Genesys Voice Platform

sip Section

5/8/2025

sip Section

- attconfnetworktonetimeout
- call_rate
- call_rate_period
- copyunknownheaders
- copyxgenesysheaders
- defaultblindxfer
- defaultbridgexfer
- defaultconsultxfer
- defaultfrom
- defaultgw
- defaulthost
- deferoutalerting
- dnis_correlationid_length
- dnis_correlationid_offset
- dtmf.crlfenable
- enable_dns_cache
- enablemaddr
- enablesendrecvevents
- enabletfci
- handlesessionrefreshsdp
- hfdisctimer
- hfprefix
- hfstopdial
- hftype
- in.bye.headers
- in.info.headers
- in.invite.headers
- in.invite.params
- info.contenttype
- localuser
- logmsg.allowed
- logmsg.maskoption
- maxtcpaccepts
- maxtcpconnections
- maxtlsaccepts
- maxtlsconnections
- min_se
- mpc.copyheaders
- mtusize
- out.info.headers
- out.invite.headers
- out.invite.params
- out.refer.headers
- out.refer.params
- outcalluseoriggw
- p-alcatel-csbu
- passertedidentity
- pcalledpartyid
- prack.support
- preferred_ipversion
- referredby
- referxferhold
- referxfertryoutbound
- referxferwaitbye
- referxferwaitnotify
- registerexpiryadjustment
- registration
- route.default.tcp
- route.default.tls
- route.default.udp
- route.dest.0
- route.dest.1
- route.dest.2
- route.dest.3
- route.dest.4
- route.dest.5
- routeset
- sdpansinprov
- sdpwarningheaders
- securerouteset
- sendalert
- sessionexpires
- sipinfoallowedcontenttypes
- tcp.portrange
- threadpoolsize
- threads
- timer_si
- timer.ci_proceeding
- timer.provretransmit
- tls.portrange
- transfermethods
- transport.0
- transport.0.tos
- transport.1
- transport.1.tos
- transport.2
- transport.2.tos
- transport.3
- transport.3.tos
- transport.4

- transport.4.tos
- transport.5
- transport.5.tos
- transport.dnsharouting
- transport.localaddress
- transport.localaddress_ipv6
- transport.localaddress.srv
- transport.routefailovertime
- transport.routerecoverytime
- transport.setuptimer.tcp
- transport.staticroutelist
- transport.unavailablewakeup
- userouteonrecording
- voipmetrics.localhost
- voipmetrics.registration
- voipmetrics.remoteserver
- voipmetrics.routeset
- vxmlinvite
- warningheaders
- xfer.copyheaders

attconfnetworktonetimeout

Default Value: 1000
Valid Values: sip.attconfnetworktonetimeout should be positive integer.
Changes Take Effect: At start/restart

Specify the network tone timeout in ms for an ATT conference, in which there is no direct way to tell if DTMF star (*) is part of network tone or user input. Since a complete network tone, which is composed of two DTMF stars (**) plus a DTMF digit, would arrive within a short period of time since the first DTMF star comes in, it is reasonable to believe that the DTMF star(s) are user inputs if no complete network tone is received within the time specified in this parameter. By default, attconfnetworktonetimeout is set to 1000 (1s).

call_rate

Default Value: 0
Valid Values: sip.call_rate should be an integer from 0 to 1000 inclusive.
Changes Take Effect: At start/restart

Specify the number of incoming calls, when not 0, that SIP line manager can accept within call_rate_period. It works along with parameter call_rate_period. For example, if call_rate is set to 10 and call_rate_period is set to 500 (ms), then SIP line manager can accept at most 10 incoming calls every 500 milliseconds. If there are more than 10 incoming calls within 500 milliseconds, the excess calls will be rejected with response 486 Busy Here. By default, call_rate is set to 0, which means no overload control at all.

call_rate_period

Default Value: 0
Valid Values: sip.call_rate_period should be non-negative integer.
Changes Take Effect: At start/restart

Specify the call rate period in milliseconds for overload control. It works along with parameter call_rate. For example, if call_rate is set to 10 and call_rate_period is set to 500 (ms), then SIP line manager can accept at most 10 incoming calls every 500 milliseconds. If there are more than 10 incoming calls within 500 milliseconds, the excess calls will be rejected with response 486 Busy Here. By default, call_rate_period is set to 0, which means no overload control at all.

copyunknownheaders

Default Value: 1
Valid Values: Choose between: 0 or 1
Changes Take Effect: At start/restart

Copy unknown headers from request to all responses. If this parameter set to Enable, all unknown SIP headers found in SIP request will be automatically copied to its responses.

copyxgenesysheaders

Default Value:
Valid Values: A valid header can only contain alphanumeric characters and '.', '-' and ':' characters
Changes Take Effect: At start/restart

Defines a list of X-Genesys custom headers to be copied from SIP requests to all responses and follow-up requests. These custom headers are copied when the copyunknownheaders configuration option is enabled. If there are no headers defined (the list is empty), all X-Genesys custom headers are treated the same as other unknown headers. The X-Genesys- prefix in each header must be omitted when the list is defined. By default, the list is empty. If you do not want the custom headers to be copied in SIP responses or follow-up requests, Genesys recommends that you set the copyxgenesysheaders configuration option value as follows: GVP-Session-Data GVP-Trunk-Prefix GVP-PSTNC-DBID GVP-CTI-Params GVP-CDR RM-Log-filters gsw-predictive-call outbound-ivr-call geo-location gvp-tenant-ports mediaserver-status GVP-Site-ID

defaultblindxfer

Default Value: REFER
Valid Values: Choose between: HKF, REFER, BRIDGE, REFERJOIN, MEDIAREDIRECT, ATTCOURTESY, ATTCONSULT, ATTCONFERENCE, ATTOOBCOURTESY, ATTOOBCONSULT, ATTOOBCONFERENCE or NEC61ISDN
Changes Take Effect: At start/restart

SIP Transfer Methods for blind transfer. HKF - HookFlash REFER - REFER-based transfer BRIDGE - BRIDGE-based transfer REFERJOIN - Consultative REFER transfer MEDIAREDIRECT - Media redirect transfer ATTCOURTESY - AT&T courtesy transfer ATTCONSULT - AT&T consult transfer ATTCONFERENCE - AT&T conference transfer ATTOOBCOURTESY - AT&T out-of-band courtesy transfer ATTOOBCONSULT - AT&T out-of-band consult transfer ATTOOBCONFERENCE - AT&T out-of-band conference transfer NEC61ISDN - Single B channel blind transfer over ISDN for NEC NEAX 61 switch

defaultbridgexfer

Default Value: BRIDGE
Valid Values: Choose between: BRIDGE, MEDIAREDIRECT or ATTCONFERENCE
Changes Take Effect: At start/restart

Default bridge type transfer method for sip. BRIDGE - BRIDGE-based transfer MEDIAREDIRECT - Media redirect transfer ATTCONFERENCE - AT&T conference transfer

defaultconsultxfer

Default Value: REFERJOIN
Valid Values: Choose between: HKF, REFER, BRIDGE, REFERJOIN, MEDIAREDIRECT, ATTCONSULT, ATTCONFERENCE, ATTOOBCONSULT or ATTOOBCONFERENCE
Changes Take Effect: At start/restart

Default consult type transfer method for sip. HKF - HookFlash REFER - REFER-based transfer BRIDGE - BRIDGE-based transfer REFERJOIN - Consultative REFER transfer MEDIAREDIRECT - Media redirect transfer ATTCONSULT - AT&T consult transfer ATTCONFERENCE - AT&T conference transfer ATTOOBCONSULT - AT&T out-of-band consult transfer ATTOOBCONFERENCE - AT&T out-of-band conference transfer

defaultfrom

Default Value:
Valid Values: A valid address can only contain alphanumeric characters, '.', '-', ':', ' ','/' and '\' characters
Changes Take Effect: At start/restart

Default From for SIP calls if none given. If a call is placed (either via transfer, call, or remdial) using SIP, and the From value is missing from the request, this parameter will supply the From header value for the SIP request.

If this parameter is not specified, the value will be set to "sip:Genesys@" + "host" + "the port specified in the sip.transport.0 parmeter".

Example:
sip.defaultfrom=sip:Genesys@sip.genesyslab.com:5070

defaultgw

Default Value:
Valid Values: A valid address can only contain alphanumeric characters, '.', '-', ':', ' ','/' and '\' characters

Changes Take Effect: At start/restart

Default host/port for SIP calls if none given. If a call is placed (either via transfer, call, or remdial) using SIP, and the destination address is a telephone address, then the call will be routed to the configured default gateway.

For instance, if a call is placed to "tel:4167360905", and this call is routed to the SIP line manager then this address will be translated into "sip:4167360905@default-gw".

If this parameter is not specified, no default gateway will be used, and calls to telephony addresses will fail.

Example:
sip.defaultgw=pstn-gw.genesyslab.com:5060

defaulthost

Default Value:
Valid Values: A valid address can only contain alphanumeric characters, '.', '-', ':', ' ','/' and '\' characters
Changes Take Effect: At start/restart

Default host/port for SIP calls if none given. If a call is placed (either via transfer, call, or remdial) using SIP, and the destination address does not contain a hostname or IP address, this parameter will supply a default hostname or IP address.

For instance, if the address "sip:1234@" is used, the default hostname will be appended. If this parameter is not specified, no default host will be used and calls that do not specify a host will fail.

Example:
sip.defaulthost=sip.genesyslab.com:5060

deferoutalerting

Default Value: 0
Valid Values: Choose between: 0 or 1
Changes Take Effect: At start/restart

Defer CallOutAlerting response to MCP. This is for early media for an outbound call. If this value is set to Enable, the platform will defer CallOutAlerting to MCP until the media session is initialized and registered. Hence, the MCP can start performing media operations on the channel after CallOutAlerting notification.

dnis_correlationid_length

Default Value: 0

Valid Values: sip.dnis_correlationid_length should be non-negative integer that is less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

If this parameter is enabled, correlation ID is extracted from the user-id portion of the DNIS, and the correlation ID portion is stripped from DNIS. Value is a non-negative integer that specifies the length of the correlation ID within the user-id.

Note the special case where correlation ID is all of user-id; '@' will be stripped away from the DNIS as well since @<hostname> does not make sense.

dnis_correlationid_offset

Default Value: 0
Valid Values: sip.dnis_correlationid_offset should be a valid integer (with minimum and maximum values as defined by the Genesys Administrator Help)
Changes Take Effect: At start/restart

If this parameter is enabled, correlation ID is extracted from the user-id portion of the DNIS, and the correlation ID portion is stripped from DNIS. Value is an integer that specifies the offset of the correlation ID within the user-id. If it is negative, it specifies the offset from the right.

Note the special case where correlation ID is all of user-id; '@' will be stripped away from the DNIS as well since @<hostname> does not make sense.

dtmf.crlfenable

Default Value: false
Valid Values: Choose between: true or false
Changes Take Effect: Immediately/session

If the flag is set to true CRLF will be added after Duration attribute

enable_dns_cache

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

Specifies if MCP should enable or disable the use of DNS cache. Enabling DNS cache increases MCP's resilience towards network issues between MCP and the DNS Servers. If the option is enabled, the target address is retrieved from the DNS cache, if available. If unavailable, a fresh DNS query will be used to retrieve the target address and the result will be cached depending on the DNS query response. If the option is disabled, target address is resolved by a fresh DNS query.

enablemaddr

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

Enables SIP VIA maddr parameter support as per RFC 3261. Disabling prevents the SIP Stack from respecting the maddr parameter (needed when multicast support requires that the maddr parameter is not used).

enablesendrecvevents

Default Value: true
Valid Values: Choose between: true or false
Changes Take Effect: Immediately/session

Enabled the receiving and sending of SIP INFO messages for application module usage. SIP INFO for other purposes (ie, DTMF) will not be affected.

enabletfci

Default Value: 0
Valid Values: Choose between: 0 or 1
Changes Take Effect: At start/restart

Allows TFCI (Telephony Free Client Interface) outbound calls. If this configuration is set to Enable, the To header of the outbound SIP INVITE request will be customized for TFCI devices.

handlesessionrefreshsdp

Default Value: matchfull
Valid Values: Choose between: matchfull, matchversion or matchnone
Changes Take Effect: Immediately/session

Defines the behavior for handling SDP in SIP session refresh requests. When set to "matchfull", the SDP received during session refresh request is compared with the previous remote SDP received and if matching, MCP returns the last sent SDP without performing SDP renegotiation. If SDP's don't match then SDP renegotiation is performed. When set to "matchversion", only the version(origin field) of SDP received during session refresh request is compared with the version of previous remote SDP received and if matching, MCP returns last sent SDP without performing SDP renegotiation. If SDP versions don't match then SDP renegotiation is performed. When set to "matchnone", no comparison is performed for the SDP received in session refresh request and SDP renegotiation is performed.

hfdisctimer

Default Value: 5000
Valid Values: sip.hfdisctimer should be positive integer and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

The timeout value (in milliseconds) to terminate SIP hookflash transfer. For "Hookflash/wait for disconnect" mode, if a BYE is not received from remote end before this timeout, then the transfer is treated as failed (otherwise, the transfer is successful). For "Hookflash/initiate disconnect" mode, if a BYE is not received from remote end, then a BYE will be sent from local end after this timeout and the transfer is treated as successful whether BYE is received from remote end or generated from local end

hfprefix

Default Value: !
Valid Values: sip.hfprefix should only contain 0-9, !, *, or none
Changes Take Effect: At start/restart

SIP hookflash transfer dialing prefix. Example: sip.hfprefix=none means dial string is exactly as specified in <transfer> sip.hfprefix=! would dial a hookflash, and then the pattern in <transfer> sip.hfprefix=*8,, would dial a '*8' followed by two pause durations

hfstopdial

Default Value: !
Valid Values: sip.hfstopdial should only contain 0-9, !
Changes Take Effect: At start/restart

digits to dial to stop a hookflash transfer. Character(s) to dial to abort a multi-phase hookflash. It will switch the connection back to original caller.

hftype

Default Value: 0
Valid Values: Choose between: 0 or 1
Changes Take Effect: At start/restart

Hook flash transfer type for sip. 0 - Wait for disconnection 1 - Force disconnectio

in.bye.headers

Default Value: Reason
Valid Values: A valid entry can only contain alphanumeric characters, '.', '-', and ':*characters, or the wildcard,* '*'
Changes Take Effect: At start/restart

Defines list of headers to expose to the application. This specifies a list of header names from the incoming BYE requests, whose values will be exposed to the application.

For example, sip.in.bye.headers = Reason. The exposed values' names will be in sip.invite.<headername>=<value> format. If this value is '*', then all headers will be exposed. If this value is 'none', then no headers will be exposed.

in.info.headers

Default Value: *
Valid Values: A valid entry can only contain alphanumeric characters, '.', '-', and ':*characters, or the wildcard,* '*'
Changes Take Effect: At start/restart

Defines list of headers to expose to the application. This specifies a list of header names from the incoming INFO requests, whose values will be exposed to the application.

For example, sip.in.info.headers = From To Via. The exposed values' names will be in sip.info.<headername>=<value> format. If this value is '*', then all headers will be exposed. If this value is 'none', then no headers will be exposed. 'none' will be ignored alongside other values.

in.invite.headers

Default Value: *
Valid Values: A valid entry can only contain alphanumeric characters, '.', '-', and ':*characters, or the wildcard,* '*'
Changes Take Effect: At start/restart

Defines list of headers to expose to the application. This specifies a list of header names from the incoming INVITE requests, whose values will be exposed to the application.

For example, sip.in.invite.headers = From To Via. The exposed values' names will be in sip.invite.<headername>=<value> format. If this value is '*', then all headers will be exposed. If this value is 'none', then no headers will be exposed. 'none' will be ignored alongside other values.

in.invite.params

Default Value: RequestURI
Valid Values: A valid entry can only contain alphanumeric characters, '.', '-', and ':*characters*

Changes Take Effect: At start/restart

Defines list of parameters to expose to the application. This specifies a list of header names from the incoming INVITE requests, whose parameter values will be exposed to the application.

For example, sip.in.invite.params = From To Via. The exposed values' names will be in sip.invite.<headername>.<paramname>=<value> format. If this value is 'none', then no parameters will be exposed. 'none' will be ignored alongside other values.

info.contenttype

Default Value: application/text
Valid Values: Any character is allowed
Changes Take Effect: At start/restart

Specifies content type of outgoing SIP INFO messages that correspond to VoiceXML <log> application events. A VoiceXML application can trigger the sending of a SIP INFO message by using <log> tag with dest="callmgr". The MCP will then send a SIP INFO message to the remote end with content being the content of the <log> tag. The default content type is "application/text".

localuser

Default Value: Genesys
Valid Values: Any string
Changes Take Effect: At start/restart

Configures the user name portion of the Contact header generated from the MCP

logmsg.allowed

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

Specifies wether or not logging SIP message is allowed. This option can disable SIP message logging regardless the [log].verbose setting.

logmsg.maskoption

Default Value: 0
Valid Values: An integer greater or equal to 0.
Changes Take Effect: At start/restart

Specifies the option to restrict SIP message logging. Each bit in the value (starting with LSB) indicates that a specific entity of the SIP message is masked. These bits can be logically OR'ed (or numerically added) and the final value is set. Currently the following bits are supported:
value 1 - indicates all unknown headers (headers other than "Via", "From", "To", "Max-Forwards", "CSeq", "Call-ID", "Contact", "Content-Length", "Content-Type", "Record-Route", "Route", "Refer-To", "Allow-Events", "Subscription-State", "Event", "RSeq", "RAck") will be masked.
value 2 - indicates all user data headers (headers starting with "X-Genesys-" except "X-Genesys-GVP-Session-Data", "X-Genesys-GVP-Session-ID", "X-Genesys-CallUUID") will be masked.
value 4 - indicates all SIP message bodies will be masked.
value 8 - indicates the SIP message bodies with the content type "application/dtmf-relay" or "application/dtmf" will be masked.
value 16 - indicates the values of MSML tag "gvp:param" with the name start with "X-Genesys-" in SIP message bodies will be masked.
For example, to mask all unknown headers and message bodies, set the value to 5 (i.e. 1 + 4). To mask all user data headers and the values of MSML tag "gvp:param" with the name start with "X-Genesys-" in SIP message bodies, set the value to 18 (i.e. 2 + 16). Default value is 0, meaning no masking at all.

maxtcpaccepts

Default Value: 100
Valid Values: The maximum number of connections must be an integer from 1 to 1000 inclusive
Changes Take Effect: At start/restart

Defines the maximum number of TCP connections that can be accepted at a time. The method for rejecting new concurrent TCP connection attempts above this amount is operating system dependant. If configured to higher than the operating system limit, the system limit will be used. Will automatically be set to [sip]maxtcpconnections if it is less than this value.

maxtcpconnections

Default Value: 100
Valid Values: The maximum number of connections must be an integer from 1 to 10000 inclusive
Changes Take Effect: At start/restart

Defines the maximum number of TCP connections concurrently established. If the maximum number of TCP connections has been reached, new SIP requests to establish TCP connections will be rejected

maxtlsaccepts

Default Value: 100
Valid Values: The maximum number of connections must be an integer from 1 to 1000 inclusive
Changes Take Effect: At start/restart

Defines the maximum number of TLS connections that can be accepted at a time. The method for rejecting new concurrent TLS connection attempts above this amount is operating system dependant.

If configured to higher than the operating system limit, the system limit will be used. Will automatically be set to [sip]maxtlsconnections if it is less than this value.

maxtlsconnections

Default Value: 100
Valid Values: The maximum number of TLS connections must be an integer from 1 to 10000 inclusive
Changes Take Effect: At start/restart

Defines the maximum number of TLS connections concurrently established. If the maximum number of TLS connections has been reached, new SIP requests to establish TLS connections will be rejected.

min_se

Default Value: 90
Valid Values: The parameter size must be an integer from 90 to 3600 inclusive
Changes Take Effect: At start/restart

Defines the Min-SE parameter in seconds. This is the minimum duration of session expiry this SIP stack will accept from a user agent client.

mpc.copyheaders

Default Value: X-Genesys-geo-location
Valid Values: A valid header can only contain alphanumeric characters, '.', '-', ':', '/' and '\' characters, and space is used to separate the headers
Changes Take Effect: At start/restart

Copy the specified headers from inbound call INVITE messages and pass them to the MPC. These headers are currently used by the third-party call recording feature only, and are copied to the outgoing INVITE messages to a recorder. If "none" is the only value present, no headers will be copied. Empty string results in the default value being used. Note that the special value "*" is not supported for this parameter.

mtusize

Default Value: 1500
Valid Values: The MTU size must be an integer from 1 to 65535 inclusive
Changes Take Effect: At start/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.

out.info.headers

Default Value: *
Valid Values: A valid entry can only contain alphanumeric characters, '.', '-', and ':*characters, or the wildcard,* '*'
Changes Take Effect: At start/restart

Defines list of headers to expose to the application. This specifies a list of header names from the outgoing INFO requests, whose values can be customized by the application.

For example, sip.out.info.headers = From To Via. The customized values' names will be in sip.info.<headername>=<value> format. If this value is '*', then all headers will be exposed. If this value is 'none', then no headers will be exposed. 'none' will be ignored alongside other values.

out.invite.headers

Default Value: *
Valid Values: A valid entry can only contain alphanumeric characters, '.', '-', and ':*characters, or the wildcard,* '*'
Changes Take Effect: At start/restart

Defines list of headers to expose to the application. This specifies a list of header names from the outgoing INVITE requests, whose values can be customized by the application.

For example, sip.out.invite.headers = From To Via. The customized values' names will be in sip.invite.<headername>=<value> format. If this value is '*', then all headers will be exposed. If this value is 'none', then no headers will be exposed. 'none' will be ignored alongside other values.

out.invite.params

Default Value: RequestURI
Valid Values: A valid entry can only contain alphanumeric characters, '.', '-', and ':*characters*
Changes Take Effect: At start/restart

Defines list of parameters to expose to the application. This specifies a list of header names from the outgoing INVITE requests, whose parameter values can be customized by the application. sip.out.invite.params = RequestURI.

The customized values' names will be in sip.invite.<headername>.<paramname>=<value> format. If this value is 'none', then no headers will be exposed. 'none' will be ignored alongside other values.

out.refer.headers

Default Value: *

Valid Values: A valid entry can only contain alphanumeric characters, '.', '-', and ':*characters, or the wildcard,* '*'
Changes Take Effect: At start/restart

Defines list of headers to expose to the application. This specifies a list of header names from the outgoing REFER requests, whose values can be customized by the application. For example, sip.out.refer.headers = From To Via.

The customized values' names will be in sip.refer.<headername>=<value> format.

out.refer.params

Default Value: RequestURI
Valid Values: A valid entry can only contain alphanumeric characters, '.', '-', and ':*characters*
Changes Take Effect: At start/restart

Defines list of parameters to expose to the application. This specifies a list of header names from the outgoing REFER requests, whose parameter values can be customized by the application. sip.out.refer.params = RequestURI.

The customized values' names will be in sip.refer.<headername>.<paramname>=<value> format.

outcalluseoriggw

Default Value: 1
Valid Values: Choose between: 0 or 1
Changes Take Effect: At start/restart

If a SIP call is placed via call or transfer, and the destination address does not contain a hostname or IP address, this parameter will determine which gateway to use. If sip.outcalluseroriggw is set to Enable, the call will be placed using the gateway of the inbound call (e.g. tel://3000 or sip:3000@; "@" is mandatory for the sip: schema in order to make the distinction between user part and host). If sip.outcalluseroriggw is set to Disable, either sip.defaultgw or sip.defaulthost will be used..

p-alcatel-csbu

Default Value: fb=notransfer;dtmf_auto=on
Valid Values: Can be an empty string or a valid SIP header string.
Changes Take Effect: Immediately/session

This parameter specifies the value to be set in the P-Alcatel-CSBU header of the 200OK response to the initial incoming INVITE, when the request contains this header. If the parameter value is empty string, no header will be set.

passertedidentity

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

This parameter specifies whether the P-Asserted-Identity header will be used as the ANI if it is found in the incoming SIP INVITE and its value will be exposed to the VXML interpreter through the session.connection.remote.uri session variable. Otherwise, the From header will be used. 0 - Do not use the P-Asserted-Identity header value for ANI 1 - Use P-Asserted-Identity header value for ANI

pcalledpartyid

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

This parameter specifies whether the P-Called-Party-ID header will be used as the DNIS, if it is found in the incoming SIP INVITE and its value will be exposed to the VXML interpreter through the session.connection.local.uri session variable. Otherwise, the To header will be used. 0 - Do not use the P-Called-Party-ID header value for DNIS 1 - Use P-Called-Party-ID header value for DNIS

prack.support

Default Value: 0
Valid Values: Choose between: 0, 1 or 2
Changes Take Effect: At start/restart

This parameter will allow the SIP Stack to send reliable the 101-199 provisional responses. The parameter value of 1 or 2 will enable the PRACK support. If the parameter value is set to 2 the MCP will include the "100rel" extension in the Require header of the outbound INVITE request, forcing a remote user that supports PRACK method to sent the provisional responses reliable. If the parameter value is set to 1, the "100rel" extension will be included in the Supported header of the outbound INVITE request giving the remote user the option to send or not the provisional responses reliable. The default parameter value is 0.

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. 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, other version will be used. Valid values are "ipv4" and "ipv6".

referredby

Default Value:
Valid Values: Can be an empty string or a valid SIP header value.
Changes Take Effect: At start/restart

Specifies the header value of Referred-By in REFER message. "none" means no Referred-By header will be included in the REFER request. Empty (default) implies the local MCP SIP URI (ie, To header for inbound call or From header for outbound call) for the dialog will be used.

referxferhold

Default Value: 0
Valid Values: Choose between: 0 or 1
Changes Take Effect: At start/restart

Put originator on hold before refer or referjoin transfer. This specifies whether to put the original caller on hold (Invite hold) before sending the REFER for the transfer.

referxfertryoutbound

Default Value: 0
Valid Values: Choose between: 0 or 1
Changes Take Effect: At start/restart

Retry REFER on the outbound leg if the REFER with Replaces request fails on the inbound leg. Valid only for REFER with Replace transfer.

referxferwaitbye

Default Value: 0
Valid Values: sip.referxferwaitbye should be a non-negative integer and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

Wait for remote to disconnect after NOTIFY. This specifies a timeout value to wait for BYE message from the remote end before sending BYE to disconnect the call. If it is zero, it will send BYE right after a NOTIFY/200 is received. If it is non-zero, it will wait for the configured timeout (in milliseconds) before sending the BYE. Values are specified in millisecond.

referxferwaitnotify

Default Value: 1
Valid Values: Choose between: 0 or 1
Changes Take Effect: At start/restart

This parameter is applicable to REFER transfer. If this is set to Enable, LMSIP2 will wait for NOTIFY with a sipflag message with a final response after receiving a 2xx REFER response. If this is set to Disable, LMSIP will not wait for NOTIFY. After that, LMSIP2 will either be sending a BYE request or expecting a BYE request from the caller depending on the value of sip.referxferwaitbye.

registerexpiryadjustment

Default Value: 10
Valid Values: sip.registerexpiryadjustment should be non-negative integer and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

Specifies the amount of time (in seconds) that the MCP should re-register with the configured registrars before their respective expiration times are reached

registration

Default Value:
Valid Values: <registration-server> <register-as> <requested-expiry> <username> <passowrd> [<routeset>]
Changes Take Effect: At start/restart

Specifies setting for registration. The system can be configured to register with one or more SIP registration servers on the network.

The format of the value for sip.registration entries is: <registration-server> <register-as> <requested-expiry> <username> <passowrd> <routeset> All parameters except routeset are compulsory.

<registration-server> - Host/port with which to register. As the domain of the location service (e.g. genesyslab.com), the "userinfo" and "@" components MUST NOT be present. sip: and sips: can be prefixed to indicate which protocol to use. sip: will be used by default.

<register-as> - SIP identity to register as. sip: or sips: can be prefixed to indicate which protocol to use. sip: will be used by default.

<requested-expiry> - Duration of registration; system will re-register after registration expires

<username> - The user name when authentication is required by the server. This may or may not be the same as register-as.A dash - should be used if no user name is needed.Anonymous will be used if the server request authentication under this setting.

<password> - The password associated with the authentication user name. To specify an empty string please use the dash - character.

<routeset> - Route set to define the list of server(s) that the REGISTER messages should go through. Each entry separated by a comma and no space in between. If left empty, the REGISTER messages will be sent directly to the registration-server. The system will attempt to register with all defined registration entries and will periodically re-register as required by the requested-expiry parameter. The system will unregister when shutting down.

e.g. sip.registration = proxy1.genesyslab.com:5064 mcp@10.0.0.101 60 -
-|sip:proxy2.genesyslab.com:5064 sip:mcp@10.0.0.102 60 user password

route.default.tcp

Default Value:
Valid Values: Must be a numeric, but can be empty
Changes Take Effect: At start/restart

Default route for TCP. The number denotes the transport defined in sip.transport.x where x is the value of this parameter and will be used when no TCP routes are found.

route.default.tls

Default Value:
Valid Values: Must be a numeric, but can be empty
Changes Take Effect: At start/restart

Default route for TLS. The number denotes the transport defined in sip.transport.x where x is the value of this parameter and will be used when no TLS routes are found.

route.default.udp

Default Value:
Valid Values: Must be a numeric, but can be empty
Changes Take Effect: At start/restart

Default route for UDP. The number denotes the transport defined in sip.transport.x where x is the value of this parameter and will be used when no UDP routes are found. If this parameter is not set, the first UDP transport found in sip.transport.x becomes the default.

route.dest.0

Default Value:
Valid Values: <Destination> <Netmask> <Transport> <Metric>

Changes Take Effect: At start/restart

This is an entry in routing table.
Format: sip.route.dest.x=[Destination] [Netmask] [Transport] [Metric]
To select an entry in routing table, we mask the outgoing IP Address with [Netmask]; if the result matches with the [Destination], we will accept that route. The [Transport] part determines the transport to use and maps to the index 'x' in one of the transports defined as sip.transport.x. In most of the cases, first accepted route will be used. Unless the protocol is specified or required (for example, when the message size is larger than mtusize, tcp is required to be used), the accepted route in routing table is also required to have matched protocol. If there.s no such route, default transport of that protocol will be used.
If all cases failed, sip.transport.0.s protocol will be obtained. The default transport of the obtained protocol will be used.
Note that [Metric] entry is needed but not used at this point.
For example: sip.route.dest.0=138.120.72.0 255.255.255.0 1 0
When we make a call to the machine 138.120.72.20, outgoing IP is masked with [netmask] using .bitwise AND. operator. In this case: 138.120.72.20 & 255.255.255.0 gives 138.120.72.0. This matches the defined [Destination] in the route. Therefore, transport in sip.transport.1 will be used.

route.dest.1

Default Value:
Valid Values: <Destination> <Netmask> <Transport> <Metric>
Changes Take Effect: At start/restart

This is an entry in routing table.
Format: sip.route.dest.x=[Destination] [Netmask] [Transport] [Metric]
To select an entry in routing table, we mask the outgoing IP Address with [Netmask]; if the result matches with the [Destination], we will accept that route. The [Transport] part determines the transport to use and maps to the index 'x' in one of the transports defined as sip.transport.x. In most of the cases, first accepted route will be used. Unless the protocol is specified or required (for example, when the message size is larger than mtusize, tcp is required to be used), the accepted route in routing table is also required to have matched protocol. If there.s no such route, default transport of that protocol will be used.
If all cases failed, sip.transport.0.s protocol will be obtained. The default transport of the obtained protocol will be used.
Note that [Metric] entry is needed but not used at this point.
For example: sip.route.dest.0=138.120.72.0 255.255.255.0 1 0
When we make a call to the machine 138.120.72.20, outgoing IP is masked with [netmask] using .bitwise AND. operator. In this case: 138.120.72.20 & 255.255.255.0 gives 138.120.72.0. This matches the defined [Destination] in the route. Therefore, transport in sip.transport.1 will be used.

route.dest.2

Default Value:
Valid Values: <Destination> <Netmask> <Transport> <Metric>
Changes Take Effect: At start/restart

This is an entry in routing table.
Format: sip.route.dest.x=[Destination] [Netmask] [Transport] [Metric]
To select an entry in routing table, we mask the outgoing IP Address with [Netmask]; if the result matches with the [Destination], we will accept that route. The [Transport] part determines the transport to use and maps to the index 'x' in one of the transports defined as sip.transport.x. In most of the cases, first accepted route will be used. Unless the protocol is specified or required (for example, when the message size is larger than mtusize, tcp is required to be used), the accepted route in routing table is also required to have matched protocol. If there.s no such route, default transport of that protocol will be used.
If all cases failed, sip.transport.0.s protocol will be obtained. The default transport of the obtained protocol will be used.
Note that [Metric] entry is needed but not used at this point.
For example: sip.route.dest.0=138.120.72.0 255.255.255.0 1 0
When we make a call to the machine 138.120.72.20, outgoing IP is masked with [netmask] using .bitwise AND. operator. In this case: 138.120.72.20 & 255.255.255.0 gives 138.120.72.0. This matches the defined [Destination] in the route. Therefore, transport in sip.transport.1 will be used.

route.dest.3

Default Value:
Valid Values: <Destination> <Netmask> <Transport> <Metric>
Changes Take Effect: At start/restart

This is an entry in routing table.
Format: sip.route.dest.x=[Destination] [Netmask] [Transport] [Metric]
To select an entry in routing table, we mask the outgoing IP Address with [Netmask]; if the result matches with the [Destination], we will accept that route. The [Transport] part determines the transport to use and maps to the index 'x' in one of the transports defined as sip.transport.x. In most of the cases, first accepted route will be used. Unless the protocol is specified or required (for example, when the message size is larger than mtusize, tcp is required to be used), the accepted route in routing table is also required to have matched protocol. If there.s no such route, default transport of that protocol will be used.
If all cases failed, sip.transport.0.s protocol will be obtained. The default transport of the obtained protocol will be used.
Note that [Metric] entry is needed but not used at this point.
For example: sip.route.dest.0=138.120.72.0 255.255.255.0 1 0
When we make a call to the machine 138.120.72.20, outgoing IP is masked with [netmask] using .bitwise AND. operator. In this case: 138.120.72.20 & 255.255.255.0 gives 138.120.72.0. This matches the defined [Destination] in the route. Therefore, transport in sip.transport.1 will be used.

route.dest.4

Default Value:
Valid Values: <Destination> <Netmask> <Transport> <Metric>
Changes Take Effect: At start/restart

This is an entry in routing table.
Format: sip.route.dest.x=[Destination] [Netmask] [Transport] [Metric]
To select an entry in routing table, we mask the outgoing IP Address with [Netmask]; if the result

matches with the [Destination], we will accept that route. The [Transport] part determines the transport to use and maps to the index 'x' in one of the transports defined as sip.transport.x. In most of the cases, first accepted route will be used. Unless the protocol is specified or required (for example, when the message size is larger than mtusize, tcp is required to be used), the accepted route in routing table is also required to have matched protocol. If there.s no such route, default transport of that protocol will be used.
If all cases failed, sip.transport.0.s protocol will be obtained. The default transport of the obtained protocol will be used.
Note that [Metric] entry is needed but not used at this point.
For example: sip.route.dest.0=138.120.72.0 255.255.255.0 1 0
When we make a call to the machine 138.120.72.20, outgoing IP is masked with [netmask] using .bitwise AND. operator. In this case: 138.120.72.20 & 255.255.255.0 gives 138.120.72.0. This matches the defined [Destination] in the route. Therefore, transport in sip.transport.1 will be used.

route.dest.5

Default Value:
Valid Values: <Destination> <Netmask> <Transport> <Metric>
Changes Take Effect: At start/restart

This is an entry in routing table.
Format: sip.route.dest.x=[Destination] [Netmask] [Transport] [Metric]
To select an entry in routing table, we mask the outgoing IP Address with [Netmask]; if the result matches with the [Destination], we will accept that route. The [Transport] part determines the transport to use and maps to the index 'x' in one of the transports defined as sip.transport.x. In most of the cases, first accepted route will be used. Unless the protocol is specified or required (for example, when the message size is larger than mtusize, tcp is required to be used), the accepted route in routing table is also required to have matched protocol. If there.s no such route, default transport of that protocol will be used.
If all cases failed, sip.transport.0.s protocol will be obtained. The default transport of the obtained protocol will be used.
Note that [Metric] entry is needed but not used at this point.
For example: sip.route.dest.0=138.120.72.0 255.255.255.0 1 0
When we make a call to the machine 138.120.72.20, outgoing IP is masked with [netmask] using .bitwise AND. operator. In this case: 138.120.72.20 & 255.255.255.0 gives 138.120.72.0. This matches the defined [Destination] in the route. Therefore, transport in sip.transport.1 will be used.

routeset

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

Defines a route set for non-secure SIP outbound calls. If defined, this route set will be inserted as the ROUTE header for all outgoing calls. This will force the MCP to send the SIP messages via this defined route set.

Each element in the routeset should be separated by a comma. This parameter can be used to define outbound proxies. Note that this routeset does not apply to SIP REGISTER messages.

sip.routeset = <sip:ip/host;priority>, ... e.g.
sip.routeset=<sip:p1.example.com;lr>,<sip:p2.domain.com;lr>,<sip:IP_RM:SIP_Port_RM;lr>

In this example, the MCP will route the request to p1.example.com, which will in turn route the message to p2.domain.com, and finally be redirected to its intended destination.

This option is not applicable for transfer outbound calls initiated using VoiceXML. A transfer outbound call will use the same route set from the call initiated the transfer.

sdpansinprov

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

If this configuration option is enabled and the incoming INVITE contains an SDP offer, MCP will generate the SDP answer in the 101-199 provisional responses. NOTE: This configuration option applies if the [sip]prack.support is set to 1 or 2 (PRACK support is enabled) or the [sip]sendalert configuration option is set to 2 (183 Session Progress response). The default value is 1.

sdpwarningheaders

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

This parameter will enable the SIP warning headers created as a result of SDP negotiation. 0 - Don't send the SDP warning headers in the SIP responses 1 - Send the SDP warning headers in the SIP responses

securerouteset

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

Defines a route set for secure SIP outbound calls. Secure SIP calls 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 outgoing calls. This will force the MCP to send the SIP messages via this defined route set.

Each element in the routeset should be separated by a comma. This parameter can be used to define outbound proxies. Note that this routeset does not apply to SIP REGISTER messages.

sip.securerouteset = <sips:ip/host;priority>, ... e.g.

sip.secureouteset=<sips:p1.example.com;lr>,<sips:p2.domain.com;lr>,<sip:IP_RM:SIP_Port_RM;lr>

In this example, the MCP will route the request to p1.example.com, which will in turn route the message to p2.domain.com, and finally be redirected to its intended destination.

This option is not applicable for transfer outbound calls initiated using VoiceXML. A transfer outbound call will use the same route set from the call initiated the transfer.

sendalert

Default Value: 1
Valid Values: Choose between: 0, 1 or 2
Changes Take Effect: Immediately/session

Specifies the SIP response for alerting. NOTE: Use the [sip]sdpansinprov configuration option to include an SDP answer in the 183 Session Progress response if incoming INVITE contains an SDP offer. The default value is 1. 0 - No SIP response 1 - Send 180 RINGING response 2 - Send 183 Session Progress response

sessionexpires

Default Value: 1800
Valid Values: The parameter size must be an integer from 90 to 3600 inclusive
Changes Take Effect: At start/restart

Defines the default session expiry value in seconds. The session timer defines the duration of which a SIP session will expire if no re-INVITEs are sent/received within this period.

sipinfoallowedcontenttypes

Default Value:
Valid Values: A valid content type can only contain alphanumeric characters, and '/' or '\'
Changes Take Effect: At start/restart

Content types in a SIP INFO messages that are allowed to be passed up to the application level. Only the defined content types would be passed up, others would be ignored. If left empty, the default value is "allowall", which means the content of all received SIP INFO messages would be passed upstream. This is a space delimited list of values.

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, MCP will let the OS choose the local port.

threadpoolsize

Default Value: 4
Valid Values: A valid value is an integer from 1 to 100 inclusive.
Changes Take Effect: At start/restart

The size of the thread pool for handling DNS queries.

threads

Default Value: 0
Valid Values: A number between 0 and 99 inclusive.
Changes Take Effect: After restart

Specifies the number of worker threads that handles the SIP requests arriving from the SIP transport layer. If the value is 0, all requests are handled within the arriving transport layer thread. Otherwise, all arriving requests are handled by hashing onto the N number of worker threads.

timer_si

Default Value: 32000
Valid Values: The parameter must be an integer that is greater than 0 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

Defines the server INVITE retransmission aborting timer in milliseconds, default value is 32000. The timer starts after a 2xx response is sent for a server INVITE. If an ACK is not received before the timer expires, a BYE message will be sent.

timer.ci_proceeding

Default Value: 120000
Valid Values: sip.timer.ci_proceeding must be an integer that is greater than 0 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

Defines the client INVITE proceeding timer in milliseconds, default value is 120000. The timer starts after a 1xx response is received for a client INVITE. If a final response is not received before the timer expires, the SIP session and dialog will be destroyed without further notice to the UAS. Note that the CI proceeding timer should be configured to be greater than the connect timeout of the outbound call (depending on how the outbound call is initiated, the connect timeout can be specified in the transfer tag, or in the remdial command). Otherwise, the Client Invite Proceeding Timer will be triggered before the connect timeout occurs, which overrides the connect timeout as a result.

timer.provretransmit

Default Value: 60000
Valid Values: [sip]timer.provretransmit must be an integer that is greater than 60000 and less than 150000.
Changes Take Effect: At start/restart

Defines the server provisional response (101-199) retransmit timer in milliseconds. The timer starts after a 101-199 provisional response is sent for the server INVITE. If a final response is not ready before the timer expires, the UA transaction will retransmit the provisional response to extend the transaction on the proxies (refresh TIMER C). Note that the [sip]timer.provretransmit value should be configured to 150000 ms if reliable provisional responses is enabled (please see the description of the [sip]prack.support parameter). If the value of the parameter is set outside the defined range, the actual value will use the boundary value. The default value is 60000.

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, MCP will let the OS choose the local port.

transfermethods

Default Value: HKF REFER REFERJOIN MEDIAREDIRECT ATTCOURTESY ATTCONSULT ATTCONFERENCE ATTOOBCOURTESY ATTOOBCONSULT ATTOOBCONFERENCE NEC61ISDN
Valid Values: Any combination of: HKF, REFER, REFERJOIN, MEDIAREDIRECT, ATTCOURTESY, ATTCONSULT, ATTCONFERENCE, ATTOOBCOURTESY, ATTOOBCONSULT, ATTOOBCONFERENCE, NEC61ISDN and none
Changes Take Effect: At start/restart

Transfer Methods for sip. The final option will be ignored if selected with other options. HKF - HookFlash REFER - REFER-based transfer REFERJOIN - Consultative REFER transfer MEDIAREDIRECT - Media redirect transfer ATTCOURTESY - AT&T courtesy transfer ATTCONSULT - AT&T consult transfer ATTCONFERENCE - AT&T conference transfer ATTOOBCOURTESY - AT&T out-of-band courtesy transfer ATTOOBCONSULT - AT&T out-of-band consult transfer ATTOOBCONFERENCE - AT&T out-of-band conference transfer NEC61ISDN - Single B channel blind transfer over ISDN for NEC NEAX 61 switch none - No Transfer Methods for sip

transport.0

Default Value: transport0 udp:any:5070
Valid Values: <transport_name> <type>:<ip-address>:<port> [parameters]
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 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_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.
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 crlenabled=true Mandatory for CRL validation. Enabling this parameter will only validate the CRL on the client connection(For Server Certificate). To validation the CRL on server connection(For Client Certificate) the verifypeer should be enabled along with this parameter. crlpaths=[CRL cert filenames with absolute path] Mandatory for CRL validation. The filenames of semi-colon separated certificates for CRL validation. 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.

transport.0.tos

Default Value: 0
Valid Values: Possible values are integers from 0 to 255 inclusive.
Changes Take Effect: At start/restart

Specifies the IP Differentiated Services Field (also known as ToS) to set in all outgoing SIP packets over transport instance 0. Note that this configuration does not work for Windows. For Windows, the setting needs to be configured at the OS level through the policy settings. Please refer to the GVP User's Guide.

transport.1

Default Value: transport1 tcp:any:5070
Valid Values: <transport_name> <type>:<ip-address>:<port> [parameters]
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 [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. port is the port number where SIP stack accepts incoming SIP messages;
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_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.
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 crlenabled=true Mandatory for CRL validation. Enabling this parameter will only validate the CRL on the client connection(For Server Certificate). To validation the CRL on server connection(For Client Certificate) the verifypeer should be enabled along with this parameter. crlpaths=[CRL cert filenames with absolute path] Mandatory for CRL validation. The filenames of semi-colon separated certificates for CRL validation. 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.

transport.1.tos

Default Value: 0
Valid Values: Possible values are integers from 0 to 255 inclusive.
Changes Take Effect: At start/restart

Specifies the IP Differentiated Services Field (also known as ToS) to set in all outgoing SIP packets over transport instance 1. Note that this configuration does not work for Windows. For Windows, the setting needs to be configured at the OS level through the policy settings. Please refer to the GVP User's Guide.

transport.2

Default Value: transport2 tls:any:5071 cert=$InstallationRoot$/config/x509_certificate.pem key=$InstallationRoot$/config/x509_private_key.pem
Valid Values: <transport_name> <type>:<ip-address>:<port> [parameters]
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 [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. port is the port number where SIP stack accepts incoming SIP messages;
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_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.
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 crlenabled=true Mandatory for CRL validation. Enabling this parameter will only validate the CRL on the client connection(For Server Certificate). To validation the CRL on server connection(For Client Certificate) the verifypeer should be enabled along with this parameter. crlpaths=[CRL cert filenames with absolute path] Mandatory for CRL validation. The filenames of semi-colon separated certificates for CRL validation. 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.

transport.2.tos

Default Value: 0
Valid Values: Possible values are integers from 0 to 255 inclusive.
Changes Take Effect: At start/restart

Specifies the IP Differentiated Services Field (also known as ToS) to set in all outgoing SIP packets over transport instance 2. Note that this configuration does not work for Windows. For Windows, the setting needs to be configured at the OS level through the policy settings. Please refer to the GVP User's Guide.

transport.3

Default Value:
Valid Values: <transport_name> <type>:<ip-address>:<port> [parameters]
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 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_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.
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 crlenabled=true Mandatory for CRL validation. Enabling this parameter will only validate the CRL on the client connection(For Server Certificate). To validation the CRL on server connection(For Client Certificate) the verifypeer should be enabled along with this parameter. crlpaths=[CRL cert filenames with absolute path] Mandatory for CRL validation. The filenames of semi-colon separated certificates for CRL validation. 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.

transport.3.tos

Default Value: 0
Valid Values: Possible values are integers from 0 to 255 inclusive.
Changes Take Effect: At start/restart

Specifies the IP Differentiated Services Field (also known as ToS) to set in all outgoing SIP packets over transport instance 3. Note that this configuration does not work for Windows. For Windows, the setting needs to be configured at the OS level through the policy settings. Please refer to the GVP User's Guide.

transport.4

Default Value:
Valid Values: <transport_name> <type>:<ip-address>:<port> [parameters]

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 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_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.
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 crlenabled=true Mandatory for CRL validation. Enabling this parameter will only validate the CRL on the client connection(For Server Certificate). To validation the CRL on server connection(For Client Certificate) the verifypeer should be enabled along with this parameter. crlpaths=[CRL cert filenames with absolute path] Mandatory for CRL validation. The filenames of semi-colon separated certificates for CRL validation. 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.

transport.4.tos

Default Value: 0
Valid Values: Possible values are integers from 0 to 255 inclusive.
Changes Take Effect: At start/restart

Specifies the IP Differentiated Services Field (also known as ToS) to set in all outgoing SIP packets over transport instance 4. Note that this configuration does not work for Windows. For Windows, the setting needs to be configured at the OS level through the policy settings. Please refer to the GVP User's Guide.

transport.5

Default Value:
Valid Values: <transport_name> <type>:<ip-address>:<port> [parameters]
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 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_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.
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 crlenabled=true Mandatory for CRL validation. Enabling this parameter will only validate the CRL on the client connection(For Server Certificate). To validation the CRL on server connection(For Client Certificate) the verifypeer should be enabled along with this parameter. crlpaths=[CRL cert filenames with absolute path] Mandatory for CRL validation. The filenames of semi-colon separated certificates for CRL validation. 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.

transport.5.tos

Default Value: 0
Valid Values: Possible values are integers from 0 to 255 inclusive.
Changes Take Effect: At start/restart

Specifies the IP Differentiated Services Field (also known as ToS) to set in all outgoing SIP packets over transport instance 5. Note that this configuration does not work for Windows. For Windows, the setting needs to be configured at the OS level through the policy settings. Please refer to the GVP User's Guide.

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.

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, 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: 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, 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: Choose between: true or 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: A number between 1 and 32 inclusive.
Changes Take Effect: At start/restart

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

transport.routerecoverytime

Default Value: 30
Valid Values: A number between 1 and 600 inclusive.
Changes Take Effect: At start/restart

Specifies the recovery time in seconds for SIP static routing and DNS HA routing. When SIP static routing or DNS HA routing is enabled and the 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.setuptimer.tcp

Default Value: 30000
Valid Values: Possible values are integers from 1000 to 32000 inclusive.
Changes Take Effect: At start/restart

Specifies the maximum wait time in milliseconds for establishing a TCP or TLS connection before marking the resource unavailable.

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.

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).

userouteonrecording

Default Value: true
Valid Values: Choose between: true or false
Changes Take Effect: Immediately/session

When performing third-party recording, this configuration will specify if the Record-Route on the incoming INVITE should be used in Route header of the INVITE for third party recording (if present). The effect of this setting would be to re-use the same Resource Manager used for incoming requests, increasing the likelihood of reaching an active Resource Manager. This overrides vrmrecorder.sip.routeset when enabled. If set to false, then MCP will use vrmrecorder.sip.routeset if present, otherwise it will not set the Route header.

voipmetrics.localhost

Default Value: sip:$LocalIP$:5070
Valid Values: Can be an empty string or a valid SIP address.
Changes Take Effect: At start/restart

sip.voipmetrics.localhost, sip.voipmetrics.remoteserver, and optionally sip.voipmetrics.routeset are used together to provide the configurability of VoIP metrics report via SIP PUBLISH method. The localhost represents the MCP performing VoIP metrics collection. The remoteserver represents the server collecting VoIP metrics report. The routeset can be optionally used to specify the route other than remote server address if alternate routes are required.

If sip.voipmetrics.remoteserver is not specified (blank in the configuration), VoIP metrics reporting will be disabled as no SIP PUBLISH method will be sent. sip.voipmetrics.localhost parameter can also be used to provide the fully qualified domain name in SIP requests. The format of the localhost is the host/port of the MCP and can be prefixed with sip: or sips: to indicate which protocol to use. sip: will be used by default. For example, sip.voipmetrics.localhost = sip:voipmetrics1.genesyslab.com:5060.

voipmetrics.registration

Default Value:
Valid Values: <registration-server> <register-as> <requested-expiry> <username> <passowrd> [<routeset>]
Changes Take Effect: At start/restart

This configuration performs exactly the same as registration configuration under sip section except it is exclusively used for VoIP metrics report. The system can be configured to register with one or more SIP registration servers on the network. If specified correctly, MCP will register itself to all registrars. If not specified, registration for VoIP metrics will not happen. For detailed information and how to configure, refer to registration configuration under sip section.

voipmetrics.remoteserver

Default Value:
Valid Values: Can be an empty string or a valid SIP address.
Changes Take Effect: At start/restart

sip.voipmetrics.localhost, sip.voipmetrics.remoteserver, and optionally sip.voipmetrics.routeset are used together to provide the configurability of VoIP metrics report via SIP PUBLISH method. The localhost represents the MCP performing VoIP metrics collection. The remoteserver represents the server collecting VoIP metrics report. The routeset can be optionally used to specify the route other than remote server address if alternate routes are required.

If sip.voipmetrics.remoteserver is not specified (blank in the configuration), VoIP metrics reporting will be disabled as no SIP PUBLISH method will be sent. sip.voipmetrics.remoteserver parameter can also be used to provide the fully qualified domain name in SIP requests. The format of the remoteserver is the host/port of the server collecting VoIP metrics through SIP PUBLISH method and can be prefixed with sip: or sips: to indicate which protocol to use. sip: will be used by default. For example, sip.voipmetrics.remoteserver = sip:voipmetrics2.genesyslab.com:5060.

voipmetrics.routeset

Default Value:
Valid Values: [sip:<ip>/<host>;<priority>][,sip:<ip>/<host>;<priority>]*
Changes Take Effect: At start/restart

Defines a route set for SIP PUBLISH for VoIP metrics report. If defined, this route set will be inserted as the ROUTE header for all SIP PUBLISH. This will force the MCP to send the SIP messages via this defined route set. Each element in the routeset should be separated by a comma and no space in between. This parameter can be used to define outbound proxies. The format is sip.voipmetrics.routeset = sip:ip1/host1;priority1,sip:ip2/host2;priority2, and so on. For example, sip.voipmetrics.routeset = sip:p1.example.com;lr,sip:p2.domain.com;lr. In this example, the MCP will route the SIP PUBLISH to p1.example.com, which will in turn route the message to p2.domain.com, and finally be redirected to its intended destination as specified in sip.voipmetrics.remoteserver.

vxmlinvite

Default Value: 1
Valid Values: Choose between: 0 or 1
Changes Take Effect: At start/restart

Specifies acceptance of VoiceXML URLs in INVITE message. It is possible for the originator of a SIP call to specify the initial VoiceXML URL that will be delivered on a session by encoding the Request-URI in the special form "sip:dialog.vxml.<URL>@host.com". The <URL> portion of the request URI must be encoded (e.g. : -> %3A). If such URLs are received, the normal DNIS mapping procedure will be bypassed, and the specified URL will be fetched.

warningheaders

Default Value: 0
Valid Values: Choose between: 0, 1 or 2
Changes Take Effect: Immediately/session

This parameter will enable the SIP warning headers. 0 - Send warning headers when the response is an error response 1 - Always send warning headers (if any) 2 - Never send warning headers

xfer.copyheaders

Default Value: *
Valid Values: A valid header can only contain alphanumeric characters, '.', '-', ':', ' ','/' and '\' characters
Changes Take Effect: Immediately

Copy specified headers from inbound call INVITE to outbound call INVITE for bridged calls and RLT calls. This parameter reads a space delimited list of header names. MCP will copy this list of header fields from an inbound call INVITE to outbound call INVITE of the same voicexml session (ie. bridged calls and RLT calls). Note that re-INVITE from the inbound call causes headers re-scan and applies latest changes on any outbound calls made within the call session. If "*" is present, all unknown headers will be copied. If "none" is the only value present, no headers will be copied. Empty string results in the default (*) being used. sip.copyheaders = VG-SS7-Xfer-Param