

# Automating Multi-Factor Authentication in Scenario Editor

# Automating Multi-Factor Authentication in Scenario Editor

Automate MFA only in approved test environments where the authentication flow is designed for repeatable testing. Do not bypass MFA protections in production or capture real user secrets in scenarios.

## Recommended options

- Use a test-only account with an approved MFA method.
- Prefer test bypass codes, sandbox identity-provider rules, or dedicated automation policies when the customer provides them.
- Store any test tokens or secrets in secured variables, not directly in steps.
- Use Scenario Editor validations to confirm the post-login state instead of relying only on timing.
- Document the identity provider, test account type, and approved MFA handling pattern.

## Validation workflow

1. Confirm that MFA automation is approved for the target environment.
2. Run the login flow once manually and document the expected challenge.
3. Add the Scenario Editor steps using test-safe inputs only.
4. Validate the landing page or authenticated state after MFA completes.
5. Review logs to confirm secrets are not printed.

**Security note:** This article is for authorized test automation only. It must not be used to weaken or bypass MFA for real users.

*Last updated: October 8, 2026*

---

Revision #3

Created 2026-07-31 15:39:50 UTC by Admin

Updated 2026-10-08 17:22:21 UTC by mmora