ManageEngine
Password Manager Pro

Security Specifications

Overview

Password Manager Pro deals with administrative passwords that offer secure access to enterprise credentials and devices. Any compromise on the security of these passwords will expose organizations to serious risks. Therefore, we've designed Password Manager Pro, to offer maximum security right from the application installation to user authentication, data transmission, storage, and throughout the usage work flow.

Besides the following security measures,we continuously strive to make the application more secure. This document briefly provides details about the security specifications of the product.

Security at Various Levels

Password Manager Pro protects data at various levels and is classified into the following categories:

Security Specifications

Vaulting Mechanism	• AES-256 Encryption • Dual encryption - at application level first and at database level again • Encryption key and encrypted data cannot reside together • FIPS 140-2 compliant mode • Multi-tenant architecture (MSP edition)
Identification & Authentication	**Strong Application Level Authentication** • Integration with identity stores like Microsoft AD, any LDAP compliant directory service, and RADIUS • Local authentication mechanism with SHA2 (SHA-512) algorithm • Smart card authentication • SAML 2.0 single sign-on

Identification & Authentication	**Two-factor Authentication** • Phone Factor • RSA SecureID • One-time unique password sent by email • Google authenticator • RADIUS authenticator • Duo Security • YubiKey
Data Integrity	**Data Transmission** • Encrypted and over HTTPS • SSL mode for client connections • Password resets through SSH **Data Storage** • Dual AES-256 encryption **Secure Remote Access** • Windows RDP, SSH, and Telnet sessions from any HTML5-compatible browser • No need for additional plug-in or agent software • Remote connections are tunneled through the Password Manager Pro server • Passwords needed to establish remote sessions do not need to be available on the user's browser • No direct connectivity between user device and remote host **Application-to-Application Password management** • HTTPS connections for inter-app communications • Verification through SSL certificate

Data Integrity	**Web GUI Input Validation** • Protection against SQL injections, cross-site scripting, buffer overflow, and other attacks
Access Control Measures	**Data Access Control** • Granular access control mechanism • Request-release workflow for password access • Audit trails • Automated periodic password resets • Password policy violation reports
Audit, Accountability Control, & Real-time Alerts	**Detection Capabilities and Non-Repudiation Measures** • Real-time alerts for password events • Raise SNMP traps and/or Syslog messages • Privileged session recording
Availability Mechanisms	**High Availability** • Redundant PMP server and database instances • Direct TCP Connection with latency for database replication • PMP Agents for network segments not directly reachable **Offline Access** • Encrypted HTML file • Additional passphrase for AES-256 encryption **Mobile Access** • Native Apps for iOS and Android platforms • Passphrase as encryption key • Offline access • Audit trails for data sync to mobile device

Disaster Recovery	**Provision for Backup** • Live and periodic database backup • Encrypted storage of backup files **Emergency Access** • Super-administrator accounts for fire-call or break-glass purposes
Automatic Connection to Websites & Applications	**Browser Extensions** • Firefox and Chrome extensions • CSP best practices • Prevention of inline JavaScript execution and AJAX requests **Bookmarklets** • Secure mechanism to bring dynamism to browser bookmarks

Security Features

1. Vaulting Mechanism: Secure by Design

1.1. Installation Master Key

- Password Manager Pro uses AES-256 encryption (the strongest known encryption that the US government has approved). The key used for encryption is auto-generated and is unique for every installation. This serves as the first-level encryption key.
- The first-level encryption key is not allowed to be kept with the Password Manager Pro installation. This is done to ensure that the encryption key and the encrypted data, in both live and backed-up databases, do not reside together.
- The recommended setup is to store the key in a physically separate server or device and ensure that it is available to the server during application start-up. Subsequently, the key is held only in the server memory and never written anywhere.
- Password Manager Pro also supports periodic rotation of the encryption key, where a new key is generated and applied to the existing data and then the old key is discarded. More info.

1.2. Database Key

- The Password Manager Pro database is secured through a separate key, which is auto-generated and unique for every installation.
- The key for the database can be stored securely within Password Manager Pro.
- Password Manager Pro also allows users to store the database key in any secured location, leaving the key accessible to only the server.
- The RDBMS is always configured to accept only secure connections (forces SSL mode for client connections) and clients can connect only from the same local host. In cases where the web server and the RDBMS have to reside in separate servers, the configuration enforces connections only from configured IP addresses.

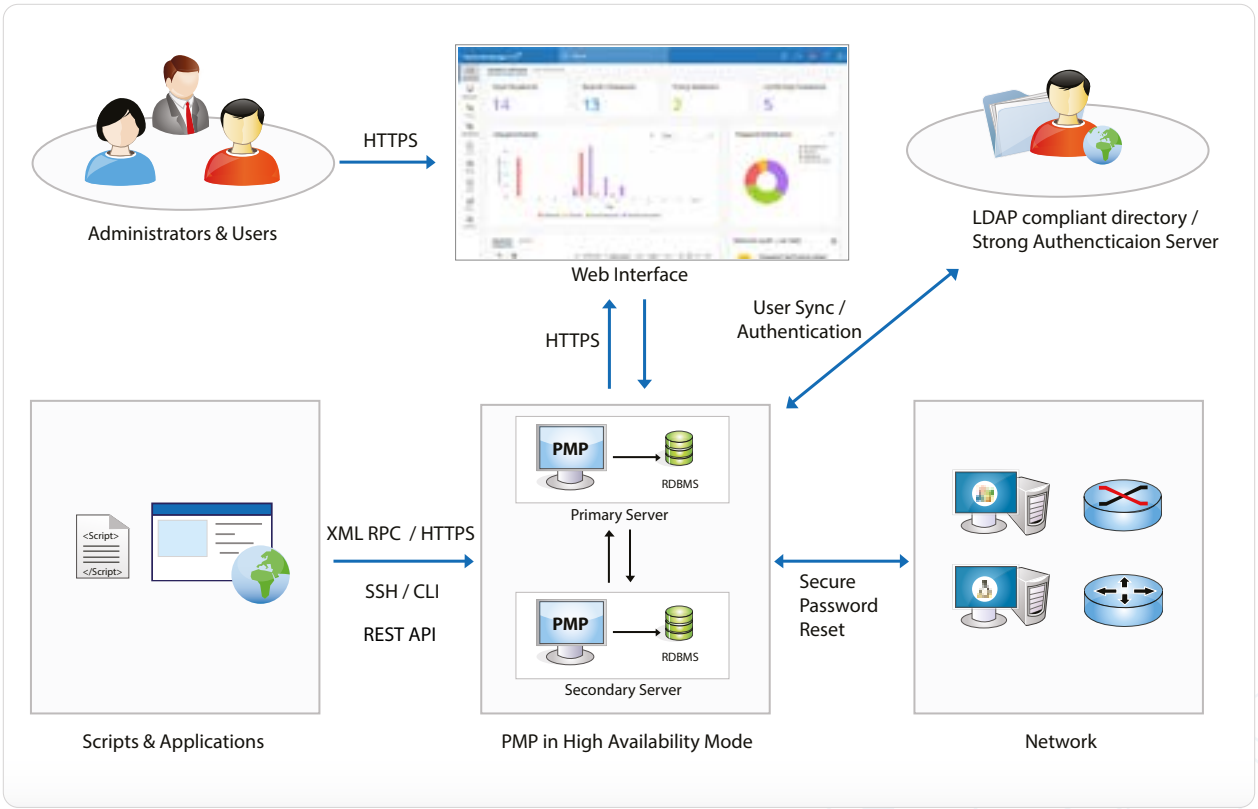
1.3. FIPS-compliant Mode

- Password Manager Pro can be set up to run in the FIPS 140-2-compliant mode (with SQL server back end) where all encryption is done through FIPS 140-2-certified systems and libraries.

1.4. Multi-tenant Architecture (MSP Edition)

- Password Manager Pro provides MSP edition for secure data segmentation between departments or in the case of MSP customers, between their customers. The segmentation is implemented at the level of database rows in the RDBMS.

Fig 1. Product Architecture



- Each department or customer that requires data segmentation is provided a value range for the unique identity for each row. All database operations performed for that department or customers is automatically restricted to that value range. For more details, click here.

2. Identification and Authentication

2.1. Strong Application Level Authentication - Various Options

Password Manager Pro provides four options for uniquely identifying the users who will be accessing the application. All the options are complemented by various two-factor authentication provisions, which provide an extra layer of security.

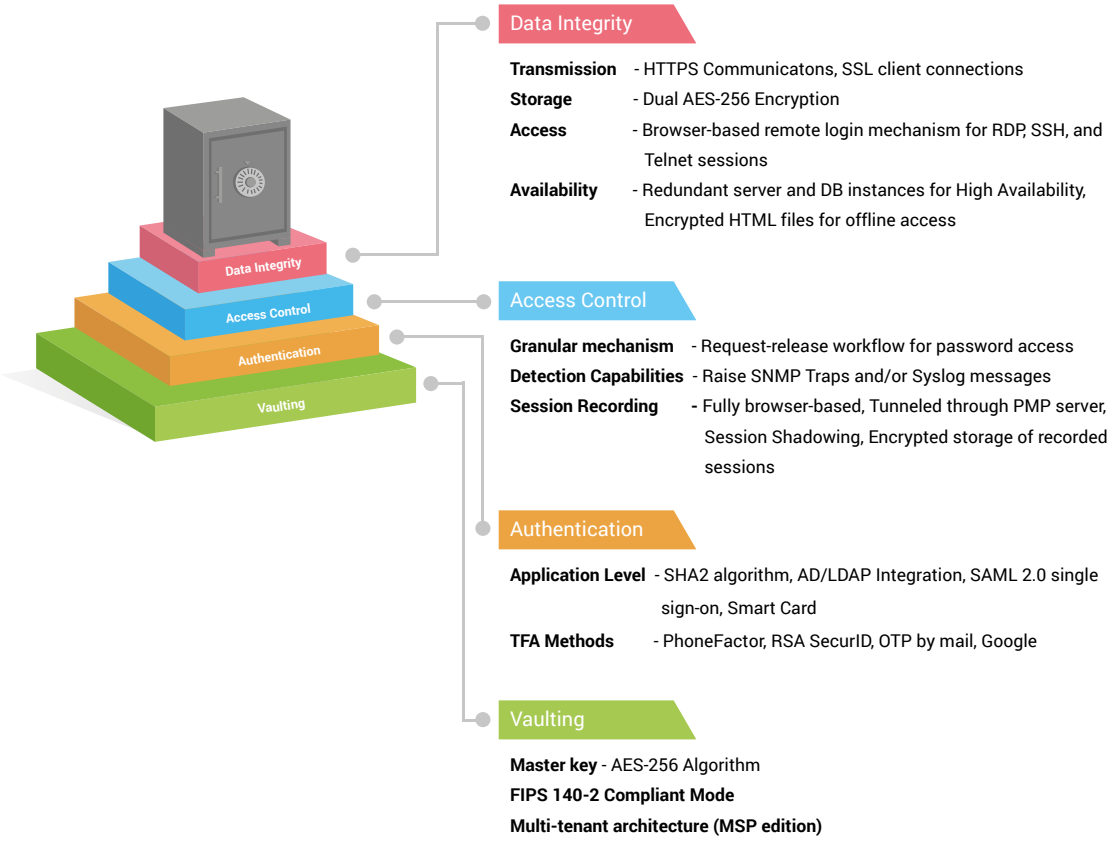
- **Integration with identity stores**: Password Manager Pro readily integrates with external identity stores like Microsoft Active Directory, any LDAP-compliant directory service (Novell eDirectory and Oracle OID), and RADIUS. Users can be imported from identity stores and the respective authentication mechanism can be leveraged. Users will be uniquely identified through their respective accounts in the identity store. More info.

- **Unique accounts and strong local authentication**: Password Manager Pro comes with a local authentication mechanism in which unique accounts are created for users. Users will be able to access the application with their credentials. Password Manager Pro employs SHA2 algorithm to generate passwords, which ensures that each login password is unique and irreversibly secured.

- **Common access card**: Password Manager Pro supports smart card authentication - the user must possess the smart card and know the personal identification number (PIN) as well. For more details, click here.

- **SAML compliant service**: Password Manager Pro offers support for SAML 2.0, which facilitates integration with Federated Identity Management Solutions for Single Sign-On. Password Manager Pro acts as the service provider (SP) and it integrates with Identity Providers (IdP) by using SAML 2.0. The integration basically involves supplying details about SP to IdP and vice versa. After you integrate Password Manager Pro with an IdP, the logged in users can log on from the respective identity provider's GUI without providing the credentials again. Fore more details, click here.

Fig 2. Product Security Architecture



2.2. Assurance Mechanism - Two-factor Authentication

To introduce an additional level of security, Password Manager Pro provides two-factor authentication. Users will be required to authenticate through two successive stages to access the web interface. The second level of authentication can be done using one of the following:

- **PhoneFactor** - This leading global provider of phone-based TFA enables simple and effective security by placing a confirmation call to your phone during the login process.
- **RSA SecurID** - Integrate RSA SecurID with Password Manager Pro to generate a one-time validation token that changes every 60 seconds.
- **Unique password through email** - Authenticate by emailing users unique passwords. The passwords validate the user for one login session and then expire.
- **Google Authenticator** - Time-based numeric tokens developed by Google can be received by installing the Google Authenticator app on your smart phone or tablet device.
- **RADIUS Authenticator** - Leverage the authentication mechanisms of any RADIUS-compliant system, such as Vasco Digipass, to create one-time passwords.

- **Duo Security** - Leverage the Duo security authentication as the second level of authentication.
- **YubiKey** - Generate one-time passwords with YubiKey as the medium for the second level of authentication.

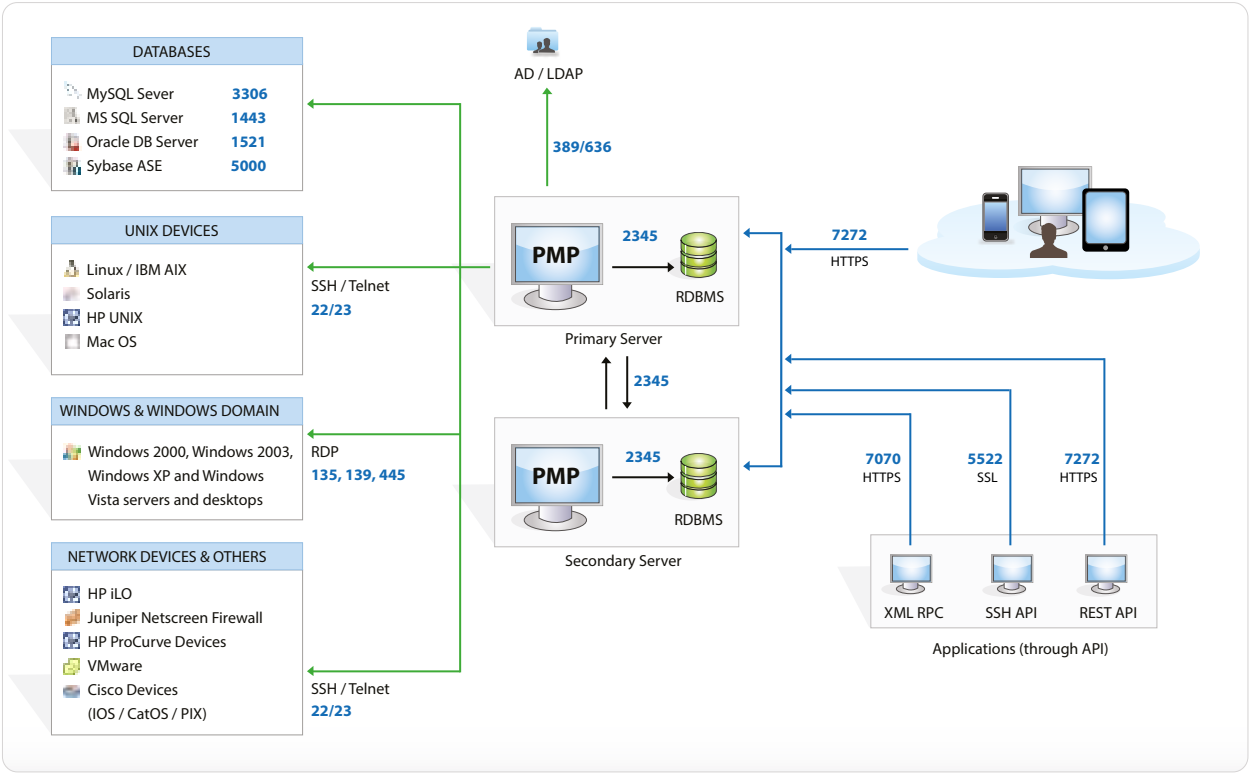
For more details, click here.

3. Data Integrity

3.1. Data Transmission

- All data transmission between the Password Manager Pro user interface and the server are encrypted and take place through HTTPS.

Fig 3. Data Flow Diagram



- All data transmission between the Password Manager Pro server and database occur over SSL.
- For remote password reset actions, there is an option to transmit user password using SSH.

- **Communication between PMP and agents**: Password Manager Pro allows agents to be deployed that can connect to the server. The communication is always one way - that is, the agent always initiates this connection. Therefore, only the server needs to be available for the agents, eliminating the need to punch firewall holes or creating VPN paths for the server to reach all agents. The agent periodically pings the server through HTTPS to check whether any operation (password reset or verify password) is pending for execution. The agent will then carry out the tasks and after completing them, will notify back the server with the results. More info.

- **Communication between Primary and Secondary servers:** Encrypted and over HTTPS

3.2. Data Storage with Dual Encryption

- Password Manager Pro is designed as a web application with a web server for business logic and RDBMS for data store.

- Upon applying appropriate initialization vectors and other standard good practices around encryption, the first-level encryption key with AES-256 algorithm is generated in the web server.

- The encrypted data is pushed to the RDBMS for storage by using SQL queries. Next, Password Manager Pro encrypts the data with built-in AES functions of RDBMS for dual layers of encryption.

- The recorded data of privileged sessions are also encrypted before storage and can be played only through proprietary player because the data is stored in the proprietary format.

3.3. Secure Remote Access

- Password Manager Pro allows users to launch highly secure, reliable, and completely emulated Windows RDP, SSH, and Telnet sessions from any HTML5-compatible browser, without the need for additional plug-in or agent software.

- Remote connections to end points are tunneled through the Password Manager Pro server, requiring no direct connectivity between the user device and remote host.

- In addition to superior reliability, the tunneled connectivity provides extreme security as passwords needed to establish remote sessions do not need to be available on the user's browser. More info.

3.4. Application-to-Application Password Management

- In the case of application-to-application passwords, Password Manager Pro exposes a web API and the applications connect and interact through HTTPS. The application's identity is verified by forcing it to issue a valid SSL certificate, matching the details that have already been recorded in PMP about the application. More info.

3.5. Web GUI Input Validation

- Password Manager Pro thoroughly validates all inputs in the GUI. Usage of special characters and HTML code are filtered, and the application is guarded against common attacks like SQL injections, cross-site scripting, buffer overflow, and other attacks.

4. Access Control Measures

4.1. Data Access Control

- All data access in Password Manager Pro is subjected to the granular access control mechanism. Password ownership and sharing practices are well defined, and users get access only to authorized passwords.

- For highly sensitive assets, an extra layer of security could be enforced by forcing the authorized users to go through a request-release mechanism. Whenever the password of a sensitive IT resource needs to be accessed, a request must be made, which goes for approval by the administrator (persons who are designated to authorize access) and is released for a limited time period. More info.

- All access to passwords (who accessed what password and when) and all operations done by the users on any resource are captured in audit trails, ensuring accountability for all users and actions.

- In addition, as part of policy enforcement, organizations can automatically randomize the passwords of sensitive IT resources periodically. Password Manager Pro assigns strong, unique passwords to assets. It also analyzes the passwords of systems for required complexity and reports violations. These provisions help prevent unauthorized access to passwords, which in turn prevents unauthorized access to systems and applications. More info.

5. Audit, Accountability Control, and Real-time Alerts

5.1. Detection Capabilities

- Password Manager Pro provides real-time alerts and notifications on various password events, including access, modification, deletion, changes in share permissions, and other specific events. More info.
- The audit module that records every user and system action also provides the ability for administrators to configure what events need to be sent to SIEM systems. The event alerts could either be sent as standard Syslog messages or SNMP Trap. More info.
- All actions performed by the users during the privileged session are video recorded and stored securely for forensic analysis.
- In addition to session recording, Password Manager Pro allows administrators to monitor privileged sessions in real time. If any suspicious activity is found, the administrator can snap the connection immediately. More info.

5.2. Non-Repudiation Measures

- Every action and scheduled task executed by users in the user interface is audited.
- The audit information, which contains details such as 'who' did 'what' operation 'when' and from 'where' is stored in the same database. The audit logs are tamper-proof, ensuring non-repudiation.
- The RDBMS is always configured to accept only secure connections (forces SSL mode for client connections), and clients can connect only from the same local host. In cases where the web server and the RDBMS have to reside in separate servers, the configuration enforces connections only from specific IP addresses.

6. Automatic Connection to Websites and Applications

6.1. Browser Extensions

- Password Manager Pro provides browser extensions for Firefox and Chrome. The extensions have been designed to ensure the highest level of data security and privacy.
- Content Security Policy (CSP) best practices are enforced to effectively combat content injection attacks.

- Inline JavaScript execution and AJAX requests to other sites have been disabled to prevent XSS attacks.

- The highest level of security has been ensured in all stages of data retrieval and transit, including

    1. Validating passphrases
    2. Retrieving encrypted data from the server
    3. Holding passwords and other sensitive data as JavaScript variables (which cannot be accessed by any external application or other extensions)
    4. Storing other data in the background as local records
    5. Passing credentials to websites

- Whenever the user logs out or remains idle for a specified time, local data gets completely erased.

6.2. Bookmarklets

- The bookmarklet allows users to log on to web applications without entering the credentials manually.

- The bookmarklet first opens the URL of the web app and then executes a script that accesses the server, retrieves the user name/password for the requested app, populates the field in the login page of the app, and submits the page for authentication.

- The script attached to the bookmarklet works only when the user is on the right login page of the application. Moreover, the bookmarklet does not work when the user is not logged on to Password Manager Pro and there is no valid session on the browser. More info.

7. Availability Mechanisms

7.1. High Availability

- Password Manager Pro provides high availability to ensure un-interrupted access to passwords, which is made possible through redundant server and database instances.

- One instance will be the primary to which all users stay connected and the other instance will be secondary/standby. The administrators and users can connect to the primary or secondary instance to access the GUI console through a desktop browser or smart phone or tablet.

- The primary and secondary servers can be installed geographically apart, even across continents, as long as they have a direct TCP connection with latency good enough for database replication.
- The servers can manage end points to which it has direct TCP connections. For managed systems that are in DMZ, or in network segments not directly reachable for the server, agents can be installed that can reach the server over standard HTTPS.
- At any point in time, data in both primary and secondary will be in sync with each other. The data replication happens through a secure, encrypted channel. More info.

7.2. Offline Access

- Password Manager Pro facilitates secure export of passwords for offline access in the form of an encrypted HTML file and even synchronizes the file to their mobile device.
- Before export, the user is asked for a passphrase to secure the data with AES-256 encryption. The offline copy can be accessed only by providing the passphrase. Moreover, this passphrase is not stored anywhere in the server.
- Whenever the user makes an offline copy of the resources/passwords shared with him/her, the activity gets reflected in the audit trail.

7.3. Mobile Access

- Password Manager Pro provides native apps for iOS and Android platforms. The mobile apps optimize ease-of-use without compromising on data security. The mobile apps are as secure as the installation and uses the same AES-256 encryption.
- The apps are guarded by an additional passphrase entered by the user, which is used as the encryption key. So, even if the mobile device is stolen, passwords cannot be deciphered in plain text.
- If two factor authentication is configured, the same becomes applicable for the mobile apps too.
- The apps do not let users stay logged in and force them to authenticate every time when accessing the app.
- Whenever an offline copy of data is made on the web server, the native app syncs the file to the user's device and this activity gets reflected on the audit trail. After the HTML file is deleted by the user, it is also erased from the user's device as part of the synchronization.

8. Disaster Recovery

8.1. Provision for Backup

- Password Manager Pro offers provision for both live backup of the database and periodic backup through scheduled tasks.

- All sensitive data in the backup file are stored in the encrypted form in a .zip file under the <**PMP_Home/backUp**> directory or under the destination directory configured by the admin.

- The backup copy will not have the encryption master key because Password Manager Pro does not allow both the encryption key and the encrypted data in both live and backed-up database to reside together. Unless one presents the encryption key, sensitive data cannot be deciphered from the backup copy.

- While a database backup operation is in progress, no configuration change can be performed in Password Manager Pro. More info.

8.2. System Failure and Recovery

- In the event of a disaster or data loss, users can quickly make a fresh install of the same version of Password Manager Pro and restore the backed-up data to the database.

- Disaster recovery for Password Manager Pro with MS SQL Server as the back-end database can be performed only with the master key initially used for encryption upon installation. More info.

8.3. Emergency Access

- For fire-call or break-glass purposes, one or a few administrators can be designated as super-administrators who will have unconditional access to all information in the system, including all passwords added to the system by other administrators.

- An administrator cannot designate himself/herself as a super administrator. It has to be approved and carried out by one or more other administrators.

- When the system has one or more super administrators configured, the user interface shows an indication to all users to that effect.

- After an admin becomes a super admin, he/she can log on to Password Manager Pro and enforce an additional option to prevent the creation of additional super admin accounts.