

CI/CD Dashboard Credential Encryption

Recommended guidance

Credential encryption for CI/CD dashboards protects sensitive values used by automation. Treat this page as security-sensitive guidance: never paste real passwords, tokens, keys, or decrypted values into documentation, tickets, chat, or screenshots.

Recommended controls

- Store secrets in approved secret managers or CI/CD credential stores.
- Encrypt values before they are committed or shared with deployment artifacts.
- Limit decryption capability to the runtime or owner that actually needs it.
- Rotate credentials when ownership, access scope, or exposure risk changes.
- Audit who can view, edit, or deploy encrypted dashboard configuration.

Validation checklist

1. Confirm the dashboard can read encrypted values at runtime.
2. Confirm logs do not print decrypted credentials.
3. Test failure behavior when a credential is missing, expired, or revoked.
4. Document rotation and emergency revocation steps.

Last updated: October 6, 2026

Revision #3

Created 2026-07-31 15:38:22 UTC by Admin

Updated 2026-10-06 18:19:16 UTC by mmora