ManageEngine
Password Manager Pro

End User Guide

Designed for Password Users and Password Auditors.

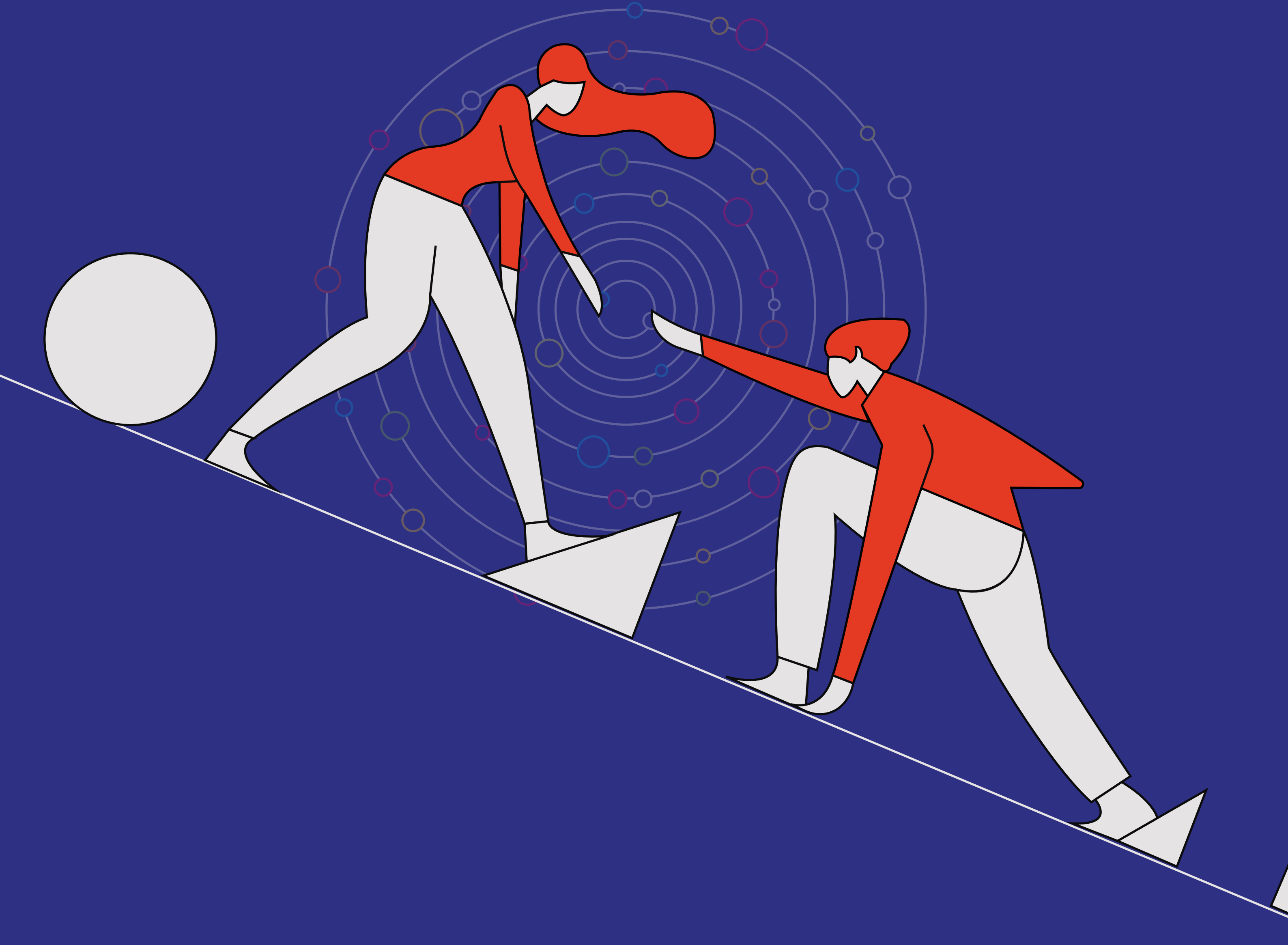


TABLE OF CONTENTS

About Password Manager Pro

ManageEngine Password Manager Pro is a comprehensive privileged account management solution that helps organizations consolidate privileged identities in a secure, centralized repository. Credentials of any sensitive IT assets such as servers, network equipment, web applications, virtual devices, and SaaS accounts—including certificates and other digital files—can be stored and managed via Password Manager Pro.

This solution also enables direct RDP, SSH, and SQL connections to remote systems through an encrypted session gateway to ensure maximum security. Its extensive auditing capability further helps in tracking who accessed what and when, thereby ensuring accountability in a multi-user environment.

About this guide

This guide is created to function as an informative collateral for the end users in Password Manager Pro, i.e users with the following roles:

1. Password Users
2. Password Auditors
3. Custom roles with the same privileges as Password Users and Password Auditors.

This guide highlights what operations end users can perform in Password Manager Pro, what modules and features they will have access to, and how they can use the solution for secure privileged account management as well as personal password management.

If you're a **Password User**, you will have access to these tabs in Password Manager Pro's web interface:

1. Resources: Here, you will find all the resources and the corresponding accounts that your administrator has shared with you.
2. Connections: Through this tab, you can launch remote connections (RDP, VNC, SSH, SQL) to target systems using the shared credentials.
3. Personal: The Personal tab lets you store your personal data like credit card numbers, bank account information, contact addresses, phone numbers, email addresses, etc. You can also protect them with an exclusive passphrase that only you'll have access to.

If you're a **Password Auditor**, apart from the aforementioned tabs, you'll also have access to the following tabs:

4. Dashboard: This tab provides an overview of all password and user-related activities in the form of tables and charts.
5. Audit: Get a complete record of who accessed which resource at what time along with trails about every single action performed by users within the application. True to your role, this tab lets you audit all the privileged activities performed on resources, resource groups, accounts, passwords, certificates, scheduled tasks, and policies in Password Manager Pro.
6. Reports: This tab helps you generate intuitive reports on password and user -related operations that you can use to enhance the management of privileged data in your organization. Apart from built-in reports, you can effortlessly filter out desired information from Password Manager Pro's database in the form of custom reports.

How secure your credentials are in Password Manager Pro.

Password Manager Pro's vaulting mechanism offers comprehensive defense against intrusion with the following measures:

- Sensitive data, like passwords and keys, undergoes dual encryption, i.e., it's encrypted once in the application using AES-256 and once in the database.
- All your personal passwords stored in Password Manager Pro will also be encrypted. To further enhance security, your administrator can also mandate that you create a strong passphrase required to access your personal passwords.
- Role-based, fine-grained user authentication ensures that users are allowed to view passwords based only on the authorization provided to them.
- All transactions through the Password Manager Pro browser take place through HTTPS.

Refer to our Security Specifications document for more details on the security measures followed by Password Manager Pro.

Important terminologies

Refer to this table for explanation about the various terms used in the guide.

Term	Definition
Resource	Any server/application/device that's usernames and passwords are to be managed by Password Manager Pro.
Resource group	A group consisting of similar resources. For example, if you have a few Windows XP resources among many other Windows servers, you can group all the Windows XP servers into a single resource group.
Account	The user account and the corresponding password to be managed by Password Manager Pro.
Remote system	A remote system is a device, application, or server to which you do not have physical access, but that you can access or manipulate via a network.

1. Connecting to Password Manager Pro's web interface

Open a browser and go to **https://<hostname>:port** (but with your host name in place of *hostname* and your port number instead of *port*). Since the connection is through HTTPS, the data communicated over this channel is secure. If a proper certificate is in place, the web console will take you to the authentication page instantly. On the other hand, if a self-signed certificate is used, then a warning message regarding certificate security will pop up, which you'll have to accept in order to proceed to the authentication page.

2. Logging in to Password Manager Pro

In the authentication page, log in to Password Manager Pro by entering your credentials. This can be done through Password Manager Pro's local authentication, or by using AD, LDAP, RADIUS, or Smartcard credentials—whichever option is configured by your administrator.

If local authentication is set up for your account, contact your administrator for the credentials. If two-factor authentication is enforced for you by your administrator, you'll have to authenticate through another stage to access Password Manager Pro's web interface. The second level of authentication can be through any of the following as set by your administrator:

- PhoneFactor Authentication
- RSA SecurID Authentication
- Google Authenticator
- Microsoft Authenticator
- Okta Verify Authenticator
- RADIUS server or Any RADIUS-compliant Authentication
- Duo Security Authentication
- YubiKey Authentication
- Unique Password sent through email

Note: *Users that don't have two-factor authentication enabled will be allowed to log in to Password Manager Pro if they complete the first level of authentication.*

3. Resources

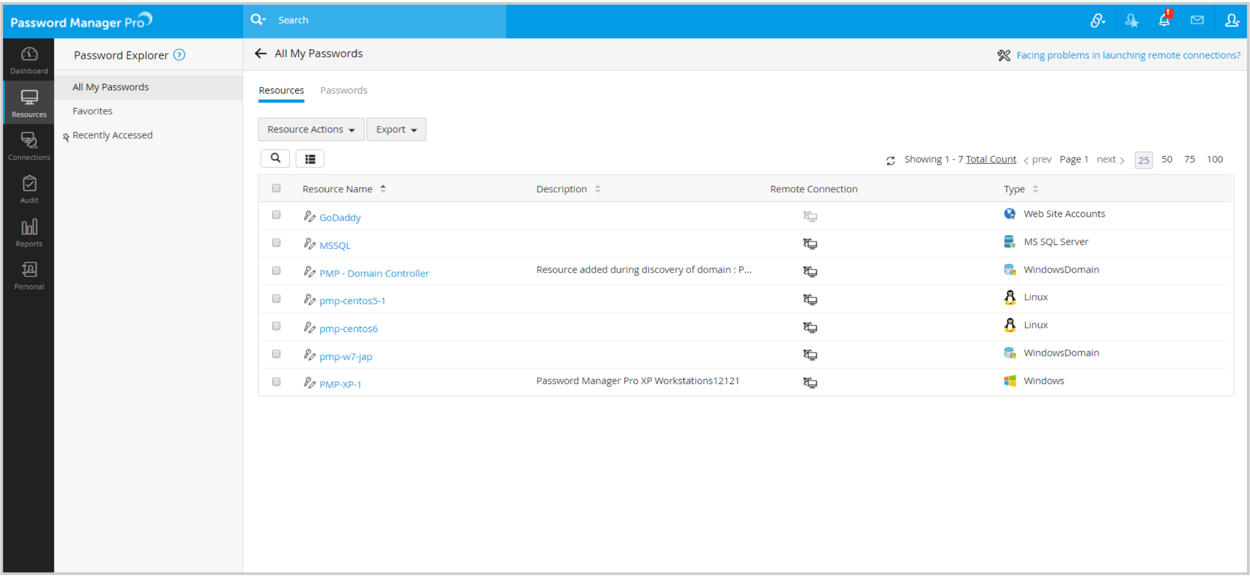
You can view all the resources shared with you by administrators as well as the corresponding account details from the *Resources* tab. The *Password Explorer* menu displays the following:

A. All My Passwords
B. Favorites
C. Recently Accessed
D. Password Explorer Tree

A. All My Passwords

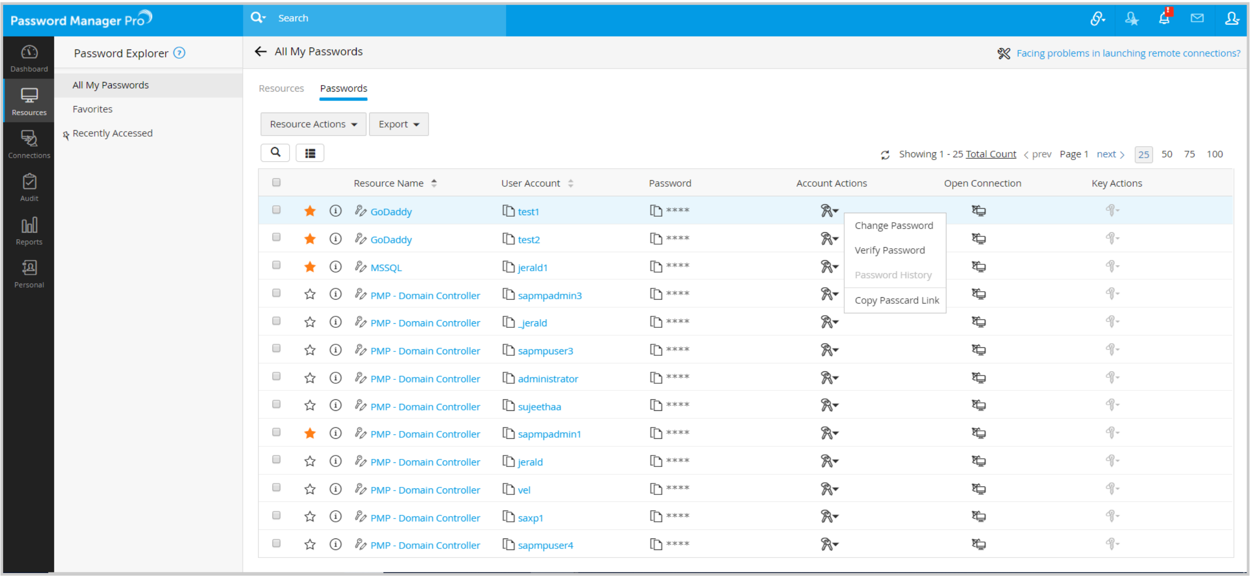
Under this tab, you can find all the resources that are shared with you, the corresponding accounts under those resources, and their respective passwords/SSH keys (masked with asterisks).

- The *Resources* tab at the top displays the resource details. From here, you can carry out resource-based operations. You can click on any resource from the list to find its accounts and the corresponding passwords.



	Resource Name	Description	Remote Connection	Type
□	GoDaddy			Web Site Accounts
□	MSSQL			MS SQL Server
□	PMP - Domain Controller	Resource added during discovery of domain : P...		WindowsDomain
□	pmp-centos5-1			Linux
□	pmp-centos6			Linux
□	pmp-w7-jap			WindowsDomain
□	PMP-XP-1	Password Manager Pro XP Workstations12121		Windows

- Under the *Passwords* tab, you can find the resources and accounts shared with you along with their respective passwords. From the *Account Actions* drop-down, you can also carry out account operations like changing and verifying passwords and viewing password history.



			Resource Name	User Account	Password	Account Actions	Open Connection	Key Actions
□	★	ⓘ	GoDaddy	test1	****			
□	★	ⓘ	GoDaddy	test2	****			
□	★	ⓘ	MSSQL	jerald1	****			
□	☆	ⓘ	PMP - Domain Controller	sapmpadmin3	****			
□	☆	ⓘ	PMP - Domain Controller	_jerald	****			
□	☆	ⓘ	PMP - Domain Controller	sapmpuser3	****			
□	☆	ⓘ	PMP - Domain Controller	administrator	****			
□	☆	ⓘ	PMP - Domain Controller	sujeethaa	****			
□	★	ⓘ	PMP - Domain Controller	sapmpadmin1	****			
□	☆	ⓘ	PMP - Domain Controller	jerald	****			
□	☆	ⓘ	PMP - Domain Controller	vel	****			
□	☆	ⓘ	PMP - Domain Controller	saxp1	****			
□	☆	ⓘ	PMP - Domain Controller	sapmpuser4	****			

Note: *You'll be allowed to view and/or change the passwords depending on the access provided to you by the resource's owner.*

Operations you can perform from the Resources tab

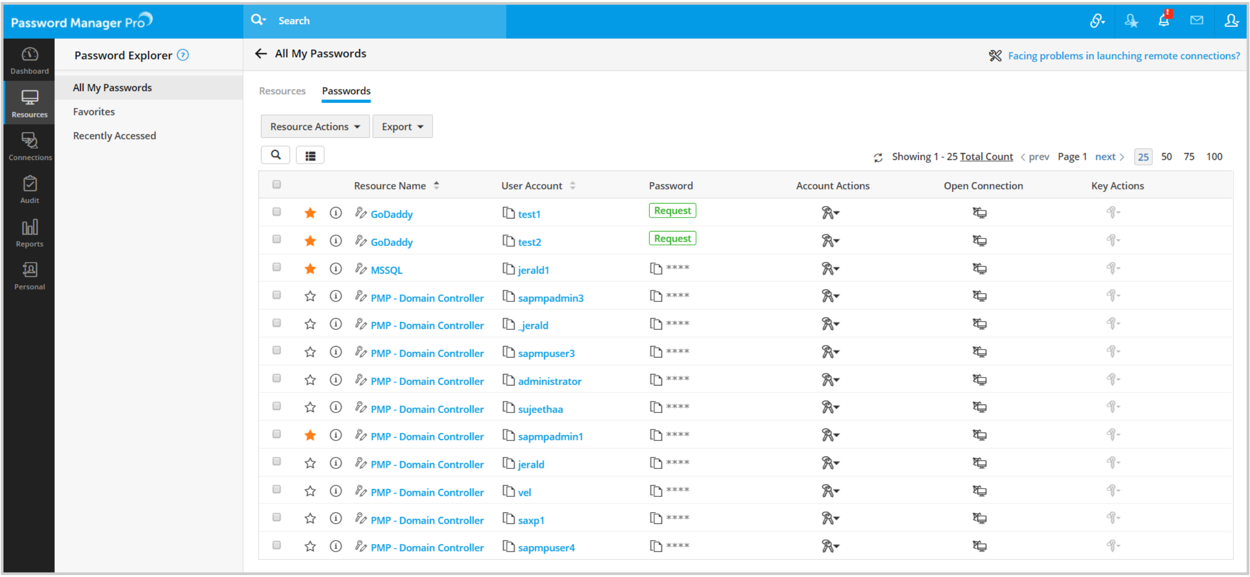
You can perform several actions from the *Resources* tab like retrieving and copying passwords, exporting passwords, searching for a particular password, or opening a remote connection to the target system.

Retrieving passwords

Case 1: Viewing passwords by clicking on the asterisks. By default, passwords are hidden and displayed as asterisks. If your administrator has not set up any restrictions for retrieving passwords, you can simply click on the asterisks to view the passwords in plaintext.

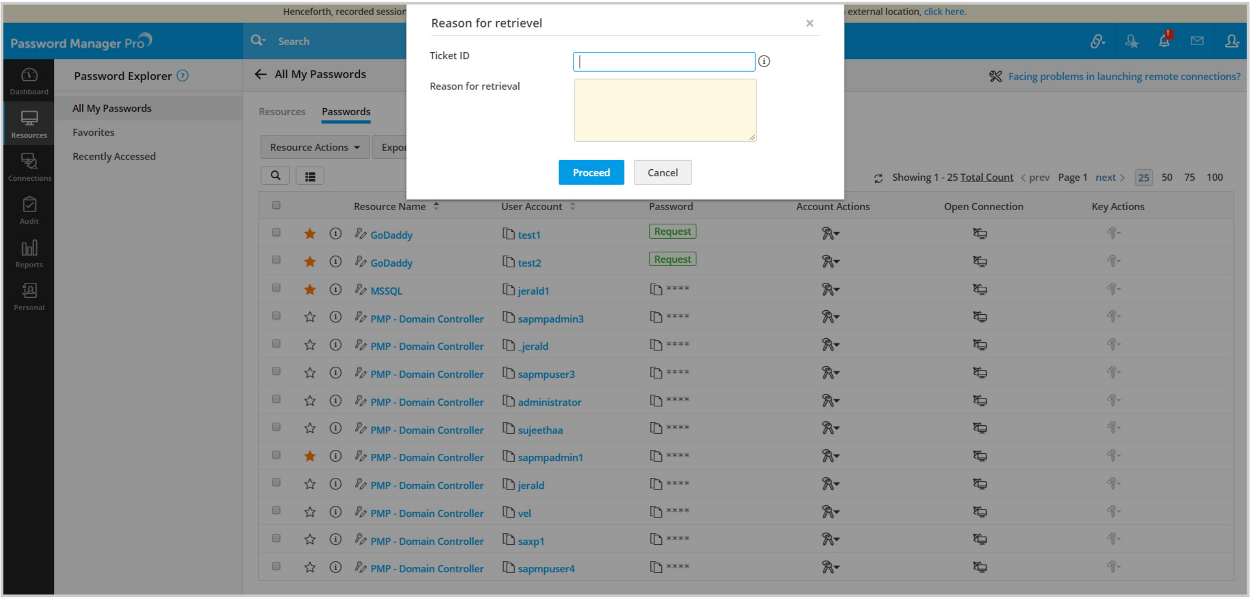
Case 2: Retrieving passwords upon providing a valid reason. In this case, when you try to view, copy, or modify passwords, you'll be prompted to enter a reason for the attempt. Once you submit a valid reason, the passwords will be available until the stipulated time set by your administrator.

Case 3: Access control workflow. There are cases when your administrator might enforce access control for selected resources. In such circumstances, Password Manager Pro will require you to raise a request to your administrator when you need to access the accounts under those resources. Resources with access control enabled will display a *Request* button as shown in the image below. Once the authorized administrator reviews and approves your request, you'll be able to access the credentials for a specific time period as provisioned by the administrator.



Resource Name	User Account	Password	Account Actions	Open Connection	Key Actions
GoDaddy	test1	Request			
GoDaddy	test2	Request			
MSSQL	jerald1	****			
PMP - Domain Controller	sapmpadmin3	****			
PMP - Domain Controller	_jerald	****			
PMP - Domain Controller	sapmpuser3	****			
PMP - Domain Controller	administrator	****			
PMP - Domain Controller	sujeethaa	****			
PMP - Domain Controller	sapmpadmin1	****			
PMP - Domain Controller	jerald	****			
PMP - Domain Controller	vel	****			
PMP - Domain Controller	saxp1	****			
PMP - Domain Controller	sapmpuser4	****			

Case 4: Retrieving passwords upon providing a valid ticket ID. If your organization routes all your privileged operations such as system password resets, remote technical assistance, and troubleshooting through a ticketing system, your administrator could have enabled this setup within Password Manager Pro. This will require you to provide a valid ticket ID or corresponding ticket details every time you require access to the privileged credentials stored in Password Manager Pro.



Reason for retrievel

Ticket ID

Reason for retrieval

Resource Name	User Account	Password	Account Actions	Open Connection	Key Actions
GoDaddy	test1	Request			
GoDaddy	test2	Request			
MSSQL	jerald1	****			
PMP - Domain Controller	sapmpadmin3	****			
PMP - Domain Controller	_jerald	****			
PMP - Domain Controller	sapmpuser3	****			
PMP - Domain Controller	administrator	****			
PMP - Domain Controller	sujeethaa	****			
PMP - Domain Controller	sapmpadmin1	****			
PMP - Domain Controller	jerald	****			
PMP - Domain Controller	vel	****			
PMP - Domain Controller	saxp1	****			
PMP - Domain Controller	sapmpuser4	****			

Copying passwords

You can directly copy the passwords by clicking on the *Copy* icon beside the asterisks to avoid exposing the credentials in plaintext. The copied passwords will be saved in the clipboard for 30 seconds by default, but will differ depending on the time stamp your administrator has configured. You can also manually clear your clipboard by clicking the *My Profile* icon in the top right corner and choosing *Clear Clipboard* from the drop-down menu.

Exporting passwords for secure offline access

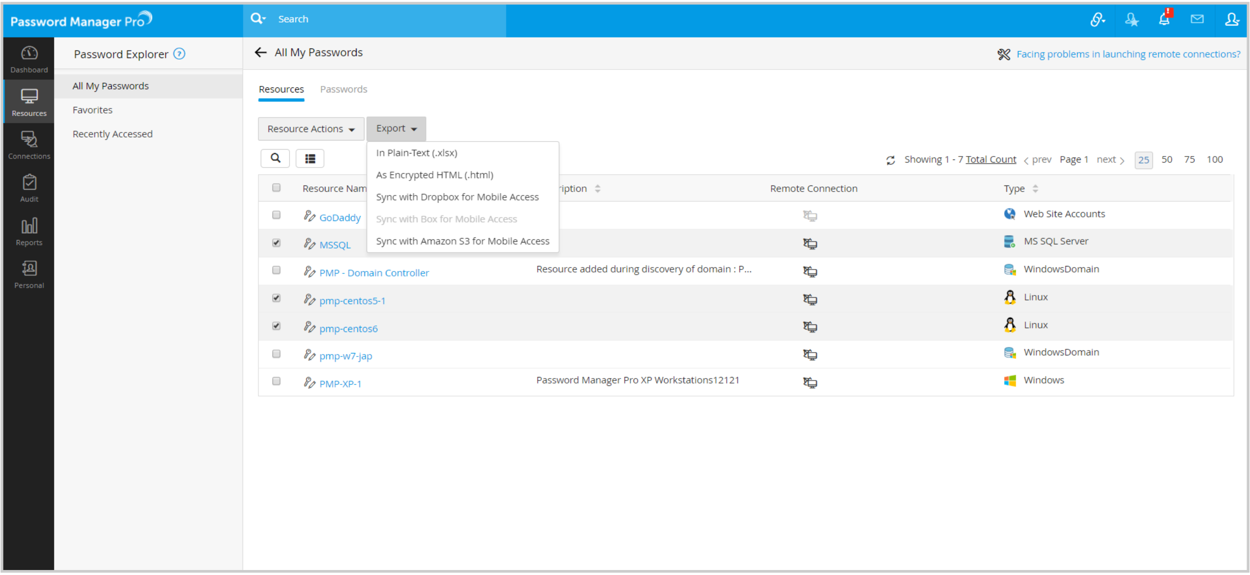
Password Manager Pro lets you export information such as resource names, account names, and passwords through multiple options for quick and secure offline access:

1. In plaintext (XLSX): This option will allow you to export resource details in plaintext to a spreadsheet. However, if your administrator has disabled the option to prevent passwords from being printed in plaintext, the passwords will be masked with asterisks in the spreadsheet.

> **Disclaimer:** *If your administrator has enabled encryption for all export operations across Password Manager Pro, the exported Excel file will be password protected. You'll have to supply the encryption passphrase every time you need access.*
> *If the administrator has enforced a global passphrase for export operations, you can retrieve the passphrase by clicking the My Profile icon on the top right corner and selecting Export Settings from the drop-down menu. There are cases when an administrator provides you with the choice to use the global passphrase or set an exclusive one for your export operations. If you prefer using your own passphrase, you can set one in the Export Settings window.*

2. As an encrypted HTML file (HTML): You can export your passwords as an HTML file for offline access. This file will be encrypted using AES-256 bit algorithm with a passphrase that you provide while exporting. You can open this file in any web browser, and access the passwords after providing the passphrase.

Password Manager Pro does not store this passphrase anywhere and we recommend you not store it anywhere either. The HTML file cannot be opened without the passphrase. In case you forget the passphrase, immediately delete the respective HTML file and then export a new file.



☐	Resource Nam	ription	Remote Connection	Type
☐	GoDaddy			Web Site Accounts
☑	MSSQL			MS SQL Server
☐	PMP - Domain Controller	Resource added during discovery of domain : P...		WindowsDomain
☑	pmp-centos5-1			Linux
☑	pmp-centos6			Linux
☐	pmp-w7-jap			WindowsDomain
☐	PMP-XP-1	Password Manager Pro XP Workstations12121		Windows

3. Sync with Dropbox for mobile access: Password Manager Pro allows you to export passwords of a resource shared with you to an encrypted file and automatically synchronize it with your Dropbox account. If enabled by your administrator, you'll find this option under the *Export* drop-down menu. Clicking on it will redirect you to the Dropbox service. Log in to your Dropbox account, authorize Password Manager Pro, and you'll be able to upload the exported password file to your Dropbox account.

4. Sync with Box for mobile access: Similar to Dropbox, you can export the required passwords to an encrypted HTML file and synchronize it with your Box account for quick offline access. Once you choose an option from the *Export* drop-down menu, you'll be prompted to log in to your Box account, and authorize Password Manager Pro to upload the exported password file to your Box account.

5. Sync with Amazon S3 for mobile access: There is also an option to export passwords to an encrypted HTML file and automatically synchronize it with your Amazon S3 account. After you select this option, Password Manager Pro will ask you to enter your access key ID, secret access key, and bucket name to sync Password
Manager Pro with your Amazon S3 account.

Search

This feature allows you to find a particular resource or account by providing the details under the respective columns.

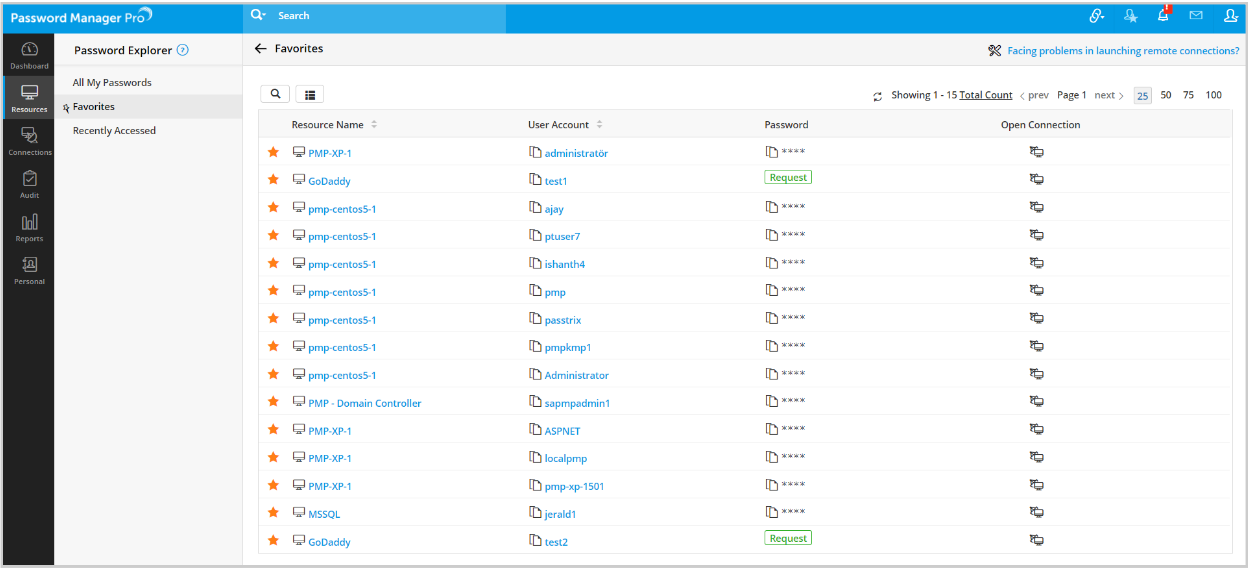
Column chooser

The *List* icon lets you define the columns you'd like to have under the *Resources* and *Passwords* sections.

B. Favorites

This option provides quick access to the list of all the passwords you've marked as favorites. Marking a password as a favorite will help you locate a particular resource and the associated password easily, so you won't have to scroll through the entire list every time. To mark a password as a favorite, simply click on the star icon to the left of the respective resource listed under *All My Passwords*.

You can also use the *Search* icon on top to find a particular password from your *Favorites* list and the *Column Chooser* icon to define the columns you'd like to have under this section.

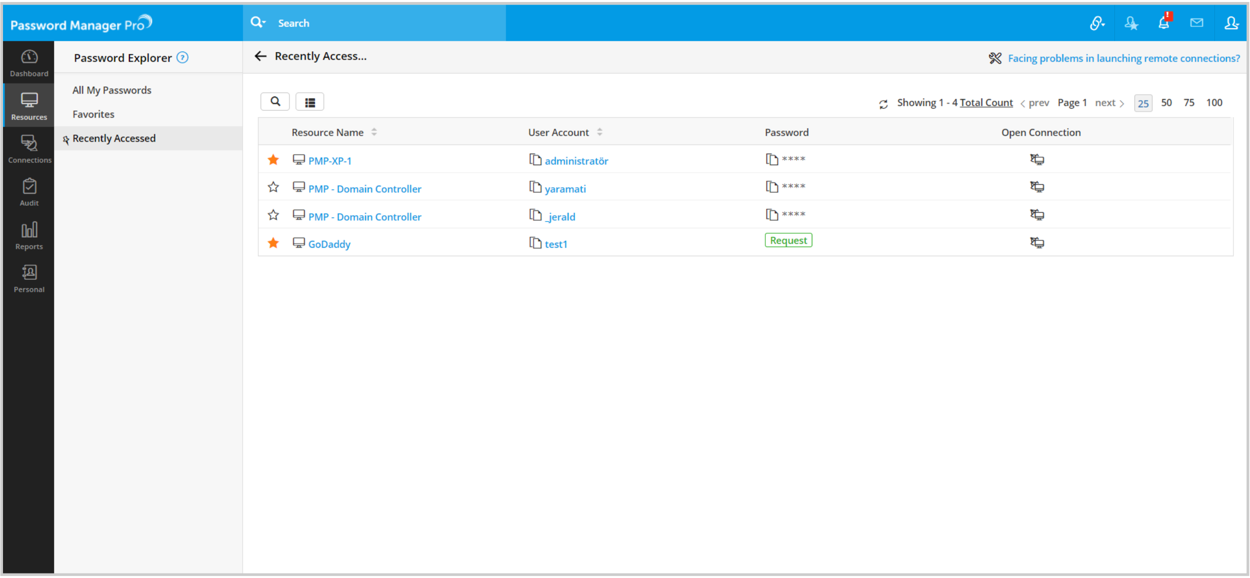


	Resource Name	User Account	Password	Open Connection
★	PMP-XP-1	administratör	****	
★	GoDaddy	test1	Request	
★	pmp-centos5-1	ajay	****	
★	pmp-centos5-1	ptuser7	****	
★	pmp-centos5-1	ishanth4	****	
★	pmp-centos5-1	pmp	****	
★	pmp-centos5-1	passtrix	****	
★	pmp-centos5-1	pmpkmp1	****	
★	pmp-centos5-1	Administrator	****	
★	PMP - Domain Controller	sapmpadmin1	****	
★	PMP-XP-1	ASPNET	****	
★	PMP-XP-1	localpmp	****	
★	PMP-XP-1	pmp-xp-1501	****	
★	MSSQL	jerald1	****	
★	GoDaddy	test2	Request	

Note: *When an administrator revokes your access to a resource that you've marked as a Favorite, the resource will automatically be removed from your 'Favorites' list.*

C. Recently Accessed

- This section helps you to view the list of recently accessed resources and their passwords.



	Resource Name	User Account	Password	Open Connection
★	PMP-XP-1	administratör	****	
☆	PMP - Domain Controller	yaramati	****	
☆	PMP - Domain Controller	_jerald	****	
★	GoDaddy	test1	Request	

- You can also use the *Search* icon on top to search for a particular resource or account from your *Recently Accessed* list. You can then define the columns you'd like to have under this section using the *Column Chooser*.

D. Password Explorer Tree

Password Manager Pro provides an option to view all the resource groups created by administrators in a hierarchical structure, i.e. tree view. Under *Password Explorer Tree*, you'll find the resource groups and subgroups that your administrator has shared with you.This tree structure depicts the resource groups of your organization for easy access, identification, and navigation. You can view the resource groups in the same structure as that of the internal grouping structure in your organization. However, you'll only be allowed to view the resources that are shared with you; resource groups that are not shared with you will be shown as empty sub-nodes (without any resources inside) in the explorer tree.

4. Connections

The *Connections* tab allows you to securely connect to remote servers and systems directly from Password Manager Pro's interface through an encrypted session gateway. Currently, you can launch RDP, VNC, SSH, and SQL sessions. Here's a quick overview of how your administrator provides you RDP capabilities for a Windows resource:

- The administrator adds a Windows resource and its respective accounts in Password Manager Pro.
- Next, they configure auto logon for the Windows resource.
- Finally, they share the resource with you.
- Now, the resource is automatically displayed in both your Resources and Connections tabs, allowing you to launch RDP connections to the resource.

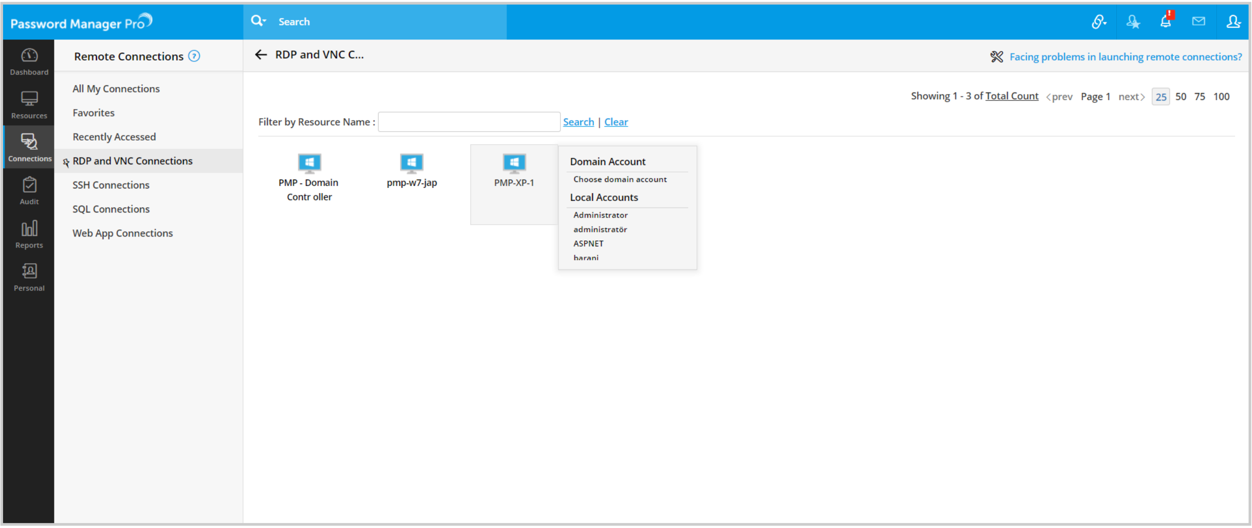
Note: *To ensure maximum security, Password Manager Pro also gives administrators the option to disable password retrieval by users for resources that support auto logon. In such cases, you will be able to directly connect to the remote resource with a single click, but you won't be able to access the account username and password of the respective resource.*

Steps to launch remote connections using Auto Logon:

1. RDP and VNC Connections

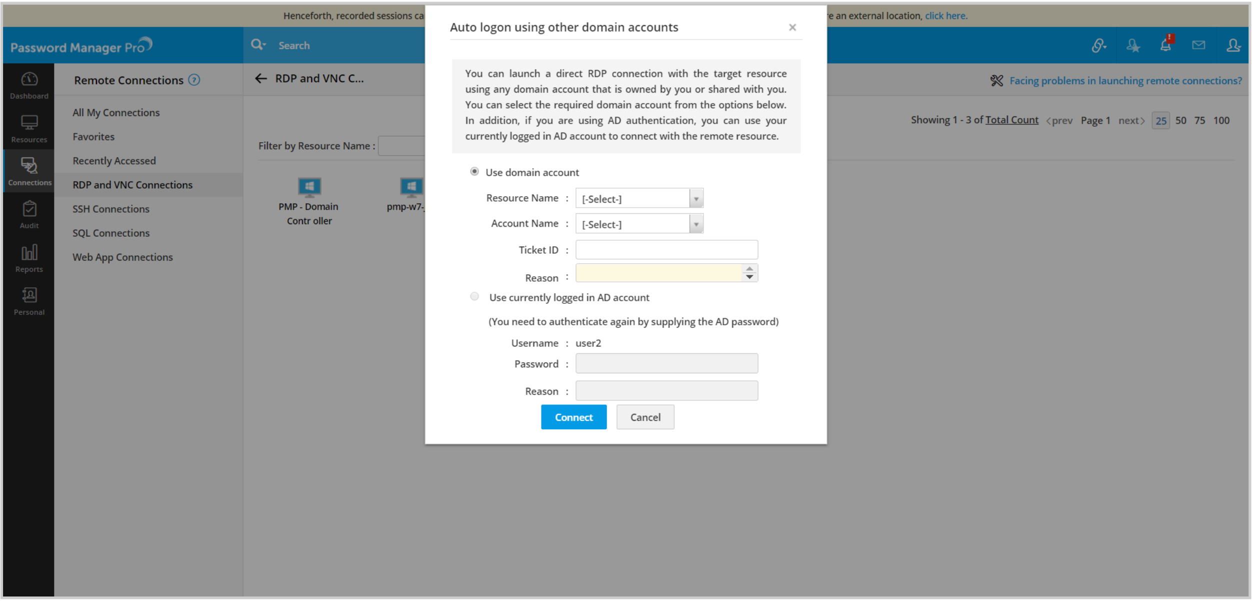
Navigate to **Connections** > **RDP and VNC Connections**, and mouse over the desired Windows resource. For an RDP connection, you typically have three options:

1. Connect using a local account: This is the default option. While delegating the respective Windows resources to you, the administrator would have shared at least one of the resource's local accounts with you. You can find the shared account under *Local Accounts* in the mouse-over menu. Clicking on the account will immediately launch the RDP connection.



2. Connect using a domain account: If your administrator has shared a domain account with you, select *Choose domain account* from the mouse-over menu. In the window that opens, select the option *Use domain account*, and then provide the domain resource name and account name. Upon adding your reason for using a domain account for the RDP connection, click *Connect*.

3. Connect using your AD account: If you've logged in to Password Manager Pro through AD/LDAP authentication, you can use those credentials to connect with a remote resource via RDP. Mouse over the resource, click on *Choose domain account*, and choose the option *Use currently logged in AD account* in the new window. Provide your AD password and the reason for launching the connection, and click *Connect*.



Auto logon using other domain accounts ×

You can launch a direct RDP connection with the target resource using any domain account that is owned by you or shared with you. You can select the required domain account from the options below. In addition, if you are using AD authentication, you can use your currently logged in AD account to connect with the remote resource.

● Use domain account

Resource Name : [-Select-]

Account Name : [-Select-]

Ticket ID :

Reason :

○ Use currently logged in AD account

(You need to authenticate again by supplying the AD password)

Username : user2

Password :

Reason :

Connect Cancel

For VNC connections, the option *Connect via VNC* will display at the top of a resource's mouse-over menu if your administrator has enabled the facility.

2. SSH Connections

This option allows you to automatically connect to any SSH-based device that is shared with you, such as a Linux server or a network device via a remote SSH session. Navigate to **Connections** > **SSH Connections** and mouse over the desired resource. For an SSH connection, you typically have three options:

1. Connect using a local account: This is the default option. While delegating the respective resources to you, the administrator would have shared at least one of the resource's local accounts with you. You can find the shared account under *Local Accounts* in the mouse-over menu. Clicking on the account will immediately launch the SSH connection.

2. Connect using a Windows domain account: Password Manager Pro allows you to launch an SSH remote terminal session using any of the Windows domain accounts stored in its database. If your administrator has shared a Windows domain account with you, select *Choose domain account* from the mouse-over menu. In the window that opens, select the domain resource name and then the account name. Upon adding your reason for using a domain account for the SSH connection, click *Connect***.**

3. Connect using your AD account: If you've logged in to Password Manager Pro through AD/LDAP authentication, you can use those credentials to connect with a remote resource via an SSH session. Mouse over the resource, click on *Choose domain account,* and choose the option *Use currently logged in AD account* in the new window. Provide your AD password, then the reason for launching the connection, and click *Connect*.

3. SQL Connections

You can automatically connect to a database instance from Password Manager Pro through a remote SQL connection. This feature is supported for MySQL, PostgreSQL, MS SQL, Sybase ASE, and Oracle DB Server databases. To launch an SQL session, click on **SQL Connections** from the *Connections* tab, mouse over the required resource, and click on the shared local account. Note that SQL connections are CLI based; they allow you to execute queries to perform operations.

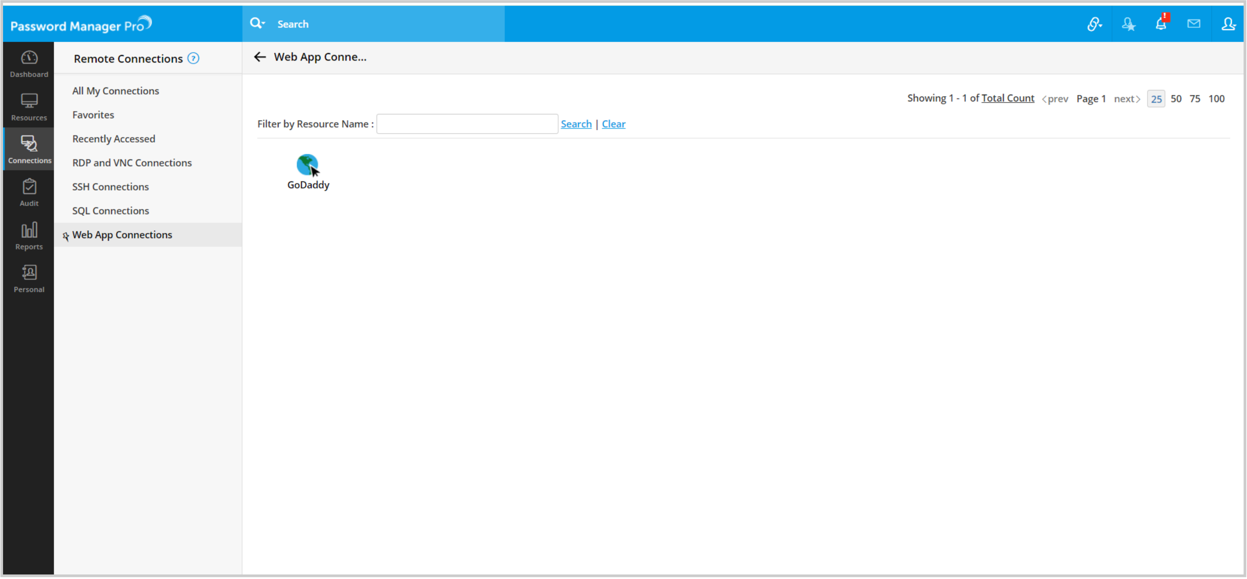
1. Connecting to database servers using your local account: To launch a remote connection to a database server, you can choose any of its local accounts that have been shared with you. You can find the shared account under *Local Accounts* in the mouse-over menu. Clicking on the account will immediately launch the SQL session.

2. Connecting to an MS SQL server using a Windows domain account: Password Manager Pro allows you to connect to MS SQL servers using any of the Windows domain accounts stored in its database. If your administrator has shared a Windows domain account with you, select *Choose domain account* from the resource's mouse-over menu. In the window that opens, select the domain resource name and then the account name under the option *Use domain account*. Upon adding your reason for using a domain account for the SQL connection, click *Connect*. Note that this feature won't be available for other database servers since they're not integrated with AD.

3. Connecting to an MS SQL server using your AD account: You can also connect to an MS SQL server using your AD/LDAP credentials, provided you've logged in to Password Manager Pro via AD/LDAP authentication. To do so, click on *Choose domain account* from the resource's mouse-over menu, and provide your AD credentials under the option *Use currently logged in AD account*. After providing a valid reason, click *Connect*. Note that this feature won't be available for other database servers since they don't support AD authentication.

4. Web App Connections

You can launch direct connections to websites or web applications (examples include GoDaddy, Slack, YellowPages, Evernote, etc.) that your administrator adds as resources and shares with you. To connect to a web-based resource directly from Password Manager Pro, navigate to **Connections** > **Web App Connections**, and click on the required web application. This will open the application in a new tab and automatically sign you into it.



Password Manager Pro

Search

Remote Connections

- All My Connections
- Favorites
- Recently Accessed
- RDP and VNC Connections
- SSH Connections
- SQL Connections
- Web App Connections

Web App Conne...

Showing 1 - 1 of Total Count ‹prev Page 1 next› 25 50 75 100

Filter by Resource Name : Search | Clear

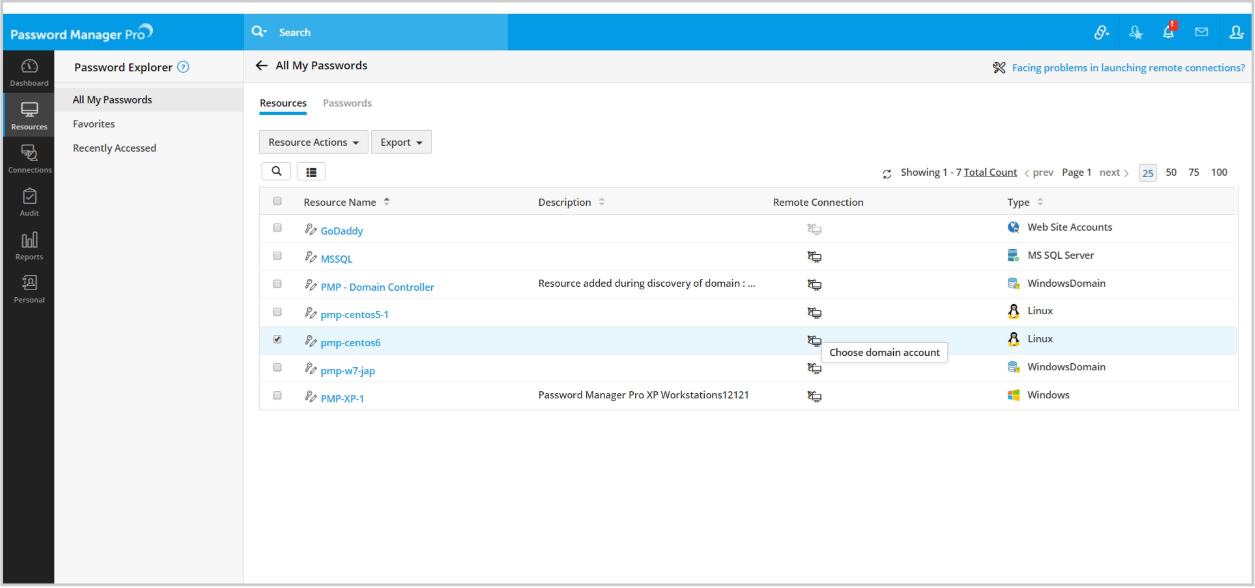
GoDaddy

Note: *This feature will work only if you've installed any of Password Manager Pro's available browser extensions as Password Manager Pro uses the browsers' auto-fill feature to automatically log you in to the respective websites and applications.*

Launching remote connections from the Resources tab

Apart from the *Connections* tab, you can also establish direct RDP, SSH, and SQL connections from the *Resources* tab.

- Navigate to the *Resources* tab, click on the *Remote Connection* icon adjacent to the desired resource, and choose the option to launch a connection using a domain account that's shared with you by your administrator.



Password Manager Pro

Search

Password Explorer

- All My Passwords
- Favorites
- Recently Accessed

All My Passwords

Facing problems in launching remote connections?

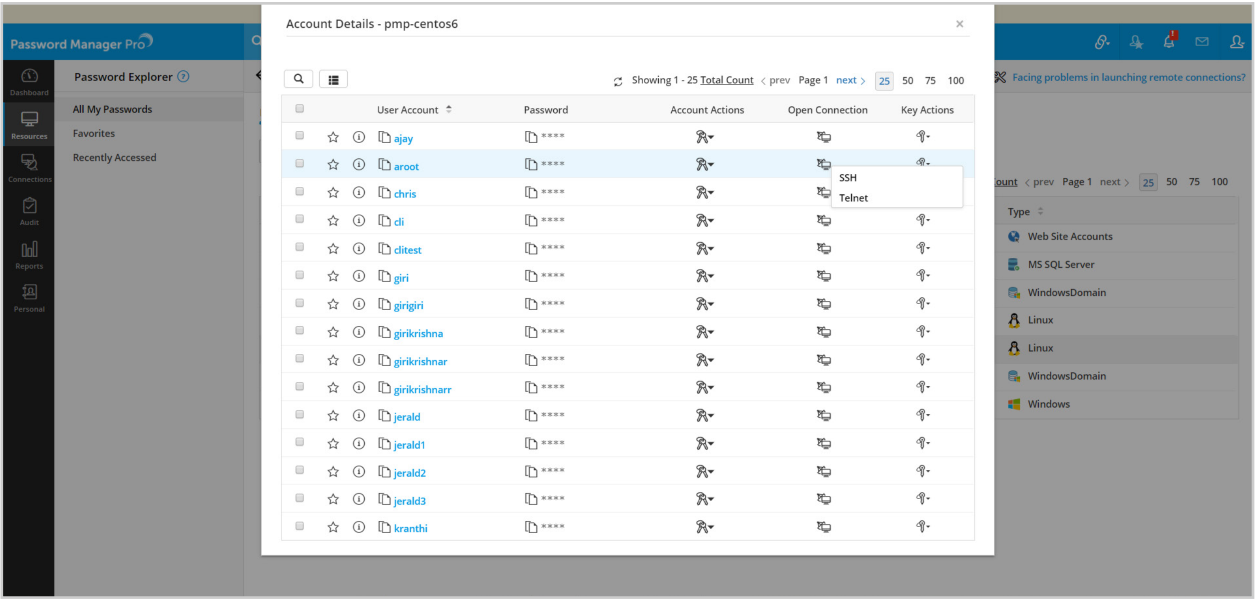
Resources Passwords

Resource Actions ▾ Export ▾

Showing 1 - 7 Total Count ‹ prev Page 1 next › 25 50 75 100

□	Resource Name	Description	Remote Connection	Type
□	GoDaddy			Web Site Accounts
□	MSSQL			MS SQL Server
□	PMP - Domain Controller	Resource added during discovery of domain : ...		WindowsDomain
□	pmp-centos5-1			Linux
☑	pmp-centos6		Choose domain account	Linux
□	pmp-w7-jap			WindowsDomain
□	PMP-XP-1	Password Manager Pro XP Workstations12121		Windows

- In the window that opens, provide the domain resource name and the account name under the option *Use domain account*, or provide your AD credentials under the option *Use currently logged in AD account* if you've logged in to Password Manager Pro via AD/LDAP authentication. Provide a valid reason for launching this connection, and click *Connect*.
- If you want to launch a connection through any of the resource's local accounts, click on the desired resource to view all the local accounts under it that are shared with you. Click on the *Open Connection* icon beside the local account you want to use and choose the desired connection mode. Next, provide a reason and/or ticket ID for launching this connection, and click *Proceed*.



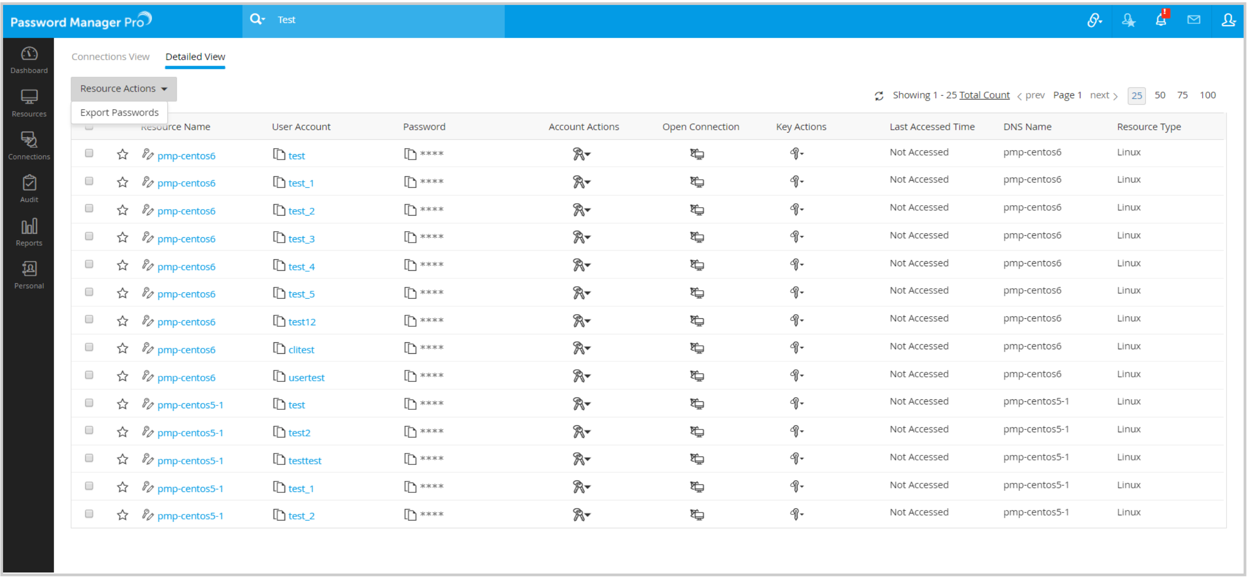
Account Details - pmp-centos6

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

User Account	Password	Account Actions	Open Connection	Key Actions
ajay	****			
aroot	****			
chris	****			
cli	****			
clitest	****			
giri	****			
girigiri	****			
girikrishna	****			
girikrishnar	****			
girikrishnarr	****			
jerald	****			
jerald1	****			
jerald2	****			
jerald3	****			
kranthi	****			

5. Global search

- The search button at the top of the screen lets you search for resources, accounts etc. across Password Manager Pro.
- Enter a valid keyword and press *Enter*, or choose the required option from the drop-down menu. Both of these options will list the resulting entries under the *Detailed View* section.
- Choose *Export Passwords* from the *Resource Actions* drop-down menu to export the data to a CSV file as per the export policies set by your administrator. Note that this option will be available only if your administrator has enabled offline access for you.
- To change a particular password from the list, click *Change Password* from the *Account Actions* drop-down menu, provide a valid reason and/or the corresponding ticket ID, and click *Save.* This menu also lists options for verifying passwords and viewing password history.

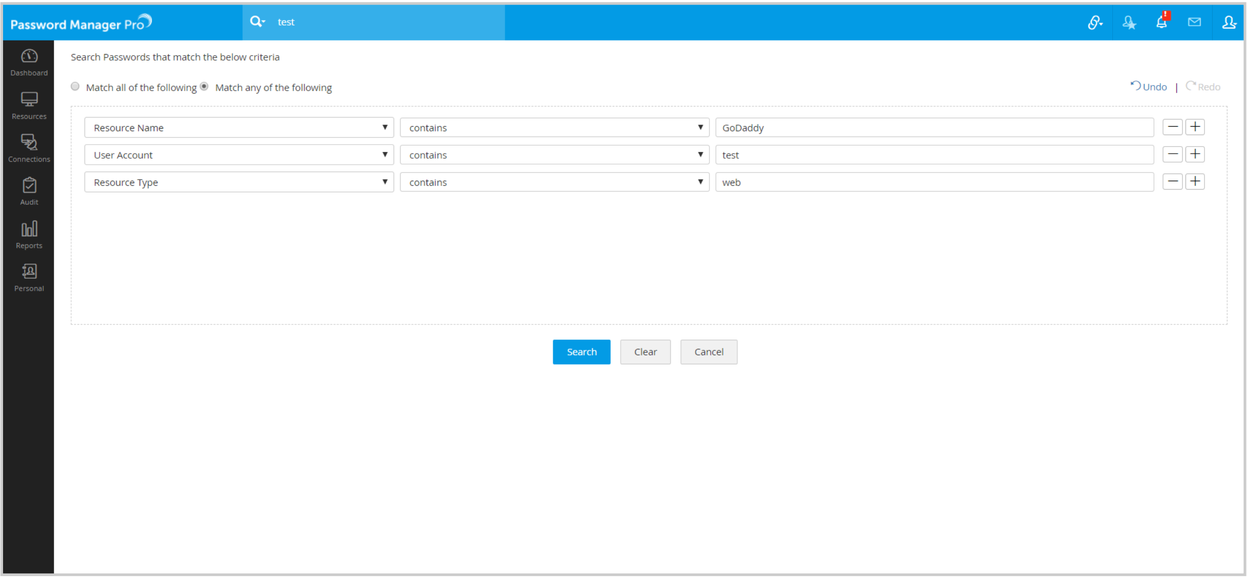


Showing 1 - 25 Total Count < prev Page 1 next > 25 50 75 100

Resource Name	User Account	Password	Account Actions	Open Connection	Key Actions	Last Accessed Time	DNS Name	Resource Type
pmp-centos6	test	****				Not Accessed	pmp-centos6	Linux
pmp-centos6	test_1	****				Not Accessed	pmp-centos6	Linux
pmp-centos6	test_2	****				Not Accessed	pmp-centos6	Linux
pmp-centos6	test_3	****				Not Accessed	pmp-centos6	Linux
pmp-centos6	test_4	****				Not Accessed	pmp-centos6	Linux
pmp-centos6	test_5	****				Not Accessed	pmp-centos6	Linux
pmp-centos6	test12	****				Not Accessed	pmp-centos6	Linux
pmp-centos6	clitest	****				Not Accessed	pmp-centos6	Linux
pmp-centos6	usertest	****				Not Accessed	pmp-centos6	Linux
pmp-centos5-1	test	****				Not Accessed	pmp-centos5-1	Linux
pmp-centos5-1	test2	****				Not Accessed	pmp-centos5-1	Linux
pmp-centos5-1	testtest	****				Not Accessed	pmp-centos5-1	Linux
pmp-centos5-1	test_1	****				Not Accessed	pmp-centos5-1	Linux
pmp-centos5-1	test_2	****				Not Accessed	pmp-centos5-1	Linux

- The *Connections View* section is similar to the *Connections* tab, except that it only displays the resources from your search results.

Advanced Search: This option under the *Search* drop-down menu lets you define your own criteria to fetch the required set of passwords matching all or any of the specified criteria.



Search Passwords that match the below criteria

○ Match all of the following ● Match any of the following

Resource Name	contains	GoDaddy
User Account	contains	test
Resource Type	contains	web

Note: *Your personal passwords will not be included in the search results.*

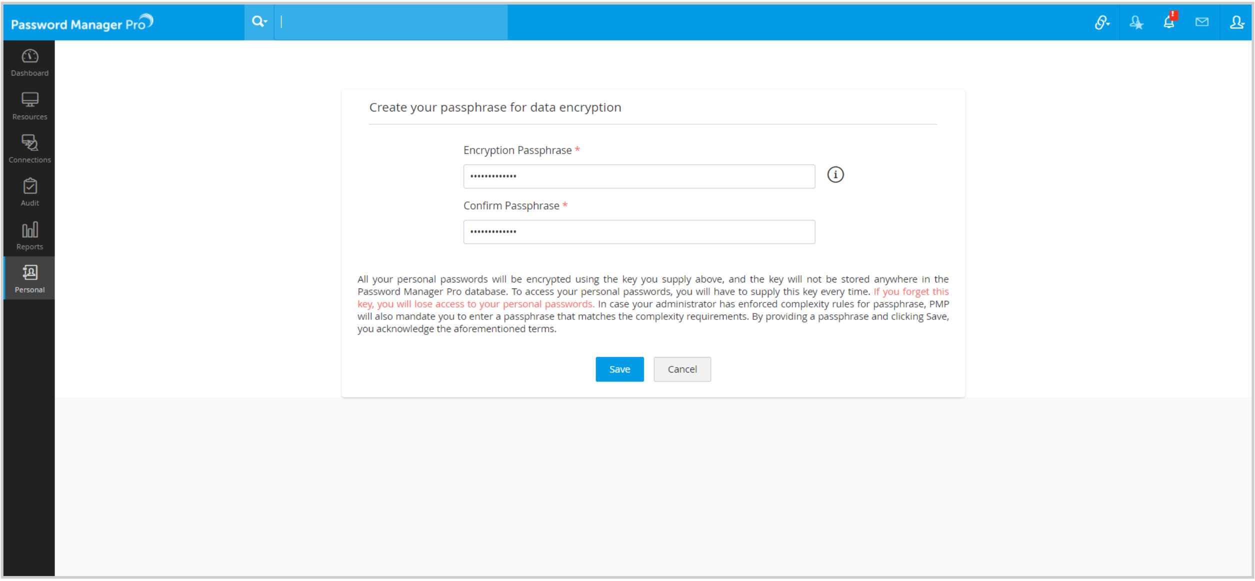
6. Personal

You'll have access to the *Persona*l tab only if your administrator has enabled the option to let you store your personal passwords in Password Manager Pro. If you have access to this tab, you can store your personal email accounts, credit card numbers, bank account information, contact addresses, phone numbers, email addresses, etc., in Password Manager Pro's web interface.

The personal information you store in Password Manager Pro will be encrypted and cannot be accessed by anyone else, ensuring complete data privacy. For enhanced security, you'll be required to create a passphrase the first time you access the Personal tab, which will be used as the encryption key for your personal passwords thereafter.

Creating a passphrase to access your personal accounts

It is strongly recommended that you create a long and easy-to-remember passphrase. You'll be prompted to enter this passphrase every time you need access to your personal passwords. Note that if you forget this passphrase, there is no way to retrieve your personal data that you've stored in Password Manager Pro.



Create your passphrase for data encryption

Encryption Passphrase * ••••••••••••••

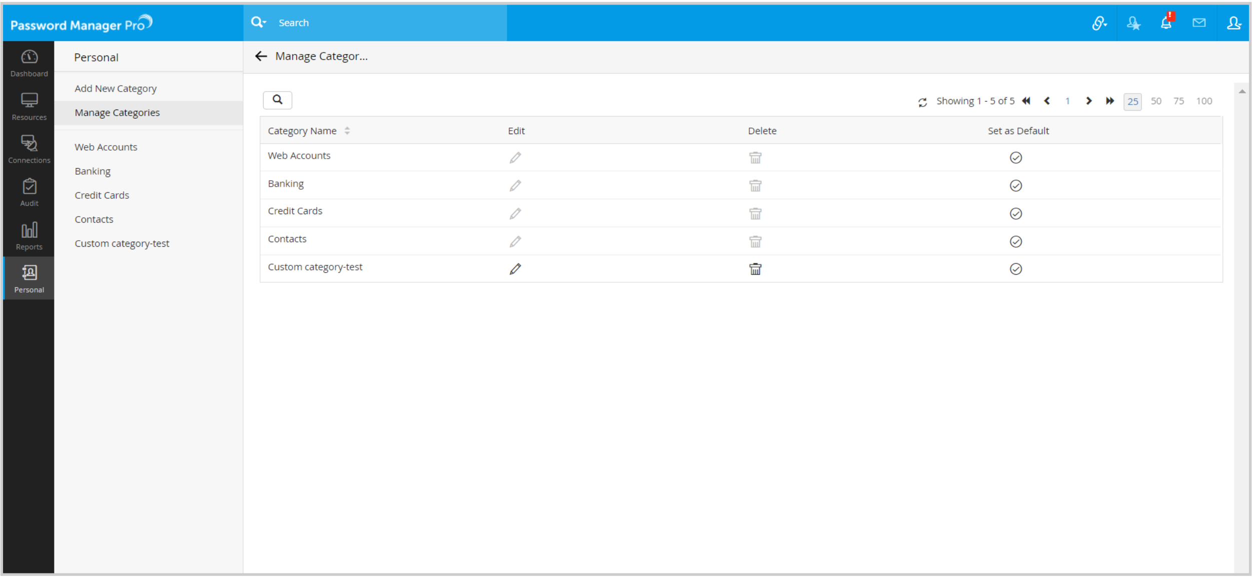
Confirm Passphrase * ••••••••••••••

All your personal passwords will be encrypted using the key you supply above, and the key will not be stored anywhere in the Password Manager Pro database. To access your personal passwords, you will have to supply this key every time. If you forget this key, you will lose access to your personal passwords. In case your administrator has enforced complexity rules for passphrase, PMP will also mandate you to enter a passphrase that matches the complexity requirements. By providing a passphrase and clicking Save, you acknowledge the aforementioned terms.

Storing Personal Accounts

Once you've set up a passphrase, you'll be able to add your personal accounts, such as web accounts, bank accounts, credit card accounts, and personal contacts lists. You can also add your own categories if the one you need isn't already available. For all these accounts, there you can add custom fields according to your requirements.

Note: *There are four default categories—Web Accounts, Banking, Credit Cards, and Contacts—that will be visible to you only if your administrator has enabled them. These categories cannot be deleted, however, you can delete the custom categories you create.*



Category Name	Edit	Delete	Set as Default
Web Accounts			✓
Banking			✓
Credit Cards			✓
Contacts			✓
Custom category-test			✓

To create personal accounts under any of the aforementioned default categories:

- Navigate to the *Personal* tab.
- Click on any of the default categories on the left.
- Click on *Add Accounts.*
- Fill in the required details, and click *Save.*
- The added accounts will be listed under the respective categories.

To delete personal accounts:

- Go to the *Personal* tab.
- Click on the required category.
- Select the accounts that need to be deleted.
- Click *Delete Accounts.*
- Confirm the action by clicking *OK.*

Note: *Discretion is advised during account deletion since the action permanently removes the selected account(s) from Password Manager Pro's database.*

Custom Fields

You can have any number of additional custom fields displayed under a particular category. To add a custom field, click on the *Customize Fields* button at the top. Your additional fields can be in any of the four formats - Character/list, Numeric, Password, Date.

You can add a maximum of nine Character/list fields, four Numeric fields, three Password fields, and four Date fields. After entering the column name, description (optional), and the default value (optional), click *Save.*

Note: *Once created, you won't be able to delete a custom field.*

Custom categories

Apart from the four default categories, you can create any number of additional categories to store other information and also add customized column names for them.

To create a custom category,

- Go to the *Personal* tab.
- Click *Add New Category.*
- Provide a name for the new category.
- Add column names containing characters, numbers, passwords, and dates.
- Save the category.

Manage categories

This option lets you edit or delete custom categories. Note that once you delete a category, you cannot restore it.

Importing passwords

Your personal account details can be imported to Password Manager Pro in bulk from a CSV/TSV file. Click on the *Import Accounts* button and submit the required details. CSV/TSV files with extensions .txt, .tsv, and .csv are supported.

Exporting passwords

Similar to the import operation, Password Manager Pro also allows you to export your personal passwords as a PDF or Excel file. To do so, click on the *Export* icon available on the top right of the screen, then choose the required option.

7. Changing your Password Manager Pro password

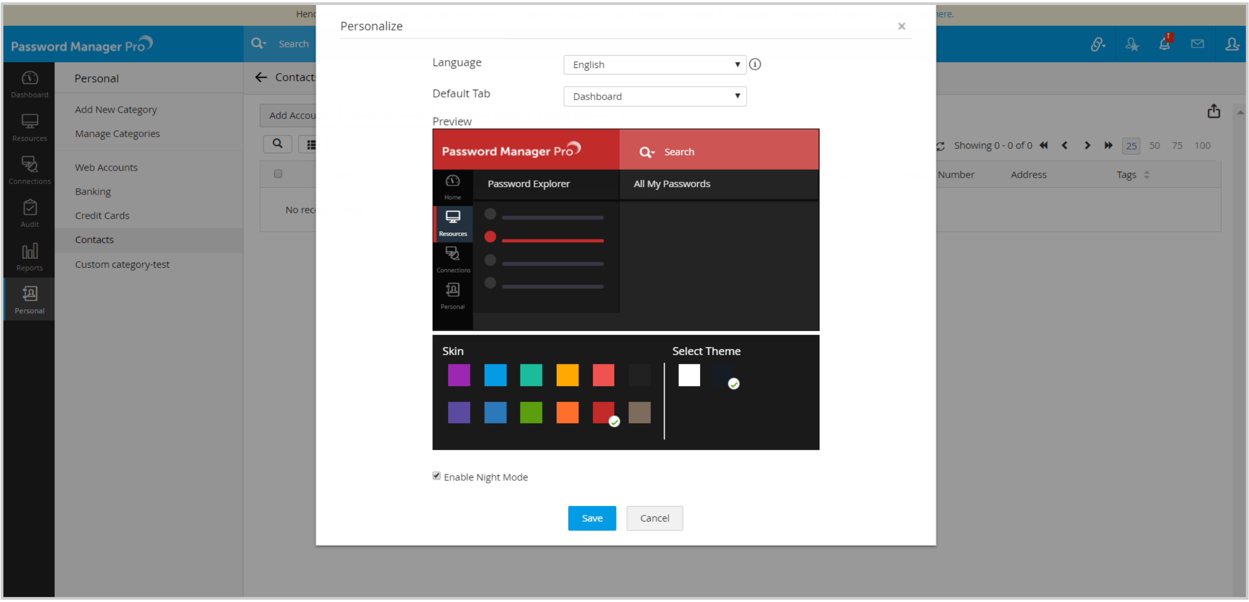
You can reset your local authentication password by clicking on *Change Password* from the drop-down list under the *My Profile* icon on the top right corner. Note that if your administrator has implemented a password policy for your organization, the new password you set here has to be in compliance with it.

The password generator can also be used to generate passwords that comply with your organization's policies. Ensure that you always remember your new password as it will not be emailed to you. If you forget your password, use the *Forgot password?* link available on the login page of Password Manager Pro to reset your password.

8. Personalized display settings

Password Manager Pro allows you to personalize the display settings for your Password Manager Pro account. To do so, click on the *My Profile* icon on the top right corner, and choose *Personalize* from the drop-down menu.

- From the *Language* drop-down menu, choose a language for the web interface. Password Manager Pro will then be available in the chosen language after you save the changes. Currently, Password Manager Pro is available in English, French, German, Japanese, Polish, Spanish, Simplified Chinese, Traditional Chinese, and Turkish.
- From the *Default Tab* drop-down menu, choose the default tab that you want displayed upon login, i.e., *Resources*, *Connections*, or *Personal* tab.
- You can also choose a background color and a theme from the available options.
- If you want to enable night mode, select the option *Enable Night Mode.*
- A quick preview of your account with all the chosen features will be shown under *Preview*.
- Click *Save* to apply the changes.


Personalize

Language: English

Default Tab: Dashboard

Preview

Skin

Select Theme

☑ Enable Night Mode

9. Browser extensions

Native browser extensions are available for Chrome, Firefox, and Internet Explorer to make your password management and auto-logon activities seamless.

Installing browser extensions

1. Chrome

- Log in to Password Manager Pro via Chrome, and choose *Browser Extensions* from the *My Profile* drop-down menu at the top right corner. This will take you to Password Manager Pro's page in Chrome's web store page. Alternatively, you can add Password Manager Pro's Chrome extension here.
- In the window that opens, click on the *Add to Chrome* button beside Password Manager Pro.
- Confirm the action by clicking on *Add* in the pop-up window.
- Once installed, the Password Manager Pro icon will be shown beside the address bar; to log in to Password Manager Pro, all you have to do is click on it.

2. Firefox

- Log in to Password Manager Pro via Firefox, and choose *Browser Extensions* from the *My Profile* drop-down menu at the top right corner. This will take you to Password Manager Pro's add-on page in Firefox. Alternatively, you can add Password Manager Pro's Firefox extension here.
- In the window that opens, click on *Add to Firefox* below ManageEngine Password Manager Pro.
- Confirm the action by clicking *Instal***l** in the pop-up window.
- The Password Manager Pro icon will be available at the end of the address bar once installed; just click on it to log in.

3. Internet Explorer

- Log in to Password Manager Pro via Internet Explorer, and choose *Browser Extensions* from the *My Profile* drop-down menu at the top right corner. This will automatically download the set up file. Alternatively, you can download the set up wizard here.
- Once done, run the Setup.exe and follow the instructions as given in the wizard.
- After installation, open an Internet Explorer browser, right-click on the *tab* bar, and click on the *Command bar* to see the Password Manager Pro add-on.
- Next, click on the *Tools* icon (Alt+X) present on top right corner, and select *Internet Options* from the drop-down menu. Navigate to **Security** > **Trusted Sites** > **Sites**, add **Password Manager Pro's URL** (https://<Password Manager Pro-Access-URL>:port), and click on *Add.*
- Now, go to the *Advanced* tab, and enable the option *Allow active content to run in files on My Computer* under the Security section. Then, click *Apply.*
- Restart the computer for the above settings to take effect.
- Once done, open the add-on and supply the credentials.

Logging in to browser extensions

In the login screen, enter the name of the host where Password Manager Pro is running and the connection port. The browser extension also supports all types of login (Local/AD/LDAP/RADIUS) and authentication mechanisms available in the web console.

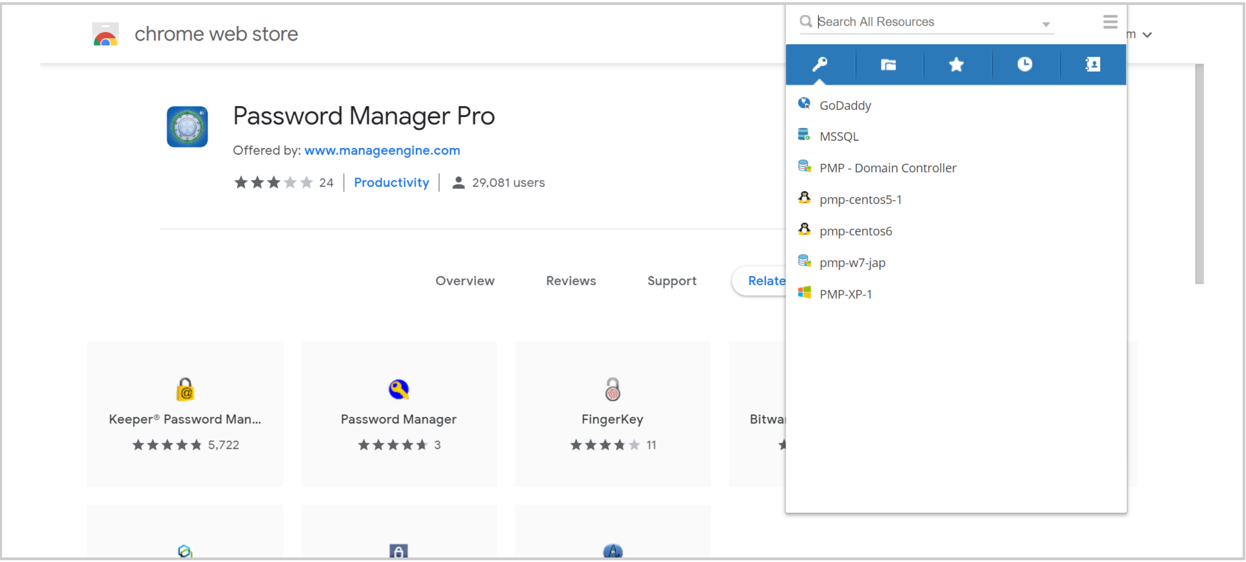
Operations you can perform using browser extensions

You can automatically log in to websites and applications from the browser itself without opening Password Manager Pro's web interface. Click on any resource shown in the *All*

Passwords tab to view the account names associated with that resource. Click on any account to view its password.

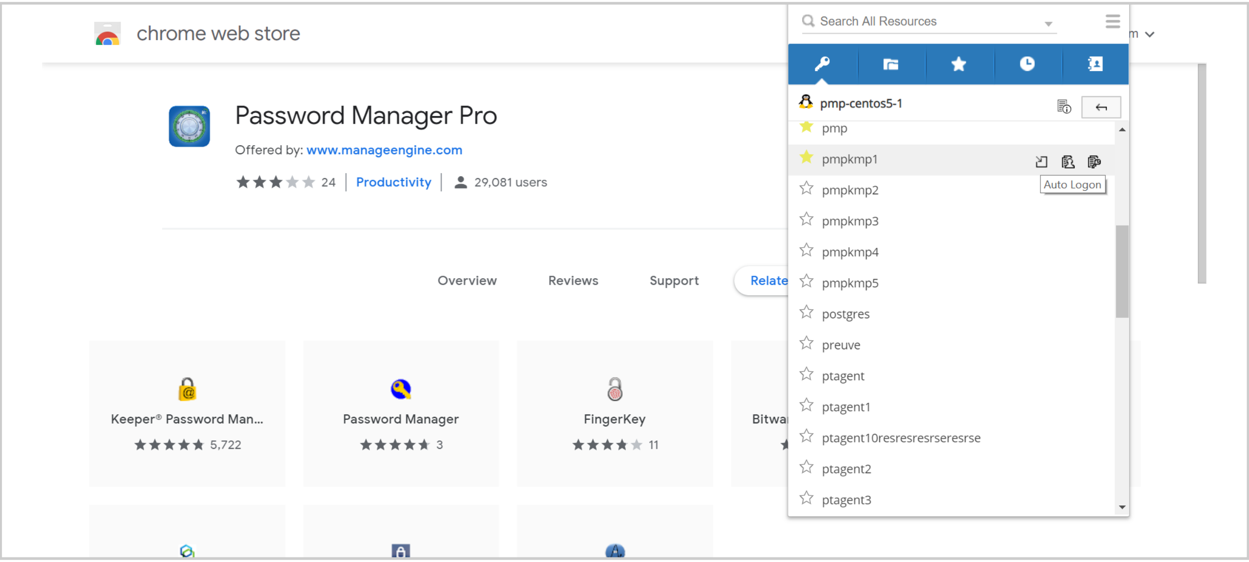
1. All Passwords

This tab in the main menu lists all the passwords available to you. Click on a particular resource to view all the accounts under it, and click on the *Resource Description* icon present beside the resource to view the resource details.



a) Automatically launch RDP or SSH sessions: This option lets you launch a direct connection to websites and Windows/Linux resources by clicking on the *Auto Logon* icon present beside an account.

b) Copy account passwords: You can also copy the username and password belonging to an account by clicking on the respective icons present beside the account.



Note: *You'll be allowed to access passwords based on the password retrieval settings configured by your administrator. Refer to the [Retrieving passwords]() section above for more details.*

2. Resource Groups

The *Resource Groups* option lets you view the passwords specific to a resource group that is shared with you by your administrator. Here, the browser extension will maintain the same tree structure of resource groups and the associated accounts as the web interface.

3. Favorite Resources

This option provides quick access to the list of all passwords that were marked as favorites by you, and helps you locate your favorite resource(s) and the associated password(s) easily. You can mark a password as a favorite by clicking on the star icon beside it.

4. Recently Used Resources

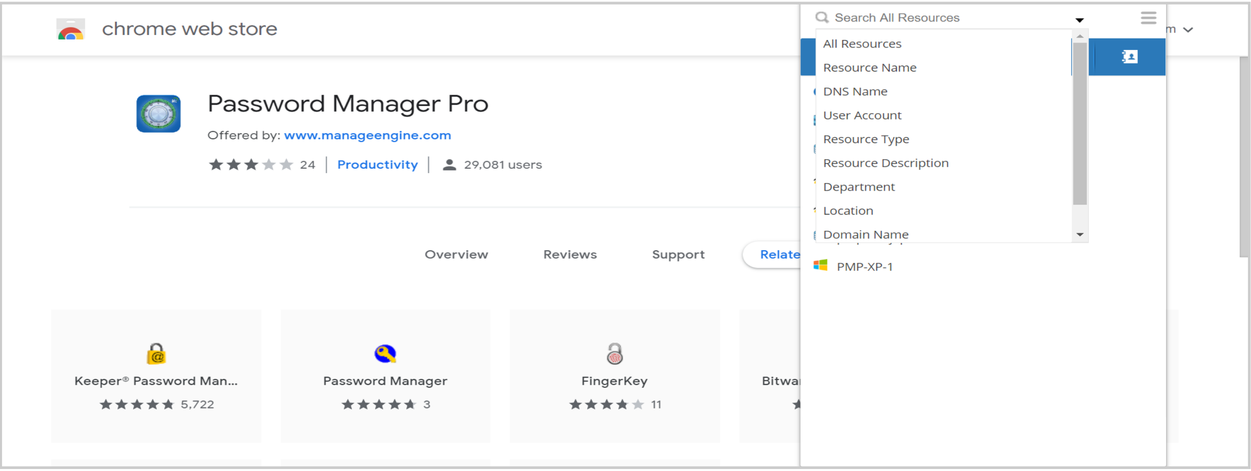
This option helps you to view the list of recently accessed resources and their passwords. You can tap on any resource from the list to view its accounts.

5. Personal Passwords

Similar to the web interface, this option lets you access all your personal passwords saved in your Password Manager Pro account.

6. Search All Resources

You can search for passwords directly from the browser extension based on several criteria including resource name, username, DNS name, user account, resource type, resource description, department, location, domain name, or additional custom fields.

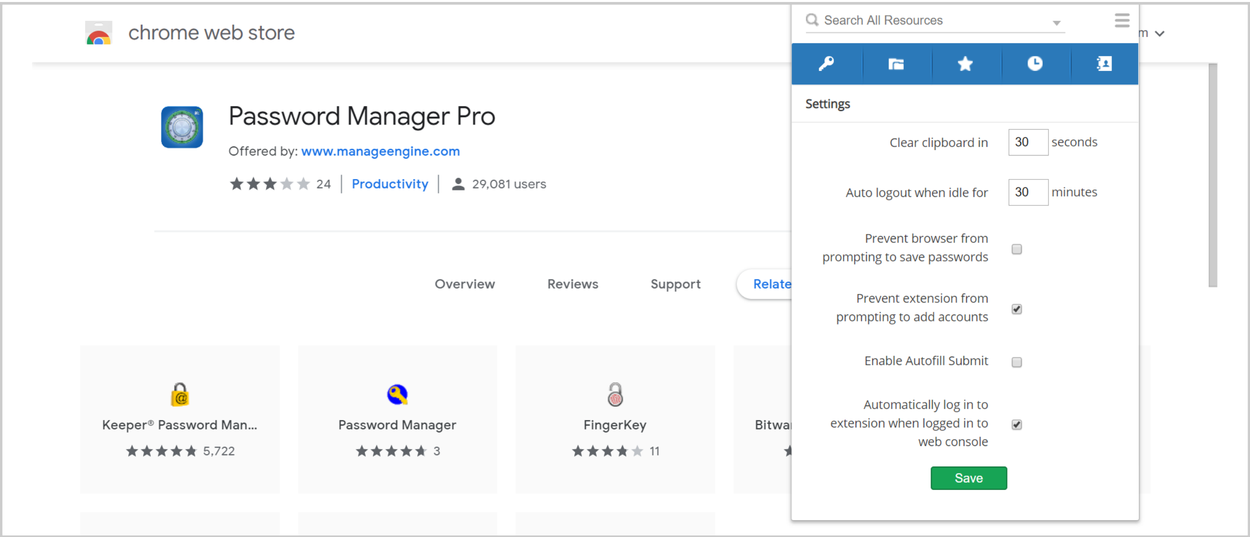


7. Settings

a) Clear clipboard in: Defines how long the copied data should remain in the clipboard after you close the app.

b) Auto logout when idle for: Shows the length of time your session will remain active once you log in. You'll be automatically logged out of a session if you remain idle for the time specified here. However, you can enter "0" here to never be logged out of a session.

c) Prevent browser from prompting to save passwords: Prevents the browser from saving your passwords for future logins.



Settings

Clear clipboard in 30 seconds

Auto logout when idle for 30 minutes

Prevent browser from prompting to save passwords ☐

Prevent extension from prompting to add accounts ☑

Enable Autofill Submit ☐

Automatically log in to extension when logged in to web console ☑

d) Prevent extension from prompting to add accounts: Lets you prevent accounts from being added to Password Manager Pro through the browser extension.

e) Enable Autofill Submit: Along with auto-filling usernames and passwords in online forms, Password Manager Pro also provides an option to auto-submit the form. You can enable this option to submit online forms in webpages automatically.

f) Automatically log in to extension when logged in to web console: Lets you automatically log in to the browser extension when you're already logged in to the Password Manager Pro web interface.

8. Automatically fill a username and password on a site/application

If you are on the login page of a website or application and if the credentials of that site or application had already been stored in Password Manager Pro, click the browser extension icon that appears on the user credentials field and select the account. The corresponding username and password will be auto-filled, and you can then manually submit them for auto logon.

10. Mobile access

Password Manager Pro provides native iOS, Android, and Windows apps to help you securely access and retrieve all the enterprise passwords that are shared with you as well as your personal passwords, **provided your administrator has allowed mobile access for you.**

- The mobile app is as secure as the desktop installation; it uses the same AES-256 encryption for storing sensitive information.
- All communication between Password Manager Pro and the mobile application is secured with the HTTPS protocol over SSL, provided you have a valid certificate issued for your server.
- The mobile app also supports two-factor authentication. If your administrator has enabled two-factor authentication, you'll be prompted to authenticate through two consecutive stages before you're given access to the mobile interface.
- After authentication, you'll be required to enter a passphrase that you'll have to provide every time you try to log in to your account. This passphrase will be used for the encryption of offline data.

Installation and getting started

Supported devices	iPhone, iPad, iPod touch	All Android devices
Compatibility	Requires iOS version 6.0 or later	Requires Android version 4.3 or later
Size	13.5MB	5.98MB
Supported languages	English, French, German, Japanese, Polish, Spanish, Simplified Chinese, Traditional Chinese, and Turkish.	English, French, German, Japanese, Polish, Spanish, Simplified Chinese, Traditional Chinese, and Turkish.

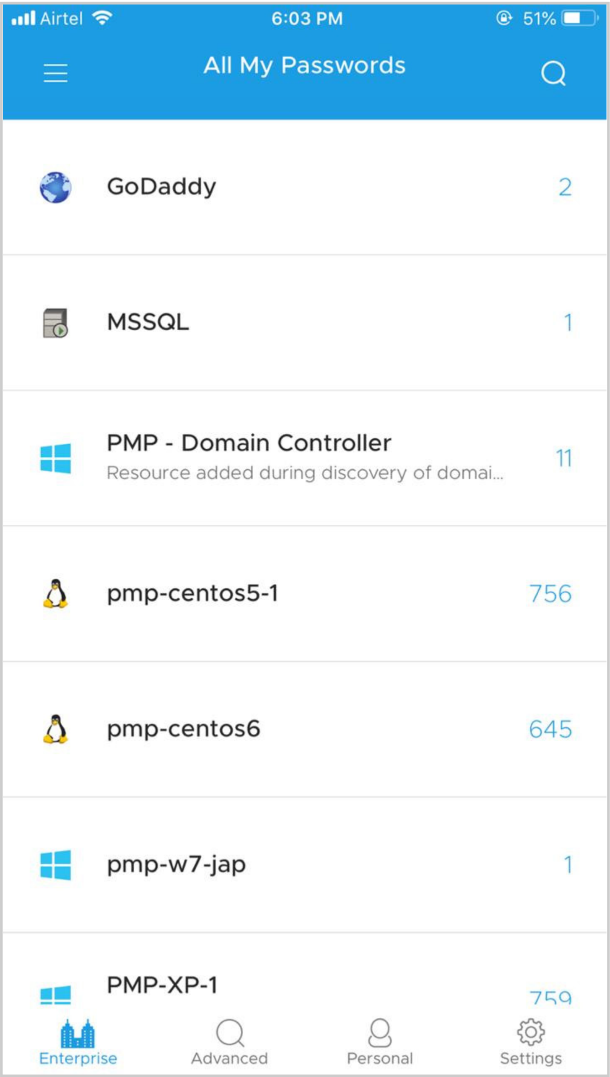
GET IT ON Google Play	Download on the App Store	Get it at BlackBerry World
Android	iOS	BlackBerry

After successfully installing the mobile application,

- Enter the server name or IP address on which Password Manager Pro is running. Ensure that the Password Manager Pro server and the mobile application are connected to the same network.
- Enter the port number.
- In case you're an MSP user, enter the name of your organization, and click Save.
- In the login screen that appears next, enter the local authentication or AD, Azure AD, LDAP, or Radius authentication credentials to log in to your Password Manager Pro account. If two-factor authentication is enabled for you, the second level of authentication will be through the two-factor authentication method configured by your administrator in the web interface.
- Set a passphrase for your account. This option will be available only if password caching for offline access has been enabled for you by your administrator. Once set, you'll have to enter this passphrase every time you need to access the app.

ManageEngine Password Manager Pro iOS

- Once you've logged in to your account, you'll find a list of all the resources shared with you in the Enterprise section.



GoDaddy	2
MSSQL	1
PMP - Domain Controller Resource added during discovery of domai...	11
pmp-centos5-1	756
pmp-centos6	645
pmp-w7-jap	1
PMP-XP-1	759

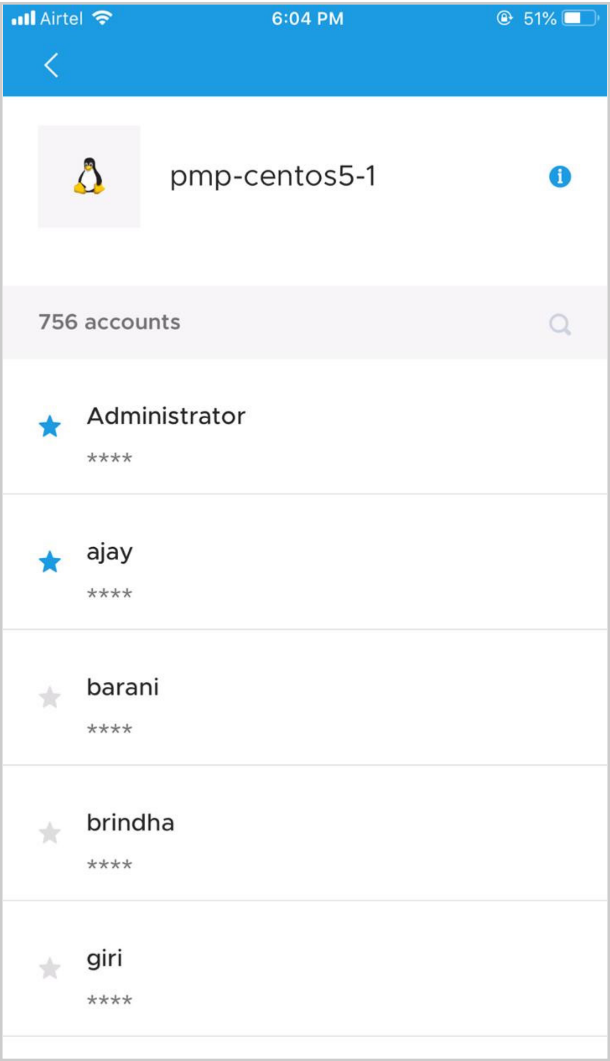
Navigation menu

You can open the navigation menu by swiping the screen from left to right or tapping the button on the top left corner of the main screen. This menu will display the following tabs:

- All My Passwords
- Favorites
- Recents
- Windows RDP Passwords
- SSH Passwords

A) All My Passwords

- Upon signing in, the app will display a list of all resources on its main screen by default. Tap on any resource to view its accounts.



Airtel 6:04 PM 51%

pmp-centos5-1

756 accounts

★ Administrator
****

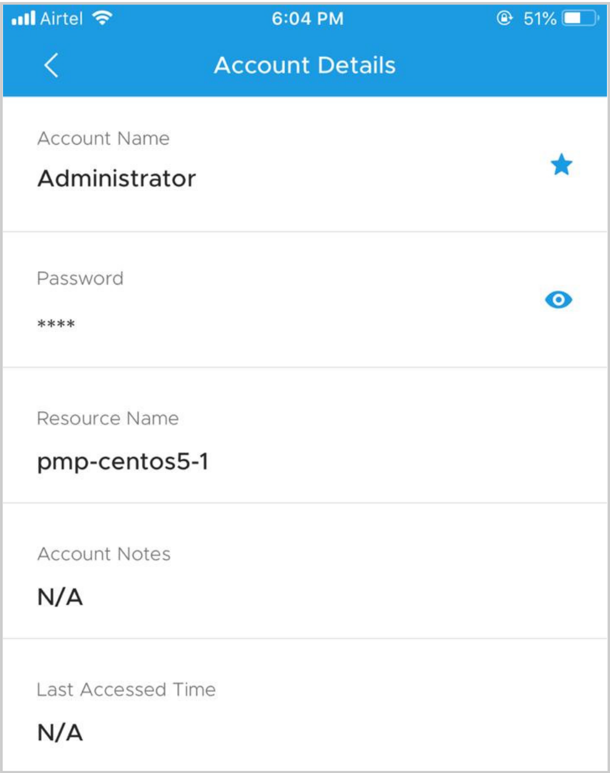
★ ajay
****

☆ barani
****

☆ brindha
****

☆ giri
****

- A single tap on any account will help you view the password (masked with asterisks), resource name, account name, and the last time it was accessed.
- Tap again on the asterisks to view the password.
- You can mark any password as a favorite by tapping the star icon. You can also remove passwords from the *Favorites* list by tapping the icon again.



Account Name
Administrator

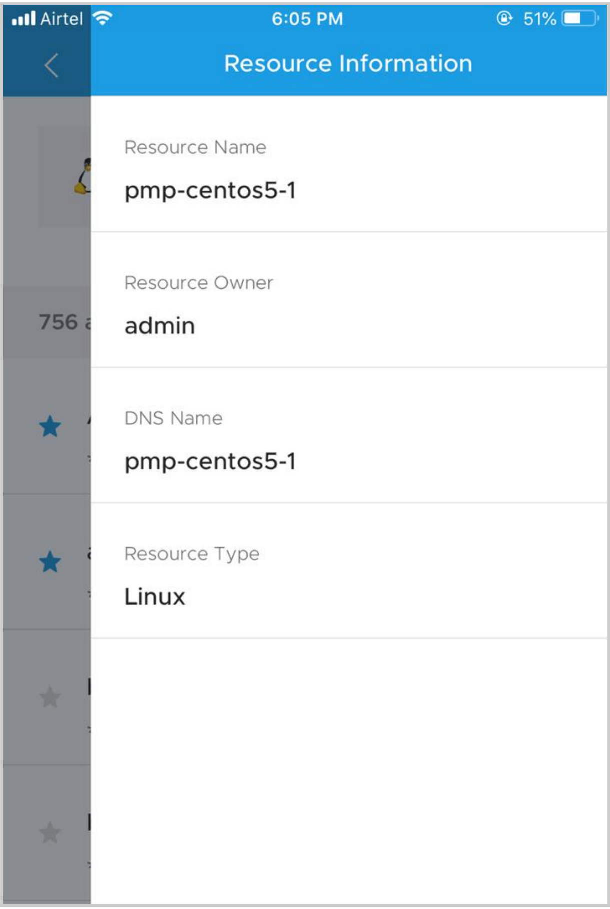
Password
****

Resource Name
pmp-centos5-1

Account Notes
N/A

Last Accessed Time
N/A

- Click on the right-most icon at the top of the screen to view the resource details including resource name, resource owner, the DNS name, etc.



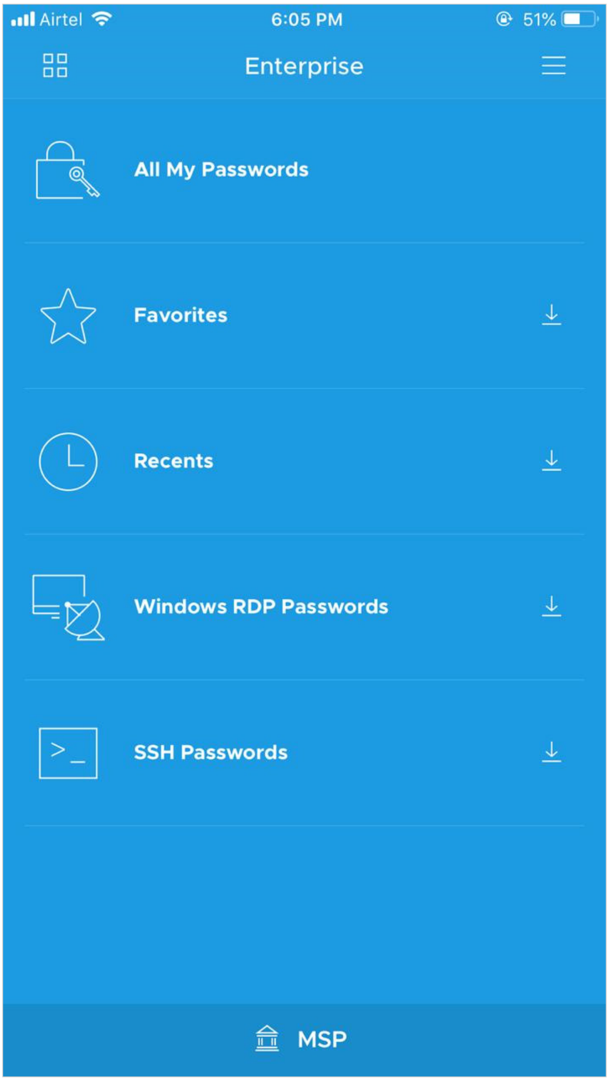
Resource Name
pmp-centos5-1

Resource Owner
admin

DNS Name
pmp-centos5-1

Resource Type
Linux

- To retrieve specific passwords like your favorites, recently accessed passwords, Windows RDP passwords, SSH passwords, etc., click on the top left button. A menu will slide in, from which you can view your desired list.



B) Favorites

This option provides quick access to the list of all the passwords that you've marked as favorites. You can mark any password as a favorite from the *All My Passwords* screen by clicking on the star icon beside the particular password.

C) Recents

This option helps you to view the list of recently accessed resources and their passwords. You can tap on any resource from the list to view its user accounts.

D) Windows RDP Passwords

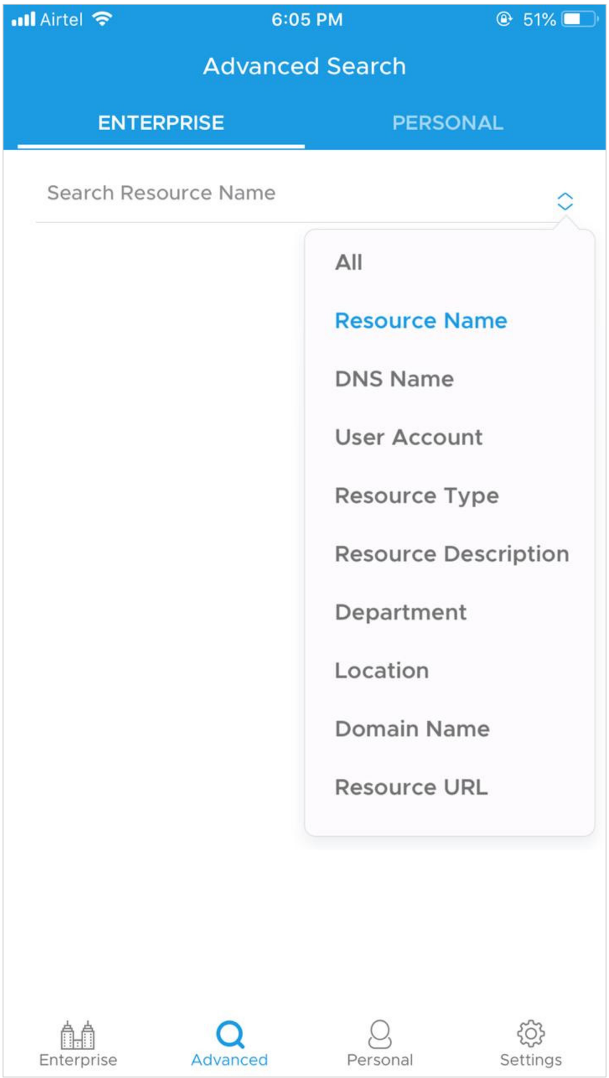
If your network has a list of heterogeneous resources, this option will help you view only the list of Windows resources. Tap on any resource from the list to view its user accounts.

E) SSH Passwords

This option helps you to view the resources that can be connected through SSH. Tap on any resource from the list to view its user accounts.

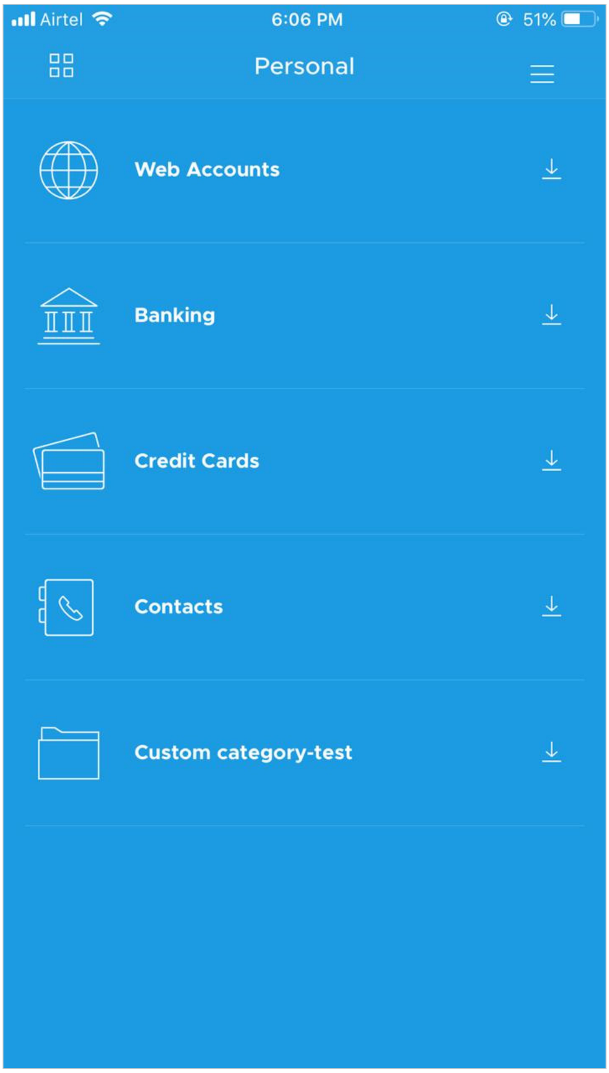
F) Advanced Search

You can search for a particular user or resource effortlessly using keywords like name, department, location, etc.



G) Personal

Apart from enterprise data, the mobile app also allows you to store and access the personal accounts that you've created via Password Manager Pro's web interface. Examples of personal data include your personal email accounts, credit card numbers, bank account information, contact details, phone numbers, and email addresses. However, you can store your personal passwords to Password Manager Pro only if your administrator has enabled the provision for you.



To learn more about how to add personal accounts via Password Manager Pro's web interface, refer to this section of our help documentation.

After adding a personal account to your Password Manager Pro account, you can access it through the mobile app by providing the passphrase you set while configuring the account.

a) Favorites: You can mark any of your personal accounts as a favorite by clicking on the star icon. However, these accounts will not be shown in the *Favorite*s list under the navigation menu.

b) Search: Find a particular account by tapping on the *Search* icon at the top of the screen and providing keywords related to the account.

H) Settings

Through the *Settings* option, you can customize various security options, view log in details, and learn about Password Manager Pro's privacy policy for its iOS app.

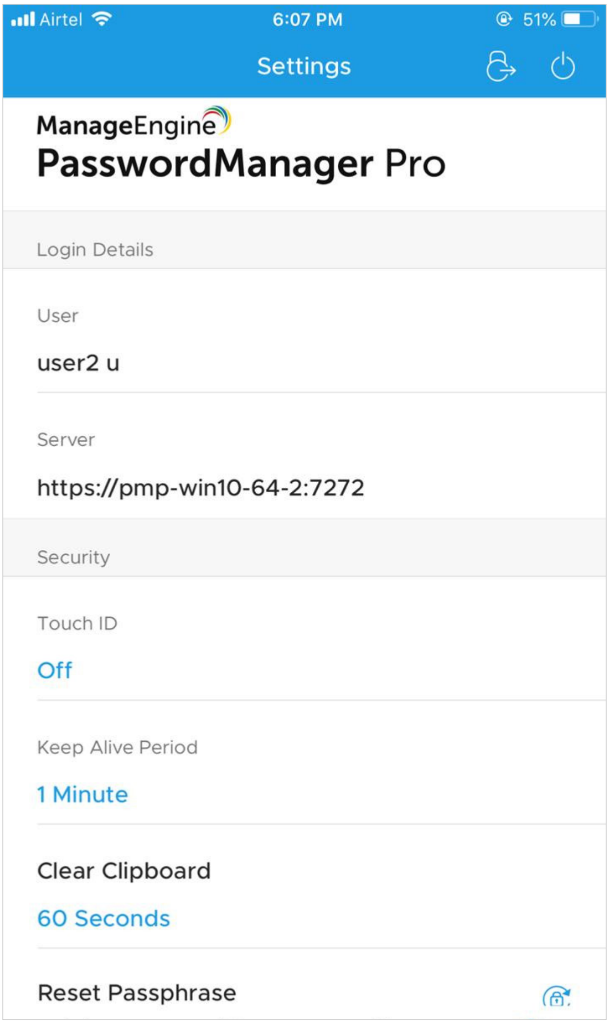
a) Login Details: Displays the username and the server address to which Password Manager Pro is currently connected. If the replication (high availability) feature is turned on, the app will also provide the secondary server details in this page. If the primary server is down, you can connect to the secondary server to maintain uninterrupted service.

b) Security: To enhance device and data security, Password Manager Pro offers several options like Touch ID, Keep Alive Period, Clear Clipboard, and Reset Passphrase.

i) Touch ID: If your device supports fingertip scanning, this setting enables you to skip entering the passphrase every time you need to access your Password Manager Pro account. You will be able to directly log in to your account by providing your touch ID.

ii) Keep Alive Period: By default, Password Manager Pro won't allow you to stay logged in to the app after you exit the app, and will force you to enter your credentials every time you need to access it. However, you can set your keep alive period as 1 minute, 2 minutes, 5 minutes, 10 minutes, or set it to be locked when you exit the app. This is helpful when you want to switch between Password Manager Pro and other apps within a certain time period. For security reasons, there is no provision to keep your app alive beyond 10 minutes, and the most secure option is to use the minimum keep alive period, i.e., 1 minute.

iii) Clear Clipboard: Define how long a copied password should remain in the clipboard—30 seconds, 60 seconds, 90 seconds, or 120 seconds. There is also an option to never clear the clipboard.



Airtel 6:07 PM 51%

Settings

ManageEngine PasswordManager Pro

Login Details

User
user2 u

Server
https://pmp-win10-64-2:7272

Security

Touch ID
Off

Keep Alive Period
1 Minute

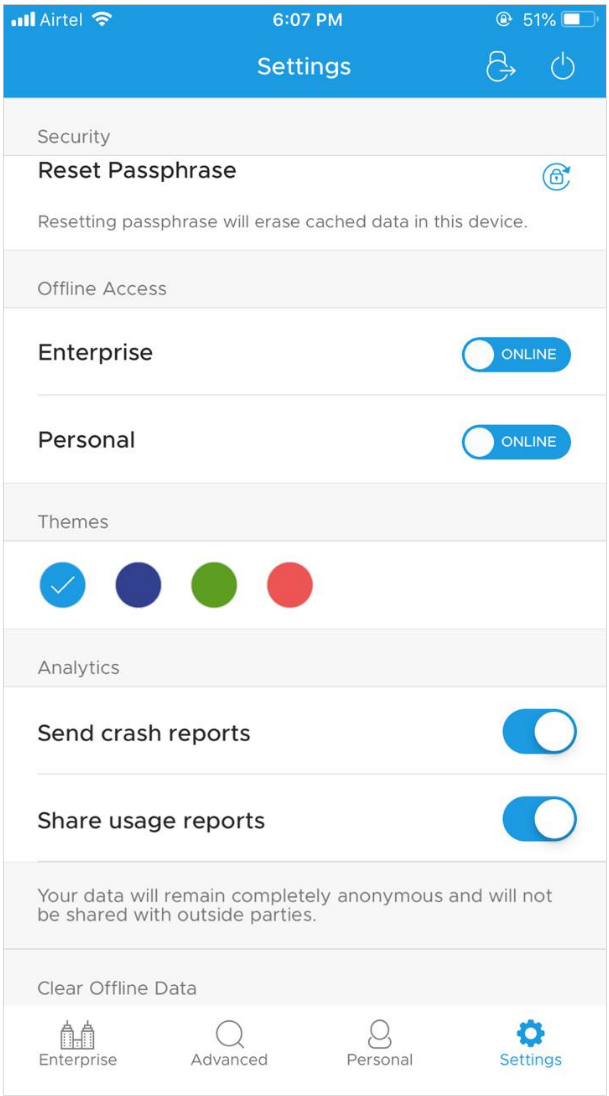
Clear Clipboard
60 Seconds

Reset Passphrase

c) Reset Passphrase: You can modify your passphrase whenever necessary, provided you're using the online mode. It's highly recommended to change the passphrase at regular intervals. Note that resetting the passphrase will erase the application's cached data from your device. This includes both enterprise and personal offline data if you've set the same passphrase for both. Otherwise, only the enterprise offline data will be erased.

d) Offline Access: Choose to use the online or offline mode for your enterprise and/ or personal accounts.

e) Themes: Choose a background color for your app from the available options.



Airtel 6:07 PM 51%

Settings

Security

Reset Passphrase

Resetting passphrase will erase cached data in this device.

Offline Access

Enterprise ONLINE

Personal ONLINE

Themes

Analytics

Send crash reports

Share usage reports

Your data will remain completely anonymous and will not be shared with outside parties.

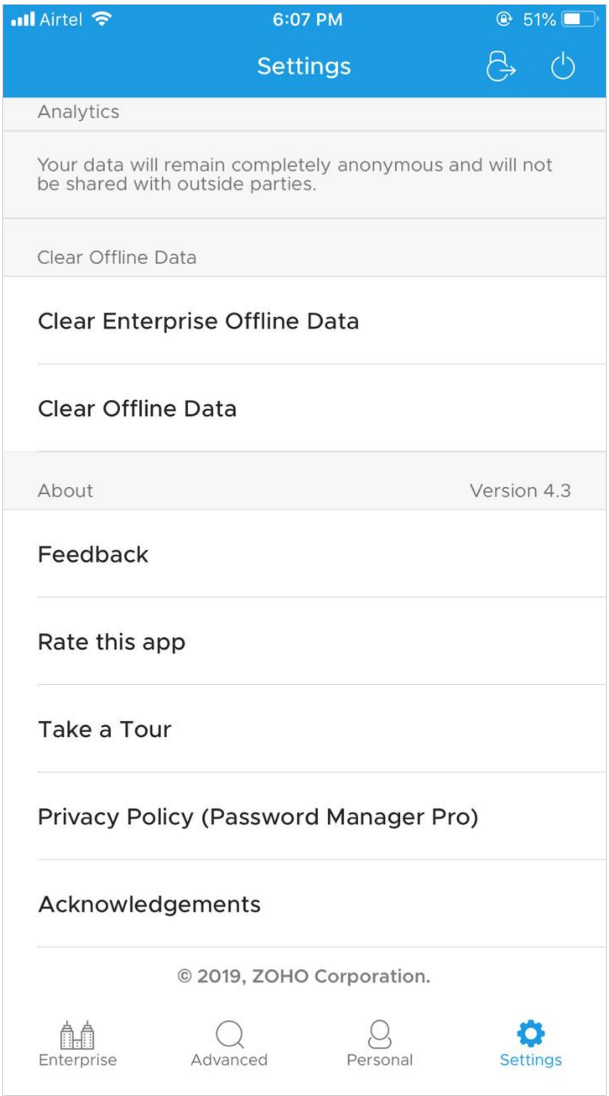
Clear Offline Data

f) Clear Offline Data: Clear your enterprise and/or personal data.

g) About: Send feedback about the product via mail, rate the product in the Play Store, learn about the product, and read the data and privacy policy.

h) Lock: You can lock the app by going to *Settings* and clicking *Lock* on the top right corner. This action will sign you out of Password Manager Pro. However, all the locally cached data will be retained. You will only have to provide the login password and passphrase to log in to your account later.

i) Logout: You can log out from the app by going to Settings and clicking the *Logout* icon on the top right corner. This action will clear all the offline data as well as the user data as per GDPR requirements.



Airtel 6:07 PM 51%

Settings

Analytics

Your data will remain completely anonymous and will not be shared with outside parties.

Clear Offline Data

Clear Enterprise Offline Data

Clear Offline Data

About Version 4.3

Feedback

Rate this app

Take a Tour

Privacy Policy (Password Manager Pro)

Acknowledgements

© 2019, ZOHO Corporation.

I) Easily copy secrets to your clipboard

To eliminate the need for manually entering the passwords, Password Manager Pro allows you to copy them to your clipboard. You can copy any password by long-pressing on it. The option to copy it will appear on the screen.

J) Provision for secure offline mode

The mobile app also facilitates secure offline mode to access passwords, when you don’t have access to the internet.

To access passwords offline, you have to download all the required passwords when you’re online before going to the offline mode. Only those passwords which are downloaded online will be available for offline access. The passwords that are viewed in online mode will also be available along with the downloaded passwords once you go offline.

Downloading every single password is practically impossible, so it is advised to download the password list you need while you're online in order to access it when in offline mode. To download a list, click on the *Download* icon that is displayed beside the particular password.

Note: *If you uninstall the application, all Password Manager Pro data will also be removed from the device.*

ManageEngine Password Manager Pro Android

The Password Manager Pro Android app supports the same features as the iOS app. Refer to this documentation for more details.

11. Role of Password Auditors in Password Manager Pro

Apart from all the above modules and features that Password Users have access to, Password Auditors additionally have access to the *Dashboard*, *Audit*, and *Reports* tabs in Password Manager Pro.

A. Dashboard

The *Dashboard* provides an overview of all password and user-related activities through various charts and tables.

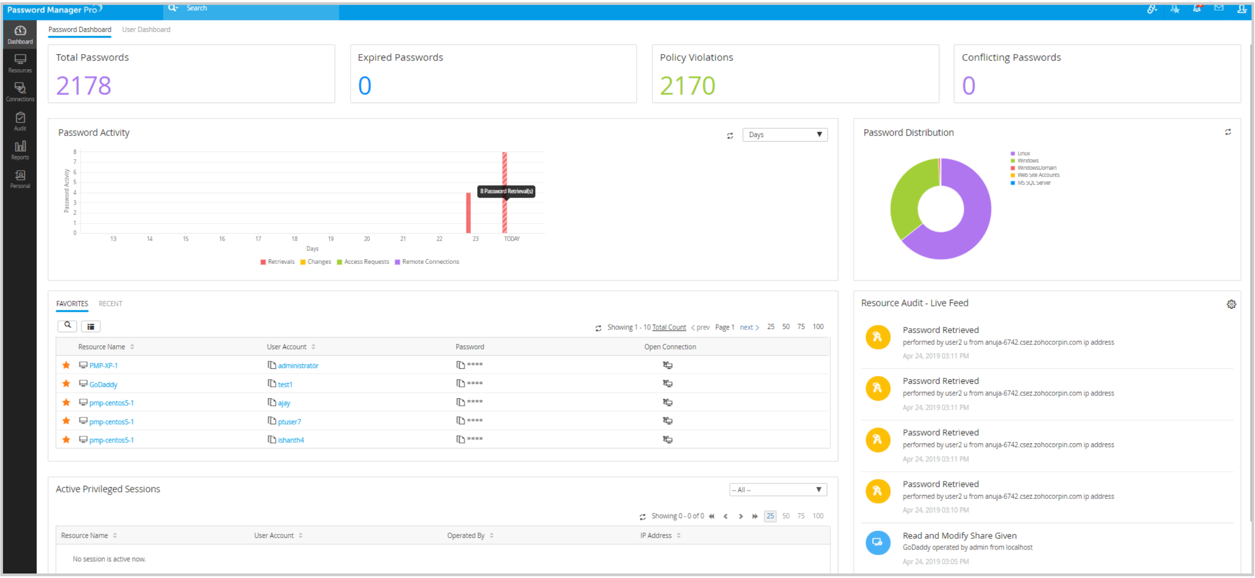
Password Dashboard

The statistical data in the *Password Dashboard* section provides the following information:

a) Expired passwords and policy violations: This provides the number of passwords that are expired and in violation of standard password policies. You can click on the numbers to view more details.

b) Password Activity: The bar chart depicts all the password-related activities like password retrievals, password changes, password access requests, and remote connections over a certain time period (last 12 minutes, hours, days, or months).

c) Password Distribution: The pie chart depicts the number of passwords distributed under each resource type (default as well as custom).



Total Passwords 2178

Expired Passwords 0

Policy Violations 2170

Conflicting Passwords 0

Showing 1 - 10 Total Count < prev Page 1 next > 25 50 75 100

	Resource Name	User Account	Password	Open Connection
★	PMP-XP-1	administratör	****	
★	GoDaddy	test1	****	
★	pmp-centos5-1	ajay	****	
★	pmp-centos5-1	ptuser7	****	
★	pmp-centos5-1	ishanth4	****	

Active Privileged Sessions

Showing 0 - 0 of 0 25 50 75 100

Resource Name	User Account	Operated By	IP Address
No session is active now.			

Resource Audit - Live Feed

Password Retrieved
performed by user2 u from anuja-6742.csez.zohocorpin.com ip address
Apr 24, 2019 03:11 PM

Password Retrieved
performed by user2 u from anuja-6742.csez.zohocorpin.com ip address
Apr 24, 2019 03:11 PM

Password Retrieved
performed by user2 u from anuja-6742.csez.zohocorpin.com ip address
Apr 24, 2019 03:11 PM

Password Retrieved
performed by user2 u from anuja-6742.csez.zohocorpin.com ip address
Apr 24, 2019 03:10 PM

Read and Modify Share Given
GoDaddy operated by admin from localhost
Apr 24, 2019 03:05 PM

d) Favorites and Recent: These lists show an overview of all the recently accessed passwords and those you've marked as favorites. You can get the resource and account details, view and/or copy the associated passwords, and open a remote connection right from the dashboard.

e) Resource Audit - Live Feed: Provides live updates on all resource, account, and password-related activities. Click on the *Settings* icon to configure the activities for which you want live updates on. You can also set the time (in minutes) for refreshing the feeds.

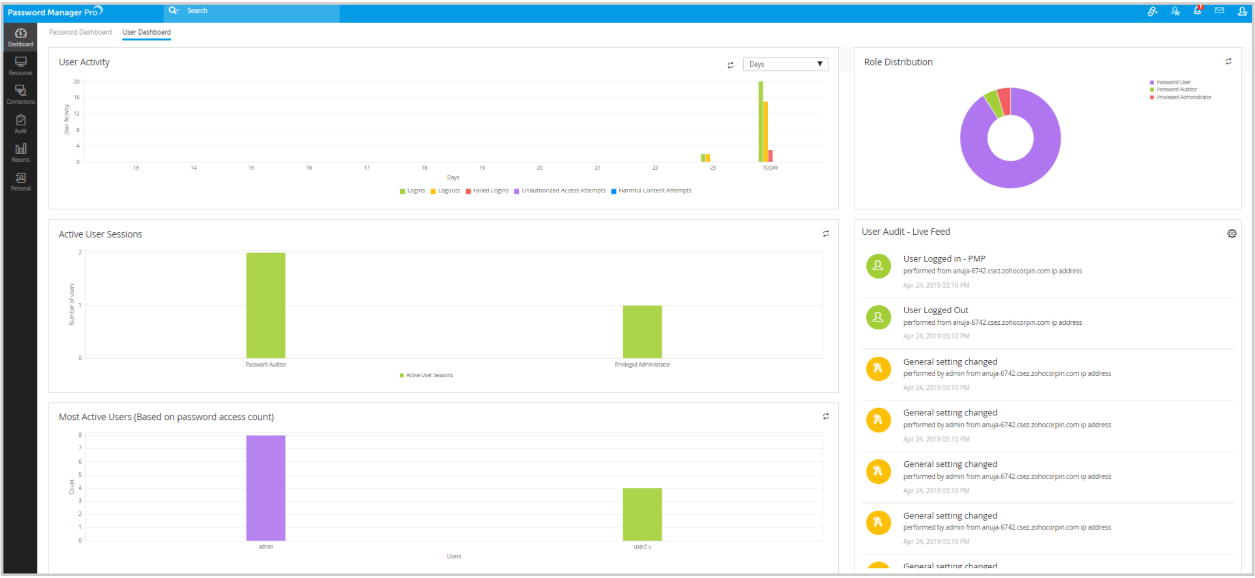
f) Active Privileged Sessions: You'll get a list of all active privileged sessions here. You can also shadow or terminate a session right from the dashboard.

User Dashboard

The *User Dashboard* section provides the following statistical data:

a) User Activity: The chart represents all user activities including successful login and logout activities, failed and unauthorized login attempts, etc., over a certain time period (last 12 minutes, hours, days, or months).

b) Role distribution: The pie chart represents the number of users under each of the default and custom roles.



User Logged in - PMP
performed from anuja-6742.csez.zohocorpin.com ip address
Apr 24, 2019 03:10 PM

User Logged Out
performed from anuja-6742.csez.zohocorpin.com ip address
Apr 24, 2019 03:10 PM

General setting changed
performed by admin from anuja-6742.csez.zohocorpin.com ip address
Apr 24, 2019 03:10 PM

General setting changed
performed by admin from anuja-6742.csez.zohocorpin.com ip address
Apr 24, 2019 03:10 PM

General setting changed
performed by admin from anuja-6742.csez.zohocorpin.com ip address
Apr 24, 2019 03:10 PM

General setting changed
performed by admin from anuja-6742.csez.zohocorpin.com ip address
Apr 24, 2019 03:10 PM

General setting changed

c) Active User Sessions: Here, you get a list of all active user sessions. You can click on the figures to get the session details.

d) User Audit - Live Feed: This provides live updates on all user activities. Click on the *Settings* icon to configure the activities for which you want live updates on. You can also set the time (in minutes) for refreshing the feeds.

e) Most Active Users: This chart represents the most active users based on the number of passwords they've accessed.

B. Audit

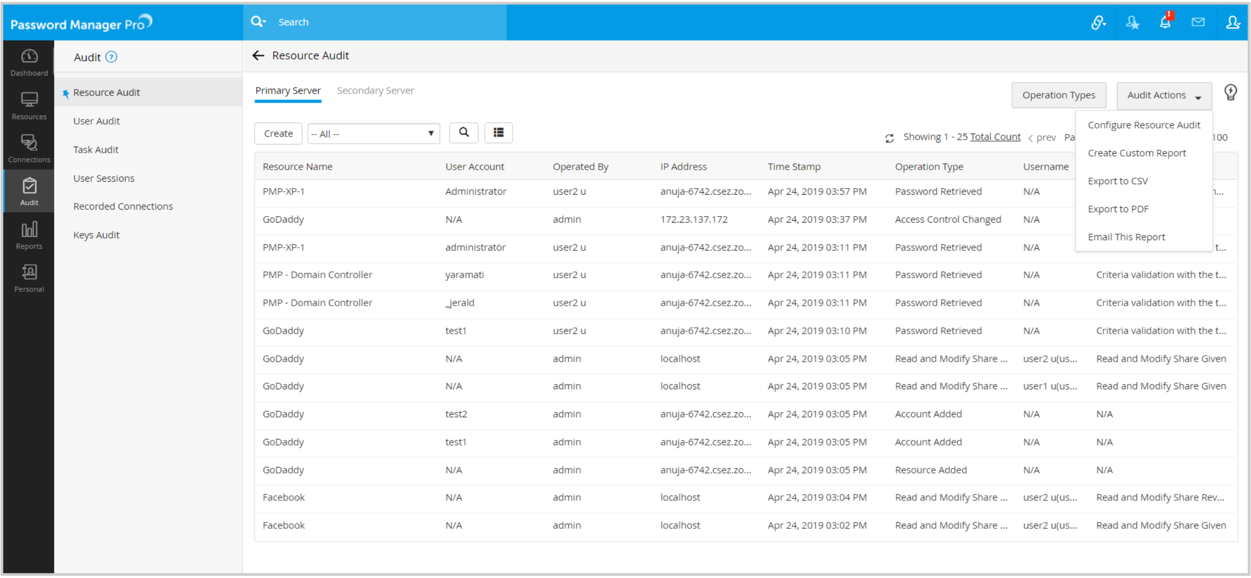
Password Manager Pro comes with an effective auditing mechanism that records trails for every single action performed by each user. You can audit all the operations performed by users on the web interface along with timestamps for each operation and the IP address from which they accessed the application.

Audit types

a) Resource audit: Capture all the operations pertaining to resources, resource groups, accounts, passwords, and policies.

b) User audit: Record all the operations performed in Password Manager Pro by any user.

c) Task audit: View the various scheduled tasks that have been created.



Resource Name	User Account	Operated By	IP Address	Time Stamp	Operation Type	Username	
PMP-XP-1	Administrator	user2 u	anuja-6742.csez.zo...	Apr 24, 2019 03:57 PM	Password Retrieved	N/A	n...
GoDaddy	N/A	admin	172.23.137.172	Apr 24, 2019 03:37 PM	Access Control Changed	N/A	
PMP-XP-1	administratör	user2 u	anuja-6742.csez.zo...	Apr 24, 2019 03:11 PM	Password Retrieved	N/A	t...
PMP - Domain Controller	yaramati	user2 u	anuja-6742.csez.zo...	Apr 24, 2019 03:11 PM	Password Retrieved	N/A	Criteria validation with the t...
PMP - Domain Controller	_jerald	user2 u	anuja-6742.csez.zo...	Apr 24, 2019 03:11 PM	Password Retrieved	N/A	Criteria validation with the t...
GoDaddy	test1	user2 u	anuja-6742.csez.zo...	Apr 24, 2019 03:10 PM	Password Retrieved	N/A	Criteria validation with the t...
GoDaddy	N/A	admin	localhost	Apr 24, 2019 03:05 PM	Read and Modify Share ...	user2 u(us...	Read and Modify Share Given
GoDaddy	N/A	admin	localhost	Apr 24, 2019 03:05 PM	Read and Modify Share ...	user1 u(us...	Read and Modify Share Given
GoDaddy	test2	admin	anuja-6742.csez.zo...	Apr 24, 2019 03:05 PM	Account Added	N/A	N/A
GoDaddy	test1	admin	anuja-6742.csez.zo...	Apr 24, 2019 03:05 PM	Account Added	N/A	N/A
GoDaddy	N/A	admin	anuja-6742.csez.zo...	Apr 24, 2019 03:05 PM	Resource Added	N/A	N/A
Facebook	N/A	admin	localhost	Apr 24, 2019 03:04 PM	Read and Modify Share ...	user2 u(us...	Read and Modify Share Rev...
Facebook	N/A	admin	localhost	Apr 24, 2019 03:02 PM	Read and Modify Share ...	user2 u(us...	Read and Modify Share Given

d) User Sessions: Count all the operations performed by a user during their active sessions.

e) Recorded Connections: Lists the recorded videos of user sessions that are launched to remote systems via Password Manager Pro. This will give you a complete picture of who did what, when, and from where.

Audit actions

Password Manager Pro audits are quite comprehensive—almost every action is audited. However, if you only want to audit specific operations, you can specify them based on the type of operation. There is also an option to send notifications to desired users whenever a specific event occurs in Password Manager Pro. Below are the operations you can perform from the *Audit* tab.

a) Configure audits

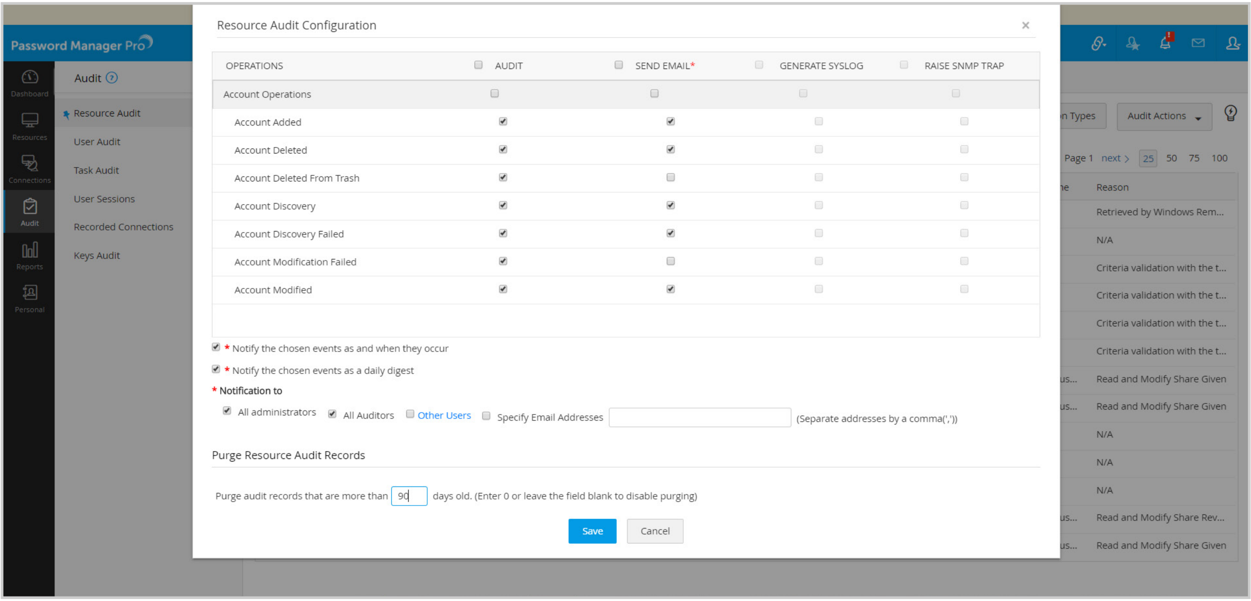
- Navigate to **Audit** > **Resource/User/Task Audit**, and click *Audit Action*s at the top right corner. From the drop-down menu, select *Configure Resource/User/Task Audit* (based on whichever audit section you're in).
- Under the *Audit* column, select the operations for which you'd like to generate audit trails; from the Send Email column, select all the operations for which you'd like to receive email notifications for.

i) Notify the chosen events as and when they occur: Enable this check box to generate instant notifications, SNMP traps, or syslog messages whenever the selected events occur inside Password Manager Pro. The SNMP traps and syslog messages can be generated only if your administrator has set up an integration with monitoring solutions.

ii) Notify the chosen events as a daily digest: Enable this option to receive a single notification every day (containing information about the selected events that occurred during the day) as a daily digest.

iii) Notification to: Select the required users, or provide details of the desired users to whom you'd like to send the notifications configured above.

iv) Purge Resource/User/Task Audit Records: To maintain disk space, you can purge older audit records by specifying the number of days they should be retained for in Password Manager Pro. For instance, if you enter 90 here, audit records that are more than 90 days old will be automatically purged by Password Manager Pro.



Resource Audit Configuration

OPERATIONS	□ AUDIT	□ SEND EMAIL*	□ GENERATE SYSLOG	□ RAISE SNMP TRAP
Account Operations	□	□	□	□
Account Added	☑	☑	□	□
Account Deleted	☑	☑	□	□
Account Deleted From Trash	☑	□	□	□
Account Discovery	☑	☑	□	□
Account Discovery Failed	☑	☑	□	□
Account Modification Failed	☑	□	□	□
Account Modified	☑	☑	□	□

☑ * Notify the chosen events as and when they occur

☑ * Notify the chosen events as a daily digest

* Notification to

☑ All administrators ☑ All Auditors □ Other Users □ Specify Email Addresses (Separate addresses by a comma(','))

Purge Resource Audit Records

Purge audit records that are more than 90 days old. (Enter 0 or leave the field blank to disable purging)

Save Cancel

b) Export to CSV / PDF

Click *Export to CSV* or *Export to PDF* from the *Audit Actions* drop-down menu to export the audit trails in the required format, and save it for future reference. Note that if your administrator has enabled encryption for all export operations across Password Manager Pro, the exported file will be password-protected and you'll have to supply theencryption passphrase to view this file. You can view or copy the passphrase by logging in to Password Manager Pro and selecting *Export*

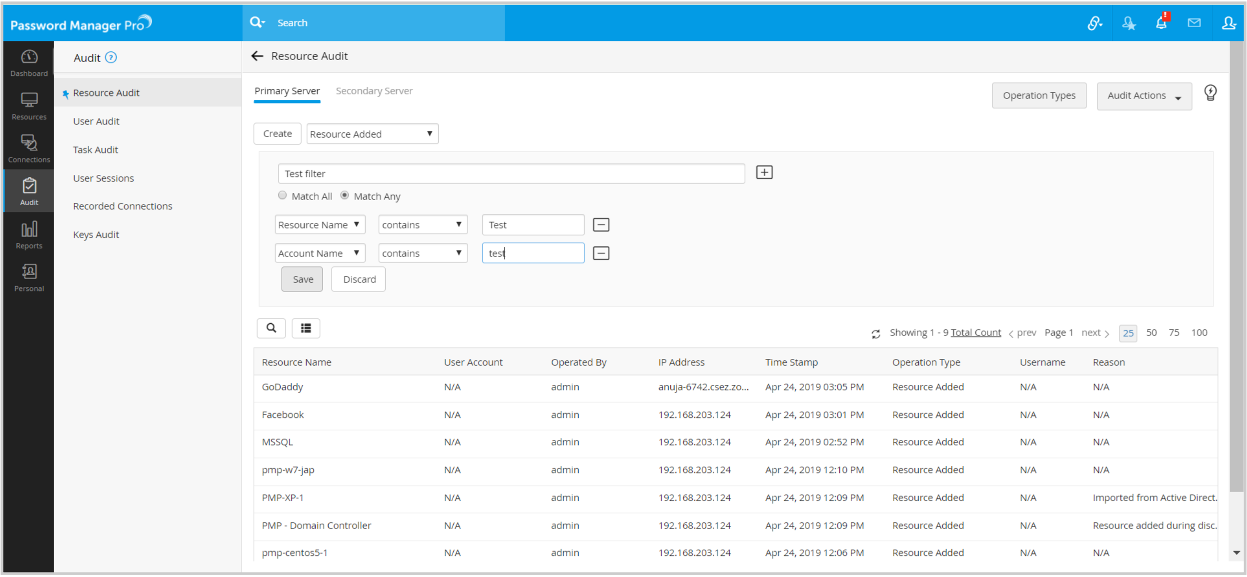
Settings from the *My Profile* drop-down menu at the top right corner. Refer to the Exporting passwords for secure offline access section above for more details.

c) Email This Report

Click on this link under *Audit Actions* to send the audit reports for a particular section to the desired users via email.

d) Creating an audit filter

- Click on the *Create* button to create customized views of audit trails by adding filters and choosing to display only those audit records that are of interest to you.
- Provide a name for your filter, enter your criteria (if you want to choose an operation type as one of the criteria, click the *Operation Types* button, and enter the preferred type). Click *Save.*



Resource Added

Test filter

○ Match All ● Match Any

Resource Name | contains | Test

Account Name | contains | test

Showing 1 - 9 Total Count ‹ prev Page 1 next › 25 50 75 100

Resource Name	User Account	Operated By	IP Address	Time Stamp	Operation Type	Username	Reason
GoDaddy	N/A	admin	anuja-6742.csez.zo...	Apr 24, 2019 03:05 PM	Resource Added	N/A	N/A
Facebook	N/A	admin	192.168.203.124	Apr 24, 2019 03:01 PM	Resource Added	N/A	N/A
MSSQL	N/A	admin	192.168.203.124	Apr 24, 2019 02:52 PM	Resource Added	N/A	N/A
pmp-w7-jap	N/A	admin	192.168.203.124	Apr 24, 2019 12:10 PM	Resource Added	N/A	N/A
PMP-XP-1	N/A	admin	192.168.203.124	Apr 24, 2019 12:09 PM	Resource Added	N/A	Imported from Active Direct.
PMP - Domain Controller	N/A	admin	192.168.203.124	Apr 24, 2019 12:09 PM	Resource Added	N/A	Resource added during disc.
pmp-centos5-1	N/A	admin	192.168.203.124	Apr 24, 2019 12:06 PM	Resource Added	N/A	N/A

e) Audit filters

Click on the drop-down menu beside *Create* to display audits belonging to a particular operation inside Password Manager Pro. The filters you create will be displayed below the title *Custom Filters* under the same drop-down menu.

f) Delete or edit a custom filter

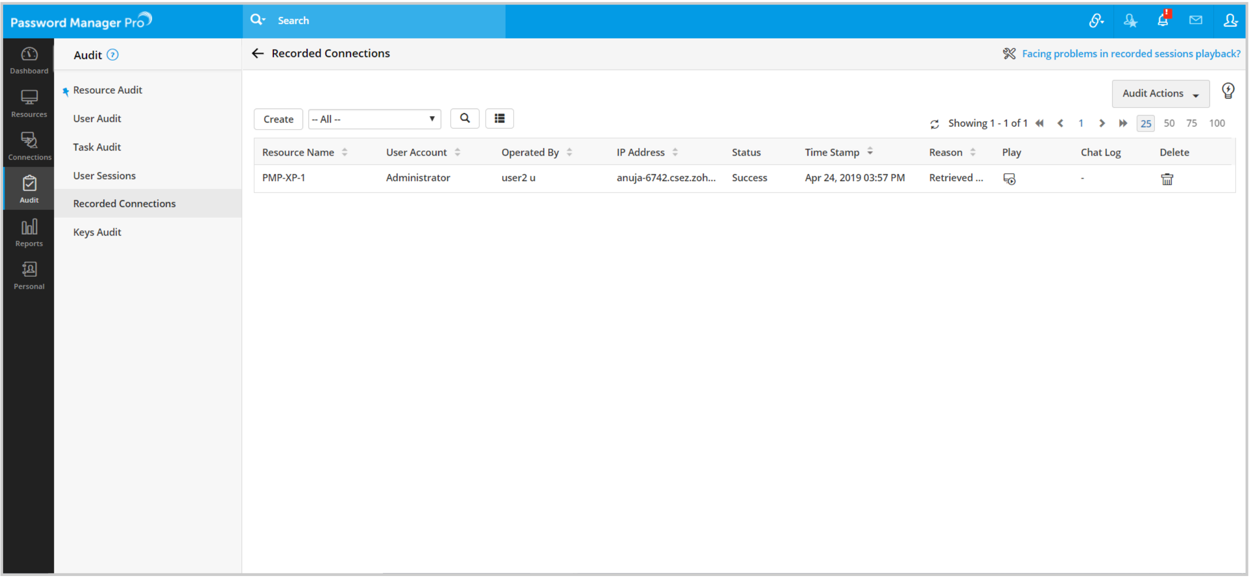
You can delete or edit a custom filter created by you by choosing it from the drop-down menu and clicking on the *Delete* or *Edit* buttons.

g) Configure Session Recording

To configure RDP, VNC, SSH, and SQL sessions, navigate to the *Recorded Connections* tab, click on *Configure Session Recording*, and choose the required options from the window that opens. From the same window, you can also specify which directory to store the recorded files to, define the backup directory, and purge recorded sessions older than a specified time.

h) View or playback the recorded sessions

- From the *Recorded Connections* tab, you can trace sessions using the name of the resource, the user who launched the session, the time at which the session was launched, etc.



Resource Name	User Account	Operated By	IP Address	Status	Time Stamp	Reason	Play	Chat Log	Delete
PMP-XP-1	Administrator	user2 u	anuja-6742.csez.zoh...	Success	Apr 24, 2019 03:57 PM	Retrieved ...		-	

- Click the *Play* icon beside each entry to view the recorded session. While viewing a recorded session, you can navigate to a specific part of the recording by clicking on the seek bar.

C. Reports

Password Manager Pro provides information on the entire privileged account management process in your enterprise in the form of comprehensive reports. You can get a wider, in-depth view of password management and privileged user activity in your organization with timed reports on password inventory snapshots, IT compliance, password sharing, user access stats, password reset history and more, helping you make well-informed decisions on password management.

Report types

Password Manager Pro provides reports under several categories and also lets you create your own reports.

a) Password Reports: Provide details about the total number of resources, passwords, and resource types in Password Manager Pro along with the ownership details, password policy compliance, password expiration, password usage, password access control workflow, unshared passwords, etc.

b) User Reports: Capture details about all users in the system with reference to password and resource access, user actions involving passwords, the resources and resource groups owned by/shared with every user, user privileges, users belonging to all user groups, password usage by all the users in the system, etc.

c) General Reports: Provide information about all password access and user activities in the system. This report is a combination of password and user reports, and it captures password statistics, password activities, password policies, password expiration, out-of-sync passwords, user statistics, user activities, etc.

d) Compliance Reports: Show your organization's level of compliance with various government and industry regulations like GDPR, PCI-DSS, ISO/IEC-27001, and NERC-CIP.

e) Custom Reports: In addition to the numerous default reports, Password Manager Pro lets you leverage the available data to meet auditing requirements, security mandates, and various compliance criteria through custom reports. For example, you can generate department-specific reports for your security audits, pull out the list of resources a former employee had access to, aggregate certain information on privileged access, and produce an integrated report to prove compliance with IT standards.

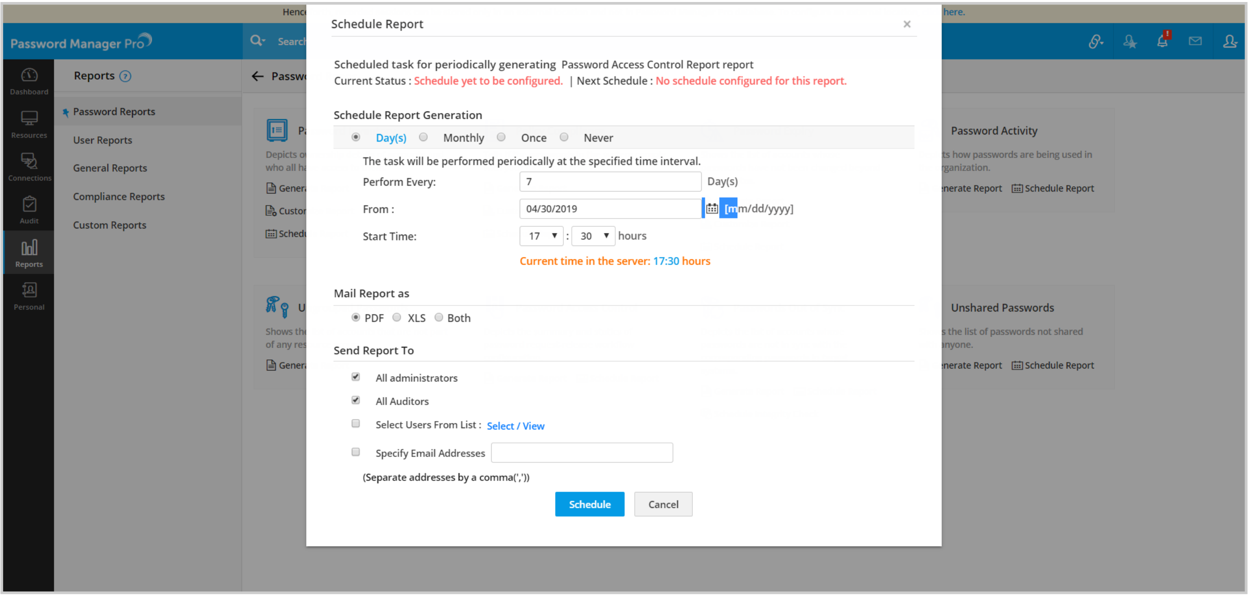
Report Actions

a) Generate Report: This helps you to instantly generate the respective report in a new window.

b) Customize Report: Found under password reports, this link allows you to customize a default report. After setting the required criteria, you can either generate a report instantly by clicking on *Generate Report*, or save the report for future use by clicking *Save*. Once saved, the report will be available under the Custom Reports section.

c) Schedule Report: Email the report in PDF and/or Excel format to the required users on a daily, monthly, or one-time basis. You can choose the recipients as a whole (all administrators/auditors), select individual users from the list, or provide the email addresses of the required users.

Note: *The schedules you create here are audited and the results will be available in the Task Audit section under the Audit tab.*



Schedule Report

Scheduled task for periodically generating Password Access Control Report report
Current Status : Schedule yet to be configured. | Next Schedule : No schedule configured for this report.

Schedule Report Generation

● Day(s) ○ Monthly ○ Once ○ Never

The task will be performed periodically at the specified time interval.

Perform Every: 7 Day(s)

From : 04/30/2019 [mm/dd/yyyy]

Start Time: 17 : 30 hours

Current time in the server: 17:30 hours

Mail Report as

● PDF ○ XLS ○ Both

Send Report To

☑ All administrators

☑ All Auditors

☐ Select Users From List : Select / View

☐ Specify Email Addresses

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

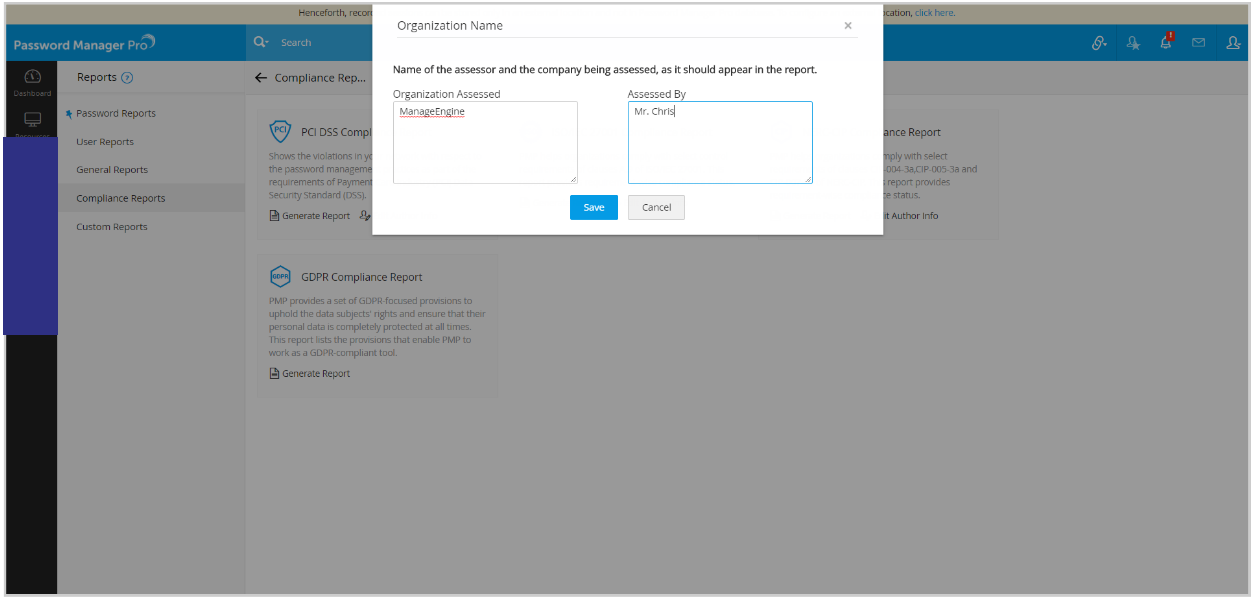
Schedule Cancel

d) Schedule Integrity Check: Available under the report category *Passwords Out of Sync*, this option helps you schedule an integrity check on a daily or monthly basis to find out which accounts have passwords stored in Password Manager Pro that are not in sync with the corresponding passwords in the target systems. To check the integrity of passwords, Password Manager Pro will try logging in to the target resources for which remote password reset has been enabled using the credentials stored in the Password Manager Pro database. If the login fails, Password Manager Pro concludes that the password is out of sync.

Note: *The schedules you create here are audited and the results will be available in the Task Audit section under the Audit tab.*

e) Find Out of Sync Passwords: This option under the report category *Passwords Out of Sync* provides an expanded list of passwords. It mentions which passwords are not in sync, who owns them, and their resource type.

f) Edit Author Info: Found under the compliance report, this option lets you provide the name of the organization being assessed and the name of the assessor as you want it to appear under *Contact Information* in the generated report.



Organization Name

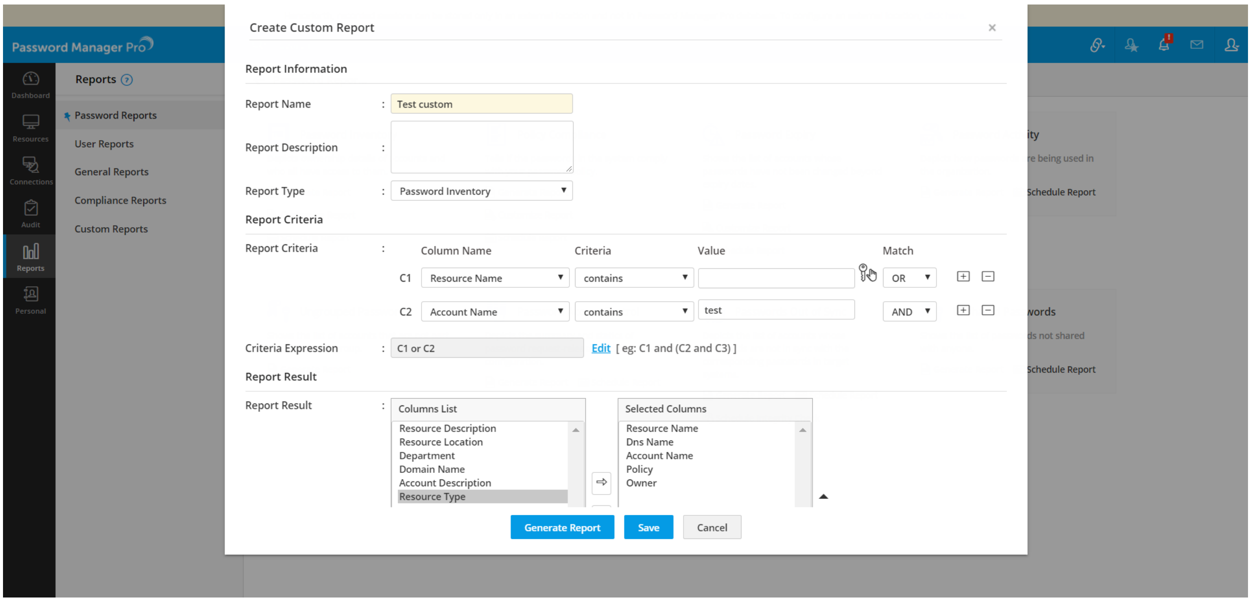
Name of the assessor and the company being assessed, as it should appear in the report.

Organization Assessed: ManageEngine

Assessed By: Mr. Chris

PMP provides a set of GDPR-focused provisions to uphold the data subjects' rights and ensure that their personal data is completely protected at all times. This report lists the provisions that enable PMP to work as a GDPR-compliant tool.

g) Create Custom Report: This button under *Custom Reports* helps you generate a custom report instantly, or save it for the future. The drop-down menu on the top right corner helps you filter out custom reports based on the report type you provided while creating the report.



Create Custom Report

Report Information

Report Name : Test custom

Report Description :

Report Type : Password Inventory

Report Criteria

Report Criteria :

	Column Name	Criteria	Value	Match
C1	Resource Name	contains		OR
C2	Account Name	contains	test	AND

Criteria Expression : C1 or C2 Edit [eg: C1 and (C2 and C3)]

Report Result

Report Result :

Columns List
Resource Description
Resource Location
Department
Domain Name
Account Description
Resource Type

Selected Columns
Resource Name
Dns Name
Account Name
Policy
Owner

Note: *The Dashboard, Reports, and Audit tabs cannot be accessed from the mobile applications.*

www.passwordmanagerpro.com

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.passwordmanagerpro.com

ManageEngine
Password Manager Pro

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