Genesys Authentication Private Edition Guide

Observability in Genesys Authentication

2/1/2026

Contents

Learn about the logs, metrics, and alerts you should monitor for Genesys Authentication.

Related documentation:
-
-
-

RSS:

- For private edition

Monitoring

Private edition services expose metrics that can be scraped by Prometheus, to support monitoring operations and alerting.

- As described on Monitoring overview and approach, you can use a tool like Grafana to create dashboards that query the Prometheus metrics to visualize operational status.

- As described on Customizing Alertmanager configuration, you can configure Alertmanager to send notifications to notification providers such as PagerDuty, to notify you when an alert is triggered because a metric has exceeded a defined threshold.

The services expose a number of Genesys-defined and third-party metrics. The metrics that are defined in third-party software used by private edition services are available for you to use as long as the third-party provider still supports them. For descriptions of available Genesys Authentication metrics, see:

- Authentication Service metrics

- Environment Service metrics

See also System metrics.

Enable monitoring

Service	CRD or annotations?	Port	Endpoint/ Selector	Metrics update interval
Authentication Service	Annotations	8081	/prometheus	Real-time
Environment Service	Annotations	8081	/prometheus	Real-time

Configure metrics

The metrics that are exposed by the Genesys Authentication services are available by default. No further configuration is required in order to define or expose these metrics. You cannot define your own custom metrics.

The Metrics pages linked to above show some of the metrics the Genesys Authentication services expose. You can also query Prometheus directly or via a dashboard to see all the metrics available from the Genesys Authentication services.

Alerting

No alerts are defined for Genesys Authentication.

Logging

Genesys Authentication outputs logs to stdout. You can extract these logs using log collectors such as logstash and Elasticsearch. For more information about logging in private edition, see Logging overview and approaches.

You can set the log level for the Authentication Service and the Environment Service using Helm chart parameters:

- services.auth.env.GWS_AUTH_logging_level_com_genesys_gws_v3
- services.environment.env.GWS_ENVIRONMENT_logging_level_com_genesys_gws_v3