Genesys Voice Platform

proxy Section

4/21/2025

proxy Section

sip.enable_dns_cache

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

Specifies if RM should enable or disable the use of DNS cache. Enabling DNS cache increases RM's resilience towards network issues between RM 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.

sip.localuser

Default Value: GVP
Valid Values:

Changes Take Effect: After restart

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

sip.logmsg.allowed

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

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

sip.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.

sip.maxtcpconnections

Default Value: 100
Valid Values: The number must be from 1 to 10000 inclusive
Changes Take Effect: After restart

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

sip.maxtlsconnections

Default Value: 100
Valid Values: The number must be from 1 to 10000 inclusive
Changes Take Effect: After restart

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

sip.min_se

Default Value: 90
Valid Values:
Changes Take Effect: After restart

Specified in seconds, this is used to calculate the minimum value of the Session-Expires header the RM is willing to accept.

sip.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.

sip.preferred_ipversion

Default Value: ipv4
Valid Values: ipv4, 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".

sip.proxy.respaddr

Default Value:

Valid Values:
Changes Take Effect: After restart

The set of addresses or domains that the Resource Manager is responsible for

sip.route.default.tcp

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

Default IPv4 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 IPv4 TCP routes are found.

sip.route.default.tcp.ipv6

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

Default IPv6 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 IPv6 TCP routes are found. If this parameter is not set, the first IPv6 TCP transport found in sip.transport.x becomes the default.

sip.route.default.tls

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

Default IPv4 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 IPv4 TLS routes are found.

sip.route.default.tls.ipv6

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

Default IPv6 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 IPv6 TLS routes are found. If this parameter is not set, the first IPv6 TLS transport found in sip.transport.x becomes the default.

sip.route.default.udp

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

Default IPv4 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 IPv4 UDP routes are found.

sip.route.default.udp.ipv6

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

Default IPv6 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 IPv6 UDP routes are found. If this parameter is not set, the first IPv6 UDP transport found in sip.transport.x becomes the default.

sip.route.dest.0

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

For each <n> in the config parameter proxy.sip.route.dests, the parameter with name proxy.sip.route.dest.<n> must be present. Each of these represents an entry in the routing table. The format is: [Destination] [Netmask] [Transport] [Metric] The [Transport] entry corresponds to the index specified in 'sip.transport.x' configuration. The 'x' is the transport interface index. Each transport specified in 'sip.transport.x' must have at least one entry in the routing table, otherwise the interface will never be used. The order of destination does matter as the routing table is linearly searched until none of the rows matches, then the default entry for the specified protocol will be used. To select an interface, take the outgoing IP address. From the list of interfaces with the matching protocol, starting from the top row, mask the IP address with [Netmask] entry and compare with [Destination] entry. If [Destination] entry matches the masked value, then stop and use the interface defined in the [Transport] column. Note that the [Metric] entry must be configured but not used at this point.

sip.route.dests

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

A list of space-delimited entries in a routing table. The entry ID starts from 0 and increments by 1 each time. For example, to specify 4 entries in the routing table, the value would be "0 1 2 3"

sip.sessionexpires

Default Value: 1800
Valid Values:
Changes Take Effect: After restart

Specified in seconds, this is used to define the duration of which a SIP session will expire if no re-INVITEs are sent/received within this period. This value would take affect only if the associate application or its parent tenant did not specify the sip.sessiontimer parameter value. When this parameter takes effect, its value will be used if (1) if the proxy.sip.min_se value is configured, if the proxy.sip.sessiontimer value is less than the proxy.sip.min_se value, it will use the proxy.sip.min_se value for session expiration, or (2) if the proxy.sip.min_se value is not configured, if the proxy.sip.sessiontimer value is less than 90, 90 will be used.

sip.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, RM will let the OS choose the local port.

sip.threadpoolsize

Default Value: 4
Valid Values:
Changes Take Effect: After restart

The size of the thread pool for handling DNS queries

sip.threads

Default Value: 5
Valid Values:
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.

sip.timer_C

Default Value: 175000
Valid Values: The timer length in millisecond must be between 100 and 1000000
Changes Take Effect: After restart

Defines a timer for client transaction to handle the case where an INVITE request never generates a final response. The timer is set when the timer sip.timer_C1 fires. If a final response is not received before this timer fires, the client transaction is considered terminated. Default value is 175000 (175 seconds).

sip.timer_C1

Default Value: 6000
Valid Values: The timer length in millisecond must be between 100 and 1000000
Changes Take Effect: After restart

Defines a timer for client transaction to handle the case where an INVITE request never generates a final response. The timer is set when an INVITE request is proxied, and reset when a provisional response with status codes 101 to 199 inclusive is received. Once it fires, the timer sip.timer_C will be set. Default value is 6000 (6 seconds).

sip.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, RM will let the OS choose the local port.

sip.transport.0

Default Value: transport0 udp:any:5060
Valid Values:
Changes Take Effect: After restart

These parameters define transport layer for SIP stack and the network interfaces that are used to process SIP requests. 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; 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;

[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. 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. Note: The max path length supported for certificate and key file/path is 259 characters.

sip.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 Differentiaed Services Field (also known as ToS) to set in all outgoing SIP packets over the SIP transport. Note that this configuration does not work for Windows 2008 and above. For Windows 2008 and above, the setting needs to be configured at the OS level through the policy settings. Please refer to the GVP User's Guide.

sip.transport.1

Default Value: transport1 tcp:any:5060
Valid Values:
Changes Take Effect: After restart

These parameters define transport layer for SIP stack and the network interfaces that are used to process SIP requests. 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; 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;

[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. 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. Note: The max path length supported for certificate and key file/path is 259 characters.

sip.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 Differentiaed Services Field (also known as ToS) to set in all outgoing SIP packets over the SIP transport. Note that this configuration does not work for Windows 2008 and above. For Windows 2008 and above, the setting needs to be configured at the OS level through the policy settings. Please refer to the GVP User's Guide.

sip.transport.2

Default Value: transport2 tls:any:5061 cert=$InstallationRoot$/config/x509_certificate.pem key=$InstallationRoot$/config/x509_private_key.pem
Valid Values:
Changes Take Effect: After restart

These parameters define transport layer for SIP stack and the network interfaces that are used to process SIP requests. 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; 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;

[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. 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. Note: The max path length supported for certificate and key file/path is 259 characters.

sip.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 Differentiaed Services Field (also known as ToS) to set in all outgoing SIP packets over the SIP transport. Note that this configuration does not work for Windows 2008 and above. For Windows 2008 and above, the setting needs to be configured at the OS level through the policy settings. Please refer to the GVP User's Guide.

sip.transport.alarmtimer

Default Value: 60000
Valid Values: sip.transport.alarmtimer must be an integer that is greater than or equal to 0 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

This parameter specifies the time interval to wait between logging failure messages which are similar in nature. An initial alarm/log is generated on the first failure and if the similar failure continues we send another alarm notification with the updated failure count once the time interval specified by this parameter expires. The default value of this parameter is 1 minute(60000 milliseconds), which means that we would send failure alarm notification for the first failure and then send another alarm notification after 1 minute. This process is repeated until the root cause for the failure has been rectified.

sip.transport.dnsharouting

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

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

sip.transport.localaddress

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

If specified, the sent-by field of the Via header and the hostport part of the Record-Route 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 Record-Route 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.

sip.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 Record-Route 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 Record-Route 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.

sip.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.

sip.transport.routefailovertime

Default Value: 5
Valid Values:
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.

sip.transport.routerecoverytime

Default Value: 30
Valid Values:
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.

sip.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.

sip.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).

sip.udprecvbuffersize

Default Value: 262144
Valid Values:
Changes Take Effect: After restart

This value configures the UDP socket buffer size used for receiving at the OS level. This value should be set with a multiple of page size (4096).

sip.udpsendbuffersize

Default Value: 135168
Valid Values:
Changes Take Effect: After restart

This value configures the UDP socket buffer size used for sending at the OS level. This value should be set with a multiple of page size (4096). The recommended optimal value is that it should not be set to larger than 135168.