

Authentication Mechanisms in AIQ Tests

Recommended guidance

Design authentication in AIQ tests so credentials, sessions, tokens, and test accounts are controlled, repeatable, and safe to use. Authentication steps should reflect the application under test and should not expose passwords or tokens in documentation, logs, screenshots, or scenario code.

Common approaches

- UI login through Scenario Editor when the login flow is part of the test objective.
- Service Suite authentication for API tokens, OAuth flows, or setup calls.
- Pre-created test accounts with known permissions and reset procedures.
- Session setup or teardown steps that keep each run independent.

Best practices

1. Use dedicated test accounts instead of personal or production accounts.
2. Store secrets in approved secure locations, not in visible steps or shared notes.
3. Validate multi-factor, SSO, captcha, or conditional-access requirements before automation.
4. Clear sessions when tests must start from a known state.
5. Document account role, environment, and cleanup expectations without revealing credentials.

Last updated: October 6, 2026

Revision #3

Created 2026-07-31 15:40:23 UTC by Admin

Updated 2026-10-06 13:26:03 UTC by mmora