



TECHNICAL SPECIFICATIONS

CLOUD-HOSTED PASSWORD MANAGER BUILT FOR IT PROFESSIONALS

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 Hub Business can help make all the difference by offering a comprehensive solution not only for IT departments but for entire organizations. Cloud-base 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 Hub Business applications need access to the internet at all times. It is accessible through a web interface.

Web Interface

- Google
- Firefox
- Opera
- Safari
- Edge

SECURITY SPECIFICATIONS

Host	<p>Microsoft Azure based on the region the user selected upon creation. Regions available :</p> <ul style="list-style-type: none"> • Australia • Canada • Europe • United States
Data Protection	<ul style="list-style-type: none"> • Sensitive information is encrypted using XChaCha20Poly1305. • Additional layer of encryption for data at rest using Microsoft's Transparent Data Encryption technology. • Complete confidentiality with zero-knowledge encryption
Data Transmission	Data in transit over TLS.
Authentication Methods	<p>Devolutions Account</p> <ul style="list-style-type: none"> • Username/Password • OAuth2 via JWS, with OpenID support • Single Sign-On • Microsoft Azure • Okta
Two-Factor Authentication	<p>On Devolutions Account:</p> <ul style="list-style-type: none"> • Authenticator – Push on Mobile – Devolutions Workspace • Authenticator App: <ul style="list-style-type: none"> - Devolutions Workspace (Android or iOS) - Google Authenticator - Microsoft Authenticator - Authy • Email • SMS
Access Control	<ul style="list-style-type: none"> • System Permission • Role-based permissions on shared vaults • Per user vault
Monitoring	<ul style="list-style-type: none"> • Activity logs • Logs and history per entry • Administration logs
Compliance	<p>SOC2 Type-II SOC3 ISO27001:2022 ISO27701:2019</p> <p>(You may find the SOC 2 and the SOC 3 report under the security tab after clicking the following link)</p>