Genesys Voice Platform

sip Section

5/4/2025

sip Section

copyunknownheaders

Default Value: 1
Valid Values:
Changes Take Effect: At start/restart

Copy unknown headers from request to all responses. If this parameter is turned on, all unknown SIP headers found in SIP request will be automatically copied to its responses. 0 is disable and 1 is enable.

localuser

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

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

maxtcpconnections

Default Value: 100
Valid Values: The maximum number of connections must be between 1 and 10000
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

maxtlsconnections

Default Value: 100
Valid Values: The maximum number of TLS connections must be between 1 and 10000
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 between 90 and 3600
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.

mtusize

Default Value: 1500
Valid Values: The MTU size must be between 1 and 65535
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.

OPTIONS.header.Accept

Default Value: application/sdp
Valid Values:
Changes Take Effect: immediately

This defines the Accept header value in the SIP OPTIONS response.

OPTIONS.header.Accept-Encoding

Default Value:
Valid Values:
Changes Take Effect: immediately

This defines the Accept-Encoding header value in the SIP OPTIONS response.

OPTIONS.header.Accept-Language

Default Value: en
Valid Values:
Changes Take Effect: immediately

This defines the Accept-Language header value in the SIP OPTIONS response

OPTIONS.header.Allow

Default Value: INVITE,ACK,CANCEL,BYE,OPTIONS,INFO
Valid Values:
Changes Take Effect: immediately

This defines the Allow header value in the SIP OPTIONS response.

OPTIONS.header.Supported

Default Value:
Valid Values:
Changes Take Effect: immediately

This defines the Supported header value in the SIP OPTIONS response.

prack.support

Default Value: 0
Valid Values:
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 CCP 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: 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".

registerexpiryadjustment

Default Value: 10
Valid Values: sip.registerexpiryadjustment should be non-negative integer
Changes Take Effect: At start/restart

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

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.

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.

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.

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.

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.

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.

route.dest.0

Default Value:
Valid Values:
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 For example (ipv6): sip.route.dest.0=2620:0:60:: FFFF:FFFF:FFFF:: 0 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:
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 For example (ipv6): sip.route.dest.0=2620:0:60:: FFFF:FFFF:FFFF:: 0 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:
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 For example (ipv6): sip.route.dest.0=2620:0:60:: FFFF:FFFF:FFFF:: 0 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:
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 For example (ipv6): sip.route.dest.0=2620:0:60:: FFFF:FFFF:FFFF:: 0 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:
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 For example (ipv6): sip.route.dest.0=2620:0:60:: FFFF:FFFF:FFFF:: 0 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:
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 For example (ipv6): sip.route.dest.0=2620:0:60:: FFFF:FFFF:FFFF:: 0 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 SIP route set for outbound calls. If defined, this route set will be inserted as the ROUTE header for all outgoing calls. This will force the platform to send the SIP messages via this defined route set.

Each element in the routeset should be seperated 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>

In this example, the Genesys Voice platform 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.

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 SIPS route set for SIPS outbound calls. If defined, this route set will be inserted as the ROUTE header for all outgoing calls. This will force the platform to send the SIP messages via this defined route set.

Each element in the routeset should be seperated 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.securerouteset=<sips:p1.example.com;lr>,<sips:p2.domain.com;lr>

In this example, the Genesys Voice platform 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.

sessionexpires

Default Value: 1800
Valid Values: The parameter size must be between 90 and 3600
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.

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, CCP will let the OS choose the local port.

threadpoolsize

Default Value: 4
Valid Values: The size of the thread pool for handling DNS queries
Changes Take Effect: At start/restart

The size of the thread pool for handling DNS queries.

threads

Default Value: 0
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.

timer.ci_proceeding

Default Value: 120000
Valid Values: sip.timer.ci_proceeding must be greater than 0
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. This ensures that a CANCEL will be sent to terminate the SIP session properly when connect timeout occurs.

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, CCP will let the OS choose the local port.

transport.0

Default Value: transport0 udp:any:5068

Valid Values:
Changes Take Effect: At start/restart

defines transport layer for SIP stack and the network interfaces that are used to process SIP requests
Format: sip.transport.x = transport_name
type:ip:port [parameters]

where transport_name is any string; type is udp/tcp/tls; ip is the IP address of the network interface that accepts incoming SIP messages; 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. Note that this is for LMSIP2.

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, SSLv2, SSLv3, SSLv23. Default to SSLv23. password=[password] Applicable to SIPS only and is optional. The password associated with the certificate and key pair. Required only if key file is password protected. cafile=[CA cert path and filename] Mandatory for TLS mutual authentication. The path and the filename of the certificate to be used for verifying the peer. The same certificate specified in cert=[cert path and filename] parameter can be used as the value here if using only 1 certificate is preferred. verifypeer=true Mandatory for TLS mutual authentication. This parameter turns on the TLS mutual authentication. verifydepth=[max depth for the certificate chain verification] Applicable only to TLS mutual authentication. This parameter sets the maximum depth for the certificate chain verification. For the default Genesys certificate provided, the recommended value is 1.

transport.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 transport instance 0. Note that this configuration does not work for Windows 2008. For Windows 2008, 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:5068
Valid Values:
Changes Take Effect: At start/restart

defines transport layer for SIP stack and the network interfaces that are used to process SIP requests
Format: sip.transport.x = transport_name

type:ip:port [parameters]

where transport_name is any string; type is udp/tcp/tls; ip is the IP address of the network interface that accepts incoming SIP messages; 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. Note that this is for LMSIP2.

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, SSLv2, SSLv3, SSLv23. Default to SSLv23. password=[password] Applicable to SIPS only and is optional. The password associated with the certificate and key pair. Required only if key file is password protected. cafile=[CA cert path and filename] Mandatory for TLS mutual authentication. The path and the filename of the certificate to be used for verifying the peer. The same certificate specified in cert=[cert path and filename] parameter can be used as the value here if using only 1 certificate is preferred. verifypeer=true Mandatory for TLS mutual authentication. This parameter turns on the TLS mutual authentication. verifydepth=[max depth for the certificate chain verification] Applicable only to TLS mutual authentication. This parameter sets the maximum depth for the certificate chain verification. For the default Genesys certificate provided, the recommended value is 1.

transport.1.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 transport instance 1. Note that this configuration does not work for Windows 2008. For Windows 2008, 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:5069 cert=$InstallationRoot$/config/x509_certificate.pem key=$InstallationRoot$/config/x509_private_key.pem
Valid Values:
Changes Take Effect: At start/restart

defines transport layer for SIP stack and the network interfaces that are used to process SIP requests
Format: sip.transport.x = transport_name
type:ip:port [parameters]

where transport_name is any string; type is udp/tcp/tls; ip is the IP address of the network interface that accepts incoming SIP messages; 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. Note that this is for LMSIP2.

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, SSLv2, SSLv3, SSLv23. Default to SSLv23. password=[password] Applicable to SIPS only and is optional. The password associated with the certificate and key pair. Required only if key file is password protected. cafile=[CA cert path and filename] Mandatory for TLS mutual authentication. The path and the filename of the certificate to be used for verifying the peer. The same certificate specified in cert=[cert path and filename] parameter can be used as the value here if using only 1 certificate is preferred. verifypeer=true Mandatory for TLS mutual authentication. This parameter turns on the TLS mutual authentication. verifydepth=[max depth for the certificate chain verification] Applicable only to TLS mutual authentication. This parameter sets the maximum depth for the certificate chain verification. For the default Genesys certificate provided, the recommended value is 1.

transport.2.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 transport instance 2. Note that this configuration does not work for Windows 2008. For Windows 2008, 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:
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; 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. Note that this is for LMSIP2.

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, SSLv2, SSLv3, SSLv23. Default to SSLv23. password=[password] Applicable to SIPS only and is optional. The password associated with the certificate and key pair. Required only if key file is password protected. cafile=[CA cert path and filename] Mandatory for TLS mutual authentication. The path and the filename of the certificate to be used for verifying the peer. The same certificate specified in cert=[cert path and filename] parameter can be used as the value here if using only 1 certificate is preferred. verifypeer=true Mandatory for TLS mutual authentication. This parameter turns on the TLS mutual authentication. verifydepth=[max depth for the certificate chain verification] Applicable only to TLS mutual authentication. This parameter sets the maximum depth for the certificate chain verification. For the default Genesys certificate provided, the recommended value is 1.

transport.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 Differentiaed 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 2008. For Windows 2008, 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:
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; 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. Note that this is for LMSIP2.

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, SSLv2, SSLv3, SSLv23. Default to SSLv23. password=[password] Applicable to SIPS only and is optional. The password associated with the certificate and key pair. Required only if key file is password protected. cafile=[CA cert path and filename] Mandatory for TLS mutual authentication. The path and the filename of the certificate to be used for verifying the peer. The

same certificate specified in cert=[cert path and filename] parameter can be used as the value here if using only 1 certificate is preferred. verifypeer=true Mandatory for TLS mutual authentication. This parameter turns on the TLS mutual authentication. verifydepth=[max depth for the certificate chain verification] Applicable only to TLS mutual authentication. This parameter sets the maximum depth for the certificate chain verification. For the default Genesys certificate provided, the recommended value is 1.

transport.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 Differentiaed 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 2008. For Windows 2008, 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:
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; 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. Note that this is for LMSIP2.

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, SSLv2, SSLv3, SSLv23. Default to SSLv23. password=[password] Applicable to SIPS only and is optional. The password associated with the certificate and key pair. Required only if key file is password protected. cafile=[CA cert path and filename] Mandatory for TLS mutual authentication. The path and the filename of the certificate to be used for verifying the peer. The same certificate specified in cert=[cert path and filename] parameter can be used as the value here if using only 1 certificate is preferred. verifypeer=true Mandatory for TLS mutual authentication. This parameter turns on the TLS mutual authentication. verifydepth=[max depth for the certificate chain verification] Applicable only to TLS mutual authentication. This parameter sets the maximum depth for the certificate chain verification. For the default Genesys certificate provided, the recommended value is 1.

transport.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 Differentiaed 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 2008. For Windows 2008, 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:
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:
Changes Take Effect: At start/restart

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

transport.localaddress_ipv6

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

If specified, the sent-by field of the Via header and the hostport part of the Contact header in the outgoing SIP message will be set to this value if a IPv6 transport is used. The value must be a hostname or domain name. If left empty the outgoing transport's actual IP and port will be used for

the Via header and the Contact header. Note that if the domain name used in the SRV record query is specified, sip.transport.localaddress.srv must be set to true to prevent the port part being automatically generated by the SIP stack.

transport.localaddress.srv

Default Value: false
Valid Values:
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.staticroutelist

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

Specifies a list of static routes. Each route group is separated by