Genesys Authentication Private Edition Guide

Authentication Service metrics and alerts

7/26/2025

Contents

Find the metrics Authentication Service exposes and the alerts defined for Authentication Service.

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

See details about:

- Authentication Service metrics
- Authentication Service alerts

Metrics

Authentication Service exposes many Genesys-defined as well as system metrics. You can query Prometheus directly to see all the available metrics. The metrics documented on this page are likely to be particularly useful. Genesys does not commit to maintain other currently available Authentication Service metrics not documented on this page.

The following system metrics are likely to be most relevant:

- api_requests_seconds_count_total
- api_requests_seconds_sum_total
- jvm_threads_deadlocked
- jvm_gc_pause_seconds_count
- jetty_threads_current
- jvm_memory_used_bytes

Metric and description	Metric details	Indicator of
gws_responses_total The number of responses grouped by HTTP code.	**Unit:** **Type:** Counter **Label:** • Code - The response status code. • Group - The goup of response codes. The values are: 4xx,5xx	

Metric and description	Metric details	Indicator of
	Sample value:	
auth_auth_system_login_errors_total The number of system login errors, excluding expired passwords, incorrect user names and so on.	**Unit:** **Type:** Counter **Label:** • contactCenter – The contact center ID. • environment – The environment ID. **Sample value:**	
psdk_conn_error_total The number of errors that occurred when the Authentication Service connected to Configuration Servers.	**Unit:** **Type:** Counter **Label:** Environment – The environment ID. **Sample value:**	
auth_context_error_total The number of errors during Configuration Server context initialization.	**Unit:** **Type:** Counter **Label:** environment – The environment ID. **Sample value:**	
auth_cs_connection_timeouts_total The number Configuration Server connection timeouts.	**Unit:** **Type:** Counter **Label:** environment – The environment ID. **Sample value:**	
auth_cs_command_timeouts_total The number of Configuration Server command timeouts.	**Unit:** **Type:** Counter **Label:** environment – The environment ID. **Sample value:**	
auth_cs_protocol_errors_total The number of Configuration Server protocol timeouts.	**Unit:** **Type:** Counter **Label:** environment – The environment ID. **Sample value:**	
auth_saml_response_errors The number of Security Assertion Markup Language (SAML) errors.	**Unit:** **Type:** Counter **Label:** contactCenter - The contact center ID. **Sample value:**	

Alerts

The following alerts are defined for Authentication Service.

Alert	Severity	Description	Based on	Threshold
GAUTH-Blue-CPU-Usage	High	A Genesys Authentication pod has CPU usage above 300% during the last 5 minutes.	container_cpu_usage_seconds_total	More than 300% in 5 minutes
GAUTH-Blue-Memory-Usage	High	A Genesys Authentication pod has memory usage above 70% in the last 5 minutes.	container_memory_usage_bytes, container_spec_memory_limit_bytes	More than 70% in 5 minutes
GAUTH-Blue-Pod-NotReady-Count	High	Genesys Authentication has 1 pod ready in the last 5 minutes.	kube_deployment_spec_replicas, kube_deployment_status_replicas_available	1 in 5 minutes
GAUTH-Blue-Pod-Restarts-Count	High	A Genesys Authentication pod has restarted 1 or more times during the last 5 minutes.	kube_pod_container_status_restarts_total	1 or more in 5 minutes
GAUTH-Blue-Memory-Usage-CRITICAL	Critical	A Genesys Authentication pod has memory usage above 90% in the last 5 minutes.	container_memory_usage_bytes	More than 90% in 5 minutes
GAUTH-Blue-Pod-Restarts-Count-CRITICAL	Critical	A Genesys Authentication pod has restarted more than 5 times in the last 5 minutes.	kube_pod_container_status_restarts_total	More than 5 in 5 minutes
GAUTH-Blue-Pods-NotReady-CRITICAL	Critical	Genesys Authentication has 0 pods ready in the last 5 minutes.	kube_deployment_status_replicas_available, kube_deployment_spec_replicas	0 in 5 minutes
auth_jvm_threads_deadlocked	Critical	Deadlocked JVM threads exist.	jvm_threads_deadlocked	0
auth_high_jvm_gc_pause_seconds_count	Critical	JVM garbage collection occurs	jvm_gc_pause_seconds_count	More than 10 in 30 seconds

Alert	Severity	Description	Based on	Threshold
		more than 10 times in the last 30 seconds.		
auth_high_5xx_responses_count	Critical	Genesys Authentication has received more than 10 5xx responses.	gws_responses_total	More than 10
auth_high_500_responses_count	Critical	Genesys Authentication has received more than 10 500 responses.	gws_responses_total	More than 10
auth_auth_login_errors	Critical	Genesys Authentication has received more than 20 login errors for the call center ID in the last 60 seconds.	auth_system_login_errors_total	More than 20 in 60 seconds
auth_total_count_of_errors_in_PSDK_connections	High	Genesys Authentication received more than 3 errors in PSDK connections in the last 30 seconds. A spike might indicate a problem with the backend or a network issue. Check the logs for details.	psdk_conn_error_total	More than 3 in 30 seconds
auth_total_count_of_errors_during_context_initialize	High	Genesys Authentication received more than 10 errors in the last 30 seconds during context initialization. A spike might indicate a network or configuration problem. Check the logs for details.	auth_context_error_total	More than 10 in 30 seconds
auth_saml_response_errors	High	Genesys Authentication received more than 20 SAML errors for the contact center ID in the last 60	auth_saml_response_errors	More than 20 in 60 seconds

Alert	Severity	Description	Based on	Threshold
		seconds.		
auth_saml_timing_errors	High	Genesys Authentication received more than 20 SAML timing errors for the contact center ID in the last 60 seconds.	auth_saml_timing_errors	More than 20 in 60 seconds