Web Services and Applications Deployment Guide

Web Services configuration options

4/23/2025

Web Services configuration options

Contents

You can set the configuration options below in the corresponding sections of the **application.yaml** file on your Web Services nodes (**server-settings.yaml** if you are installing Web Services and Applications version 8.5.201.09 or earlier). For details, see Configuring Web Services.

logging

Settings in this section are listed under "logging".

config

Default Value: `logback.xml`
Valid Values: A valid path
Mandatory: No
Specifies the path to the **logback.xml** file. You created this file (or Web Services created it for you) as part of Deploying the web application.

file

Default Value: `cloud.log`
Valid Values: A valid file name
Mandatory: No
Specifies the name of the log file. This value is stored in *${LOG_FILE}* which may be used in **logback.xml**.

path

Default Value: `/var/log/jetty9`
Valid Values: A valid path
Mandatory: No
Specifies the path to the log file. This value is stored in *${LOG_PATH}* which may be used in **logback.xml**.

jetty

Settings in this section are listed under "jetty".

cookies

Default Value: None
Valid Values:

Name	Mandatory	Default Value	Description
httpOnly	No	true	If true, it sets an HTTP-only flag for session

Name	Mandatory	Default Value	Description
			cookies.
secure	No	false	If true, it sets the secure cookie flag for session cookies.
sameSite	Yes	None	Specifies what should be returned as SameSite cookie attribute value in response for Jetty's session cookie. Valid values are `None`, `Lax`, or `Strict`.
partitioned	No	false	If true, it sets the `Partitioned` flag for session cookies.

Mandatory: No
Specifies how Jetty should handle cookies. For example:

```
cookies:
    httpOnly: true
    secure: true
    sameSite: None
```

These options only take effect if **enableSsl** is set to `true`.

host

Default Value: `0.0.0.0`
Valid Values: A host name or IP address
Mandatory: No
Specifies the host name or IP address of the Jetty host. In versions 8.5.201.18 and later, this value should be the same as `GWS_HOST` you defined as part of Deploying the web application.

port

Default Value: `8090`
Valid Values: A valid port
Mandatory: No
Specifies the port of the Jetty host. In versions 8.5.201.18 and later, this value should be the same as `GWS_PORT` you defined as part of Deploying the web application.

idleTimeout

Default Value: `30000`
Valid Values: An integer greater than 0
Mandatory: No
Specifies the maximum idle time, in milliseconds, for a connection.

soLingerTime

Default Value: `-1`
Valid Values: An integer greater than 0, or -1 to disable
Mandatory: No
Specifies the socket linger time.

sessionMaxInactiveInterval

Default Value: `1800`
Valid Values: An integer greater than 0
Mandatory: No
Specifies the period, in seconds, after which a session is deemed idle and saved to session memory.

enableWorkerName

Default Value: `true`
Valid Values: `true`, `false`
Mandatory: No
Specifies whether to add the **WorkerName** parameter into the JSESSIONID cookie.

enableRequestLog

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
Enables request logging. If you set the value to `true`, you must also set values for the requestLog option.

requestHeaderSize

Default Value: 8192
Valid Values: Any positive integer value greater than the default value

Specifies the allowed request header size for the Jetty servlet container.

responseHeaderSize

Default Value: 8192
Valid Values: Any positive integer value greater than the default value

Specifies the allowed response header size for the Jetty servlet container.

requestLog

Default Value: None
Valid Values:

Name	Mandatory	Default Value	Description
filename	No	yyyy_mm_dd.cloud-request.log	Specifies the log file name format.
filenameDateFormat	No	yyyy_MM_dd	Specifies the log file name date format.
logTimeZone	No	GMT	Specifies the timestamp time zone used in the log.
retainDays	No	90	Specifies the time interval, in days, for which Jetty should retain logs.
append	No	true	Specifies whether Jetty appends to the request log file or starts a new file.
extended	No	true	Specifies whether Jetty logs extended data.
logCookies	No	true	Specifies whether Jetty logs request cookies.
logLatency	No	true	Specifies whether Jetty logs the request latency.
preferProxiedForAddress	No	true	Specifies whether Jetty logs IP address or the IP address from the X-Forwarded-For request header.

Mandatory: No
Specifies how Jetty should handle request logging. For example:

```
enableRequestLog: true
  requestLog:
    filename: yyyy_mm_dd.cloud-request.log
    filenameDateFormat: yyyy_MM_dd
    logTimeZone: GMT
    retainDays: 90
    append: true
    extended: true
    logCookies: false
    logLatency: true
    preferProxiedForAddress: true
```

These options only take effect if enableRequestLog is set to `true`.

enableSsl

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
Enables Secure Sockets Layer support. If you set the value to `true`, you must also set values for the ssl option.

ssl

Default Value: None
Valid Values:

Name	Mandatory	Default Value	Description
port	No	443	The SSL port. This option is the equivalent of the Jetty "https.port" variable.
securePort	No	8443	The port to which integral or confidential security constraints are redirected. This option is the equivalent of the Jetty "jetty.secure.port" variable.
idleTimeout	No	30000	The maximum idle time, in milliseconds, for a connection.
soLingerTime	No	-1	The socket linger time. A value of -1 disables this option.
keyStorePath	No	None	The keystore path.
keyStorePassword	No	None	The keystore password.
keyManagerPassword	No	None	The key manager password.
keyStoreProvider	No	None	The keystore provider.
keyStoreType	No	JKS	The key store type.
trustStorePath	No	None	The truststore path.
trustStorePassword	No	None	The truststore password.
trustStoreProvider	No	None	The truststore provider.
trustStoreType	No	JKS	The truststore type.
needClientAuth	No	None	Set this option to true if SSL needs client authentication.
wantClientAuth	No	None	Set this option to true if SSL wants client authentication.
certAlias	No	None	The alias of the SSL certificate for the connector.
validateCerts	No	None	Set this option to true if the SSL certificate has to be validated.
validatePeerCerts	No	None	Set this option to true if SSL certificates of the

Name	Mandatory	Default Value	Description
			peer have to be validated.
trustAll	No	None	Set this option to true if all certificates should be trusted if there is no keySstore or truststore.
renegotiationAllowed	No	None	Set this option to true if TLS renegotiation is allowed.
excludeCipherSuites	No	None	Specifies the array of cipher suite names to exclude from enabled cipher suites.
includeCipherSuites	No	None	Specifies the array of cipher suite names to include in enabled cipher suites.
endpointIdentificationAlgorithm	No	None	Specifies the endpoint identification algorithm. Set this option to "HTTPS" to enable hostname verification.
includeProtocols	No	None	The array of protocol names (protocol versions) to include for use on this engine.
excludeProtocols	No	None	The array of protocol names (protocol versions) to exclude from use on this engine.
enableHsts	No	false	If set to `true`, Genesys Web Services (GWS) provides support for HTTP Strict Transport Security (HSTS) protocol. HSTS prevents Man-in-the-Middle attacks that can occur in unsecure (HTTP) browser sessions. The following string is inserted in the response header: `Strict-Transport-Security: max-age=31536000 ; includeSubDomains` This string tells the browser to not accept any untrusted, expired, or revoked TLS certificates from the domain.

Name	Mandatory	Default Value	Description

enableNonSecureToSecureRedirect	No	false	Redirects HTTP requests to HTTPS.
			
			When enabled, the following string is sent in the response header:
			
			`HTTP/1.1 302 Found`
			`Location: https://...`

Mandatory: No
Specifies how Jetty should handle support for Secure Sockets Layer. For example:

```
enableSsl: true
 ssl:
   port: 443
   securePort: 8443
   idleTimeout: 30000
   soLingerTime: -1
```

These options only take effect if **enableSsl** is set to `true`.

cookies

Default Value: None
Valid Values:

Name	Mandatory	Default Value	Description
httpOnly	No	true	If true, it sets an HTTP-only flag for session cookies.
secure	No	false	If true, it sets the secure cookie flag for session cookies.

Mandatory: No
Specifies how Jetty should handle cookies. For example:

```
cookies:
   httpOnly: true
   secure: true
```

These options only take effect if **enableSsl** is set to `true`.

sessionCookieName

Default Value: `JSESSIONID`
Valid Values: Any string which can be used as a cookie name as per RFC 6265
Mandatory: No
Defines the name of the session cookie used by Web Services.

enableXXSSProtection

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
Enables XSS Protection and the following header is added to the response.

```
X-XSS-Protection: 1
```

enableXXSSProtectionBlockMode

Default Value: `true`
Valid Values: `true`, `false`
Mandatory: No
When enabled, blocks the page from being rendered by sending the following header in the response:

```
X-XSS-Protection: 1; mode=block
```

enableXContentTypeOptions

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
When enabled, content sniffing is disabled by sending the following header in the response:

```
X-Content-Type-Options: nosniff
```

xFrameOptions

The X-Frame-Options HTTP response header can be used to indicate whether a browser should be allowed to render a page in a <frame>, <iframe>, or <object>. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Default Value: None
Valid Values: DENY, SAMEORIGIN, ALLOW-FROM
Mandatory: No
When enabled, the following header is added to the response.

```
X-Frame-Options: DENY
```

xFrameOptionsAllowFromUri

Default Value: None
Valid Values: A valid URI
Mandatory: No
When enabled, **xFrameOptions** is set to ALLOW-FROM, and only iframes from the specified URI are allowed. The following header is added to the response.

```
X-Frame-Options: ALLOW-FROM https://example.com/
```

This header is not supported by all browsers. For the list of browser types and versions that support the X-Frame-Options header, please refer to Clickjacking Defense Cheat Sheet.

xFrameOptionsExcludedUris

Default Value: None
Valid Values: List of URIs
Mandatory: No
Responses for requests from the specified URIs will not contain the X-Frame-Options header. The URIs must be relative and start with a slash (/) symbol. They must not contain the hostname and the port information. This is a workaround for browsers that do not support xFrameOptions.

> **Important**
>
> If you are using a browser that does not fully support xFrameOptions, it is highly recommended to list the URIs in the **xFrameOptionsExcludedUris** option to exclude these pages from the Clickjacking prevention:

```
jetty:
  ...
  xFrameOptionsExcludedUris:
    - /ui/crm-adapter/index.html
    - /ui/crm-workspace/index.html
    - /ui/dashboard/index.html
    - /ui/ad/v1/disaster-recovery.html
```

cassandraCluster

Settings in this section are listed under "cassandraCluster".

thrift_port

Default Value: `9160`
Valid Values: A valid port
Mandatory: No
Specifies the port for Thrift to listen for clients. It should be the same as the `rpc_port` you set in the **cassandra.yaml** file as part of the Configuring Cassandra procedure.

jmx_port

Default Value: 7199
Valid Values: A valid port
Mandatory: No
Specifies the port Cassandra uses for Java Manage Extension (JMX).

keyspace

Default Value: `sipfs`
Valid Values: A valid keyspace name
Mandatory: No
Specifies the name of the Cassandra keyspace. This name should be the same as the keyspace name you set while Creating the Cassandra keyspace. If you used the keyspace creation scripts that come with Web Services and Applications, then you can leave this value as `sipfs`.

nodes

Default Value: None
Valid Values: A comma-separated list of IP addresses or host names
Mandatory: No
Specifies the Cassandra node IPs or host names.

backup_nodes

Default Value: None
Valid Values: A comma-separated list of IP addresses or host names
Mandatory: No
Specifies the backup Cassandra node IPs or host names. This option is intended for deployments that have two separate Cassandra data centers — Web Services switches from primary to backup if the primary nodes are unavailable. If your deployment is small with only one data center, you can ignore this option.

replication_factor

Default Value: None
Valid Values: An integer less than the number of nodes in the cluster
Mandatory: No
Specifies a replication factor appropriate for your Cassandra topology. This value should be the same as the replication factor you set in Step 2 of the Creating the Cassandra keyspace procedure.

read_consistency_level

Default Value: None
Valid Values: `CL_ONE`, `CL_QUORUM`, `CL_LOCAL_QUORUM`
Mandatory: No
Specifies the read consistency level appropriate for your Cassandra topology:

Development (1 Cassandra node)	Single Data Center (1 data center with a minimum of three Cassandra nodes)	Two Data Centers (data centers with a minimum of three Cassandra nodes in each data center)
CL_ONE	CL_QUORUM	CL_LOCAL_QUORUM

write_consistency_level

Default Value: None
Valid Values: `CL_ONE`, `CL_QUORUM`, `CL_LOCAL_QUORUM`
Mandatory: No
Specifies the write consistency level appropriate for your Cassandra topology:

Development (1 Cassandra node)	Single Data Center (1 data center with a minimum of three Cassandra nodes)	Two Data Centers (data centers with a minimum of three Cassandra nodes in each data center)
CL_ONE	CL_QUORUM	CL_LOCAL_QUORUM

max_conns_per_host

Default Value: 16
Valid Values: An integer greater than 0
Mandatory: No
Specifies the maximum number of connections to allocate for a single host's pool.

max_cons

Default Value: 48
Valid Values: An integer greater than 0
Mandatory: No
Specifies the maximum number of connections in the pool.

max_pending_conns_per_host

Default Value: `80`
Valid Values: An integer greater than 0
Mandatory: No
Specifies the maximum number of pending connection attempts per host.

max_blocked_threads_per_host

Default Value: `160`
Valid Values: An integer greater than 0
Mandatory: No
Specifies the maximum number of blocked clients for a host.

cassandraVersion

Default Value: None
Valid Values: `1.1` or `1.2`
Mandatory: No
Specifies the Cassandra version for your Web Services and Applications deployment.

useSSL

Default Value: None
Valid Values: `true`, `false`
Mandatory: No
Specifies whether Cassandra should use Secure Sockets Layer (SSL). This option is only valid for Cassandra 1.2.x.

serverSettings

Settings in this section are listed under "serverSettings".

URLs

externalApiUrlV2

Default Value: None
Valid Values: A public schema-based URL ending with `/api/v2`.
Mandatory: Yes
Specifies the prefix used for resources in the public API. In a development environment, the host and port should be set to the host name or IP address of the Web Services node. In a production environment, the host and port should be set to the host name or IP address of the load balancer in a production environment. For example, `https://192.0.2.20/api/v2`.

internalApiUrlV2

Default Value: None
Valid Values: A public schema-based URL ending with `/internal-api`.
Mandatory: Yes
Specifies the prefix used for internal resources. In a development environment, the host and port should be set to the host name or IP address of the Web Services node. In a production environment, the host and port should be set to the host name or IP address of the load balancer in a production environment. For example, `http://192.0.2.20/internal-api`.

Platform API Settings

excludeFields

Default Value: -
Valid Values: A list of strings.
Mandatory: No
Enables filtering of specified fields from the Platform Configuration API responses.

Sample

The following setting will filter out the **password** field from the response.

```
...
serverSettings:
  ...
  platformApiSettings:
    excludeFields:
      - password
```

Paths

pathPrefix

Default Value:
Valid Values: A valid prefix
Mandatory: No
Specifies a prefix that Web Services adds to the relative URIs it includes in responses. For example, if you set **pathPrefix** to `/api/v2` and make the following request:

```
GET http://localhost:8080/api/v2/devices
```

Web Services returns the following response:

```
{
   "statusCode":0,
   "paths":[
      "/api/v2/devices/971ed91d-82bf-490b-94d2-02d240165764",
      "/api/v2/devices/a3f9e854-54d8-4260-bea3-d6e450ee7df0"
   ],
   "uris":[
      "http://localhost:8080/api/v2/devices/7c7ab1f7-e596-41bc-9ff4-4a12c489865f",
      "http://localhost:8080/api/v2/devices/a3f9e854-54d8-4260-bea3-d6e450ee7df0"
   ]
}
```

Notice that `paths` includes relative URIs with the `/api/v2` prefix.

General

chatServerRejoinAttempts

Default Value: `5`
Valid Values: `Any positive integer`
Mandatory: No
Specifies the number of join attempts to a chat session.

chatServerRejoinDelay

Default Value: `10000`
Valid Values: `Any positive integer`
Mandatory: No
Specifies the delay, in milliseconds, between join attempts to a chat session.

updateInteractionForSetContact

Default Value: `false`

Valid Values: `true`, `false`
Mandatory: No
Introduced: 8.5.202.96
Specifies whether Web Services `RequestUpdateInteraction` instead of `RequestAssignInteractionToContact` when the `SetContact` request is called. Using `RequestUpdateInteraction` prevents UCS from updating the `ThreadId` interaction attribute. In some scenarios, updates to this attribute can cause an interaction to become orphaned in the UCS database.

sendParticipantsUpdatedBeforeStatusChange

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
Introduced: 8.5.202.84
Specifies the order in which GWS sends `ParticipantsUpdated` and `StatusChange` notifications. To make sure that after reconnecting to Chat Server GWS send the `ParticipantsUpdated` notification first and then the `StatusChange` notification, set the value of this option to `true`.

disableCreatorAppIdUpdates

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
Introduced: 8.5.202.84
Preserves the original `CreatorAppId` of an interaction in UCS. Set the value of this option to `true` to make sure that the `CreatorAppId` is not changed after reconnecting to Chat Server.

enableAgentWorkbinStatisticsOptimization

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
Turns on synchronization of the `users_index_employee_id` table, which improves the performance of the `RequestStats` operation. It is necessary to perform a force synchronization of Cassandra with Configuration Server after enabling this option.

> **Important**
> Applicable only for environments with a large number of agents and only when delay is observed on the GWS side.

enableIntermediateParticipantNicknameFix

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
Specifies how the nickname of a participant in the chat message of the application CometD notification is displayed. By default (the `false` value of the option), the latest nickname of a participant is displayed for all messages in the chat transcript. When this option is set to `true`,

messages of the participant who changed the nickname are displayed with the actual nickname at the time when messages were sent.

enableNotificationOnPullChat

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
Enables sending of a notification with interaction properties while pulling chat interaction from a workbin. By default, the same notification is sent to other media types.

Add the following notification to the application.yaml file:

```
...
serverSettings:
  ...
  enableNotificationOnPullChat: true
```

enableJoinOnPullChat

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
Enables joining to the chat session of the chat interaction that is being pulled from a workbin. Following notification is a chat transcript similar to the one which is sent for the Accept operation.

Add the following notification to the application.yaml file:

```
...
serverSettings:
  ...
  enableJoinOnPullChat: true
```

enableSaveEmailReplyUserDataToUCS

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
Introduced: 8.5.202.85
Enables GWS to save the UserData of the parent email interaction to the child email interaction for Reply and ReplyAll operations. When set to `true`, GWS sends the AttachedData filled with the UserData of the parent interaction to UCS and UCS can render the corresponding field codes in Standard Responses.

enableUcsOrphanedScrollCleanup

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
When enabled, Web Services cleans up the orphan "Scrolls" from Universal Contact Server (UCS) that consume memory. When Web Services gets a list of interactions from UCS that has more than 1000 results, it creates a "Scroll" that must be released by Web Services when it is no longer needed.

enableFindOrCreateCallSearchInMemory

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
When enabled, Web Services searches for a call in memory, if the call is not found in Cassandra.

enableSyncConnectionToIxnServer

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
When enabled, Web Services waits for a configured amount of time for the Interaction Server connection to open before trying to send requests. You can use the **syncConnectionToIxnServerTimeout** option to adjust the wait time.

syncConnectionToIxnServerTimeout

Default Value: `3000`
Valid Values: positive integer
Mandatory: No
Defines the wait time for opening the connection to Interaction Server when the **enableSyncConnectionToIxnServer** option is enabled.

enableNotReadyOnConferenceInviteExpiration

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
When enabled, Web Services changes an agent's state when the agent does not answer an invite to Consult or Conference by a queue (routing-based). You can configure the status, which will be set using the **statusNameOnConferenceInviteExpiration** option.

statusNameOnConferenceInviteExpiration

Default Value: `NotReady`
Valid Values: name of the agent's status
Mandatory: No
Defines the status which will be set when the agent does not answer an invite to Consult or Conference by a queue (routing-based), and the **enableNotReadyOnConferenceInviteExpiration** is enabled.

enableEmailCaseInsensitive

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
Enables enforcing case-insensitive comparison of email addresses to remove the sender's address from recipients lists ("To", "Cc", "Bcc") while replying all in an email interaction.

enableInteractionRequestPull

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
When enabled, Web Services gets the current interaction from Interaction Server if an agent is disconnected from one Web Services node and is reconnected to another. This feature is only applicable if the agent reconnects using the same Workspace Web Edition instance. It does not apply to any active consultations or supervisors associated with the interaction. Previously, it was possible to have more than one agent in the same chat session when an agent switched connections to a new node while handling an interaction.

iwsDispositionCodeSync

Default Value: `10000`
Valid Values: positive integer
Mandatory: No
Enables Web Services to synchronize disposition codes with Workspace Web Edition. To turn on this feature, set **iwsDispositionCodeSync** to `true` on all nodes (this is done by default), and set the syncNode option to true on one node.

temporaryAuthenticationTokenTTL

Default Value: 300
Valid Values: An integer greater than 0
Mandatory: No
Specifies the time to live, in seconds, for the temporary authentication token.

enableCsrfProtection

Default Value:
Valid Values: `true`, `false`
Mandatory: No
Enables cross site request forgery protection. If you set the value to `true`, make sure you use the default values for **exposedHeaders** in the crossOriginSettings option. If you have already updated the **exposedHeaders**, just make sure the values include the defaults.

enableOpenIDConnect

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
Specifies whether Web Services uses OAuth 2.0 authentication.

enableStaleSessionsMonitoring

Default Value: `true`
Valid Values: `true`, `false`
Mandatory: No
Specifies whether Web Services should run its StaleSessionsMonitor process to periodically poll Cassandra for expired CometD sessions. This process releases any devices that might not have been released as part of EndContactCenterSession if CometD session information was lost.

requestTakeSnapshotTimeout

Default Value: `10000`
Valid Values: positive integer
Mandatory: No
Defines the timeout for the **GetContent** operation. This API request leads to sending **RequestTakeSnapshot** to Interaction Server. In some cases, when there are lots of interactions in a queue, this request could take a long time.

staleSessionsMonitorSettings

Default Value: None
Valid Values:

Name	Mandatory	Default Value	Description
monitoringInterval	No	60	Specifies, in seconds, how often Web Services scans for expired CometD sessions.
expiredSessionAge	No	180	Specifies the age, in seconds, at which Web Services considers the CometD session to be expired.

Mandatory: No
Specifies the configuration for monitoring expired CometD sessions. For example:

```
...
staleSessionsMonitorSettings:
    monitoringInterval: 60
    expiredSessionAge: 180
```

includeMessageType

Default Value: `false`
Valid Values: `true, false`
Mandatory: No
Specifies whether to include the original message type of a chat message in the MessageLogUpdated CometD notification when you make a SendMessage request with the Chat API.

enableInteractionPropertiesForStandardResponse

Default Value: `false`
Valid Values: `true, false`
Mandatory: No
Introduced: 8.5.202.90
Specifies whether Web Services uses the interaction properties from Interaction Server to render standard responses instead of using the interaction attributes from Universal Contact Server.

enableSpecificTwoStepTransferForAvayaSwitch

Default Value: false
Valid Values: true, false
Mandatory: No
Introduced: 8.5.202.94
When set to `true`, Web Services enables agents to complete a call transfer to a consultation target while the consultation call is on hold.

> **Important**
> This option is used for Avaya switch environments only.

enableStatusForOfflineChatOnRecovery

Default Value: false
Valid Values: true, false
Mandatory: No
Introduced: 8.5.202.97
When set to `true`, if an offline chat interaction is restored for an agent on a different node, the interaction has the 'LeftChat' status along with the list of corresponding capabilities.
To ensure that interactions are recovered as well as having the status set, Genesys recommends that when using this feature, you also set the value of the **enableSyncConnectionToIxnServer** to `enabled`.

enablePutOnHoldInWorkbin

Default Value: false
Valid Values: true, false
Mandatory: No
Introduced: 8.5.202.97
Specifies whether or not chat interactions can be put on hold in a workbin and then reopened later to continue the chat.

enableChatSynchronization

Default Value: false
Valid Values: true, false
Mandatory: No
Introduced: 8.5.202.97
Enable this option so that Web Services and Applications will display all chat messages for the current chat session. Previously, few messages could be lost if they were sent closely after an agent joined the chat session.

Timeouts

activationFailFastPeriod

Default Value: 10000
Valid Values: Any integer greater than 0
Mandatory: Yes
Determines fast-fail period length after a failure. Any attempt to reconnect to a Genesys server within the time specified by the **activationFailFastPeriod** option results in an immediate failure. To understand how this option works, consider this scenario:

- Agent A logs in to a GWS node. Note that connection to tserver is not active yet. GWS attempts to connect to tserver and the connection attempt fails.
- Agent B attempts to login within the **activationFailFastPeriod**. GWS does not attempt to connect to tserver. The agent is authenticated, but is not logged into the voice channel.
- After **activationFailFastPeriod** expires, Agent C attempts to login. GWS connects to TServer if the authentication is successful. Note that if the connection attempt fails, the activationFailFastPeriod is restarted again.

activationTimeout

Default Value: 12000
Valid Values: An integer greater than 0
Mandatory: No
Specifies the timeout, in milliseconds, for connecting to any Genesys server (except Configuration Server). This may include several individual attempts if the initial attempt to connect is unsuccessful.

> **Important**
> The activation timeout for Configuration Server is specified with the `configServerActivationTimeout` option.

chatServerConnectionTimeout

Default Value: 7000
Valid Values: Any positive integer
Mandatory: No
Specifies the timeout, in milliseconds, after which the attempt to connect to the Chat Server fails.

chatServerReconnectTimeout

Default Value: 10000
Valid Values: Any positive integer
Mandatory: No
Specifies the delay, in milliseconds, between attempts to connect to the Chat Server.

configServerActivationTimeout

Default Value: 35000
Valid Values: An integer greater than 0
Mandatory: No
Specifies the timeout, in milliseconds, for connecting to Configuration Server. This may include several individual attempts if the initial attempt to connect is unsuccessful.

configServerConnectionTimeout

Default Value: 15000
Valid Values: An integer greater than 0
Mandatory: No
Specifies the timeout, in milliseconds, for an individual connection attempt to Configuration Server.

connectionTimeout

Default Value: 4000
Valid Values: An integer greater than 0
Mandatory: No
Specifies the timeout, in milliseconds, for an individual connection attempt to any Genesys server (except Configuration Server).

> **Important**
> The connection timeout for Configuration Server is specified with the `configServerConnectionTimeout` option.

contactCenterSynchronizationTimeout

Default Value: 60000
Valid Values: An integer greater than 0
Mandatory: No
Specifies how often the syncNode looks for newly created contact centers.

inactiveUserTimeout

Default Value: 60
Valid Values: An integer greater than 0
Mandatory: No
Specifies the interval, in seconds, at which the inactive user cleanup process is run by the server. This process is run to invalidate HTTP sessions for users who have been deleted or whose user roles have changed.

reconnectAttempts

Default Value: 1
Valid Values: An integer greater than 0
Mandatory: Yes

Specifies the number of attempts Web Services makes to connect to any Genesys server before attempting to connect to the backup.

reconnectTimeout

Default Value: 10000
Valid Values: An integer greater than 0
Mandatory: Yes
Specifies the timeout, in milliseconds, between the reconnect attempts.

agentSessionCleanUpTimeout

Default Value: 60000 (ms)
Valid Values: Any positive integer.
Mandatory: No
Specify the timeout in milliseconds before the agent session cleanup procedure is initiated.

platformConfigurationReadTimeout

Default value: 10000
Valid values: Any positive integer.
Specify the timeout (in milliseconds) for platform configuration read requests. If an invalid or a negative value is provided, a warning message will be logged and the default value would be applied.

OPS account

opsUserName

Default Value: None
Valid Values: Any alphanumeric value that can include special characters
Mandatory: Yes
Specifies the name of the Web Services super user. Web Services creates this user at startup.

opsUserPassword

Default Value: None
Valid Values: Any alphanumeric value, including special characters
Mandatory: Yes
Specifies the password for the Web Services super user. Web Services creates this user at startup.

Configuration Server credentials

applicationName

Default Value: None
Valid Values: A valid application name
Mandatory: Yes
The name of the Web Services node application object in Configuration Server. For example, `WS_Node`.

applicationType

Default Value: None
Valid Values: A valid application type
Mandatory: Yes
The type of the Web Services node application object in Configuration Server. This value should be `CFGGenericClient`.

cmeUserName

Default Value: None
Valid Values: A valid Configuration Server user
Mandatory: Yes
The username that the Web Services server uses to connect to Configuration Server.

> **Important**
>
> Genesys recommends that you use the provided "default" account in Configuration Server. It is possible to use a different account, but you must take care in configuring the user's account permissions. Outside of a lab setting, this is best done in consultation with Genesys.

cmePassword

Default Value: None
Valid Values: A valid password
Mandatory: Yes
The password for the Configuration Server user Web Services uses to connect to Configuration Server.

syncNode

Default Value: None
Valid Values: `true, false`
Mandatory: No
Specifies whether the node is the synchronization node. This node is responsible for importing objects from Configuration Server into Cassandra, subscribing to changes notifications with Configuration Server, and processing updates.

> **Important**
>
> In each Web Services cluster, one node must be configured as the synchronization node: `syncNode = true`. All other nodes in the cluster must have `syncNode = false`.

synchronizationCmeEventsPrefilterEnabled

This option is deprecated in 8.5.2.

enableVirtualQueueSynchronization

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
Specifies whether the syncNode imports virtual queues from the Configuration Layer.

Statistics

locationAwareMonitoringDistribution

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No

Enables you to configure additional connections to different StatServers. GWS chooses the one that is "visible" from the GWS node (based on the location specified in the connection).

Set this option to `true` on all nodes only when deploying multiple data centers.

> **Important**
>
> - This option applies only to multi-data center environments.
> - The statistics collected in a multi-data center environment will not be displayed properly without both this option and the **enableMultipleDataCenterMonitoring** option set to `true`.

enableMultipleDataCenterMonitoring

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No

Enables statistics collection for each data center in a multiple data center configuration.

Set this option to `true` on all nodes only when deploying multiple data centers.

> **Important**

- This option applies only to multi-data center environments.
- The statistics collected in a multi-data center environment will not be displayed properly without both this option and the **locationAwareMonitoringDistribution** option set to `true`.

statConnectionTimeout

Default Value: `5000`
Valid Values: A positive integer greater than 0
Mandatory: No
Specifies the connection timeout, in milliseconds, for connecting to Stat Server.

statReconnectAttempts

Default Value: 1
Valid Values: A positive integer
Mandatory: No
Specifies the number of reconnect attempts before switching to the backup Stat Server, if the connection to the primary Stat Server is lost.

statReconnectTimeout

Default Value: `10000`
Valid Values: An integer greater than 0
Mandatory: No
Specifies the timeout, in milliseconds, before reconnecting to Stat Server.

statOpenTimeout

Default Value: `60000`
Valid Values: An integer greater than 0
Mandatory: No
Specifies the timeout, in milliseconds, between when a request is sent to Stat Server to open a statistic and when Web Services server determines the statistic has not been opened. If the timeout expires, the Web Services server discards the request and sends a new one.

statisticsWritesCL

This option is no longer applicable as of release 8.5.201.09.

statisticsMonitorMultimediaChannelStates

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
Specifies whether to monitor user states on non-voice channels.

reportingSyncInterval

Default Value: 30
Valid Values: An integer greater than 0
Mandatory: No
Specifies the interval, in seconds, for the reporting services to poll the database for information about the activities of other monitoring nodes and for the current state of the contact center configuration. If you set this option to a larger value, it decreases the load on the database, but also increases the timeout for detecting nodes that are down and objects that are added or updated in contact centers.

> **Important**
> The value of this option specifies the rate of scheduling, not the delay between when the previous polling finishes and the new polling starts.

enableElasticSearchIndexing

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
Specifies whether the configuration information and statistics should be indexed to Elasticsearch. If set to `true`, you must set the crClusterName option.

statisticsOpenRetryInterval

Default Value: `60` (1 hour)
Valid Values: An integer greater than 0
Mandatory: No
Specifies the interval, in minutes, for trying to reopen failed statistics. For example, if a statistic cannot be opened on Stat Server, it is marked as failed and then the server attempts to reopen the stat once every hour (the default value of **statisticsOpenRetryInterval**).

Multi regional supporting

nodePath

Default Value: None
Valid Values: A location and node ID, separated by a "/" — for example, `/US/node1`
Mandatory: Yes
Specifies the location and ID of the Web Services node within the deployment topology. This value must be unique across the deployment. For example, a value of `/US/node1` means that the node is located in the US region and has an ID of "node1". The node ID can be the hostname, the IP address, or any other unique identifier.

nodeId

Default Value: None
Valid Values: Any unique identifier, such as the node host name or IP

Mandatory: No
Specifies the unique identifier for the Web Services node. Each node in a cluster must have a unique `nodeId`.

SSL and CA

caCertificate

Default Value: None
Valid Values: Path to a signed certificate
Mandatory: No
Specifies the path to a certificate signed by a Certificate Authority. The file must be in the `.pem` or `.jks` format (if `.jks`, you can also set jksPassword). The certificate can be used if the WS_Cluster application uses Transport Layer Security (TLS) to connect to Genesys servers. This option is also mandatory to enable SAML authentication.

jksPassword

Default Value: None
Valid Values: Password for the key storage
Mandatory: No
Specifies the password for the key storage set in caCertificate, when the certificate is in `.jks` format. This option is mandatory to enable SAML authentication.

SAML

samlSettings

Default Value: None
Valid Values:

Name	Mandatory	Default Value	Description
serviceProviderEntityId	No	If omitted, Web Services uses the value of the externalApiUrlV2 option.	Specifies the service provider entity ID to be used in the metadata.
encryptionKeyName	Yes	None	Specifies the Security Assertion Markup Language (SAML) encryption key name. This key has to be present in the JKS key storage specified in the caCertificate option.
encryptionKeyPassword	No	If omitted, Web Services uses the value of the jksPassword option.	Specifies the password used to extract the SAML encryption key from JKS storage.
signMetadata	No	true	Specifies whether generated metadata is signed with an XML

Name	Mandatory	Default Value	Description
			signature that uses the certificate with the alias of **signingKeyName**.
signingKeyName	Yes	None	Specifies the SAML signing key name. This key has to be present in the JKS key storage specified in the caCertificate option.
signingKeyPassword	No	If omitted, Web Services uses the value of the jksPassword option.	Specifies the password used to extract the SAML signing key from JKS storage.
tlsKeyName	No	None	Specifies the TLS key name. This key has to be present in the JKS key storage specified in the caCertificate option.
tlsKeyPassword	No	If omitted, Web Services uses the value of the jksPassword option.	Specifies the password used to extract the SAML TLS key from JKS storage.
responseSkewTime	No	60	Specifies the maximum difference, in seconds, between the local time and time of the assertion creation which still allows message to be processed. Determines the maximum difference between clocks of the IDP and SP servers.
defaultBinding	No	SSO_ARTIFACT	Specifies the default SAML binding Web Services uses. The valid values are: SSO_POST, SSO_PAOS, SSO_ARTIFACT, HOKSSO_POST, or HOKSSO_ARTIFACT.
requestSigned	No	true	Specifies whether this service signs authentication requests.
wantAssertionSigned	No	true	Specifies whether this service requires signed assertions.
identityProviderMetadata	Yes	None	Specifies the path or URL for the identity provider XML metadata file. You can set this

Name	Mandatory	Default Value	Description
			option to the path to a physical location or, if the metadata file is exposed by the remote server over HTTP, you can specify the URL (in this case, Web Services applies a 5-second default request timeout).
secureRelayState	No	false	If false, the RelayState attribute Web Services passes to the Identity Provider during SAML authentication contains the original URL (from the "referer" header) requested by the client. If true, Web Services instead saves the original RelayState in Cassandra and uses an alphanumeric token that can identify the RelayState.
secureRelayStateTTL	No	3600 (1 hour)	Specifies, in seconds, the time-to-live for the RelayState record in Cassandra. This setting is only used if **secureRelayState** is set to true.
useExternalUserId	No	false	Specifies whether Web Services should use the external user ID, a property of the CfgPerson object in the Configuration Database , for SAML authentication. If false, Web Services uses the username. If true, Web Service uses the external user ID.
maxAuthenticationAge	No	7200 (2 hours)	Specifies the maximum time, in seconds, between a user's authentication and when the authentication statement is processed.

Mandatory: No
Specifies the configuration for Security Assertion Markup Language (SAML) authentication for Web Services. For example:

```
...
samlSettings:
    serviceProviderEntityId: 10.10.15.60
    encryptionKeyName: client
    signingKeyName: client
    identityProviderMetadata: http://ipd.company.host/saml/metadata/idp-metadata.xml
    responseSkewTime: 120
    defaultBinding: SSO_POST
```

CORS

crossOriginSettings

Default Value: None
Valid Values:

Name	Mandatory	Default Value	Description
allowedOrigins	No	None	Specifies a comma-separated list of allowed origins supported by this Web Services node. For example, http://*.genesys.com, http://*.genesyslab.com
allowedMethods	No	GET,POST,PUT,DELETE,OPTIONS	Specifies a comma-separated list of HTTP methods supported by the server.
allowedHeaders	No	X-Requested-With,Content-Type,Accept,Origin,Cookie,authorization,sid,surl,ContactCenterId	Specifies whether to include the Access-Control-Allow-Headers header as part of the response to a pre-flight request. This specifies which header field names can be used during the actual request.
allowCredentials	No	true	Specifies the value of the Access-Control-Allow-Credentials header. This should typically be left at the default value.
corsFilterCacheTimeToLive	No	120	Specifies the delay after the contact center allowDomain updating takes effect.
exposedHeaders	No	X-CSRF-HEADER,X-CSRF-TOKEN	Specifies which custom headers are allowed in cross-origin HTTP responses. This should typically be left at the

Name	Mandatory	Default Value	Description
			default value. If you do modify the value and you enable the enableCsrfProtection option, make sure the value for **exposedHeaders** includes `X-CSRF-HEADER,X-CSRF-TOKEN`.

Mandatory: No
Specifies the configuration for cross-origin resource sharing in Web Services. For example:

```
...
crossOriginSettings:
    corsFilterCacheTimeToLive: 120
    allowedOrigins: http://*.genesys.com, http://*.genesyslab.com
    allowedMethods: GET,POST,PUT,DELETE,OPTIONS
    allowedHeaders: "X-Requested-With,Content-Type,Accept,
Origin,Cookie,authorization,ssid,surl,ContactCenterId"
    allowCredentials: true
    exposedHeaders: "X-CSRF-HEADER,X-CSRF-TOKEN"
```

Elasticsearch

elasticSearchSettings

Default Value: None
Valid Values:

Name	Mandatory	Default Value	Description
clientNode	No	false	Specifies whether the current Web Services node acts as an Elasticsearch client or server.
crClusterName	No	None	Specifies the name of the cluster to enable search functionality in Elasticsearch. If this option is not present, search functionality is not enabled.
indexPerContactCenter	No	false	Enables indexing on a per-contact center basis. If false, there is only one index for all current statistics.
enableScheduledIndexVerification	No	false	Enables scheduled index verification on the

Name	Mandatory	Default Value	Description
			Web Services node. This means that the node goes through all objects handled by Elasticsearch and makes sure they still exist in Cassandra and vice versa.
indexVerificationInterval	No	720 minutes (12 hours)	Specifies an interval, in minutes, between index verifications for this Web Services node.
enableIndexVerificationAtStartUp	No	true	Enables index verification at start-up on this node. This means that, at start-up, the node goes through all objects handled by Elasticsearch and makes sure they still exist in Cassandra and vice versa.
retriesOnConflict	No	3	Controls how many times to retry if there is a version conflict when updating a document.
useTransportClient	No	false	Specifies whether Web Services should use a transport client for Elasticsearch. If true, then Web Services ignores the **clientNode** setting.
transportClient	Yes, if **useTransportClient** is true.	Values specified in TransportClientSettings	TransportClientSettings]] in the next table.

TransportClientSettings

Name	Mandatory	Default Value	Description
nodes	Yes, if **useTransportClient** is true.	null	Specifies the list of Elasticsearch nodes the transport client should connect to.
useSniff	no	false	Specifies if the transport client should us sniffing functionality and perform auto-discovery of Elasticsearch nodes in the cluster.

Name	Mandatory	Default Value	Description
ignoreClusterName	no	false	Specifies if Web Services should ignore the name of the cluster when connecting to the cluster.
pingTimeout	no	5000	Specifies, in milliseconds, the ping timeout for Elasticsearch nodes.
nodesSamplerInterval	no	5000	Specifies, in milliseconds, how often Web Services should sample/ping the Elasticsearch nodes listed and connected.

Mandatory: No
Specifies the configuration for Elasticsearch in Web Services. For example:

```
...
elasticSearchSettings:
    clientNode: true
    indexPerContactCenter: false
    enableScheduledIndexVerification: true
    indexVerificationInterval: 60
    retriesOnConflict: 2
    useTransportClient: true
    transportClient:
        nodes:
             - {host: 127.0.0.1, port: 9300}
        useSniff: true
        ignoreClusterName: true
        pingTimeout: 10000
        nodesSamplerInterval: 10000
```

Screen Recording

screenRecordingSettings

Default Value: None
Valid Values:

Name	Mandatory	Default Value	Description
screenRecordingVoiceEnabled	No	false	Specifies whether the current Web Services node supports screen recording for voice interactions. If false, the node rejects CometD requests from the ScreenRecording Client for agents with the voice channel.

Name	Mandatory	Default Value	Description
screenRecordingEServicesEnabled	No	false	Specifies whether the current Web Services node supports screen recording for non-voice interactions. If false, the node rejects CometD requests from the ScreenRecording Client for agents with the eServices channel.
recordingInteractionEventsTTL	No	172800	Specifies the time to live (TTL) for Cassandra to cache a screen recording interaction event.
clientSessionManagerCacheTTL	No	60	Specifies the TTL for the Web Services node to cache agent information (such as the agent's name) so that the node doesn't have to read the information from Web Services on each request.
contactCenterInfoManagerCacheTTL	No	90	Specifies the TTL for the Web Services node to cache contact center information so that the node doesn't have to read the information from Web Services on each request.

Mandatory: No
Specifies the screen recording configuration parameters. For example:

```
...
screenRecordingSettings:
   screenRecordingVoiceEnabled: false
   screenRecordingEServicesEnabled: false
   recordingInteractionEventsTTL: 172800
   clientSessionManagerCacheTTL: 60
   contactCenterInfoManagerCacheTTL: 90
```

Caching

cachingSettings

Default Value: None
Valid Values:

Name	Mandatory	Default Value	Description
agentStatesTTL	No	30	The time to live (TTL), in seconds, for contact-center agent states in cache.
businessAttributesTTL	No	30	The time to live (TTL), in seconds, for contact-center business attributes in cache.
businessUnitsWithSubresourcesTTL	No	30	The time, in seconds, when cache is re-read and updated from Cassandra.
cleanupPeriod	No	1800	The interval, in seconds, between caches cleanup (eviction of expired elements).
contactCenterFeaturesTTL	No	30	The time to live (TTL), in seconds, for contact-center feature IDs in cache.
contactCenterSettingsTTL	No	30	The time to live (TTL), in seconds, for contact-center custom settings in cache.
enableBlockingStrategyForBusinessUnitsWithSubresourcesCache	No	false	Specifies whether business units with subresources cache should utilize blocking approach or not.
enableBlockingStrategyForContactCenterSettingsCache	No	false	Specifies whether ContactCenter settings cache should utilize blocking approach or not.
enableBusinessUnitsWithSubresourcesCaching	No	false	Specifies whether business units with subresources should be served via cache or via direct Cassandra reads.
enableSystemWideBlockingStrategy	No	false	Specifies whether all caches should utilize blocking approach or not.
enableSystemWideCaching	No	false	Specifies if caching is used system-wide (`true`) or only during statistics evaluation (`false`).
skillsTTL	No	30	The time to live (TTL), in seconds, for contact-

Name	Mandatory	Default Value	Description
			center skills in cache.
transactionsTTL	No	30	The time to live (TTL), in seconds, for contact-center transactions in cache.
virtualAgentGroupsTTL	No	30	The time to live (TTL), in seconds, for contact-center virtual agent groups in cache.
voiceContextCaching	No	false	Specifies whether to use in-memory cached context for processing voice events. Using caching reduces the processing time, but you can expect delays in configuration information propagation.
voiceContextRefreshInterval	No	30	The interval, in seconds, between refreshes of the context caches for voice event processing. The service reads configuration information from the database and then refreshes the corresponding caches.

Mandatory: No
Specifies how Web Services should handle various caching scenarios. For example:

```
...
cachingSettings:
   enableSystemWideCaching: true
   agentStatesTTL: 30
   contactCenterFeaturesTTL: 30
   contactCenterSettingsTTL: 30
   voiceContextCaching: true
   voiceContextRefreshInterval: 60
```

DoS Filter

enableDosFilter

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
Enables the denial of service filter. If you set the value to `true`, you must also set values for the dosFilterSettings option.

dosFilterSettings

Default Value: None
Valid Values:

Name	Mandatory	Default Value	Description
maxRequestsPerSec	No	25	Specifies the maximum number of requests from a connection per second. Requests that exceed this are first delayed, then throttled.
delayMs	No	100	Specifies the delay, in milliseconds, imposed on all requests over the rate limit, before they are considered at all. Valid values: • -1 = reject request • 0 = no delay • Any other number = delay in milliseconds
maxWaitMs	No	50	Specifies the length of time, in milliseconds, to blocking wait for the throttle semaphore.
throttledRequests	No	5	Specifies the number of requests over the rate limit that are able to be considered at once.
throttleMs	No	30000	Specifies the length of time, in milliseconds, to asynchronously wait for semaphore.
maxRequestMs	No	30000	Specifies the length of time, in milliseconds, to allow the request to run.
maxIdleTrackerMs	No	30000	Specifies the length of time, in milliseconds, to keep track of request rates for a connection, before deciding that the user has gone away, and discarding the connection.
insertHeaders	No	true	If true, DoSFilter headers are inserted into the response.
trackSessions	No	true	If true, the usage rate is

Name	Mandatory	Default Value	Description
			tracked by session if a session exists.
remotePort	No	false	If true and session tracking is not used, then the rate is tracked by IP + port (effectively connection).
ipWhitelist	No	""	A comma-separated list of IP addresses that is not rate limited.

Mandatory: No
Specifies how Web Services should handle denial of service. For example:

```
...
enableDosFilter: true
dosFilterSettings:
   maxRequestsPerSec: 30
   ipWhitelist: 192.168.0.1,192.168.0.2
```

These options only take effect if enableDosFilter is set to `true`.

Account management

accountManagement

Default Value: None
Valid Values:

Name	Mandatory	Default Value	Description

forgotPasswordEmailTemplate	No	None	The template to use for an email that is sent to a user who forgets his or her password.
			
			`forgotPasswordEmailTemplate:`
			`  from: <from address>`
			`  subject: <Subject line>`
			`  body: <Email body>`

accountCreatedEmailTemplate	No	None	The template to use for a email that is sent to a user who creates a new account. `accountCreatedEmailTemplate:`

Name	Mandatory	Default Value	Description
			from: <from address> subject: <Subject line> body: <Email body>
smtpServer	No	None	The SMTP server configuration information. smtpServer: host: <smtp host name> port: <smtp port> userName: <user name for the account> password: <password in plain text> timeout: <optional SMTP timeout>

Mandatory: No
Specifies the configuration for the email notification and email server used when creating a new user. This option accepts the email server's login configuration, as well as email templates for resetting and creating user passwords. For example:

```
accountManagement:
     forgotPasswordEmailTemplate:
             from: <from address>
             subject: <Subject line>
             body: <Email body>
     accountCreatedEmailTemplate:
             from: <from address>
             subject: <Subject line>
             body: <Email body>
     smtpServer:
             host: <smtp host name>
             port: <smtp port>
             userName: <user name for the account>
             password: <password in plain text>
             timeout: <optional SMTP timeout>
```

CometD

cometDSettings

Default Value: None
Valid Values:

Name	Mandatory	Default Value	Description
cometdSessionExpirationTimeout	No	60	Specifies the timeout for the CometD session to expire on disconnect. It might take an additional minute for the session to be closed after it expires. If you set this option to -1, the session never expires. An agent can login again before the end of this timeout to disable session expiration.
closeHttpSessionOnCometDExpiration	No	true	Enables or disables HTTP session invalidation when CometD times out.
cookieHttpOnly	No	true	If true, it sets an HTTP-only flag for CometD's session cookies.
cookieSecure	No	false	If true, it sets the secure cookie flag for CometD's session cookies.
cookieSameSite	Yes	None	Specifies what should be returned as SameSite cookie attribute value in response for CometD's session cookie. Valid values are: None, Lax, or Strict.
maxSessionsPerBrowser	No	1	The maximum number of sessions (tabs/frames) allowed to long poll from the same browser; a negative value allows unlimited sessions.
multiSessionInterval	No	2000	Specifies the period of time, in milliseconds, for the client normal polling period, in case the server detects more sessions (tabs/frames) connected from the same browser than allowed by the `maxSessionsPerBrowser` parameter. A non-positive value means that additional sessions will be disconnected.

Mandatory: No
Specifies the configuration for the CometD-specific transport server embedded into the Web Services application. For example:

```
cometDSettings:
    cometdSessionExpirationTimeout: 60
    closeHttpSessionOnCometDExpiration: true
    maxSessionsPerBrowser: 2
    multiSessionInterval: 4000
```

And specifies how CometD's session cookie should be handled. For example:

```
cometDSettings:
    cookieHttpOnly: true
    cookieSecure: true
    cookieSameSite: None
```

Cookie options take effect only if **enableSsl** is set to true.

Log header

enableLogHeader

Default Value: `true`
Valid Values: `true`, `false`
Mandatory: No
Specifies whether Web Services includes a header in its main log file. This header contains key information about the Web Services installation, including the version, start time, libraries, and any applicable settings from the **applications.yaml** file.

excludeAppSettings

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
Specifies if application setting should be excluded from the Log Header functionality.

Routing Point Monitoring

enableRPMonitoring

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
Specifies whether Web Services will support call supervision for monitoring routing points.

Switch Prefixes

enableDialingPlanAvayaSwitchPrefixProcessing

Default Value: `false`
Valid Values: `true`, `false`

Mandatory: No
When enabled, Web Services will compare participant numbers with and without prefixes on outbound calls to avoid rendering redundant participants.

dialingPlanAvayaSwitchPrefix

Default Value: 9
Valid Values: Any positive integer
Mandatory: No
Specifies the outbound call prefix used on Avaya switches.

updateOnStartup

> **Important**
>
> In previous releases, a GWS server restart automatically updated global information. Now the updates are set to false by default. If you want to configure the GWS to update all global information, use the following configuration sample:
>
> ```
> updateOnStartup:
>         statistics: true
>         opsCredentials: true
>         features: true
> ```

opsCredentials

Default Value: false
Valid Values: true, false
Mandatory: No
Specifies whether to update the global ops credentials to the values specified in configuration file.

statistics

Default Value: false
Valid Values: true, false
Mandatory: No
Specifies whether to update statistic definitions to the values specified in corresponding configuration file. This option is taken into consideration only on StatNodes.

features

Default Value: false
Valid Values: true, false
Mandatory: No
Specifies whether to update feature definitions to the values specified in corresponding configuration file.

SIP Cluster Support

useEmployeeIdAsAgentLoginForSIPCluster

Default Value: false
Valid Values: true, false
Mandatory: No
Specifies if Web Services has to use the employee ID of the agent as the login ID.

> **Important**
> This option is used in SIP Cluster environments only.

onPremiseSettings

Settings in this section are listed under "onPremiseSettings".

cmeHost

Default Value: None
Valid Values: A valid IP address or host name
Mandatory: No
Specifies the Configuration Server host name (FQDN) or IP.

cmePort

Default Value: None
Valid Values: A valid port
Mandatory: No
Specifies the Configuration Server port.

backupCmeHost

Default Value: None
Valid Values: A valid IP address or host name
Mandatory: No
Specifies the backup Configuration Server host name (FQDN) or IP. You should only configure this option if there is a backup Configuration Server in the Genesys environment and you want high-availability support.

backupCmePort

Default Value: None
Valid Values: A valid port
Mandatory: No

Specifies the backup Configuration Server port. You should only configure this option if there is a backup Configuration Server in the Genesys environment and you want high-availability support.

countryCode

Default Value: None
Valid Values: A two-letter country code
Mandatory: No
The premise contact center's country code. For example, US.

tlsEnabled

Default Value: None
Valid Values: `true`, `false`
Mandatory: No
Specifies whether Web Services should create a secured connection to Configuration Server the first time it starts.

StandardResponse Caching

Overview

Default cache setting is one hour. However, the tree is not cached, only request to UCS is cached.

```
Default timeToLiveSeconds = 3600; maxEntriesLocalHeap = 10000.
```

Example

```
Request to GetRootCategories – it will be cached for 1 hour.
Request to GetCategory(x) – it will be cached for 1 hour.
You make any changes to Category x – you will not receive it for 1 hour.
You make a change to Category y.
You make a request to GetCategory(y) – you will receive the latest from the server and it
will be cached for 1 hour.
```

Cache Managing

You must provide the following settings in the **application.yaml** file to change default parameters for caching:

```
serverSettings:
 cachingSettings:
   dedicatedCacheSettings:
      - cacheName: ContactServerCategoriesCache
        timeToLiveSeconds: <TTL>
        maxEntriesLocalHeap: <Heap size>
      - cacheName: ContactServerStandardResponsesCache
        timeToLiveSeconds: <TTL>
        maxEntriesLocalHeap: <Heap size
```