zendesk developers

API Basics > Best practices

Events security best practices

ON THIS PAGE

Custom events are powerful because they can be emitted from a wide range of sources. However, with great power comes great responsibility. The following practices should be considered when building a partner or custom integration with Zendesk events.

Proxy Events API requests

Interactions with the Events API should never occur directly from your website. The API key for your Zendesk account should never be exposed publicly. We suggest proxying requests to track events from your website via a backend or third party middleware.

Properties should be strictly defined where possible

If you're proxying Events requests via your own backend, the properties of the event should be well-defined. Zendesk recommends locking in the schemas for your event properties when building your integrations, especially if events are tracked against an unauthenticated backend API. This prevents bad actors from forging requests and malicious events making their way into your Zendesk account and presented to agents.

Join our developer community

Forum Blog Slack