Web Real-Time Communications

Genesys Configuration Options Current

1/27/2022

Table of Contents

Web Real-Time Communications Options Reference

Welcome to the Options Reference for Web Real-Time Communications. This document provides full information about all the configuration options that are set on the Web Real-Time Communications application object and in Web Real-Time Communications–related configuration sections on other objects, such as DNs.

> **Important**
>
> This content is under development and might not be comprehensive or completely up to date. Refer to Configuration Options in the *Deployment Guide* for additional information.

Web Real-Time Communications Gateway

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

- ems
- log
- rsmp
- snmp

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

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

object).

Section	Option	Default	Changes Take Effect
ems	logconfig.MFSINK	*|*|*	immediately
ems	metricsconfig.MFSINK	*	immediately
log	all	../logs/rsmplog	immediately
log	check-point	1	immediately
log	compatible-output-priority	false	immediately
log	debug	../logs/rsmplog	immediately
log	expire	20	immediately
log	interaction	../logs/rsmplog	immediately
log	keep-startup-file	false	After restart
log	memory		immediately
log	messagefile		Immediately, if an application cannot find its *.lms file at startup
log	message_format	short	immediately
log	print-attributes	false	immediately
log	segment	10000	immediately
log	spool		immediately
log	standard	../logs/rsmplog	immediately
log	time_convert	local	immediately
log	time_format	time	immediately
log	trace	../logs/rsmplog	immediately
log	verbose	debug	immediately
rsmp	allow-anonymous-user	true	At start or restart
rsmp	allow-ipv6	false	At start or restart
rsmp	codecs	(pcmu,pcma,opus,g729,telephone-event=126,vp8=100,h264=(pt=108,fmtp="[profile-level-id=42000B;packetization-mode=1]"))	At start or restart
rsmp	domain-whitelist		At start or restart
rsmp	enable-https	false	At start or restart
rsmp	enable-transcoding	false	At start or restart
rsmp	http-port	8086	At start or restart
rsmp	http-trace	false	At start or restart
rsmp	https-cert		At start or restart
rsmp	https-cert-key		At start or restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
rsmp	https-trusted-ca		At start or restart
rsmp	reporting-service-type	WebRTC	At start or restart
rsmp	rtp-address		At start or restart
rsmp	rtp-trace-level	1	At start or restart
rsmp	sip-added-codecs	(vp8,h264)	At start or restart
rsmp	sip-address		At start or restart
rsmp	sip-disallowed-codecs		At start or restart
rsmp	sip-no-avpf	true	At start or restart
rsmp	sip-no-rtcpfb	false	At start or restart
rsmp	sip-port	5066	At start or restart
rsmp	sip-preferred-ipversion	ipv4	At start or restart
rsmp	sip-proxy	127.0.0.1	At start or restart
rsmp	sip-register		At start or restart
rsmp	sip-rtp-max-port	9999	At start or restart
rsmp	sip-rtp-min-port	9000	At start or restart
rsmp	sip-srtp-mode	none	At start or restart
rsmp	sip-tls-cert		At start or restart
rsmp	sip-tls-cert-key		At start or restart
rsmp	sip-tls-port	0	At start or restart
rsmp	sip-tls-trusted-ca		At start or restart
rsmp	stun-server		At start or restart
rsmp	turn-passwd		At start or restart
rsmp	turn-relay-type	0	At start or restart
rsmp	turn-server		At start or restart
rsmp	turn-user		At start or restart
rsmp	web-added-codecs	(pcmu,vp8)	At start or restart
rsmp	web-disallowed-codecs		At start or restart
rsmp	web-dtls-certificate	../config/ x509_certificate.pem	At start or restart
rsmp	web-dtls-cipherlist		At start or restart
rsmp	web-dtls-keypassword		At start or restart
rsmp	web-dtls-privatekey		At start or restart
rsmp	web-enable-dtls	true	At start or restart
rsmp	web-ice-addresses		At start or restart
rsmp	web-media-bundle	true	At start or restart
rsmp	web-nack-enabled	true	At start or restart
rsmp	web-pli-always	true	At start or restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
rsmp	web-pli-mintime	1000	At start or restart
rsmp	web-rtcp-mux	true	At start or restart
rsmp	web-rtp-max-port	36999	At start or restart
rsmp	web-rtp-min-port	36000	At start or restart
snmp	timeout	100	At start or restart
Section	**Option**	**Default**	**Changes Take Effect**

ems Section

> This content is under development and might not be comprehensive or completely up to date. For full information, see Configuration Options in the *Deployment Guide*.

logconfig.MFSINK

Default Value: *|*|*
Valid Values: Pipe-delimited ranges for log levels, module IDs, and specifier IDs. Ranges can be comma-separated integers or ranges of integers or "*".
Changes Take Effect: immediately

Controls the log messages that are sent to the MF sink. The format is "levels|moduleIDs|specifierIDs" (repeated if necessary). The values between the pipes can be in the format: "m-n,o,p" (for example, "0-4, 5, 6"). The wildcard character "*" can also be used to indicate all valid numbers. For example: "*|*|*" indicates that all log messages should be sent to the sink. Alternatively, "0,1|0-10|*|4|*|*" indicates that CRITICAL(0) and ERROR(1) level messages with module IDs in the range 0-10 will be sent to the sink; and all INFO(4) level messages will be sent as well.

metricsconfig.MFSINK

Default Value: *
Valid Values: Comma-separated list of metric values or ranges. A metric value must be between 0 and 141 inclusive. The values "*" and blank are also allowed.
Changes Take Effect: immediately

Specifies the metrics that are delivered to the MF Sink. "*" indicates that all metrics will be sent to the sink. Alternatively, "5-10,50-55,70,71" indicates that metrics with IDs 5, 6, 7, 8, 9, 10, 50, 51, 52, 53, 54, 55, 70, and 71 will be sent to the MF sink.

log Section

> This content is under development and might not be comprehensive or completely up to date. For full information, see Configuration Options in the *Deployment Guide*.

all

Default Value: ../logs/rsmplog

Valid Values:

- **stdout** Log events are sent to the standard output (stdout).
- **stderr** Log events are sent to the standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to **network** enables an application to send log events of the standard, interaction, and trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends all log events. The log output types must be separated by a comma when more than one output level is configured.

check-point

Default Value: 1
Valid Values: 0 - 24
Changes Take Effect: immediately

Specifies, in hours, how often the application generates a check point log event, to divide the log into sections of equal time. By default, the application generates this log event every hour. Setting the option to 0 prevents the generation of check-point events.

compatible-output-priority

Default Value: false

Valid Values:

- **true** The log of the level specified by "Log Output Options" is sent to the specified output.
- **false** The log of the level specified by "Log Output Options" and higher levels is sent to the specified output.
Changes Take Effect: immediately
Specifies whether the application uses 6.x output logic.

debug

Default Value: ../logs/rsmplog

Valid Values:

- **stdout** Log events are sent to the standard output (stdout).
- **stderr** Log events are sent to the standard error output (stderr).
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of application performance.
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the debug log level option to **network** enables an application to send log events of the standard, interaction, and trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
Changes Take Effect: immediately
Specifies the outputs to which an application sends the log events of the debug level and higher (that is, log events of the standard, interaction, trace, and debug levels). The log output types must be separated by a comma when more than one output level is configured.

expire

Default Value: 20

Valid Values:

- **false** No expiration; all generated segments are stored.
- **[number] file or [number]** Sets the maximum number of log files to store. Specify a number from 1-100.
- **[number] day** Sets the maximum number of days before log files are deleted. Specify a number from

1-100.
Changes Take Effect: immediately
Determines whether log files expire. If they do, sets the measurement for determining when they expire, along with the maximum number of files (segments) or days before the files are removed.

interaction

Default Value: ../logs/rsmplog

Valid Values:

- **stdout** Log events are sent to the standard output (stdout).
- **stderr** Log events are sent to the standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the interaction log level option to **network** enables an application to send log events of the standard and interaction levels to Message Server.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends the log events of the interaction level and higher (that is, log events of the standard and interaction levels). The log outputs must be separated by a comma when more than one output level is configured.

keep-startup-file

Default Value: false

Valid Values:

- **false** No startup segment of the log is kept.
- **true** A startup segment of the log is kept. The size of the segment equals the value of the segment option.
- **[number] KB** Sets the maximum size, in kilobytes, for a startup segment of the log.
- **[number] MB** Sets the maximum size, in megabytes, for a startup segment of the log.
  Changes Take Effect: After restart
  Specifies whether a startup segment of the log, containing the initial T-Server configuration, is to be kept. If it is, this option can be set to true or to a specific size. If set to true, the size of the initial segment will be equal to the size of the regular log segment defined by the segment option. The value of this option will be ignored if segmentation is turned off (that is, if the segment option set to false).

memory

Default Value:
Valid Values: [string] (memory file name)
Changes Take Effect: immediately

Specifies the name of the file to which the application regularly prints a snapshot of the memory output, if it is configured to do this. The new snapshot overwrites the previously written data. If the application terminates abnormally, this file will contain the latest log messages. Memory output is not recommended for processors with a CPU frequency lower than 600 MHz.

message_format

Default Value: short

Valid Values:

- **short** An application uses compressed headers when writing log records to its log file.
- **full** An application uses complete headers when writing log records to its log file.
  Changes Take Effect: immediately
  Specifies the format of log record headers that an application uses when writing logs in the log file. Using compressed log record headers improves application performance and reduces the log file's size. With the value set to short:
- Headers of the log file or the log file segment contain information about the application (such as the application name, application type, host type, and time zone), whereas single log records within the file or segment omit this information.
- A log message priority is abbreviated to Std, Int, Trc, or Dbg, for standard, interaction, trace, or debug messages, respectively.
- The message ID does not contain the prefix GCTI or the application type ID.
  A log record in the full format looks like this:
  2002-05-07T18:11:38.196 Standard localhost cfg_dbserver GCTI-00-05060 Application started
  A log record in the short format looks like this:
  2002-05-07T18:15:33.952 Std 05060 Application started

messagefile

Default Value:
Valid Values: [string].lms (message file name)
Changes Take Effect: Immediately, if an application cannot find its *.lms file at startup

Specifies the file name for application-specific log events. The name must be valid for the operating system on which the application is running. The option value can also contain the absolute path to the application-specific *.lms file. Otherwise, an application looks for the file in its working directory.

print-attributes

Default Value: false
Valid Values:
Changes Take Effect: immediately

Specifies whether the application attaches extended attributes, if any exist, to log events that it sends to log output. Typically, log events of the interaction log level and audit-related log events contain extended attributes. Setting this option to true enables audit capabilities, but negatively affects performance. Genesys recommends enabling this option for Solution Control Server and Configuration Server when using audit tracking. For other applications, refer to Genesys Combined Log Events Help to find out whether an application generates interaction-level and audit-related log events; if it does, enable the option only when testing new interaction scenarios.

segment

Default Value: 10000

Valid Values:

- **false** No segmentation is allowed.
- **[number] KB or [number]** Sets the maximum segment size, in kilobytes. The minimum segment size is 100 KB.
- **[number] MB** Sets the maximum segment size, in megabytes.
- **[number] hr** Sets the number of hours for the segment to stay open. The minimum number is 1 hour.
  Changes Take Effect: immediately
  Specifies whether there is a segmentation limit for a log file. If there is, sets the mode of measurement, along with the maximum size. If the current log segment exceeds the size set by this option, the file is closed and a new one is created.

spool

Default Value:
Valid Values: [path] (the folder, with the full path to it)
Changes Take Effect: immediately

Specifies the folder, including full path to it, in which an application creates temporary files related to network log output. If you change the option value while the application is running, the change does not affect the currently open network output.

standard

Default Value: ../logs/rsmplog

Valid Values:

- **stdout** Log events are sent to the standard output (stdout).
- **stderr** Log events are sent to the standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the standard log level option to **network** enables an application to send log events of the standard level to Message Server.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends the log events of the standard level. The log output types must be separated by a comma when more than one output level is configured.

time_convert

Default Value: local
Valid Values:
Changes Take Effect: immediately

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

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

time_format

Default Value: time
Valid Values:
Changes Take Effect: immediately

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

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

trace

Default Value: ../logs/rsmplog

Valid Values:

- **stdout** Log events are sent to the standard output (stdout).
- **stderr** Log events are sent to the standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the trace log level option to **network** enables an application to send log events of the standard, interaction, and trace levels to Message Server.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends the log events of the trace level and higher (that is, log events of the standard, interaction, and trace levels). The log outputs must be separated by a comma when more than one output level is configured.

verbose

Default Value: debug

Valid Values:

- **all** All log events (that is, log events of the standard, trace, interaction, and debug levels) are generated.

- **debug** The same as all.
- **trace** Log events of the trace level and higher (that is, log events of the standard, interaction, and trace levels) are generated, but log events of the debug level are not generated.
- **interaction** Log events of the interaction level and higher (that is, log events of the standard and interaction levels) are generated, but log events of the trace and debug levels are not generated.
- **standard** Log events of the standard level are generated, but log events of the interaction, trace, and debug levels are not generated.
- **none** No output is produced.
  Changes Take Effect: immediately
  Determines whether a log output is created. If it is, specifies the minimum level of log events generated. The log events levels, starting with the highest priority level, are standard, interaction, trace, and debug.

rsmp Section

> This content is under development and might not be comprehensive or completely up to date. For full information, see Configuration Options in the *Deployment Guide*.

allow-anonymous-user

Default Value: true
Valid Values:
Changes Take Effect: At start or restart

Set this to true (default) to enable anonymous users to sign-in to the WebRTC Gateway. If set to false then only registered users for SIP Server can sign-in.

allow-ipv6

Default Value: false
Valid Values:
Changes Take Effect: At start or restart

Controls whether IPv6 is allowed in the WebRTC Gateway.

codecs

Default Value: (pcmu,pcma,opus,g729,telephone-event=126,vp8=100,h264=(pt=108,fmtp="[profile-level-id=42000B;packetization-mode=1]"))
Valid Values:
Changes Take Effect: At start or restart

Codecs that are not listed here will not be used in an offer or answer. The codec's clock rate (in Hz) can also be specified with the name following a '/'. The codecs currently supported are: pcmu (G.711 mu-Law), pcma (G.711 A-Law), g722, g723 (G.723.1), g729 (G.729/a/b), iLBC, iSAC/16000, iSAC/32000, vp8, h264, telephone-event and opus (non-transcoding case). A default payload type number can be specified using the format name=<pt>, or name=(pt=<pt>). The latter format needs to be used if an fmtp is to be specified, which will be specified as fmtp=<fmtp>. A comma is used as a separator between the different values. All or part of the fmtp value can be enclosed within square brackets, where those brackets will be removed when used in an offer, and in the case of an answer, the brackets and the content will be replaced by the fmtp value from the remote offer.

domain-whitelist

Default Value:
Valid Values:
Changes Take Effect: At start or restart

A list of comma separated domain values that are used to match the domain in the Origin header of HTTP requests. If there is no match, a "403 Forbidden" error will be returned, although an empty (default) whitelist will disallow this checking altogether. Each domain entry may have wildcard character '*' to specify arbitrary scheme, port or sub-domains. Here is a sample whitelist: "https://my.foo.com:8081, http://*.foo2.com, *://*.sub.foo3.com:*, *foo4.com". A '*' at start would match HTTP or HTTPS. If it is immediately followed by a domain name or if a '*' comes after "://" before the domain name, then any sub-domain with the specified name will match; otherwise, domain names will have to exactly match. Also, ":*" at the end would match any port. If no port specified, however, then the default HTTP port 80 is assumed.

enable-https

Default Value: false
Valid Values:
Changes Take Effect: At start or restart

Enables HTTPS

enable-transcoding

Default Value: false
Valid Values:
Changes Take Effect: At start or restart

Transcoding of audio and/or video between the SIP and Web sides is enabled this value is set to true. Otherwise, transcoding will be disabled. When enabled, transcoding will be activated for a media type, only when there is no common codec negotiated between the sides, or when a codec sent by one side is not supported by the other side.

http-port

Default Value: 8086
Valid Values:
Changes Take Effect: At start or restart

HTTP or HTTPS port

http-trace

Default Value: false
Valid Values:
Changes Take Effect: At start or restart

Traces HTTP requests and responses

https-cert

Default Value:
Valid Values:
Changes Take Effect: At start or restart

For Windows, the thumbprint obtained from the user certificate generated for the host. For Linux, the

fullpath of the host certificate file (.pem).

https-cert-key

Default Value:
Valid Values:
Changes Take Effect: At start or restart

Applicable for Linux only. The fullpath of the host private key file (.pem).

https-trusted-ca

Default Value:
Valid Values:
Changes Take Effect: At start or restart

Applicable for Linux only. The fullpath of the Certificate Authority file (.pem).

reporting-service-type

Default Value: WebRTC
Valid Values:
Changes Take Effect: At start or restart

SIP calls are reported out of the box when SIP Server and ICON are configured. When this parameter is set, the service_type key-value pair is sent to SIP Server and then reported to ICON. This allows the reports for the WebRTC service to be filtered based on the service type specified here. To disable the sending of a service type set this parameter value to "none".

rtp-address

Default Value:
Valid Values:
Changes Take Effect: At start or restart

Allows for configuration of a specific IP address for SDP c= line. If not set, the stack will attempt to detect the IP address automatically. This is useful for AWS instances or multi-homed hosts. For example, in an AWS instance you can set this to the elastic-IP. This setting applies to the SIP side only.

rtp-trace-level

Default Value: 1

Valid Values:

- **0** Print "key" packets only (1st RTP/RTCP and last RTCP) to keep log small.
- **1** Print RTP/RTCP packets periodically, but no more than 1 pkt per second.
- **2** Print more often, and always print all errors and "bad" packets.
- **3** Print a few RTP packets per second and all RTCP and "bad" packets.
- **4** Print ALL packets - WARNING: log will be huge, may affect performance.
  Changes Take Effect: At start or restart
  The RTP trace level controls how many packets are printed into the log.

sip-added-codecs

Default Value: (vp8,h264)
Valid Values:
Changes Take Effect: At start or restart

When transcoding is enabled, codecs from this list will be appended to the codec list for offers to a SIP endpoint, after removing any codecs that are already in the original offer. If not specified here, the pt and the fmtp values will be used from the list specified in the codecs option. Note that at least one video codec should be specified, and this codec should most likely be supported by the SIP side. Otherwise, the call may fail even if transcoding is supported. For example, if the Web side offers only VP8, and the SIP side only supports H.264, sip-added-codecs will need to contain h264. If a common audio codec is disallowed on one side, then it should be added to the other side for similar reasons. For video upgrade case on the SIP side, with REFER for example, it is good to have VP8 too.

sip-address

Default Value:
Valid Values:
Changes Take Effect: At start or restart

Allows for configuration of a specific IP address for SIP Via or Contact. If not set, the stack will attempt to detect the IP address automatically. This is useful for AWS instances or multi-homed hosts. For example, in an AWS instance you can set this to the elastic-IP.

sip-disallowed-codecs

Default Value:
Valid Values:
Changes Take Effect: At start or restart

Disallowed codecs for the SIP side. An offer or answer to the SIP side may not use any of these codecs.

sip-no-avpf

Default Value: true
Valid Values:
Changes Take Effect: At start or restart

Set this to true in order not to negotiate AVPF in SDP on the SIP side (RFC4585). This is necessary to work with SIP endpoints that do not support AVPF. Note that regardless of the value of this option, if sip-no-rtcpfb = false, RTCP feedback messages will be forwarded to the SIP side. These settings are useful for a Chrome-to-Chrome call.

sip-no-rtcpfb

Default Value: false
Valid Values:
Changes Take Effect: At start or restart

If set to false, RTCP feedback messages sent by a WebRTC client in accordance with RFC4585 will be forwarded to the corresponding SIP endpoint in a call. A true value will disable this. Note that even though endpoints should ignore RTCP packets of unknown types, some may have issues with this.

sip-port

Default Value: 5066
Valid Values:
Changes Take Effect: At start or restart

SIP Port

sip-preferred-ipversion

Default Value: ipv4
Valid Values:
Changes Take Effect: At start or restart

Preferred IP version to be used for SIP.

sip-proxy

Default Value: 127.0.0.1
Valid Values:
Changes Take Effect: At start or restart

The SIP Proxy and Registrar to be used by the WebRTC Gateway. In all scenarios a Genesys SIP Server is specified as the proxy and registrar.

sip-register

Default Value:
Valid Values:
Changes Take Effect: At start or restart

The list of DNs configured in SIP Server for registration.

sip-rtp-max-port

Default Value: 9999
Valid Values:
Changes Take Effect: At start or restart

UDP port range for SIP-side RTP connection.

sip-rtp-min-port

Default Value: 9000
Valid Values:
Changes Take Effect: At start or restart

UDP port range for SIP-side RTP connection.

sip-srtp-mode

Default Value: none
Valid Values:
Changes Take Effect: At start or restart

SRTP mode that is to be used in SDP negotiation on the SIP side.

sip-tls-cert

Default Value:
Valid Values:
Changes Take Effect: At start or restart

For Windows, the thumbprint obtained from the user certificate generated for the host. For Linux, the fullpath of the host certificate file (.pem)

sip-tls-cert-key

Default Value:
Valid Values:
Changes Take Effect: At start or restart

Applicable for Linux only. The fullpath of the host private key file (.pem).

sip-tls-port

Default Value: 0
Valid Values:
Changes Take Effect: At start or restart

SIP TLS Port. To disable TLS transport for SIP traffic altogether, set to 0.

sip-tls-trusted-ca

Default Value:
Valid Values:
Changes Take Effect: At start or restart

Applicable for Linux only. The fullpath of the Certificate Authority file (.pem).

stun-server

Default Value:
Valid Values:
Changes Take Effect: At start or restart

Optional STUN server specification (port may be omitted, if default STUN port 3478 is used). Only local addresses are gathered when STUN or TURN is not configured.

turn-passwd

Default Value:
Valid Values:
Changes Take Effect: At start or restart

The TURN password to use for the allocation.

turn-relay-type

Default Value: 0
Valid Values:
Changes Take Effect: At start or restart

The type of relay to use. TCP(1) and UDP(0) are supported; TLS is not supported. The default is UDP.

turn-server

Default Value:
Valid Values:
Changes Take Effect: At start or restart

Optional TURN server specification (port may be omitted, if default TURN port 3478 is used). Only local addresses are gathered when STUN or TURN is not configured.

turn-user

Default Value:
Valid Values:
Changes Take Effect: At start or restart

The TURN username to use for the allocation.

web-added-codecs

Default Value: (pcmu,vp8)
Valid Values:
Changes Take Effect: At start or restart

When transcoding is enabled, codecs from this list will be appended to the codec list for offers to a WebRTC endpoint, after removing any codecs that are already in the original offer. The other comments for sip-added-codecs are applicable here as well.

web-disallowed-codecs

Default Value:
Valid Values:
Changes Take Effect: At start or restart

Disallowed codecs for the WebRTC side. An offer or answer to the Web side may not use any of these codecs.

web-dtls-certificate

Default Value: ../config/x509_certificate.pem
Valid Values:
Changes Take Effect: At start or restart

Path of the X.509 certificate file to be used with Web-side DTLS. This file can also contain the private key for the certificate, in which case web-dtls-privatekey does not need to be set. The certificate file is mandatory for DTLS to work. The default certificate already contains the private key.

web-dtls-cipherlist

Default Value:
Valid Values:
Changes Take Effect: At start or restart

A list of cipher strings to be used with DTLS on the Web side. For information on the format, see http://www.openssl.org/docs/apps/ciphers.html#CIPHER_STRINGS. The default cipher string should work well.

web-dtls-keypassword

Default Value:
Valid Values:
Changes Take Effect: At start or restart

The password for the private key specified using web-dtls-privatekey, if used.

web-dtls-privatekey

Default Value:
Valid Values:
Changes Take Effect: At start or restart

Path of the private key file for the certificate specified in web-dtls-certificate. This parameter is not necessary if the certificate file also contains the private key.

web-enable-dtls

Default Value: true
Valid Values:
Changes Take Effect: At start or restart

When this is set to true, DTLS-SRTP (RFC 5763) will be enabled on the Web side. When enabled, it will be signalled in an SDP offer sent

by the gateway using the fingerprint attributes, though there will also be crypto attributes in SDP for SDES-SRTP (RFC 4568) support. When an offer or answer comes in with only crypto attributes, then SDES-SRTP will still be supported. When this is set to false, only SDES-SRTP will be supported.

web-ice-addresses

Default Value:
Valid Values:
Changes Take Effect: At start or restart

Allows for configuration of a local IP address' list to be used with ICE on the Web/ROAP side. Comma is the delimiter, and each IP address could be IPv4 or IPv6 (no need for square brackets). These addresses are used by ICE to gather host candidates.

web-media-bundle

Default Value: true
Valid Values:
Changes Take Effect: At start or restart

Set this to true to enable media bundling on the ROAP side (see http://tools.ietf.org/html/draft-ietf-mmusic-sdp-bundle-negotiation-03). When enabled, it will be signalled in an SDP offer sent by the gateway, and it will be accepted from an inbound SDP offer. If both sides agree, then the same media port will be used for both audio and video. Set this to false if media bundling is not to be used.

web-nack-enabled

Default Value: true
Valid Values:
Changes Take Effect: At start or restart

Set this to true (default) to enable RTCP NACK (transport layer) feedback messages as per RFC4585. Set this to false to disable this feature. The minimum time between two NACK messages is currently restricted to one second.

web-pli-always

Default Value: true
Valid Values:
Changes Take Effect: At start or restart

If this parameter is set to true and web-pli-mintime is nonzero, RTCP PLI feedback messages (RFC4585) will be sent on a Web-side video leg at every web-pli-mintime interval, regardless of transcoding or packet losses.

web-pli-mintime

Default Value: 1000
Valid Values: The parameter must be an integer.
Changes Take Effect: At start or restart

The minimum time period, in milliseconds, between two RTCP PLI feedback messages (RFC4585) that can be sent on a Web-side video leg. If this value is 0, PLI transmission is disabled. The actual time between two PLI messages depends on various things: if web-pli-always is true, one message will be sent every web-pli-mintime milliseconds. Otherwise, if transcoding is on, a message will be sent when the number of lost packets during web-pli-mintime exceed a specific threshold.

web-rtcp-mux

Default Value: true
Valid Values:
Changes Take Effect: At start or restart

Set this to true to enable rtcp-mux on the ROAP side, as per RFC 5761. When enabled, it will be signalled in an SDP offer sent by the gateway, and it will be accepted from an inbound SDP offer. If both sides agree, then the same port will be used for both RTP and RTCP. Set this to false if rtcp-mux is not to be used. Note: If web-rtcp-mux is false, then web-media-bundle cannot be true, as it would not make sense.

web-rtp-max-port

Default Value: 36999
Valid Values:
Changes Take Effect: At start or restart

Maximum UDP port value for ICE (ROAP-side RTP connection). If not specified or zero, then ICE agent is free to select ports by itself (ports in the recommended range of 36000 through 36999 are opened in both Genesys and Amazon cloud firewalls).

web-rtp-min-port

Default Value: 36000
Valid Values:
Changes Take Effect: At start or restart

Minimum UDP port value for ICE (ROAP-side RTP connection). If not specified or zero, then ICE agent is free to select ports by itself (ports in the recommended range of 36000 through 36999 are opened in both Genesys and Amazon cloud firewalls).

snmp Section

> This content is under development and might not be comprehensive or completely up to date. For full information, see Configuration Options in the *Deployment Guide*.

timeout

Default Value: 100
Valid Values: The parameter must be an integer value greater than zero.
Changes Take Effect: At start or restart

The maximum amount of time that SNMP can wait for a new task. This value is specified in milliseconds.