## Overview

The Subscription Editor is a built-in web UI for managing metric subscriptions, maintenance windows, anomaly review, reports, and AI-powered discovery. It is available on all tiers at:

`https://<editor-domain>/editor`

The editor is protected by Cognito authentication. On advanced+ tiers, RBAC is enforced via Cognito groups (`admin` = full access, `viewer` = read-only).

**Note**: A landing page has been provided with links to the editor and OpenSearch (`https://<editor-domain>/`).

## Layout

- **Left panel:** Subscription list with status badges, trend indicators, and keyboard navigation (↑↓)
- **Right panel:** Edit form, anomaly viewer, maintenance windows, reports, or discovery wizard
- **Header:** Tier info, timezone selector, navigation buttons (Reload, Anomalies, Maintenance, Reports, ✨ Discover, Versions, Logout)

## Creating a Subscription

1. Click **+** in the left panel header
2. Fill in the required fields (Description, Namespace, Metric Name)
3. Configure dimensions, stat, period, threshold, and direction
4. Click **Save**

On save, the editor validates the configuration server-side and syncs the CloudWatch Metric Stream to include the new namespace.

## Subscription Fields

| Field | Description | Default |
|---|---|---|
| `Description` | Human-readable name (required, must be unique) | — |
| `Namespace` | CloudWatch namespace (e.g. AWS/Lambda, AWS/EC2) | — |
| `Metric Name` | The metric within the namespace. Clear and Preview to see all available. | — |

| | | |
|---|---|---|
| `Account ID` | Blank = local only. * = all accounts. Or select specific accounts. | local |
| `Enabled` | Whether actively collecting and alerting | Yes |
| `Stat` | Aggregation: Average, Sum, Maximum, Minimum, SampleCount, p99/p95/p90 | Average |
| `Dimensions` | JSON object. `{}` = all resources. Use `".*"` for wildcard per-resource monitoring. Select from dropdown or type custom. | {} |
| `Period` | Aggregation period: 60s, 5m, 15m, 1h | 60s |
| `Threshold` | Z-score sensitivity (1.0–10.0). Lower = more sensitive. 3.0 catches top 0.3% outliers. | 3.0 |
| `Baseline (days)` | Training period override. 0 = use tier default. | 0 |
| `Direction` | **High** = only spikes. **Low** = only drops. **Both** = either. | Both |
| `Corr. Window` | Minutes before/after anomaly to search Log Processor for errors | 5 |
| `Retention` | Days to keep anomaly records. 0 = tier default. (advanced+) | 0 |
| `Email` | Send email alerts. "No (silent)" records anomalies without emailing. | Yes |
| `Email threshold` | Only email when score exceeds this. 0 = use anomaly threshold. | 0 |
| `Runbook URL` | Optional URL included in alert emails for quick incident response. | — |

Those on advanced or above tiers will see ✨Tune button, upon clicking AI will suggest some recommendations to tune the subscription.

## Dimensions & Wildcards

Dimensions control which specific resources are monitored:

- `{}` — Monitor the aggregate (all resources combined into one datapoint)
- `{"FunctionName": "my-func"}` — Monitor a specific resource
- `{"FunctionName": ".*"}` — Monitor each resource independently (wildcard). Each matching resource gets its own baseline.

Click the ✨ icon next to the dimensions field to wildcard all dimension keys.

## Preview

The **Preview** button fetches recent metric data to verify the subscription is configured correctly:

| Action | Behavior |
|---|---|
| Click | Query local CloudWatch for last 1 hour |
| `Shift`+Click | Query local CloudWatch for last 24 hours |
| `Ctrl`+Click | Query OpenSearch for last 1 hour (cross-account data) |
| `Ctrl`+`Shift`+Click | Query OpenSearch for last 24 hours |

When multiple dimension combinations exist, Preview shows a table with the latest value for each. The OpenSearch query includes an **Account** column showing which account the data came from.

## Baseline Display

Click **Baseline** to view the learned behavior pattern. Shows a 7-column grid (Mon–Sun) with sparkline charts, mean±stddev bands, and training percentage. Hidden until training exceeds 50%.

## Anomalies Panel

Click **Anomalies** in the header to view recent detections:

- Paginated list with score, description, timestamp

- Detail panel: full metadata, dimensions, CloudWatch console deep link, Metrics Insights query
- AI Explanation (advanced+): natural language analysis of why the anomaly occurred
- Trend indicator: worsening/improving/stable/new
- Dismiss individual or all anomalies

## Maintenance Windows

Click **Maintenance** to suppress alerts during known events:

- **Scheduled:** Recurring on specific days/time (UTC) with duration
- **Ad-hoc:** Starts immediately for a set duration
- Select which subscriptions are affected (default: all)
- Active windows show a green **ACTIVE** badge

## Reports

Click **Reports** to manage anomaly summary reports (advanced+):

- **Generate:** Create an on-demand HTML report with cost analysis
- **Schedule:** Auto-email on selected days with configurable lookback window (1–30 days)
- Download or preview past reports inline

## Discovery Wizard

Click ✨ to open the Discovery panel:

- **Active metrics:** Shows all CloudWatch metrics currently emitting data in your account (refreshed every 6h)
- **Catalog metrics:** Toggle "Show all AWS metrics" to see the full catalog (479 metrics across 57 namespaces)
- **Quick-start chips:** One-click templates for common monitoring patterns (Lambda errors, ALB 5xx, RDS CPU, etc.)
- **AI Suggest (advanced+):** Describe what you want to monitor in natural language. Press Enter or click ✨ Suggest. Bedrock returns a complete subscription configuration.
- **Subscribe button:** Pre-fills the subscription form from the selected metric
- **Refresh ↻:** Triggers a synchronous discovery scan (~30s)

## Version History

Click **Versions** to view the S3 version history of your configuration:

- View timestamps, sizes, and current version indicator
- **Diff:** Compare any version against current (additions in green, removals in red)
- **Restore:** One-click rollback to any previous version (admin only)
- **Download:** Export any version as JSON

## Keyboard Shortcuts

| Key | Context | Action |
|---|---|---|
| ↑ ↓ | Subscription list | Navigate subscriptions |
| ↑ ↓ | Anomaly list | Navigate anomalies (auto-pages) |
| ↑ ↓ | Maintenance list | Navigate windows |
| Double-click | Subscription list | Toggle enabled/disabled |
| Enter | AI prompt | Submit suggestion request |

## SNS Message Attributes

All anomaly alerts include SNS message attributes for filter-based routing:

| Attribute | Type | Description |
|---|---|---|
| `score` | Number | Anomaly score (0–10) |
| `severity` | String | low / medium / high / critical |
| `namespace` | String | CloudWatch namespace |

| | | |
|---|---|---|
| `metricName` | String | Metric name |
| `subscriptionId` | String | Subscription identifier |
| `description` | String | Subscription description |
| `accountId` | String | Source account ID |

Use these to create SNS subscription filter policies for routing specific alerts to Slack, PagerDuty, Lambda, or other targets.

## Tips

- Start with a high threshold (4.0–5.0) and lower it as the baseline matures
- Use **direction: high** for error metrics, **direction: low** for availability metrics
- Wildcard dimensions (`".*"`) create independent baselines per resource — powerful but increases detection cycles
- Use maintenance windows during deployments to avoid false positives
- The **Email threshold** field lets you record all anomalies but only email on high-severity ones
- Clone subscriptions to quickly set up similar monitoring with different thresholds or dimensions