Devolutions

Devolutions
Password Hub

TECHNICAL SPECIFICATIONS

OVERVIEW

Managing passwords is becoming a nightmare and an important security challenge for IT departments and organizations worldwide. Privileged access to critical assets are protected using shared passwords, which can easily lead to data breaches and insider attacks if not managed properly. Securing passwords is a complex task that the vast majority of IT pros must address. The challenge resides in finding the thin line between security and accessibility. Privileged passwords for both administrators and users must be secured in an encrypted and hardened vault without compromising user experience.

Devolutions Password Hub can help make all the difference by offering a comprehensive solution not only for IT departments but for entire organizations. Starting with an on-premises encrypted database where company-wide passwords are securely stored, administrators and users can access privileged passwords through our web-based application.

Passwords are brokered to applications on behalf of the user based on his or her individual set of permissions and security rights defined by the admin using our role-based access control. Every entry or action in a session is then logged for complete audit trails and compliance reporting.

SYSTEM REQUIREMENTS

Devolutions Password Hub applications need access to the internet at all times. It is accessible through a web interface, desktop applications, mobile applications and a command-line interface.

Web Interface

- Google
- Firefox
- Opera
- Safari
- Edge

Desktop Applications

- Windows 7 or later
- macOS Yosemite 10.10 or later
- Ubuntu Linux 12.04 or later
- Fedora 21
- Debian 8

Mobile Applications

- Android Marshmallow
- iOS 10

Command-Line Interface

- Windows 7 or later

SECURITY SPECIFICATIONS

Host	Microsoft Azure based on the region the user selected upon creation.
Data Protection	• Sensitive information is encrypted using AES 256 GCM. • Encryption keys protected using Microsoft's Key Vault technology with RSA 4096. • Additional layer of encryption for data at rest using Microsoft's Transparent Data Encryption technology.
Data Transmission	Data in transit over TLS.
Authentication Methods	Devolutions Account • Username/Password • OAuth2 via JWS, with OpenID support
Two-Factor Authentication	On Devolutions Account: • Authenticator – Push on Mobile – Devolutions Authenticator • Authenticator App: - Devolutions Authenticator (Android or iOS) - Google Authenticator - Microsoft Authenticator - Authy • Email • SMS
Access Control	• Role-based permissions on shared vaults • Per user private vault
Monitoring	• Activity logs • Logs and history per entry • Administration logs
Compliance	SOC2 Type-II (in progress, ETA for report is March 2020)

Devolutions | CONTROL THE IT CHAOS

For more information, please visit us at **https://devolutions.net**