

# SecureVault FAQs

**Document ID:** FAQ-PRD-SV-001 **Last Updated:** March 2024 **Owner:** SecureVault Product Team **Category:** Product - SecureVault

---

## Getting Started

### Q: What is SecureVault?

**A:** SecureVault is NovaTech's enterprise secrets management platform for securely storing, accessing, and managing sensitive data including:  
- API keys and tokens  
- Database credentials  
- Encryption keys  
- Certificates  
- Configuration secrets

---

### Q: How do I access SecureVault?

#### A:

**Web UI:** 1. Go to [app.novatech.com/securevault](http://app.novatech.com/securevault) 2. Log in with SSO 3. Navigate to your team's secrets

#### CLI:

```
# Install CLI
brew install novatech/tap/securevault

# Login
securevault login

# Access secrets
securevault get secret/myapp/db-password
```

#### API:

```
curl -H "Authorization: Bearer $TOKEN" \
      https://api.securevault.novatech.com/v1/secret/data/myapp
```

---

**Q:** What's the difference between secret paths?

**A:**

Path Prefix	Purpose
secret/	General secrets (default)
database/	Dynamic database credentials
aws/	Dynamic AWS credentials
pki/	Certificate management
transit/	Encryption as a service

---

## Secrets Management

**Q:** How do I create a secret?

**A:**

**CLI:**

```
securevault put secret/myapp/api-key value="sk-12345"
```

**Multiple values:**

```
securevault put secret/myapp/database \
  username="admin" \
  password="secret123" \
  host="db.example.com"
```

---

**Q:** How do I retrieve a secret?

**A:**

**CLI:**

```
# Get all fields
securevault get secret/myapp/database

# Get specific field
securevault get secret/myapp/database -field=password
```

**In code (Node.js):**

```
const { SecureVault } = require('@novatech/securevault');

const client = new SecureVault();
const secret = await client.read('secret/data/myapp/database');
console.log(secret.data.password);
```

---

**Q: Can I store files as secrets?**

**A:** Yes, for files up to 1MB:

```
# Store a certificate
securevault put secret/myapp/cert \
  cert=@/path/to/cert.pem \
  key=@/path/to/key.pem
```

For larger files, store in encrypted S3 and keep the key in SecureVault.

---

**Q: How do I update a secret?**

**A:**

```
# Update specific fields (preserves other fields)
securevault patch secret/myapp/database password="newpassword"

# Replace all fields
securevault put secret/myapp/database username="new" password="new"
```

---

**Q: Can I see previous versions of a secret?**

**A:** Yes, SecureVault maintains version history:

```
# List versions
securevault get secret/myapp/database -versions

# Get specific version
securevault get secret/myapp/database -version=3
```

Version history is retained for 30 days (configurable).

---

## Access Control

**Q: How do I grant access to a secret?**

**A:** Use policies to grant access:

```
# Create a policy
securevault policy write myapp-read - <<EOF
path "secret/data/myapp/*" {
    capabilities = ["read", "list"]
}
EOF

# Attach to a user or service account
securevault policy attach myapp-read --entity user@novatech.com
```

---

**Q: What are the available capabilities?**

**A:**

Capability	Description
create	Create new secrets
read	Read secret values
update	Update existing secrets
delete	Delete secrets
list	List secret paths

---

**Q: How do service accounts authenticate?**

**A:** Service accounts use:

**AppRole (recommended):**

```

# Get role ID and secret ID
securevault read auth/approle/role/myapp/role-id
securevault write -f auth/approle/role/myapp/secret-id

# Authenticate
securevault write auth/approle/login \
    role_id="xxx" secret_id="yyy"

```

**Kubernetes:**

```

annotations:
  vault.novatech.com/agent-inject: "true"
  vault.novatech.com/role: "myapp"

```

---

**Q:** Can I require approval for sensitive secrets?

**A:** Yes, enable Control Groups:

```

path "secret/data/production/*" {
  capabilities = ["read"]
  control_group = {
    factor " approvers" {
      identity {
        group_names = ["security-team"]
        approvals = 1
      }
    }
  }
}

```

---

## Secret Rotation

**Q:** How does automatic rotation work?

**A:** SecureVault can automatically rotate secrets:

```

# rotation-config.yaml
rotation:

```

```
- path: secret/myapp/api-key
  interval: 30d
  rotation_policy: generate-new
  notify:
    - myapp-team@novatech.com
```

---

**Q:** How do I rotate database credentials?

**A:** Use dynamic secrets for automatic rotation:

```
# Configure database connection
securevault write database/config/mydb \
  plugin_name=postgresql-database-plugin \
  connection_url="postgresql://{{username}}:{{password}}@db.example.com:5432" \
  allowed_roles="myapp-role"

# Create role
securevault write database/roles/myapp-role \
  db_name=mydb \
  creation_statements="CREATE ROLE \"{{name}}\" WITH LOGIN PASSWORD '{{password}}';" \
  default_ttl="1h" \
  max_ttl="24h"

# Get credentials (new every time)
securevault read database/creds/myapp-role
```

---

**Q:** What happens when a secret rotates while my app is running?

**A:** Use the SecureVault agent for seamless rotation:  
- Agent watches for changes  
- Updates local secret cache  
- Can trigger application reload  
- No downtime required

---

## Integration

**Q:** How do I use SecureVault with Kubernetes?

**A:** Use the SecureVault sidecar injector:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: myapp
spec:
  template:
    metadata:
      annotations:
        vault.novatech.com/agent-inject: "true"
        vault.novatech.com/role: "myapp"
        vault.novatech.com/agent-inject-secret-db: "secret/data/myapp/database"
    spec:
      containers:
        - name: myapp
          env:
            - name: DB_PASSWORD
              valueFrom:
                secretKeyRef:
                  name: db-secret
                  key: password
```

---

**Q:** How do I use SecureVault with DevPipeline?

**A:** Add to your pipeline.yaml:

```
jobs:
  deploy:
    secrets:
      from: securevault
      path: secret/data/deploy
    script:
      - echo "Using token: $DEPLOY_TOKEN"
```

---

**Q:** Is there a Terraform provider?

**A:** Yes:

```
provider "securevault" {
  address = "https://securevault.novatech.com"
```

```
}

data "securevault_generic_secret" "db" {
  path = "secret/data/myapp/database"
}

output "db_host" {
  value = data.securevault_generic_secret.db.data["host"]
}
```

---

## Security

**Q: How are secrets encrypted?**

**A:** SecureVault uses multiple layers of encryption: - **At rest:** AES-256-GCM - **In transit:** TLS 1.3 - **Master key:** Protected by HSM (Enterprise)

---

**Q: Who can see my secrets?**

**A:** Access is controlled by policies: - Only users/services with explicit policy grants - SecureVault admins can manage policies but not read secrets - All access is logged in the audit trail

---

**Q: How do I audit secret access?**

**A:** View audit logs:

```
# CLI
securevault audit list --path secret/myapp

# UI
SecureVault → Audit → Filter by path
```

Logs include: who, what, when, from where.

---

---

**Q: What if SecureVault is unavailable?**

**A:** Best practices: 1. Use the agent with caching enabled 2. Configure response wrapping for initial secrets 3. Multi-region setup for high availability 4. Regular backup testing

---

## Troubleshooting

**Q: “Permission denied” error**

**A:** Check: 1. Your policy includes the path 2. Token hasn’t expired 3. Capability matches operation

Debug:

```
securevault token lookup
securevault token capabilities secret/myapp/database
```

---

**Q: “Secret not found” error**

**A:** Check: 1. Correct path (remember secret/data/ prefix for KV v2) 2. Secret exists: `securevault list secret/myapp` 3. Secret isn’t deleted (check metadata)

---

**Q: Token expired during operation**

**A:** Enable token renewal:

```
# Check token TTL
securevault token lookup

# Renew token
securevault token renew

# Use auto-renewal in applications
```

---

**Q: How do I recover a deleted secret?**

**A:** If soft-delete is enabled:

```
# List deleted secrets
securevault list -deleted secret/metadata/myapp

# Recover
securevault undelete secret/data/myapp/api-key
```

---

## Billing

**Q: How is SecureVault billed?**

**A:**

Component	Unit
Secrets stored	Per secret per month
API requests	Per 10,000 requests
Dynamic secrets	Per generation

Check usage at **Settings → Usage & Billing**.

---

**Q: What's included in each plan?**

**A:**

Feature	Starter	Professional	Enterprise
Secrets	100	10,000	Unlimited
API requests	100K/mo	10M/mo	Unlimited
Dynamic secrets	No	Yes	Yes
HSM	No	No	Yes
Namespaces	No	Yes	Yes

---

## Contact

- **Documentation:** [docs.novatech.com/securevault](https://docs.novatech.com/securevault)
  - **Support:** [support@novatech.com](mailto:support@novatech.com)
  - **Slack:** `#securevault-help`
- 

*Last reviewed: March 2024*