Overview

API

Everything the Admin Console does is an API — the console is just a client.

Authentication

Create an **API credential** in the console (**API Credentials** in the left nav): you get a client ID/secret for the OAuth 2.0 **client_credentials** grant. Each credential carries explicit **scopes**, an optional IP allow-list, and an expiry; every use is attributable in the audit log.

```
curl -X POST https://<your-console-host>/api/oauth/token \
  -d grant_type=client_credentials \
  -d client_id=... -d client_secret=... -d scope="audit:read"
```

Typical uses

- Pull audit events into your own tooling (or use the SIEM export).
- Manage policy (MCP rules, detector actions) from infrastructure-as-code.
- Automate provider-key rotation.

Conventions

JSON in/out; standard HTTP statuses; errors carry a human-readable message. Credentials are revocable instantly from the console.

Revision #2
Created 2026-08-01 13:06:32 UTC by Sentilai Docs
Updated 2026-08-05 20:39:05 UTC by Sentilai Docs