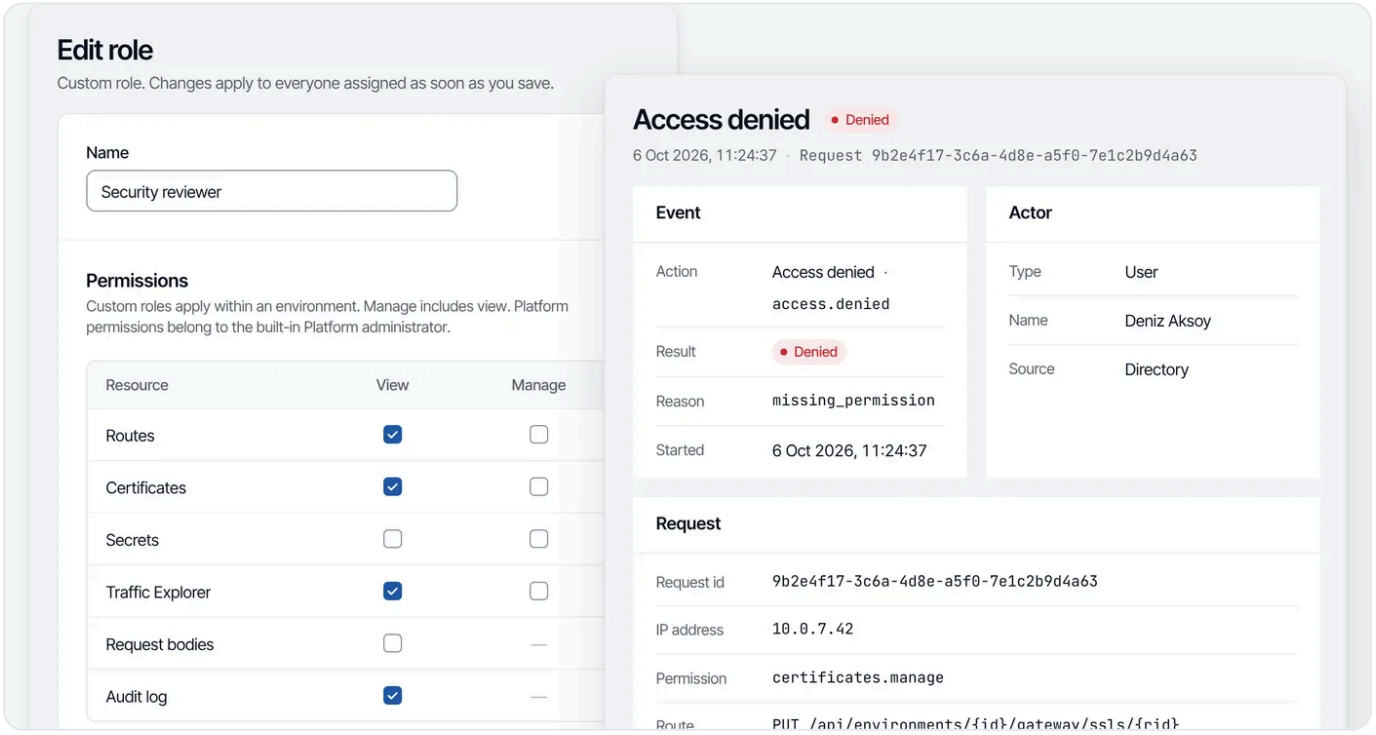
# A control at the gateway for each risk to your APIs

Authentication, access rules, request validation and data masking for every API, with certificates and secrets in the same console and an audit log in which every change is a record. Each control is a plugin with its own form; attach it to a route, a service or a consumer, or apply it to every request in an Environment.

## Five risks, five controls

| | |
|---|---|
| **Unknown callers** | Authentication with OpenID Connect, LDAP, SAML, Keycloak, JWT, API keys, HMAC and mutual TLS, basic authentication or Keycloak authorization; several methods on one Route with multi-auth. |
| **Too many requests** | Limits on requests, request rates and concurrent connections by client, Consumer or a key you choose, with counters shared across gateway nodes. |
| **Unwanted clients** | Allow or deny by IP address or network, by User-Agent and by URI pattern; CORS rules; Routes restricted to named Consumers or groups. |
| **Malformed requests** | Requests that do not match a JSON schema or your OpenAPI document are refused before they reach the backend. |
| **Sensitive data in logs** | Headers, query parameters and body fields you name are masked before a request record is stored; authorization, cookie and API-key headers are masked by default. Viewing a recorded body takes its own permission and is itself written to the audit log. |




A custom role's permission grid, View or Manage per resource, and an attempt it does not allow recorded as Denied with the permission it needed.

## Certificates and secrets

**Certificates**
Server certificates per hostname; client certificates required from the CA you provide, with paths you skip. The console lists every certificate with its expiry and flags the ones close to it.

**Your certificate authority**
Add your organization's CA for every HTTPS connection of an Environment; certificate verification cannot be turned off.

**Secret managers**
Keep secrets in Vault, AWS Secrets Manager or GCP Secret Manager and refer to them from G8; a secret entered in a form is masked in the console, in request records and in the audit log.

## Who may change what

**Console access**
Sign-in with local accounts or Microsoft Active Directory; directory groups map to built-in or custom roles, View or Manage per resource, assigned per Environment. A Viewer sees read-only forms, and a save attempt is refused with 403 and recorded.

**Service accounts**
Tokens for CI/CD hold Environment roles only: gateway configuration, never users, roles or Environments.

**Protected Environments**
A Protected Environment asks for the resource name before a destructive action, and cannot itself be deleted.

## The audit log

Every change is written as an audit record before it is applied; a refused change is a record too. Each record carries the actor, the request id, the IP address and the object before and after, secrets masked on both sides; a change a role forbids is a Denied record, one the engine refuses a Failed record with the engine's reason. Kept 365 days by default in your PostgreSQL, with CSV export and a log line for your SIEM.

## For the security review of the installation

Four pages for your infrastructure and security teams: the G8 Deployment and Security Brief.

| | |
|---|---|
| **Container and profile** | Minimal image, non-root user; OpenShift under the default restricted security profile. |
| **Stored secrets** | Engine admin keys and directory passwords sealed with AES-256-GCM under a key you hold; the server does not start without it; rotation. |
| **What leaves the network** | Nothing leaves your network except the traffic you route to LLM providers. No telemetry, no vendor connection. |

NEXT STEP

Bring your identity provider and one API; we show the controls, the roles and the audit log. Request a demo at g8.dev/request-a-demo or write to hello@g8.dev. Read next: G8 Deployment and Security Brief (4 pages), at g8.dev/downloads.

g8.dev/request-a-demo · hello@g8.dev