

EC2 Credentials for AIQ Integrations

EC2 Credentials for AIQ Integrations

Use this article when AIQ needs to access AWS EC2 resources. Prefer IAM roles or instance profiles whenever possible, and use static credentials only when the customer security model explicitly requires them.

Security guidance

- Prefer EC2 instance profiles, IAM roles, or temporary credentials over long-lived access keys.
- Use a dedicated integration identity with least-privilege permissions.
- Store secrets in an approved secret store or secured AIQ configuration.
- Do not print access keys, secret keys, or session tokens in output logs.
- Rotate credentials and remove unused access promptly.

Validation workflow

1. Confirm the AWS account, region, and resources AIQ must access.
2. Run a small read-only validation first.
3. Review AWS logs such as CloudTrail to verify the expected actions only.
4. Document owner, purpose, permissions, rotation date, and support contact.

Last updated: October 9, 2026

Revision #4

Created 2026-07-31 16:28:57 UTC by Admin

Updated 2026-10-09 22:38:50 UTC by mmora