PASSMAN

PASSMAN FEATURES

PassMan securely stores passwords that protect business secrets and provides transparency regarding who has access to critical systems.

PASSWORD MANAGEMENT AND ENCRYPTION

Function	Description
Encryption	The system stores data in encrypted form (AES-256 bit), and a master code is required to unlock the vault.
Centralized password management	Users' passwords are stored in a secure, central location, which can only be accessed with the appropriate permissions.
Password management	Users have the ability to create, store, change and reset passwords with appropriate security parameters.
Password sharing	Shared passwords can be securely and granularly configured for sharing between users, resulting in controlled and traceable password management.
One-Time Password (OTP) sharing	This feature allows users to share unique, one-time passwords (OTPs) with each other.
Password import	Existing password lists can be imported, including from browsers.
Private folder	Each user has a folder that no one, not even the superuser, can access.
User's own encryption key	Data stored in the private (personal) folder can be encrypted with the user's own encryption key. This key is not saved on the server.
Secure sharing with external email addresses	Passwords (or files) can be easily shared with individuals who do not use PassMan.
Password policies	This allows regulation of password length, complexity, uniqueness, and validity period, reducing the security risks associated with weak passwords.
Strong password generation	The system can generate passwords based on specific criteria (policies), so users do not have to come up with passwords themselves.
Attachments	There is an option for securely storing files and documents containing sensitive information.

Password change on remote systems (including automatic changes)	Regular password changes are necessary for security reasons but often pose challenges. Automatic password change provides a solution for this task as well.
Instant password validity check (on remote systems)	It is possible to check whether the passwords stored in PassMan for accounts match the passwords set on the target systems at that moment. It attempts to log in to the respective system with the given password.
Scheduled password valitidy check (on remote systems)	The software monitors on a schedule whether the passwords of accounts stored in the Vault match the passwords set on the target systems. It attempts to log in to the respective system with the given password. A report on the results is sent to the specified users.
SSH key rotation support (including automatic changes)	The system is capable of storing, generating, and rotating SSH keys, including automatic changes.
Storage and restoration of previous passwords	Passwords valid at a specific point in time can be restored. This is especially useful for systems restored from old backups.

ACCESS AND PERMISSION MANAGEMENT

Function	Description
User and group management	User accounts and groups can be managed and created, facilitating centralized and transparent permission management.
Temporary permissions	The user can access sensitive data only for a specified period. Limiting unnecessary access time reduces the risk of internal misuse.
Secret login (without password visibility)	The user logs into a target system without having permission to view the password, which reduces the risk of misuse.
Linked user accounts	A user account can be linked to multiple devices, allowing login to various applications/websites using the same user account (e.g., Apple ID).
AD integrated login	Users do not need to register separately in the system; they can log in using their AD credentials. Access to which passwords they can use must be managed within PassMan.
SSO (SAML2, Open LDAP)	Users can access multiple applications with a single authentication process using SAML2 or OpenLDAP standards.
Two-Factor Authentication (2FA)	Two-factor authentication requires two different authentication methods for user identification. In the case of PassMan, traditional (username/password) login can be complemented with its own QR code authentication or a one-time login code generated by an external authentication application.
Role-based access	Access to secrets can be regulated based on predefined roles or permission groups.

Permission request process	Users have the option to request access to systems and accounts, allowing them to use a password only when truly necessary for their work tasks and for as long as needed.
Mandatory note feature	For certain features, it can be configured to require a mandatory note to be provided.
Emergency access	In exceptional circumstances (e.g., system failure), administrators need immediate access to resources because there is no time to wait for human approval.
Secondary approval login	It is possible to approve or deny my login from another device within the mobile application.
Secondary approval access	For certain actions, such as password viewing, a re-login password request or mobile approval can be set up to verify the identity of the person executing the action.
Full access super admin role	This role provides the highest level of permissions, allowing modifications to all system settings. However, affected individuals will receive notifications about such changes. Its primary function is to enable the export of system data and to allow for the retrieval of any potentially "lost" data.

AUDITING AND REPORTING

Function	Description
Auditability (activity log)	All operations performed in the system are logged, allowing users to see who did what and when.
Auditor role	A dedicated role for external auditors (read-only access) that assists in compliance during potential audits. Users with this role can view the activity log data.
SIEM integration	The system can be integrated with SIEM systems, meaning log data is automatically transferred to the configured external log collection system.
Session recording and playback	This feature allows for the recording of user activities and their later review. It provides a precise view of what the user was doing at a given moment.
Built-in reports	Automatically generated reports provide instant answers to daily password management-related questions, supporting quick analysis and decision-making.
Alerts, notifications	The system can send alerts and notifications via email, allowing timely intervention before any damage occurs.

AUTOMATION AND CONVENIENCE

Function	Description
1-Click login to websites	With PassMan-stored username/password data, users can log into a website or web application with a single click.
Automatic password autofill in browser	When navigating to the login page of websites or web applications, the system automatically fills in the passwords and logs into the target system using the stored credentials.
1-Click remote access (web console)	Using the username/password data stored in PassMan, users can log into Windows (RDP) and Linux (SSH) machines with a single click through the web console running in the browser. There is no need for a separate console program, and users do not need to copy the username/password pairs.
Account discovery (Windows)	Instead of time-consuming manual input, the system can automatically discover user accounts, aiding in the identification and management of hidden or unused accounts, thereby enhancing security. PassMan can discover local and domain accounts, including service accounts, for Windows machines.
Automatic scheduled backup	To ensure continuous security, the system automatically creates database backups at regular intervals.

SYSTEM MAINTENANCE AND SUPPORT

Function	Description
Pre-installed virtual machine	PassMan requires a running environment such as VMware, MS Hyper-V, or ProxMox. The virtual machine includes all necessary software (operating system, database, web server, security software, etc.); there is no need to install and configure server programs. The default setup time is 15 to 60 minutes.
High Availability (Cluster)	PassMan ensures high availability with a 3-node cluster solution.
External load balancer support	In a corporate environment, a load balancer solution is typically available. This allows the cluster system to actively utilize nodes that would otherwise only come into play in case of a failure. As a result, the system's performance can be significantly increased without the need to expand existing resources.
Quick system recovery	The system can quickly restore to a previous, functional state to minimize downtime and reduce data loss.
Password export	The system allows for the export of an existing database (data stored in the password manager), which can only be performed by a user with a super administrator role in PassMan.

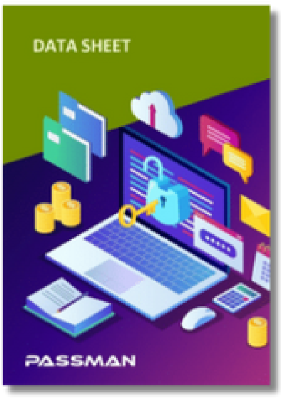
Vendor support	Vendor support provides direct access to the system developers, who assist in resolving issues and answering questions. This ensures faster troubleshooting and continuous system updates.

MOBILITY AND ACCESS OPTIONS

Function	Description
Native Windows and Linux Programs	Windows and Linux programs are available that enable 1-click login on the client machine using Windows Remote Desktop (RDP) or PuTTY (SSH) solutions.
Mobile app (iOS, Android)	The mobile application (iOS, Android) allows users to access the system and manage their accounts from their mobile devices, increasing flexibility and accessibility, even on the go.
Browser extensions	Browser extensions available for various browsers (including Chrome, Safari, Firefox, and Edge for PassMan) provide users with added convenience for web logins, password saving, and other password management activities.
Full integration with Jira and Jira Cloud app	The Jira integration enhances workflow efficiency by allowing password management based on Jira permissions and replacing the typically "stored" text passwords in Jira tickets with easily insertable, secure login links.
Hosting / Data Storage Location	Cloud / On-premise

Learn more about PassMan!

Secure password storage and sharing. Automated password rotation for GDPR compliance, with PAM functionality for NIS2 compliance. Deployment on server or as a cloud service.



passman.co

support.passman.co

+36 1 299 0225