Web Real-Time Communications

rsmp Section

4/24/2025

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).