Genesys Voice Platform

vrmrecorder Section

12/20/2025

vrmrecorder Section

sip.localport

Default Value: 7090
Valid Values: The port number must be from 1030 to 65535 inclusive
Changes Take Effect: At start/restart

The Local Non-secure SIP Port used by the VRMRecorder Client when SIP UDP and SIP TCP are used.

sip.localsecureport

Default Value: 7091
Valid Values: The port number must be from 1030 to 65535 inclusive
Changes Take Effect: At start/restart

The Local Secure SIP Port used by the VRMRecorder Client when SIP TLS is used.

sip.preferred_ipversion

Default Value: ipv4
Valid Values: Choose between: IPv4 or IPv6
Changes Take Effect: At start/restart

Preferred IP version to be used in SIP by the VRMRecorder. When multiple IP addresses with different IP versions are resolved from a destination address, the first address from the list with the preferred IP version will be used. However, if there is no sip.transport defined for the preferred version, the other version will be used. Valid values are "ipv4" and "ipv6".

sip.routeset

Default Value:
Valid Values: A valid routeset must have the format as specified in [sip] routeset description
Changes Take Effect: At start/restart

Defines a route set for non-secure SIP connections to third party recorders by the VRMRecorder client. If defined, this route set will be inserted as the ROUTE header for all VRMRecorder SIP sessions. This will force the MCP to send the SIP messages via this defined route set. Please see "[sip] routeset" for format and other descriptions. The typical value for this would be the Resource Manager (RM) address, as all recorder requests go through the RM.

sip.securerouteset

Default Value:
Valid Values: A valid secure routeset must have the format as specified in its description
Changes Take Effect: At start/restart

Defines a route set for secure SIP connections to third party recorders. The URI for secure connections should specify the "sips:" scheme or "tls" transport. If the secure route set is defined, this route set will be inserted as the ROUTE header for all VRMRecorder secure SIP sessions. This will force the MCP to send the secure SIP messages via this defined route set. Please see "[sip] secureroutеset" for format and other descriptions. The typical value for this would be the Resource Manager (RM)'s secure address, as all recorder requests go through the RM.

sip.transport.0

Default Value: transport0 udp:any:7090
Valid Values: <transport_name> <type>:<ip-address>:<port> [parameters]
Changes Take Effect: At start/restart

The SIP UDP Transport used by the VRMRecorder Client. Format: sip.transport.x = transport_name type:ip:port

where: transport_name is any string type is udp/tcp/tls ip is the IP address of the network interface that accepts incoming SIP messages port is the port number where SIP stack accepts incoming SIP messages
If ip is an IPv6 address, [] must be used. To define a transport to listen to all IPv4 interfaces, use "any" or "any4" for ip. To define a transport to listen to all IPv6 interfaces, use "any6" for ip. Remarks: The default transport is the smallest non-empty ID. If all transport.x values are empty, UDP, TCP, and TLS

transports will all be enabled and respectively listen from ports 5060, 5060, and 5061 on any network interface. TLS transport will use the certificate, x509_certificate.pem, and key, x509_private_key.pem, in the config directory. UDP will be the default transport.

sip.transport.1

Default Value: transport1 tcp:any:7090
Valid Values: <transport_name> <type>:<ip-address>:<port> [parameters]
Changes Take Effect: At start/restart

The SIP TCP Transport used by the VRMRecorder Client. Format: sip.transport.x = transport_name type:ip:port

where: transport_name is any string type is udp/tcp/tls ip is the IP address of the network interface that accepts incoming SIP messages port is the port number where SIP stack accepts incoming SIP messages
If ip is an IPv6 address, [] must be used.
To define a transport to listen to all IPv4 interfaces, use "any" or "any4" for ip. To define a transport to listen to all IPv6 interfaces, use "any6" for ip. Remarks: The default transport is the smallest non-empty ID. If all transport.x values are empty, UDP, TCP, and TLS transports will all be enabled and respectively listen from ports 5060, 5060, and 5061 on any network interface. TLS transport will use the certificate, x509_certificate.pem, and key, x509_private_key.pem, in the config directory. UDP will be the default transport.

sip.transport.2

Default Value: transport2 tls:any:7091 TLSv1_2
Valid Values: <transport_name> <type>:<ip-address>:<port> [parameters]
Changes Take Effect: At start/restart

The SIP TLS Transport used by the VRMRecorder Client. Format: sip.transport.x = transport_name type:ip:port [parameters]

where: transport_name is any string type is udp/tcp/tls ip is the IP address of the network interface that accepts incoming SIP messages port is the port number where SIP stack accepts incoming SIP messages [parameters] defines any extra SIP transport parameters. Note that this is for LMSIP2.

If ip is an IPv6 address, [] must be used. To define a transport to listen to all IPv4 interfaces, use "any" or "any4" for ip. To define a transport to listen to all IPv6 interfaces, use "any6" for ip. Example:
cert=[cert path and filename] Applicable to SIPS only and mandatory if using SIPS. The path and the filename of the TLS certificate to be used.
key=[key path and filename] Applicable to SIPS only and mandatory if using SIPS. The path and the filename of the TLS key to be used.
type=[Type of secure transport] Applicable to SIPS only and is optional. The type of secure transport to be used and value can be TLSv1_2, TLSv1_1, TLSv1, SSLv3, or SSLv23. The default value is TLSv1. Note that SSLv2 is no longer supported.
password=[password] Applicable to SIPS only and is optional. The password associated with the certificate and key pair. Required only if key file is password protected.
cafile=[CA cert path and filename] Mandatory for TLS mutual authentication. The path and the

filename of the certificate to be used for verifying the peer. The same certificate specified in cert=[cert path and filename] parameter can be used as the value here if using only 1 certificate is preferred.
verifypeer=true Mandatory for TLS mutual authentication. This parameter turns on the TLS mutual authentication.
verifydepth=[max depth for the certificate chain verification] Applicable only to TLS mutual authentication. This parameter sets the maximum depth for the certificate chain verification. For the default Genesys certificate provided, the recommended value is 1.
tls-cipher-list=[List of ciphers that are applicable for the socket] Applicable only to TLS socket - both server and client sockets. This parameter allows selecting a list of cipher suites used in TLS. This option is transfered to a third-party library and describes a possible set of cipher suites. Refer to https://www.openssl.org/docs/man1.0.2/man1/ciphers.html for Cipher list format. Default is ALL:!EXPORT:!LOW:!aNULL:!eNULL:!SSLv2 Remarks: The default transport is the smallest non-empty ID. If all transport.x values are empty, UDP, TCP, and TLS transports will all be enabled and respectively listen from ports 5060, 5060, and 5061 on any network interface. TLS transport will use the certificate, x509_certificate.pem, and key, x509_private_key.pem, in the config directory. UDP will be the default transport. Note: The max path length supported for certificate and key file is 259 characters.

sip.transport.dnsharouting

Default Value: false
Valid Values: Choose between: true or false
Changes Take Effect: At start/restart

Specifies whether the DNS HA routing based on RFC3263 should be turned on. If turned off, alternate records returned from the DNS query will not be tried. Otherwise, alternate records returned from the DNS query will be tried based on RFC3263.

sip.transport.localaddress

Default Value:
Valid Values: Specify a valid IP Address, hostname or domain name
Changes Take Effect: At start/restart

If specified, the sent-by field of the Via header and the hostport part of the Contact header in the outgoing SIP message will be set to this value if a IPv4 transport is used. The value must be a hostname or domain name if [sip].transport.localaddress.srv is set to true, otherwise when [sip].transport.localaddress.srv is set to false an IP address or hostname can be used for the value. If left empty the outgoing transport's actual IP and port will be used for the Via header and the Contact header. Note that if the domain name used in the SRV record query is specified, vrmrecorder.sip.transport.localaddress.srv must be set to true to prevent the port part being automatically generated by the SIP stack.

sip.transport.localaddress_ipv6

Default Value:

Valid Values: Specify a valid hostname or domain name
Changes Take Effect: At start/restart

If specified, the sent-by field of the Via header and the hostport part of the Contact header in the outgoing SIP message will be set to this value if a IPv6 transport is used. The value must be a hostname or domain name. If left empty the outgoing transport's actual IP and port will be used for the Via header and the Contact header. Note that if the domain name used in the SRV record query is specified, vrmrecorder.sip.transport.localaddress.srv must be set to true to prevent the port part being automatically generated by the SIP stack.

sip.transport.localaddress.srv

Default Value: false
Valid Values: Choose between: true or false
Changes Take Effect: At start/restart

Specifies whether the mrcpv2client.transport.localaddress contains an SRV domain name. If set to true, port part will not be automatically generated by the SIP stack. Otherwise, the outgoing transport's port will used together with the hostname specified by the vrmrecorder.sip.transport.localaddress.

sip.transport.staticroutelist

Default Value:
Valid Values: Can be an empty string or a valid "|" separated list of static routes. Check the description for further details.
Changes Take Effect: At start/restart

Specifies a list of static routes. Each route group is separated by |. Each static route group is a list of IP addresses separated by comma. Within the route group, each IP address could substitute each other as an alternate route destination if sending a SIP request to one of the IP address fails. For example, 10.0.0.1,10.0.0.2|10.0.10.1,10.0.10.2 specified two static route groups, and each group specified two routes that are alternative to each other. Default value is an empty list.

sip.transport.unavailablewakeup

Default Value: true
Valid Values: Choose between: true or false
Changes Take Effect: At start/restart

Specifies whether unavailable route destinations can be made active if needed before the route recover timer expires. The unavailable destinations would be made active only when all destinations corresponding to a static route group or DNS SRV domain are unavailable. This parameter is applicable when SIP stack is running under HA mode (Static route list or DNS SRV routing).

toheadermode

Default Value: toparams
Valid Values: Choose between: legacy, uriparams, toparams or bothtoanduriparams
Changes Take Effect: Immediately/session

The To Header Mode for Third Party Call Recording. If set to "legacy", the MCP will copy the Request URI of the INVITE request into the To Header, identical to pre-GVP 8.5.0 behavior. If set to "uriparams", the Request URI parameters will be included in the Request URI part of the To Header. If set to "toparams", the Request URI parameters will be included in the To params of the To Header. If set to "bothtoanduriparams", the Request URI parameters will be included in both the Request URI part of the To Header and the To params of the To Header.

websocket.asio_worker_threads

Default Value: 3
Valid Values: Any positive integer value.
Changes Take Effect: At start/restart

Number of threads used to handle WebSocket connections.

websocket.buffer_size

Default Value: 200
Valid Values: A number between 0 and 5000 inclusive, incremented by 20.
Changes Take Effect: Immediately

The duration of audio data (in milliseconds) that will be buffered before delivering it to the server. Must be an integer in the range of 0 to 5000 milliseconds. The value must be a multiple of 20, which is tipically the size of a single packet, otherwise, it will be rounded down. Buffering will be disabled if value is set to 0. Default value is 200 milliseconds.

websocket.ssl_ca_file

Default Value:
Valid Values: Can be an empty string or a valid file name.
Changes Take Effect: Immediately

The file name holding one or more certificates to verify the peer with.

websocket.ssl_ca_path

Default Value:

Valid Values: Can be an empty string or a valid folder path.
Changes Take Effect: Immediately

The path holding multiple CA certificates to verify the peer with. The certificate directory must be prepared using the openssl c_rehash utility.

websocket.ssl_cert

Default Value:
Valid Values: Can be an empty string or a valid file name.
Changes Take Effect: Immediately

The file name of your certificate. The file format must be "PEM".

websocket.ssl_key

Default Value:
Valid Values: Can be an empty string or a valid file name.
Changes Take Effect: Immediately

The file name of the private key. The file format must be "PEM".

websocket.ssl_verify_peer

Default Value: 0
Valid Values: Choose between: 0 or 1
Changes Take Effect: Immediately

Whether or not to verify the peer's certificate. When this option is set, one of ssl_ca_file or ssl_ca_path should be set.

websocket.streaming_percentage

Default Value: 100
Valid Values: A number between 0 and 100 inclusive.
Changes Take Effect: Immediately

MCP runs an algorithm for every call to verify if it can or cannot be streamed, the algorithm will be based on the percetage provided in this parameter. Therefore, setting the parameter to 100 means that all calls will be streamed, and setting it to 0, means that no calls will be streamed. Default value is 100 percent.