Webhook payload and signature

Alerts · https://rulemancer.com/blog/docs/webhook-signature/

Every webhook delivery is a JSON POST with two headers that let your endpoint verify origin and freshness.

Headers

Header	Value
`X-Rulemancer-Timestamp`	Unix time in seconds when the request was built
`X-Rulemancer-Signature`	`sha256=` + HMAC-SHA256 of `timestamp.body` using the endpoint secret
`User-Agent`	`Rulemancer-Webhook/1.0`

Verifying

1. Read the raw body exactly as sent — do not re-serialise JSON.
2. Build the string `timestamp + "." + body`.
3. Compute HMAC-SHA256 with the endpoint secret and compare in constant time.
4. Reject requests whose timestamp is older than a few minutes to block replays.

Payload shape

Each event includes the bot, the pair, the event name and a timestamp; trade events add fill price, quantity and fee. Failures are visible in the webhook log with the HTTP status the endpoint returned, and they never block the bot.

Related reading

Alerts that reach you: Telegram, email and signed webhooks

All documentation · Start free