



DevOps Secrets Management

Balance speed, agility, and security

Rapid, iterative DevOps workflows often expose many security vulnerabilities directly tied to privilege management. Every container, server, and application can have privileged access – dramatically expanding the attack surface for intruders looking for an entry point. It's challenging to balance high-speed, dynamic DevOps practices and RPA deployments with necessary security policies. Delinea's DevOps Secrets Vault automates secrets management to provide DevOps teams speed and agility to stay productive without sacrificing security. It addresses all scenarios where machines exchange secrets, including databases and applications for software and infrastructure deployment, testing, orchestration, and configuration.

✓ Enable greater agility, ease of use, and reduced overhead

- Manage secrets at the speed and scale of DevOps pipelines and RPA deployments.
- Adopt DevOps and RPA principles securely without the infrastructure burden of provisioning on-premise vault instances.
- Eliminate the risk of disparate vault instances and decrease the cost of ownership with a SaaS solution.
- Issue X.509 and SSH certificates, enabling automated certificate signing and distribution.

✓ Get started rapidly

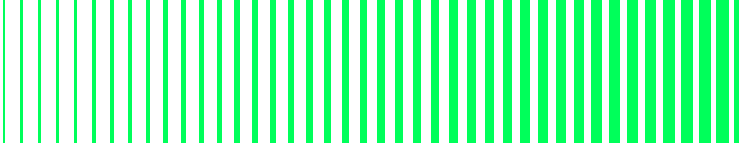
- Cloud-based solution with REST API and command-line interface helps you get started fast.
- Connect to any platform in your DevOps pipeline or RPA deployment.
- Take advantage of infinite scalability.

✓ Maximize the productivity of development, security, and operations teams

- Automate the deprovisioning of secrets when they are no longer needed.
- Minimize privileged account sprawl.
- Allow flexibility with a platform-agnostic solution.
- Eliminate the need to build and maintain your infrastructure.

✓ De-risk operations within dynamic, elastic environments

- Harden attack surface by controlling privileged access.
- Eliminate the need to hard code secrets within code and scripts.
- Provide centralized, unified, auditable management and enforcement of secrets access.
- Remove standing access to critical infrastructure with dynamic secrets.



Embrace modern DevOps seamlessly and securely

DevOps Secrets Vault is a high-velocity vault capable of high-speed secrets creation, archiving, and retrieval. It centralizes management, enforces access controls, and provides automated logging trails. You can minimize privileged account sprawl and harden your attack surface to lower risk without sacrificing productivity.

Establish a Secure DevOps Vault – Store privileged credentials in an encrypted, centralized SaaS-based vault in minutes rather than hours.

Centralize Secrets – Eliminate disparate vault instances with a platform-agnostic solution that enforces secure secrets access and provides complete auditing.

Automate and Scale – Choose your automated interface (CLI and API) built for the speed and scale of DevOps pipelines and RPA deployments and tools.

Manage Secrets – Remove standing access to databases (MySQL, PostgreSQL, and Oracle), as well as cloud platforms (AWS, Azure, and GCP).

Issue Certificates – Issue X.509 and SSH certificates, which enables automated certificate signing and distribution.

```
(3) Pass (Linux only)
(4) Windows Credential Manager (Windows only)
Selection:
Please enter directory for file store (default: /root/.thy):
Please enter cache strategy for secrets:
(1) Never (default)
(2) Server then cache
(3) Cache then server
(4) Cache then server, but allow expired cache if server unreachable
Selection:
Please enter auth type:
(1) Password (default)
(2) Client Credential
(3) AWS IAM (federated)
(4) Azure (federated)
Selection:
Please enter username for password auth: admin
Please enter password for password auth:
Please enter password for password auth (confirm):
root@collector:~/.thyctic# ./thy auth
{
  "accessToken": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhbnNpdjI6ImFkbWVudG9wcm90IiwiaWF0IjoiEjE1MDA4NTAxOTU5In",
  "refreshToken": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhbnNpdjI6ImFkbWVudG9wcm90IiwiaWF0IjoiEjE1MDA4NTAxOTU5In",
  "expiresIn": 3600,
  "granted": "2019-02-11T00:45:13.25872771Z",
  "refreshToken": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhbnNpdjI6ImFkbWVudG9wcm90IiwiaWF0IjoiEjE1MDA4NTAxOTU5In",
  "tokenType": "bearer"
}
root@collector:~/.thyctic# ./thy secret read main
{"attributes": null, "data": {"password": "nothing2"}, "id": "d94a8203-b70f-4a0f-b9ac-e1881b4f04fd", "path": "main"}root@collector:~/.thyctic# ./thy secret read main -b
{
  "attributes": null,
  "data": {
    "password": "nothing2"
  },
  "id": "d94a8203-b70f-4a0f-b9ac-e1881b4f04fd",
  "path": "main"
}
```

Key features

Protect secrets that DevOps teams and RPA tools need to access applications, services, and databases with:

- Advanced automation
- Infinite scalability
- Local caching
- Cloud authentication
- High availability and disaster recovery
- OpenID Connect authentication
- Dynamic secrets for IaaS and databases
- Certificate issuance
- Multi-language and CI/CD tools support
- Integration with PAM and SIEM tools
- Ephemeral credentials with TTL
- Single-use URLs for bootstrapping

Try DevOps Secrets Vault for free at [Delinea.com](https://delinea.com)

Delinea

Delinea is a leading provider of Privileged Access Management (PAM) solutions for the modern, hybrid enterprise. The Delinea Platform seamlessly extends PAM by providing authorization for all identities, controlling access to an organization's most critical hybrid cloud infrastructure and sensitive data to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies. delinea.com