Genesys Voice Platform

sip Section

4/16/2025

sip Section

localuser

Default Value: CTIConnector
Valid Values:
Changes Take Effect: At start/restart

Configures the user name portion of the Contact header generated from the platform.

mtusize

Default Value: 1500
Valid Values:
Changes Take Effect: After restart

Defines the Maximum Transmission Unit (MTU) of the network interfaces. If a SIP request size is within 200 bytes of this value, the request will be sent on a congestion controlled transport protocol, such as TCP.

tcp.portrange

Default Value:
Valid Values: Possible values are the empty string or low-high, where low and high are integers from 1030 to 65535 inclusive
Changes Take Effect: At start/restart

The local TCP port range to be used for SIP transport. If this parameter is not specified, CTIC will let

the OS choose the local port.

tls.portrange

Default Value:
Valid Values: Possible values are the empty string or low-high, where low and high are integers from 1030 to 65535 inclusive
Changes Take Effect: At start/restart

The local TLS port range to be used for SIP transport. If this parameter is not specified, CTIC will let the OS choose the local port.

transport.0

Default Value: transport0 udp:any:5080
Valid Values:
Changes Take Effect: At start/restart

defines transport layer for SIP stack and the network interfaces that are used to process SIP requests
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; 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. port is the port number where SIP stack accepts incoming SIP messages;
[parameters] defines any extra SIP transport parameters.

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, SSLv3, SSLv23, TLSv1_1, TLSv1_2. Default to TLSv1_2. 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.

transport.1

Default Value: transport1 tcp:any:5080

Valid Values:
Changes Take Effect: At start/restart

defines transport layer for SIP stack and the network interfaces that are used to process SIP requests
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; 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. port is the port number where SIP stack accepts incoming SIP messages;
[parameters] defines any extra SIP transport parameters.

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, SSLv3, SSLv23, TLSv1_1, TLSv1_2. Default to TLSv1_2. 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.

transport.2

Default Value: transport2 tls:any:5081 cert=$InstallationRoot$/config/x509_certificate.pem key=$InstallationRoot$/config/x509_private_key.pem
Valid Values:
Changes Take Effect: At start/restart

defines transport layer for SIP stack and the network interfaces that are used to process SIP requests
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; 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. port is the port number where SIP stack accepts incoming SIP messages;
[parameters] defines any extra SIP transport parameters.

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, SSLv3, SSLv23, TLSv1_1, TLSv1_2. Default to TLSv1_2. 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.

transport.localaddress

Default Value:
Valid Values:
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 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, sip.transport.localaddress.srv must be set to true to prevent the port part being automatically generated by the SIP stack.

transport.localaddress_ipv6

Default Value:
Valid Values:
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, sip.transport.localaddress.srv must be set to true to prevent the port part being automatically generated by the SIP stack.

transport.localaddress.srv

Default Value: false
Valid Values: true, false
Changes Take Effect: At start/restart

Specifies whether the sip.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 sip.transport.localaddress.

transport.routefailovertime

Default Value: 5
Valid Values:
Changes Take Effect: At start/restart

Specifies the failover time in seconds for SIP static routing. If a SIP request has not received a response within the failover time, and SIP static routing is enabled, the SIP request will be retransmitted to an alternate route as specified in the SIP static route list.

transport.routerecoverytime

Default Value: 30
Valid Values:
Changes Take Effect: At start/restart

Specifies the recovery time in seconds for SIP static routing. When SIP static routing is enabled a route is marked as unavailable due to error or SIP response timeout, the route will be marked as available again after the recovery time.

transport.staticroutelist

Default Value:
Valid Values:
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.

transport.unavailablewakeup

Default Value: true
Valid Values: true, 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).