

Testing checklist: identity and access management service

Source: <https://howtotestaproduct.com/how-to-test/identity-provider/>

Generated: 2026-10-07. Licence: CC BY 4.0.

☐ 1. release smoke tests

Done when: On every build, a test user signs in through SAML and OIDC to a sample app, a wrong password is refused, and sign-out ends the session in the sample app.

Risks: fraud-abuse, data-breach. Tool class: browser automation. Usually run by: QA engineer.

☐ 2. regression suite

Done when: On every release, a wrong password through the directory connector is refused, a session revoked in the admin console no longer opens the sample relying app, recovery still asks for the user's enrolled MFA factor, and any failure blocks the release.

Risks: fraud-abuse, data-breach. Tool class: test management. Usually run by: QA engineer.

☐ 3. penetration testing

Done when: A tester holding a HAR file or copied session cookie from a support ticket cannot reuse it to reach the admin console, and replay from a new device and IP is refused.

Risks: data-breach, fraud-abuse. Tool class: proxy. Usually run by: security specialist.

☐ 4. unit tests

Done when: Credential and cache-key checks refuse a wrong password for usernames of every length in the fixed sample set, including the longest the directory allows.

Risks: fraud-abuse. Tool class: unit framework. Usually run by: developer.

☐ 5. integration tests

Done when: With a directory connector enabled and MFA off for a test app, a sign-in with the right username and a wrong password is refused straight after that user's successful sign-in.

Risks: fraud-abuse. Tool class: API client. Usually run by: developer.

☐ 6. end-to-end functional tests

Done when: Enrolment, step-up MFA, password reset and account recovery each end in the expected state, and recovery never skips the user's enrolled factor.

Risks: fraud-abuse. Tool class: browser automation. Usually run by: QA engineer.

☐ 7. compliance checks

Done when: MFA phone numbers and recovery emails are tagged security-only, no marketing or analytics export includes them, and support uploads are scrubbed of tokens on receipt.

Risks: regulatory-penalty, data-breach. Tool class: test management. Usually run by: product manager.

☐ 8. accessibility testing

Done when: A screen-reader user and a keyboard-only user complete sign-in, MFA enrolment and recovery with a password manager or passkey and without solving a puzzle.

Risks: accessibility-liability. Tool class: accessibility checker. Usually run by: accessibility specialist.

☐ 9. security scanning

Done when: The scan of the admin console, token endpoints and support upload flow has no open high findings.

Risks: data-breach. Tool class: DAST scanner. Usually run by: security specialist.

☐ 10. resilience and failure testing

Done when: With the session store or quota service behind token validation cut in staging, existing sessions stay valid until expiry, new sign-ins show a clear error, and service returns without a manual restart.

Risks: dependency-failure. Tool class: chaos tool. Usually run by: developer.