Security Configuration and Required Secrets

This document outlines the required secrets and security configuration for the Audityzer GitHub Actions workflows.

Required Secrets

Core Secrets (Required)

These secrets are automatically provided by GitHub or must be configured in repository settings:

1. **GITHUB_TOKEN** (Automatic)
   - Automatically provided by GitHub Actions
   - Used for: Creating releases, uploading artifacts, GitHub Pages deployment
   - Permissions: `contents: write`, `pages: write`, `security-events: write`

Optional Secrets (For Enhanced Functionality)

1. **NPM_TOKEN** (Optional - for NPM publishing)
   - Purpose: Publishing packages to NPM registry
   - How to get: Create token at https://www.npmjs.com/settings/tokens
   - Required scopes: `Automation` or `Publish`
   - Add to: Repository Settings > Secrets and variables > Actions

2. **SNYK_TOKEN** (Optional - for enhanced security scanning)
   - Purpose: Advanced vulnerability scanning with Snyk
   - How to get: Sign up at https://snyk.io and get API token
   - Add to: Repository Settings > Secrets and variables > Actions

3. **SEMGREP_APP_TOKEN** (Optional - for SAST scanning)
   - Purpose: Static Application Security Testing with Semgrep
   - How to get: Sign up at https://semgrep.dev and get app token
   - Add to: Repository Settings > Secrets and variables > Actions

4. **CODECOV_TOKEN** (Optional - for coverage reporting)
   - Purpose: Upload test coverage reports to Codecov
   - How to get: Connect repository at https://codecov.io
   - Add to: Repository Settings > Secrets and variables > Actions

How to Add Secrets

1. Go to your repository on GitHub
2. Click on **Settings** tab
3. In the left sidebar, click **Secrets and variables** > **Actions**
4. Click **New repository secret**
5. Enter the secret name and value
6. Click **Add secret**

Environment Configuration

GitHub Pages Setup

1. Go to repository **Settings** > **Pages**
2. Set source to **GitHub Actions**
3. The workflows will automatically deploy to:
   - Production: `https://yourusername.github.io/audityzer`
   - Staging: `https://yourusername.github.io/audityzer/staging`

Branch Protection (Recommended)

1. Go to **Settings** > **Branches**
2. Add rule for `main` branch:
   - Require pull request reviews
   - Require status checks to pass
   - Include administrators

Security Best Practices

Workflow Permissions

Our workflows use minimal required permissions:
- `contents: read/write` - For checking out code and creating releases
- `security-events: write` - For uploading security scan results
- `pages: write` - For GitHub Pages deployment
- `packages: write` - For publishing packages

Secret Management

- Never commit secrets to the repository
- Use environment-specific secrets when possible
- Regularly rotate API tokens
- Monitor secret usage in workflow logs

Dependency Security

- Dependabot is enabled for automatic dependency updates
- Security scanning runs on every push and PR
- Weekly scheduled security scans

Troubleshooting

Common Issues

1. **Workflow fails with “startup_failure”**
   - Check YAML syntax in workflow files
   - Verify all required secrets are configured
   - Check repository permissions

2. **NPM publishing fails**
   - Verify NPM_TOKEN is valid and has publish permissions
   - Check package.json version is not already published

3. **Security scans fail**
   - SNYK_TOKEN and SEMGREP_APP_TOKEN are optional
   - Workflows will continue without these tokens (with warnings)

4. **GitHub Pages deployment fails**
   - Ensure Pages is enabled in repository settings
   - Check GITHUB_TOKEN has sufficient permissions

Getting Help

- Check workflow logs in the Actions tab
- Review GitHub Actions documentation
- Check individual action documentation for specific issues

Workflow Status

Current Workflows

- **CI/CD Pipeline** (`ci-cd-clean.yml`) - Build, test, and deploy
- **Security Scanning** (`security-clean.yml`) - CodeQL, dependency scan, SAST
- **Automated Release** (`release-clean.yml`) - Semantic versioning and releases

Monitoring

Monitor workflow status at: `https://github.com/yourusername/audityzer/actions`

Last updated: June 14, 2025