1. How can I find out what resources have been shared to which users? Is there a GUI tab, preferably controlled by a super administrator, from where this data can be taken?

You can make use of the Password Inventory in canned reports to get details on sharing and ownership of resources. We don't have a dedicated tab but next to every user and user group, we have provided the access snapshot under 'Reports' which will give you the details of sharing and permission levels.

2. Why is that when multiple users/groups are exported from AD, those users/groups are displayed multiple times in PMP?

In Password Manager Pro, a user can be part of multiple groups. Hence, if you import multiple user groups then the user will be imported once in PMP but he will also be a part of all the groups imported.

3. Our environment has different types of resources whose management will be taken care of by the respective teams separately. Our requirement is for 3 different administrators to manage resources and passwords but these three admins are not able to manage from one PMP admin console.

You can make use of the Password Administrator role in PMP where the administrator can only manage the passwords but they will not be able to do any other administrator-related operations like importing users, configuring disaster recovery, etc. So, one admin will take the responsibility of adding all the passwords and sharing it with full permission to other administrators.

4. What is the new role called 'Privileged Administrator' and how is it different from the 'Administrator' role?

Privileged Administrators, in addition to having all administrator privileges, also have a few additional permissions.
They have the privilege to configure privacy and security controls available under **Privacy Settings, IP Restrictions,** and **Emergency Measures**. Please refer the below table for a detailed difference between the roles.

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

5. How can we discover accounts and passwords through a non-domain server like the Windows server that could have many local accounts?

In order to discover local accounts from non-domain servers, you have to add a local admin account to the resource, then click on **Actions -> Configure Remote Password Reset** and provide the local admin account in the "administrator account" field. Now, if you click on 'Discover Accounts', it will discover all the accounts in the non-domain server.

6. We have a desktop as a part of the domain and we need to discover the local account and its password. When we discover the accounts through PMP, both the account name and password fields are displayed as User1.Lastname. How do we collect the user name and password on desktops that are part of the domain?

No application has the ability to pull the existing passwords. Hence, when you discover the member servers, PMP will only discover the server along with the accounts in it. We use the account name itself as password simply to not leave the password field empty. Also, for discovering the accounts from member server, you have to run the PMP service with a privileged domain account.