ManageEngine Password Manager Pro Vs Thycotic Secret Server

Features Comparison Sheet

(As per information available on Thycotic Secret Server's website on March 23, 2018.)

Feature	ManageEngine Password Manager Pro	Thycotic Secret Server
Password Storage & Management		
Centralized, Secure Repository of Privileged Passwords	Yes	Yes
Automatic Discovery of IT Assets and Privileged Accounts	Yes	Yes
Web-based Access	Yes	Yes
Storing & Managing Shared Accounts	Yes	Yes
Application-to-Application (A-to-A), Application-to-Database (A-to-DB) Password Management to Eliminate Hard-coded Passwords	Yes	Yes
Windows Service Accounts Password Management	Yes	Yes
Options for A-to-A and A-to-DB Password Management	RESTful APIs, Web Service (XML-RPC based) and Command Line (SSH-CLI)	Web Services API
Password Encryption	AES 256-bit Algorithm	AES 256-bit Algorithm
Password Ownership	Yes	Yes
Selective Sharing of Passwords	Yes	Yes

Fine-grained, role-based permission to view/ edit/manage Passwords	Yes	Yes
Grouping Resources / Passwords Bulk Operation	Yes	Yes
Storing Files, Images, Digital Identities	Yes	Yes
Remote Password Reset		
Synchronizing Passwords of Remote Resources	Yes	Yes
Deploying Agents for Remote Password Reset	Yes	Yes
Agent-less Remote Password Reset	Yes	Yes
Scheduled, Automatic Password Rotation	Yes	Yes
Verifying the Integrity of the Passwords in Target Systems	Yes	Yes
Windows Service Account Reset	Yes	Yes
Provision for triggering any follow-up action after Password Reset	Yes	Yes
Direct Connection to Remote Resources in Data Centers by Configuring Landing Servers (Jump Servers)	Yes	Yes
Platforms Support for Remote Password Reset		
Supported Platforms for Remote Password Reset	**Operating Systems** Windows, Windows Domain, Flavors of UNIX and Linux, Solaris, Mac OS, HP iLO **Windows Applications** Service accounts,	• Active Directory • Blue Coat • LDAP (Active Directory, OpenLDAP, LDAPS) • Unix/Linux/Mac (incl. root)

	Scheduled Tasks, IIS Application Pools, COM+ **Databases** MS SQL Server, MySQL Server, Oracle DB Server, Sybase ASE **Network Devices** Cisco Devices (IOS, CatOS, PIX), HP ProCurve devices and Juniper Netscreen Devices **Directories** LDAP Server (Novell eDirectory, Oracle OID, OpenLDAP and any other LDAP Server) **Virtual Environments** VMware vCenter and ESX/ESXi **Cloud Environment** Amazon Web Services, Microsoft Azure, Google Apps, Rackspace, Salesforce	• MS SQL Server • Oracle • Sybase • MySQL • VMware ESX • DSEE • Cisco • SonicWALL • Juniper • Enterasys • WatchGuard • Checkpoint • Dell DRAC • HP iLO • Open LDAP • ODBC • SSH/Telnet • PostgreSQL • Salesforce • SAP • AS/400 • Google • Amazon • Windows Live

	Note: Apart from the list of devices/resources mentioned above, Password Manager Pro supports remote password reset of other resources through a feature named "Password Reset Listener".	
Password Access Control Workflow		
Enforcing authorized users to request the release of specified accounts only after approval one or more designated approvers for dual approval	Yes	Yes
Time-limited access to passwords	Yes	Yes
Exclusive access to passwords for users	Yes	Yes
Notifications / Alerts on Check-in, Check-out of Passwords	Yes	Yes
Password Auto-reset after the end of exclusive use by a user	Yes	Yes
SSH Key & SSL Certificate Management		
Automated SSH/SSL Discovery	Yes	N/A
SSH Key Pair Creation and User Association	Yes	Yes
SSH Keys Periodic Rotation	Yes	Yes
Certificate life cycle management (acquisition, deployment and auto renewal from third party CAs)	Yes	N/A
Generate self-signed certificates	Yes	N/A

CSR Process Management	Yes	N/A
SSL Certificate Deployment & Validity Tracking	Yes	N/A
SSL Vulnerability Scanning	Yes	N/A
SSL Certificate Expiration Alerts	Yes	N/A
Authentication		
AD/LDAP Authentication	Both AD & LDAP	AD Authentication
RADIUS Server Authentication	Yes	Yes
LDAP servers supported	Novell eDirectory, Oracle OID, OpenLDAP and any other LDAP server	-
Native Authentication by Application	Yes	Yes
Smart Card / PKI / Certificate Authentication	Yes (Smart card authentication native to the product, configured in the user interface in a few simple steps.)	Yes (Not native to the product but leverages smart card authentication support from underlying Microsoft IIS system. Two levels of configuration required at both IIS and the product as explained in https://support.thycotic.com/kb/a545/does-secret-server-support-smart-cards.aspx)
SAML Authentication	Yes	Yes
Two-factor Authentication	Yes	Yes
User Management		

Importing Users from AD/LDAP	Import from AD & LDAP	Import from AD
User Groups for Bulk Operations	Yes	Yes
Role-based Access Restrictions	Yes	Yes
Optional Super-admin with Access to all Managed Passwords (Break Glass Provisions)	Yes	Yes
Password Event Notifications		
Notifications on Password Retrieval, Reset, Expiry, Ownership Change etc	Yes	Yes
Password Policies & Compliance		
Pre-built Password Policies of Varying Standards of Strength	Yes	Yes
Provision for Creating Custom Policies	Yes	Yes
Enforcing Usage of Strong Passwords, Standard Password Practices	Yes	Yes
Checking Password for Compliance to Standards	Yes	Yes
Audit & Reports		
Logging all access to passwords – 'who', 'what' and 'when' of password access	Yes	Yes
Complete record of all password management operations performed	Yes	Yes
Complete record of all user activities	Yes	Yes
Integration with SIEM tools	Yes. Raises SNMP Traps, Syslog messages and emails	Yes. Logs to a CEF or Syslog listener
Reports on Password Inventory, Policy Compliance, Password Expiry etc	Yes	Yes

Out-of-the-box reports on Government and Industry Regulations	PCI-DSS, ISO/IEC-27001, NERC-CIP	PCI-DSS, SOX, HIPPAA, Basel II, NIST 800-53, 201 CMR 17
Sending Reports by Email	Yes	Yes
Generating Reports in PDF	Yes	Not Known
Custom Reports	Yes	Yes
Backup, Disaster Recovery & High Availability		
Scheduled Backup of Database	Yes	Yes
Live Backup through Data Replication	Yes	Yes
Tools for Disaster Recovery	Yes	Yes
Uninterrupted Access to Passwords (High Availability)	Yes	Yes
Uninterrupted access to passwords (Fail-over Service)	Yes	Yes
Security Aspects		
Encryption Key Hiding	Yes	Yes
Penetration Test by Third-party Experts	Yes. Password Manager Pro has passed the penetration testing by Seibert Media.	Not Known
Two-factor Authentication	Yes	Yes
Options for Two-Factor Authentication	• PhoneFactor - a phone-based authentication service • RSA SecurID authentication • Google Authenticator	• Authentication through confirmation emails • RSA Tokens • Google Authenticator • Duo Security

	• Duo Security • Any RADIUS-compliant two-factor authentication mechanism • A one-time, randomly generated unique password sent by PMP to the user by Email	
Session Protection	SSL	SSL
Data Transmission	HTTPS	HTTPS
Data Storage	AES-256	AES-256
Dual Encryption	Dual encryption of passwords and files for extra security. Sensitive data are now encrypted once in the application (AES 256-bit) and once in the database. The encryption key is auto-generated and is unique for every installation. For production instances, PMP does not allow the encryption key to be stored within its installation folder. This is done to ensure that the encryption key and the	DoubleLock - An additional custom encryption key that can be accessed only with a password that's unique per user.

	encrypted data, in both live and backed-up database, do not reside together.	
Provision to prevent cross-site scripting	Provision to prevent the execution of malicious code/script in the application to combat cross-site scripting	Yes
FIPS 140-2 Compliance	Yes	Yes
Monitoring Failed Login Attempts	Yes	Yes
Termination of inactive user sessions	Yes	Yes
Tools & Utilities		
Importing Passwords	Yes	Yes
Ticketing system Integration	Yes	Yes
Direct Connection to Target Systems, Managed Devices, Websites	Yes (HTML-5 powered first-in-class remote login mechanisms. From any HTML5-compatible browser, users can launch highly secure, reliable and completely emulated Windows RDP, SSH and Telnet sessions with a single click, without the need for helper scripts, additional plug-in or agent software)	Yes
Remote Sessions (RDP, SSH & Telnet) from iPad & other Tablet Devices	Yes	Not Known

Options for Opening Automatic Connection	• RDP • VNC • SQL • SSH • Telnet	• RDP • SSH • PuTTY • Custom Launcher
Secure Offline Access	Yes. (1) Through native mobile app (2) Export passwords in the form of an AES-256 encrypted, HTML file for offline access. Option to automatically sync the offline data to smartphones or tablet devices via Dropbox.	Yes
Exporting Passwords in various formats	Yes	Yes
Password Generator	Yes	Yes
Password History	Yes	Yes
Separate Personal Password Management	Yes (Users are provided the option to supply their own encryption key to encrypt personal passwords. This ensures absolutely no one else can ever see user's personal passwords in plain text, including administrators that have access to the password database)	Yes (Implemented as a feature where a folder is not allowed to be shared with other users. But administrators have access to user's personal password folder in the break glass mode, right in the product user interface)

Client Customization to Suit Specific Needs	Yes	Yes
Mobile Support & Native Apps	Yes (Android, iOS and Windows)	Yes (Android, Blackberry, iOS, Windows)
Browser Extensions	Yes (IE, Chrome, Firefox)	Yes (IE, Chrome, Firefox, Safari)
Privileged Session Management		
Privileged Session Recording & Playback	Yes	Yes
Session Shadowing / Dual Controls	Yes	Yes
Multi-Tenancy		
Multi-Tenant Architecture	Yes	No (Multi-tenancy available only for Secret Server SaaS version)
Platform Support for Product Installation, Licensing		
Supported Platforms for Server Installation	Windows & Linux	Windows
Cloud-ready	Yes (AWS, Azure)	Yes
Licensing Model	Based on the number of administrators and password administrators alone. No restriction on the number of users, passwords to be stored. Convenient Annual Subscription & Perpetual Options. Simple, transparent and	Based on the number of every single active user. Different editions come with different pricing models; some are not published. Within editions, there is base price, per user price, additional add on module charges.

	all inclusive pricing. All details are published on the website.	Relatively complex and non-transparent pricing.

Disclaimer: The above comparison chart has been compiled after gathering relevant information from the website and user guide of Thycotic Secret Server as on March 23, 2018. Though every care has been taken to ensure the correctness of the information provided herein, minor variations might be found in the feature set. In case you find any discrepancies, please write to us to support@passwordmanagerpro.com.