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

Web Real-Time Communications Deployment Guide

Configuration Options Reference

12/14/2025

Contents

Configuration Options Reference

The WebRTC configuration options are listed below. Click on an option name to display its properties.

ems

logconfig.MFSINK

logconfig.MFSINK (MF Sink Log Filter)			
Description	**Valid values**	**Default value**	**Takes effect**
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.	Pipe-delimited ranges for log levels, module IDs, and specifier IDs. Ranges can be comma-separated integers or ranges of integers or "*".	*|*|*	immediately

metricsconfig.MFSINK

metricsconfig.MFSINK (MF Sink Metrics Filter)			
Description	**Valid values**	**Default value**	**Takes effect**
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.	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.	*	immediately

log

all

all (Output for level all)			
Description	**Valid values**	**Default value**	**Takes effect**
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.	• **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	../logs/rsmplog	immediately

	the application's working directory.		

check-point

check-point (Check point interval)			
Description	**Valid values**	**Default value**	**Takes effect**
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.	0 - 24	1	immediately

compatible-output-priority

compatible-output-priority (Enable 6.X compatible log output priority)			
Description	**Valid values**	**Default value**	**Takes effect**
Specifies whether the application uses 6.x output logic.	• **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.	false	immediately

debug

debug (Output for level debug)			
Description	**Valid values**	**Default value**	**Takes effect**
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	• **stdout** — Log events are sent to the standard output (stdout). • **stderr** — Log events are sent to the	../logs/rsmplog	immediately

output types must be separated by a comma when more than one output level is configured.	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.		

expire

expire (Log Expiration)			
Description	**Valid values**	**Default value**	**Takes effect**
Determines whether log files expire. If they do, sets the measurement for determining when they expire, along with the maximum number	• **false** — No expiration; all generated segments are stored.	20	immediately

of files (segments) or days before the files are removed.	• **[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.		

interaction

interaction (Output for level interaction)

Description	Valid values	Default value	Takes effect
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.	• **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	../logs/rsmplog	immediately

	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.		

keep-startup-file

keep-startup-file (Keep startup log file)

Description	Valid values	Default value	Takes effect
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).	- **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.	false	After restart

memory

memory (Memory snapshot file name)

Description	Valid values	Default value	Takes effect
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	[string] (memory file name)	(blank)	immediately

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

message_format (Log messages format)			
Description	**Valid values**	**Default value**	**Takes effect**
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	• **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.	short	immediately

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

messagefile (Message file)			
Description	**Valid values**	**Default value**	**Takes effect**
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.	[string].lms (message file name)	(blank)	Immediately, if an application cannot find its *.lms file at startup

print-attributes

print-attributes (Enable printing extended attributes)			
Description	**Valid values**	**Default value**	**Takes effect**
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	• **true** Attaches extended attributes, if any exist, to a log event sent to log output. • **false** Does not attach extended attributes to a log event sent to log output.	false	immediately

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

segment (Log Segmentation)

Description	Valid values	Default value	Takes effect
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.	• **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.	10000	immediately

spool

spool (Folder for the temporary network log output files)

Description	Valid values	Default value	Takes effect
Specifies the folder, including full path to it, in which an application creates temporary files related to network log	[path] (the folder, with the full path to it)	(blank)	immediately

output. If you change the option value while the application is running, the change does not affect the currently open network output.			

standard

standard (Output for level standard)			
Description	**Valid values**	**Default value**	**Takes effect**
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.	• **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	../logs/rsmplog	immediately

	working directory.		

time_convert

time_convert (Time generation for log messages)			
Description	**Valid values**	**Default value**	**Takes effect**
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).	- **local** - **utc**	local	immediately

time_format

time_format (Time format for log messages)			
Description	**Valid values**	**Default value**	**Takes effect**
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	- **time** - **locale** - **ISO8601**	time	immediately

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

trace (Output for level trace)			
Description	**Valid values**	**Default value**	**Takes effect**
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.	• **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**	../logs/rsmplog	immediately

	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.		

verbose

verbose (Verbose Level)			
Description	**Valid values**	**Default value**	**Takes effect**
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.	• **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	debug	immediately

	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.		

rsmp

allow-anonymous-user

allow-anonymous-user (Allow Anonymous User)			
Description	**Valid values**	**Default value**	**Takes effect**
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.	true, false	true	At start or restart

allow-ipv6

allow-ipv6 (Allow IPv6)			
Description	**Valid values**	**Default value**	**Takes effect**
Controls whether IPv6 is allowed in the WebRTC Gateway.	true, false	false	At start or restart

codecs

codecs (Supported and Default Media Codecs)			
Description	**Valid values**	**Default value**	**Takes effect**

Codecs that are not listed here will not be used in an offer or answer. The codecs currently supported are: • pcmu (G.711 mu-Law) • pcma (G.711 A-Law) • g722 • g729 (G.729/a/b) • opus (non-transcoding case) • iSAC/16000 (non-transcoding case) • iSAC/32000 (non-transcoding case) • telephone-event • vp8 • h264	A comma separated list of supported codecs (from the Description column) within brackets. A codec's clock rate (in Hz) can optionally be specified after its name followed by a '/'. 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. See the default value for an example.	(g722,pcmu,pcma,opus,g729,telephone-event=126,vp8=100,h264=(pt=108,fmtp= "[profile-level-id=42000B;packetization-mode=1]"))	At start or restart

domain-whitelist

domain-whitelist (List of allowed domains)			
Description	**Valid values**	**Default value**	**Takes effect**
Specifies a comma-separated white-list of allowed domains. A wildcard character (*) will be allowed in a domain value for specifying an arbitrary scheme, sub-domain, or port, as illustrated below: • *://sub.foo.com:8080—Any URL scheme, that is, either `http` or `https`, is accepted. • https://*.foo.com:8090—Any sub-domain of `foo.com` is accepted. • http://*.foo.com:*—Any port number or sub-domain is accepted.	See description	(blank)	At start or restart

• *foo.com:*—Any scheme, port, or sub-domain is accepted. Note that if the port number is not specified, then the default HTTP port 80 is assumed. • A check will be performed against this list only if the request contains an `Origin` header. Requests without an `Origin` header are not necessarily Cross-Origin Resource Sharing (CORS) requests. If the domain value in the `Origin` header matches any of the values in the white-list, then the request will be accepted, and the `Access-Control-Allow-Origin` header in the response will be populated with the `Origin` value. • If the value of the white-list is empty (which is the default), then CORS checking will be disabled. The `Access-Control-Allow-Origin` header in the response will still be set using the `Origin` value in the request, if there is one; otherwise, the value of this header will be set to `*`. • If the white-list contains valid values, and the `Origin` header doesn't exist or match any of the white-list domains,			

then the request will be rejected with an HTTP response code of `403 Forbidden`.			

enable-https

enable-https (Enable HTTPS)			
Description	**Valid values**	**Default value**	**Takes effect**
Enables HTTPS. When set to true, the other https-* parameters need to be set correctly using the host's security certificate as well. When enabled, the WebRTC Gateway supports secure HTTPS requests only. Non-secure HTTP requests will not work. Note that HTTPS is required with the latest Chrome browser by default. If an HTTPS proxy is used between the browser/client and the gateway, and it can convert the HTTPS requests to HTTP, then HTTPS does not need to be enabled here.	true, false	false	At start or restart

enable-transcoding

enable-transcoding (Enable Transcoding)			
Description	**Valid values**	**Default value**	**Takes effect**
Transcoding of audio and/or video between the SIP and Web sides is enabled if 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	true, false	true	At start or restart

side.			

http-port

http-port (HTTP Port)			
Description	**Valid values**	**Default value**	**Takes effect**
The HTTP or HTTPS port used for WebRTC signaling. Port 443 is recommended for HTTPS.		8086	At start or restart

https-cert

https-cert (HTTPS Certificate)			
Description	**Valid values**	**Default value**	**Takes effect**
For Windows, the thumbprint obtained from the user certificate generated for the host. For Linux, the fullpath of the host certificate file (.pem).		(blank)	At start or restart

https-cert-key

https-cert-key (HTTPS Certificate Key)			
Description	**Valid values**	**Default value**	**Takes effect**
Applicable for Linux only. The fullpath of the host private key file (.pem).		(blank)	At start or restart

https-trusted-ca

https-trusted-ca (HTTPS Certificate Authority)			
Description	**Valid values**	**Default value**	**Takes effect**
Applicable for Linux only. The fullpath of the Certificate Authority file (.pem).		(blank)	At start or restart

http-trace

http-trace (HTTP Trace)			
Description	**Valid values**	**Default value**	**Takes effect**
Traces HTTP requests and responses	true, false	false	At start or restart

reporting-service-type

reporting-service-type (WebRTC Reporting Service Type)

Description	Valid values	Default value	Takes effect
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".		WebRTC	At start or restart

rtp-address

rtp-address (RTP Address)

Description	Valid values	Default value	Takes effect
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.		(blank)	At start or restart

rtp-trace-level

rtp-trace-level (RTP Trace Level)

Description	Valid values	Default value	Takes effect
The RTP trace level controls how many packets are printed into the log.	• **0** — Print "key" packets only (1st RTP/RTCP and last RTCP) to keep log small. • **1** — Print RTP/RTCP	1	At start or restart

	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.		

sip-added-codecs

sip-added-codecs (SIP Added Codecs)			
Description	**Valid values**	**Default value**	**Takes effect**
When transcoding is enabled, codecs from this list will be appended to the codec list for offers to a SIP endpoint, except for the codecs that are already in the original offer. Note that all codecs in an offer from one side will be added to the resulting offer to the other side.	List of codecs using the same format as codecs option. 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. Note, however, that the answer to the Web side will contain only H.264 based on the reply from the SIP side, unless web-added-codecs contains vp8. This may not be an issue for audio, given that pcmu is supported by both sides. However, if a common audio codec is disallowed on one side, then it should be added to the other side for similar reasons as those given for video codecs.	(vp8,h264)	At start or restart

sip-address

sip-address (SIP Address)			
Description	**Valid values**	**Default value**	**Takes effect**
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.		(blank)	At start or restart

sip-disallowed-codecs

sip-disallowed-codecs (SIP Disallowed Codecs)			
Description	**Valid values**	**Default value**	**Takes effect**
Disallowed codecs for the SIP side. An offer or answer to the SIP side may not use any of these codecs.	List of codecs using the same format as the codecs option. No need to specify "pt" or "fmpt" for a codec.	(blank)	At start or restart

sip-no-avpf

sip-no-avpf (SIP Side AVPF Negotiation)			
Description	**Valid values**	**Default value**	**Takes effect**
Set this to true in order not to negotiate AVPF in SDP on the SIP side (RFC 4585). 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.	true, false	true	At start or restart

sip-no-rtcpfb

sip-no-rtcpfb (Forwarding RTCP Feedback Messages to SIP Side)			
Description	**Valid values**	**Default value**	**Takes effect**
If set to false, RTCP feedback messages sent by a WebRTC client in accordance with (RFC	true, false	false	At start or restart

4585) 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

sip-port			
Description	**Valid values**	**Default value**	**Takes effect**
Local port used for SIP signaling.		5066	At start or restart

sip-preferred-ipversion

sip-preferred-ipversion (Preferred IP version to be used for SIP)			
Description	**Valid values**	**Default value**	**Takes effect**
Preferred IP version to be used for SIP.	• **ipv4** IPv4 • **ipv6** IPv6	ipv4	At start or restart

sip-proxy

sip-proxy (SIP Proxy)			
Description	**Valid values**	**Default value**	**Takes effect**
The IP address(es) or the FQDN(s) of one or two (in the case of HA) SIP Server(s), separated by a comma. Optionally the port can be specified for each address, separated by a colon (:). If the default SIP port 5060 is used, it can be omitted. In all scenarios, Genesys SIP Servers are specified, and are used by the WebRTC Gateway as both SIP Proxy and Registrar. Only one address is used at a time, and the gateway switches to the other when a timeout is	It should be in the following format: <IP-address|FQDN>[:<port>][,<IP-address|FQDN>[:<port>]]	127.0.0.1	At start or restart

detected with a SIP request. Therefore, warm failover can be achieved by specifying two SIP Servers configured in HA mode.			

sip-proxy-srv

sip-proxy-srv			
Description	**Valid values**	**Default value**	**Takes effect**
The DNS SRV address for the HA SIP Server pair (without the port number), of which the addresses are specified using the `sip-proxy` option. When a SIP request arrives with the SRV address, the gateway will translate it to the currently active SIP Server address and use it in its response.		(blank)	At start or restart

sip-register

sip-register (List of DNs for Registration)			
Description	**Valid values**	**Default value**	**Takes effect**
A list of comma separated entries that specify DNs configured in the SIP Server. Any web client that registers with the gateway using an ID that matches any one of these DNs will be registered with the SIP Server by the gateway, so that it can receive calls via the SIP Server and the gateway. Therefore, a new deployment should set this parameter correctly before it can work with the SIP Server.	Each entry can be a single DN, a range of DNs specified with two hard coded values separated by a hyphen (-), or a range of DNs specified using wildcard characters (* and/or ?). A valid DN string contains only digits [0-9], ‘+’ (as prefix), and/or the wildcard characters. Any leading zeros are preserved. Example: `1020,2020-2050,003000,556*,100*10,123??78,+408555`	(blank)	At start or restart

sip-rtp-max-port

sip-rtp-max-port (SIP-side Max RTP Port)			
Description	**Valid values**	**Default value**	**Takes effect**
UDP port range for SIP-		9999	At start or restart

side RTP connection.			

sip-rtp-min-port

sip-rtp-min-port (SIP-side Min RTP Port)			
Description	**Valid values**	**Default value**	**Takes effect**
UDP port range for SIP-side RTP connection.		9000	At start or restart

sip-srtp-mode

sip-srtp-mode (SIP Side SRTP Mode)			
Description	**Valid values**	**Default value**	**Takes effect**
SRTP mode that is to be used in SDP negotiation on the SIP side.	• **none** no SRTP will be used • **optional** offer two m-lines with and without SRTP (for each media), and accept either • **strict** offer secure option only with SRTP; reject any non-secure offers	none	At start or restart

sip-tls-cert

sip-tls-cert (SIP TLS Certificate)			
Description	**Valid values**	**Default value**	**Takes effect**
For Windows, the thumbprint obtained from the user certificate generated for the host. For Linux, the fullpath of the host certificate file (.pem)		(blank)	At start or restart

sip-tls-cert-key

sip-tls-cert-key (SIP TLS Certificate Key)			
Description	**Valid values**	**Default value**	**Takes effect**
Applicable for Linux only. The fullpath of the host private key file (.pem).		(blank)	At start or restart

sip-tls-port

sip-tls-port (SIP TLS Port)			
Description	**Valid values**	**Default value**	**Takes effect**
SIP TLS Port. To disable TLS transport for SIP traffic altogether, set to 0.		0	At start or restart

sip-tls-trusted-ca

sip-tls-trusted-ca (SIP TLS Certificate Authority)			
Description	**Valid values**	**Default value**	**Takes effect**
Applicable for Linux only. The fullpath of the Certificate Authority file (.pem).		(blank)	At start or restart

stun-server

stun-server (STUN Server)			
Description	**Valid values**	**Default value**	**Takes effect**
Optional STUN server specification (port may be omitted, if default STUN port 3478 is used). When the gateway is in a private network with only the host's private address visible to it, a STUN server sitting outside that network may be required by the ICE processing for gathering the host's public (server reflexive) address. Only local addresses are gathered when STUN or TURN is not configured.	<IP-address|FQDN>[:<port>], where port can be omitted, if default port 3478 is used.	(blank)	At start or restart

turn-passwd

turn-passwd (TURN Password)			
Description	**Valid values**	**Default value**	**Takes effect**
The TURN password to use for the allocation.		(blank)	At start or restart

turn-relay-type

turn-relay-type (TURN Relay Type)			
Description	**Valid values**	**Default value**	**Takes effect**

The type of relay to use. TCP(1) and UDP(0) are supported; TLS is not supported. The default is UDP. If this parameter is not defined, but the TURN server URL contains the query string "transport=tcp", then TCP will be chosen.		0	At start or restart

turn-server

turn-server (TURN Server)			
Description	**Valid values**	**Default value**	**Takes effect**
Optional TURN server specification. A TURN server is not typically required on the gateway side, but it may need to be configured on the browser/client side when there is a strict firewall between the client and the gateway that will prevent RTP/UDP traffic. Only local addresses are gathered when STUN or TURN is not configured.	<IP-address|FQDN>[:<port>], where port can be omitted, if default port 3478 is used.	(blank)	At start or restart

turn-user

turn-user (TURN User)			
Description	**Valid values**	**Default value**	**Takes effect**
The TURN username to use for the allocation.		(blank)	At start or restart

use-sid-from-url

use-sid-from-url (Use Session Id from URL)			
Description	**Valid values**	**Default value**	**Takes effect**
When this is set to true, Genesys WebRTC Gateway uses HTTP request URL parameters or value of Cookie header to match HTTP request with existing client session. If it is false, Genesys WebRTC Gateway uses value of Cookie header to match	true, false	true	After Genesys WebRTC Gateway restart

the HTTP request with existing client session. **Note:** This option works with Genesys WebRTC Java Script API from version 8.5.210.35.			

web-added-codecs

web-added-codecs (Web Added Codecs)			
Description	**Valid values**	**Default value**	**Takes effect**
When transcoding is enabled, codecs from this list will be appended to the codec list for offers to a WebRTC endpoint, except for the codecs that are already in the original offer. If G.722 is not supported on the SIP side, and yet G.722 is desired on the Web side, add "g722" to web-added-codecs for the cases where the SDP offer comes from the SIP side. Note that transcoding will take place in this case between G.722 and the audio codec used on the SIP side. The other comments for sip-added-codecs are applicable here as well.	List of codecs using the same format as `sip-added-codecs` option.	(g722,pcmu,vp8)	At start or restart

web-disable-sdes

web-disable-sdes			
Description	**Valid values**	**Default value**	**Takes effect**
When this is set to true, the crypto attribute to support SDES-SRTP (RFC 4568) will not be in initial offers to Web clients. If it is false, initial offers will have both fingerprint and crypto attributes. Note that this option does not prevent supporting SDES-SRTP when the client only offers crypto	true, false	true	At start or restart

attribute(s). However, SDES-SRTP use is discouraged, and only Chrome supports it for backward compatibility.			

web-disallowed-codecs

web-disallowed-codecs (Web Disallowed Codecs)			
Description	**Valid values**	**Default value**	**Takes effect**
Disallowed codecs for the WebRTC side. An offer or answer to the Web side may not use any of these codecs.	List of codecs using the same format as `sip-disallowed-codecs` option.	(h264)	At start or restart

web-dtls-certificate

web-dtls-certificate (Certificate for Web-side DTLS)			
Description	**Valid values**	**Default value**	**Takes effect**
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.		../config/ x509_certificate.pem	At start or restart

web-dtls-cipherlist

web-dtls-cipherlist (Cipher List for DTLS)			
Description	**Valid values**	**Default value**	**Takes effect**
A list of cipher strings to be used with DTLS on the Web side. For information on the format, see OpenSSL ciphers. The default cipher string should work well.		(blank)	At start or restart

web-dtls-keypassword

web-dtls-keypassword (Password for DTLS Certificate Key)			
Description	**Valid values**	**Default value**	**Takes effect**

The password for the private key specified using web-dtls-privatekey, if used.		(blank)	At start or restart

web-dtls-privatekey

web-dtls-privatekey (Private Key for DTLS Certificate)			
Description	**Valid values**	**Default value**	**Takes effect**
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.		(blank)	At start or restart

web-enable-dtls

web-enable-dtls (Enable DTLS on the Web-side)			
Description	**Valid values**	**Default value**	**Takes effect**
When this is set to true, DTLS-SRTP (RFC 5763) will be enabled on the Web side. When enabled, it will be signaled 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, provided that SDES-SRTP is not disabled using the option `web-disable-sdes`. 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.	true, false	true	At start or restart

web-ice-addresses

web-ice-addresses (Web ICE addresses)			
Description	**Valid values**	**Default value**	**Takes effect**
Allows configuration of a local IP address list to	A comma-separated list of valid IP addresses.		At restart

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 the host candidates.			

web-media-bundle

web-media-bundle (Media Bundle on Web-side)			
Description	**Valid values**	**Default value**	**Takes effect**
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. With media bundle, it is assumed that RTCP multiplexing is also supported. Disabling this bundle option is discouraged.	true, false	true	At start or restart

web-nack-enabled

web-nack-enabled (Enable Web Side NACK Sending)			
Description	**Valid values**	**Default value**	**Takes effect**
Set this to true (default) to enable RTCP NACK (transport layer) feedback messages as per (RFC 4585). Set this to false to disable this feature. The minimum time between two NACK messages is currently restricted to one second.	true, false	true	At start or restart

web-offer-bundle-only

web-offer-bundle-only			
Description	**Valid values**	**Default value**	**Takes effect**
This option helps to work around some renegotiation issues with Firefox. When an older version of Firefox without bundle support is used (version 37 and lower), set this option to `false`.	true, false	true	At start or restart

web-pli-always

web-pli-always (Force Web Side PLI Requests)			
Description	**Valid values**	**Default value**	**Takes effect**
If this parameter is set to true and web-pli-mintime is nonzero, RTCP PLI feedback messages (RFC 4585) will be sent on a Web-side video leg at every web-pli-mintime interval, regardless of transcoding or packet losses.	true, false	true	At start or restart

web-pli-mintime

web-pli-mintime (Minimum Time Interval for Web Side PLI Requests)			
Description	**Valid values**	**Default value**	**Takes effect**
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	The parameter must be an integer.	1000	At start or restart

specific threshold.			

web-rtcp-mux

web-rtcp-mux (RTCP-Mux on the Web-side)			
Description	**Valid values**	**Default value**	**Takes effect**
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.	true, false	true	At start or restart

web-rtp-max-port

web-rtp-max-port (ROAP-side Max RTP Port)			
Description	**Valid values**	**Default value**	**Takes effect**
Maximum UDP port value for ICE (ROAP-side RTP connection).		36999	At start or restart

web-rtp-min-port

web-rtp-min-port (ROAP-side Min RTP Port)			
Description	**Valid values**	**Default value**	**Takes effect**
Minimum UDP port value for ICE (ROAP-side RTP connection).		36000	At start or restart

snmp

SNMP settings.

timeout

timeout (SNMP Task Timeout)

Description	Valid values	Default value	Takes effect
The maximum amount of time that SNMP can wait for a new task. This value is specified in milliseconds.	The parameter must be an integer value greater than zero.	100	At start or restart