Vault Beta

Read about the basics of Vault

Quick View

What it does	Provides secure storage of secrets, cryptographic keys, and authentication tokens. Easily manage, rotate, and revoke secrets, cryptographic keys, and authentication tokens.
Supported Languages	• Node.js SDK • Golang SDK • Python SDK • Java SDK
Capabilities	• Provides secure storage and access of secrets, keys, and tokens • Generate symmetric and asymmetric keys for encryption, signing, and signature verification • Configure and manage rotation policies to stay compliant • Maintain multiple versions of keys for decryption and signature verification • Revoke and rotate keys and tokens immediately in case of emergency • Sign and verify JWT tokens for AuthN

Why use the Vault service?

The Vault service can help you manage keys and secrets, and their rotation policies, ensuring that they're rotated on a schedule consistent with your organization's requirements. Rotation is an important aspect in your application's security in limiting the scope of a breach.

As an example, with Vault's ability to manage Pangea API Tokens, if a token was unknowingly exposed in a public Git repository, but had a short rotation period, it would limit the amount of time that an attacker could use that token before it was deactivated. Additionally, in using the Vault service to manage Pangea API tokens, if a key leak was discovered, the token could immediately be rotated with the current key being deactivated and a new key being provisioned. This would allow the breach to be contained with minimal impact to the operation of your application's functionality.

About Vault

The Vault service helps you manage two critical components of data security:

- Secrets
- Keys

When managed well and in an automated manner, secrets and keys can help you build a strong security management system.

Secrets

Secrets are non-human readable, private digital authentication credentials that grant access to protected information. Proper secrets management is essential to secure your app's data and your users' personal information.

We support the following:

- generating new secrets
- manually rotating a secret and providing a new secret
- revoking a secret
- updating metadata
- retrieving a secret
- setting rotation policies

Tip

It is considered best practice to automate as much of your secret management process as possible. Avoid human errors or hard-coding secrets.

Keys

A key is a string of characters used within an encryption algorithm for altering data so that it appears random. Like a physical key, it locks (encrypts) data so that only someone with the right key can unlock (decrypt) it. Typically, your app will be dealing with keys generated by your providers.

- generating new keys
- storing and managing API keys
- signing a message and/or verify a signature (for asymmetric keys only)
- encrypting/decrypting a message
- manually rotate a key (key bytes can be either user-provided or Pangea-generated)
- revoking keys
- updating metadata
- retrieving keys
- setting rotation policies

Note

If a key is managed, the user can use the key for signing, encrypting, etc, but they can't retrieve the key content.

Metadata

Metadata refers to the information and context you provide about specific keys and/or secrets. Metadata is useful because it provides a summary of basic details about data. This additional context makes discovering and working with data much easier and faster. Metadata can help you organize different types of data, document capabilities, note limitations, and elucidate the relationship between different data types.

For details on adding or updating metadata, visit the pages below:

- Keys - Add or update metadata
- Secrets - Add or update metadata

Rotation Policies

Rotating keys (and other forms of access credentials) is a widely-accepted best practice for excellent data security management - especially automated systems. The Vault service can help you build an automated credential rotation system. Every industry has its own best practices for the time between credential rotation; because of this, Vault allows you to tailor rotation intervals to your exact requirements.

For details on adding or updating rotation policies, visit the pages below:

- Keys - Configure rotation policies
- Secrets - Configure rotation policies

Tip

Your rotation policies will vary according to your unique use case, and security and compliance requirements.

Pangea Token Integration

In addition to helping you manage secrets/keys generated by third-party providers, the Vault service allows you to create and store a Pangea token that can be used to access any enabled Pangea endpoints.

For more details on managing tokens, visit the page below:

- Pangea Token - Create a token
- Pangea Token - Import a token

Was this article helpful? 👍 Yes 👎 No Contact us ↗