

Create an AWS IAM Access Key for AIQ Integrations

Create an AWS IAM Access Key for AIQ Integrations

Create an AWS IAM access key only when an AIQ integration requires programmatic AWS access and a role-based approach is not available. Follow the customer's cloud security policy and use the minimum permissions required.

Security checklist

- Prefer IAM roles, temporary credentials, or workload identity when supported.
- Create keys for a dedicated integration user, not a personal administrator account.
- Attach a least-privilege policy scoped to the required AWS service and resource.
- Store the access key and secret in an approved secret manager or secured AIQ configuration.
- Rotate keys on a defined schedule and remove unused keys immediately.

Validation workflow

1. Test the integration with the minimum required permissions.
2. Confirm logs do not print the access key or secret.
3. Document key owner, purpose, creation date, rotation date, and AWS account.
4. Disable the key if the integration is retired or replaced by a role-based method.

Last updated: October 8, 2026

Revision #3

Created 2026-07-31 16:29:37 UTC by Admin

Updated 2026-10-08 19:28:51 UTC by mmora