Genesys Interaction Recording Solution Guide

Configuration Options

4/22/2025

Contents

Configuration Options

You can set the configuration options below in the corresponding sections of the **application.yaml** file on your Interaction Recording Web Services nodes. For details, see Configuring Interaction Recording Web Services.

> **Important**
>
> When editing the **application.yaml** file, the values for the configuration options that are strings must be enclosed in double quotation marks in certain cases. Specifically:
>
> - For string options only, the values `YES`, `NO`, `ON`, `OFF`, `TRUE`, `FALSE` (in upper or lower case) must be quoted.
> - If the option is a boolean (true/false) option, then any of the values in the previous bullet can be used without quotes.
> - Values that look like numbers but are treated as strings (for example; PINs, phone numbers, encryption keys), that begin with leading zeroes must be quoted.
> - Avoid placing leading zeroes on numeric options; doing so will cause your option to be interpreted as an octal value.
>
> For example, specifying `crRegion: NO` (indicating Norway) will be interpreted as `crRegion: FALSE`. Instead, this must be specified using double quotation marks `crRegion: “NO”`.

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 Interaction Recording 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**.

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. This value should be the same as `GWS_HOST` you defined as part of Deploying the Web Application.

port

Default Value: `8080`
Valid Values: A valid port
Mandatory: No
Specifies the port of the Jetty host. 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 sessionCookieName cookie.

enableRequestLog

Default Value: `true`
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.

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.

Name	Mandatory	Default Value	Description
keyStoreProvider	No	None	The keystore provider.
keyStoreType	No	JKS	The keystore 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 peer have to be validated.
trustAll	No	None	Set this option to true if all certificates should be trusted if there is no keystore 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.

Name	Mandatory	Default Value	Description
excludeProtocols	No	None	The array of protocol names (protocol versions) to exclude from use on this engine.

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`.

httpOnly

Default Value: `true`
Valid Values: `true`, `false`
Mandatory: No
If true, it sets an HTTP-only flag for session cookies.

secure

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
If true, it sets a secure cookie flag for session cookies.

sessionCookieName

Default Value: `GIRJSESSID`
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 Interaction Recording Web Services.

sessionCookieName can only contain the following characters:

- Letters: a-z or A-Z
- Digits: 0-9
- Hyphen (-)
- Underscore (_)

cassandraCluster

Settings in this section are listed under **cassandraCluster** for Cassandra 4.1.

native_transport_port

Default Value: `9042`
Valid Values: A valid port
Mandatory: No
Specifies the port used by CQL. This is required if not using the default port.

dataCenterName

Default Value: `datacenter1`
Valid Values: Name of the primary datacenter used by the new CQL driver
Mandatory: No
Name of the primary datacenter used by the new CQL driver. The required value can be found by running `nodetool status` on the Cassandra instance. This is required if not using the default datacenter name.

backupDataCenterName

Default Value: `datacenter1`
Valid Values: Name of the secondary datacenter used by the new CQL driver if there is a secondary datacenter
Mandatory: No
Name of the secondary datacenter used by the new CQL driver if there is a secondary datacenter. The required value can be found by running `nodetool status` on the Cassandra instance. This is required if using a Multi datacenter Cassandra. and not using the default secondary datacenter name.

switchOverUnHealthyNodes

Default Value: `-1`
Valid Values: The number of nodes in the primary Cassandra datacenter that need to fail before RWS will attempt to switch to the backup datacenter.
Mandatory: No
The number of nodes in the primary Cassandra datacenter that need to fail before RWS will attempt to switch to the backup datacenter. The default value is -1, meaning that no attempt to switchover will be made. This is required only if using a Multi datacenter Cassandra.

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: Yes
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 Interaction Recording Web Services, 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: Yes
Specifies the Cassandra node IP addresses 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 IP addresses or host names. This option is intended for deployments that have two separate Cassandra data centers — Interaction Recording 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 or equal to the number of nodes in the cluster
Mandatory: Yes
Specifies a replication factor appropriate for your Cassandra topology. This value must 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: Yes
Specifies the read consistency level appropriate for your Cassandra topology:

Development (1 Cassandra node)	Single Datacenter (1 datacenter with a minimum of three Cassandra nodes)	Two Datacenters (datacenters with a minimum of three Cassandra nodes in each datacenter)
CL_ONE	CL_QUORUM	CL_LOCAL_QUORUM

write_consistency_level

Default Value: None
Valid Values: `CL_ONE`, `CL_QUORUM`, `CL_LOCAL_QUORUM`
Mandatory: Yes
Specifies the write consistency level appropriate for your Cassandra topology:

Development (1 Cassandra node)	Single Datacenter (1 datacenter with a minimum of three Cassandra nodes)	Two Datacenters (datacenters with a minimum of three Cassandra nodes in each datacenter)
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: 4.1.4
Valid Values: `Cassandra version`
Mandatory: No
Specifies the Cassandra version for your Interaction Recording Web Services 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 versions 1.2.x and higher.

truststore

Default Value: None
Valid Values: A valid path.
Mandatory: No
Specifies the path to the truststore.

truststorePassword

Default Value: None
Valid Values: A valid password.
Mandatory: No
Specifies the password for the truststore.

userName

Default Value: None
Valid Values: A valid Cassandra username.
Mandatory: No
Specifies the username if Cassandra is configured to use authentication.

password

Default Value: None
Valid Values: A valid Cassandra password.
Mandatory: No
Specifies the password if Cassandra is configured to use authentication.

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 Interaction Recording 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 Interaction Recording 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`.

undocumentedExternalApiUrl

Default Value: None
Valid Values: A public schema-based URL ending with `/internal-api`.
Mandatory: Yes
Specifies the reachable Interaction Recording Web Services server address for the SpeechMiner UI and the Screen Recording Service. For example, `http://192.0.2.20:8090/internal-api`

Paths

pathPrefix

Default Value:
Valid Values: A valid prefix
Mandatory: No
Specifies a prefix that Interaction Recording 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
```

Interaction Recording 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.

internalPathPrefix

Default Value: Empty

Valid Values: A valid prefix
Mandatory: No
Specifies a prefix that Interaction Recording Web Services adds to the relative URIs that it includes in responses to internal APIs. See pathPrefix for details.

General

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: `false`
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.

> **Important**
>
> If CSRF protection is enabled, then the label/tagging and deletion prevention functionality cannot be used in SpeechMiner, as SpeechMiner does not support CSRF.

Timeouts

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.

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.

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 Interaction Recording 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.

OPS account

opsUserName

Default Value: None
Valid Values: Any alphanumeric value that can include special characters
Mandatory: Yes
Specifies the name of the Interaction Recording Web Services super user. Interaction Recording Web Services creates or updates this user at startup if **opsCredentials** is set to `true` in the **updateOnStartup** section of the **application.yaml** file.

opsUserPassword

Default Value: None
Valid Values: Any alphanumeric value, including special characters
Mandatory: Yes
Specifies the password for the Interaction Recording Web Services super user. Interaction Recording Web Services creates or updates the password for the **ops** user at startup if **opsCredentials** is set to `true` in the **updateOnStartup** section of the **application.yaml** file.

CME credentials

applicationName

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

applicationType

Default Value: None
Valid Values: A valid application type
Mandatory: Yes
The type of the Interaction Recording 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 Interaction Recording 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 Interaction Recording Web Services uses to connect to Configuration Server.

syncNode

Default Value: `false`
Valid Values: `true, false`
Mandatory: Yes (for sync node), No (all other nodes)
Specifies whether the node is the synchronization node. This node is responsible for importing objects from Configuration Server into Cassandra, subscribing to change notifications with Configuration Server, and processing updates.

> **Important**
>
> In each Interaction Recording Web Services cluster or shared Interaction Recording Web Services and Web Services and Applications cluster, if both are deployed, one node in the cluster must be configured as the synchronization node: `syncNode: true`. All other nodes in the cluster must have `syncNode: false`.

ConfigServer String Encoding

configServerDefaultEncoding

Default Value: `windows-1252`
Valid Values: A valid java string encoding
Mandatory: No
The configuration server can be installed in one of two modes. One mode uses UTF-8 for encoding strings; the other uses the default character encoding of the machine that the configuration server is installed on. If you are using UTF-8, RWS will communicate using UTF-8 and this parameter is not used. If you are not using UTF-8, this value should be set to the value of the default string encoding of the machine that the configuration server is installed on.

Call Recording

createCallRecordingCF

Default Value: `false`
Valid Values: `true`, `false`
Mandatory: No
Specifies if the column families required for Call Recording will be created when a contact center is created.

crClusterName

Default Value: None
Valid Values: A valid cluster name
Mandatory: Yes
Specifies the name of the cluster to enable search functionality in Elasticsearch. The value must be the same for all Interaction Recording Web Services nodes in the cluster and must match the **cluster.name** parameter configured in **elasticsearch.yml** for each Elasticsearch node. For example, if there are five nodes in the Interaction Recording Web Services cluster, all five nodes must have the same value as in the **crClusterName** option.

crRegion

Default Value: None
Valid Values: String
Mandatory: Yes
Specifies the name of the region where the Interaction Recording Web Services node is located. Ensure that this value is the same on all RWS nodes.

cryptoSecurityKey

Default Value: None
Valid Values: A valid security key
Mandatory: Yes
Specifies the security key used for encryption for call recording settings stored in the database. The value must be the same for all Interaction Recording Web Services nodes in the cluster. For example, if there are five nodes in the Interaction Recording Web Services cluster, all five nodes must have the same value as in the **cryptoSecurityKey** option.

webDAVMaxConnection

Default Value: `50`
Valid Values: An integer greater than `0`.
Mandatory: No
Specifies the maximum number of WebDAV client TCP connections to each route. When the number of WebDAV client requests to the same WebDAV server are less than this value, a new TCP connection is established for better performance. Otherwise, the new request is queued until any ongoing request finishes.

webDAVMaxTotalConnection

Default value: `10` * value of webDAVMaxConnection
Valid Values: An integer greater than `0`.
Mandatory: No
Specifies the maximum number of TCP connections from the Interaction Recording Web Services node to all WebDAV storage.

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 Interaction Recording 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 address
Mandatory: No
Specifies the unique identifier for the Interaction Recording 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 or empty
Mandatory: No
Specifies the path to a file containing a certificate for a Certificate Authority. The file must be in the `.pem` or `.jks` format (if `.jks`, you can also set jksPassword). The certificate will be used if the IRWS_Cluster application uses Transport Layer Security (TLS) to connect to the Configuration Server, SIP Server, and Interaction Server. If left empty, or if the parameter is not specified, the certificates returned from the servers will not be validated.

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. You can specify an encrypted password. For more information on encrypting a password, see Password Encryption.

webDAVTrustedCA

Default Value: `true`
Valid Values: `true`, `false`, or a path to a file containing a certificate for a Certificate Authority
Mandatory: No
When using a secure connection to the WebDAV Server, controls whether the certificate is validated, and how. If set to `false`, the certificate presented by the WebDAV Server will not be validated. If set to `true`, the certificate presented by the WebDAV Server will be validated by **caCerts** in `$JAVA_HOME/jre/lib/security`. Otherwise, specifies the path to a file containing a certificate for a Certificate Authority. The file must be in the .pem or .jks format (if it is in .jks format, you can also set webDAVJksPassword).

webDAVJksPassword

Default Value: None
Valid Values: Password for the key storage
Mandatory: No
Specifies the password for the key storage set in webDAVTrustedCA when the certificate is in .jks format. You can specify an encrypted password. For more information on encrypting a password, see Password Encryption.

rcsTrustedCA

Default Value: `true`
Valid Values: `true`, `false`, or a path to a file containing a certificate for a Certificate Authority
Mandatory: No
When using a secure connection to the Recording Crypto Server, controls whether the certificate is validated, and how. If set to `false`, the certificate presented by RCS will not be validated. If set to `true`, the certificate presented by RCS will be validated by **caCerts** in `$JAVA_HOME/jre/lib/security`. Otherwise, specifies the path to a file containing a certificate for a Certificate Authority. The file must be in the .pem or .jks format (if it is in .jks format, you can also set rcsJksPassword).

rcsJksPassword

Default Value: None
Valid Values: Password for the key storage
Mandatory: No
Specifies the password for the key storage set in rcsTrustedCA when the certificate is in .jks format. You can specify an encrypted password. For more information on encrypting a password, see Password Encryption.

speechMinerTrustedCA

Default Value: `true`
Valid Values: `true`, `false`, or a path to a file containing a certificate for a Certificate Authority
Mandatory: No
When using a secure connection to the SpeechMiner Interaction Receiver, controls whether the certificate is validated, and how. If set to `false`, the certificate presented by the SpeechMiner Interaction Receiver will not be validated. If set to `true`, the certificate presented by the SpeechMiner Interaction Receiver will be validated by **caCerts** in `$JAVA_HOME/jre/lib/security`. Otherwise, specifies the path to a file containing a certificate for a Certificate Authority. The file must be in the .pem or .jks format (if it is in .jks format, you can also set speechMinerJksPassword).

speechMinerJksPassword

Default Value: None
Valid Values: Password for the key storage
Mandatory: No
Specifies the password for the key storage set in speechMinerTrustedCA when the certificate is in .jks format. You can specify an encrypted password. For more information on encrypting a password, see Password Encryption.

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 Interaction Recording 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, X-CSRF-TOKEN,authorization, ssid, 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 for how long (in seconds) the cross origin settings are cached before being reloaded.
exposedHeaders	No	X-CSRF-HEADER,X-CSRF-TOKEN	Specifies which custom headers are allowed in

Name	Mandatory	Default Value	Description
			cross-origin HTTP responses. This should typically be left at the 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 Interaction Recording 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
retriesOnConflict	No	3	Controls how many times to retry if there is a version conflict when updating a document.
waitToIndexTimeout	No	5000	Specifies the length of time (in milliseconds) that the Interaction Recording Web Services will wait while Elasticsearch is indexing data.
scanReadTimeoutSeconds	No	60	Specifies the length of time that the Interaction Recording Web Services waits for Elasticsearch to return results from setting up a scan and

Name	Mandatory	Default Value	Description
			scroll search request.
countReadTimeoutSeconds	No	60	Specifies the length of time that the Interaction Recording Web Services waits for Elasticsearch to return results from a count search request.
scrollTimeoutSeconds	No	240	Specifies how long Elasticsearch should keep the Search Context alive when handling scan and scroll requests from the Muxer and MLM components. This value must be long enough to process each batch of results. However, it does not need to be long enough to process all data. You can change this value based on the performance results in your environment.
useTransportClient	No	true	Specifies whether Interaction Recording Web Services should use a transport client for Elasticsearch.
transportClient	Yes, if **useTransportClient** is true.	Values specified in TransportClientSettings	Specifies the configuration Interaction Recording Web Services should use for the transport client. For details see TransportClientSettings in the next table.
useRestClient	no	false	Specifies whether Interaction Recording Web Services should use a REST client for Elasticsearch. This is only applicable for Elasticsearch 7.16.3.
restClient	Yes, if **useRestClient** is true.	Values specified in RestClientSettings.	Specifies the configuration Interaction Recording Web Services should use for the REST client. For details, see RestClientSettings in the next table. This is only applicable for Elasticsearch 7.16.3.

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 use sniffing functionality and perform auto-discovery of Elasticsearch nodes in the cluster.
ignoreClusterName	no	false	Specifies if Interaction Recording 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 Interaction Recording Web Services should sample/ping the Elasticsearch nodes listed and connected.

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

```
...
elasticSearchSettings:
    retriesOnConflict: 2
    waitToIndexTimeout: 5000
    useTransportClient: true
    transportClient:
        nodes:
             - {host: 127.0.0.1, port: 9300}
        useSniff: true
        ignoreClusterName: true
        pingTimeout: 10000
        nodesSamplerInterval: 10000
    scanReadTimeoutSeconds: 60
    countReadTimeoutSeconds: 60
    scrollTimeoutSeconds: 240
```

RestClientSettings

Name	Mandatory	Default Value	Description
nodes	Yes, if **useRestClient** is true.	null	Specifies the list of Elasticsearch nodes the REST client should connect to.

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

```
...
elasticSearchSettings:
    retriesOnConflict: 2
    waitToIndexTimeout: 5000
    useTransportClient: false
    transportClient:
        nodes:
             - {host: 127.0.0.1, port: 9300}
        useSniff: false
        ignoreClusterName: false
        pingTimeout: 10000
        nodesSamplerInterval: 10000
    useRestClient: true
    restClient:
        nodes: - {host: 127.0.0.1, port: 9200}
    scanReadTimeoutSeconds: 60
    countReadTimeoutSeconds: 60
    scrollTimeoutSeconds: 240
```

Recording

recordingSettings

Default Value: None
Valid Values:

Name	Mandatory	Default Value	Description
auditLogDeletedFiles	No	None	If set to true, Interaction Recording Web Services generates an audit log for each individual recording file that is deleted.
recordCryptoServerDecryptMaxConnection	No	50	Specifies the maximum TCP connections to each Recording Crypto Server instance defined in local-decrypt-uri-prefix settings. See Screen Recording Local Decrypt URI Prefix for details.
recordCryptoServerDecryptMaxTotalConnection	No	10 * recordCryptoServer	Specifies the maximum TCP connections to all

Name	Mandatory	Default Value	Description
		DecryptMaxConnection	Recording Crypto Server instances defined in local-decrypt-uri-prefix settings. See Screen Recording Local Decrypt URI Prefix for details.
recordCryptoServerDecrypt	SocketTimeout	30000	Specifies the socket timeout, in milliseconds, for TCP connections to Recording Crypto Server instances defined in local-decrypt-uri-prefix settings. See Screen Recording Local Decrypt URI Prefix for details.
keyspaceNameSettingsCache	SecondsTTL	300	Specifies the time to live in seconds of the keyspace name for a given contact center and location from Cassandra in a cache.
regionsSettingsCacheSeconds	TTL	300	Specifies the time to live in seconds of a regions setting for a location stored in Cassandra in a cache.

Mandatory: No
Specifies the configuration for recording in Interaction Recording Web Services. For example:

```
recordingSettings:
    auditLogDeletedFiles: true
    recordCryptoServerDecryptMaxConnection: 50
    recordCryptoServerDecryptMaxTotalConnection: 500
    recordCryptoServerDecryptSocketTimeout: 30000
    regionsSettingsCacheSecondsTTL: 300
```

Screen Recording

screenRecordingSettings

Default Value: None
Valid Values:

Name	Mandatory	Default Value	Description
enableSameSiteCookieForScreenRecordingPlayback		false	Specifies whether Interaction Recording Web Services will return the `SameSite=None` and `Secure` cookie attributes on the cookie used when playing back

Name	Mandatory	Default Value	Description
			screen recordings from the SpeechMiner browser application. **Important:** Before enabling this option, ensure that the connection between the SpeechMiner browser application and RWS is configured to use HTTPS. If you set this option to `true` and are using HTTP, the cookie will not be returned by the browser.
screenRecordingVoiceEnabled	No	false	Specifies whether the current Interaction Recording Web Services node supports screen recording for voice interactions. If set to `false`, the node rejects CometD requests from the Screen Recording Service for agents with the voice channel.
screenRecordingEServicesEnabled	No	false	Specifies whether the current Interaction Recording Web Services node supports screen recording for non-voice interactions. If set to `false`, the node rejects CometD requests from the Screen Recording Service 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 Interaction Recording 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 Interaction Recording Web Services on each request.
contactCenterInfoManagerCacheTTL	No	90	Specifies the TTL for the Interaction Recording Web Services node to

Name	Mandatory	Default Value	Description
			cache contact center information so that the node doesn't have to read the information from Interaction Recording Web Services on each request.

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

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

Screen Recording Connections Reporting

reportingEnabled

Default Value: `false`
Valid Values: `true, false`
Mandatory: No
Enables the Screen Recording Connection Reporting feature.

createReportingCF

Default Value: `false`
Valid Values: `true, false`
Mandatory: No
Specifies if the column families required for Screen Recording Connection reporting will be created when a contact center is created.

connectionInfoHoursTTL

Default Value: `7 * 24`
Valid Values: Integer
Mandatory: No
Specifies the Time To Live (in hours) to use when writing columns to the `src_rep_node_<id>` column family. Screen Recording Service (SR Service) connections older than the Time to Live will not be listed in the SR Service connection information queries.

historyCountsMinutesTTL

Default Value: `24 * 60`
Valid Values: Integer
Mandatory: No
Specifies the Time To Live (in minutes) to use when writing columns to the `src_rep_hist_<id>`

column family. This number determines the maximum number of values that can be reported for a statistic in historic count queries.

Multimedia Disaster Recovery

drMonitoringDelay

Default Value: `1800`
Valid Values: Integer
Mandatory: No
Specifies the interval (in seconds) that will be used for monitoring Disaster Recovery synchronization.

Caching

cachingSettings

Default Value: None
Valid Values:

Name	Mandatory	Default Value	Description
contactCenterFeaturesTTL	No	30	The TTL, in seconds, for contact-center feature IDs in cache.
contactCenterSettingsTTL	No	30	The TTL, in seconds, for contact-center custom settings in cache.

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

```
...
cachingSettings:
   contactCenterFeaturesTTL: 30
   contactCenterSettingsTTL: 30
```

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 set to `true`, DoSFilter headers are inserted into the response.
trackSessions	No	true	If set to `true`, the usage rate is tracked by session if a session exists.
remotePort	No	false	If set to `true` and session tracking is not

Name	Mandatory	Default Value	Description
			used, then the rate is tracked by IP address + port (effectively connection).
ipWhitelist	No	""	A comma-separated list of IP addresses that is not rate limited.

Mandatory: No
Specifies how Interaction Recording 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`.

multiPartResolverMaxUploadSize

Default Value: 536870912
Valid Values: Integer
Mandatory: Yes
This parameter should be aligned with `maxDurationMinutes`, so if you change its value, ensure that you also consider the `maxDurationMinutes` value specified within the Advanced Configuration for the Screen Recording Service section in the Deploying the Screen Recording Service - Advanced Configuration page. The maximum size of a file that can be uploaded by the Screen Recording Service must be less than or equal to the `multiPartResolverMaxUploadSize`.

multiPartResolverMaxInMemorySize

Default Value: 67108864
Valid Values: Integer
Mandatory: Yes
Specifies the maximum allowed size (in bytes) before uploads are written to disk.

Media Life Cycle management

backgroundScheduledMediaOperationsSettings

Default Value: None
Valid Values:

Name	Mandatory	Default Value	Description
enableBackgroundScheduledMediaOperations	No	false	Specifies whether this Interaction Recording Web Services node can perform MLM operations.

Name	Mandatory	Default Value	Description
schedulerThreads	No	4	Specifies the number of scheduler worker threads.
schedulePollingInterval	No	60	Specifies how often, in seconds, Interaction Recording Web Services polls for gir-scheduler settings and synchronizes the rule schedule.
speechMinerMaxConnection	No	20	Specifies the maximum number of concurrent TCP connections for the same route when Interaction Recording Web Services issues API requests to SpeechMiner.
speechMinerMaxTotalConnection	No	-1	Specifies the size of the connection pool when Interaction Recording Web Services issues API requests to SpeechMiner. If the value of this option is less than 1, Interaction Recording Web Services sets the size of the pool to the value speechMinerMaxConnection * 10.
speechMinerSocketTimeout	No	60000	Specifies how long Interaction Recording Web Services should wait, in milliseconds, for the SpeechMiner API response before timing out.
defaultBackupExportURI	No	None	Specifies the location to store backed up recordings. For example, file:///tmp/archLocDefault.
useFullPathInMediaFileBackup	No	false	Specifies whether to include the full path or file name only during an MLM backup operation
enableScanAndScroll	No	false	Specifies whether to turn on the feature where MLM uses Elasticsearch scan and scroll queries to

Name	Mandatory	Default Value	Description
			determine the recording IDs on which to act.
scanIntervalsPerDay	No	24	When MLM is configured to use Elasticsearch scan and scroll queries to determine the recording IDs on which to act, this parameter determines the number of scan intervals used in a day of recordings. Reduce this value to reduce the number of Elasticsearch scan queries performed by an MLM Task for its work, assuming that all other things remain equal. Reducing this value also increases the lifetime of the search context created by each Elasticsearch scan query, which in turn increases the number of open file descriptors in use by Elasticsearch. **Note**: When configuring, ensure that the number of seconds in a day (i.e. 24 * 60 * 60) is exactly divisible by the configured value.

Mandatory: No
Specifies the configuration for Interaction Recording Web Services to schedule purge and backup events. For example:

```
backgroundScheduledMediaOperationsSettings:
    enableBackgroundScheduledMediaOperations: true
    schedulerThreads: 4
    schedulePollingInterval: 60
    speechMinerMaxConnection: 20
    speechMinerMaxTotalConnection: -1
    speechMinerSocketTimeout: 60000
    defaultBackupExportURI:
    useFullPathInMediaFileBackup: false
    enableScanAndScroll: true
    scanIntervalsPerDay: 24
```

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 log in again before the end of this timeout to disable session expiration.
closeHttpSessionOnCometDExpiration	No	true	Enables or disables HTTP session invalidation when CometD times out.
maxSessionsPerBrowser	No	1	Specifies 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 Interaction Recording Web Services application. For example:

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

Log header

enableLogHeader

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

updateOnPremiseInfoInterval

Default Value: `600`
Valid Values: Integer
Mandatory: No
Specifies a period (in seconds) during which the premise environment log header information is updated.

updateOnStartup

opsCredentials

Default Value: `false`
Valid Values: true, false
Mandatory: No
Changes take effect: When the Interaction Recording Web Services server is started or restarted.
Specifies whether to update the stored ops credentials to the values specified in the **opsUserName** and **opsUserPassword** parameters.

features

Default Value: `false`
Valid Values: `true, false`
Mandatory: No
Changes take effect: When the Interaction Recording Web Services server is started or restarted.
Specifies whether to update the supported features to the list specified in the **feature-definitions.json** file. See Enabling features in the Feature Definitions file for details.

onPremiseSettings

Settings in this section are listed under **onPremiseSettings**.

> **Important**

- The following settings should be specified for the sync node (syncNode: true). They are not required on the other nodes in the cluster.
- Note that settings under **onPremiseSettings** are used only once during the first initialization of RWS on the sync node. Further changes in the environment are retrieved from the Configuration Server directly. If a setting is configured incorrectly, please contact Genesys Customer Care for support.

cmeHost

Default Value: None
Valid Values: A valid IP address or host name
Mandatory: Yes (for sync node), No (all other nodes)
Specifies the Configuration Server host name (FQDN) or IP address.

cmePort

Default Value: None
Valid Values: A valid port
Mandatory: Yes (for sync node), No (all other nodes)
Specifies the Configuration Server port.

backupCmeHost

Default Value: None
Valid Values: A valid IP address or host name
Mandatory: Yes (for sync node), No (all other nodes)
Specifies the backup Configuration Server host name (FQDN) or IP address. 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: Yes (for sync node), No (all other nodes)
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: Yes (for sync node), No (all other nodes)
The premise contact center's country code. For example, `"US"`.

tlsEnabled

Default Value: None
Valid Values: `true`, `false`
Mandatory: Yes (for sync node), No (all other nodes)
Specifies whether Interaction Recording Web Services should use a secure connection to the Configuration Server.