

1. Will the user who configures access control be able to bypass the Request button or do they have to follow the workflow?

Access control can be configured only by the owners of the specific resource and assign different administrators as authorized admins to approve the request. Being the owner of the Resource, access control will not be applied for the person who configures it.

2. Is there a way to share user credentials from one resource to different groups?

Yes. Sharing can be done from an individual account level, resource level, and resource group level in Password Manager Pro; the same can be done with different sets of users with different access levels.

3. When I try to manually add a new DB resource such as an SQL server, I get a message that the 'Resource already exists' if the same name is in use for an existing Windows server resource.

The SQL server should be added as a separate resource in Password Manager Pro. The resource name is unique and cannot be duplicated. So, you have to add the SQL server resource with a different resource name and provide the Windows server host name/FQDN in the DNS name field, which will be used for the communication for remote management.

4. Can you make resource fields mandatory? Like the 'Department' field?

Unfortunately, it is not possible to make any field as mandatory at this moment. We will add it to our 'to-do' list and try to implement in one of the future versions.

5. I'm confused on DB passwords. If I have a Windows or Linux server that is also an SQL or Oracle DB server, how do I add DB accounts to the server?

You have to add SQL or Oracle DB server as a separate resource in Password Manager Pro with its own local accounts. The resource name is unique and it is not possible to have multiple Resources with the same name. So add the resource with a Resource name that you can identify in the vault and provide the same DNS/Hostname for all the resources.

6. What is the difference between Windows Agent and Windows Domain Agent?

Windows agent is to manage the local account passwords on Windows endpoints/servers and Windows domain agent is for Domain Account password management.

7. Is there any way to add an approver to all resources in access control, maintaining the same configuration?

We will take this as a feature request and try to implement a bulk edit option in one of our future releases.

8. How can one add applications URL, as in web-based applications?

When you add a resource manually in Password Manager Pro, you have to specify the resource type as website accounts and the URL should be added in the Resource URL field. The same applies when you do it in bulk through a CSV file as well.

9. Should we add new approvers for each resource individually under access control configuration?

Yes. At present, new approvers should be added one by one. We will analyse the feasibility to provide a bulk option and implement in one of our upcoming releases. Thank you for the suggestion.

10. Do you plan to support Linux/UNIX discovery over SSH? Telnet is not considered secure and therefore usually not enabled on most boxes.

Yes. We understand that telnet is not secure and our development team is already looking for an alternate option for Linux resource discovery other than telnet.

11. Can you connect to multiple domains?

Yes.

12. In what version did the Access Control get released?

The access control was implemented in one of our older versions that was released in 2015.

13. Why wouldn't discovery of a particular server not capture a local admin password?

If you are discovering resources using Windows AD automatic discovery, PMP will be able to identify the local accounts. On the other hand, if it is a work group computer that has been added manually or through a CSV import into the vault, you have to select Resource actions --> Configure Remote Password Reset and select an admin account.

14. How can an administrator tell if there are passwords to which they do not have access to? So they can double check if someone else failed to share it with them.

Administrator will be able to pull Resource/Resource group, User/User group specific reports to get the complete information about the sharing.

15. Does the discovery collect the actual password to the account?

No, it doesn't. Not only PMP, no application has the ability to pull passwords from devices, servers or applications. Instead, once the accounts are discovered, PMP randomizes the passwords, assigns a new, unique password for each account, and stores them in the vault.

16. Are imported AD credentials secure in PMP?

Yes, of course. As far as AD is concerned, PMP imports service account to be managed and they are encrypted with dual layer of encryption and stored in our database. Secondly, when PMP imports the end user account to allow login to the application, it just fetches the user info like name, login name and object GUID from AD; it doesn't import the passwords. Every time a user logs in to the PMP application, it contacts AD to authenticate the users.

17. What flavors of Linux agent does it support? Is it RPM based or would you need to compile manually?

Supports all flavors of Linux and it is RPM based so it doesn't require to be compiled manually.

18. Wouldn't the preferred method be to import resources (Windows Servers) from Active Directory?

Yes. That is the preferred and the easiest way to discover all the Windows end points.

19. Are all the domain service accounts stored under the domain controller resource?

Yes. Domain service accounts get added under the domain controller resource and their resource type is tagged as Windows Domain.

20. What is the difference between privilege levels in PMP?

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

Modify Passwords: Users and User groups can both access and carry out modifications to the shared resources. However, this privilege does not allow the other users to change 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.

21. Can we manage passwords from AD service accounts?

Yes. Password Manager Pro can remotely manage the passwords of your service account, scheduled task accounts and app pool accounts.

22. How can remote login methods, such as RDP or SSH, be enabled for custom resource types?

Once you create the custom resource type in PMP, navigate to the Admin tab and select **Auto logon helper** under **Customization**. Here you should be able to edit the required method and assign the new resource type to the list and save.

23. Is it possible to give a user access to a resource, use RDP, and only see/reset their own password? We were hoping to use PMP as a jump box since it records sessions.

Yes, it is possible. Apart from the password reset of their own domain account, the users will be able to use PMP with their domain account to connect to any server. Please contact us at pmp-eval@manageengine.com for more info.

24. My database is getting full, what is the best practice to clean up the transaction logs on PMP?

Please contact us at passwordmanagerpro-support@manageengine.com and one of our support engineers will help you.

25. What is the difference between Administrator vs Super Admin vs Password Admin?

1) Administrators set up, configure, and manage the PMP application. Users with this role can manage all user, resource and password related operations, as well as access audit records and reports. However, they can view only those resources and passwords that were created by them and the ones shared with them by other users.

2) Password Administrators can perform resource and password-related operations. However, they can view only those resources and passwords that were created by them and the ones shared with them by other users.

3) Privileged Administrators have the same privileges as an administrator. In addition, they also have the privilege to configure privacy and security controls available under Privacy Settings, IP Restrictions, and Emergency Measures.

4) Super Administrator will have access to all the resources added in PMP by all administrators regardless of sharing.

26. Why do our resources show up as belonging to a user that created the resource?

Yes, the person who creates a resource becomes the owner of it in Password Manager Pro. The owner can either share the resource or transfer the ownership to a new user.

27. Can you have 2 active directory domains in your password manager pro?

Yes. You can have two AD domains in Password Manager Pro.

Please refer to the [help guide](#) for directions on how to add an Active Directory domain in Password Manager Pro; the same method can be used to add multiple AD domains as well.

28. Can you please go over when to use the Windows Agent again?

Windows agents are to be used only on Windows servers and endpoints and to be used only on DMZ servers where PMP server will not have direct connectivity using WMI/RPC ports.

29. Server is discovered successfully but no local admin account/password gets captured.

Please contact us at passwordmanagerpro-support@manageengine.com and one of our support engineers will help you.

30. What firewall ports need to be opened to use PMP from an iOS or Android device?

The web server https port should be open between the device and PMP server to access PMP from the mobile app.

31. What is the method of removing AD resources when they have been removed from domain?

1) When you delete the resource in AD, it should get synchronized with PMP and the Resource will be removed from the Resource Group synced with PMP. You can run a report for ungrouped resources via the Reports tab to identify the deleted resource and manually remove it from PMP.

Else, 2) You can disable the resource from AD before deletion and PMP will identify the resource and mark it to the disabled resources in the Resource group filter and you will be able to bulk select and delete the resources manually from PMP.