SecureVault Audit Logging Guide

Document ID: PRD-SV-030 **Last Updated:** 2024-02-15 **Owner:** SecureVault Product Team **Classification:** Public

---

Overview

SecureVault provides comprehensive audit logging for all operations. This guide covers how to access, understand, and export audit logs for compliance and security monitoring.

What's Logged

Authentication Events

Event	Description
`auth.login.success`	Successful authentication
`auth.login.failure`	Failed authentication attempt
`auth.logout`	User logout
`auth.token.create`	New token issued
`auth.token.revoke`	Token revoked
`auth.mfa.success`	MFA verification successful
`auth.mfa.failure`	MFA verification failed

Secret Operations

Event	Description
`secret.read`	Secret accessed
`secret.create`	New secret created
`secret.update`	Secret value updated
`secret.delete`	Secret deleted
`secret.list`	Secrets listed
`secret.metadata.read`	Metadata accessed

Policy Operations

Event	Description
`policy.create`	New policy created
`policy.update`	Policy modified
`policy.delete`	Policy removed
`policy.attach`	Policy attached to identity
`policy.detach`	Policy detached

Administrative Operations

Event	Description
`admin.user.create`	User account created
`admin.user.delete`	User account deleted
`admin.user.update`	User account modified
`admin.config.update`	Configuration changed
`admin.seal`	Vault sealed
`admin.unseal`	Vault unsealed

Log Format

Standard Log Entry

```
{
  "timestamp": "2024-02-15T14:30:00.000Z",
  "event_type": "secret.read",
  "event_id": "evt_abc123def456",
  "actor": {
    "type": "user",
    "id": "user_12345",
    "email": "john.doe@example.com",
    "ip_address": "192.168.1.100"
  },
  "resource": {
    "type": "secret",
    "path": "myapp/production/database/password",
    "version": 3
  },
  "result": {
```

```json
    "status": "success",
    "response_time_ms": 12
  },
  "context": {
    "request_id": "req_xyz789",
    "client_version": "1.2.3",
    "auth_method": "approle"
  }
}
```

Log Fields

Field	Description
`timestamp`	ISO 8601 UTC timestamp
`event_type`	Type of operation
`event_id`	Unique event identifier
`actor`	Who performed the action
`resource`	What was accessed/modified
`result`	Outcome of the operation
`context`	Additional context

Accessing Audit Logs

Web UI

1. Go to **Settings → Audit Logs**
2. Use filters to narrow results
3. Click events for details
4. Export as needed

CLI

```bash
# List recent audit events
securevault audit list --limit 100

# Filter by event type
securevault audit list --type secret.read

# Filter by user
securevault audit list --actor-email john@example.com
```

```
# Filter by time range
securevault audit list --from "2024-02-01" --to "2024-02-15"

# Filter by path
securevault audit list --path "myapp/production/*"
```

API

```
# List audit events
curl https://api.securevault.novatech.com/v1/audit/events \
  -H "Authorization: Bearer $TOKEN" \
  -d "limit=100" \
  -d "event_type=secret.read"

# Get specific event
curl https://api.securevault.novatech.com/v1/audit/events/evt_abc123 \
  -H "Authorization: Bearer $TOKEN"
```

Filtering Options

Time Range

```
# Last 24 hours
securevault audit list --since 24h

# Specific date range
securevault audit list --from "2024-02-01T00:00:00Z" --to "2024-02-15T23:59:59Z"

# Last 7 days
securevault audit list --since 7d
```

Event Type

```
# Single event type
securevault audit list --type secret.read

# Multiple event types
securevault audit list --type secret.read,secret.create,secret.update

# All secret events
securevault audit list --type "secret.*"
```

Actor

```
# By email
securevault audit list --actor-email john@example.com

# By user ID
securevault audit list --actor-id user_12345

# By IP address
securevault audit list --actor-ip 192.168.1.100

# By auth method
securevault audit list --auth-method approle
```

Resource

```
# By exact path
securevault audit list --path myapp/production/database/password

# By path prefix
securevault audit list --path-prefix myapp/production/

# By glob pattern
securevault audit list --path "myapp/*/database/*"
```

Result

```
# Only failures
securevault audit list --status failure

# Only successes
securevault audit list --status success
```

Exporting Logs

Manual Export

Via UI: 1. Go to **Settings** → **Audit Logs** 2. Apply desired filters 3. Click **Export** 4. Choose format (JSON, CSV) 5. Download file

Via CLI:

```
# Export to JSON
securevault audit export --format json --output audit.json --since 30d

# Export to CSV
securevault audit export --format csv --output audit.csv --since 30d

# Export specific events
securevault audit export --type secret.read --format json --output reads.json
```

Automated Export

Configure continuous log export to your SIEM:

```
# Export configuration
audit_export:
  enabled: true
  destination:
    type: s3
    bucket: my-audit-logs
    prefix: securevault/
    region: us-west-2
  format: json
  batch_size: 1000
  interval: 5m
```

Supported Destinations

Destination	Configuration
Amazon S3	Bucket, prefix, credentials
Google Cloud Storage	Bucket, prefix, service account
Azure Blob Storage	Container, credentials
Splunk	HEC endpoint, token
Datadog	API key, site
Elasticsearch	Cluster URL, index
Custom webhook	URL, headers

SIEM Integration

Splunk

```
audit_export:
  destination:
    type: splunk
    hec_url: https://splunk.example.com:8088
    hec_token: ${SPLUNK_HEC_TOKEN}
    index: securevault_audit
    source_type: securevault:audit
```

Datadog

```
audit_export:
  destination:
    type: datadog
    api_key: ${DATADOG_API_KEY}
    site: datadoghq.com
    service: securevault
    source: securevault
```

Elasticsearch

```
audit_export:
  destination:
    type: elasticsearch
    url: https://elasticsearch.example.com:9200
    index: securevault-audit
    username: ${ES_USER}
    password: ${ES_PASSWORD}
```

Compliance Reports

Pre-Built Reports

Report	Description	Frequency
Access Summary	Who accessed what	Daily/Weekly
Failed Authentications	Failed login attempts	Daily
Policy Changes	Policy modifications	Daily

Report	Description	Frequency
Admin Actions	Administrative operations	Daily
Secret Lifecycle	Create/update/delete events	Weekly

Generating Reports

Via UI: 1. Go to **Settings** → **Reports** 2. Select report type 3. Choose date range 4. Click **Generate** 5. Download PDF/CSV

Via CLI:

```
# Generate access summary report
securevault report generate access-summary --period last-week --output report.pdf

# Generate compliance report
securevault report generate compliance --standard soc2 --period last-month
```

Scheduled Reports

```
reports:
  - name: weekly-access-summary
    type: access-summary
    schedule: "0 9 * * 1"  # Monday 9 AM
    recipients:
      - security@example.com
    format: pdf

  - name: daily-failed-auth
    type: failed-authentications
    schedule: "0 8 * * *"  # Daily 8 AM
    recipients:
      - security@example.com
    format: csv
```

Alerting on Audit Events

Configuring Alerts

```
audit_alerts:
  - name: multiple-failed-logins
```

```
    condition: |
      event_type == "auth.login.failure"
      AND count(by: actor.id, window: 5m) > 5
    severity: high
    notification:
      - channel: slack
        webhook: ${SLACK_WEBHOOK}
      - channel: pagerduty
        service_key: ${PD_SERVICE_KEY}

  - name: admin-action-outside-hours
    condition: |
      event_type starts_with "admin."
      AND hour(timestamp) NOT BETWEEN 9 AND 17
    severity: medium
    notification:
      - channel: email
        recipients: security@example.com
```

Common Alert Scenarios

Scenario	Condition
Brute force attempt	5+ failed logins in 5 minutes
Unusual access pattern	Access from new IP/location
After-hours admin activity	Admin operations outside business hours
Bulk secret access	100+ secrets read in 1 minute
Policy modification	Any policy change
High-privilege secret access	Access to restricted paths

Retention

Default Retention

Plan	Retention Period
Free	7 days
Team	30 days
Business	90 days
Enterprise	1 year (configurable)

Extended Retention

For compliance requirements: - Export logs to your own storage - Configure longer retention in Enterprise plan - Archive to cold storage after active period

Data Deletion

After retention period: - Logs are permanently deleted - No recovery possible - Export before expiration if needed

---

Best Practices

Security

1. **Export to SIEM** for long-term retention
2. **Set up alerts** for suspicious activity
3. **Review logs regularly** for anomalies
4. **Protect log exports** with encryption

Compliance

1. **Document retention** requirements
2. **Generate regular reports** for auditors
3. **Maintain chain of custody** for exported logs
4. **Test log completeness** periodically

Operations

1. **Monitor log volume** for anomalies
2. **Set up dashboards** for visibility
3. **Define escalation procedures** for alerts
4. **Train team** on log interpretation

Troubleshooting

Missing Logs

- Check time zone settings

- Verify event type filters
- Ensure audit logging is enabled
- Check permissions for log access

Export Failures

- Verify destination credentials
- Check network connectivity
- Review export configuration
- Check destination capacity

Related Documents: Access Control Guide (PRD-SV-010), CLI Reference (PRD-SV-020), SOC 2 Overview (COM-SC-001)