Triggers and event payloads

Workflow

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

LAST UPDATED
2026-08-25

SOURCE
Open this article online

Triggers and event payloads

The trigger defines when a published workflow may start and what initial context it receives.

Magento event triggers

The builder catalogue lists registered Magento events by area. Search for the exact event name, select it and confirm the event identifier on the trigger card. Event coverage depends on the installed Magento modules and the events they dispatch.

Mapped events produce a normalized payload. For a customer-save event, the payload includes a customer entity with fields such as customer ID, email, first name, last name and group ID. Sales-order events expose an order entity with fields such as increment ID, state, status, grand total and customer reference.

Do not assume that an arbitrary Magento model field is present in every event payload. Use the trigger's mapped entity fields or inspect a privacy-safe recent run before writing a condition.

Other trigger types

The runtime also supports manual, schedule, API, webhook, provider-event and raw trigger nodes. API and provider triggers have authenticated REST endpoints. Webhook triggers can require a timestamped signature and nonce. Schedule triggers depend on Magento cron.

Choose one trigger that owns the business start. Two published definitions may listen to the same event, but each creates its own independent run.

Payload structure

Magento-mapped events use the following broad structure:

```
{
  "workflow_event": {
    "schema_version": 1,
    "provider": "magento",
    "event_name": "customer_save_after_data_object"
  },
  "event": {
    "name": "customer_save_after_data_object",
    "provider": "magento"
  },
  "entity": {
    "entity_type": "customer",
    "customer_id": 24,
```

```
    "group_id": 2
  },
  "data": {}
}
```

Treat run payloads as business data. Access to payload display is protected by a separate Admin permission, and API credentials should receive only the permissions their integration needs.