Genesys Voice Platform

mrcpv2client Section

4/7/2025

mrcpv2client Section

sip.transport.0

Default Value: transport0 udp:any:7080
Valid Values: <transport_name> <type>:<ip-address>:<port> [parameters]
Changes Take Effect: At start/restart

The SIP UDP Transport used by the MRCPV2 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:7080
Valid Values: <transport_name> <type>:<ip-address>:<port> [parameters]
Changes Take Effect: At start/restart

The SIP TCP Transport used by the MRCPV2 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:7081 type=TLSv1
Valid Values: <transport_name> <type>:<ip-address>:<port> [parameters]
Changes Take Effect: At start/restart

The SIP TLS Transport used by the MRCPV2 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.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, mrcpv2client.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 mrcpv2client.sip.transport.localaddress.