This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Genesys Web Engagement

Genesys Configuration Options Current

12/29/2021

Table of Contents

Genesys Web Engagement Options Reference

Welcome to the Options Reference for Genesys Web Engagement. This document describes the configuration options for the following components of Genesys Web Engagement:

Web Engagement Server

Options for this component are contained in the following configuration sections:

- cep
- chat
- engagement
- log
- pacing
- queues
- security
- userData
- webcallback

> **Tip**
>
> In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.
>
> **Power users: Download a CSV file** containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
cep	domainSeparation	false	After start/restart
cep	synchronizeDRLFilesInCluster	true	Immediately
chat	connectionTimeout	5	After start/restart
chat	identifyCreateContact	3	Immediately
chat	queueKey	1:webme	Immediately
chat	refreshPoolSize	10	After start/restart
chat	refreshTaskPeriod	2	After start/restart
chat	requestTimeout	5	After start/restart
chat	sessionRestorationTimeout	30	After start/restart
chat	webengagementChatQueue	Webengagement_Chat	Immediately
engagement	defaultEngagementChannel		Immediately
engagement	engagementExpirationTime	30	Immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
engagement	registrationFormExpirationTime	120	Immediately
engagement	strictEngagementMode	false	Immediately
engagement	userIdentifier	EmailAddress	Immediately
engagement	visitExpirationTime	0	Immediately
log	all	stdout	Immediately
log	compressMethod		Immediately
log	debug	stdout	Immediately
log	outputPattern	%d{HH:mm:ss,SSS}{UTC} [%5p] %-30c{1} - %m %ex%n	Immediately
log	standard	stdout	Immediately
log	trace	stdout	Immediately
log	verbose	standard	Immediately
pacing	algorithm	SUPER_PROGRESSIVE	After start/restart
pacing	chatGroups	Web Engagement Chat	After start/restart
pacing	optimizationGoal	3	After start/restart
pacing	optimizationTarget	ABANDONMENT_RATE	After start/restart
pacing	proactiveRatio	0	After start/restart
pacing	refreshPeriod	5	After start/restart
pacing	voiceGroups		After start/restart
queues	queueAccepted	Webengagement_Accepted	Immediately
queues	queueEngaged	Webengagement_Engaged	Immediately
queues	queueFailed	Webengagement_Failed	Immediately
queues	queueMissed	Webengagement_Missed	Immediately
queues	queueQualified	Webengagement_Qualified	Immediately
queues	queueRejected	Webengagement_Rejected	Immediately
queues	queueTimeout	Webengagement_Timeout	Immediately
security	auth-scheme	none	After start/restart
security	password		After start/restart
security	user-id		After start/restart
userData	eventType.ACTIONABLE		Immediately
userData	keysToPropagate		Immediately
userData	SignIn	timezoneOffset	Immediately
userData	UserInfo	timezoneOffset	Immediately
userData	VisitStarted	timezoneOffset	Immediately
webcallback	phoneNumber	PhoneNumber	Immediately
webcallback	webcallbackQueueSubmit	New	Immediately
Section	**Option**	**Default**	**Changes Take Effect**

Web Engagement Cluster

Options for this component are contained in the following configuration sections:

- cep
- chat
- cluster
- cluster-dispatcher
- cluster-dispatchers
- cometd
- elasticsearch
- engagement
- esArea
- kibana
- log
- metrics
- pacing
- privacy
- queues
- security
- userData
- web
- webcallback

> **Tip**
>
> In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.
>
> **Power users: Download a CSV file** containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
cep	cepSessionCacheSize	10000	After server restart
cep	cepSessionCacheTtl	600	After server restart
cep	domainSeparation	false	After server restart
cep	synchronizeDRLFilesInCluster	true	Immediately
chat	connectionTimeout	10	After server restart
chat	identifyCreateContact	3	Immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
chat	queueKey		After server restart
chat	refreshPoolSize	10	After server restart
chat	refreshTaskPeriod	2	After server restart
chat	requestTimeout	5	After server restart
chat	sessionRestorationTimeout	30	After session restart
chat	webengagementChatQueue		After server restart
cluster	cluster-size	No default value	After restart
cluster-dispatcher	startup-reporting	No default value	After restart
cluster-dispatchers	startup-reporting	No default value	After restart
cometD	heartBeatTimeout	0	Immediately
cometd	interval	0	After server restart
cometd	maxInterval	15	After server restart
cometd	maxSessionsPerBrowser	1	After server restart
cometd	timeout	30	After server restart
cometd	transports	org.cometd.websocket.server.JettyWebSocketTransport, org.cometd.server.transport.JSONTransport, org.cometd.server.transport.JSONPTransport	After server restart
elasticsearch	http-read-only	true	After start or restart
engagement	defaultEngagementChannel		Immediately
engagement	engagementExpirationTime	30	
engagement	registrationFormExpirationTime	120	Immediately
engagement	strategiesControlWebengagementIxn	true	Immediately
engagement	strictEngagementMode	true	Immediately
engagement	userIdentifier	EmailAddress	Immediately
engagement	visitExpirationTime	86400 (24 hours)	Immediately
esArea	name	gpe	After restart
kibana	elasticsearch_url	http://localhost:9200	After start or restart
kibana	enabled	true	After start or restart
kibana	host	localhost	Immediately
kibana	kibana_index	gpe.kibana	Immediately
kibana	port	5601	After start or restart
log	affectedLoggers	The default value is an empty string, which means that there aren't any affected loggers.	Immediately
log	all	stdout	After start/restart
log	debug	stdout	Immediately
log	expire	3	After restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
log	message-format	custom	Immediately
log	outputPattern	%d{HH:mm:ss,SSS}{UTC} [%5p] [%thread] %-30c{2} - %m %ex%n"	Immediately
log	segment	1000	After restart
log	standard	stdout	Immediately
log	suppress-data	true	Immediately
log	time_convert	local	Immediately
log	time_format	time	Immediately
log	trace	stdout	Immediately
log	verbose	standard	Immediately
metrics	EventDuration.threshold	1000	Immediately
metrics	GcFrequency.threshold	24	Immediately
metrics	GcLatency.threshold	1000	Immediately
metrics	HeapMemoryUsage.threshold	0.8	Immediately
metrics	monitoring.event.timer.slidingWindowSize	10	After server restart
metrics	reporter.console.enabled	false	Immediately
metrics	reporter.console.logFrequency	30min	Immediately
metrics	reporter.jmx.enabled	true	Immediately
metrics	reporter.log.enabled	false	Immediately
metrics	reporter.log.logFrequency	30min	Immediately
metrics	reporter.messageServer.enabled	true	Immediately
metrics	reporter.messageServer.logFrequency	30min	Immediately
pacing	algorithm	SUPER_PROGRESSIVE	After server restart
pacing	chatGroups		After start/restart
pacing	interactionMinProcessingTime	20	After server restart
pacing	optimizationGoal	3	After server restart
pacing	optimizationTarget		After server restart
pacing	proactiveRatio	100	After server restart
pacing	refreshPeriod	2	After server restart
pacing	voiceGroups		After server restart
privacy	collectActualIPs	false	After server restart
privacy	collectForwardedIPs	false	After server restart
privacy	geoMode	LOCATION	After server restart
privacy	pathToGeoDB	./gwe/resources/geo/GeoLite2-City.mmdb	After server restart
queues	queueAccepted	Webengagement_Accepted	Immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
queues	queueEngaged	Webengagement_Engaged	Immediately
queues	queueFailed	Webengagement_Failed	Immediately
queues	queueMissed	Webengagement_Missed	Immediately
queues	queueQualified	Webengagement_Qualified	Immediately
queues	queueRejected	Webengagement_Rejected	Immediately
queues	queueTimeout	Webengagement_Timeout	Immediately
security	auth-scheme	none	After server restart
security	certificate		After server restart
security	certificate-key		After server restart
security	key-entry-password	none	After server restart
security	keystore-password	none	After server restart
security	password		After server restart
security	provider	DEFAULT	After server restart
security	trusted-ca		After server restart
security	truststore-password	none	After server restart
security	user-id		After server restart
userData	attach812StyleUserData	true	Immediately
userData	eventName.SignIn		Immediately
userData	eventName.UserInfo		Immediately
userData	eventName.VisitStarted	timezoneOffset	Immediately
userData	eventType.ACTIONABLE	rule	Immediately
userData	keysToPropagate		Immediately
web	cors.allowedHeaders	x-requested-with,content-type,accept,origin,authorization,cookie	After server restart
web	cors.allowedMethods	GET,POST,OPTIONS,HEAD,DELETE	After server restart
web	cors.allowedOrigins	*	After server restart
web	cors.urlMapping	*	After server restart
web	jsonp.whiteList	^_gt\.setCategory$, ^_gt\.setDSL$, ^jQuery\d*_\d*$	After server restart
web	staticResourcesCacheControl	public, max-age=1800	After server restart
web	staticResourcesCacheControlPattern	^(https?://).*$	After restart
webcallback	phoneNumber	PhoneNumber	Immediately
webcallback	webcallbackQueueSubmit	**New**	Immediately
Section	**Option**	**Default**	**Changes Take Effect**

cep Section

cepSessionCacheSize

Default Value: 10000
Valid Values: positive integer greater than 100
Changes Take Effect: After server restart

Defines the size of the cache that is used for storing DRL sessions. This value should be not less than expected maximum count of simultaneous visits on a particular server.

cepSessionCacheTtl

Default Value: 600
Valid Values: positive integer greater than 300
Changes Take Effect: After server restart

Inactivity timeout (in seconds) on the DRL session. After the timeout value is reached, the session is treated as invalid and removed from the cache.

domainSeparation

Default Value: false
Valid Values: true, false
Changes Take Effect: After server restart

Specifies whether the DROOLS knowledge base should be separated by domains and sub-domains.

synchronizeDRLFilesInCluster

Default Value: true

Valid Values: true, false
Changes Take Effect: Immediately

Defines synchronization of the DRL file. If true, the DRL file will be synchronized through the database layer. If false, the DRL file will *not* be synchronized, that is, it will be used as is for each Web Engagement server node.

chat Section

connectionTimeout

Default Value: 10
Valid Values: A positive integer between 1 and 10
Changes Take Effect: After server restart

Specifies the timeout, in seconds, for the connection to Chat Server. After the timeout value is reached, all sessions associated with the lost Chat Server are marked for restoration.

identifyCreateContact

Default Value: 3
Valid Values: 1, 2, or 3
Changes Take Effect: Immediately

Specifies how a contact should be processed in the Contact Server.
Note: This option is applicable for proactive chat sessions only. For reactive chat sessions, you can specify the related parameter in the chat widget. See the createContact API docs for details.

Note: Web Engagement does not work with Contact Server directly, it only passes a parameter value, which has one of the following meanings:

- 1— Do not try to identify this contact and do not try to create it.
- 2—Try to identify this contact, but do not create it if absent.
- 3—Try to identify this contact and create it if absent.

queueKey

Default Value:

Valid Values: Key defined in the **endpoints**:<*tenantID*> section of the Chat Server application.
Changes Take Effect: After server restart

This option is mandatory.

The key in the connected Chat Server that specifies the entry point for the Chat Routing strategy (Interaction Queue). For instance, in the Environment tenant this would be a key defined in the **endpoints:1** section of the Chat Server application.

refreshPoolSize

Default Value: 10
Valid Values: See below
Changes Take Effect: After server restart

Specifies the number of threads used for processing requests to Chat Server.

Valid Values: Any positive integer between 1 and 99.
Use the following formula to calculate the recommended value:
`peak_chat_sessions_count / (refreshPeriod * 5)`
Where:

- `refreshPeriod` is the value of the refreshTaskPeriod option
- `peak_chat_sessions_count` is the maximum number of simultaneous chat sessions planned for one GWE Server

refreshTaskPeriod

Default Value: 2
Valid Values: A positive integer between 1 and 5
Changes Take Effect: After server restart

Specifies how often, in seconds, to refresh the chat content in the chat session.

requestTimeout

Default Value: 5
Valid Values: A positive integer between 1 and 10
Changes Take Effect: After server restart

Specifies the timeout, in seconds, for requests to Chat Server.

sessionRestorationTimeout

Default Value: 30
Valid Values: A positive integer between 5 and 300
Changes Take Effect: After session restart

Specifies the time, in seconds, during which the Web Engagement Server tries to restore a broken chat session. A session can be broken, for example, if Chat Server crashes.

webengagementChatQueue

Default Value:
Valid Values: The name of a valid Interaction Queue
Changes Take Effect: After server restart

This option is mandatory.

The name of the Interaction Queue that is used as the entry point to the Chat Routing strategy. This queue must correspond to the queue specified by the key set in the **queueKey** option.

cluster Section

cluster-size

Default Value: No default value
Valid Values: Any positive integer
Changes Take Effect: After restart
Discontinued: 8.5.100.08

Describes the minimum size of a viable Web Engagement cluster.

This option has a significant impact on the overall status of the Web Engagement cluster. The cluster will not be considered as "started" until a majority of the specified cluster size is reached.

For example, if your cluster consists of three nodes, it will not be switched into a "started" state until at least two Web Engagement servers are up and running.

If this value is not specified, the cluster size is calculated based on the total number of Web Engagement Server applications connected to the current Web Engagement Cluster application.

cluster-dispatchers Section

startup-reporting

Default Value: No default value
Valid Values: reporting-dispatcher:reporting
Changes Take Effect: After restart
Introduced: 8.5.200.02

This option enables cluster dispatcher for GWE reporting.

cometd Section

heartBeatTimeout

Default Value: 0
Valid Values: Any positive integer
Changes Take Effect: Immediately

Maximum number of seconds that the cometD connection can remain inactive before the server considers the client (browser) to be inactive. Note: "Ping" packets are not considered as activity-related.

This option is used when configuring the CometD Activity Extension (see https://docs.cometd.org/current/reference/#_extensions_activity).

interval

Default Value: 0
Valid Values: positive integer
Changes Take Effect: After server restart

The maximum number of seconds that the client must wait between the end of one long poll request and the start of the next. Corresponds to standard CometD **interval** option: http://cometd.org/documentation/cometd-java/server/configuration.

maxInterval

Default Value: 15
Valid Values: positive integer
Changes Take Effect: After server restart

The maximum number of seconds that the server will wait for a new long poll from a client before that client is considered invalid and is removed. Corresponds to the standard CometD **maxInterval**

option: http://cometd.org/documentation/cometd-java/server/configuration.

maxSessionsPerBrowser

Default Value: 1
Valid Values:
Changes Take Effect: After server restart

Maximum count of CometD connections opened per browser connection.

timeout

Default Value: 30
Valid Values: positive integer
Changes Take Effect: After server restart

The maximum number of seconds that the server will wait for a message before responding to a long poll with an empty response. Corresponds to the standard CometD **timeout** option: http://cometd.org/documentation/cometd-java/server/configuration.

transports

Default Value: org.cometd.websocket.server.JettyWebSocketTransport, org.cometd.server.transport.JSONTransport, org.cometd.server.transport.JSONPTransport
Valid Values: comma-separated names of classes which implement CometD transport
Changes Take Effect: After server restart

Comma-separated list of allowed CometD transports. By default, all transports are supported. This option is useful if, for example, you need to to turn off the websocket transport on the server side.

elasticsearch Section

Most of this section is for internal use only. Therefore, you should avoid changing the options in this section, which should be modified only by authorized Genesys representatives, except for the option listed below.

If you need to configure other aspects of Genesys Web Engagement's indexing capabilities, please contact your Genesys representative.

http-read-only

Default Value: true
Valid Values: true, false
Changes Take Effect: After start or restart

Indicates whether Elasticsearch is read only. If you need to import Pulse templates, you must set this option to `false` to make Elasticsearch available for writing.

engagement Section

defaultEngagementChannel

Default Value:
Valid Values: The name of an engagement channel that is known to the Engagement Logic strategy. The valid default values are proactiveChat and proactiveCallback.
Changes Take Effect: Immediately

Specifies the name of the default engagement channel. If specified and not empty, the related channel is selected for engagements by the default Engagement Logic strategy and the results of the pacing algorithm are ignored. Genesys recommends that you only set this option during application development.

engagementExpirationTime

Default Value: 30
Valid Values: positive integer from 10 to 1800
Changes Take Effect:

Specifies the number of seconds during which the **webengagement** interaction is considered to be valid. This time is applicable for the **webengagement** interaction from the time the interaction is created until the moment the engagement invitation is sent to the visitor.

registrationFormExpirationTime

Default Value: 120
Valid Values: positive integer from 10 to 1800
Changes Take Effect: Immediately

Specifies the number of seconds during which an engagement attempt is treated as alive in the state

of "waiting for the form to be completed by the visitor". During this period, new engagement invitations will be blocked if the server is running in **strictEngagementMode**.

strategiesControlWebengagementIxn

Default Value: true
Valid Values: true, false
Changes Take Effect: Immediately

If true, the Web Engagement Server will not apply additional actions to a **webengagement** Open Media interaction, other than submitting it to Interaction Server and updating its **UserData**. In this case, the strategies are responsible for the interaction lifecycle. If false, the Web Engagement Server will be responsible for moving the interaction through the Interaction Queues and, eventually, for stopping the interaction. A value of `false` provides behavior compatible with 8.1.2 strategies.

strictEngagementMode

Default Value: true
Valid Values: true, false
Changes Take Effect: Immediately

If true, instructs the system to allow only one engagement at a time for a particular visit. If false, multiple engagement attempts will be allowed. A value of `true` corresponds to the behavior of GWE 8.1.2.

userIdentifier

Default Value: EmailAddress
Valid Values: A valid **UserData** key
Changes Take Effect: Immediately

Specifies the name of the **UserData** key that is used by Contact Server as the key for the customer identification process.

visitExpirationTime

Default Value: 86400 (24 hours)
Valid Values: nonnegative integer
Changes Take Effect: Immediately

Specifies the number of seconds during which a visit is considered valid. The visit expiration time is checked during each request for categories. A value of `0` means that the visit never expires.

esArea Section

name

Default Value: gpe
Valid Values: String with valid Elasticsearch index name
Changes Take Effect: After restart
Introduced: 8.5.200.02

Specifies the name of the Elasticsearch index to be used for storing GWE-related configuration data.

kibana Section

elasticsearch_url

Default Value: http://localhost:9200
Valid Values: A valid URL that points to the Elasticsearch port
Changes Take Effect: After start or restart

Specifies the location of the Elasticsearch HTTP port. **Note:** The Elasticsearch port is not specified in the default settings for external Cassandra. Because of this, you should use the default value of `9200`. If you need to use a different port for Elasticsearch, use the `-Des.http.port` option to set that value. For more information, refer to Deploy a Cassandra Cluster Node.

enabled

Default Value: true
Valid Values: true, false
Changes Take Effect: After start or restart

Indicates whether the Kibana server is started during GWE Server startup. The Kibana server is used in the Advanced Reporting Dashboard.

host

Default Value: localhost
Valid Values: string
Changes Take Effect: Immediately
Introduced: 8.5.1

Specifies the server where Kibana is hosted.

kibana_index

Default Value: gpe.kibana
Valid Values: string
Changes Take Effect: Immediately
Introduced: 8.5.1

Specifies the index to be used by Kibana.

port

Default Value: 5601
Valid Values: Any positive integer valid for specifying a port ID
Changes Take Effect: After start or restart

Specifies the port on which the Kibana server is listening. Used only if the Kibana server is started.

log Section

affectedLoggers

Default Value: The default value is an empty string, which means that there aren't any affected loggers.
Valid Values: Comma-separated list of logger names, specified in the LOG4J2.xml. For example: com.genesyslab.webme.commons,PROTOCOL,org.apache.cassandra
Changes Take Effect: Immediately

Verbosity settings are explicitly applied for loggers, as specified in the extended description.

Extended Description: Verbosity settings are explicitly applied for the following loggers:

- Loggers that are not declared explicitly in the `log4j2.xml` configuration file.
- Loggers that are specified explicitly in the `log4j2.xml` and are specified in the value for this `affectedLoggers` option.

For other loggers specified in `log4j2.xml`, but not mentioned in the value for this option, the verbosity level is not re-applied.

Here is a use case for when you might need to set this option:

- Cassandra needs to write error messages to a log file, and at the same time, Genesys components also need to write debug messages to the log file.

To resolve this use case, you would:

1. Specify the following logger in `log4j2.xml`: `<logger name="org.apache.cassandra" level="error" additivity="false">`
2. **Do not** include `org.apache.cassandra` in the value for the `affectedLoggers` option.

3. The default `log4j2.xml` file contains the following logger: `<logger name="com.genesyslab.platform" level="info" additivity="false">`
4. Include `com.genesyslab.platform` in the value for the `affectedLoggers` option.
5. Set the verbose option to debug.

In the sample above, the value of `affectedLoggers` should be `com.genesyslab.platform`. Error (but no debug or info) messages from Cassandra will be available in logs, and debug messages from `com.genesyslab.platform` will be available in logs.

all

Default Value: stdout
Valid Values: See table
Changes Take Effect: After start/restart

Specifies the outputs to which an application sends all log events. The log output types must be separated by a comma when more than one output is configured. For example: `all = stdout, logfile`

Valid Values (log output types):

`stdout`	Log events are sent to the Standard output (`stdout`).
`stderr`	Log events are sent to the Standard error output (`stderr`).
`network`	Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database.Setting the `all` log level option to the `network` output enables an application to send log events of the `Standard`, `Interaction`, and `Trace` levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
`memory`	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
`[filename]`	Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

debug

Default Value: stdout
Valid Values: see table
Changes Take Effect: Immediately

Specifies the outputs to which an application sends the log events of the Debug level and higher (that is, log events of the Standard, Interaction, and Trace levels).

The log outputs must be separated by a comma when more than one output is configured. For example: debug = stderr, network.

Valid Values:

stdout	Log events are sent to the Standard output (stdout).
stderr	Log events are sent to the Standard error output (stderr).
network	Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database.
[filename]	Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

expire

Default Value: 3
Valid Values: See table
Changes Take Effect: After restart

Determines whether log files expire. If they do, sets the measurement for determining when they expire, along with the maximum number of files (segments) or days before the files are removed. This option is ignored if log output is not configured to be sent to a log file.

Valid Values:

false	No expiration; all generated segments are stored.
<number> file or <number>	Sets the maximum number of log files to store. Specify a number from 1—1000.
<number> day	Sets the maximum number of days before log files are deleted. Specify a number from 1—100.

message-format

Default Value: custom
Valid Values: custom, full, medium, short
Changes Take Effect: Immediately

Specifies the format of log record headers that an application uses when writing logs in the log file. The value custom assumes that the format is specified in the **outputPattern** option.

outputPattern

Default Value: %d{HH:mm:ss,SSS}{UTC} [%5p] [%thread] %-30c{2} - %m %ex%n"
Valid Values: %d{HH:mm:ss,SSS}{UTC} [%5p] [%thread] %-30c{2} - %m %ex%n
Changes Take Effect: Immediately

Log4j/Log4j2 pattern used to format output messages. Applies when `message-format` is set to `custom`.

segment

Default Value: 1000
Valid Values: See table
Changes Take Effect: After restart

Specifies whether there is a segmentation limit for a log file. If there is, sets the mode of measurement, along with the maximum size. If the current log segment exceeds the size set by this option, the file is closed and a new one is created. This option is ignored if log output is not configured to be sent to a log file.

Valid Values:

`false`	No segmentation is allowed.
`<number> KB or <number>`	Sets the maximum segment size, in kilobytes. The minimum segment size is `100 KB`.
`<number> MB`	Sets the maximum segment size, in megabytes.
`<number> hr`	Sets the number of hours for the segment to stay open. The minimum number is 1 hour.

standard

Default Value: stdout
Valid Values: See table
Changes Take Effect: Immediately

Specifies the outputs to which an application sends the log events of the `Standard` level. The log output types must be separated by a comma when more than one output is configured. For example: `standard = stderr, network`

Valid Values:

`stdout`	Log events are sent to the Standard output (`stdout`).

`stderr`	Log events are sent to the Standard error output (`stderr`).
`network`	Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database.
`memory`	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
`[filename]`	Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

suppress-data

Default Value: true
Valid Values: true, false
Changes Take Effect: Immediately

When enabled, this option masks custom data in logs with asterisks (***). This helps to prevent the exposure of personally-identifiable information in the GWE Server logs.

time_convert

Default Value: local
Valid Values: See table
Changes Take Effect: Immediately

Specifies the system in which an application calculates the log record time when generating a log file. The time is converted from the time in seconds since 00:00:00 UTC, January 1, 1970.

Valid Values:

`local`	The time of log record generation is expressed as a local time, based on the time zone and any seasonal adjustments. Time zone information of the application’s host computer is used.
`utc`	The time of log record generation is expressed as Coordinated Universal Time (UTC).

time_format

Default Value: time
Valid Values: See table
Changes Take Effect: Immediately

Specifies how to represent, in a log file, the time when an application generates log records. A log record's time field in the ISO 8601 format looks like this: `2001-07-24T04:58:10.123`

Valid Values:

`time`	The time string is formatted according to the `HH:MM:SS.sss` (hours, minutes, seconds, and milliseconds) format.
`locale`	The time string is formatted according to the system's locale.
`ISO8601`	The date in the time string is formatted according to the ISO 8601 format. Fractional seconds are given in milliseconds.

trace

Default Value: stdout
Valid Values: See table
Changes Take Effect: Immediately

Specifies the outputs to which an application sends the log events of the `Trace` level and higher (that is, log events of the `Standard`, `Interaction`, and `Trace` levels). The log outputs must be separated by a comma when more than one output is configured. For example: `trace = stderr, network`

Valid Values:

`stdout`	Log events are sent to the Standard output (`stdout`).
`stderr`	Log events are sent to the Standard error output (`stderr`).
`network`	Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database.
`memory`	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
`[filename]`	Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

verbose

Default Value: standard
Valid Values: See table
Changes Take Effect: Immediately

Determines whether a log output is created. If it is, specifies the minimum level of log events generated. The log events levels, starting with the highest priority level, are Standard, Interaction, Trace, and Debug.

Valid Values:

`all`	All log events (that is, log events of the Standard, Trace, Interaction, and Debug levels) are generated.
`debug`	The same as `all`.
`trace`	Log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels) are generated, but log events of the Debug level are not generated.
`interaction`	Log events of the Interaction level and higher (that is, log events of the Standard and Interaction levels) are generated, but log events of the Trace and Debug levels are not generated.
`standard`	Log events of the Standard level are generated, but log events of the Interaction, Trace, and Debug levels are not generated.
`none`	No output is produced.

metrics Section

EventDuration.threshold

Default Value: 1000
Valid Values: The number of milliseconds
Changes Take Effect: Immediately

Defines the average event processing time threshold value in milliseconds.

GcFrequency.threshold

Default Value: 24
Valid Values: A positive numeric value
Changes Take Effect: Immediately

Defines how many times garbage collection can occur within a given hour.

GcLatency.threshold

Default Value: 1000
Valid Values: The number of milliseconds
Changes Take Effect: Immediately

Defines the garbage collection latency threshold value, in milliseconds, in relation to the last time the garbage was collected within the configured time interval.

HeapMemoryUsage.threshold

Default Value: 0.8
Valid Values: A decimal fraction between 0 and 1
Changes Take Effect: Immediately

Defines the heap memory usage threshold value. This is the ratio of used heap memory to the maximum heap memory.

monitoring.event.timer.slidingWindowSize

Default Value: 10
Valid Values: Any positive integer
Changes Take Effect: After server restart

Defines how many of the most recent measurements will be applied when calculating a metric.

reporter.console.enabled

Default Value: false
Valid Values: true, false
Changes Take Effect: Immediately

Enables or disables metrics reporting to the **stdout** console.

reporter.console.logFrequency

Default Value: 30min
Valid Values: An expression containing a positive integer and the units being measured, such as ms, s, min, h, d. For example: 30min, 50s.
Changes Take Effect: Immediately

Defines the reporting frequency for logging to the **stdout** console.

reporter.jmx.enabled

Default Value: true
Valid Values: true, false
Changes Take Effect: Immediately

Enables or disables the JMX reporter.

reporter.log.enabled

Default Value: false
Valid Values: true, false
Changes Take Effect: Immediately

Enables or disables metrics reporting to a file.

reporter.log.logFrequency

Default Value: 30min
Valid Values: An expression containing a positive integer and the units being measured, such as ms, s, min, h, d. For example: 30min, 50s.
Changes Take Effect: Immediately

Defines the reporting frequency for logging to a file.

reporter.messageServer.enabled

Default Value: true
Valid Values: true, false
Changes Take Effect: Immediately

Enables or disables the Message Server reporter.

reporter.messageServer.logFrequency

Default Value: 30min
Valid Values: An expression containing a positive integer and the units being measured, such as ms, s, min, h, d. For example: 30min, 50s.
Changes Take Effect: Immediately

Defines the reporting frequency for the Message Server reporter.

pacing Section

algorithm

Default Value: SUPER_PROGRESSIVE
Valid Values: SUPER_PROGRESSIVE, SUPER_PROGRESSIVE_DUAL, PREDICTIVE_B, PREDICTIVE_B_DUAL
Changes Take Effect: After server restart

This option is mandatory.

Specifies which type of pacing algorithm should be used by the system.

chatGroups

Default Value:
Valid Values: Comma-separated list of group names. Each item should be the valid name of an Agent Group in the Genesys Configuration Layer. For example: `Chat Group 1,Chat Group 2`.
Changes Take Effect: After start/restart

This option is mandatory.

Specifies a list of groups used by the pacing algorithm for predictions on the chat channel.

interactionMinProcessingTime

Default Value: 20
Valid Values: An integer from 5 to 60
Changes Take Effect: After server restart

Specifies the minimum number of seconds during which an interaction should be alive in order to participate in the calculation of inbound reactive traffic.
This option allows the Web Engagement server to prevent the corruption of results provided by dual

pacing algorithms in the presence of low-volume malicious traffic (where visitors continually start chat interactions and then immediately close them without delivering them to an agent).

optimizationGoal

Default Value: 3
Valid Values: An integer from 0 to 100
Changes Take Effect: After server restart

Specifies the percentage goal for the optimization target; the value you set for this option depends on the value you set for the **optimizationTarget** option. **For example:** No more than 3% of Abandoned interactions, or no less than a 75% Busy factor for the agents.

optimizationTarget

Default Value:
Valid Values: `ABANDONMENT_RATE` or `BUSY_FACTOR`
Changes Take Effect: After server restart

This option is mandatory.

Specifies the optimization target for the pacing algorithm.

proactiveRatio

Default Value: 100
Valid Values: An integer from 0 to 100
Changes Take Effect: After server restart

Specifies the minimum percentage of agent resources that are reserved to handle proactive interactions. If `0` is specified, no resources are specifically allocated to handle proactive interactions (note that proactive traffic is still allowed). If `100` is specified, all resources are allocated to handle proactive interactions and no reactive interactions are allowed.

refreshPeriod

Default Value: 2
Valid Values: An integer from 1 to 5
Changes Take Effect: After server restart

Specifies, in seconds, the frequency of predictions produced by the pacing algorithm.

voiceGroups

Default Value:
Valid Values: Comma-separated list of group names. Each item must be the valid name of an Agent Group in the Genesys Configuration Layer.
Changes Take Effect: After server restart

Specifies a comma-separated list of groups used by the pacing algorithm for predictions on the **webcallback** channel.

Note: By default, Web Engagement 8.5 (as opposed to GWE 8.1.2) does not provision the value of the **voiceGroups** option. You must fill in this value manually if you want to use the **webcallback** channel.

For example: `Webcallback Group 1,Webcallback Group 2`.

privacy Section

collectActualIPs

Default Value: false
Valid Values: true, false
Changes Take Effect: After server restart

If true, the IP addresses of visitors will be collected and stored in the database.

collectForwardedIPs

Default Value: false
Valid Values: true, false
Changes Take Effect: After server restart

If true, the IP addresses that the visitor arrived from will be collected and stored in the database.

geoMode

Default Value: LOCATION
Valid Values: OFF, LOCATION
Changes Take Effect: After server restart

The precision of the geolocation service. **Note:** This option will only work if collectActualIPs is enabled.

pathToGeoDB

Default Value: ./gwe/resources/geo/GeoLite2-City.mmdb
Valid Values: Any valid path to a GeoDB file

Changes Take Effect: After server restart

The path to the MaxMind GeoDB file.

queues Section

queueAccepted

Default Value: Webengagement_Accepted
Valid Values: The name of an existing Interaction Queue
Changes Take Effect: Immediately

This option is mandatory.

Specifies the name of the Interaction Queue where the **webengagement** interaction is placed after a visitor accepts an engagement invitation.

queueEngaged

Default Value: Webengagement_Engaged
Valid Values: The name of an existing Interaction Queue
Changes Take Effect: Immediately

This option is mandatory.

Specifies the name of the Interaction Queue where the **webengagement** interaction is placed after a positive engagement decision is made in the Engagement Logic SCXML strategy.

queueFailed

Default Value: Webengagement_Failed
Valid Values: The name of an existing Interaction Queue
Changes Take Effect: Immediately

This option is mandatory.

Specifies the name of the Interaction Queue where the **webengagement** interaction is placed after an error in the strategy or in the Web Engagement Server.

queueMissed

Default Value: Webengagement_Missed
Valid Values: The name of an existing Interaction Queue
Changes Take Effect: Immediately

This option is mandatory.

Specifies the name of the Interaction Queue where the **webengagement** interaction is placed as the result of a negative decision in the Engagement Logic strategy.

queueQualified

Default Value: Webengagement_Qualified
Valid Values: The name of an existing Interaction Queue
Changes Take Effect: Immediately

This option is mandatory.

Specifies the name of the Interaction Queue where the **webengagement** interaction is placed after a HotLead event is triggered by Complex Event Processing on the Web Engagement Server side. This queue is the entry point to the execution of the Engagement Logic strategy.

queueRejected

Default Value: Webengagement_Rejected
Valid Values: The name of an existing Interaction Queue
Changes Take Effect: Immediately

This option is mandatory.

Specifies the name of the Interaction Queue where the **webengagement** interaction is placed after a visitor rejects an engagement invitation.

queueTimeout

Default Value: Webengagement_Timeout
Valid Values: The name of an existing Interaction Queue
Changes Take Effect: Immediately

This option is mandatory.

Specifies the name of the Interaction Queue where the **webengagement** interaction is placed after a visitor's browser sends the Timeout disposition code for the engagement invitation or after the Engagement Logic strategy is finalized by a timeout while waiting for a disposition code.

security Section

auth-scheme

Default Value: none
Valid Values: none, basic
Changes Take Effect: After server restart

Specifies the HTTP authentication scheme used to secure REST requests to the Web Engagement Server.

certificate

Default Value:
Valid Values: A path, which can use both forward and backward slash characters.
Changes Take Effect: After server restart

Specifies the location of an X.509 certificate to be used by application.

certificate-key

Default Value:
Valid Values: A path, which can use both forward and backward slash characters.
Changes Take Effect: After server restart

Specifies the location of a PKCS#8 private key to be used by the application in conjunction with the certificate.

key-entry-password

Default Value: none
Valid Values: String
Changes Take Effect: After server restart

Password for the specific key inside of key storage.

keystore-password

Default Value: none
Valid Values: String
Changes Take Effect: After server restart

Password for the JKS key storage.

password

Default Value:
Valid Values: Any string
Changes Take Effect: After server restart

The password used in the authentication process for REST requests to the Web Engagement Server.

provider

Default Value: DEFAULT
Valid Values: DEFAULT, JKS, MSCAPI, PKCS11, PEM
Changes Take Effect: After server restart

Type of trusted storage. The default provider uses a trust store shipped with the current JDK distribution. It is located at **$JAVA_HOME/jre/lib/security/cacerts**

trusted-ca

Default Value:
Valid Values: A path, which can use both forward and backward slash characters.
Changes Take Effect: After server restart

Specifies the location of an X.509 certificate to be used by the application to validate remote party certificates.

truststore-password

Default Value: none
Valid Values: String
Changes Take Effect: After server restart

Password for the JKS trusted storage.

user-id

Default Value:
Valid Values: Any string
Changes Take Effect: After server restart

The User ID used in the authentication process for REST requests to the Web Engagement Server.

userData Section

attach812StyleUserData

Default Value: true
Valid Values: true, false
Changes Take Effect: Immediately

If true, the Web Engagement Server will attach 8.1.2–style user data to the **webengagement** OM interaction. The following keys will be affected: **jsonEvent**, **ixnType**, **engagements_in_progress**, **engagement_type** and **engagement_attempts**. If false, only Web Engagement 8.5–style data will be added.

eventName.SignIn

Default Value:
Valid Values: Comma-separated list of fields expected in data object of **SignIn** event.
Changes Take Effect: Immediately

A comma-separated list of fields from the data object of a **SignIn** event that belongs to the current session. The value of these fields will be added to the User Data of the **webengagement** Open Media interaction prior to submitting it into the Interaction Queue.

Starting with release 8.5.100.13, the following patterns are supported:

* to describe "all keys"
prefix_* to describe "all keys starting with prefix_"
***_suffix** to describe "all keys ending in _suffix"

eventName.UserInfo

Default Value:
Valid Values: Comma-separated list of fields expected in data object of **UserInfo** event.
Changes Take Effect: Immediately

A comma-separated list of fields from the data object of a **UserInfo** event that belongs to the current session. The value of these fields will be added to the User Data of the **webengagement** Open Media interaction prior to submitting it into the Interaction Queue.

Starting with release 8.5.100.13, the following patterns are supported:

* to describe "all keys"
prefix_* to describe "all keys starting with prefix_"
***_suffix** to describe "all keys ending in _suffix"

eventName.VisitStarted

Default Value: timezoneOffset
Valid Values: Comma-separated list of fields expected in data object of **VisitStarted** event.
Changes Take Effect: Immediately

A comma-separated list of fields from the data object of a **VisitStarted** event. The value of these fields will be added to the User Data of the **webengagement** Open Media interaction prior to submitting it into the Interaction Queue.

Starting with release 8.5.100.13, the following patterns are supported:

* to describe "all keys"
prefix_* to describe "all keys starting with prefix_"
***_suffix** to describe "all keys ending in _suffix"

eventType.ACTIONABLE

Default Value: rule
Valid Values: A comma-separated list of fields expected in the data object of an **ACTIONABLE** event.
Changes Take Effect: Immediately

A comma-separated list of fields expected in the data object of an **ACTIONABLE** event. The value of these fields will be added to the User Data of the **webengagement** Open Media interaction prior to submitting it into the Interaction Queue.

Starting with release 8.5.100.13, the following patterns are supported:

* to describe "all keys"
prefix_* to describe "all keys starting with prefix_"
***_suffix** to describe "all keys ending in _suffix"

keysToPropagate

Default Value:

Valid Values: Comma-separated list of fields expected in the data object of an ACTIONABLE event.
Changes Take Effect: Immediately

A comma-separated list of keys. The specified keys will be copied from the data object of ACTIONABLE event into the userData object of notification message and later attached as UserData of the chat interaction.

Starting with release 8.5.100.13, the following patterns are supported:

* to describe "all keys"
prefix_* to describe "all keys starting with prefix_"
***_suffix** to describe "all keys ending in _suffix"

web Section

cors.allowedHeaders

Default Value: x-requested-with,content-type,accept,origin,authorization,cookie
Valid Values: Comma-separated list of HTTP headers
Changes Take Effect: After server restart

A comma-separated list of HTTP headers that are allowed to be specified when accessing the resources. If the value is a single *, this means that any headers will be accepted.

cors.allowedMethods

Default Value: GET,POST,OPTIONS,HEAD,DELETE
Valid Values: Comma-separated list of valid HTTP methods
Changes Take Effect: After server restart
Introduced: 8.5.000.29

A comma separated list of HTTP methods that are allowed to be specified when accessing the resources.

cors.allowedOrigins

Default Value: *
Valid Values: See the explanation in the description.
Changes Take Effect: After server restart

A comma-separated list of origins that are allowed to access the resources. The default value is *, meaning all origins. If an allowed origin contains one or more * characters (for example `http://*.domain.com`), then * characters are converted to `.*`, `.` characters are escaped to `\.`, and the resulting allowed origin is interpreted as a regular expression. Allowed origins can therefore be more complex expressions such as `https?://*.domain.[a-z]{3}`, which matches either `http` or

`https`, multiple subdomains, and any 3 letter top-level domain, such as `.com`, `.net`, or `.org`.

cors.urlMapping

Default Value: *
Valid Values: Any string that contains a URL mapping parameter that follows the Servlet 3.0 mapping specification (chapter 12.2 Specification of Mappings), as documented at http://download.oracle.com/otn-pub/jcp/servlet-3.0-fr-eval-oth-JSpec/servlet-3_0-final-spec.pdf.
Changes Take Effect: After server restart

Defines a filter mapping with the given URL patterns and dispatcher types for the CORS Filter.

jsonp.whiteList

Default Value: ^_gt\.setCategory$, ^_gt\.setDSL$, ^jQuery\d*_\d*$
Valid Values: A comma-delimited list of regular expressions, each of which specifies the name of one of the allowed callback functions. These names normally have a format of **obj.callback**.
Changes Take Effect: After server restart
Introduced: 8.5.000.42

Defines a white list of regular expressions that specify the object and callback names allowed for JSONP requests.

staticResourcesCacheControl

Default Value: public, max-age=1800
Valid Values: See below
Changes Take Effect: After server restart

Define configuration of cache-control header for static web resources.

Valid Values: Any values that follow the cache-control header specification, such as:

- Deny request caching: `private, no-cache, no-store, max-age=0`
- Allow request caching for 1800 seconds: `public, max-age=1800`

For more information, refer to: http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html and http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html.

staticResourcesCacheControlPattern

Default Value: ^(http)://.*$
Valid Values: ^(http)://.*$
Changes Take Effect: After restart

This regular expression defines the URL pattern of static resources that will be affected by the behavior prescribed by the **staticResourcesCacheControl** option.

The default pattern (^(http)://.*$) indicates "all static resources accessed through the http schema.”

The wildcard (.*) indicates “all static resources.”

webcallback Section

phoneNumber

Default Value: PhoneNumber
Valid Values: A valid **UserData** key
Changes Take Effect: Immediately

Specifies the name of the key that is used by Workspace Desktop Edition to obtain the phone number from the interaction's User Data.

webcallbackQueueSubmit

Default Value: New
Valid Values: The name of an existing Interaction Queue object
Changes Take Effect: Immediately

Specifies the Interaction Queue that is used as the entry point to the **webcallback** routing strategy.

Data Processing Server

Options for this component are contained in the following configuration sections:

- cassandraEmbedded
- spark

> **Tip**
>
> In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.
>
> **Power users: Download a CSV file** containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
cassandraEmbedded	listenAddress		After start or restart
cassandraEmbedded	rpcAddress		After start or restart
spark	startMode	worker	After start or restart
Section	**Option**	**Default**	**Changes Take Effect**

cassandraEmbedded Section

listenAddress

Default Value:
Valid Values: Valid IP address or hostname of the host where the Web Engagement Server is running
Changes Take Effect: After start or restart

This option is mandatory.

The IP address or hostname that Cassandra binds to for connecting to other Cassandra nodes.

rpcAddress

Default Value:
Valid Values: Valid IP address or hostname of the host where the Web Engagement Server is running
Changes Take Effect: After start or restart

This option is mandatory.

The listen address for thrift client connections.

spark Section

startMode

Default Value: worker
Valid Values: off, worker, or both
Changes Take Effect: After start or restart

The mode that will be used when starting Spark. If set to `off`, Spark will not be started by Data Processing Server, and will instead have its state managed externally. If set to `worker`, only a worker node will be started. If set to `both`, both a worker node and a master node are started. **Note:** Genesys recommends that you set this option for each node to clearly specify the role. However, you can set the Cluster object to `worker` mode and override that value for the master node by setting that node to `both`.

Data Processing Cluster

Options for this component are contained in the following configuration sections:

- cassandraEmbedded
- cassandraKeyspace
- log
- spark

> **Tip**
>
> In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.
>
> **Power users: Download a CSV file** containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
cassandraEmbedded	authenticator	AllowAllAuthenticator	After start or restart
cassandraEmbedded	authorizer	AllowAllAuthorizer	After start or restart
cassandraEmbedded	clusterName	Cluster	After start or restart
cassandraEmbedded	commitLogDirectory	./storage/commitlog	After start or restart
cassandraEmbedded	commitLogSync	periodic	After start or restart
cassandraEmbedded	commitLogSyncPeriod	10000	After start or restart
cassandraEmbedded	configFile		After start or restart
cassandraEmbedded	dataDirectory	./storage/data	After start or restart
cassandraEmbedded	enabled	true	After start or restart
cassandraEmbedded	encryption.client.clientAuth	false	After start or restart
cassandraEmbedded	encryption.client.enabled	false	After start or restart
cassandraEmbedded	encryption.client.keystore	conf/.keystore	After start or restart
cassandraEmbedded	encryption.client.keystorePassword	cassandra	After start or restart
cassandraEmbedded	encryption.client.truststore	conf/.truststore	After start or restart
cassandraEmbedded	encryption.client.truststorePassword	*truststore_password*	After start or restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
cassandraEmbedded	encryption.server.clientAuth	false	After start or restart
cassandraEmbedded	encryption.server.internode	none	After start or restart
cassandraEmbedded	encryption.server.keystore	conf/.keystore	After start or restart
cassandraEmbedded	encryption.server.keystorePassword	cassandra	After start or restart
cassandraEmbedded	encryption.server.truststore	conf/.truststore	After start or restart
cassandraEmbedded	encryption.server.truststorePassword	cassandra	After start or restart
cassandraEmbedded	endpointSnitch	GossipingPropertyFileSnitch	After start or restart
cassandraEmbedded	nativeTransportPort	9042	After start or restart
cassandraEmbedded	numTokens	256	After start or restart
cassandraEmbedded	partitioner	org.apache.cassandra.dht.Murmur3Partitioner	After start or restart
cassandraEmbedded	readTimeout	5000	After start or restart
cassandraEmbedded	rpcPort	9160	After start or restart
cassandraEmbedded	savedCachesDirectory	./storage/saved_caches	After start or restart
cassandraEmbedded	seedNodes		After start or restart
cassandraEmbedded	sslStoragePort	7001	After start or restart
cassandraEmbedded	storagePort	7000	After start or restart
cassandraEmbedded	writeTimeout	2000	After start or restart
cassandraKeyspace	dataCompression	LZ4	After start or restart
cassandraKeyspace	name	none	After start or restart
cassandraKeyspace	password		After start or restart
cassandraKeyspace	readConsistencyLevel	LOCAL_QUORUM	After start or restart
cassandraKeyspace	replicationStrategy	NetworkTopologyStrategy	After start or restart
cassandraKeyspace	replicationStrategyParams	'OperationalDC':1	After start or restart
cassandraKeyspace	retention.entity.all	0 seconds (8.5.1 and later); 15 (8.5.0)	After start or restart
cassandraKeyspace	retention.entity.<object>	0 seconds (8.5.1); none (8.5.0)	After start or restart
cassandraKeyspace	retention.time-unit	day	After start or restart
cassandraKeyspace	transportCompression	NONE	After start or restart
cassandraKeyspace	userName		After start or restart
cassandraKeyspace	writeConsistencyLevel	LOCAL_QUORUM	After start or restart
log	affectedLoggers	The default value is an empty string, which means that there aren't any affected loggers.	Immediately
log	all	stdout	After start/restart
log	expire	3	After restart
log	segment	1000	After restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
log	standard	stdout	Immediately
log	time_convert	local	Immediately
log	time_format	time	Immediately
log	trace	stdout	Immediately
log	verbose	standard	Immediately
spark	executorMemory	None	After start or restart
spark	host	None	After start or restart
spark	masterWebPort	8080	After start or restart
spark	port	7077	After start or restart
spark	sparkHeartbeatTimeout	60	After start or restart
spark	sparkStartTimeout	20	After start or restart
spark	startMode	worker	After start or restart
spark	uri	None	After start or restart
spark	workerWebPort	8081	After start or restart
Section	**Option**	**Default**	**Changes Take Effect**

cassandraEmbedded Section

authenticator

Default Value: AllowAllAuthenticator
Valid Values: AllowAllAuthenticator, PasswordAuthenticator
Changes Take Effect: After start or restart

The authentication backend, as described at http://docs.datastax.com/en/cassandra/2.1/cassandra/security/secure_about_native_authenticate_c.html.

authorizer

Default Value: AllowAllAuthorizer
Valid Values: AllowAllAuthorizer, CassandraAuthorizer
Changes Take Effect: After start or restart

The authorization backend, as described at http://docs.datastax.com/en/cassandra/2.1/cassandra/security/secure_about_native_authorize_c.html.

clusterName

Default Value: Cluster
Valid Values: Valid string
Changes Take Effect: After start or restart

The name of the cluster. This setting prevents nodes in one logical cluster from joining another. All nodes in a cluster must have the same value.

commitLogDirectory

Default Value: ./storage/commitlog
Valid Values: Valid folder path
Changes Take Effect: After start or restart

The directory where the commit log is stored.

commitLogSync

Default Value: periodic
Valid Values: periodic, batch
Changes Take Effect: After start or restart

The method that Cassandra uses to acknowledge writes, as described at http://docs.datastax.com/en/cassandra/2.1/cassandra/dml/dml_durability_c.html.

commitLogSyncPeriod

Default Value: 10000
Valid Values: Valid integer
Changes Take Effect: After start or restart

The period that Cassandra uses to acknowledge writes (in milliseconds).

configFile

Default Value:
Valid Values: Valid YAML file path
Changes Take Effect: After start or restart

Embedded Cassandra external configuration YAML file path. Overrides all Cassandra settings.

dataDirectory

Default Value: ./storage/data
Valid Values: Valid folder path
Changes Take Effect: After start or restart

The directory location where table data (SSTables) is stored. Cassandra distributes data evenly across the location, subject to the granularity of the configured compaction strategy.

enabled

Default Value: true
Valid Values: true, false
Changes Take Effect: After start or restart

Indicates whether the Embedded Cassandra service is enabled.

encryption.client.clientAuth

Default Value: false
Valid Values: true, false
Changes Take Effect: After start or restart

Enables or disables certificate authentication.

encryption.client.enabled

Default Value: false
Valid Values: true, false
Changes Take Effect: After start or restart

Enables or disables client-to-node encryption. You must also generate keys and provide the appropriate key and trust store locations and passwords. No custom encryption options are currently enabled, as described at http://docs.datastax.com/en/cassandra/2.1/cassandra/security/secureSSLClientToNode_t.html.

encryption.client.keystore

Default Value: conf/.keystore
Valid Values: Valid path
Changes Take Effect: After start or restart

The location of a client-side Java keystore (JKS) suitable for use with Java Secure Socket Extension (JSSE), which is the Java version of the Secure Sockets Layer (SSL), and Transport Layer Security (TLS) protocols. The keystore contains the private key used to encrypt outgoing messages.

encryption.client.keystorePassword

Default Value: cassandra
Valid Values: Valid string
Changes Take Effect: After start or restart

Password for the client-side keystore. This must match the password used when generating the keystore and truststore.

encryption.client.truststore

Default Value: conf/.truststore
Valid Values: Valid path
Changes Take Effect: After start or restart

Set if **encryption.client.clientAuth** is true.

encryption.client.truststorePassword

Default Value: *truststore_password*
Valid Values: Valid string
Changes Take Effect: After start or restart

Set if **encryption.client.clientAuth** is true.

encryption.server.clientAuth

Default Value: false
Valid Values: true, false
Changes Take Effect: After start or restart

Enables or disables certificate authentication.

encryption.server.internode

Default Value: none
Valid Values: none, all, dc, rack
Changes Take Effect: After start or restart

Enables or disables inter-node encryption. You must also generate keys and provide the appropriate key and trust store locations and passwords. No custom encryption options are currently enabled, as described at http://docs.datastax.com/en/cassandra/2.1/cassandra/security/secureSSLNodeToNode_t.html.

encryption.server.keystore

Default Value: conf/.keystore
Valid Values: Valid path
Changes Take Effect: After start or restart

The location of a server-side Java keystore (JKS) suitable for use with Java Secure Socket Extension (JSSE), which is the Java version of the Secure Sockets Layer (SSL), and Transport Layer Security (TLS) protocols. The keystore contains the private key used to encrypt outgoing messages.

encryption.server.keystorePassword

Default Value: cassandra
Valid Values: Valid string
Changes Take Effect: After start or restart

Password for the server-side keystore.

encryption.server.truststore

Default Value: conf/.truststore
Valid Values: Valid path
Changes Take Effect: After start or restart

Location of the truststore containing the trusted certificate for authenticating remote servers.

encryption.server.truststorePassword

Default Value: cassandra
Valid Values: Valid string
Changes Take Effect: After start or restart

Password for the truststore.

endpointSnitch

Default Value: GossipingPropertyFileSnitch
Valid Values: SimpleSnitch, GossipingPropertyFileSnitch, PropertyFileSnitch, Ec2Snitch, Ec2MultiRegionSnitch, RackInferringSnitch
Changes Take Effect: After start or restart

A snitch determines which data centers and racks nodes belong to. They inform Cassandra about the network topology so that requests are routed efficiently. They also allow Cassandra to distribute replicas by grouping machines into data centers and racks. Specifically, the replication strategy places the replicas based on the information provided by the new snitch as described at http://docs.datastax.com/en/cassandra/2.1/cassandra/architecture/architectureSnitchesAbout_c.html.

nativeTransportPort

Default Value: 9042
Valid Values: Valid port number
Changes Take Effect: After start or restart

Port on which the CQL native transport listens for clients.

numTokens

Default Value: 256
Valid Values: Valid integer
Changes Take Effect: After start or restart

Defines the number of tokens randomly assigned to this node on the ring when using virtual nodes (vnodes). The more tokens, relative to other nodes, the larger the proportion of data that the node stores.

partitioner

Default Value: org.apache.cassandra.dht.Murmur3Partitioner
Valid Values: org.apache.cassandra.dht.RandomPartitioner, org.apache.cassandra.dht.RandomPartitioner, org.apache.cassandra.dht.Murmur3Partitioner
Changes Take Effect: After start or restart

A partitioner determines how data is distributed across the nodes in the cluster (including replicas). Basically, a partitioner is a function for deriving a token representing a row from its partition key, typically by hashing. Each row of data is then distributed across the cluster by the value of the token, as described at http://docs.datastax.com/en/cassandra/2.1/cassandra/architecture/architecturePartitionerAbout_c.html.

readTimeout

Default Value: 5000
Valid Values: Valid long
Changes Take Effect: After start or restart

The time (in milliseconds) that the coordinator waits for read operations to complete.

rpcPort

Default Value: 9160
Valid Values: Valid port number
Changes Take Effect: After start or restart

Thrift port for client connections.

savedCachesDirectory

Default Value: ./storage/saved_caches
Valid Values: Valid folder path
Changes Take Effect: After start or restart

The directory location where table key and row caches are stored.

seedNodes

Default Value:
Valid Values: A single or comma-delimited list of IP addresses
Changes Take Effect: After start or restart

A comma-delimited list of IP addresses used by gossip for bootstrapping new nodes joining a cluster. In multiple data-center clusters, the seed list should include at least one node from each data center (replication group). More than a single seed node per data center is recommended for fault tolerance. Otherwise, gossip has to communicate with another data center when bootstrapping a node. Making every node a seed node is **not** recommended because of increased maintenance and reduced gossip performance. Gossip optimization is not critical, but Genesys recommends that you use a small seed list. For more information, refer to https://docs.datastax.com/en/cassandra/2.0/cassandra/architecture/architectureGossipAbout_c.html.

sslStoragePort

Default Value: 7001
Valid Values: Valid port number

Changes Take Effect: After start or restart

The SSL port for encrypted communication. Not used unless enabled in the **encryption.server.internode** option.

storagePort

Default Value: 7000
Valid Values: Valid port number
Changes Take Effect: After start or restart

The port for inter-node communication.

writeTimeout

Default Value: 2000
Valid Values: Valid long
Changes Take Effect: After start or restart

The time (in milliseconds) that the coordinator waits for write operations to complete.

cassandraKeyspace Section

dataCompression

Default Value: LZ4
Valid Values: NONE, SNAPPY, LZ4, DEFLATE
Changes Take Effect: After start or restart

Stored data compression method.

name

Default Value: none
Valid Values: A lowercase string that begins with an alphanumeric character and continues with a sequence of alphanumeric characters and underscores, with a maximum length of 48 characters.
Changes Take Effect: After start or restart

Cassandra keyspace name.

password

Default Value:
Valid Values: Valid string
Changes Take Effect: After start or restart

The user's password

readConsistencyLevel

Default Value: LOCAL_QUORUM
Valid Values: EACH_QUORUM, QUORUM, LOCAL_QUORUM
Changes Take Effect: After start or restart

Consistency level for read operations, as described at http://docs.datastax.com/en/cassandra/2.1/cassandra/dml/dml_config_consistency_c.html.

replicationStrategy

Default Value: NetworkTopologyStrategy
Valid Values: SimpleStrategy, NetworkTopologyStrategy
Changes Take Effect: After start or restart

Replication strategy name, as described at http://docs.datastax.com/en/cassandra/2.0/cassandra/architecture/architectureDataDistributeReplication_c.html.

> ### Warning
> Genesys strongly recomends **not** using `SimpleStrategy`. If you use `SimpleStrategy`, you cannot use more than one data center and KeySpaces you create will be difficult to migrate to `NetworkTopologyStrategy` once they contain a lot of data. Also see https://docs.datastax.com/en/cassandra/2.0/cassandra/architecture/architectureDataDistributeReplication_c.html

If you set your replication strategy to `SimpleStrategy` you must also:

- Configure a replication factor in the replicationStrategyParams option.
- For embedded Cassandra, set the endpointSnitch option of the [cassandraEmbedded] section to `SimpleSnitch`.
- For external Cassandra, set `endpoint_snitch: SimpleSnitch` in your cassandra.yaml file.

replicationStrategyParams

Default Value: 'OperationalDC':1
Valid Values: See the Cassandra replication configuration
Changes Take Effect: After start or restart

A comma-separated list of replication strategy parameters, where every list item is a colon-separated pair whose first item is the data center name enclosed in single quotes and whose second item is the number of replicas for that data center. For example, `'OperationalDC1': 3, 'OperationalDC2': 2` indicates that the `OperationalDC1` data center includes 3 data replicas, while `OperationDC2` includes

2 data replicas. For more information, consult http://docs.datastax.com/en/cassandra/2.0/cassandra/architecture/architectureDataDistributeReplication_c.html.

retention.entity.all

Default Value: 0 seconds (8.5.1 and later); 15 (8.5.0)
Valid Values: String (8.5.1); Integer (8.5.0)
Changes Take Effect: After start or restart
Modified: 8.5.1

Starting with version 8.5.1, this value (as a string) specifies the time to live (TTL) for all entities in the Cassandra database, in the `n time-unit` format. For example, `1 second`.

In version 8.5.0, this value (as an integer) specifies the time to live (TTL) for all entities in the Cassandra database, in the time units set in the `retention.time-unit` option.

This option affects all business entities in the database.

retention.entity.<object>

Default Value: 0 seconds (8.5.1); none (8.5.0)
Valid Values: string (8.5.1); integer (8.5.0)
Changes Take Effect: After start or restart
Modified: 8.5.1

As of version 8.5.1, this value (as a string) specifies the time-to-live (TTL) for specific business entities in the Cassandra database, in the format "n time-unit". For example, `1 day`. This option only affects the business entity specified by <object>.

In version 8.5.0, this value (as an integer) specifies the time-to-live (TTL) for the selected entity, in the time units set in the options. <object> must be replaced with a business entity name.

retention.time-unit

Default Value: day
Valid Values: sec, min, hour, day, month
Changes Take Effect: After start or restart
Discontinued: 8.5.1

Defines the time units for the expiration period set in the **retention.entity.all** and **retention.entity.*** options.

transportCompression

Default Value: NONE
Valid Values: NONE, SNAPPY, LZ4
Changes Take Effect: After start or restart

The transport Compression method.

userName

Default Value:
Valid Values: Valid string
Changes Take Effect: After start or restart

The user's name

writeConsistencyLevel

Default Value: LOCAL_QUORUM
Valid Values: EACH_QUORUM, QUORUM,LOCAL_QUORUM
Changes Take Effect: After start or restart

Consistency level for write operations, as described at http://docs.datastax.com/en/cassandra/2.1/cassandra/dml/dml_config_consistency_c.html.

log Section

affectedLoggers

Default Value: The default value is an empty string, which means that there aren't any affected loggers.
Valid Values: Comma-separated list of logger names, specified in LOG4J2.xml. For example: com.genesyslab.webme.commons,PROTOCOL,org.apache.cassandra
Changes Take Effect: Immediately

Verbosity settings are explicitly applied for some loggers, as discussed in the extended description.

Extended description

Verbosity settings are explicitly applied for the following loggers:

- Loggers that are not declared explicitly in the `log4j2.xml` configuration file.
- Loggers that are specified explicitly in the `log4j2.xml` and are specified in the value for this `affectedLoggers` option.

For other loggers specified in `log4j2.xml`, but not mentioned in the value for this option, the verbosity level is not re-applied.

Here is a use case for when you might need to set this option:

- Cassandra needs to write error messages to a log file, and at the same time, Genesys components also need to write debug messages to the log file.

To resolve this use case, you would:

1. Specify the following logger in `log4j2.xml`: `<logger name="org.apache.cassandra" level="error" additivity="false">`
2. **Do not** include `org.apache.cassandra` in the value for the `affectedLoggers` option.
3. The default `log4j2.xml` file contains the following logger: `<logger name="com.genesyslab.platform" level="info" additivity="false">`

4. Include `com.genesyslab.platform` in the value for the `affectedLoggers` option.
5. Set the verbose option to debug.

In the sample above, the value of `affectedLoggers` should be `com.genesyslab.platform`. Error (but no debug or info) messages from Cassandra will be available in logs, and debug messages from `com.genesyslab.platform` will be available in logs.

all

Default Value: stdout
Valid Values: See table
Changes Take Effect: After start/restart

Specifies the outputs to which an application sends all log events. The log output types must be separated by a comma when more than one output is configured. For example: `all = stdout, logfile`

Valid Values (log output types):

`stdout`	Log events are sent to the Standard output (`stdout`).
`stderr`	Log events are sent to the Standard error output (`stderr`).
`network`	Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database.Setting the `all` log level option to the `network` output enables an application to send log events of the `Standard`, `Interaction`, and `Trace` levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
`memory`	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
`[filename]`	Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

expire

Default Value: 3
Valid Values: See table
Changes Take Effect: After restart

Determines whether log files expire. If they do, sets the measurement for determining when they expire, along with the maximum number of files (segments) or days before the files are removed.

This option is ignored if log output is not configured to be sent to a log file.

Valid Values (log output types):

`false`	No expiration; all generated segments are stored.
`<number> file or <number>`	Sets the maximum number of log files to store. Specify a number from `1`—`1000`.
`<number> day`	Sets the maximum number of days before log files are deleted. Specify a number from `1`—`100`.

> **Warning**
> If an option's value is set incorrectly — out of the range of valid values — it will automatically be reset to `10`.

segment

Default Value: 1000
Valid Values: See table
Changes Take Effect: After restart

Specifies whether there is a segmentation limit for a log file. If there is, sets the mode of measurement, along with the maximum size. If the current log segment exceeds the size set by this option, the file is closed and a new one is created. This option is ignored if log output is not configured to be sent to a log file.

Valid Values (log output types):

`false`	No segmentation is allowed.
`<number> KB or <number>`	Sets the maximum segment size, in kilobytes. The minimum segment size is `100 KB`.
`<number> MB`	Sets the maximum segment size, in megabytes.
`<number> hr`	Sets the number of hours for the segment to stay open. The minimum number is 1 hour.

standard

Default Value: stdout
Valid Values: See table
Changes Take Effect: Immediately

Specifies the outputs to which an application sends the log events of the `Standard` level. The log output types must be separated by a comma when more than one output is configured. For example: `standard = stderr, network`

Valid Values (log output types):

`stdout`	Log events are sent to the Standard output (`stdout`).
`stderr`	Log events are sent to the Standard error output (`stderr`).
`network`	Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database.
`memory`	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
`[filename]`	Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

time_convert

Default Value: local
Valid Values: See table
Changes Take Effect: Immediately

Specifies the system in which an application calculates the log record time when generating a log file. The time is converted from the time in seconds since 00:00:00 UTC, January 1, 1970.

Valid Values (log output types):

`local`	The time of log record generation is expressed as a local time, based on the time zone and any seasonal adjustments. Time zone information of the application’s host computer is used.
`utc`	The time of log record generation is expressed as Coordinated Universal Time (UTC).

time_format

Default Value: time
Valid Values: See table
Changes Take Effect: Immediately

Specifies how to represent, in a log file, the time when an application generates log records. A log record's time field in the ISO 8601 format looks like this: `2001-07-24T04:58:10.123`

Valid Values (log output types):

<tt>time</tt>	The time string is formatted according to the <tt>HH:MM:SS.sss</tt> (hours, minutes, seconds, and milliseconds) format.
<tt>locale</tt>	The time string is formatted according to the system's locale.
<tt>ISO8601</tt>	The date in the time string is formatted according to the ISO 8601 format. Fractional seconds are given in milliseconds.

trace

Default Value: stdout
Valid Values: See table
Changes Take Effect: Immediately

Specifies the outputs to which an application sends the log events of the `Trace` level and higher (that is, log events of the `Standard`, `Interaction`, and `Trace` levels). The log outputs must be separated by a comma when more than one output is configured. For example: `trace = stderr, network`

Valid Values (log output types):

`stdout`	Log events are sent to the Standard output (`stdout`).
`stderr`	Log events are sent to the Standard error output (`stderr`).
`network`	Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database.
`memory`	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
`[filename]`	Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

verbose

Default Value: standard
Valid Values: See table
Changes Take Effect: Immediately

Determines whether a log output is created. If it is, specifies the minimum level of log events generated. The log events levels, starting with the highest priority level, are Standard, Interaction, Trace, and Debug.

Valid Values (log output types):

`all`	All log events (that is, log events of the Standard, Trace, Interaction, and Debug levels) are generated.
`debug`	The same as `all`.
`trace`	Log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels) are generated, but log events of the Debug level are not generated.
`interaction`	Log events of the Interaction level and higher (that is, log events of the Standard and Interaction levels) are generated, but log events of the Trace and Debug levels are not generated.
`standard`	Log events of the Standard level are generated, but log events of the Interaction, Trace, and Debug levels are not generated.
`none`	No output is produced.

spark Section

executorMemory

Default Value: None
Valid Values: Valid memory limit
Changes Take Effect: After start or restart

Use this option to manage the amount of memory used by Spark for executing tasks on each node. Genesys recommends at least two gigabytes per node, but more memory can improve performance if hardware allows. For information about the format, consult the Spark documentation.

host

Default Value: None
Valid Values: *hostname of the Spark Master node*
Changes Take Effect: After start or restart

The name of the Spark Master host. The value should be the same as what Java's **InetAddress.getLocalHost()** would return for the specified host.

masterWebPort

Default Value: 8080
Valid Values: Valid port number
Changes Take Effect: After start or restart

The number of the TCP port that the Spark Master web UI will listen on. Note that this option is provided for cases when the default port has already been used by another service.

port

Default Value: 7077
Valid Values: Valid port number
Changes Take Effect: After start or restart

The port number of the Spark Master host.

sparkHeartbeatTimeout

Default Value: 60
Valid Values: Positive integer
Changes Take Effect: After start or restart

The timeout value in seconds between two heartbeat calls to the Spark metrics API.

sparkStartTimeout

Default Value: 20
Valid Values: Positive integer
Changes Take Effect: After start or restart

The timeout value in seconds between a Spark start or restart and the first time its API is checked. On slower machines, it makes sense to increase this value so that Spark has enough time to start successfully (without initiating a restart cycle).

startMode

Default Value: worker
Valid Values: off, worker, or both
Changes Take Effect: After start or restart

The mode that will be used when starting Spark. If set to `off`, Spark will not be started by Data Processing Server, and will instead have its state managed externally. If set to `worker`, only a worker node will be started. If set to `both`, both a worker node and a master node are started. **Note:** Genesys recommends that you set this option for each node to clearly specify the role. However, you can set the Cluster object to `worker` mode and override that value for the master node by setting that node to `both`.

uri

Default Value: None
Valid Values: Valid Spark URI

Changes Take Effect: After start or restart

Advanced. For situations when Spark is running externally, you must set the URI instead of the host and port. The URI must include the protocol, in addition to the host and port.

workerWebPort

Default Value: 8081
Valid Values: Valid port number
Changes Take Effect: After start or restart

The number of the TCP port that the Spark Worker web UI will listen on. Note that this option is provided for cases when the default port has already been used by another service.

Cassandra Resource Access Point

Options for this component are contained in the following configuration sections:

- resource

> **Tip**
>
> In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.
>
> **Power users: Download a CSV file** containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
resource	type	cassandra	
Section	**Option**	**Default**	**Changes Take Effect**

resource Section

type

Default Value: cassandra
Valid Values: cassandra
Changes Take Effect:

This option is mandatory.

A marker that defines this as the Cassandra Resource Access Point

Change History

Content under development