1. Introduction
2. Installation instructions
3. Basic settings
   • Configure mail server
   • Configure proxy
   • Configure security settings
   • Change the logo
4. User provisioning and management
   • Add users
   • Configure two-factor authentication
   • Create user groups
   • Set password policy
5. Password management
   • Add your resources
   • Create resource groups
   • Share account(s), resource(s), and resource group(s)
   • Configure access control workflow
   • Configure remote password reset
   • Configuring reset schedules
   • Configure password actions
6. Advanced features
   • Direct connection to websites and applications
   • Direct connection to remote systems
   • APIs to eliminate hard-coded credentials
   • Ticketing system integration
7. High availability configuration
8. Disaster recovery configuration
9. Audit settings
10. Reports
11. General settings
12. Offline access
13. Mobile access
14. Browser extensions
15. Security specifications for review
16. Best practices to follow
17. Contact details for technical assistance
Thank you for deploying ManageEngine Password Manager Pro to manage the privileged identities in your organization. This guide will provide you the basic information necessary to help you get started.

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

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

Enter all details including server name, port, sender email id, access URL, and type of authentication. Then save the configuration.
Next, you specify how you will connect to the Internet: directly or over a proxy. Configure this setting by going to Admin and Proxy Server Settings (under the General tab).

You’ll see two options here:

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

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

You can then configure certain, other basic security settings based on your specific requirements by going to Admin, General Settings, and Security Settings.

You’ll see two options:

- The first option prevents the execution of malicious scripts or code. Set the severity level as low or high.
1. If you select “Severity Low,” Password Manager Pro will start identifying the malicious scripts and code that are potentially harmful, add them to the blacklist, and prevent their execution.

2. If you select “Severity High,” Password Manager Pro will stop the execution of any script or code that contains HTML tags and attributes. Please enable this option for enhanced security. To execute a genuine script or code that contains disallowed tags and attributes, you can temporarily disable this option and re-enable it immediately after finishing your task.

- The **Activate Auto Logon** setting lets you allow or disallow your users to use Password Manager Pro’s browser extensions.

The above screenshot depicts how a customized login page looks in the web interface. For more detailed instructions for rebranding, go to this [help document](#).
After configuring the basic settings, the next step is to create accounts for your users in Password Manager Pro.

### Add users

You can add users to Password Manager Pro in many ways. If you are using corporate identity stores such as AD or LDAP, you can integrate them with Password Manager Pro and import users. You can also import users in bulk from a .CSV file or add users manually. For detailed information on adding users, check out the documents listed below:

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

### Configure two-factor authentication (recommended)

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

1. First level authentication through native or AD or LDAP.
2. Second level authentication through any one of the mechanisms below

- PhoneFactor
- Unique password through email
- RSA SecurID
- Google Authenticator
- Radius-compliant TFA

To turn on this setting, navigate to Admin, Users, and then Two-factor Authentication settings in the web interface.
Create user groups

After adding users, you can group them to carry out operations in bulk. For example, you can create a group that contains all Windows administrators. Then, you can allot passwords in bulk to this user group. To create a user group(s), navigate to Admin, Users, and then User Groups. You will find detailed information on creating user group(s) in this section of our help documentation.

Set password policy

Password Manager Pro helps enforce strong password use at all levels—be it the users’ local authentication passwords or the passwords for managed IT resources. Password Manager Pro comes with a built-in password generator to generate passwords based on the complexity levels you define in the password policies.

You can specify various conditions including minimum length, mixed characters, numerals, and more, and the generator will create the passwords as required. By default, Password Manager Pro provides three types of policies: low, medium, and strong. You can use any of these or create your own policy. You can create new password policies from the Admin, Customize, and then Password Policies section.
You can find more detailed instructions for configuring password policies in this section of our help documentation.

The term “resource” refers to all devices and applications whose privileged accounts are to be managed by Password Manager Pro. You can add your resources in various ways: a) scan your network and discover flavors of Windows, Linux, VMware, and network devices, along with their associated privileged accounts; b) import the Windows resources from your domain; c) import disparate resources in bulk from a .CSV; or d) add resources one by one, manually. You can find detailed information regarding the above options in the following sections of our help documentation.
After adding resources, you can group them for better organization and easier management. Resources can be grouped either by specifying a set of criteria or by selecting individual resources. Assuming you provide criteria, whenever a new resource is added that matches the criteria, it automatically becomes a part of that group.

When a resource is added or deleted from a group, it affects the password access shared through the group. You can view the hierarchal structure of the resources in a tree form for navigational convenience.

To create a resource group(s), navigate to Links, and then Add Resource Group. You will find detailed instructions for creating resource groups in this section of our documentation.
You can share an individual account or all accounts within a resource or a group of resources with required users or user groups in a single click. While sharing resources with other users, you can also set varying access privileges:
<table>
<thead>
<tr>
<th>Access Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View only</td>
<td>User can only access the password.</td>
</tr>
<tr>
<td>Modify</td>
<td>User can both access and modify the password that is shared. The modify privilege does not allow other users to change any other attribute of the resource.</td>
</tr>
<tr>
<td>Manage</td>
<td>You can delegate complete management of a resource group and associated resources. This includes providing share permissions to other users as well.</td>
</tr>
<tr>
<td>Share without revealing the password in plain-text</td>
<td>You can also share passwords without revealing them in plain-text in the GUI. This can be done from <strong>Admin, General, General Settings</strong>, and then <strong>Password Retrieval</strong>. The checkbox for the option “Allow users to retrieve passwords for which auto logon is configured” should not be selected to exercise this option.</td>
</tr>
</tbody>
</table>

You can find more detailed information in this section of our [documentation](https://www.passwordmanagerpro.com).

### Configure access control workflow

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

You can configure access controls by navigating to the **Resource** menu, selecting the resources for which you want to configure access controls, and clicking **Configure Access Control** from the **More Options** drop-down.
You can find more detailed instructions and use cases for configuring access control workflows in this section of our documentation.

Configure remote password reset

Password Manager Pro helps you reset passwords for a wide range of target systems anytime on demand or automatically at periodic intervals on multiple platforms across physical, virtual, and cloud infrastructures. Password reset can be done in two ways:
Notifications can be sent to users before and after the remote password reset process.

**Remote password reset: Basic configuration**

The basic configuration required for remote password reset can be carried out as a part of the resource addition. For already added resources, this can also be carried out by editing the resources. This configuration depends on the type of resource being added. Detailed instructions for configuring remote password reset for different types of resources can be found in this section of our [documentation](#).

**Configuring reset schedules**

You can periodically reset the passwords of remote resources by creating reset schedules. This can be done at the resource group level. Password Manager Pro will assign a strong, unique password to each account belonging to the resource group. To configure the reset schedule, you need to click the schedule icon present for each required resource group.
Configure password actions

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

Detailed information on configuring reset schedules is available in this section of our documentation.
These settings can be configured at the resource group level. To configure this setting, navigate to Resources, Resource Group, and then click the icon for each resource group to enable notifications. Detailed information on configuring password actions notifications can be found in this section of our documentation.

Direct connection to websites and applications

You can launch a direct connection to websites and applications from within Password Manager Pro’s web interface by configuring automatic login. This can be done in two ways: by one-click login through installing bookmarklets on browsers, or by native browser extensions. You can find more detailed information in the following sections of our documentation.

- Using Bookmarklet
- Using Browser Extensions

Direction connection to remote systems

Password Manager Pro provides an option to automatically log you in to remote target systems directly from the Password Manager Pro web interface with two options:

- Auto-logon gateway for launching Windows RDP, SSH, and Telnet sessions.
- Auto-logon helper scripts for launching custom programs from the user’s browser.

Detailed information on how to use these options, as well as their comparative merits and demerits are available in this section of our help documentation.

APIs to eliminate hard-coded credentials

Various applications require access to databases and other applications frequently to query business-related information. This communication process is usually automated by embedding the application credentials in plain text within configuration files and scripts. While hard-coding credentials makes a technician’s job easier, it’s also an easy launch point for hackers.
Password Manager Pro eliminates hard-coded passwords with secure APIs for application-to-application (A-to-A) and application-to-database (A-to-DB) password management.

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

Navigate to **Admin, General**, and then **Password Management API to configure the APIs**. For detailed instructions on configuring the password management API, refer to this section of our **documentation**.

---

**Ticketing system integration**

Password Manager Pro lets you integrate a range of ticketing systems to automatically validate service requests related to privileged access. The integration ensures that users can access authorized privileged passwords only with a valid ticket ID. This integration also extends to the Password Manager Pro workflow, which helps you grant approvals to access requests with automatic validation of corresponding service requests in the ticketing system.

To configure this setting, navigate to **Admin, General**, and then **Ticketing System Integration**. Detailed instructions on the help desk integration are available in this section of our help **documentation**.
For uninterrupted password access, Password Manager Pro offers a high-availability architecture that uses a redundant Password Manager Pro server and database instances. The high-availability configuration varies in accordance with the back-end database used. The following sections of our help documentation will guide you through the process of establishing high availability.

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

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

- **Live Backup**
- **Scheduled Backup**

To configure a data backup, navigate to **Admin, General, and then Database Backup**.

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

Auditing in Password Manager Pro has been classified into three types:

- **Resource audit**: All operations pertaining to resources, resource groups, accounts, passwords, shares, and policies
- **User audit**: All operations performed in Password Manager Pro by a Password Manager Pro user are captured under User audit.
- **Task audit**: Records of the creation of various scheduled tasks.
Information on the entire password management process in your enterprise is presented in the form of comprehensive reports in Password Manager Pro. The status and summaries of different activities such as password inventory, policy compliance, password expiry, user activity, and more are provided in the form of tables and graphs that help IT administrators make well-informed decisions on password management. Password Manager Pro provides reports under several categories and also lets you create your own reports.

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

To view and configure reports, navigate to the Reports tab in the web interface. You can find more detailed instructions in this section of our documentation.
Password Manager Pro provides multiple options for secure offline access and safekeeping of password information.

- The most basic option is to export the resource name, account name, and passwords in plain-text in a spreadsheet.
- The more secure option is to export the passwords in an encrypted HTML file.
- You can also automatically synchronize the exported HTML file to users’ mobile devices through Dropbox. Typical use case scenarios for this option include:
  1. A managed service provider (MSP) using Password Manager Pro to store the shared passwords of their clients and technicians visiting clients, both of which have no access to Password Manager Pro installed in their network.
  2. Technicians working in DMZs with no access to the Password Manager Pro web interface.

Administrators can decide which option (encrypted HTML or auto-sync to mobile devices) should be used in their organization. In addition, the export can be enabled or disabled for specific users or user groups as needed. More detailed information on exporting passwords can be found in this section of our documentation.

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

- **Android**
- **iOS**
- **Windows**
To smooth out the process of password management and auto-logon, Password Manager Pro gives you the option of securely synchronizing passwords across browsers through native browser extensions. The extensions auto-fill passwords for websites and web applications and launch RDP and SSH sessions. In addition, the extensions allow you to view all passwords, resource groups, favorites, and recently used, and provides a search option.

Once you deploy an extension, you will be able to perform most password management operations directly from the browser extension, while Password Manager Pro runs in the background.

Currently, extensions are available for Chrome and Firefox.

Password Manager Pro lets you selectively enable or disable various settings based on the specific needs of your organization. You can choose to enforce or disable various policies through these settings. Navigate to Admin, General, and then General Settings to customize your options.
Password Manager Pro has been designed to offer maximum security from the application installation to user authentication, data transmission, storage, and throughout the usage workflow. You can review Password Manager Pro’s security specifications [here](#) and decide on the proper security configurations for your organization.

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

If you have any problems getting started with the product or if you get stuck in the middle of something, remember that our tech support team is just an email or call away.

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