REQUESTER USERID).

Sample Requests

```
curl -X POST -k -H "Content-Type: text/json" https://192.168.xx.xx:7272/restapi/json/v1/accounts/7/requester/34/approve?AUTHTOKEN=iddPyMeUOnv9huR%2BzLfan1GbB4VYZ4%2F7UDHfbpY8socCJ7C1%2BVUyhjtcRHlysShHeLf9va63EEkt%0A4x%2FG42EYLQ%3D%3D
```

Sample Output

```
{
"operation" : {

            "name" : "ADMIN_REQUEST_APPROVE"

            "result" : {
                        "status"    :     "Success"
```

```
                "message" : "Password Approved successfully"
                }

        }

}
```

13.To Check-in Password Approved by Admin

Description

Method to check-in the password approved by the admin. The account and requester IDs have to passed in the URL for the same.

URL

```
https://<Host-Name-of-PMP-Server OR IP address>:7272/restapi/json/v1/accounts/{accountid}/requester/{requesterid}/checkin?AUTHTOKEN=(The token you have generated and copied from the GUI)
```

HTTP METHOD:

POST

Input Data :

None

Note: Requester ID is the same as the ID of the user who has requested the password. REQUESTEDID can be obtained from the GET PASSWORDREQUEST API(REQUESTER USERID).

Sample Requests

```
curl -X POST -k -H "Content-Type: text/json" https://192.168.xx.xx:7272/restapi/json/v1/accounts/7/requester/34/checkin?AUTHTOKEN=iddPyMeUOnv9huR%2BzLfan1GbB4VYZ4%2F7UDHfbpY8socCJ7C1%2BVUyhjtcRHlysShHeLf9va63EEkt%0A4x%2FG42EYLQ%3D%3D
```

Sample Output

```
{
```

```
 "operation" : {

            "name" : "ADMIN_REQUEST_CHECKIN"

            "result" : {
                    "status"    :    "Success"
                      "message" : "Password have been checked in successfully"
                      }

            }

}
```

14. To Checkout the Password approved by the Admin

Description
Method to checkout the password after being approved by the admin after request. The account ID had to be passed for the same in the URL.
URL

```
https://<Host-Name-of-PMP-Server OR IP
address>:7272/restapi/json/v1/accounts/{accountid}/checkout?AUTHTOKEN=<token>&IN
PUT_DATA=<json>
```

HTTP METHOD:

POST

Input Data

On account of customized settings that demand reason for password checkout, you need to pass the following as input.

Sample Input

```
{
"operation"    :    {
           "Details":    {
                        "REASON":"N/A"
```

```
                    }
            }
}
```

Sample Requests

```
curl -X POST -k -H "Content-Type: text/json"
https://192.168.xx.xx:7272/restapi/json/v1/accounts/7/checkout?INPUT_DATA= {
"operation" : { "Details" : { "REASON" :
"N/A"}}}&AUTHTOKEN=iddPyMeUOnv9huR%2BzLfan1GbB4VYZ4%2F7UDHfbpY8socCJ7C1
%2BVUyhjtcRHlysShHeLf9va63EEkt%0A4x%2FG42EYLQ%3D%3D
```

Sample Output

```
{
"operation" : {
            "name" : "REQUEST_CHECKOUT"

            "result" : {
                        "status" : "Success"
                              "message" : "Password have been checked out successfully"
                        }

             "Details":

                        {
                           "STATUS" : "***** [checkIn]"
                        }
            }

}
```

15.To create a new User

Description

Method to add an user

URL

https://severname:port/restapi/json/v1/user?AUTHTOKEN=<token>&INPUT_DATA=<json>

HTTP METHOD:

POST

Input Data (Optional Inputs are given in Grey)

```
{
   "operation": {
      "Details": {
       "USERNAME": "jason"
       "FIRSTNAME": "Jason"
       "LASTNAME": "Thomas"
       "EMAIL": "jason@opmanager.com"
       "PASSWORD":"Pa55w0Rd123"
       "POLICY": "Strong"
       "ROLE": "Administrator|Password Administrator|Password Auditor|Password User"
       "ISSUPERADMIN": "true|false",
       "DEPARTMENT": "NOC",
       "LOCATION": "Level 10 - South Wing",
       "ENABLEMOBILEACCESS": "true|false",
       "LANDLINE_COUNTRYCODE": "+1",
       "LANDLINE": "925-965-9647",
       "LANDLINE_EXT": "4675",
       "MOBILE_COUNTRYCODE": "+1",
       "MOBILE": "925-965-9648",
       "PHONEFACTOR_USERNAME": "jason1",
       "RSAUSERNAME": "jason2",
       "ENABLETWOFACTOR": "true|false",
       "PRIMARYCONTACT": "landline|mobile"
      }

   }
}
```

Sample Output

```
{
        "operation":{"name":"CREATE_USER",
        "result":{"status":"Success",
        "message":"User Created Successfully"
                }
           }
}
```

Rebranding PMP

If you want to replace the PMP logo appearing on the login screen and on the web-interface with that of yours, you can do so from the web-interface itself. It is preferable to have your logo of the size 210 * 50 pixels.

To rebrand the logo,

- Go to the "Admin" tab
- Click "Customize >> Rebrand"
- Browse and choose the required image
- Click "Save"
-

TThe PMP will appear with rebranded look

Configuring Legal Banner in Login Page

PMP provides the option to configure a legal banner in the PMP login page. If you want your users to accept certain terms and conditions before logging into PMP, you may configure and enable this option. At any point, this legal banner can be disabled.

You can specify the 'Display Label' for the legal banner, the text to be displayed as the 'Acceptance Button' and also the detailed legal content that has to displayed upon clicking the legal banner link.

After specifying these, you can save the settings. Once this is done, from the next login onwards, these settings will be shown in the login page.

Note: Only whe the legal content text box is filled, legal banner will be shown in the Login Page. If this field is left empty, legal banner will be disabled.

Displaying Messages to PMP Users

If you want to display a common message to all PMP administrators or users, you can do so from PMP. The 'Message Board' feature helps achieve this. For example, to do maintenance you decide to down the PMP server for a few hours, you can intimate the decision to all the administrators/users using this feature. The common message entered by you will be displayed to all the users/administrators as you decide.

This feature enables you to display the message as a banner on PMP GUI. In addition, you can choose to send the same message as an email notification. When you choose to display the message as a banner, you have the option to specify the time period up to which the message will remain in force.

To display the message,

- Go to the "Admin" tab
- Click "Users >> Message Board"
- In the text field, enter the common message which you wish to display
- Specify to whom you wish to display the message
- Specify the type of display - online alert or email notification or both
- If you choose online alert, the message will be indicated by the icon  in the PMP GUI. When users click that, the message will be displayed as a banner
- When you choose the option 'Email Notification', PMP will take the respective email ids from the user database and send out mails
- Click "Save"

Email Templates

(Feature available only in Enterprise Edition)

Customizing the Email Notification Content

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. If you want, you can customize the content and have your own content.

To customize the email content,

- Go to the "Admin" tab
- Click "Customize >> Email Templates"

In the UI that opens,

- Select the required category - User Management, Password Management & General Administration
- You can preview the existing email content by clicking the link "Preview"
- If you want to edit the content, click "Edit Template"
- You can specify a customized message in the Subject Line
- You can also modify the body content
- While entering the content of the body, you can specify placeholders for certain values like user name. The exact user name will be replaced with the placeholders at runtime
- Click "Save"

The email notifications of the respective categories will have the new content.

Note 1 : PMP facilitates customizing most of the email content in PMP. However, email notifications on reports and alerts are not customizable.

Note 2 : You can use html tags in your customized message with the restriction that only single quotes be used inside the html tags instead of double quote. For example: instead of , you need to use

Audit & Notifications

As PMP deals with sensitive passwords, it comes with an effective auditing mechanism to record who accessed what resource and when along with trails about every single action performed by the user. All operations performed by users on the GUI are audited with the timestamp and the IP address from where they accessed the application.

- Audit in PMP has been classified into three types:
- Resource Audit - all operations pertaining to resources, resource groups, accounts, passwords, shares and policies
- User Audit - all operations performed in PMP by a 'PMP user' are captured under 'User Audit'
- Task Audit - records of various scheduled tasks created

PMP audit is quite comprehensive and almost all actions are audited. There may be requirements to audit only the specific operations. To facilitate that, within each audit type, PMP provides the flexibility to audit only the required operations. There is also option to send notifications to required recipients whenever a chosen event (audit trail of your choice) occurs in PMP.

Resource Audit

All operations pertaining to 'resources' are captured under 'Resource Audit'.

To view resource audit

Navigate to Audit >> Resource Audit

To record only specific trails in resource audit

Click the icon "Configure Audit" present in the Resource Audit page

In the UI that opens, select the operations for which you want audit records to be generated. Leave the checkbox against all other operations blank

To receive notifications, traps, syslog messages on generation of audit records

If you want to receive notifications, SNMP traps or syslog messages on the occurrence of a particular event, you can select the respective check-boxes against the required

operation (If you choose to receive SNMP traps Before selecting an option here, make sure you have carried out SNMP Trap/Syslog settings)

PMP provides the flexibility of sending separate notifications to each and every occurrence of the desired event. If you do not wish to be flooded with emails, you can choose to receive a single notification every day (containing information about all the events generated on the day) in the form a daily digest

You can also specify the list of recipients list for notifications

Click "Save"

Purging Resource Audit Trails

Almost all operations pertaining to resources performed in PMP are audited and the trails are stored in the database. Naturally, the resource 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

To purge the records that are older than a specified number of days, specify the number in the text-box against the field "Purge Audit Records".

Click "Save". The Resource Audit records that are older than the number of days specified by you, will be purged

Exporting Resource Audit Trails as PDF/CSV Report

The Audit Trails could be exported as a PDF/CSV file. You can store it in a secure location for reference purpose. Click the button "Export to PDF"or "Export to CSV" as required

Resource Audit Filters

You can create customized views for filtering and viewing only those audit records that are of interest to you. For example, in Resource Audit, if you want to filter and view the audit trails for the accounts added for specific resources, you can create a custom filter by specifying your criteria.

To create an audit filter,

- Click the link "Add" present beside 'Manage Custom Filters'

- Select the required column names from the drop-down
- Enter your criteria (If you want to enter operation type as criteria, click the link 'View Operation Types', refer to the list and enter the required name as it is)
- Click "Save"

User Audit

All operations performed in PMP by a 'PMP user' are captured under 'User Audit'.

To view user audit

- Navigate to Audit >> User Audit

To record only specific trails in user audit

- Click the icon "Configure Audit" present in the User Audit page
- In the UI that opens, select the operations for which you want audit records to be generated. Leave the checkbox against all other operations blank

To receive notifications on generation of audit records

- If you want to receive notifications, SNMP traps or syslog messages on the occurrence of a particular event, you can select the respective check-boxes against the required operation (If you choose to receive SNMP traps Before selecting an option here, make sure you have carried out SNMP Trap/Syslog settings)
- PMP provides the flexibility of sending separate notifications to each and every occurrence of the desired event. If you do not wish to be flooded with emails, you can choose to receive a single notification every day (containing information about all the events generated on the day) in the form a daily digest
- You can also specify the list of recipients list for notifications
- Click "Save"

Purging User Audit Trails

- Almost all operations performed by a user are audited and the trails are stored in the database. Naturally, the user 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
- To purge the records that are older than a specified number of days, specify the

number in the text-box against the field "Purge Audit Records".
- Click "Save". The Resource Audit records that are older than the number of days specified by you, will be deleted from the database once and for all

Exporting User Audit Trails as PDF/CSV Report

- The Audit Trails could be exported as a PDF/CSV file. You can store it in a secure location for reference purpose. Click the button "Export to PDF"or "Export to CSV" as required

User Audit Filters

You can create customized views for filtering and viewing only those audit records that are of interest to you. For example, in User Audit, if you want to filter and view the audit trails for the accounts added for specific resources, you can create a custom filter by specifying your criteria.

To create an audit filter,

- Click the link "Add" present beside 'Manage Custom Filters'
- Select the required column names from the drop-down
- Enter your criteria (If you want to enter operation type as criteria, click the link 'View Operation Types', refer to the list and enter the required name as it is)
- Click "Save"

Task Audit

Records of various scheduled tasks created and executed in PMP are captured as part of task audit.

To view user audit

- Navigate to Audit >> Task Audit

To record only specific trails in resource audit

- Click the icon "Configure Audit" present in the Task Audit page
- In the UI that opens, select the operations for which you want audit records to be

generated. Leave the checkbox against all other operations blank

To receive notifications on generation of audit records

- If you want to receive notifications, SNMP traps or syslog messages on the occurrence of a particular event, you can select the respective check-boxes against the required operation (If you choose to receive SNMP traps Before selecting an option here, make sure you have carried out SNMP Trap/Syslog settings)
- PMP provides the flexibility of sending separate notifications to each and every occurrence of the desired event. If you do not wish to be flooded with emails, you can choose to receive a single notification every day (containing information about all the events generated on the day) in the form a daily digest
- You can also specify the list of recipients list for notifications
- Click "Save"

Purging Task Audit Trails

- Almost all operations performed by a user are audited and the trails are stored in the database. Naturally, the user 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
- To purge the records that are older than a specified number of days, specify the number in the text-box against the field "Purge Audit Records"
- Click "Save". The Task Audit records that are older than the number of days specified by you, will be deleted from the database once and for all

Exporting Task Audit Trails as PDF/CSV Report

- The Audit Trails could be exported as a PDF/CSV file. You can store it in a secure location for reference purpose. Click the button "Export to PDF"or "Export to CSV" as required

Task Audit Filters

You can create customized views for filtering and viewing only those audit records that are of interest to you. For example, in Task Audit, if you want to filter and view the audit trails for the database backup schedules created by specific users, you can create a custom filter by specifying your criteria.

To create an audit filter,

- Click the link "Add" present beside 'Manage Custom Filters'
- Select the required column names from the drop-down
- Enter your criteria (If you want to enter operation type as criteria, click the link 'View Operation Types', refer to the list and enter the required name as it is)
- Click "Save"

- Does PMP record Password viewing attempts and retrievals by users?
  Yes, PMP records all operations performed by the user including the password viewing and copying operations. From audit trails, you can get a comprehensive list of all the actions and attempts by the users with password retrieval. The list of operations that are audited (with the timestamp and the IP address) includes:
  - User accounts created, deleted and modified
  - Users logging in and logging off the application
  - Resources and passwords created, accessed, modified and deleted

How are the audit logs protected against modification?

All the audit records are stored in the MySQL database. To ensure security, the MySQL server has been configured not to accept connections from remote hosts. In addition, the password to access the MySQL server is randomly generated for every PMP installation. So, unless people gain entry into the database, the audit records cannot be modified.

Reports

(Feature available only in Premium and Enterprise Editions)

Contents

Overview

The information on the entire password management process in your enterprise is presented in the form of comprehensive reports in PMP. The status and summaries of the different activities such as password inventory, policy compliance, password expiry, user activity etc are provided in the form of tables and graphs, which assist the IT administrators to make a well-informed decisions on password management.

Password Manager Pro provides about nine canned reports classified under four types. In addition, there is provision to create custom reports.

Canned Reports

Types of Reports

PMP provides four types of reports –

- Password Reports
- User Reports
- General Reports
- Compliance Reports

Password Reports

All details pertaining to the device properties, hardware properties, firmware details, audit details pertaining to the devices etc have been presented under Network Reports.

To access the Network Reports, just go to the "Reports" tab.

Report Name	What does it Convey	Additional Information
Password Inventory Report	This report provides a snapshot of details about the total number of resources, passwords, resource types and users present in PMP. Besides, it provides details about the ownership of each password/resource and details about the time at which the passwords were accessed. There are three sections in this report: Password Policy Compliance - Summary Report This section lists down the details in summary about the total number of passwords, total number of passwords that comply to the policy and total number of passwords that are non-compliant. Policy Violation by Resource Type This section provides a pie-chart showing the number of passwords that are non-compliant to the defined policy based on the resource type. Password Compliance - Detailed Report This section lists down the compliance details of all the resources (whether they are compliant with the defined policy or not). It also depicts the number of violations in each resource and the ownership details of resources and passwords in tabular form. You can make a search in this report by clicking the icon present at the top-right hand corner of the table.	This report can be generated in the form of PDF and can be emailed to required recipients. Click the links "Export to PDF" and "Email this Report" to do the required operation. Schedule Report
Password Compliance Report	This report provides a snapshot of details about the passwords that comply to the password policy set by the administrator and the ones that do not comply. Besides, it provides details about the ownership of each password. Also, in the case of the passwords which are	This report can be generated in the form of PDF and can be emailed to required recipients. Click the links "Export to PDF" and "Email this Report" to do the required operation.

Report Name	What does it Convey	Additional Information
	found to be non-compliant, details about non-compliance are also provided. This helps in taking the required corrective action immediately to make them compliant. There are three sections in this report: Password Policy Compliance - Summary Report This section lists down the details in summary about the total number of passwords, total number of passwords that comply to the policy and total number of passwords that are non-compliant. Policy Violation by Resource Type This section provides a pie-chart showing the number of passwords that are non-compliant to the defined policy based on the resource type. Password Compliance - Detailed Report This section lists down the compliance details of all the resources (whether they are compliant with the defined policy or not). It also depicts the number of violations in each resource and the ownership details of resources and passwords in tabular form. You can make a search in this report by clicking the icon present at the top-right hand corner of the table.	
Password Expiry Report	This report provides information about the validity details of passwords. In other words, it provides details about the passwords that have expired and the passwords that are valid. There are three sections in this report: Password Expiry - Summary Report This section lists down the details in summary about the total number of	This report can be generated in the form of PDF and can be emailed to required recipients. Click the links "Export to PDF" and "Email this Report" to do the required operation.

Report Name	What does it Convey	Additional Information
	passwords, total number of expired passwords and total number of valid passwords. Password Expiry by Resource Type This section provides a pie-chart showing the number of expired passwords in each resource type. Password Expiry - Detailed Report This section lists down the expiry/validity details of all the resources. It also depicts the number of expired/valid passwords in each resource and the ownership details of resources and passwords in tabular form. You can make a search in this report by clicking the icon present at the top-right hand corner of the table.	
Password Activity Report	This report provides information about the usage details of all passwords in the system. It provides details about the passwords that were most accessed during a specific time period, the ones that were least accessed, average access per day, per week, passwords that were frequently reset etc. There are six sections in this report: Activity Statistics - Summary Report This section lists down the details in summary about the total number of passwords, average access per day/ per week, average password age, the number of passwords for which reset is supported, number of passwords that were reset using agents, number of passwords that were reset without agents, number of failures in password reset etc. Top 10 Passwords Access Count This section provides a graph showing the top 10 passwords that were accessed	This report can be generated in the form of PDF and can be emailed to required recipients. Click the links "Export to PDF" and "Email this Report" to do the required operation.

Report Name	What does it Convey	Additional Information
	most. Top 10 Passwords Reset Count This section provides a graph showing the top 10 passwords that were reset most. Bottom 10 Passwords Access Count This section provides a graph showing the least accessed 10 passwords. Bottom 10 Passwords Reset Count This section provides a graph showing the least reset 10 passwords. Password Activity Details This section provides the following details about the passwords that are in sync with the target systems: Date of creation of the password, number of times the password had been accessed from the date of creation, number of time the password underwent changes, the time at which the password was accessed/changed last, the frequency at which the password is being accessed every day, the frequency at which the password is being changed every week etc. List of resources for which access control workflow has been activated This section lists all the resources for which password access control workflow has been activated List of resources for which access control workflow has been deactivated This section lists all the resources for which password access control workflow has been deactivated List of resources for which access control workflow has not been configured This section lists all the resources for	

Report Name	What does it Convey	Additional Information
	which password access control workflow has not been configured at all	
Password Integrity Report	Passwords of resources such as servers, databases, network devices and other applications are stored in PMP. It is quite possible that someone who have administrative access to these resources could access the resource directly and change the password of the administrative account. In such cases, the password stored in PMP would be outdated and will not be of use to the users who access PMP for the password. PMP provides option for checking the integrity of passwords at any point of time on demand and also at periodic intervals. You can create a scheduled task for carrying out the integrity check at periodic intervals. Click "Schedule Report" and fill-in the details. You can also generate the integrity report at any point of time by clicking the link"Generate Report". When you do so, you will get the results of the automatic integrity check done by PMP at 1 AM every day for all the accounts for which remote synchronization has been enabled. The results of the current day's check done at 1 AM will be depicted in the report. In case, you want to carry out integrity check at any moment on demand to get latest details, you need to click the option "Run Integrity Check". PMP will try to establish connection with the target systems for all the accounts for which remote password reset has been enabled. Once the connection is established, it tries to login with the credentials stores in PMP. If login does not succeed, PMP concludes that the password is out of sync. In case, PMP is not even able to establish connection with the system due to	This report can be generated in the form of PDF and can be emailed to required recipients. Click the links "Export to PDF" and "Email this Report" to do the required operation.

Report Name	What does it Convey	Additional Information
	some network problem, it will not be taken as password out of sync. A consolidated notification would be emailed to all the administrators and auditors. The Password Integrity report provides information if the passwords in the system are in sync with the corresponding passwords in the target systems. There are two sections in this report: LPassword Integrity - Summary Report This section lists down the details in summary about the total number of passwords for which reset is supported, passwords for which reset is done using agents, number of passwords that were reset using agents, number of passwords in the system are in sync with the corresponding passwords in the target systems, number of passwords that are out of sync etc. Password Integrity - Details This section provides details about the integrity status, who carried out password reset, the time at which the reset was done etc.	
Ungrouped Passwords	Passwords stored in PMP are part of resources and the resources can be grouped into resource groups. Certain resources may not be part of any resource group. The passwords belonging to such resources are listed in this report.	
Password Access Control	Provides complete details about the password access control workflow scenario of your organizations. List of resources for which access control has been enabled, resources for which access control is activated/deactivated, resources for which the requests are automatically approved, list of password release	

Report Name	What does it Convey	Additional Information
	requests approved/denied etc are depicted through this report.	

User Reports

Report Name	What does it Convey	Additional Information
User Access Report	This report provides details about all users in the system with reference to password and resource access. This report has three sections: User Statistics - Summary Report This report can be generated in the form of PDF and can be emailed to required recipients. Click the links "Export to PDF" and "Email this Report" to do the required operation. Details such as the number of new users added during the last five days, users deleted, role change, number of invalid login attempts, users who carried out password reset during the past five days, users who did not login during the last five days, total number of users/user groups in the system, user roles etc are presented as part of this report. User Activity Summary Report The actions performed by users on passwords such as password retrieval, password reset etc captured as part of this summary report. This report provides the number of such actions done by each user. Similarly, the number of password actions performed by members of each user group are also depicted. User Access Details The resources and resource groups that are owned by/shared to each user are depicted as part of this report. The privileges allowed for	This report can be generated in the form of PDF and can be emailed to required recipients. Click the links"Export to PDF" and "Email this Report" to do the required operation.

Report Name	What does it Convey	Additional Information
	the user are also listed. User Group Access Details The list of users who are members of the group, resource groups that are owned by/shared to the user group are depicted as part of this report.	
User Activity Report	This report provides details about the password usage of all the users in the system. This report has four sections: Activity Statistics - Summary Report The total number of passwords accessed by users and user groups during a specified time period are depicted in the form of graphs. Top 10 Users - Login/Access/Reset The list of the top 10 users who performed most login attempts, most password access and most password resets. Bottom 10 Users - Login/Access/Reset The list of 10 users who performed least login attempts, least password access and least password resets. User Activity Details All details about users, including the total number of login attempts made, number of invalid attempts, number of passwords accessed, number of passwords reset are depicted.	This report can be generated in the form of PDF and can be emailed to required recipients. Click the links"Export to PDF" and "Email this Report" to do the required operation.

General Reports

Report Name	What does it Convey	Additional Information
Executive Report	This report provides a snapshot of all password access and user activities in the system. It is a combined report of	This report can be generated in the form of PDF and can be emailed to required recipients. Click the links "Export to PDF"and "Email this Report" to do the

Report Name	What does it Convey	Additional Information
	Password and User reports. It provides details, in summary, about the following: Password Statistics, Password Activity, Password Policy, Password Expiry, Password Out of Sync, User Statistics and User Activity.	required operation.

Compliance Report

(Feature available only in Enterprise Edition)

Report Name	What does it Convey	Additional Information
PCI DSS Compliance Report The PCI DSS stands for Payment Card Industry Data Security Standard. It is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. It represents a set of rules that need to be adhered to by businesses that process credit cardholder information, to ensure data is protected. The PCI Data Security Standard is comprised of 12 general requirements designed to: • Build and maintain a secure network • Protect cardholder data • Ensure the maintenance of vulnerability management programs • Implement strong access control measures • Regularly monitor and test networks • Ensure the maintenance of information security policies	This reports the violations in your network from the requirements of Payment Card Industry (PCI) Data Security Standard (DSS), relevant to the use and management practices of shared administrative, software and service account passwords of various systems. PCI DSS requirements 2,3,7,8,10 & 12 are covered in this report. Note: In order to adhere to "all" the requirements of the PCI DSS standard completely, you will need other tools and security procedures to be implemented.	You have the option to generate separate compliance reports for each PCI DSS requirement 2,3,7,8,10 & 12. You can also generate a consolidated PCI DSS report too. This report can be generated in the form of PDF and can be emailed to required recipients. Click the links "Export to PDF" and"Email this Report" to do the required operation.

Report Name	What does it Convey	Additional Information
This standard is governed by PCI Security Standards Council https://www.pcisecuritystandards.org/		

Scheduling Report Generation

All reports can be scheduled to be generated at periodic intervals. The reports thus generated can be sent via email to required recipients. To create a schedule for any report,

- go to "Reports" tab
- click the link "Schedule Report" available under the name of each report
- in the GUI that opens, select the required schedule - every day / every month / only once
- provide the date / time at which the schedule has to commence
- enter the list of email ids to which the report has to be emailed
- click "Schedule".

The result of the scheduled task created here are audited and can be viewed from the "Task Audit" section.

To terminate an already created schedule,

- Click the link "Schedule Report" available under the name of report (for which the schedule has to be terminated)
- In the GUI that opens, select the option "Never"
- Click "Schedule"
- The schedule will be terminated

Custom Reports

(Feature available only in Enterprise Edition)

You can create customized reports out of the four canned reports (Password Inventory, Password Compliance, Password Expiry and Password Integrity) and two audit reports (Resource Audit and User Audit). You can specify certain criteria and create customized reports as per your needs.

The custom reports have been designed to bring out specific information from the PMP database as per your needs. The canned reports provide a snapshot of details in general. On

the other hand, you can create a custom report out of this canned report to get specific details.

For instance, let us take the case of creating a custom report out of Password Inventory Report.

Assume that you want to get a report on the resources owned by 'User A' in 'Network Administration' department. You can create a custom report from the 'Password Inventory Report' by specifying the criteria as Resources from 'Department' 'Network Administration' AND 'Owner' name as 'User A'.

The real power of the custom reports lies in the fact that you can specify criteria expression and cull out information catering to your more specific needs.
Let us take another example to explain this:

Assume that your need is to take a list of all the sensitive passwords belonging to the resource types Windows and Windows Domain, Linux and Cisco, owned by a particular administrator - say John. Also, you want to get details on the share permissions for those passwords - with whom the passwords have been shared.

Here, the following are the conditions:

- Sensitive accounts with names 'administrator' on Windows and Windows Domain, 'root' on Linux and 'enable' on Cisco are to be identified
- Among such accounts, only those that are owned by john are to be identified

So, the criteria will be as follows:

To identify the 'administrator' accounts on Windows/Windows Domain, the criteria is

- Resource Type starts with Windows (take this as column C1)
- Account Name is administrator (take this as column C2)

To identify the 'root' accounts on Linux, the criteria is

- Resource Type is Linux (take this as column C3)
- Account Name is root (take this as column C4)

To identify the 'enable' accounts on Cisco devices, the criteria is

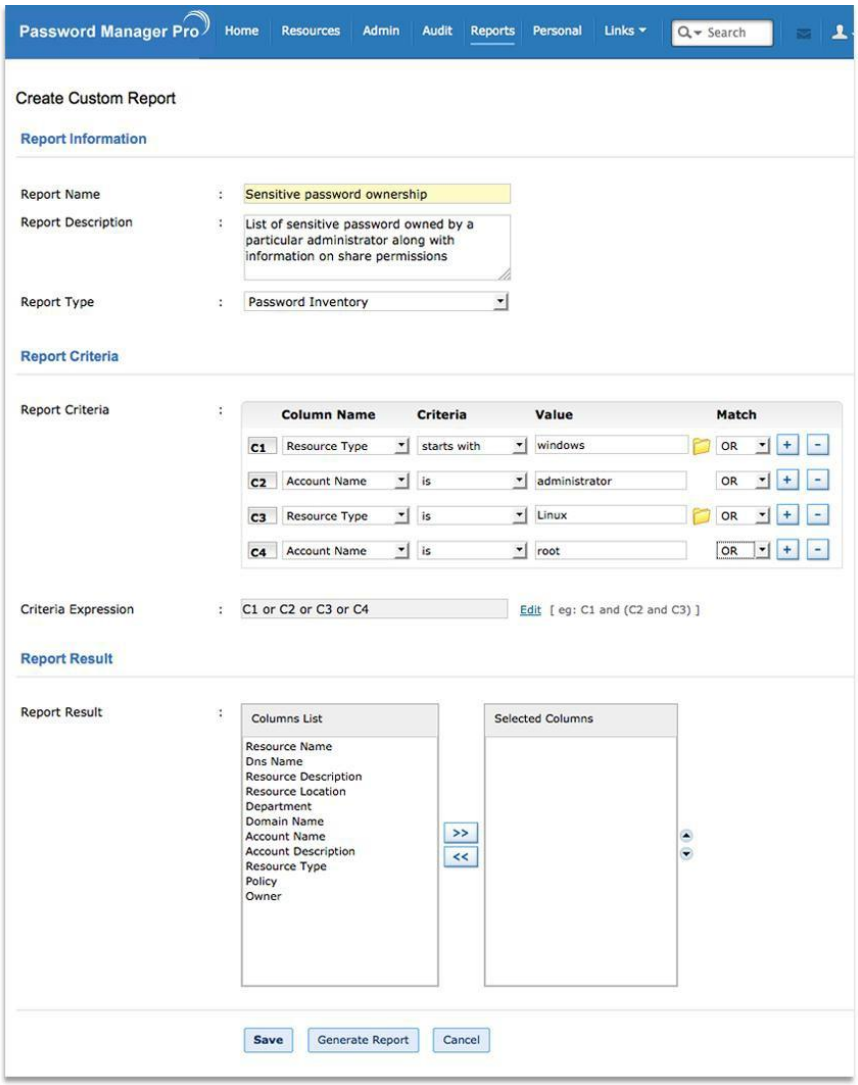
- Resource Type contains Cisco (take this as column C5)
- Account Name is root (take this as column C6)

To identify the resources owned by john

- Owner is John (take this as column C7)

Now, you need to specify the criteria expression to combine the above factors:
((C1 and C2) or (C3 and C4) or (C5 and C6)) and C7

That means, you want to identify the resources/accounts complying to any and all the criteria listed above and finally match the ownership.



How to create custom reports?

To create custom reports,

- go to "Reports" tab
- click the link "Custom Reports"
- click the link "Create Custom Reports" available on top right hand corner

- in the GUI that opens, provide a name for the custom report being created; enter description for easy identification of the report
- select the type of report out of which you wish to create the custom report
- specify the criteria based on which the custom report has to be created. Refer to the example above on specifying the criteria. In case, you want to specify multiple values for the same column name, enter the entries in comma separated form. In the example above, in case, you want to generate the report pertaining to two departments - Network Administration and Finance departments, enter the values for the column'Department' as Network Administration,Finance.
- in case, you want to specify advanced criteria, edit the control expressions field; you can specify advanced conditions using expressions. Refer to the example above for details.
- you have the option to control the number and order of columns to be displayed in the custom report. From "Select Columns" on LHS, choose the required columns. Use the up, down arrows on the RHS to control the arrangement of the columns in the report
- click "Save" to save the entries. Click "Generate Report" to generate the customized report.

Custom Reports - Use Case

By leveraging the power of the custom reports, you can meet many of your auditing requirements with ease. Following is just one use case

Exit Audit Report

Continuously assessing the vulnerability with respect to password access is one of the important auditing requirements. When an administrator, who had active access to the privileged passwords leaves the organization, it is imperative to assess the vulnerability. This requires taking a list of all the passwords that were accessed by the particular user during a specified time period and then initiate steps to change the passwords.

Taking a report on all the password management operations performed by the particular administrator during a specified time period, could serve as 'Exit Audit Report'. Custom reports help you generate a report to achieve this precisely. All that you need to do is to get the report out of the 'Resource Audit'.

- Specify the time period for the custom report
- Select the criteria as 'Operation Type' contains (C1) (just leave the criteria field blank to represent that you want to take a report on all operations)
- 'Operated by' 'User A' (C2) who is leaving the organization

The resultant report will provide you list of password management operations performed by the particular administrator during the time range specified.

Custom Reports out of 'Resource Audit' and 'User Audit' would prove highly useful as you would be able to meet most of your auditing requirements by properly leveraging them.

SNMP Traps, Syslog Settings

(Feature available only in Enterprise Edition)

Sending SNMP Traps & Syslog Messages to Management Systems

Password Manager Pro facilitates raising SNMP Traps and/or Syslog messages to you management systems on the occurrence of various password actions and Audit Events. SNMP trap sending and Syslog message forwarding is a two-step process:

- First you need to configure the SNMP and/or Syslog settings. This has to be done from Admin >> General >> SNMP/Syslog Settings
- You need to select the events for which you wish to generate traps or syslog messages. This can be done from Audit >> Configure Audit and Resource Groups >> Password Actions.

SNMP Trap Settings

PMP sends a SNMP v2c trap to the desired host and port. The varbinds include the resource name, account name, user name who operated, IP address from which the user operated, date and time and the reason of the operation that resulted in the event.

To specify SNMP trap settings,

- Go to the "Admin" tab
- Click "General >> SNMP Trap/Syslog Settings"
- In the UI that opens, enter the name of the host which has to receive the traps, its port and the SNMP community
- Click "Save"

Syslog Settings

A RFC-3164 compliant Syslog message will be generated and sent to the configured host and port, using the chosen protocol (TCP or UDP). Default facility name will be AUTH, but you can change it to any of the unassigned facility name form the pick list. The format of the Syslog message sent form PMP will be:
{LOGGED_IN_USERNAME:IPADDRESS} {OPERATION_TYPE} {OPERATED_TIME} {STATUS_OF_OPERATION} {PMP_SERVER_NAME} {RESOURCE_NAME:ACCOUNT_NAME: REASON}

To specify Syslog settings,

- Go to the "Admin" tab
- Click "General >> SNMP Trap/Syslog Settings"
- In the UI that opens, enter the name of the host which has to receive the traps, its port and the SNMP community
- Click "Save"

Note 1: After carrying out the settings here, You need to select the events for which you wish to generate traps or syslog messages. This can be done from Audit >> Configure Audit and Resource Groups >> Password Actions. Only then, PMP will start sending traps/messages.

Optional General Settings

In PMP, there are certain important features such as enforcement of password policy, 'Forgot Password' option to reset PMP user passwords, email notification on PMP user creation or role modification, provision for managing personal passwords, exporting resources, remote password reset etc.

While these features are very much needed for certain organizations, some others find them a hindrance. To cater to the needs of these two sets of user, PMP strikes balance through the general optional settings.

To access the settings page,

- Go to "Admin" tab
- Click "General Settings" under the section "General"
- In the UI that opens, following options are listed
- Password Retrieval
- Password Reset
- Resource/ Password Creation
- Resource Group Management
- User Management
- High Availability
- Personal Passwords

Password Retrieval

Allow password users and auditors to retrieve passwords for which 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, you can take a decision on allowing/restricting access to passwords. Select the checkbox to allow access and uncheck it to restrict.

Automatically hide passwords after X seconds (specify '0' to never hide passwords automatically)

By default, passwords are shown in hidden form behind asterisks. On clicking the asterisks, the passwords appear in plain text. By default, the passwords are shown for 10 seconds only. After that, they will be automatically hidden. If you want to increase or decrease this

time period, specify the desired value in seconds. If you specify 0, passwords will continue to remain in plain text until you click the password to hide.

Automatically clear clipboard data after seconds (specify '0' to never clear clipboard automatically)

PMP leverages clipboard utility of browsers to copy passwords when you intend to copy and paste passwords. By default, the copied passwords will be available for pasting for 30 seconds. If you want to increase or decrease this time period, specify the desired value in seconds. If you specify 0, clipboard will not be cleared automatically.

Include passwords when resource details are exported to CSV format

When you export PMP resources to a CSV file, by default, password of the accounts are included in plain text. In case, for security reasons, you wish to mask the password in the report, you can do so by unchecking this checkbox. Once you uncheck this option, the passwords would be masked in the exported CSV file.

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. If you want to force your users to provide a reason why access to the password was needed, you can enable this option by selecting the checkbox.

When access control is enabled and a password has been released to a 'password user', allow admins to view the password

When password access control is enabled and when a user is viewing the password, no one else would be allowed concurrent view by default. While giving the exclusive access to a user temporarily, PMP provides the flexibility to enable administrators view the password concurrently. Through a simple administrative setting from "General Settings", users will be able to do that, if required. If you select this check box the user who makes a request for a password, will not have the exclusive privilege. All PMP administrators will be able to view the password concurrently.

Enable display of Password History in Home tab

By default, in Home tab, Password History icon remains grayed out. If you want to enable it, select this check box. Once you do this, Password History will be displayed to all users.
Allow all admin users to manipulate the entire explorer tree

PMP offers provision to allow admin users to manipulate the entire explorer tree structure as they wish. Once this is enabled, PMP creates an organization wide, global explorer tree structure containing the names of resource groups under a root node. Any administrator in PMP would be able to create/edit the explorer tree structure of resource groups. The tree structure will be accessible to all admins, password admins and end users. Admins and password admins can add their resource groups anywhere into the global tree and the whole structure will be available for view to all the end users. If this option is disabled, users can modify only their portion of the tree.

Collapse password explorer tree view in Home Tab

By default, the nodes of the password explorer tree are shown in expanded form. By enabling this option, the explorer tree can be viewed in collapsed format.
Password Reset

Enforce users to provide a reason when changing the resource password

When resource passwords are changed by a user, by default, it is not mandatory to add a comment providing the reason for the change. However, enforcing the users to enter a comment would be a good practice and aid in auditing user actions. If you want to enforce this, select this checkbox. Once you do this, users will be prompted to enter a comment as reason when attempting change password.

Default selection for user initiated remote password change action

One of the important capabilities of PMP is Remote password reset, which enables users to change password of a resource in PMP console and apply the change in the remote resource instantaneously. This remote synchronization of passwords can be done for resources of the type Windows, Windows Domain and Linux. By default, when you try to change the password of an account belonging to the above three types, the remote synchronization option is enabled. If you want to disable this option, click the radio button "Do not apply changes to the resource". At any point of time, you can override this option while invoking the change password option.

Wait for X seconds between stopping and starting the services after service account password reset

For every Windows domain account for which the service account reset is enabled, PMP will find out the services which use that particular domain account as service account, and automatically reset the service account password if this domain password is changed. In

certain cases, there would be requirements for stopping and starting the services. In such cases, you can configure PMP to wait for a specified time period (in seconds) between stopping and starting the services. By default, PMP waits for 60 seconds. You may configure it in accordance with your needs.

Enforce users to provide two different accounts for use with remote password reset for UNIX / Linux resources

To enable remote password reset for UNIX/Linux resource types, you can enforce users to provide two different accounts for password reset. If you do not opt this, users will be allowed to enable remote synchronization with just one account.

Resource/Password Creation

Enforce password policy during resource or password creation

By default, when you are adding your resource to PMP, it does not check for compliance to the password policy already defined by the IT administrator. It is enforced only at the time of doing change password. In case, you wish to check policy compliance at the time of resource / account addition itself, just click this checkbox. Once you click this, you will be permitted to add your resource / account only if the password is in accordance with the policy defined.

When agents are deployed in resources for remote password reset, the accounts in the resource are automatically added to PMP. There is also option to synchronize account addition or deletion afterwards:

- Sync account addition:
  If you enable this option, whenever a new account gets added to the resource, that will be synchronized in PMP too.
- Sync account deletion:
  If you enable this option, whenever an account gets deleted in the resource, that will be synchronized in PMP too. The account will be deleted in PMP too.

Resource Group Management

Show the option to create static resource groups by picking resources individually
By default, two options are available for resource group creation - static resource group creation by picking resources individually and dynamic group creation by specifying criteria. If you want to remove the option of static resource group creation, de-select this check box.

Once you do this, you will have only one option for resource group creation - dynamic group creation by specifying a criteria.

User Management

Automatically log off users after X minutes of inactivity

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. If a user is inactive with the GUI for the specified time limit, the user will be automatically logged out of the session. By default, if PMP remains unattended for 30 minutes, user will be automatically logged out. If you specify '0' as the value, the users will not be logged out for inactivity.

Allow 'Local Authentication' when AD/LDAP authentication is enabled

As explained earlier, PMP provides three types of authentication - LDAP authentication, AD authentication and PMP's local authentication. By default, PMP allows local authentication along with LDAP or AD authentication. If you want to strictly the restrict to LDAP or AD authentication alone, uncheck the checkbox. Once you do this, the PMP users would be allowed to login using their workstation password alone.

Configure default-selected domain in the login screen. (Applicable only when AD authentication is enabled).

If you have users from various domains, the PMP login screen will list-down all the domains in the drop-down. For ease of use, you may specify the domain used by the largest number of users or the frequently used domain here. Once you do so, that domain will be shown selected by default in the login screen.

Show 'Forgot Password' option in the login screen

If a PMP user forgets his/her login password, they can rely on the 'Forgot Password' option, which sends a new login password to that user via email. By default, this option remains enabled. If you do want to display this option, uncheck the checkbox. Once you do this, from the login onwards, this option would not be visible to all the users.

Notify users through email during account creation or modification

By default, whenever a new user account is added in PMP or an existing account is modified, an email is triggered to the respective user with information about the login password in the case of new user addition and details of changes (in the case of account modification) are sent. If you want to disable this option, uncheck this checkbox. Once you do this, emails will not be sent on user addition or modification.

Enable 'Support Link' for Password Administrators

By default, PMP users with the role 'Password Administrator' will not be able to view the 'Support' tab in the GUI. If you want Password Administrators to view the support tab, select the checkbox.

Notify Users through Email 30 and 15 days Prior to PMP License Expiry

Prior to the expiry of PMP license, email notifications could be sent to all administrators or to any desired user(s). Two notifications will be sent - one, 30 days prior to the expiry and another 15 days earlier.

High Availability

Check High Availability Status Every --- Minutes

In High Availability set up, constant replication of data takes place between Primary and Standby servers. High Availability status 'Alive' indicates perfect data replication and data synchronization. If there happens any disruption like network problems between Primary and Standby (in turn between the databases), the status will get changed to 'Failed'. This may happen when there is no communication/connection between the database of primary server and that of the standby server.

When the connection gets reestablished, data synchronization will happen and both databases will be in sync with each other. During the intervening period, those who have connected to the primary and standby will not face any disruption in service. This status is only an indication of the connection/communication between databases and does not warrant any troubleshooting.

To check the status periodically and get notifications, select this option and specify the time interval in minutes.

Personal Passwords

Allow users to manage their personal passwords

PMP provides personal password management feature as a value addition to individual users to manage their personal passwords such as credit card PIN numbers, bank accounts etc while using the software for enterprise password management. The personal password management belongs exclusively to the individual users. If you do not want to allow personal password management for your PMP users, uncheck this checkbox. Once you do this, the 'Personal' tab will not appear in the PMP GUI.

Allow users to choose their own encryption key for managing personal passwords

By default, when you allow users to manage their personal passwords, PMP provides three options to secure the personal passwords - using the encryption key provided by the customers and storing it / using the encryption key provided by the customers and not storing it / using PMP's encryption key. When you allow the users to manage personal passwords, you can either allow the users to define their own encryption key or force them to use PMP's encryption key itself. If you want to allow them to choose their own personal passwords, select the checkbox. This option will take effect only for those users who are added after setting this.

Provision for storing personal information

There is provision for storing passwords of personal applications in the PMP web interface. For example, you can store personal email account information, credit card numbers, banking accounts, contact addresses, phone numbers, email ids etc. These information can be accessed only by the respective user. Secure storage, retrieval and viewing of details are assured.

Deciding the encryption key, the first step

Before you start adding your personal details, choose how secure you want PMP Pro to maintain your personal passwords. All your personal passwords will be encrypted and stored in the database. Tell Password Manager Pro about the encryption key to be used by choosing one of the options given below. This is a one time configuration which cannot be changed later, so make your choice carefully.

Option 1: Use my encryption key and do not store it (recommended)

All your passwords will be encrypted using the key supplied by you and the key will not be stored in the PMP database. To access your personal passwords you will have to supply this key every time and if you forget this key you will lose all your passwords. This is useful in cases where you store sensitive personal data.
If you want to choose this option, go to "Personal Tab" and click the option and enter the encryption key in the text field.

Option 2: Use my encryption key and store it

All your passwords will be encrypted using the key supplied by you. The key will be stored securely in the PMP database. During the subsequent password retrievals, you need not specify the key and it is also not necessary that you remember this key.
If you want to choose this option, go to "Personal Tab" and click the option and enter the encryption key in the text field.

Option 3: Use PMP's Encryption Key

All your passwords will be encrypted with the same key as the enterprise passwords. You do not have to supply or remember any encryption keys.

If you want to choose this option, go to "Personal Tab" and click the option and enter the encryption key in the text field.

Storing Personal Accounts

After choosing the encryption key, you can proceed with adding your personal accounts such as web accounts, bank accounts, credit card accounts and personal contacts list. You can also add your own categories depending on your needs.

For all the above, there is provision to add custom fields in accordance to your requirements.

Note: There are four default categories - Web Accounts, Banking, Credit Cards and Contacts. These categories cannot be deleted. However, the custom categories created by you can be deleted at your will.

Web Accounts

To add a New Web Account,

- Go to "Personal" Tab
- Click "Web Accounts" in the drop-down "Show entries of" present at the RHS
- In the GUI that comes up, click the button "Add Accounts"
- Fill in the required details
- Click "Save"

Can I add Custom Fields?

Yes, you can have any number of additional custom fields. To add a custom field, click the button "Customize Fields". Your additional fields can be in any of the following four formats - Character/list, Numeric, Password, Date&Time. A maximum of nine character/list fields could be added. Four numeric fields, three password fields and four date&time fields could be added. Once you click "Save", the custom fields get added to the web accounts column. Custom fields, once added, cannot be deleted.

To Delete Accounts,

- Go to "Personal" Tab
- Click "Web Accounts" in the drop-down "Show entries of" present at the RHS
- Click the button "Delete Accounts"
- Click "Save"

Note: Once you delete accounts, they will be deleted from the database once and for all. So, exercise care before deleting accounts.

Banking Accounts

To add a New Account,

- Go to "Personal" Tab
- Click "Banking Accounts" in the drop-down "Show entries of" present at the RHS
- Click the button "Add Accounts"
- Fill in the required details such as Bank Name, Account Number, Branch etc. Leave unwanted fields blank.
- Click "Save"

Can I add Custom Fields?

Yes, you can have any number of additional custom fields. To add a custom field, click the button "Customize Fields". Your additional fields can be in any of the following four formats - Character/list, Numeric, Password, Date & Time. A maximum of nine character/list fields could be added. Four numeric fields, three password fields and four date&time fields could be added. Once you click "Save", the custom fields get added to the web accounts column. Custom fields, once added, cannot be deleted.

To Delete Accounts,

- Go to "Personal" Tab
- Click "Banking Accounts" in the drop-down "Show entries of" present at the RHS
- Click the button "Delete Accounts"
- Click "Save"

Note: Once you delete accounts, they will be deleted from the database once and for all. So, exercise care before deleting accounts.

Credit Card Accounts

To add a New Account,

- Go to "Personal" Tab
- Click "Credit Card" in the drop-down "Show entries of" present at the RHS

- Click the button "Add Accounts"
- Fill in the required details such as Card Name, Card Number, PIN, Phone Number etc. Leave unwanted fields blank.
- Click "Save"

Can I add Custom Fields?

Yes, you can have any number of additional custom fields. To add a custom field, click the button "Customize Fields". Your additional fields can be in any of the following four formats - Character/list, Numeric, Password, Date & Time. A maximum of nine character/list fields could be added. Four numeric fields, three password fields and four date & time fields could be added. Once you click "Save", the custom fields get added to the web accounts column. Custom fields, once added, cannot be deleted.

To Delete Accounts,

- Go to "Personal" Tab
- Click "Credit Card" in the drop-down "Show entries of" present at the RHS
- Click the button "Delete Accounts"
- Click "Save"

Note: Once you delete accounts, they will be deleted from the database once and for all. So, exercise care before deleting accounts.

Personal Contacts

To add a New Web Account,

- Go to "Personal" Tab
- Click "Contacts" in the drop-down "Show entries of" present at the RHS
- Click the button "Add Accounts"
- Fill in the required details
- Click "Save"

Can I add Custom Fields?

Yes, you can have any number of additional custom fields. To add a custom field, click the button "Customize Fields". Your additional fields can be in any of the following four formats - Character/list, Numeric, Password, Date & Time. A maximum of nine character/list fields

could be added. Four numeric fields, three password fields and four date & time fields could be added. Once you click "Save", the custom fields get added to the web accounts column. Custom fields, once added, cannot be deleted.

To Delete Accounts,

- Go to "Personal" Tab
- Click "Contacts" in the drop-down "Show entries of" present at the RHS
- Click the button "Delete Accounts"
- Click "Save"

Note: Once you delete accounts, they will be deleted from the database once and for all. So, exercise care before deleting accounts.

Creating Custom Categories

Apart from the four default categories explained above, you can create any number of additional categories to store other information. For instance, if you wish to store details about the properties owned by you, just one more category could be added. You can have your own names for the columns.

To create a custom category,

- Go to "Personal" Tab
- Click the link "Add New Category" available at the top right hand corner of the GUI
- In the UI that opens, provide a name for the new category
- Enter column names for the category. You can add column names containing characters, numbers, passwords and date & time.
- Click "Save"

Note: If any of the custom categories are no longer required, you can delete them by clicking the "X" mark against their name in the "Manage Categories" page. Once you delete the categories, they will be deleted from the database once and for all. So, exercise care before deleting.

Password Manager Pro - FAQ

Contents

Web Interface, Authentication

1. Why are my users not notified of their PMP accounts?

Users are notified of their PMP accounts only through email. If they do not get the notification email, check

- if you have configured the mail server settings properly with the details of the SMTP server in your environment
- if you have provided valid credentials as part of mail server settings, as some mail servers require them for mails to be sent
- if the 'Sender E-Mail ID' is properly configured as some mail servers reject emails sent without the from address or mails originating from unknown domains

2. What are the authentication schemes available in PMP?

You can use one of the following three mechanisms:

- Active Directory: When enabled, the authentication request is forwarded to the configured domain controller and based on the result, the user is allowed or denied access into PMP. The user name, password and the domain are supplied in the PMP login screen. This scheme works only for users whose details have been imported previously from AD. Available only when PMP server is installed on Windows system.
- LDAP Directory: When enabled, the authentication request is forwarded to the configured LDAP directory server and based on the result, the user is allowed or denied access into PMP. The user name and password and the option to use LDAP authentication are supplied in the PMP login screen. This scheme works only for users whose details have been imported previously from the LDAP directory
- PMP Local Authentication: The authentication is done locally by the PMP server. Irrespective of AD or LDAP authentication being enabled, this scheme is always available for the users to choose in the login page. This scheme has a separate

password for users and the AD or LDAP passwords are never stored in the PMP database.

- Two Factor Authentication: Option to enforce users to identify themselves with two unique factors before they are granted access to PMP web-interface. While the existing authentication mechanism of PMP (native authentication / AD / LDAP) will be the first authentication factor, the second authentication factor could be either a unique password generated by PMP and sent through email or RSA SecurID one-time password, which changes every sixty seconds. For RSA part, PMP has entered into a technology partnership with RSA SecurID two-factor authentication system.

3. What are the user roles available in PMP? What are their access levels?

PMP comes with four pre-defined roles.

1. Administrators
2. Password Administrators
3. Password Users
4. Password Auditors

Any administrator can be made as "Super Administrator" with the privilege to view and manage all resources. Refer help documentation for details on access levels.

4. What if I forget my PMP login password?

If you were already given a valid PMP account, you can use the 'Forgot Password?' link available in the login page to reset the password. The user name/e-mail id pair supplied should match the one already configured for the user and in that case, the password will be reset for that user and the new password will be emailed to that email id.

5. Why does Internet Explorer 7 (and other browsers) complain while accessing PMP console?

The PMP web console always uses HTTPS to communicate with the PMP server. The PMP server comes with a default self-signed SSL certificate, which the standard web browsers will not recognize and issue a warning. Particularly IE 7's warning message appears serious. Ignoring this warning still guarantees encrypted communication between the PMP console and the server but if you want your users to be particularly sure that they are connecting only to the PMP server, you will need to install a SSL certificate that you have bought from a certificate authority, that is recognised by all standard web browsers.

6. Can I change the default port 7272 occupied by PMP?

Yes, you can change the default port as explained below:

- Go to <PMP_Installation_Folder>\conf directory and open the server.xml file
- Replace the entry '7272' with the port number of your choice. Note that there will be 7272 entries within comments too and all should be replaced.

Security

1. How secure are my passwords in PMP?

Ensuring the secure storage of passwords and offering high defence against intrusion are the mandatory requirements of PMP. The following measures ensure the high level security for the passwords:

- Passwords are encrypted using the Advanced Encryption Standard (AES), which is currently the strongest encryption algorithm, and stored in the database. (AES has been adopted as an encryption standard by the U.S. Government)
- The database which stores all the passwords accepts connections only from the host that it is running on and is not visible externally
- Role-based, fine-grained user access control mechanism ensures that the users are allowed to view the passwords based on the authorization provided
- All transactions between the PMP console and the server take place through HTTPS
- In-built Password Generator can help you generate strong passwords

For detailed information, refer to Product Security Specifications document.

2. Can we install our own SSL certificate? How?

Refer to the FAQ section in website.

3. How secure are the A-to-A, A-to-DB password management done through Password Management APIs?

The web API exposed by PMP forms the basis for Application-to-Application/Database Password Management in PMP. The applications connect and interact with PMP through HTTPS. The application's identity is verified by forcing it to issue a valid SSL certificate, matching the details already provided to PMP corresponding to that application.

password reset

1. Can I also change resource passwords from the PMP console?

Yes, of course. PMP can change the passwords currently for Windows, Windows domain and Linux systems. Capability to change passwords of other types of resources like databases, routers, switches etc will be gradually added. PMP supports both agent-based and agent-less modes of changing passwords.

2. When to use the agent and agent-less modes for password reset?

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 communication between the PMP server and agent takes place through TCP for normal information and HTTPS for password transfer and hence communication paths must exist (ports to be kept open) between the server and agent.

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.

3. Can I enable agentless password reset if I add my own resource type for other distributions of Linux / other versions of Windows?

Yes, you can. As long as your resource type label contains the string 'Linux' or 'Windows', you can still configure agentless password reset for those resources.

Example of valid resource type labels to enable password reset:
Debian Linux, Linux - Cent OS, SuSE Linux, Windows XP Workstation, Windows 2003 Server

4. Is there a way to do remote password reset for resource types other than the ones for which remote reset is supported now?

Yes, you can make use of Password Reset Listeners, which enable invoking a custom script or executable as a follow-up action to Password Reset action in PMP. Refer to Password Reset Listener for more details.

5. How to troubleshoot when password reset does not happen?

In the agent mode,

- Check if the agent is running by looking at the Windows active process list for the entry 'PMPAgent.exe' or the presence of a process named PMPAgent in Linux
- Check if the account in which the agent is installed has sufficient privileges to make password changes

In the agentless mode,

- Check if the right set of administrative credentials have been provided and the remote synchronization option is enabled
- Check if the necessary services are running on the resource (Telnet / SSH for Linux, RPC for Windows)
- Check if the resource is reachable from the PMP server using the DNS name provided

6. Windows domain password reset fails with the error message: "The authentication mechanism is unknown"

This happens when PMP is run as a Windows service and the 'Log on as" property of the service is set to the local system account. Change it to any domain user account to be able to reset domain passwords. Follow the instructions below to effect that setting:

- Go to the Windows Services applet (from Control Panel --> Administrative Tools --> Services)

- Select the 'ManageEngine PMP' service, right-click --> choose Properties
- Click the Log On tab and choose the 'This Account' radio button and provide the username and password of any domain user - in the format \
- Save the configuration and restart the server

7. What are the prerequisites for enabling Windows Service Account Reset?

Before enabling windows service account reset, ensure if the following services are enabled in the servers where the dependent services are running:

- Windows RPC service should have been enabled
- Windows Management Instrumentation (WMI) service should have been enabled

8. Does domain SSO work across firewalls / VPNs?

The domain Single Sign On (windows integrated authentication) is achieved in the Windows environment by setting non-standard parameters in the HTTP header, which are usually stripped off by devices like firewalls / VPNs. PMP is designed for use within the network. So, if you have users connecting from outside the network, you cannot have SSO this enabled.
Backup & Disaster Recovery

1. Can I setup disaster recovery for the PMP database?

Yes, you can. PMP can periodically backup the entire contents of the database, which can be configured through the PMP console. Refer help documentation for more details.

2. Where does the backup data get stored? Is it encrypted?

All sensitive data in the backup file are stored in encrypted form in a .zip file under <PMP_Install_Directory/backUp> directory. It is recommended that you backup this file in your secure, secondary storage for disaster recovery.

General

1. Do I need any prerequisite software to be installed before using PMP?

There is no prerequisite software installation required to use PMP.

2. Can others see the resources added by me?

Except super administrators (if configured in your PMP set up), no one, including admin users will be able to see the resources added by you. Apart from this, decide to share your resources with other administrators, they will be able to see tham.

3. Can I add my own attributes to PMP resources?

Yes, you can extend the attributes of the PMP resource and user account to include details that are specific to your needs. Refer the help documentation for more details.

4. What if a user who has not shared his sensitive passwords, leaves the enterprise?

This can very well happen in any enterprise, but with PMP you need not worry about passwords getting orphaned. Administrators can 'transfer' resources owned by users to other administrator users and in the process they have no access to those resources themselves, unless they do the transfer to their name. Refer the help documentation for more details.

5. Can I run custom queries to generate results for integration with other reporting systems?

Yes, you can. Please contact us at support@passwordmanagerpro.com with your specific request and we will help you with the relevant SQL query to generate XML output.

6. Can I rebrand PMP with our logo?

Yes. If you want to replace the PMP logo appearing on the login screen and on the web-interface with that of yours, you can do so from the web-interface itself. It is preferable to have your logo of the size 210 * 50 pixels.

To rebrand the logo,

- Go to the "Admin" tab
- Click "Customize >> Rebrand"
- Browse and choose the required image
- Click "Save"
- The PMP will appear with rebranded look

7. Does PMP record Password viewing attempts and retrievals by users?

Yes, PMP records all operations performed by the user including the password viewing and copying operations. From audit trails, you can get a comprehensive list of all the actions and attempts by the users with password retrieval. The list of operations that are audited (with the timestamp and the IP address) includes:

- User accounts created, deleted and modified
- Users logging in and logging off the application
- Resources and passwords created, accessed, modified and deleted

8. Does PMP provide high availability support?

Yes, refer to High Availability section in the Help Documentation for more details

Licensing

1. What is the Licensing Policy for PMP?

There are three license types:

- Evaluation download valid for 30 days capable of supporting a maximum of 2 administrators
- Free Edition licensed software allows you to have 1 administrator and manage up to 10 resources. Valid forever.
- Registered Version - need to buy license based on the number of administrators required and the type of edition Standard/Premium/Enterprise Edition:
    - Standard - If your requirement is to have a secure, password repository to store your passwords and selectively share them among enterprise users, Standard Edition would be ideal.
    - Premium - Apart from storing and sharing your passwords, if you wish to have enterprise-class password management features such as remote password reset, password alerts and notifications, application-to-application password management, reports, high-availability and others, Premium edition would be the best choice.
    - Enterprise - If you require more enterprise-class features like auto discovery of privileged accounts, integration with ticketing systems and SIEM solutions, jump server configuration, application-to-application password management, out-of-the-box compliance reports, SQL server / cluster as backend database, Enterprise edition will be ideal.

2. Can I buy a permanent license for PMP? What are the options available?

Though PMP follows an annual subscription model for pricing, we also provide perpetual licensing option. The perpetual license will cost three times the annual subscription price, with 20% AMS from the second year.
Contact sales@manageengine.com and support@passwordmanagerpro.com for more details.

3. Can PMP support more than 100 administrators?

Yes, very much. If you want a license with more than 100 administrator users, please contact sales@manageengine.com andsupport@passwordmanagerpro.com for more details.

4. Can I extend my evaluation to include more administrator users or for more number of days?

Yes. Fill in the required details in the website and we will send you the license keys.

5. Do I have to reinstall PMP when moving to Premium/Enterprise Edition?

No. You need not have to reinstall or shut down the server. You just need to enter the new license file in the "License" link present in the top right corner of the PMP web interface. FAQ Section in our website is updated frequently. Refer to that for more information.