

Preferences

- [Preferences](#)
- [Report Templates](#)
- [Git Credentials in AIQ](#)
- [EC2 Credentials for AIQ Integrations](#)

Preferences

Contents:

- [Repositories](#)
- [Report Templates](#)
- [Application Performance Monitoring Integration](#)
- [GIT Credentials](#)
- [EC2 Credentials](#)

Report Templates

The Reports preferences page is used to create report templates.

1. Navigate to AIQ > **Global Options** > **Preferences** > **Reports** tab.

Repository **Reports** APM Integration Git Credentials EC2 Credentials AIQ Credentials

Select Template ▼

Save Cancel

Template Name

☐ Functional Report ☐ Steps Summary ☐ Iteration Summary

☐ Scalability Report ☐ Server Side Only ☐ Server Side Only

☐ Test Case Execution Count ☐ Use milliseconds ☐ Use milliseconds

☐ Test Nodes ☐ Test Case Name ☐ Test Case Name

☐ Failures Report ☐ Step Name ☐ Step Name

☐ Security Report ☐ Request ☐ Request

☐ Resource Correlation ☐ Response Code ☐ Response Code

☐ Success Count ☐ Success Count

☐ Failure ☐ Failure

☐ Total Step ☐ Total Step

☐ Total Request ☐ Total Request

☐ Average Duration ☐ Average Duration

☐ Duration Standard Deviation ☐ Duration Standard Deviation

☐ Minimum Duration ☐ Minimum Duration

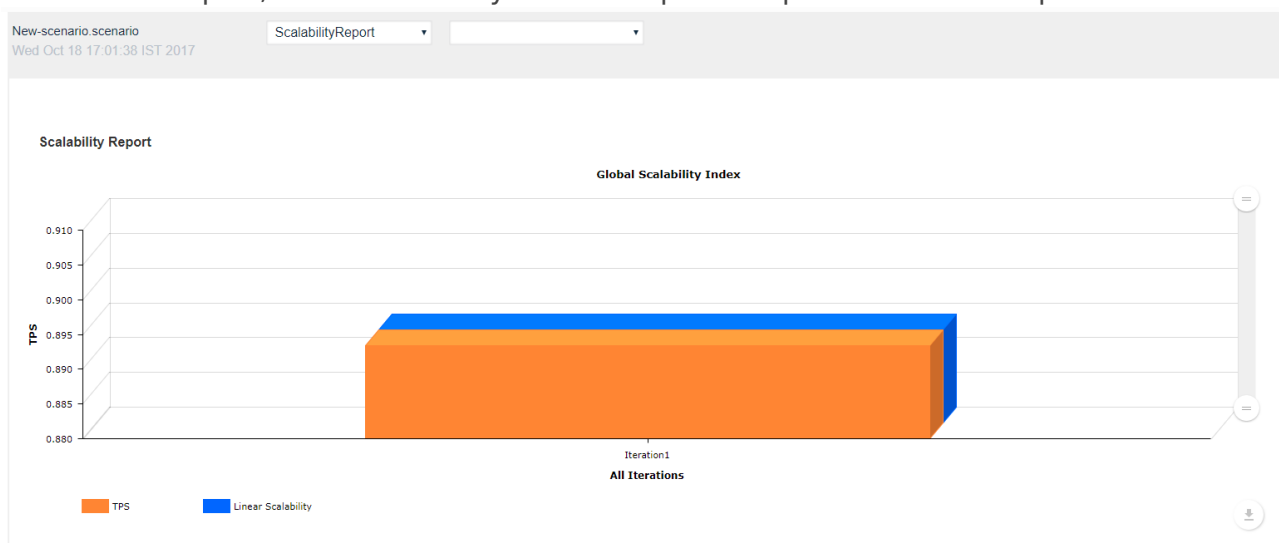
☐ Duration 85 Percentile ☐ Duration 85 Percentile

☐ Duration 90 Percentile ☐ Duration 90 Percentile

☐ Duration 95 Percentile ☐ Duration 95 Percentile

☐ Maximum Duration ☐ Mode Duration

2. Enter a valid name for the new **Report Template**.
3. Select the required report options.
4. Click **Save**.
5. The newly created Report Template can be seen in the All Reports drop down on the Report Analysis page. Navigate to AIQ > Reports.
6. To view the report, select the newly created report template from the drop-down.



See the [About Reports](#) section for more detailed information on reporting in AIQ.

Last updated: July 17, 2023

If you have any feedback on this topic, please contact us at documentation@appvance.ai

Git Credentials in AIQ

Recommended guidance

Use Git credentials in AIQ only for approved repository access. Credentials should be scoped, rotated, and stored through approved mechanisms instead of being copied into scenario steps, documentation, logs, or shared screenshots.

Credential options

- Personal access tokens or service-account tokens approved for automation.
- SSH keys managed by the repository owner or platform team.
- Read-only access when AIQ only needs to pull repository content.
- Write access only when the workflow explicitly requires AIQ to push changes.

Security checklist

1. Confirm the repository, branch, project, and required access level.
2. Use least privilege and avoid broad organization-level access.
3. Document owner, expiration, rotation, and revocation process.
4. Test repository connectivity without exposing the credential value.
5. Remove old credentials when users leave or repository ownership changes.

Last updated: October 6, 2026

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