

Testing checklist: video conferencing tool

Source: <https://howtotestaproduct.com/how-to-test/video-conferencing/>

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

☐ 1. release smoke tests

Done when: On every build, each client installs from the store or notarized build without a warning, two test accounts on different platforms join a passcode meeting, see and hear each other, share a screen, the host ends the meeting for all, and after the desktop client is uninstalled a test web page can no longer start or join a meeting through it.

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

☐ 2. regression suite

Done when: The intruder, recording-access and uninstall cases rerun on every release, and any intruder join blocks the release.

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

☐ 3. penetration testing

Done when: A tester without an invite cannot join a passcode or waiting-room meeting by guessing IDs, and cannot open a cloud recording link without signing in as an allowed user.

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

☐ 4. end-to-end functional tests

Done when: Waiting room, passcode, meeting lock, remove participant and host-only screen share each stop a test intruder account in a scripted meeting.

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

☐ 5. compliance checks

Done when: Every security claim in marketing and in the app (encryption type, recording storage) matches a design document signed by a security specialist, and the release notes name every helper or local service the desktop installer adds.

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

☐ 6. accessibility testing

Done when: A screen-reader user joins, mutes, raises a hand and reads chat by keyboard alone, and live captions appear for a speaking test user.

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

☐ 7. integration tests

Done when: A proxy capture of app open shows no third-party SDK sending device data before the user picks that SDK's feature.

Risks: data-breach. Tool class: proxy. Usually run by: developer.

☐ 8. security scanning

Done when: The scan of client builds and the recording service has no open high findings, and the desktop installer leaves no local web server listening after uninstall.

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

☐ 9. device and browser compatibility

Done when: The current and previous OS versions on iOS, Android, Windows and macOS install the client, pass notarization or store pre-checks, and join the same meeting.

Risks: store-rejection. Tool class: device cloud. Usually run by: QA engineer.