

Validate CAPTCHA Text Capture in Approved Test Environments

Validate CAPTCHA Text Capture in Approved Test Environments

Use this article only for approved test environments where CAPTCHA images are provided as controlled test fixtures. Do not use AIQ automation to bypass CAPTCHA or defeat anti-bot protections on production systems.

Safe testing approach

- Use a sandbox CAPTCHA, static fixture, or customer-approved test mode.
- Validate OCR or text-extraction behavior only when the CAPTCHA provider and application owner permit it.
- Keep expected values in test data, not in production user flows.
- Record whether the test is validating OCR quality, application handling, or a downstream business rule.
- Use Service Suite or Scenario Editor assertions to verify the expected result without weakening real security controls.

Validation workflow

1. Confirm written approval or documented test-mode support for the CAPTCHA scenario.
2. Run the test with a known fixture and expected extracted value.
3. Validate success and failure behavior separately.
4. Review logs to ensure no real user credentials, session data, or sensitive images are captured.

Security note: CAPTCHA is a security control. This content must not be used as a guide for bypassing CAPTCHA on live systems.

Last updated: October 8, 2026

Revision #3

Created 2026-07-31 15:39:32 UTC by Admin

Updated 2026-10-08 17:22:27 UTC by mmora