

Configure an S3 Repository in AIQ

Configure an S3 Repository in AIQ

Use an Amazon S3 repository when AIQ needs to read or write test assets, files, evidence, or integration payloads in AWS object storage. Corrected the title spelling and updated the page around current repository and AWS security practices.

Configuration checklist

- Confirm AWS account, region, bucket name, prefix/path, encryption, and lifecycle policy.
- Prefer IAM roles, instance profiles, or temporary credentials over static access keys.
- Grant only the required S3 actions for the specific bucket and prefix.
- Use server-side encryption and customer-approved retention settings.
- Document ownership, cost tags, cleanup policy, and access-review cadence.

Validation workflow

1. Validate read/write access with a small non-sensitive test file.
2. Run the AIQ workflow that uses the S3 repository.
3. Review AWS and AIQ logs for permission, region, bucket, path, or encryption errors.
4. Confirm lifecycle or cleanup rules do not remove required evidence too early.

Last updated: October 9, 2026

Revision #4

Created 2026-07-31 16:29:02 UTC by Admin

Updated 2026-10-10 00:10:54 UTC by mmora