ManageEngine

Password Manager Pro

GETTING STARTED GUIDE

For Password Manager Pro Administrators

www.passwordmanagerpro.com

Table of contents

Introduction

Thank you for choosing ManageEngine's Password Manager Pro to manage your organization's privileged identities. This guide will provide you with the basic information necessary to help you get started.

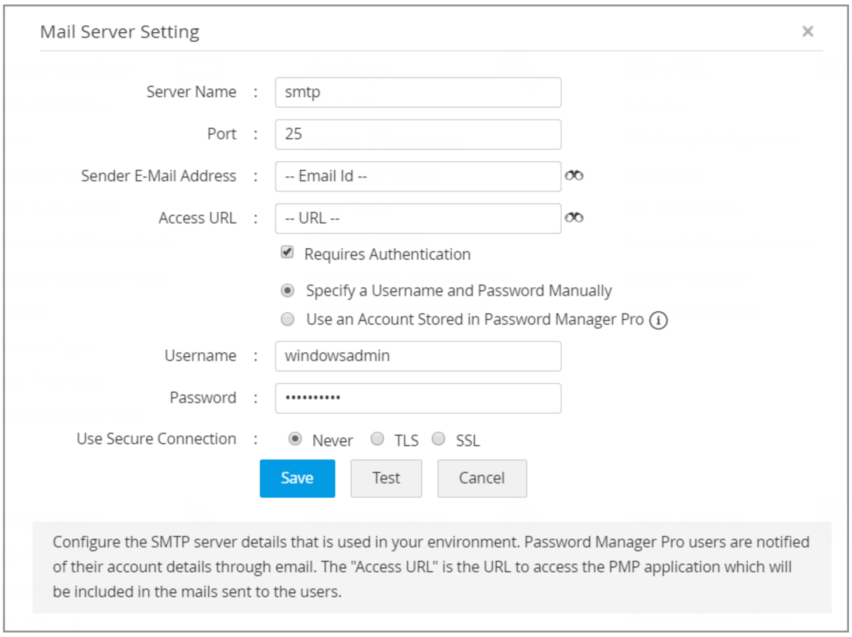
Installation

If you haven't yet installed Password Manager Pro, follow the steps detailed in the user manual and install it. This guide will help you start the server and connect to the web interface.

Basic Settings

Configure mail server

After installation, you need to configure certain basic settings. First, configure the mail server so that Password Manager Pro can send emails directly from within the application, without an external mail client. You also need to configure the SMTP server details here. Password Manager Pro users are notified of their account details and password actions only through email, so it's important that this is set up correctly.



Mail Server Setting ×

Server Name : smtp
Port : 25
Sender E-Mail Address : -- Email Id --
Access URL : -- URL --

☑ Requires Authentication

● Specify a Username and Password Manually
○ Use an Account Stored in Password Manager Pro ⓘ

Username : windowsadmin
Password : ••••••••••

Use Secure Connection : ● Never ○ TLS ○ SSL

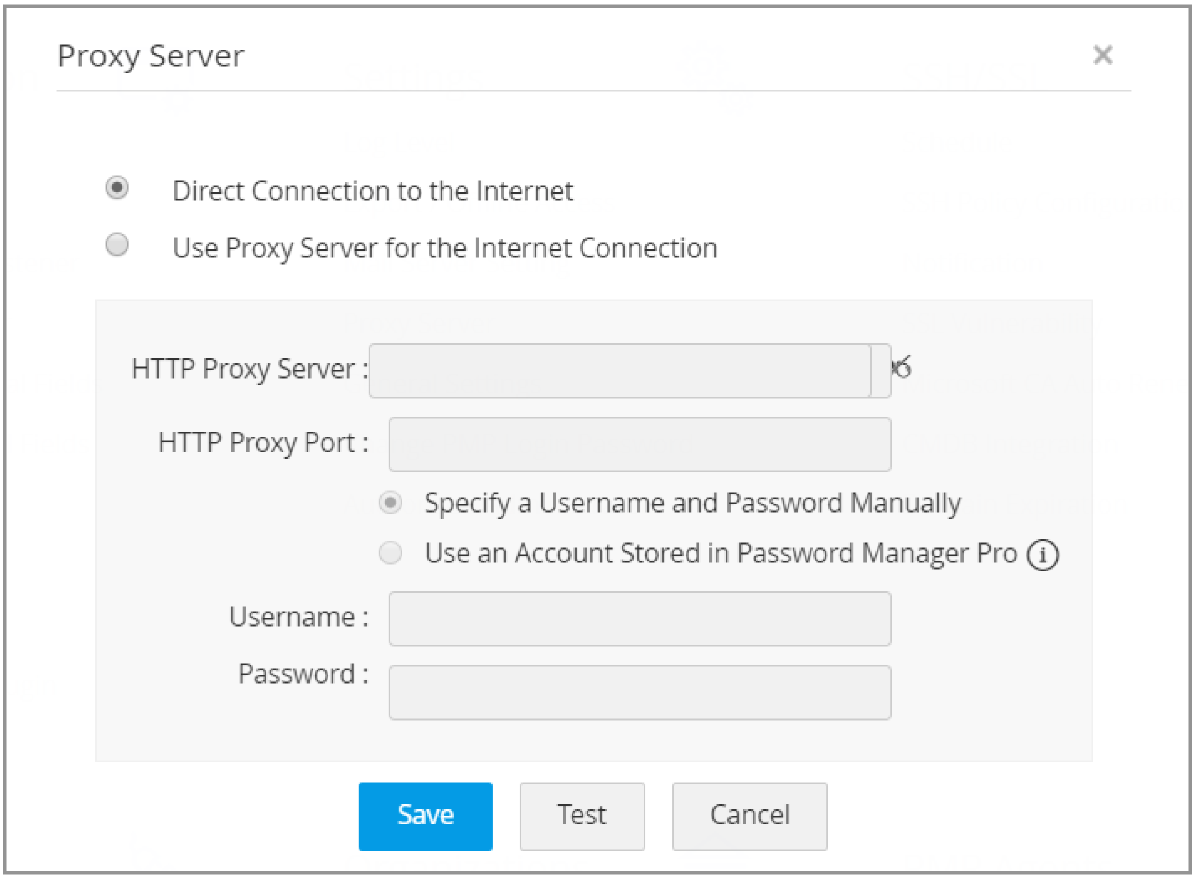
Configure the SMTP server details that is used in your environment. Password Manager Pro users are notified of their account details through email. The "Access URL" is the URL to access the PMP application which will be included in the mails sent to the users.

Enter all details including server name, port, sender email id, access URL, and type of authentication. Then save the configuration.

Configure proxy

Next, specify how you will connect to the Internet: directly or over a proxy. Configure this setting by going to **Admin** tab, under **Settings** > **Proxy Server.**
You'll see two options here:

- Direct connection to the internet
- Use proxy server for the internet connection



Proxy Server

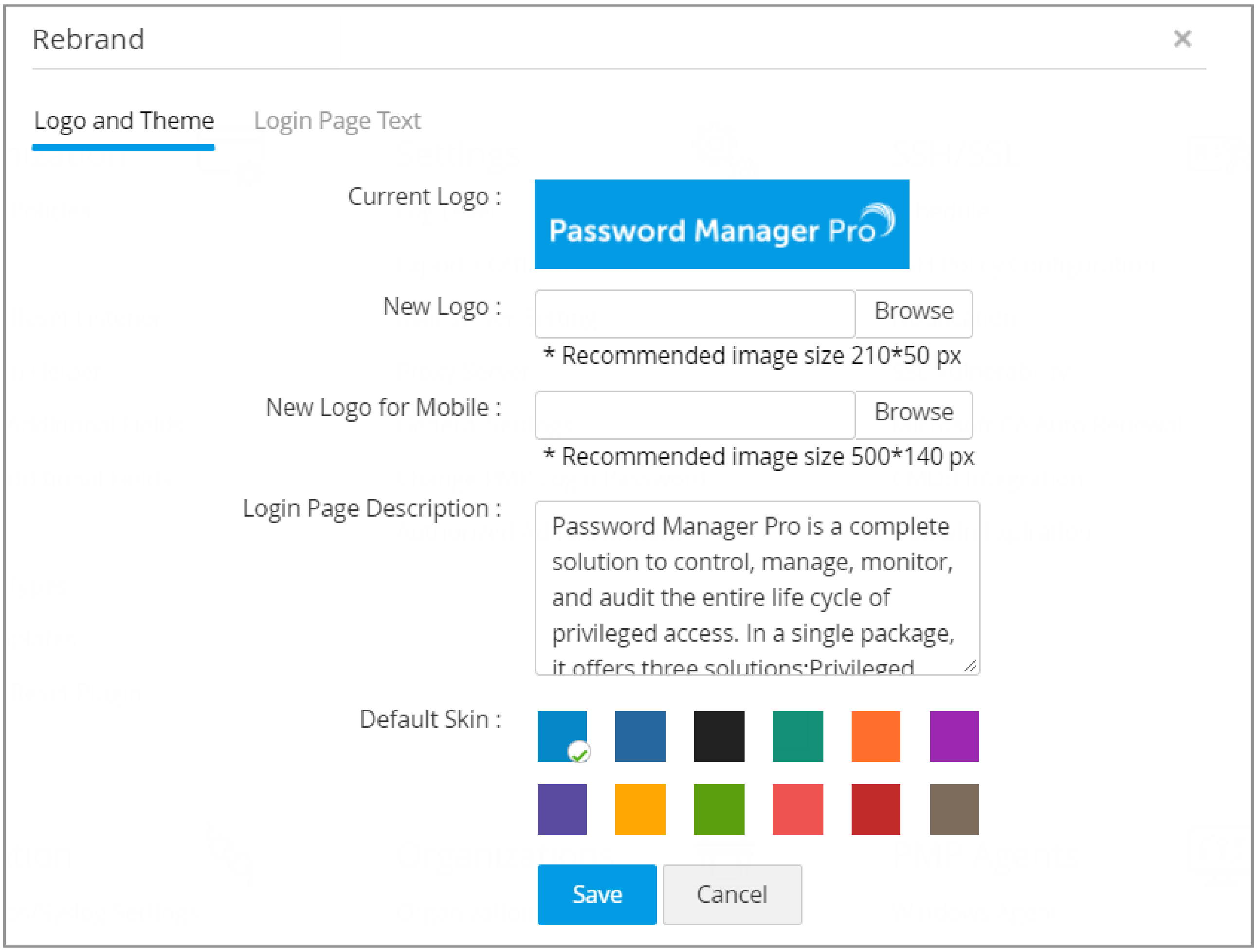
● Direct Connection to the Internet
○ Use Proxy Server for the Internet Connection

HTTP Proxy Server :
HTTP Proxy Port :
● Specify a Username and Password Manually
○ Use an Account Stored in Password Manager Pro
Username :
Password :

If your internet connection is over a proxy, configure proxy server settings, such as HTTP proxy server name, proxy port, type of authentication, and the username and password used for the connection.

Change the logo

If you want to replace Password Manager Pro's logo in the GUI with your company logo, you can do so with a simple setting change. The recommended logo size is 210 x 50 pixels. To effect the change, navigate to the **Admin** tab and click **Rebrand** under the **Customize** section.



Rebrand

Current Logo :

New Logo :

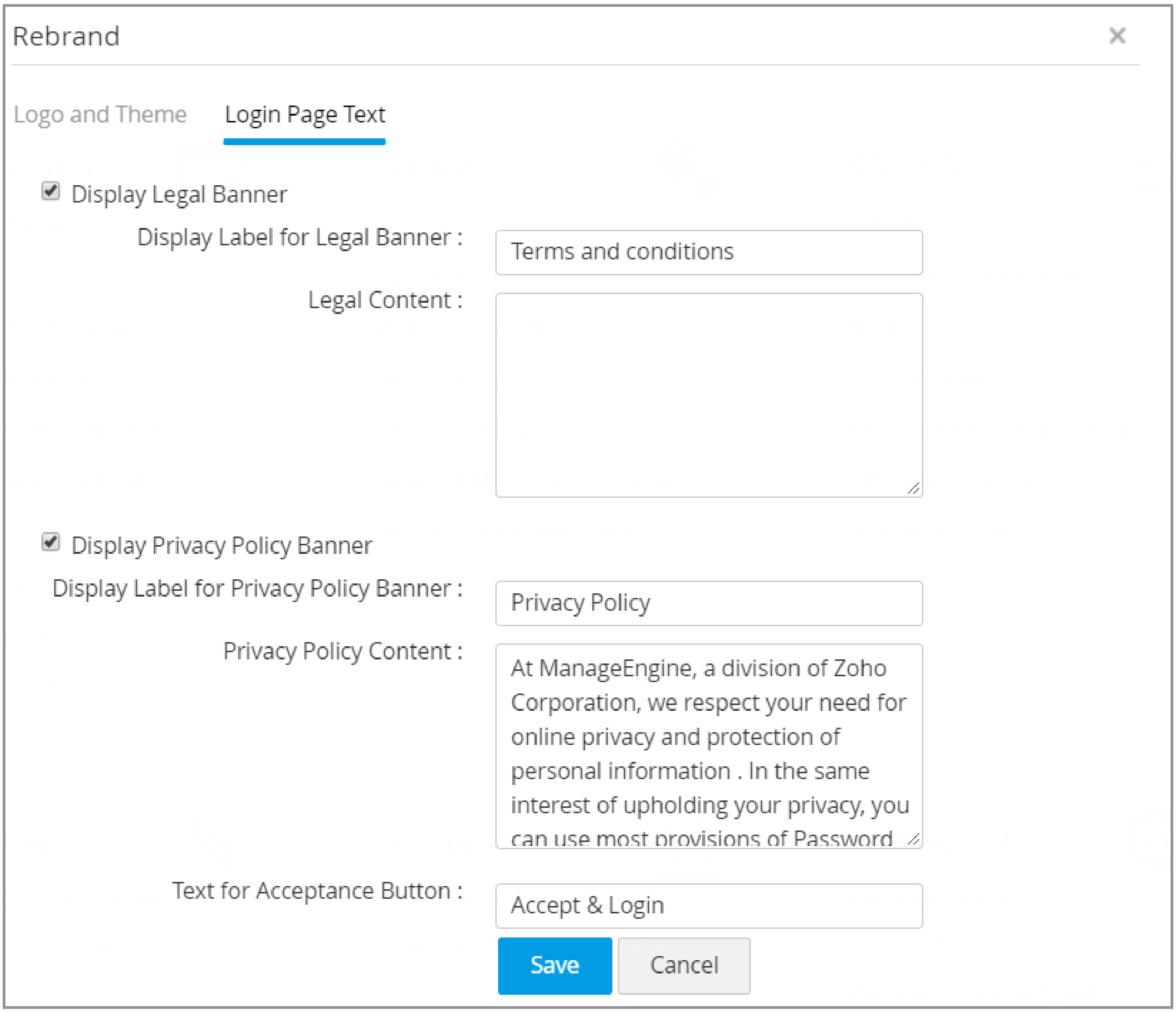
* Recommended image size 210*50 px

New Logo for Mobile :

* Recommended image size 500*140 px

Login Page Description : Password Manager Pro is a complete solution to control, manage, monitor, and audit the entire life cycle of privileged access. In a single package, it offers three solutions:Privileged

Default Skin : 🟦✓ 🟦 ⬛ 🟩 🟧 🟪 🟪 🟨 🟩 🟥 🟥 🟫



Rebrand

☑ Display Legal Banner

Display Label for Legal Banner : Terms and conditions

Legal Content :

☑ Display Privacy Policy Banner

Display Label for Privacy Policy Banner : Privacy Policy

Privacy Policy Content : At ManageEngine, a division of Zoho Corporation, we respect your need for online privacy and protection of personal information . In the same interest of upholding your privacy, you can use most provisions of Password

Text for Acceptance Button : Accept & Login

Apart from logo change, there are a number of other customizations that can be done, such as changing the login page description and GUI skin color, displaying a company-specific banner for privacy policy and legal purposes.

For detailed instructions on rebranding, you can refer to this help document.

User Provisioning and Management

After configuring the basic settings, the next step is to create accounts for your users in Password Manager Pro.

Add users

There are several ways in which you can add users to Password Manager Pro. Password Manager Pro offers the provision to import users from corporate identity stores such as AD, LDAP or Azure AD through integration. You can also import users in bulk from a CSV or add users manually. For detailed information on adding users, check out the documents listed below:

- Import users from AD or LDAP
- Import users from LDAP
- Import users from Azure AD
- Import users from CSV
- Add users manually

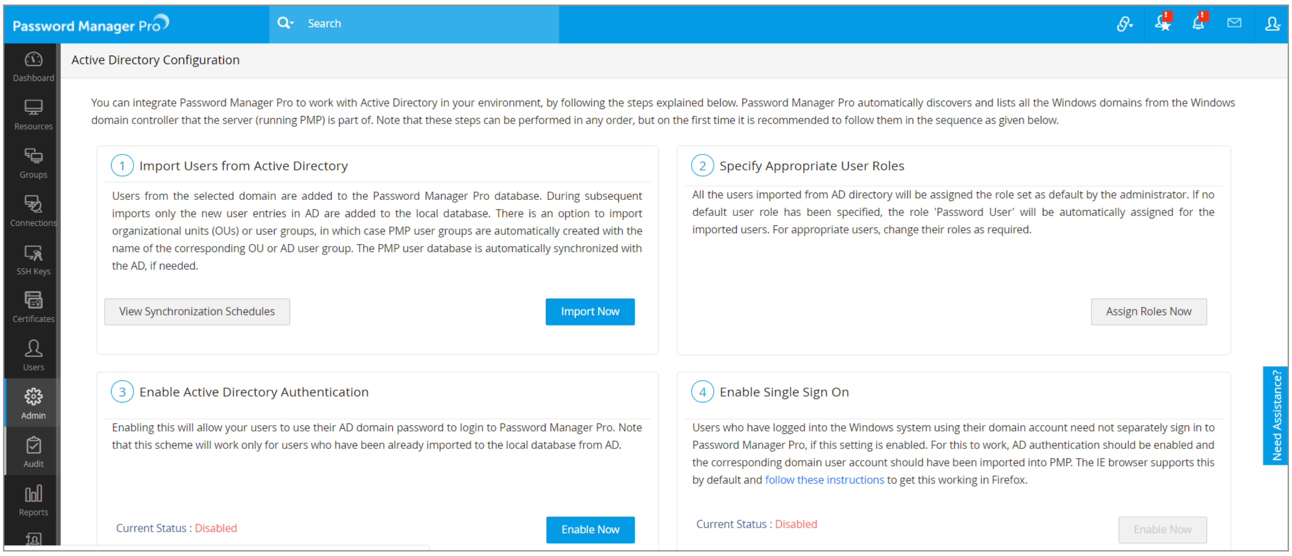
Set up a first level authentication

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. Password Manager Pro provides various authentication options and users can choose the ones that suit their environment better. Apart from Password Manager Pro's local authentication, there is provision for leveraging the authentication of external identity stores such as Active Directory/LDAP.

Authentication through AD

To allow users to login to Password Manager Pro using their AD domain passwords, navigate to **Admin** > **Authentication** > **Active Directory** and enable the active directory authentication option.

> **Note:** This authentication scheme will work only for users who have already been imported to the local database from Active Directory.



Active Directory Configuration

You can integrate Password Manager Pro to work with Active Directory in your environment, by following the steps explained below. Password Manager Pro automatically discovers and lists all the Windows domains from the Windows domain controller that the server (running PMP) is part of. 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.

1 Import Users from Active Directory

Users from the selected domain are added to the Password Manager Pro database. During subsequent imports only the new user entries in AD are added to the local database. There is an option to import organizational units (OUs) or user groups, in which case PMP user groups are automatically created with the name of the corresponding OU or AD user group. The PMP user database is automatically synchronized with the AD, if needed.

View Synchronization Schedules | Import Now

2 Specify Appropriate User Roles

All the users imported from AD directory will be assigned the role set as default by the administrator. If no default user role has been specified, the role 'Password User' will be automatically assigned for the imported users. For appropriate users, change their roles as required.

Assign Roles Now

3 Enable Active Directory Authentication

Enabling this will allow your users to use their AD domain password to login to Password Manager Pro. Note that this scheme will work only for users who have been already imported to the local database from AD.

Current Status : Disabled | Enable Now

4 Enable Single Sign On

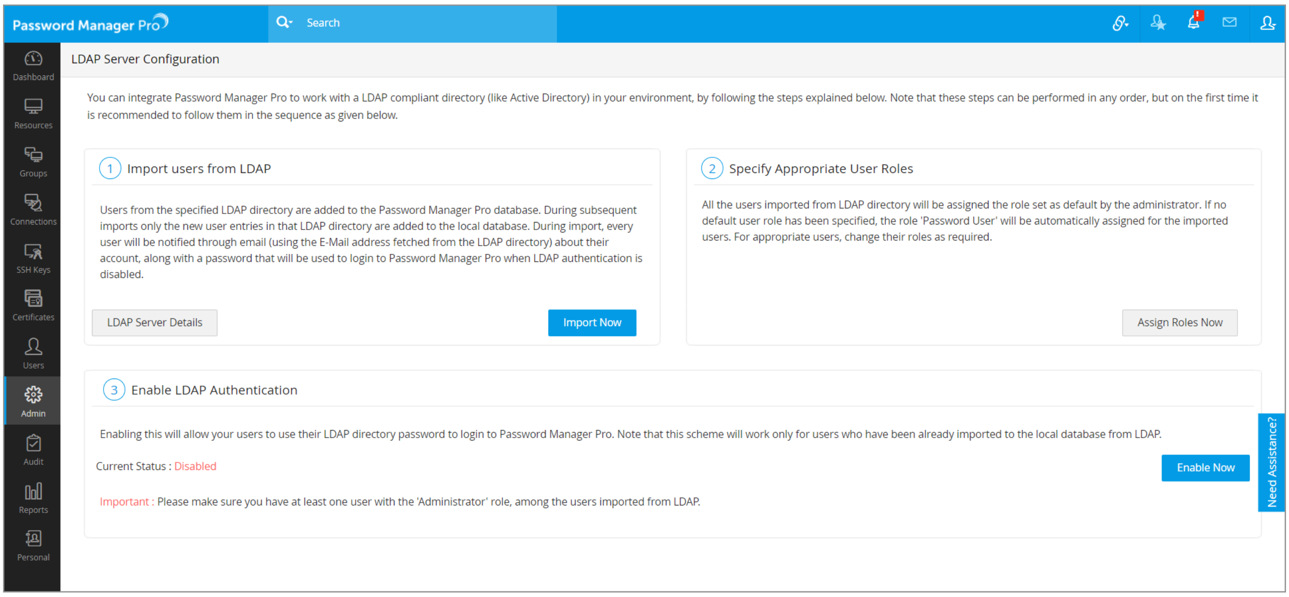
Users who have logged into the Windows system using their domain account need not separately sign in to Password Manager Pro, if this setting is enabled. For this to work, AD authentication should be enabled and the corresponding domain user account should have been imported into PMP. The IE browser supports this by default and follow these instructions to get this working in Firefox.

Current Status : Disabled | Enable Now

Authentication through LDAP

To allow users to login to Password Manager Pro using their LDAP directory passwords, navigate to **Admin** > **Authentication** > **LDAP** and enable the LDAP authentication option.

Note: This authentication scheme will work only for users who have already been imported to the local database from LDAP.



LDAP Server Configuration

You can integrate Password Manager Pro 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.

1 Import users from LDAP

Users from the specified LDAP directory are added to the Password Manager Pro database. During subsequent imports only the new user entries in that LDAP directory are added to the local database. During import, every user will be notified through email (using the E-Mail address fetched from the LDAP directory) about their account, along with a password that will be used to login to Password Manager Pro when LDAP authentication is disabled.

LDAP Server Details | Import Now

2 Specify Appropriate User Roles

All the users imported from LDAP directory will be assigned the role set as default by the administrator. If no default user role has been specified, the role 'Password User' will be automatically assigned for the imported users. For appropriate users, change their roles as required.

Assign Roles Now

3 Enable LDAP Authentication

Enabling this will allow your users to use their LDAP directory password to login to Password Manager Pro. Note that this scheme will work only for users who have been already imported to the local database from LDAP.

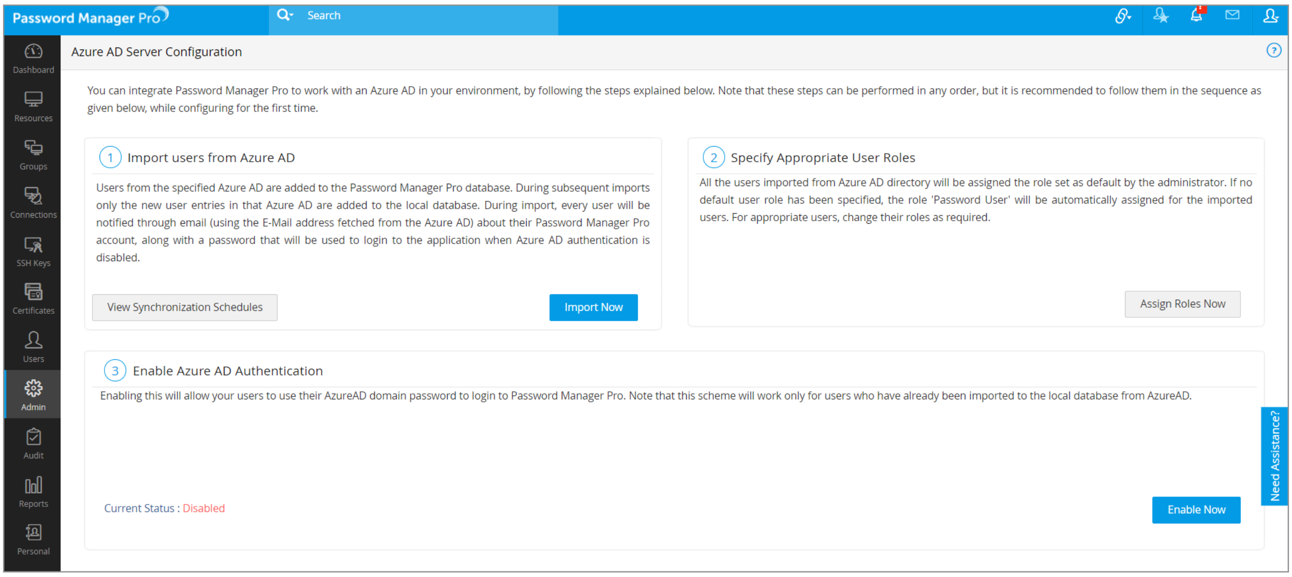
Current Status : Disabled | Enable Now

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

Authentication through Azure AD

To allow users to login to Password Manager Pro using their Azure AD domain passwords, navigate to **Admin** > **Authentication** > **Azure AD** and enable the Azure AD authentication option.

Note: This authentication scheme will work only for users who have already been imported to the local database from Azure AD.



Azure AD Server Configuration

You can integrate Password Manager Pro to work with an Azure AD in your environment, by following the steps explained below. Note that these steps can be performed in any order, but it is recommended to follow them in the sequence as given below, while configuring for the first time.

1 Import users from Azure AD

Users from the specified Azure AD are added to the Password Manager Pro database. During subsequent imports only the new user entries in that Azure AD are added to the local database. During import, every user will be notified through email (using the E-Mail address fetched from the Azure AD) about their Password Manager Pro account, along with a password that will be used to login to the application when Azure AD authentication is disabled.

View Synchronization Schedules | Import Now

2 Specify Appropriate User Roles

All the users imported from Azure AD directory will be assigned the role set as default by the administrator. If no default user role has been specified, the role 'Password User' will be automatically assigned for the imported users. For appropriate users, change their roles as required.

Assign Roles Now

3 Enable Azure AD Authentication

Enabling this will allow your users to use their AzureAD domain password to login to Password Manager Pro. Note that this scheme will work only for users who have already been imported to the local database from AzureAD.

Current Status : Disabled

Enable Now

In addition to this, Password Manager Pro also offers the following first level authentication mechanisms:

Smart-card authentication

If you have a smart-card authentication system in your environment, you can configure Password Manager Pro to authenticate users with their smart cards and their personal identification number (PIN), bypassing other first factor authentication methods like AD, LDAP or Local Authentication.

To turn this setting on, navigate to **Admin tab** > **Authentication** > select **Smart card / PKI / Certificate** in the web interface. For detailed instructions to set up Smart Card authentication, refer to this section of the help documentation.

RADIUS

You can integrate Password Manager Pro with RADIUS server in your environment and leverage the RADIUS authentication for user access, bypassing the local authentication provided by PMP.

To turn this setting on, navigate to **Admin tab** > **Authentication** > select **RADIUS** in the web interface. For detailed instructions on RADIUS server integration, refer to this section of the documentation.

SAML SSO

Password Manager Pro 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 involves supplying details about SP to IdP and vice-versa. Once you integrate PMP with an IdP, the users just need to login to the IdP and then, they can automatically login to PMP from the respective identity provider's GUI without having to provide credentials again.

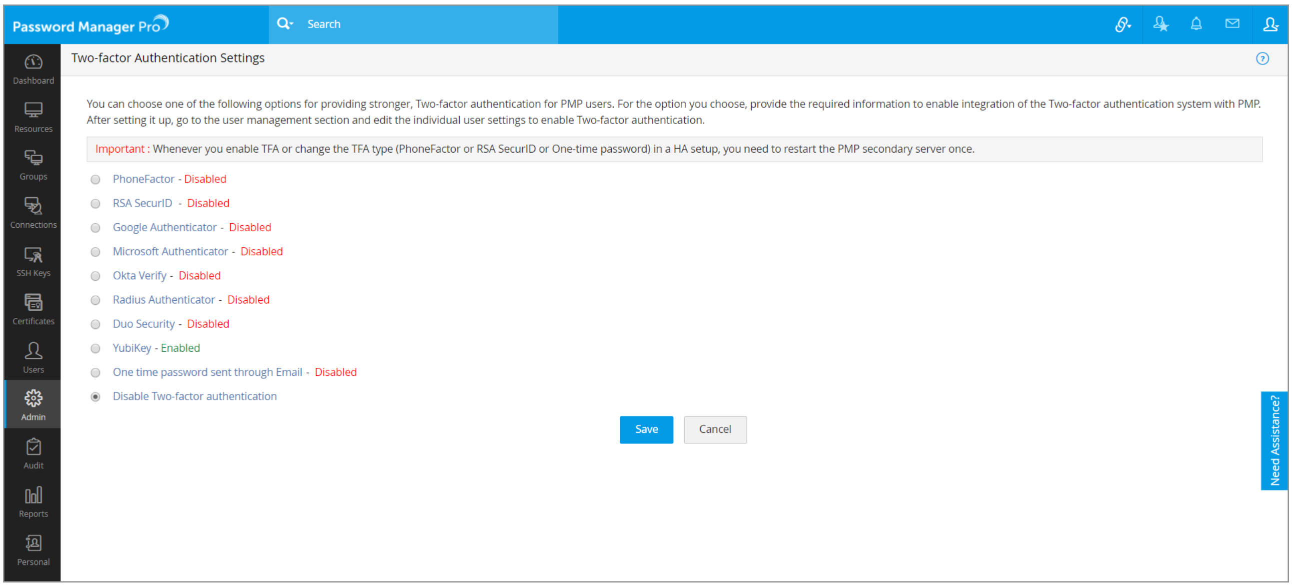
To turn this setting on, navigate to **Admin tab** > **Authentication** > select **SAML Single Sign On** in the web interface. For detailed instructions on SAML Single Sign On authentication, refer to this section of the documentation.

Configure two-factor authentication (recommended)

If your organization requires an additional layer of security, you can configure two-factor authentication (TFA) and mandate users to go through two successive stages of authentication before login. Once configured, your users will have to go through two steps:

1. First level authentication through native or AD or LDAP.
2. Second level authentication through any one of the mechanisms below:
    - PhoneFactor
    - RSA SecurID
    - Google Authenticator
    - Microsoft Authenticator

- Okta Verify
- RADIUS Authenticator
- Duo Security
- Yubikey
- A unique one time password through email



Two-factor Authentication Settings

You can choose one of the following options for providing stronger, Two-factor authentication for PMP users. For the option you choose, provide the required information to enable integration of the Two-factor authentication system with PMP. After setting it up, go to the user management section and edit the individual user settings to enable Two-factor authentication.

Important : Whenever you enable TFA or change the TFA type (PhoneFactor or RSA SecurID or One-time password) in a HA setup, you need to restart the PMP secondary server once.

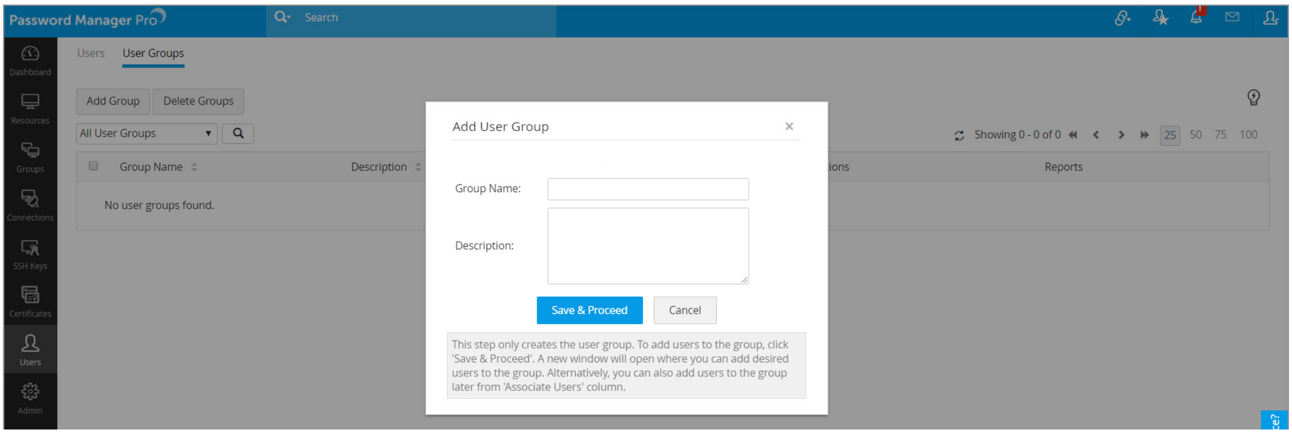
○ PhoneFactor - Disabled
○ RSA SecurID - Disabled
○ Google Authenticator - Disabled
○ Microsoft Authenticator - Disabled
○ Okta Verify - Disabled
○ Radius Authenticator - Disabled
○ Duo Security - Disabled
○ YubiKey - Enabled
○ One time password sent through Email - Disabled
● Disable Two-factor authentication

Save Cancel

To turn this setting on, navigate to **Admin tab** > **Authentication** > **Two-factor Authentication** in the web interface.

Create user groups

After adding users, you can group them to carry out operations in bulk. For example, you can create a user group for all Windows administrators and then allot passwords in bulk to this particular user group. To create a user group, navigate to the **Users** tab > **User Groups** and click on **'Add Group.'** You will find detailed information on creating user groups in this section of our help documentation.



No user groups found.

Add User Group

Group Name:

Description:

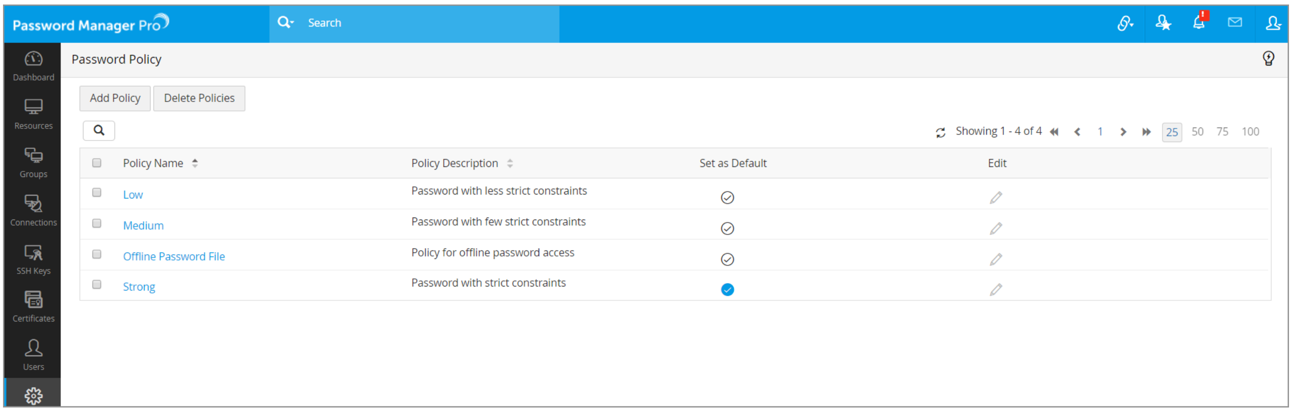
Save & Proceed Cancel

This step only creates the user group. To add users to the group, click 'Save & Proceed'. A new window will open where you can add desired users to the group. Alternatively, you can also add users to the group later from 'Associate Users' column.

Set password policy

Password Manager Pro helps enforce strong password policies at all levels—be it the users' local authentication passwords or the passwords for managed IT resources. Password Manager Pro comes with a built-in password generator that can generate passwords based on the level of complexity defined in the password policies.

You can specify various conditions including minimum length, mixed characters, numerals, and more, and the generator will create the passwords as required. By default, Password Manager Pro provides three types of policies: low, medium, and strong. You can choose from one of these or create your own custom policy. You can create new password policies from the **Admin** > **Customize** > **Password Policies** section.



□	Policy Name	Policy Description	Set as Default	Edit
□	Low	Password with less strict constraints	○	✎
□	Medium	Password with few strict constraints	○	✎
□	Offline Password File	Policy for offline password access	○	✎
□	Strong	Password with strict constraints	●	✎

You can find detailed instructions on configuring password policies in this section of our help documentation.

Password Management

Add your resources

The term “resource” refers to all devices and applications whose privileged accounts are to be managed by Password Manager Pro. There are various ways to add your resources to Password Manager Pro:

- Scan your network and discover flavors of Windows, Linux, VMware, and network devices, along with their associated privileged accounts.
- Import the Windows resources from your domain.
- Import disparate resources in bulk from a CSV/Tab separated file.

When uploading resource information via a CSV/Tab separated file, it can be shared in two ways

1. As a normal file
2. As a Password-protected ZIP File

Normal File: This option can be used to upload a plain text CSV/Tab separated file directly in which the data is saved as either comma or tab separated values.

Password-protected ZIP File: This option can be used if you wish to upload a password-protected ZIP folder containing the CSV/Tab separated file. If you choose this file format, you must also provide the password and specify the name of the target CSV/Tab separated file in the ‘File Name’ field. In case the ‘File Name’ field is left empty, PMP will automatically import information from the first CSV/Tab separated file that it accessed in the unzipped folder.

- Add resources one by one, manually.

You can find detailed information on the above options in the following sections of our help documentation.

- Privileged Accounts Discovery
- Importing Resources from Active Directory and via a CSV/Tab separated file or KeePass
- Adding Resources Manually

Create resource groups

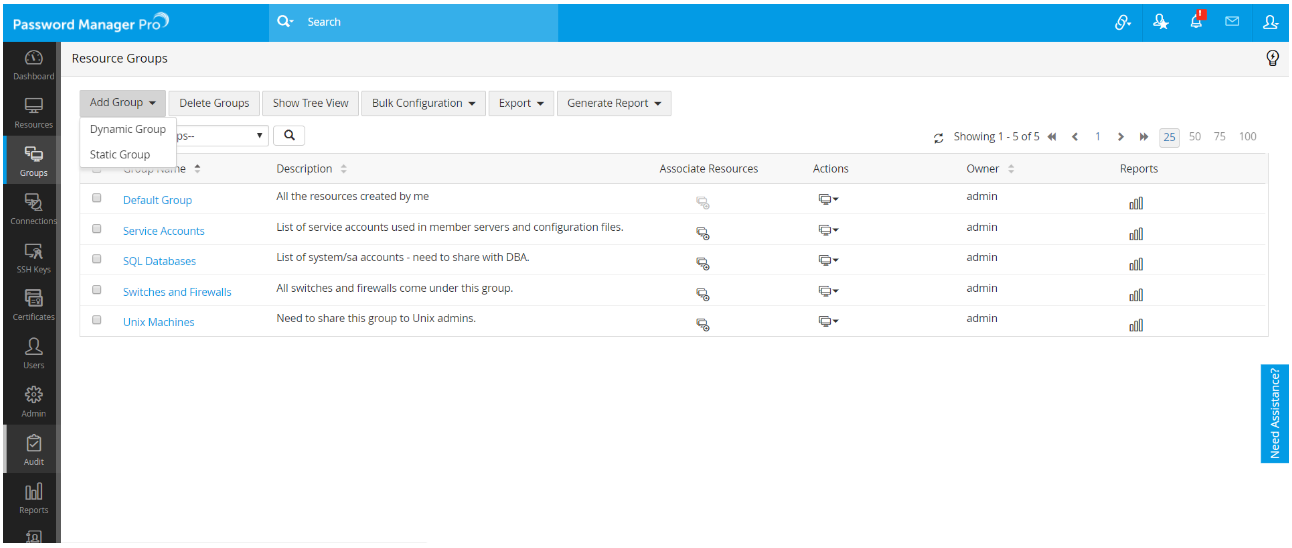
After adding resources, you can group them for better organization and easier management. Resources can be grouped either by specifying a set of criteria or by selecting individual resources.

For static groups, resources are to be added and removed manually, as needed. Whereas in case of a dynamic group, i.e. criteria-based, whenever a newly added resource matches the criteria of an existing group, it automatically becomes a part of that group.

When a resource is added or deleted from a group, it affects the password access shared through the group. That is, when a particular resource group is shared with users, they can see passwords of only the resources that are part of the group at the time of sharing.

To create a resource group(s), navigate to the **Groups,** click **Add Group** and then select **Dynamic Group** or **Static Group.**

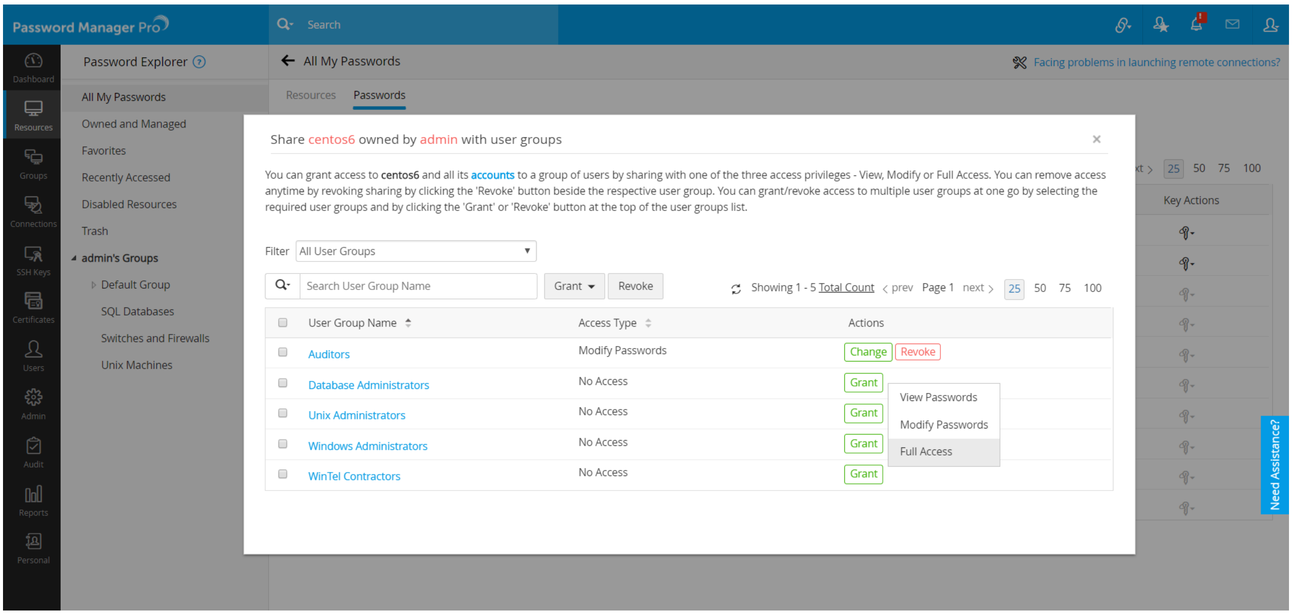
You will find detailed instructions for creating resource groups in [this section]() of our documentation.



Group Name	Description	Associate Resources	Actions	Owner	Reports
Default Group	All the resources created by me			admin	
Service Accounts	List of service accounts used in member servers and configuration files.			admin	
SQL Databases	List of system/sa accounts - need to share with DBA.			admin	
Switches and Firewalls	All switches and firewalls come under this group.			admin	
Unix Machines	Need to share this group to Unix admins.			admin	

Share accounts, resources, and resource groups

In a single click, you can share an individual account or all accounts within a resource or a group of resources with any users or user groups. While sharing resources with other users, you can also set varying access privileges:



Share centos6 owned by admin with user groups

You can grant access to **centos6** and all its accounts to a group of users by sharing with one of the three access privileges - View, Modify or Full Access. You can remove access anytime by revoking sharing by clicking the 'Revoke' button beside the respective user group. You can grant/revoke access to multiple user groups at one go by selecting the required user groups and by clicking the 'Grant' or 'Revoke' button at the top of the user groups list.

Filter: All User Groups

Search User Group Name | Grant | Revoke | Showing 1 - 5 Total Count ‹ prev Page 1 next › 25 50 75 100

□	User Group Name	Access Type	Actions
□	Auditors	Modify Passwords	Change Revoke
□	Database Administrators	No Access	Grant
□	Unix Administrators	No Access	Grant
□	Windows Administrators	No Access	Grant
□	WinTel Contractors	No Access	Grant

View Passwords: Users and User groups can only access the passwords.

Modify Passwords: Users and User groups can view and edit passwords of the shared resources. However, this privilege does not allow them access to the ‘Resource Actions’ section, which restricts users from changing any other attribute of the resource.

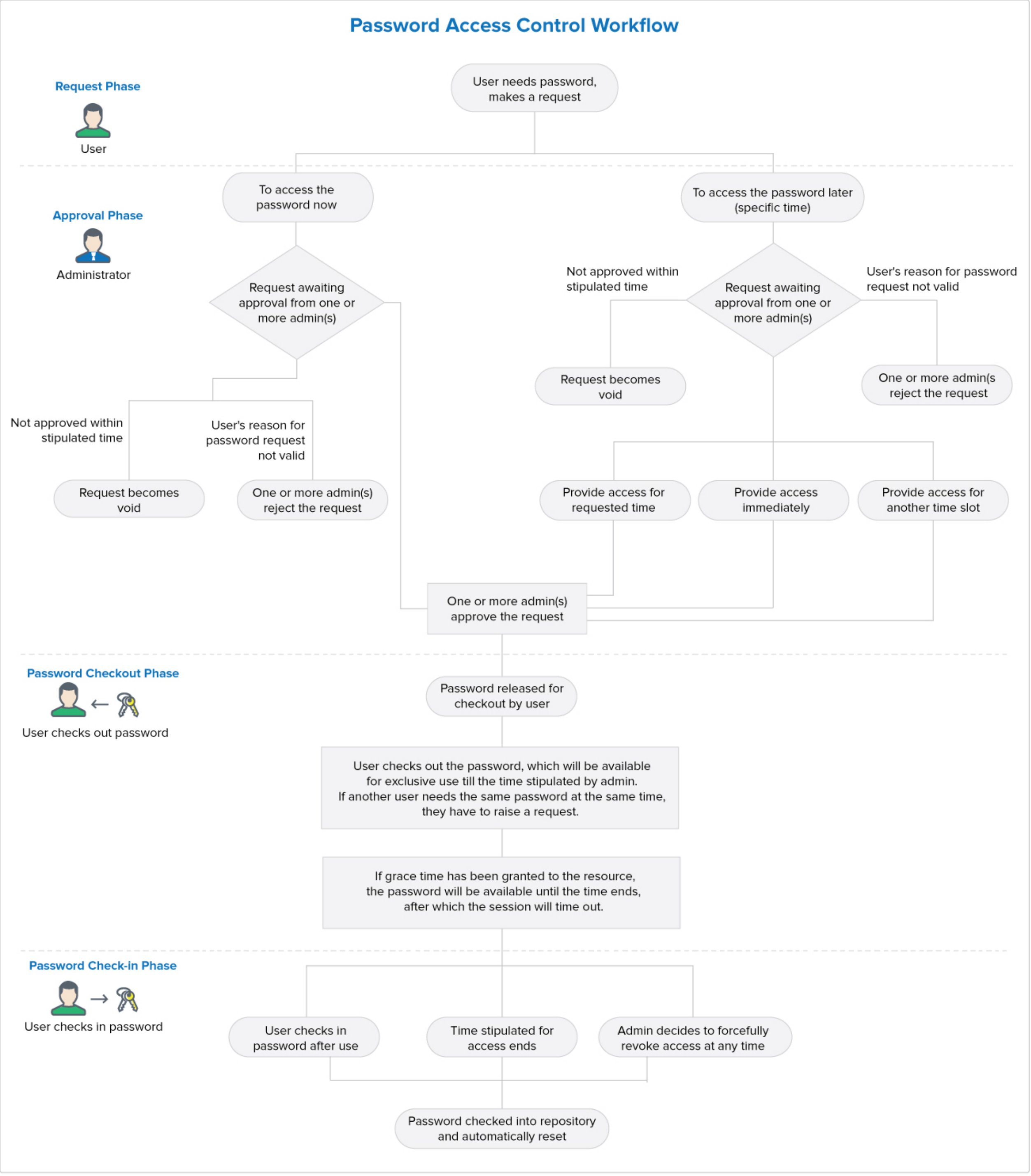
Full Access: Users and User groups have complete management of resource / resource group. They can even re-share the resource or password with other users.

You can find detailed information on sharing resources in this section of our documentation.

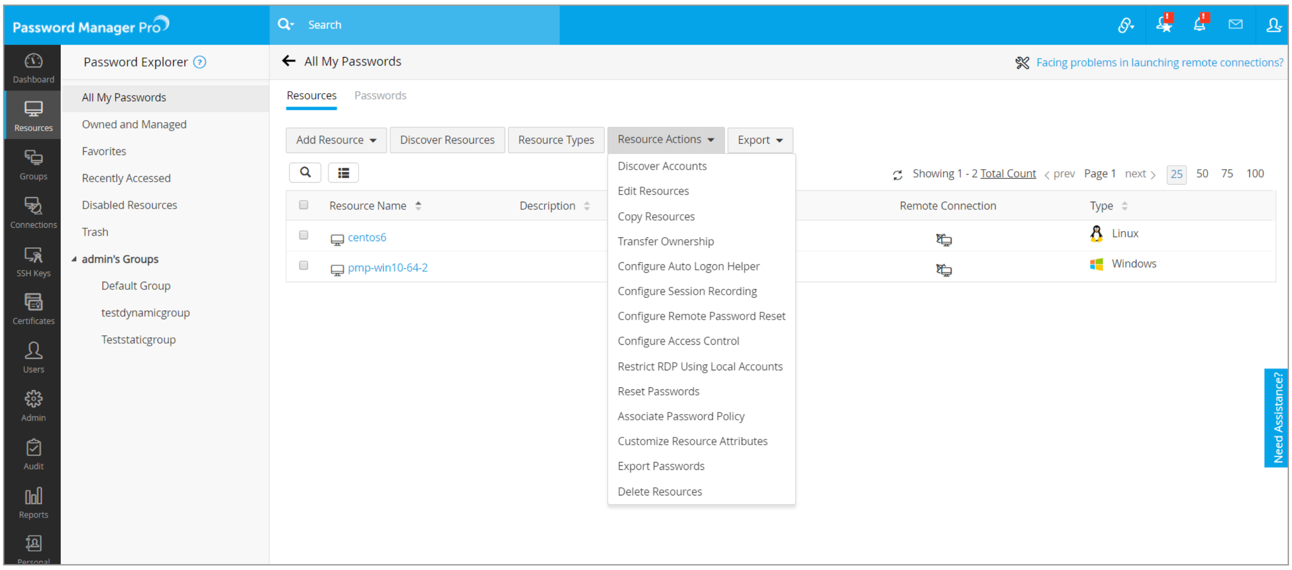
Note: Password Manager Pro allows users to share passwords without revealing them in plaintext in the GUI. This can be done from **Admin** > **General Settings** > **Password Retrieval**. The checkbox for the option **“Allow plain text view of passwords, if auto logon is configured”** should not be selected to exercise this option.

Configure access control workflow

After a successful login to Password Manager Pro, users get instant access to the passwords that are owned by them or shared with them. If needed, you can add an extra layer of security by requiring your users to go through request-release approvals. This mechanism follows a well-defined workflow—users get access only upon administrative approval. The password can be released for a limited period of time, at the end of which it will automatically be reset.


Password Access Control Workflow
Request Phase
User
User needs password, makes a request
Approval Phase
Administrator
To access the password now
To access the password later (specific time)
Request awaiting approval from one or more admin(s)
Not approved within stipulated time
User's reason for password request not valid
Request becomes void
One or more admin(s) reject the request
Request awaiting approval from one or more admin(s)
Not approved within stipulated time
User's reason for password request not valid
Request becomes void
One or more admin(s reject the request
Provide access for requested time
Provide access immediately
Provide access for another time slot
One or more admin(s) approve the request
Password Checkout Phase
User checks out password
Password released for checkout by user
User checks out the password, which will be available for exclusive use till the time stipulated by admin. If another user needs the same password at the same time, they have to raise a request.
If grace time has been granted to the resource, the password will be available until the time ends, after which the session will time out.
Password Check-in Phase
User checks in password
User checks in password after use
Time stipulated for access ends
Admin decides to forcefully revoke access at any time
Password checked into repository and automatically reset

To configure access controls, navigate to the **Resource** tab, select the resources for which you want to configure access controls, and click on **Configure Access Control** from the **Resource Actions** drop-down menu.



Password Manager Pro

Search

Password Explorer

- All My Passwords
- Owned and Managed
- Favorites
- Recently Accessed
- Disabled Resources
- Trash
- admin's Groups
  - Default Group
  - testdynamicgroup
  - Teststaticgroup

All My Passwords

Facing problems in launching remote connections?

Resources | Passwords

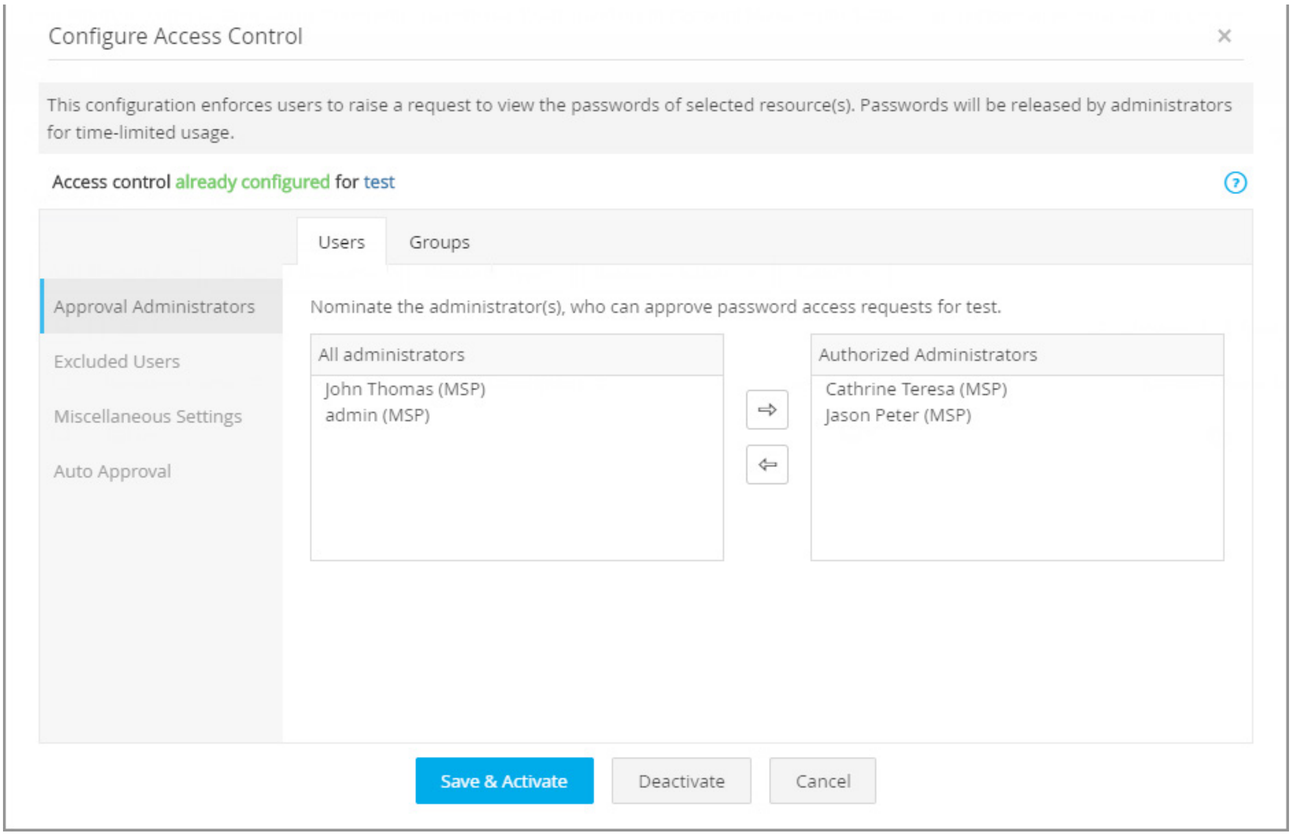
Add Resource | Discover Resources | Resource Types | Resource Actions | Export

Resource Actions:

- Discover Accounts
- Edit Resources
- Copy Resources
- Transfer Ownership
- Configure Auto Logon Helper
- Configure Session Recording
- Configure Remote Password Reset
- Configure Access Control
- Restrict RDP Using Local Accounts
- Reset Passwords
- Associate Password Policy
- Customize Resource Attributes
- Export Passwords
- Delete Resources

Showing 1 - 2 Total Count prev Page 1 next 25 50 75 100

Resource Name	Description	Remote Connection	Type
centos6			Linux
pmp-win10-64-2			Windows



Configure Access Control

This configuration enforces users to raise a request to view the passwords of selected resource(s). Passwords will be released by administrators for time-limited usage.

Access control already configured for test

Users | Groups

- Approval Administrators
- Excluded Users
- Miscellaneous Settings
- Auto Approval

Nominate the administrator(s), who can approve password access requests for test.

All administrators	Authorized Administrators
John Thomas (MSP) admin (MSP)	Cathrine Teresa (MSP) Jason Peter (MSP)

Save & Activate | Deactivate | Cancel

You can find detailed instructions and use cases for configuring access control workflows in this section of our documentation.

Configure remote password reset

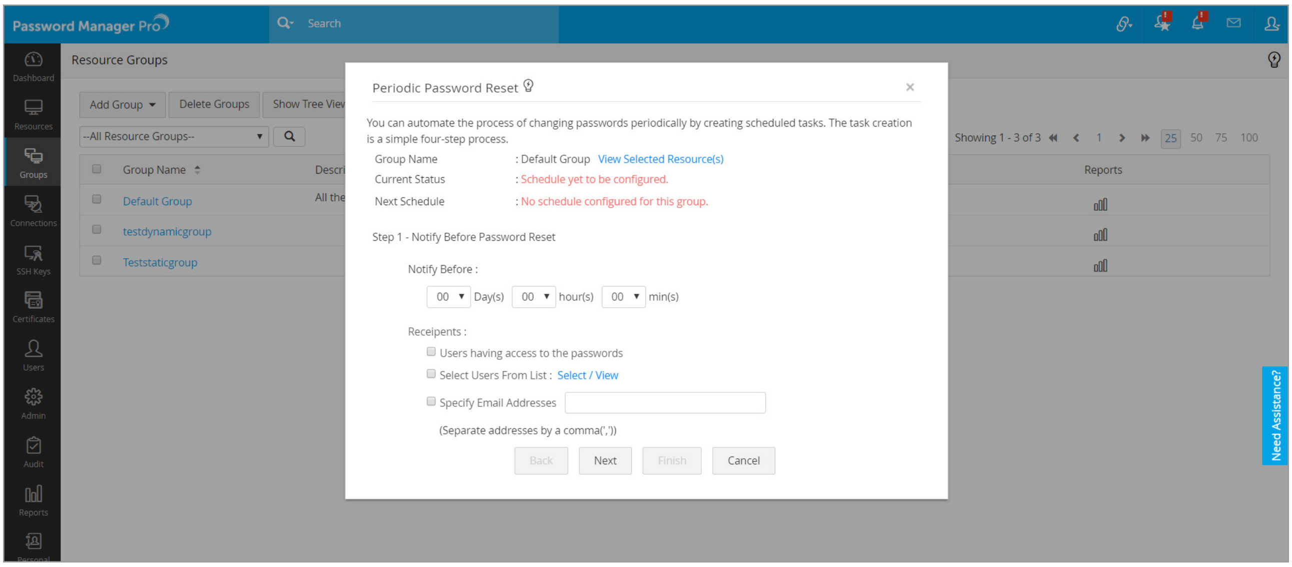
Password Manager Pro helps you reset passwords for a wide range of target systems on demand at any time or automatically at periodic intervals on multiple platforms across physical, virtual, and cloud infrastructures. Password reset can be done in two ways:

With agents	Agent-based resets come in handy when you have to reset passwords for resources without direct connectivity, such as those in DMZ locations or with firewall restrictions. To accomplish these password resets, Password Manager Pro deploys an agent to the remote host to execute the task. All communication between the agent and the application server is one way and over HTTPS.
Without agents	Password Manager Pro directly connects to the target system and changes the password.

Notifications can be sent to users before and after the remote password reset process. The basic configuration required for remote password reset can be carried out as a part of the resource addition. For already added resources, this can also be carried out by editing the resources. This configuration depends on the type of resource being added. Detailed instructions for configuring remote password reset for different types of resources can be found in this section of our documentation.

Configure periodic password reset

You can periodically reset the passwords of remote resources by creating reset schedules. This can be done at the resource group level. Password Manager Pro will assign a strong, unique password to each account belonging to the resource group. To configure periodic password reset, navigate to the Groups tab, Click the **“Actions”** icon against the required resource group and select Periodic Password Reset from the drop-down.



Periodic Password Reset

You can automate the process of changing passwords periodically by creating scheduled tasks. The task creation is a simple four-step process.

Group Name	: Default Group View Selected Resource(s)
Current Status	: Schedule yet to be configured.
Next Schedule	: No schedule configured for this group.

Step 1 - Notify Before Password Reset

Notify Before :

00 Day(s) 00 hour(s) 00 min(s)

Receipents :

□ Users having access to the passwords

□ Select Users From List : Select / View

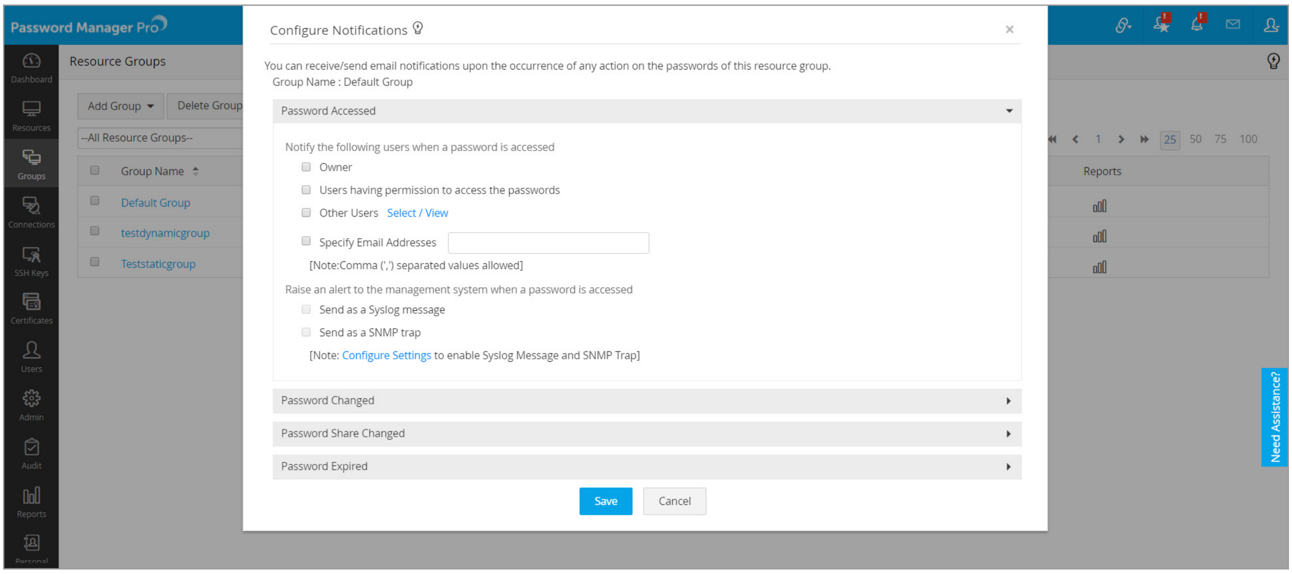
□ Specify Email Addresses

(Separate addresses by a comma(','))

Detailed information on configuring password reset schedules is available in [this section](#) of our documentation.

Configure notifications for password actions

When any action is performed on a password—be it a password access, modification, or changing the share permission when the password expires or when password policy is violated—notifications are sent to the password owners, those who have access to the passwords, and/or to any other users as desired by the administrators. The Password Action Notification feature helps you achieve this.



Configure Notifications

You can receive/send email notifications upon the occurrence of any action on the passwords of this resource group.
Group Name : Default Group

Password Accessed

Notify the following users when a password is accessed

- □ Owner
- □ Users having permission to access the passwords
- □ Other Users Select / View
- □ Specify Email Addresses

[Note:Comma (',') separated values allowed]

Raise an alert to the management system when a password is accessed

- □ Send as a Syslog message
- □ Send as a SNMP trap

[Note: Configure Settings to enable Syslog Message and SNMP Trap]

Password Changed

Password Share Changed

Password Expired

Save Cancel

These settings can be configured at the resource group level. Navigate to the Groups tab, click on the **“Actions”** icon against the group for which you need to enable action notifications and select **“Configure Notifications”** from the drop-down list.Detailed information on configuring password actions notifications can be found in this section of our documentation.

Advanced Features

Direct connection to websites and applications

By configuring automatic login, you can launch a direct connection to websites and applications from within Password Manager Pro’s web interface. This can be done by using native browser extensions.

You can find detailed information for Chrome, Firefox, and IE browser extensions in the following sections of our documentation.

- Browser extension for Chrome
- Browser extension for Firefox
- Browser extension for IE

Direct connection to remote systems

Password Manager Pro allows you to automatically log in to remote target systems directly from its web interface with the Auto-logon gateway option. Auto-logon gateway is useful for launching Windows RDP, VNC, SSH, and SQL sessions. Detailed information on how to use this feature is available in this section of our help documentation.

APIs to eliminate hard-coded credentials

Various applications require access to databases and other applications frequently to query business-related information. This communication process is usually automated by embedding the application credentials in plain text within configuration files and scripts. While hard-coding credentials makes a technician’s job easier, it’s also an easy launch point for hackers.

Application-to-application password management

Password Manager Pro eliminates hard-coded passwords with secure APIs for application-to-application (A-to-A) password management. Password Manager Pro provides password management APIs, through which any business application or script can query and retrieve passwords to connect with other applications or databases. This way, the A-to-A passwords are also subject to security best practices such as periodic password rotation, without needing to make manual updates in multiple places.

To configure the APIs, navigate to **Admin** > **Configuration** > **Password Management API.**

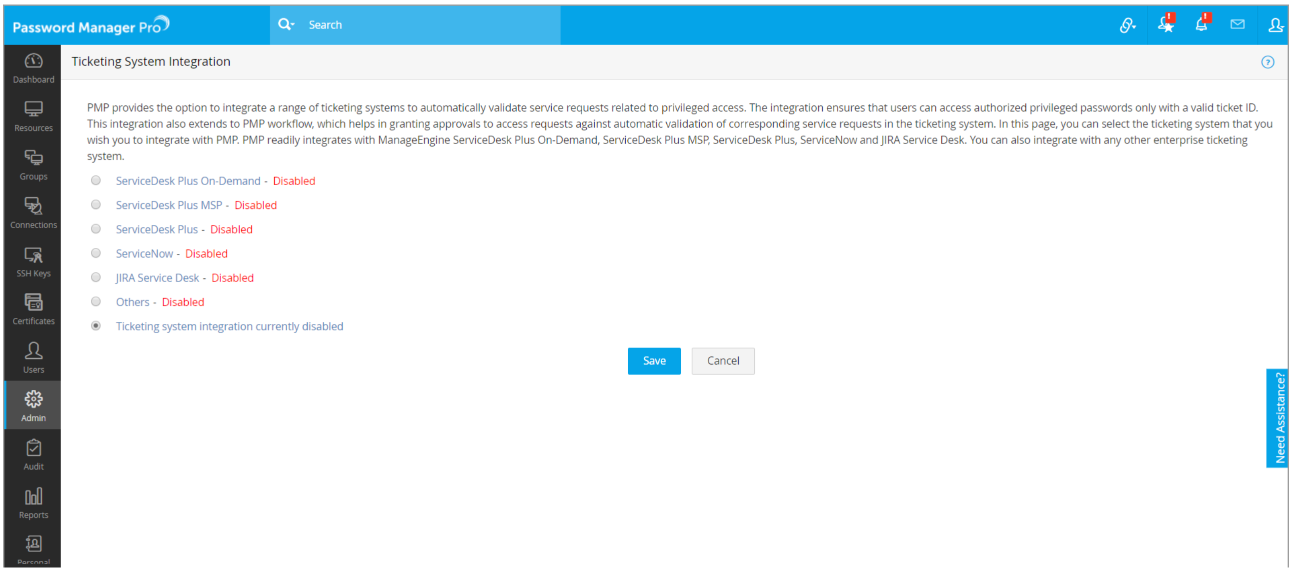
For detailed instructions on configuring the password management API, refer to this section of our documentation

Rest API

The most widely-used API in Password Manager Pro is the REpresentational State Transfer (REST) or the RESTful API. The APIs that belong to this category allow you to add resources, accounts, retrieve passwords, resource/account details and update passwords programmatically. The first step in the process of configuring password management APIs involves creation of API user accounts in Password Manager Pro. For detailed instructions on this, refer to this section of the help documentation.

Ticketing system integration

Password Manager Pro lets you 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 Password Manager Pro workflow, which helps you grant approvals to access requests with automatic validation of corresponding service requests in the ticketing system.



Ticketing System Integration

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. In this page, you can select the ticketing system that you wish you to integrate with PMP. PMP readily integrates with ManageEngine ServiceDesk Plus On-Demand, ServiceDesk Plus MSP, ServiceDesk Plus, ServiceNow and JIRA Service Desk. You can also integrate with any other enterprise ticketing system.

○ ServiceDesk Plus On-Demand - Disabled
○ ServiceDesk Plus MSP - Disabled
○ ServiceDesk Plus - Disabled
○ ServiceNow - Disabled
○ JIRA Service Desk - Disabled
○ Others - Disabled
● Ticketing system integration currently disabled

Save Cancel

To configure this setting, navigate to **Admin tab** > **Integration** > **Ticketing System Integration**. Detailed instructions on the help desk integration are available in this section of our help documentation.

High-availability configuration

For uninterrupted password access, Password Manager Pro offers a high-availability architecture that uses redundant Password Manager Pro server and database instances. The high-availability configuration varies according to the back-end database used. The following sections of our help documentation will guide you through the process of establishing high availability.

- High Availability (PostgreSQL)
- High Availability (MS SQL)
- Fail Over Service

Disaster recovery configuration

You can also configure a backup of Password Manager Pro's database to recover in the event of disasters. Password Manager Pro provides two options to configure database backup:

- Live Backup
- Scheduled Backup.

To configure a data backup, navigate to **Admin** > **Configuration** > **Database Backup**. You can refer to this section of our documentation for more information.

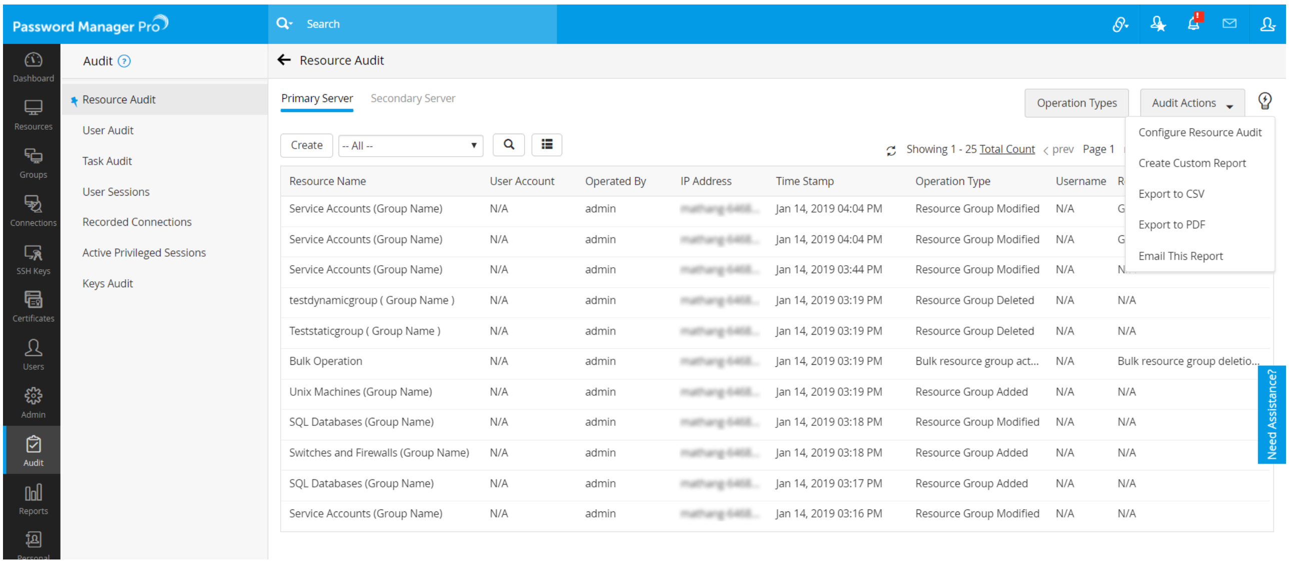
Audit settings

Password Manager Pro comes with an effective auditing mechanism to record trails for every single action performed by each user. All operations performed by users on the GUI are audited with the timestamp for each operation and the IP address from which the user accessed the application. Auditing in Password Manager Pro can be classified into three types:

- **Resource audit** : All operations pertaining to resources, resource groups, accounts, passwords, shares, and policies
- **User audit** : All operations performed in Password Manager Pro by a Password Manager Pro user are captured under User audit.

- **Task audit** : Records of the creation of various scheduled tasks.

The Password Manager Pro audits are quite comprehensive—almost every action is audited. If you only want to audit specific operations, you can specify them based on audit type operation. You can also send notifications to the required recipients whenever a chosen event (audit trail of your choice) occurs.



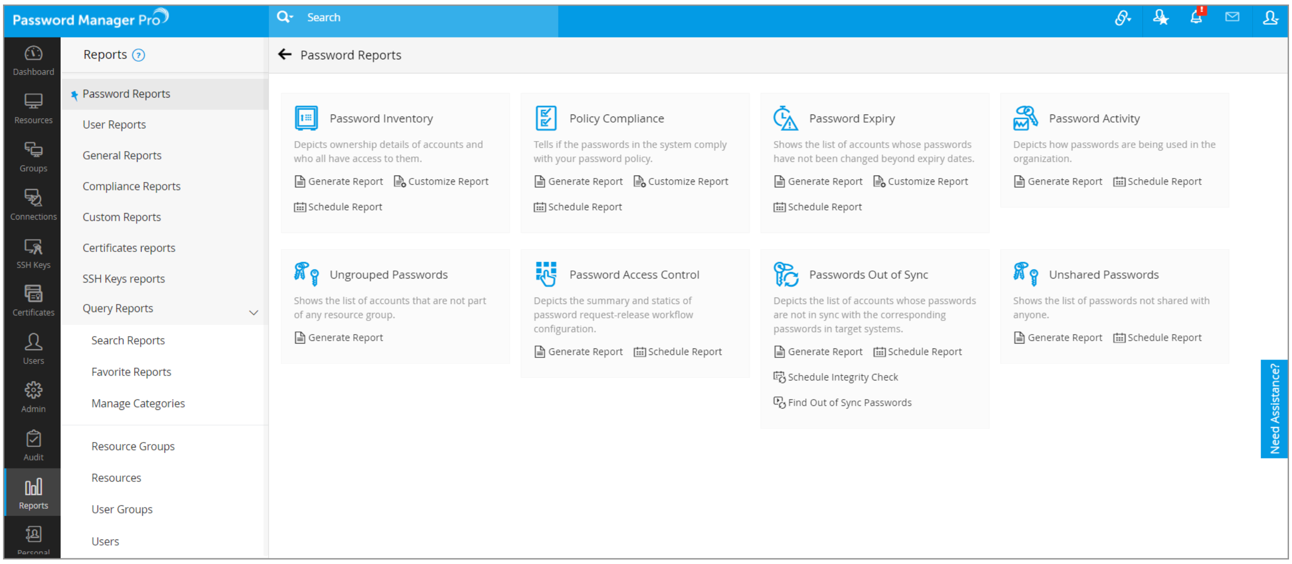
Showing 1 - 25 Total Count < prev Page 1

Resource Name	User Account	Operated By	IP Address	Time Stamp	Operation Type	Username	R
Service Accounts (Group Name)	N/A	admin	[redacted]	Jan 14, 2019 04:04 PM	Resource Group Modified	N/A	G
Service Accounts (Group Name)	N/A	admin	[redacted]	Jan 14, 2019 04:04 PM	Resource Group Modified	N/A	G
Service Accounts (Group Name)	N/A	admin	[redacted]	Jan 14, 2019 03:44 PM	Resource Group Modified	N/A	N
testdynamicgroup (Group Name)	N/A	admin	[redacted]	Jan 14, 2019 03:19 PM	Resource Group Deleted	N/A	N/A
Teststaticgroup (Group Name)	N/A	admin	[redacted]	Jan 14, 2019 03:19 PM	Resource Group Deleted	N/A	N/A
Bulk Operation	N/A	admin	[redacted]	Jan 14, 2019 03:19 PM	Bulk resource group act...	N/A	Bulk resource group deletio...
Unix Machines (Group Name)	N/A	admin	[redacted]	Jan 14, 2019 03:19 PM	Resource Group Added	N/A	N/A
SQL Databases (Group Name)	N/A	admin	[redacted]	Jan 14, 2019 03:18 PM	Resource Group Modified	N/A	N/A
Switches and Firewalls (Group Name)	N/A	admin	[redacted]	Jan 14, 2019 03:18 PM	Resource Group Added	N/A	N/A
SQL Databases (Group Name)	N/A	admin	[redacted]	Jan 14, 2019 03:17 PM	Resource Group Added	N/A	N/A
Service Accounts (Group Name)	N/A	admin	[redacted]	Jan 14, 2019 03:16 PM	Resource Group Modified	N/A	N/A

You can configure each of these audits in the Audit tab on the web interface. More instructions on configuring audits can be found in this section of our documentation.

Reports

Information on the entire privileged account management process in your enterprise is presented in the form of comprehensive reports in Password Manager Pro. The status and summaries of different activities such as password inventory, policy compliance, password expiry, user activity, and more are provided in the form of tables and graphs that help IT administrators make well-informed decisions on password management. Password Manager Pro provides reports under several categories and also lets you create your own reports.



Password Inventory: Depicts ownership details of accounts and who all have access to them.

Policy Compliance: Tells if the passwords in the system comply with your password policy.

Password Expiry: Shows the list of accounts whose passwords have not been changed beyond expiry dates.

Password Activity: Depicts how passwords are being used in the organization.

Ungrouped Passwords: Shows the list of accounts that are not part of any resource group.

Password Access Control: Depicts the summary and statics of password request-release workflow configuration.

Passwords Out of Sync: Depicts the list of accounts whose passwords are not in sync with the corresponding passwords in target systems.

Unshared Passwords: Shows the list of passwords not shared with anyone.

To view and configure reports, navigate to the **Reports** tab in the web interface. You can find detailed instructions in this section of our documentation.

Offline access

Password Manager Pro provides multiple options for secure offline access and safekeeping of password information.

- The most 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 in an encrypted HTML file.
- You can also automatically synchronize the exported HTML file to users' mobile devices through their Dropbox, Box, and Amazon S3 cloud accounts.

Typical use case scenarios for this option include:

1. A managed service provider (MSP) using Password Manager Pro to store the shared passwords of their clients and technicians visiting clients, both of whom have no access to Password Manager Pro installed in their network.
2. Technicians working in DMZs with no access to the Password Manager Pro web interface. Administrators can decide which option (encrypted HTML or auto-sync to mobile devices) should be used in their organization. In addition, the export can be enabled or disabled for specific users or user groups as needed.

More information on exporting passwords can be found in this section of our documentation.

Mobile access

The native mobile app is helpful to securely retrieve passwords on the go. The list of supported mobile platforms and detailed instructions for each platform is given below.

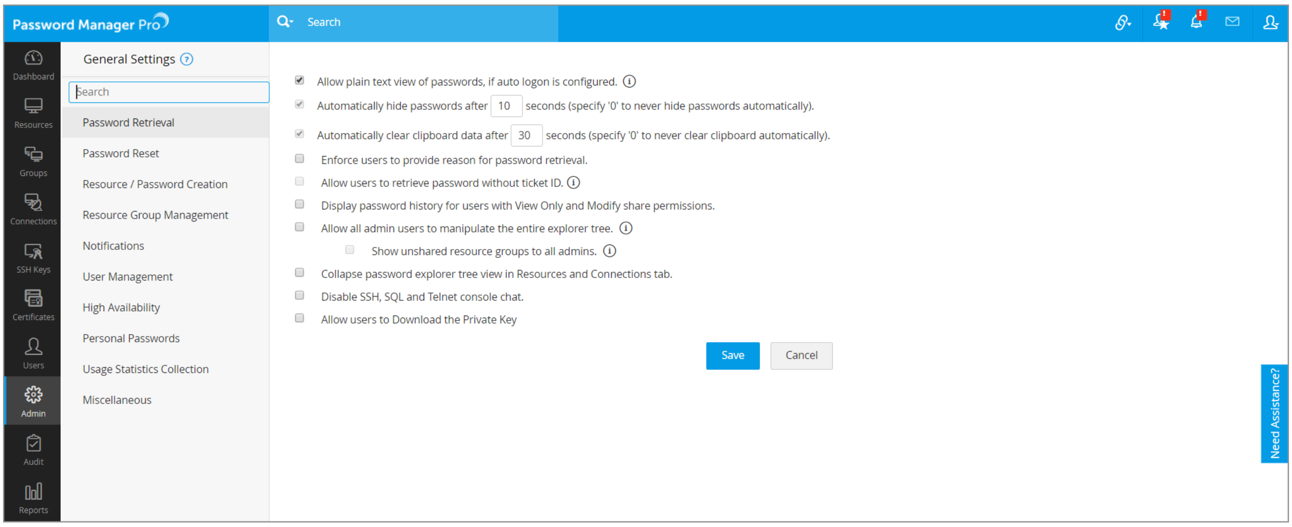
- Android
- iOS

Browser extensions

To smooth out the process of password management and auto-logon, Password Manager Pro gives you the option of securely synchronizing passwords across browsers through native browser extensions. The extensions will be able to auto fill passwords for websites and web applications and also launch RDP and SSH sessions. In addition, the extensions allow you to view all passwords, resource groups, favorites, and recently used, and provides a search option. Once you deploy an extension, you will be able to perform most password management operations directly from the browser extension, while Password Manager Pro runs in the back-ground. Currently, extensions are available for Chrome, Firefox, and IE.

General settings

Password Manager Pro lets you selectively enable or disable various settings based on the specific needs of your organization. You can choose to enforce or disable various policies through these settings. Navigate to **Admin** > **Settings** > **General Settings** to customize your options.



General Settings

- Password Retrieval
- Password Reset
- Resource / Password Creation
- Resource Group Management
- Notifications
- User Management
- High Availability
- Personal Passwords
- Usage Statistics Collection
- Miscellaneous

☑ Allow plain text view of passwords, if auto logon is configured.

☑ Automatically hide passwords after 10 seconds (specify '0' to never hide passwords automatically).

☑ Automatically clear clipboard data after 30 seconds (specify '0' to never clear clipboard automatically).

□ Enforce users to provide reason for password retrieval.

□ Allow users to retrieve password without ticket ID.

□ Display password history for users with View Only and Modify share permissions.

□ Allow all admin users to manipulate the entire explorer tree.

□ Show unshared resource groups to all admins.

□ Collapse password explorer tree view in Resources and Connections tab.

□ Disable SSH, SQL and Telnet console chat.

□ Allow users to Download the Private Key

Save Cancel

Security specifications for review

Password Manager Pro has been designed to offer maximum security from the installation of the application to user authentication, data transmission, storage, and throughout the usage workflow. You can review Password Manager Pro's security specifications here and decide on the appropriate security configurations for your organization.

Best practices to follow

You can follow certain best practices at all stages—product installation, configuration, setup, and deployment—with a special focus on data security. Refer to the best practices guide for details.

Contact details for technical assistance

If you face problems getting started with the product or if you are in need of any further assistance, our tech support team is just an email or a phone call away.

Email: **passwordmanagerpro-support@manageengine.com**
Toll-free number: **+1-408-454-4014**