DATASHEET

Privileged Password Manager

Secure shared and privileged credentials with a privileged password safe

Benefits

- Provides compliant management of shared, privileged and critical account passwords
- Delivers individual accountability for shared account access
- Deploys easily as a secure, scalable, purpose-built appliance
- Enables quick addition of users, accounts and systems under management through auto discovery
- Easily expands to include session audit, recording and command control

System requirements

For a complete list of system requirements, visit oneidentity.com/privileged-password-manager

Managing elevated and shared access credentials is one of the biggest challenges facing complex heterogeneous organizations today. Administrators must be able to access the systems they manage with sufficient rights to do their jobs, but organizations must control that access to ensure security and regulatory compliance.

Privileged Password Manager automates, controls and secures the entire process of granting administrators the credentials necessary to perform their duties. Privileged Password Manager is a critical component of One Identity privileged account management solutions and is deployed on a secure, hardened appliance.

Privileged Password Manager ensures that administrative access is granted according to established policy, with appropriate approvals; that all actions are fully audited and tracked; and that the password is changed immediately upon its return.

ONE IDENTITY™

Closing application password holes

One of the most vulnerable – but often overlooked – aspects of IS security is the embedded passwords required for applications to talk to each other or to databases. Often these passwords are hardcoded in scripts, procedures and programs with simple CLI or API calls. Privileged Password Manager replaces hardcoded passwords with programmatic calls that dynamically retrieve account credentials.

Features

Release control – Manages password requests from authorized users, programs and scripts for the accounts they are entitled to access, via a secure web browser connection with support for mobile devices. A password request can be automatically approved or require any level of manual approvals.

Change control – Supports configurable, granular change control of shared credentials, including time-based, last-use-based, and manual or forced change.

Auto discovery of:

- **Accounts and systems –** Instantly discovers new accounts and systems, with optional notifications and automatic enrollment in management.
- **Users –** Automatically provisions users and maps permissions using your LDAP or Microsoft® Active Directory® environment.

Application password support – Replaces hardcoded passwords in scripts, procedures and other programs:

- **Programmatic access –** Includes both a command-line interface (CLI) and an application programming interface (API) with access for C++, Java, .NET and Perl. Connectivity is via SSH with DSS key exchange.
- **Role-based access –** Supports role-based access for the CLI and API. You add a "programmatic" user with either "basic" access or "admin" access. Basic access enables the CLI or API to request account passwords and be granted access for authorized targets or accounts; this is appropriate, for example, for a "requestor." Admin access enables the CLI or API to perform administrative tasks.
- **Optimal performance –** Natively executes approximately 100 call requests per minute. For applications requiring higher performance, an optional cache supports more than 1,000 password requests a second, for your most demanding applications.
- **Extensive command set –** Includes a comprehensive set of commands that can be executed via the CLI or API. Beyond simple "Get Password" commands, the solution supports extensive admin-level commands to provide tight integration with existing enterprise tools and workflows.

Enterprise-ready integration – Integrates with existing directories, ticketing systems and user authentication sources, including Active Directory and LDAP. It also fully supports two-factor authentication through One Identity's Defender™ or other third-party products. A robust CLI/API supports integration with existing workflows and tools, including reviewer notification and escalation workflows.

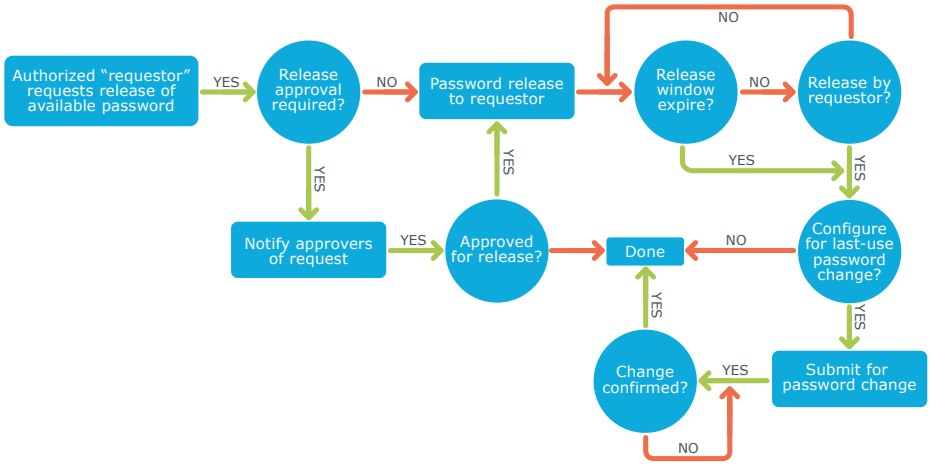
Secure appliance – Lacks a console port or console-level interface – the appliance can only be accessed via a secure, role-based web interface that provides protection from host admin attacks, as well as OS, database or other system-level modifications. It also has an internal firewall that protects against external network-based attacks and provides auditing capabilities.

Scalable appliance – Provides secure, enterprise-ready access and management of shared credentials for more than 250,000 accounts at once.

Secure password storage – Encrypts all passwords stored in Privileged Password Management using AES-256 bit encryption. In addition, the appliance itself also includes full disk encryption using BitLocker™ Drive Encryption.

Robust target support – Manages shared credentials on the widest range of target servers, network devices and applications.

Handheld device support – Supports password request, approval and retrieval via handheld devices, which is configurable on a per-user basis.



With Privileged Password Manager, password request approvals can be fully automated or configured for one or more levels of approvals.

For more information

To learn more about Privileged Password Manager visit oneidentity.com/privileged-password-manager

ONE IDENTITY™