

MFA Authentication Automation Guidance

Last reviewed: September 30, 2026

Use this article to decide how AIQ tests should handle applications protected by multi-factor authentication.

What changed in this article

- Reframed MFA automation around approved test-environment patterns instead of bypassing or weakening MFA.
- Added guidance for test accounts, pre-authorized sessions, API token flows, IdP test policies, and audit requirements.
- Added a warning that real user OTPs, personal devices, and production MFA prompts should not be automated in shared tests.

Validation workflow

1. Confirm the approved MFA strategy with the application owner or identity team before building the scenario.
2. Use a controlled test account, test IdP policy, or token-based flow that is explicitly approved for automation.
3. Record evidence of the authentication path without logging OTPs, recovery codes, personal phone numbers, or secrets.

Review note: This page now treats MFA as a security control to coordinate around, not a popup to defeat.

Last updated: September 30, 2026

If you have feedback on this topic, contact documentation@appvance.ai.

Revision #3

Created 2026-07-31 15:40:30 UTC by Admin

Updated 2026-09-30 17:05:16 UTC by mmora