

User Management

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

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

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

Role	Operations					
	Manage Users	Manage Resources	Manage Passwords	View Passwords	Managing Personal Passwords	View Audit & Reports
Administrator	✓	✓	✓	✓	✓	✓
Password Administrator	✗	✓	✓	✓	✓	✗
Password User	✗	✗	✗	✓	✓	✗
Password Auditor	✗	✗	✗	✓	✓	✓

Irrespective of the role, the personal passwords remain exclusive to the individual user and other users have no control over them.