



Permissions and security

Workflow

Guide for Magento administrators, technical project owners, and implementation teams.

LAST UPDATED
2026-08-25

SOURCE
[Open this article online](#)

Permissions and security

Open **System > Permissions > User Roles**, edit a role and expand the Workflow resources.

Permission	Grants
Manage Workflows	Definition grid, builder and management API access.
Publish Workflows	Publish, archive and restore operations.
Simulate Workflows	Simulation in Admin or through the management API.
View Workflow Run Payloads	Access to stored run payload details.
Advanced Workflow Features	Global Workflow Engine configuration and advanced features.
Operate Workflow Tasks	Task grid, task decisions and task-decision API.
Trigger Workflows via API	API and provider trigger endpoints.

Separate authoring, publishing and task operation for processes that affect orders or customer data. A reviewer who approves a purchase does not automatically need permission to edit or publish its workflow.

Payload privacy

Event and run payloads can contain names, email addresses, order values and internal identifiers. Grant payload viewing only to roles that need it. Redact payloads before sharing diagnostics outside the authorized support path.

Webhook and expression controls

Use a narrow webhook host allowlist. An empty allowlist denies all hosts;  allows all public hosts. Private and unsafe destinations remain subject to runtime protections, but a broad allowlist still enlarges the outbound integration surface.

Limit who can enable expressions, expose additional flat-model prefixes or import definitions. Imported JSON and expressions are executable business configuration and should receive the same review as a code deployment.

Inbound signed webhook triggers depend on a current timestamp and unused nonce. Keep system clocks synchronized and never expose signing secrets in workflow names, exports or screenshots.