VAULT

Store and Manage Your Passwords and Other Sensitive Data in One Convenient, Secure, Location

What is Vault?

Vault is a “secrets management software” which allows users to secure, store, and manage access to secure passwords, security keys, certificates and other “secrets”, or sensitive data. Users can manage their own Vault instance, and control access to stored secrets for other users and/or applications.

Why do I need Vault?

Vault provides an encrypted secure platform for Children’s Hospital of Philadelphia (CHOP) Research Institute research teams to store multiple passwords, security keys, and other sensitive data as well as delegate specific user/application access. Users can also configure their Vault space in variety of ways, including its web user interface, command line tool, or HTTP API.

Though similar security management software is available, none have the full capabilities of Vault. Vault’s ability to seamless work with multitudes of other systems, putting it at a large advantage over other systems, such as Amazon or Microsoft, which generally only work well with their own products. Edging out its competitors, Vault can also manage Public Key Infrastructure (PKI) certificates, Secure Shell (SSH) keys, dynamic and limited-use secrets, and has built-in support for multiple cloud vendors. When users or applications no longer require access to Vault, permission can be revoked, all in one location.

Within CHOP Research Institute, several research groups, including the Department of Biomedical and Health Informatics, already use Vault to manage and organize their secure passwords and other sensitive data.

How do I get Vault?

As a centralized RIS Service, all CHOP Research Institute faculty, staff, and administrators can utilize Vault. Faculty and staff new to Vault will be provided an individual namespace in Vault for their team. Staff can submit a request for a new Vault namespace or administrative access to an existing Vault namespace through the RIS self-service portal, CIRRUS. Individuals considered owners of a CHOP Research Vault namespace will be responsible for administration of their space, including management of additional user access.

For more information on using Vault, review the User Documentation.

What's an example of Vault in action?

As a researcher, or member of a research team, you likely utilize many databases and applications to collect and analyze data. Rather than storing the account and password credentials for each of these within these databases or applications, Vault can store these credentials securely and provide you and your team with a single access token. This token can be dynamic and generate a new token each time, or it can be a static token and only be made available for a set time period. Also, as the owner of a Vault namespace, you can control who on your team has access to Vault, adding / removing study coordinators, research assistants and other study staff members as needed.

Summary

Vault is a powerful tool for securely storing a variety of sensitive data, including API keys, tokens, passwords, and certificates. It further allows users to control access to this sensitive data, and can be configured to meet the users' needs.

Resources:

- Vault New Namespace Request
- Vault - RIS User Documentation
- Cirrus
- Research Information Services
- RIS Infrastructure Services