

Enterprise-Managed Chrome Policies for AIQ Testing

Recommended guidance

Enterprise-managed Chrome policies can change how Scenario Editor tests behave. Before changing a scenario, confirm whether Chrome policies control downloads, popups, certificates, extensions, permissions, proxy settings, site isolation, or automatic updates.

Symptoms of policy interference

- Downloads are blocked or saved to an unexpected location.
- Camera, microphone, location, clipboard, or notification prompts behave differently than expected.
- Extensions, certificates, proxy settings, or security warnings cannot be changed by the user.
- Playback differs between a corporate workstation and a clean Test Node.
- Chrome updates occur automatically and change test behavior.

Recommended checks

1. Open Chrome policy information on the affected machine and identify managed settings.
2. Compare the affected machine with a known-good Test Node.
3. Coordinate policy changes with IT instead of bypassing enterprise controls.
4. Document required browser policies for AIQ execution environments.
5. Retest affected scenarios after policy, browser, driver, or Test Node changes.

Important: Do not instruct users to bypass security policies. Work with the customer's IT team to define approved settings for AIQ testing.

Last updated: October 5, 2026

