Web Real-Time Communications Deployment Guide

Platform Configuration

12/16/2025

Contents

Platform Configuration

The following topics discuss the important configuration options that you may need to set in the rsmp section of your WebRTC gateway application object, before start using the WebRTC gateway. For further information on these options and other possible configuration options, please refer to Configuration Options Reference.

Configure the following deployment specific options first:

- `sip-proxy`—The address and port of your Genesys SIP-Server, for example: `<host-name>:<port>`.
- `sip-register`—The list of DNs configured in SIP Server for use by the WebRTC Gateway, for example: `8100-8199,9000,9002,9800-9820`. A client can use any one of these DNs to register itself with the SIP Server via the gateway for receiving calls. A 'callee' DN that is used by the client to make an outbound call to does not need to be in this list. In this case, the user will be registered by the gateway as anonymous.
- `stun-server`—The address and port of the STUN server to be used, for example: `<host-name>:<port>`. This option is not mandatory, but Genesys recommends that you configure it before using the WebRTC Gateway. This option is required when the WebRTC gateway is in a private network and it cannot find out its public address by itself.
- `http-port`—The HTTP or HTTPS port of the WebRTC Gateway used for signaling with the browser. The default value is `8086`, which may need to be changed depending on the network configuration. It's is recommended that port 443 is used for HTTPS.

Configuring HTTPS

For enabling HTTPS on the WebRTC gateway, you need an SSL certificate from a public Certificate Authority (CA), and need to set the following gateway configuration parameters to appropriate values: `enable-https`, `https-cert`, `https-cert-key` and `https-trusted-ca` (the last two are for Linux only). Note that the port used for HTTPS is still specified using `http-port`, and HTTP is not supported when HTTPS is enabled.

> **Important**
>
> Chrome by default requires that HTTPS is used for enabling media device access on the host machine.

If you have a Load Balancer (LB) or proxy fronting the WebRTC Gateway, you need an SSL certificate installed for the LB or proxy. In this case, HTTP, instead of HTTPS, could be used between the LB/proxy and the gateway, provided these two are in a secure network. You may still need to use HTTPS between the browser and the LB/proxy.

Enabling DTLS-SRTP

DTLS-SRTP (RFC 5763) is enabled on the web side by default. However, if you need to re-enable it for some reason, simply set the `web-enable-dtls` configuration option to `true`.

When `web-enable-dtls` is 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 `web-enable-dtls` is set to `false`, only SDES-SRTP will be supported.

> **Important**
>
> Only Chromium based browsers support SDES-SRTP for historical reasons, and the WebRTC standard demands that DTLS-SRTP is used.

Enabling SRTP for the SIP Side

SRTP is not enabled on the SIP side by default. If the SIP agent and the WebRTC Gateway are in the same local/private network, you may not need to enable it. If needed, you can enable it by setting the gateway configuration parameter `sip-srtp-mode` to an appropriate vlaue (`optional` or `strict`).

Configuring Secure SIP (SIPS)

Use of SIPS is not enabled by default. If the SIP agent and the WebRTC gateway are in the same local/private network, you may not need to enable it. To enable it, you need an SSL certificate from a public Certificate Authority (CA), and need to set the following gateway configuration parameters to appropriate values: `sip-tls-port`, `sip-tls-cert`, `sip-tls-cert-key` and `sip-tls-trusted-ca` (the last two are for Linux only).

Configuring a Specific IP Address for SIP or RTP

When a different IP address than what is automatically detected by the gateway needs to be used for SIP or RTP, you can use the following options to configure this address. This is useful for AWS instances or multi-homed hosts. `sip-address`: This value will be used in SIP Via and/or Contact headers, that indicate the address to which SIP messages should be sent. `rtp-address`: This value will be used for SDP c= line, that indicates the address to which RTP should be sent.

Configuring RTP Port Ranges

You do not normally need to change the port ranges used for RTP. If required, however, you could configure these using options `sip-rtp-min-port`, `sip-rtp-max-port`, `web-rtp-min-port`, and `web-rtp-max-port`.

Configuring Media Codecs

Although you should not need to, if required, you could disable or change the priority order of the supported media codecs using options `codecs`, `sip-added-codecs`, `web-added-codecs`, `sip-disallowed-codecs`, and `web-disallowed-codecs`. Note that the codec list in an SDP created by the the gateway for a client, including the order of codecs, is always based on the offer or answer SDP from the other client, and only the codecs in `sip-added-codecs` or `web-added-codecs` (depending on whether the SDP is to be sent to the SIP or Web client) are appended to this codec list; not all the codecs from the codecs option are included in the SDP.

Disabling Anonymous Sign-in

The option `allow-anonymous-user` can be used to disable anonymous sign-ins from the WebRTC client by setting it to 'false'. When disabled, only valid DNs on the SIP server can be used to sign-in. This option has the default value of 'true'.

Configuring Cross Origin Resource Sharing (CORS)

The WebRTC gateway supports CORS to restrict HTTP[S] access from arbitrary domains. A list of allowed domains can be configured using the option domain-whitelist. See Security Considerations for more information.

SIP Server High Availability

When DNS SRV is used for SIP Server High Availability (HA), you must configure the WebRTC Gateway:

- Set `rsmp.sip-proxy` with the IP addresses or the FQDNs of the SIP Servers, separated by a comma.
- Set `rsmp.sip-proxy-srv` to the SIP Server SRV address.

The Gateway will start with the first sip-proxy address. When a request to the current address times-out, the Gateway will switch to the other address and then back. When a request arrives from SIP Server with its SRV address, it will be translated to the current active SIP Server address before sending a response.