This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Genesys Voice Platform

Genesys Configuration Options Current

12/29/2021

Table of Contents

Genesys Voice Platform Options Reference

Welcome to the Options Reference for Genesys Voice Platform. This document describes the configuration options for the following components of Genesys Voice Platform:

Core GVP Components

- Resource Manager
- Media Control Platform
- Reporting Server

Speech-Related Components

- MRCP Proxy
- MRCPv1_ASR
- MRCPv1_TTS
- MRCPv2_ASR
- MRCPv2_TTS

Connectors

- CTI Connector
- UCM Connector
- PSTN Connector

Others

- Policy Server
- Reporting Plug-in for GAX
- Call Control Platform
- Supplementary Services Gateway

- Third Party Call Recorder

Descriptions of configuration options provided in this *Options Reference* are definitive. Refer to the GVP Supplemental Documentation for those GVP and Media Server components that are not yet covered in the *Options Reference.*

Core GVP Components

The following components are considered as the core components of Genesys Voice Platform since they play a vital role in servicing a call:

- Resource Manager

  The Resource Manager (RM) controls the access and routing to all resources in a GVP 8.5 deployment. The Resource Manager is the first element to process requests for services, and it interacts with the Configuration Server to determine the Interactive Voice Recognition (IVR) Profile to be associated with the session. The RM manages resources that can deliver services including Voice Extensible Markup Language (VoiceXML) or Call Control Extensible Markup Language (CCXML) execution, and provide media services including Announcements, Conferencing and Recording. The RM pushes the profile to a component that can deliver the service, such as the Media Control Platform or Call Control Platform, or CTI Connector.

  For more information about the Resource Manager application, see Resource Manager in the *GVP Deployment Guide*. For the Resource Manager configuration options, see Resource Manager Options in this document.

- Media Control Platform

  The Media Control Platform (MCP) is the core component of GVP, and it executes the actual voice applications in the solution. In addition, it is used by other communication layer components, such as SIP Server, to provide media services in support of broader customer service scenarios, such as agent interactions, queuing and many other functions.

  For more information about the MCP, see Media Control Platform in the *GVP Deployment Guide*. For the MCP configuration options, see Media Control Platform Options in this document.

- Reporting Server

  The Reporting Server (RS) component of GVP provides a comprehensive view of the calls serviced by a GVP deployment. The Reporting Server receives data from the Media Control Platform for VoiceXML applications, from the Call Control Platform for CCXML applications, and from other components involved in servicing a call, such as the Resource Manager.

  For more information about the RS, see Reporting Server in the *GVP*

Deployment Guide. For the RS configuration options, see Reporting Server Options in this document.

Resource Manager

Options for this component are contained in the following configuration sections:

- cluster
- ems
- gvp
- gvp.context-services-authentication
- gvp.general
- gvp.log
- gvp.policy
- gvp.policy.call-info
- gvp.policy.dbmp
- gvp.policy.dialing-rules
- gvp.policy.speech-resources
- gvp.policy.sqa
- gvp.service-parameters
- gvp.service-prerequisite
- log
- monitor
- mrcpv2pxy
- OPM
- proxy
- registrar
- rm
- snmp
- subscription

> ## Tip
>
> In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.
>
> **Power users: Download a CSV file** containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
cluster	cafile	$InstallationRoot$/config/x509_certificate.pem	After restart
cluster	certfile	$InstallationRoot$/config/x509_certificate.pem	After restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
cluster	certkeyfile	$InstallationRoot$/config/x509_private_key.pem	After restart
cluster	electiontimer	3000	After restart
cluster	failoverscript	$InstallationRoot$/bin/NLB.bat	After restart
cluster	ha-mode	none	After restart
cluster	heartbeattimer	2000	After restart
cluster	hotstandby	false	After restart
cluster	initial-electiontimer	10000	After restart
cluster	member.1		After restart
cluster	member.2		After restart
cluster	members	1 2	After restart
cluster	mymemberid		After restart
cluster	other-active-rmnode-ip		After restart
cluster	tlstype	TLSv1_2	After restart
cluster	usetls	0	After restart
cluster	verifydepth		After restart
cluster	verifypeer	false	After restart
cluster	virtual-ip		After restart
cluster	virtual-ip-in-via	true	After restart
ems	logconfig.MFSINK	*|*|*	immediately
ems	metricsconfig.MFSINK	*	immediately
ems	ors.reportinginterval	60	At start/restart
ems	rc.amq_connection_send_timeout	60	At start/restart
ems	rc.cdr.batch_size	500	At start/restart
ems	rc.cdr.local_queue_max	1000000	At start/restart
ems	rc.cdr.local_queue_path	cdrQueue_rm.db	At start/restart
ems	rc.cdr.max_throughput	0	At start/restart
ems	rc.certificate		at start/restart
ems	rc.keystore_certificate		at start/restart
ems	rc.keystore_password		at start/restart
ems	rc.ors.batch_size	500	At start/restart
ems	rc.ors.local_queue_max	1000000	At start/restart
ems	rc.ors.local_queue_path	orsQueue_rm.db	At start/restart
ems	rc.truststore_certificate		at start/restart
gvp	nic.eth0		After restart
gvp	nic.eth1		After restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
gvp	nic.linkattribute	MII Status:	After restart
gvp	nic.upvalue	up	After restart
gvp	nics		After restart
gvp.context-services-authentication	password		immediately
gvp.context-services-authentication	username		immediately
gvp.general	application-confmaxsize		immediately
gvp.general	cisco-record-file	CUCM/call-$REFCI$-at-$AGENTDN$-on-$DATE$	immediately
gvp.general	service-type		immediately
gvp.general	sip.sessiontimer		immediately
gvp.general	toll-free-number		immediately
gvp.general	VirtualReportingTag1		immediately
gvp.general	VirtualReportingTag2		immediately
gvp.log	metricsfilter		immediately
gvp.policy			immediately
gvp.policy	announcement-allowed	true	immediately
gvp.policy	announcement-capability-requirement		immediately
gvp.policy	announcement-forbidden-respcode	403	immediately
gvp.policy	announcement-forbidden-set-alarm	false	immediately
gvp.policy	announcement-level2-burst-limit		immediately
gvp.policy	announcement-level3-burst-limit		immediately
gvp.policy	announcement-usage-limit		immediately
gvp.policy	announcement-usage-limit-exceeded-respcode	480	immediately
gvp.policy	announcement-usage-limit-exceeded-set-alarm	false	immediately
gvp.policy	announcement-usage-limit-per-session		immediately
gvp.policy	asr-reserve	false	immediately
gvp.policy	burst-allowed	false	immediately
gvp.policy	burst-set-alarm	false	immediately
gvp.policy	ccxml-capability-		immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
	requirement		
gvp.policy	ccxml-level2-burst-limit		immediately
gvp.policy	ccxml-level3-burst-limit		immediately
gvp.policy	ccxml-usage-limit		immediately
gvp.policy	ccxml-usage-limit-exceeded-alarm	false	immediately
gvp.policy	ccxml-usage-limit-exceeded-respcode	480	immediately
gvp.policy	ccxml-usage-limit-per-session		immediately
gvp.policy	conference-allowed	true	immediately
gvp.policy	conference-capability-requirement		immediately
gvp.policy	conference-forbidden-respcode	403	immediately
gvp.policy	conference-forbidden-set-alarm	false	immediately
gvp.policy	conference-level2-burst-limit		immediately
gvp.policy	conference-level3-burst-limit		immediately
gvp.policy	conference-usage-limit		immediately
gvp.policy	conference-usage-limit-exceeded-respcode	480	immediately
gvp.policy	conference-usage-limit-exceeded-set-alarm	false	immediately
gvp.policy	conference-usage-limit-per-session		immediately
gvp.policy	cpd-allowed	true	immediately
gvp.policy	cpd-capability-requirement		immediately
gvp.policy	cpd-forbidden-respcode	403	immediately
gvp.policy	cpd-forbidden-set-alarm	false	immediately
gvp.policy	cpd-level2-burst-limit		immediately
gvp.policy	cpd-level3-burst-limit		immediately
gvp.policy	cpd-usage-limit		immediately
gvp.policy	cpd-usage-limit-exceeded-respcode	480	immediately
gvp.policy	cpd-usage-limit-exceeded-set-alarm	false	immediately
gvp.policy	cpd-usage-limit-per-		immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
	session		
gvp.policy	cti-allowed	true	immediately
gvp.policy	dialing-rule-forbidden-respcode	403	immediately
gvp.policy	dialing-rule-forbidden-set-alarm	false	immediately
gvp.policy	disable-amr	false	immediately
gvp.policy	disable-amrwb	false	immediately
gvp.policy	disable-g729	false	immediately
gvp.policy	disable-video	false	immediately
gvp.policy	inbound-level2-burst-limit		immediately
gvp.policy	inbound-level3-burst-limit		immediately
gvp.policy	inbound-usage-limit		immediately
gvp.policy	inbound-usage-limit-exceeded-respcode	480	immediately
gvp.policy	inbound-usage-limit-exceeded-set-alarm	false	immediately
gvp.policy	level2-burst-limit		immediately
gvp.policy	level3-burst-limit		immediately
gvp.policy	max-subdialog-depth		immediately
gvp.policy	mcp-asr-usage-mode	per-call	immediately
gvp.policy	mcp-sendrecv-enabled	true	immediately
gvp.policy	msml-allowed	true	immediately
gvp.policy	msml-capability-requirement		immediately
gvp.policy	msml-forbidden-respcode	403	immediately
gvp.policy	msml-forbidden-set-alarm	false	immediately
gvp.policy	msml-level2-burst-limit		immediately
gvp.policy	msml-level3-burst-limit		immediately
gvp.policy	msml-usage-limit		immediately
gvp.policy	msml-usage-limit-exceeded-respcode	480	immediately
gvp.policy	msml-usage-limit-exceeded-set-alarm	false	immediately
gvp.policy	msml-usage-limit-per-session		immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
gvp.policy	outbound-call-allowed	true	immediately
gvp.policy	outbound-call-forbidden-respcode	403	immediately
gvp.policy	outbound-call-forbidden-set-alarm	false	immediately
gvp.policy	outbound-level2-burst-limit		immediately
gvp.policy	outbound-level3-burst-limit		immediately
gvp.policy	outbound-usage-limit		immediately
gvp.policy	outbound-usage-limit-exceeded-respcode	480	immediately
gvp.policy	outbound-usage-limit-exceeded-set-alarm	false	immediately
gvp.policy	prediction-factor	1.0	immediately
gvp.policy	recordingclient-allowed	true	immediately
gvp.policy	recordingclient-capability-requirement		immediately
gvp.policy	recordingclient-forbidden-respcode	403	immediately
gvp.policy	recordingclient-forbidden-set-alarm	false	immediately
gvp.policy	recordingclient-level2-burst-limit		immediately
gvp.policy	recordingclient-level3-burst-limit		immediately
gvp.policy	recordingclient-usage-limit		immediately
gvp.policy	recordingclient-usage-limit-exceeded-respcode	480	immediately
gvp.policy	recordingclient-usage-limit-exceeded-set-alarm	false	immediately
gvp.policy	recordingclient-usage-limit-per-session		immediately
gvp.policy	recordingserver-allowed	true	immediately
gvp.policy	recordingserver-capability-requirement		immediately
gvp.policy	recordingserver-forbidden-respcode	403	immediately
gvp.policy	recordingserver-forbidden-set-alarm	false	immediately
gvp.policy	recordingserver-		immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
	level2-burst-limit		
gvp.policy	recordingserver-level3-burst-limit		immediately
gvp.policy	recordingserver-usage-limit		immediately
gvp.policy	recordingserver-usage-limit-exceeded-respcode	480	immediately
gvp.policy	recordingserver-usage-limit-exceeded-set-alarm	false	immediately
gvp.policy	recordingserver-usage-limit-per-session		immediately
gvp.policy	retry-on-speech-reserve-failure	true	immediately
gvp.policy	speech-reserve-failure-response	0	immediately
gvp.policy	transfer-allowed	true	immediately
gvp.policy	transfer-forbidden-respcode	403	immediately
gvp.policy	transfer-forbidden-set-alarm	false	immediately
gvp.policy	treatment-allowed	true	immediately
gvp.policy	treatment-capability-requirement		immediately
gvp.policy	treatment-forbidden-respcode	403	immediately
gvp.policy	treatment-forbidden-set-alarm	false	immediately
gvp.policy	treatment-level2-burst-limit		immediately
gvp.policy	treatment-level3-burst-limit		immediately
gvp.policy	treatment-usage-limit		immediately
gvp.policy	treatment-usage-limit-exceeded-respcode	480	immediately
gvp.policy	treatment-usage-limit-exceeded-set-alarm	false	immediately
gvp.policy	treatment-usage-limit-per-session		immediately
gvp.policy	tts-reserve	false	immediately
gvp.policy	usage-limit-exceeded-respcode	480	immediately
gvp.policy	usage-limit-exceeded-	false	immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
	set-alarm		
gvp.policy	usage-limits		immediately
gvp.policy	use-same-gateway	always	immediately
gvp.policy	voicexml-capability-requirement		immediately
gvp.policy	voicexml-dialog-allowed	true	immediately
gvp.policy	voicexml-dialog-forbidden-respcode	403	immediately
gvp.policy	voicexml-dialog-forbidden-set-alarm	false	immediately
gvp.policy	voicexml-level2-burst-limit		immediately
gvp.policy	voicexml-level3-burst-limit		immediately
gvp.policy	voicexml-usage-limit		immediately
gvp.policy	voicexml-usage-limit-exceeded-respcode	480	immediately
gvp.policy	voicexml-usage-limit-exceeded-set-alarm	false	immediately
gvp.policy	voicexml-usage-limit-per-session		immediately
gvp.policy.call-info	rule-1		immediately
gvp.policy.call-info	rule-2		immediately
gvp.policy.dbmp	rs.db.retention.cdr.default	30	immediately
gvp.policy.dbmp	rs.db.retention.events.default	7	immediately
gvp.policy.dbmp	rs.db.retention.latencies.daily.default	90	immediately
gvp.policy.dbmp	rs.db.retention.latencies.hourly.default	7	immediately
gvp.policy.dbmp	rs.db.retention.latencies.monthly.default	1095	immediately
gvp.policy.dbmp	rs.db.retention.latencies.weekly.default	364	immediately
gvp.policy.dbmp	rs.db.retention.operations.30min.default	7	immediately
gvp.policy.dbmp	rs.db.retention.operations.5min.default	0	immediately
gvp.policy.dbmp	rs.db.retention.operations.daily.default	90	immediately
gvp.policy.dbmp	rs.db.retention.operations.hourly.default	7	immediately
gvp.policy.dbmp	rs.db.retention.operations.monthly.default	1095	immediately
gvp.policy.dbmp	rs.db.retention.operations.weekly.default	364	immediately
gvp.policy.dbmp	rs.db.retention.sq.daily.default	90	immediately
gvp.policy.dbmp	rs.db.retention.sq.failures.default	365	immediately
gvp.policy.dbmp	rs.db.retention.sq.hourly.default	7	immediately
gvp.policy.dbmp	rs.db.retention.sq.monthly.default	365	immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
gvp.policy.dbmp	rs.db.retention.sq.weekly.default	180	immediately
gvp.policy.dbmp	rs.db.retention.var.30min.default	7	immediately
gvp.policy.dbmp	rs.db.retention.var.5min.default	0	immediately
gvp.policy.dbmp	rs.db.retention.var.daily.default	90	immediately
gvp.policy.dbmp	rs.db.retention.var.hourly.default	7	immediately
gvp.policy.dbmp	rs.db.retention.var.monthly.default	1095	immediately
gvp.policy.dbmp	rs.db.retention.var.weekly.default	364	immediately
gvp.policy.dialing-rules	rule-1		immediately
gvp.policy.dialing-rules	rule-2		immediately
gvp.policy.speech-resources	asr.defaultengine		immediately
gvp.policy.speech-resources	authorizedasrengines		immediately
gvp.policy.speech-resources	authorizedttsengines		immediately
gvp.policy.speech-resources	defaultlanguage		immediately
gvp.policy.speech-resources	nsssessionxml		immediately
gvp.policy.speech-resources	tts.defaultengine		immediately
gvp.policy.sqa	error.notification.threshold	-1	immediately
gvp.service-parameters		fixed,2	immediately
gvp.service-parameters	cti.DefaultAgent	fixed	immediately
gvp.service-parameters	cti.icm.enableBridgeXfer	fixed,0	immediately
gvp.service-parameters	cti.icm.ScriptMapping	fixed,TFN	immediately
gvp.service-parameters	cti.icm.ServiceID	fixed,	immediately
gvp.service-parameters	cti.TransferOnCTI	fixed,no	immediately
gvp.service-parameters	recordingclient.audiosrc		immediately
gvp.service-parameters	recordingclient.AWSAccessKeyId		immediately
gvp.service-parameters	recordingclient.AWSAccessKeyId2		immediately
gvp.service-parameters	recordingclient.AWSSecretAccessKey		immediately
gvp.service-parameters	recordingclient.AWSSecretAccessKey2		immediately
gvp.service-parameters	recordingclient.callrec_authorization		immediately
gvp.service-parameters	recordingclient.callrec_dest		immediately
gvp.service-parameters	recordingclient.httpauthorization		immediately
gvp.service-parameters	recordingclient.httpauthorization2		immediately
gvp.service-parameters	recordingclient.recdest	fixed,sip:$LocalIP$:5060	immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
gvp.service-parameters	recordingclient.recdest2	fixed,sip:$LocalIP$:5060	immediately
gvp.service-parameters	recordingclient.recmediactl	fixed,2	immediately
gvp.service-parameters	recordingclient.tonesilenceduration		immediately
gvp.service-parameters	recordingclient.type		immediately
gvp.service-parameters	recordingclient.type2		immediately
gvp.service-parameters	voicexml.gvp.appmodule	fixed,VXML-NG	immediately
gvp.service-parameters	voicexml.gvpi.$adn-flag$	fixed,0	immediately
gvp.service-parameters	voicexml.gvpi.$asrplatform$	fixed,	immediately
gvp.service-parameters	voicexml.gvpi.$asrwavfilelog$	fixed,FALSE	immediately
gvp.service-parameters	voicexml.gvpi.$badxmlpageposturl$	fixed,	immediately
gvp.service-parameters	voicexml.gvpi.$call-trace-url$	fixed,	immediately
gvp.service-parameters	voicexml.gvpi.$ccerror-telnum$	fixed,	immediately
gvp.service-parameters	voicexml.gvpi.$cpatimeout$	fixed,0	immediately
gvp.service-parameters	voicexml.gvpi.$cti_endcall_on_agentleg_hup$	fixed,1	immediately
gvp.service-parameters	voicexml.gvpi.$debug-url$	fixed,	immediately
gvp.service-parameters	voicexml.gvpi.$default-language$	fixed,en-US	immediately
gvp.service-parameters	voicexml.gvpi.$dtmf_nomatch_utterance_enabled$	fixed,TRUE	immediately
gvp.service-parameters	voicexml.gvpi.$ivr-tmo$	fixed,6	immediately
gvp.service-parameters	voicexml.gvpi.$outbound-call-limit$	fixed,21600	immediately
gvp.service-parameters	voicexml.gvpi.$record-pages$	fixed,0	immediately
gvp.service-parameters	voicexml.gvpi.$rexfertimeout$	fixed,60	immediately
gvp.service-parameters	voicexml.gvpi.$tntenable$	fixed,0	immediately
gvp.service-parameters	voicexml.gvpi.$tntreclaimcode$	fixed,*7	immediately
gvp.service-parameters	voicexml.gvpi.$tntscript$	fixed,	immediately
gvp.service-parameters	voicexml.gvpi.$transactional-record$	fixed,0	immediately
gvp.service-parameters	voicexml.gvpi.$transactional-record-posturl$		immediately
gvp.service-parameters	voicexml.gvpi.$transfer-option$	fixed,	immediately
gvp.service-parameters	voicexml.gvpi.$transfer-type$	fixed,	immediately
gvp.service-parameters	voicexml.gvpi.$transferscript-	fixed,	immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
	url$		
gvp.service-parameters	voicexml.gvpi.$trap-url$	fixed,	immediately
gvp.service-parameters	voicexml.gvpi.$tts-gender$	fixed,MALE	immediately
gvp.service-parameters	voicexml.gvpi.$tts-vendor$	fixed,	immediately
gvp.service-prerequisite	alternatevoicexml		immediately
gvp.service-prerequisite	announcement-url		immediately
gvp.service-prerequisite	conference-id		immediately
gvp.service-prerequisite	default-properties-page		immediately
gvp.service-prerequisite	initial-page-url		immediately
log	all	../logs/ResourceMgr	immediately
log	check-point	1	immediately
log	compatible-output-priority	false	immediately
log	debug	../logs/ResourceMgr	immediately
log	expire	20	immediately
log	interaction	../logs/ResourceMgr	immediately
log	keep-startup-file	false	After restart
log	memory		immediately
log	memory-storage-size		When memory output is created
log	messagefile		Immediately, if an application cannot find its *.lms file at startup
log	message_format	short	immediately
log	print-attributes	false	immediately
log	segment	10000	immediately
log	spool		immediately
log	standard	../logs/ResourceMgr	immediately
log	time_convert	local	immediately
log	time_format	ISO8601	immediately
log	trace	../logs/ResourceMgr	immediately
log	verbose	standard	immediately
monitor	optionsofflineresp	503	At start/restart
monitor	sip.enable_dns_cache	true	At start/restart
monitor	sip.localuser	GVP	After restart
monitor	sip.logmsg.allowed	true	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
monitor	sip.logmsg.maskoption	0	At start/restart
monitor	sip.mtusize	1500	After restart
monitor	sip.preferred_ipversion	ipv4	At start/restart
monitor	sip.proxy.optionsinterval	2000	After restart
monitor	sip.proxy.release-recordingclient-session-on-fail	true	After restart
monitor	sip.proxy.release-recordingserver-session-on-fail	true	After restart
monitor	sip.proxy.releaseconfonfailure	true	After restart
monitor	sip.proxy.unavailoptionsinterval	5000	After restart
monitor	sip.route.default.tcp		At start/restart
monitor	sip.route.default.tcp.ipv6		At start/restart
monitor	sip.route.default.tls		At start/restart
monitor	sip.route.default.tls.ipv6		At start/restart
monitor	sip.route.default.udp		At start/restart
monitor	sip.route.default.udp.ipv6		At start/restart
monitor	sip.tcp.portrange		At start/restart
monitor	sip.tls.portrange		At start/restart
monitor	sip.transport.0	transport0 udp:any:5064	After restart
monitor	sip.transport.0.tos	0	At start/restart
monitor	sip.transport.1	transport1 tcp:any:5064	After restart
monitor	sip.transport.1.tos	0	At start/restart
monitor	sip.transport.2	transport2 tls:any:5065 cert=$InstallationRoot$/config/x509_certificate.pem key=$InstallationRoot$/config/x509_private_key.pem	After restart
monitor	sip.transport.2.tos	0	At start/restart
monitor	sip.transport.dnsharouting	false	At start/restart
monitor	sip.transport.localaddress		At start/restart
monitor	sip.transport.localaddress.srv	false	At start/restart
monitor	sip.transport.localaddress_ipv6		At start/restart
monitor	sip.transport.routefailovertime	5	At start/restart
monitor	sip.transport.routerecoverytime	30	At start/restart
monitor	sip.transport.setuptimer.tcp	30000	At start/restart
monitor	sip.transport.unavailablewarmup	true	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
mrcpv2pxy	default-resource-port-capacity	500	After restart
mrcpv2pxy	enable_dns_cache	true	At start/restart
mrcpv2pxy	enable_mrcpv2_proxy	0	After restart
mrcpv2pxy	fips_enabled	false	After restart
mrcpv2pxy	options-errresp-on-noresources	true	After restart
mrcpv2pxy	options_response_contenttype	application/text	After restart
mrcpv2pxy	options_response_msg_body	v=0%0D%0Am=application 9 TCP/MRCPv2 1%0D%0Aa=resource:mrcpv2proxy%0D%0A	After restart
mrcpv2pxy	resolve-addr-for-aor-match	false	After restart
mrcpv2pxy	resource-no-match-respcode	480	After restart
mrcpv2pxy	resource-unavailable-respcode	480	After restart
mrcpv2pxy	suspend-mode-respcode	503	After restart
OPM	Transaction_dbid		immediately
proxy	sip.enable_dns_cache	true	At start/restart
proxy	sip.localuser	GVP	After restart
proxy	sip.logmsg.allowed	true	At start/restart
proxy	sip.logmsg.maskoption	0	At start/restart
proxy	sip.maxtcpconnections	100	After restart
proxy	sip.maxtlsconnections	100	After restart
proxy	sip.min_se	90	After restart
proxy	sip.mtusize	1500	After restart
proxy	sip.preferred_ipversion	ipv4	At start/restart
proxy	sip.proxy.respaddr		After restart
proxy	sip.route.default.tcp		At start/restart
proxy	sip.route.default.tcp.ipv6		At start/restart
proxy	sip.route.default.tls		At start/restart
proxy	sip.route.default.tls.ipv6		At start/restart
proxy	sip.route.default.udp		At start/restart
proxy	sip.route.default.udp.ipv6		At start/restart
proxy	sip.route.dest.0		After restart
proxy	sip.route.dests		After restart
proxy	sip.sessionexpires	1800	After restart
proxy	sip.tcp.portrange		At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
proxy	sip.threadpoolsize	4	After restart
proxy	sip.threads	5	After restart
proxy	sip.timer_C	175000	After restart
proxy	sip.timer_C1	6000	After restart
proxy	sip.tls.portrange		At start/restart
proxy	sip.transport.0	transport0 udp:any:5060	After restart
proxy	sip.transport.0.tos	0	At start/restart
proxy	sip.transport.1	transport1 tcp:any:5060	After restart
proxy	sip.transport.1.tos	0	At start/restart
proxy	sip.transport.2	transport2 tls:any:5061 cert=$InstallationRoot$/config/x509_certificate.pem key=$InstallationRoot$/config/x509_private_key.pem	After restart
proxy	sip.transport.2.tos	0	At start/restart
proxy	sip.transport.alarmtimer	60000	At start/restart
proxy	sip.transport.dnsharouting	false	At start/restart
proxy	sip.transport.localaddress		At start/restart
proxy	sip.transport.localaddress.srv	false	At start/restart
proxy	sip.transport.localaddress_ipv6		At start/restart
proxy	sip.transport.routefailovertime	5	At start/restart
proxy	sip.transport.routerecoverytime	30	At start/restart
proxy	sip.transport.setuptimer.tcp	30000	At start/restart
proxy	sip.transport.unavailablewakeup	true	At start/restart
proxy	sip.udprecvbuffersize	262144	After restart
proxy	sip.udpsendbuffersize	135168	After restart
registrar	sip.enable_dns_cache	true	At start/restart
registrar	sip.localuser	GVP	After restart
registrar	sip.logmsg.allowed	true	At start/restart
registrar	sip.logmsg.maskoption	0	At start/restart
registrar	sip.preferred_ipversion	ipv4	At start/restart
registrar	sip.registrar.domain		After restart
registrar	sip.registrar.maxexpirytime	60	After restart
registrar	sip.registrar.minexpirytime	60	After restart
registrar	sip.route.default.tcp		At start/restart
registrar	sip.route.default.tcp.ipv6		At start/restart
registrar	sip.route.default.tls		At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
registrar	sip.route.default.tls.ipv6		At start/restart
registrar	sip.route.default.udp		At start/restart
registrar	sip.route.default.udp.ipv6		At start/restart
registrar	sip.tcp.portrange		At start/restart
registrar	sip.tls.portrange		At start/restart
registrar	sip.transport.0	transport0 udp:any:5062	After restart
registrar	sip.transport.0.tos	0	At start/restart
registrar	sip.transport.1	transport1 tcp:any:5062	After restart
registrar	sip.transport.1.tos	0	At start/restart
registrar	sip.transport.2	transport2 tls:any:5063 cert=$InstallationRoot$/config/x509_certificate.pem key=$InstallationRoot$/config/x509_private_key.pem	After restart
registrar	sip.transport.2.tos	0	At start/restart
registrar	sip.transport.dnsharouting	false	At start/restart
registrar	sip.transport.localaddress		At start/restart
registrar	sip.transport.localaddress.srv	false	At start/restart
registrar	sip.transport.localaddress_ipv6		At start/restart
registrar	sip.transport.routefailovertime	5	At start/restart
registrar	sip.transport.routerecoverytime	30	At start/restart
registrar	sip.transport.setuptimer.tcp	30000	At start/restart
registrar	sip.transport.unavailablewakeup	true	At start/restart
rm	conference-cleanup-timer		After restart
rm	conference-sip-error-respcode	480	After restart
rm	cti-unavailable-action	answer	After restart
rm	cti-unavailable-respcode	404	After restart
rm	default-resource-port-capacity	500	After restart
rm	enable_dns_cache	true	At start/restart
rm	fips_enabled	false	After restart
rm	ignore-ruri-tenant-dbid	false	After restart
rm	options-errresp-on-noresources	true	After restart
rm	options_response_contenttype	application/text	After restart
rm	options_response_msg_body		After restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
rm	pass-capability-params-to-ctic	true	After restart
rm	pass-tenantid-parameter-to-gateway	true	After restart
rm	reject-on-geo-location-nomatch	recordingclient,recordingserver	immediately
rm	resolve-addr-for-aor-match	false	After restart
rm	resource-no-match-respcode	480	After restart
rm	resource-unavailable-respcode	480	After restart
rm	rewrite-referto-header	true	After restart
rm	sip-header-for-cti-dnis	request-uri	immediately
rm	sip-header-for-dnis	history-info	immediately
rm	suspend-mode-respcode	503	After restart
rm	treat-campaign-as-conference	true	After restart
rm	voicexml-recording-allowed	true	After restart
snmp	timeout	100	At start/restart
subscription	notify-all-mcp-status	true	After restart
subscription	notify-interval	5000	After restart
subscription	sip.enable_dns_cache	true	At start/restart
subscription	sip.localuser	GVP	After restart
subscription	sip.logmsg.allowed	true	At start/restart
subscription	sip.logmsg.maskoption	0	At start/restart
subscription	sip.mtusize	1500	After restart
subscription	sip.preferred_ipversion	ipv4	At start/restart
subscription	sip.route.default.tcp		At start/restart
subscription	sip.route.default.tcp.ipv6		At start/restart
subscription	sip.route.default.tls		At start/restart
subscription	sip.route.default.tls.ipv6		At start/restart
subscription	sip.route.default.udp		At start/restart
subscription	sip.route.default.udp.ipv6		At start/restart
subscription	sip.tcp.portrange		At start/restart
subscription	sip.tls.portrange		At start/restart
subscription	sip.transport.0	transport0 udp:any:5066	After restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
subscription	sip.transport.0.tos	0	At start/restart
subscription	sip.transport.1	transport1 tcp:any:5066	After restart
subscription	sip.transport.1.tos	0	At start/restart
subscription	sip.transport.2	transport2 tls:any:5067 cert=$InstallationRoot$/config/ x509_certificate.pem key=$InstallationRoot$/config/ x509_private_key.pem	After restart
subscription	sip.transport.2.tos	0	At start/restart
subscription	sip.transport.dnsharouting	false	At start/restart
subscription	sip.transport.localaddress		At start/restart
subscription	sip.transport.localaddress.srv	false	At start/restart
subscription	sip.transport.localaddress_ipv6		At start/restart
subscription	sip.transport.routefailovertime	5	At start/restart
subscription	sip.transport.routerecoverytime	30	At start/restart
subscription	sip.transport.setuptimer.tcp	30000	At start/restart
subscription	sip.transport.unavailablewakeup	true	At start/restart
subscription	subscription-duration	600	After restart
Section	**Option**	**Default**	**Changes Take Effect**

cluster Section

- cafile
- certfile
- certkeyfile
- electiontimer
- failoverscript
- ha-mode
- heartbeattimer
- hotstandby
- initial-electiontimer
- member.1
- member.2
- members
- mymemberid
- other-active-rmnode-ip
- tlstype
- usetls
- verifydepth
- verifypeer
- virtual-ip
- virtual-ip-in-via

cafile

Default Value: $InstallationRoot$/config/x509_certificate.pem
Valid Values:
Changes Take Effect: After restart

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 certfile parameter can be used as the value here if using only 1 certificate is preferred

certfile

Default Value: $InstallationRoot$/config/x509_certificate.pem
Valid Values:
Changes Take Effect: After restart

The path and the filename of the TLS server certificate to be used. The certificate should be in x509 format

certkeyfile

Default Value: $InstallationRoot$/config/x509_private_key.pem
Valid Values:
Changes Take Effect: After restart

The path and the filename of the TLS key to be used for TLS server certificate.

electiontimer

Default Value: 3000
Valid Values: Number must be from 1000 to 10000 inclusive
Changes Take Effect: After restart

Election timer in milli-seconds. If there is no response from remote member(s) for the election process after the specified milli-seconds, this node will become the master. Local resource manager will become the active node.

failoverscript

Default Value: $InstallationRoot$/bin/NLB.bat
Valid Values:
Changes Take Effect: After restart

Absolute path to the executable fail over script. For NLB: NLB.bat

ha-mode

Default Value: none
Valid Values: none, active-standby, active-active
Changes Take Effect: After restart

By default, this will be set to none (stand-alone mode). For active-standby HA configuration this parameter should be set to active-standby, where only one RM is capable of taking calls at a time. For active-active configuration this parameter should be set to active-active, where both RM instances are capable of handling requests. The configuration cluster.virtual-ip is also mandatory if running in active-standby or active-active mode.

heartbeattimer

Default Value: 2000
Valid Values:
Changes Take Effect: After restart

Heart beat interval between cluster members for determining health of each other.

hotstandby

Default Value: false
Valid Values: true, false
Changes Take Effect: After restart

This parameter has effect only if cluster.virtual-ip parameter is non-empty. If "true", this parameter mandates that the RM cluster run in hot-standby redundancy mode where call data is replicated to other RM node for SIP dialog redundancy. Otherwise, this parameter mandates that the RM cluster be run in warm-standby redundancy mode where SIP dialog redundancy is not supported, but the new requests will be handled by the other healthy RM node.

initial-electiontimer

Default Value: 10000
Valid Values: Number must be from 1000 to 60000 inclusive
Changes Take Effect: After restart

Election timer in milli-seconds for initial election during RM startup. If there is no response from remote member(s) for the election process after the specified milli-seconds, this node will become the master. Local resource manager will become the active node.

member.1

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

Describes the IP and TCP port on which the member ID 1 can be reached. The format is IP:Port where IP and Port specifies where this RM node can be reached for cluster communication.

member.2

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

Describes the IP and TCP port on which the member ID 2 can be reached. The format is IP:Port where IP and Port specifies where this RM node can be reached for cluster communication.

members

Default Value: 1 2

Valid Values:
Changes Take Effect: After restart

List of ID's of the members in the cluster (unsigned integers 1 to 32 delimited by space). For NLB, the ID's correspond to the unique host identifier (priority) number specified for each of the NLB cluster machines.

mymemberid

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

Indicates this cluster manager instance's member ID (select one among the ID's listed in cluster.members).

other-active-rmnode-ip

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

If non-empty, this parameter indicates that this RM node is part of a RM active-active cluster and the value specifies the IP address of other active RM in the same cluster. In active-active HA mode using SIP Server, this value should be configured with IP address which takes SIP traffic in other active RM node. In stand-alone, active-standby and active-active (Using load balancer like F5) HA modes, this parameter must be left empty.

tlstype

Default Value: TLSv1_2
Valid Values:
Changes Take Effect: After restart

The type of secure transport to be used and value can be TLSv1, SSLv3, SSLv23, TLSv1_1, TLSv1_2. Defaults to TLSv1_2. Note that SSLv2 is no longer supported. Note that this needs to be set to the same value on both RM nodes.

usetls

Default Value: 0
Valid Values:
Changes Take Effect: After restart

This parameter sets whether to use TCP or TLS for inter-node communication. Setting this paramter value to 0 makes RM use TCP as the transport, and TLS otherwise. Default value is '0'

verifydepth

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

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. This could be an integer. The default OpenSSL supported value is 100.

verifypeer

Default Value: false
Valid Values: true, false
Changes Take Effect: After restart

Mandatory for TLS mutual authentication. This parameter turns on the TLS mutual authentication. Defaults to false

virtual-ip

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

If non-empty, this parameter indicates that this RM node is part of a RM cluster and the value specifies the virtual IP address of the RM cluster this RM node is part of. In HA mode, this value gets written into the Record-Route and Via header (if cluster.virtual-ip-in-via is true). This parameter takes precedence over proxy.sip.transport.localaddress if both are specified. In stand-alone mode, this parameter must be left empty.

virtual-ip-in-via

Default Value: true
Valid Values: true, false
Changes Take Effect: After restart

This parameter takes effect only in HA mode. If set to true, virtual-ip will be written into the Via header when the SIP requests are forwarded. Otherwise, address specified by the proxy.sip.transport.localaddress parameter or the private IP address associated with the transport will be written into the Via header.

ems Section

- logconfig.MFSINK
- metricsconfig.MFSINK
- ors.reportinginterval
- rc.amq_connection_send_timeout
- rc.cdr.batch_size
- rc.cdr.local_queue_max
- rc.cdr.local_queue_path
- rc.cdr.max_throughput
- rc.certificate
- rc.keystore_certificate
- rc.keystore_password
- rc.ors.batch_size
- rc.ors.local_queue_max
- rc.ors.local_queue_path
- rc.truststore_certificate

logconfig.MFSINK

Default Value: *|*|*
Valid Values: Pipe delimited ranges for log levels, module IDs and specifier IDs. Ranges can be comma separated integers or range of integers or '*'.
Changes Take Effect: immediately

Controls the log messages that are sent to the MF sink. The format is 'levels|moduleIDs|specifierIDs' (repeated if necessary). The values between the pipes can be in the format: 'm-n,o,p' (ie "0-4, 5,6"). The wildcard character '*' can also be used to indicate all valid numbers. Example: '*|*|*' indicates that all log messages should be sent to the sink. Alternatively, '0,1|0-10|*|4|*|*' indicates that CRITICAL(0) and ERROR(1) level messages with module IDs in the range 0-10 will be sent to the sink; and all INFO(4) level messages will be sent as well.

metricsconfig.MFSINK

Default Value: *
Valid Values: Comma separated list of metric values or ranges. A metric value must be between 0 and 141 inclusive. The values '*' and blank are also allowed.
Changes Take Effect: immediately

Specifies the metrics that are delivered to the MF Sink. '*' indicates that all metrics will be sent to the sink. Alternatively, '5-10,50-55,70,71' indicates that metrics with IDs 5,6,7,8,9,10,50,51,52,53,54,55,70 and 71 will be sent to the MF sink.

ors.reportinginterval

Default Value: 60
Valid Values: An integer between 1-299 inclusive.
Changes Take Effect: At start/restart

Interval (seconds) accumulated operational reports are submitted to the Reporting Server

rc.amq_connection_send_timeout

Default Value: 60
Valid Values: An integer greater than or equal to 45.
Changes Take Effect: At start/restart

This option specifies the maximum time in seconds to wait for ActiveMQ Producer Send Message response.

rc.cdr.batch_size

Default Value: 500
Valid Values: An integer between 1-5000 inclusive.
Changes Take Effect: At start/restart

The number of CDR messages queued up by the reporting client before sending them up to the reporting server. A higher batch size (e.g. 50 records) will lessen bandwidth constraints, at the cost of making sending CDR data at larger intervals.

rc.cdr.local_queue_max

Default Value: 1000000
Valid Values: An integer greater or equal to -1.
Changes Take Effect: At start/restart

This option specifies the maximum number of data items to the local database for CDR reporting. Queuing to the local database will occur either when the Reporting Server is unavailable, or when data is being provided to the Client faster than the Server can consume it. A value of -1 indicates an "unlimited" number of records will be allowed. A value of 0 indicates that no records will be persisted locally and data will be discarded if the RS is unavailable.

rc.cdr.local_queue_path

Default Value: cdrQueue_rm.db
Valid Values: Path to the DB file.

Changes Take Effect: At start/restart

The full path of the local database file used to locally persist data for CDRs.

rc.cdr.max_throughput

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

This option specifies the maximum rate at which CDR data, in bytes per second, is sent to the Reporting Server. A value of 0 (default) indicates that CDR data will be sent as quickly as possible.

rc.certificate

Default Value:
Valid Values: File path
Changes Take Effect: at start/restart

The file name of the TLS certificate in "PEM" format. Required to connect to the Reporting Server (ActiveMQ) over TLS.

rc.keystore_certificate

Default Value:
Valid Values: File path
Changes Take Effect: at start/restart
Introduced: 9.0.010.68

The file name of the TLS KeyStore certificate in "PEM" format. Required to connect to the Reporting Server (ActiveMQ) over TLS.

rc.keystore_password

Default Value:
Valid Values: KeyStore Password
Changes Take Effect: at start/restart
Introduced: 9.0.010.68

The password for Reporting Client keyStore. Required to connect to the Reporting Server (ActiveMQ) over TLS.

rc.ors.batch_size

Default Value: 500
Valid Values: An integer between 1-5000 inclusive.
Changes Take Effect: At start/restart

The number of OR messages queued up by the reporting client before sending them up to the reporting server.

rc.ors.local_queue_max

Default Value: 1000000
Valid Values: An integer greater or equal to -1.
Changes Take Effect: At start/restart

This option specifies the maximum number of data items to the local database for Operational Reporting. Queuing to the local database will occur either when the Reporting Server is unavailable, or when data is being provided to the Client fdaster than the Server can consume it. A value of -1 indicates an "unlimited" number of records will be allowed. A value of 0 indicates that no records will be persisted locally and data will be discarded if the RS is unavailable.

rc.ors.local_queue_path

Default Value: orsQueue_rm.db
Valid Values: Path to the DB file.
Changes Take Effect: At start/restart

The full path of the local database file used to locally persist data for Operational Reporting.

rc.truststore_certificate

Default Value:
Valid Values: File path
Changes Take Effect: at start/restart
Introduced: 9.0.010.68

The file name of the TLS TrustStore certificate in "PEM" format. Required to connect to the Reporting Server (ActiveMQ) over TLS.

gvp Section

- nic.eth0
- nic.eth1
- nic.linkattribute
- nic.upvalue
- nics

nic.eth0

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

If nics parameter does not explicitly specify 0 as one of the values, this parameter will be ignored. For Windows, MAC address (in hexadecimal format) of the NIC to be monitored MUST be specified here. For Linux, full path to the bonding driver status file can be specified here(default value /proc/net/bonding/bond0 recommended). If the value is left empty or the bonding driver status file cannot be opened for reading, then eth0 will be directly monitored.

nic.eth1

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

If nics parameter does not explicitly specify 1 as one of the values, this parameter will be ignored. For Windows, MAC address (in hexadecimal format) of the NIC to be monitored MUST be specified here. For Linux, full path to the bonding driver status file can be specified here(default value /proc/net/bonding/bond0 recommended). If the value is left empty or the bonding driver status file cannot be opened for reading, then eth1 will be directly monitored.

nic.linkattribute

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

This parameter only affects Linux. On Linux when bonding driver is configured, the string specified in this parameter together with nic.upvalue will be used in determining the health. If left empty, defaults to 'MII Status'.

nic.upvalue

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

This parameter only affects Linux. On Linux when bonding driver is configured, the string specified in this parameter together with nic.linkattribute will be used in determining the health. If left empty, default to 'up'.

nics

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

This parameter specifies the list of NICS specified by nic.eth<n> parameters to be monitored. List of integer <n> can be specified with the space as the delimiter. If this parameter is left empty, note: - on Windows, all NICs will be discovered and monitored. - on Linux, if bonding driver is installed for bond0, then /net/proc/bonding/bond0 will be monitored. Otherwise eth0 to eth<n> will be auto detected and directly monitored. - on both Windows and Linux, all nic.eth<n> parameters will be ignored.

gvp.context-services-authentication Section

- password
- username

password

Default Value:
Valid Values:
Changes Take Effect: immediately

Context Service Authentication Password

username

Default Value:
Valid Values:
Changes Take Effect: immediately

Context Service Authentication Username

gvp-general Section

application-confmaxsize

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

For conference application, user can specify optionally the maximum number of conferences allowed

cisco-record-file

Default Value: CUCM/call-$REFCI$-at-$AGENTDN$-on-$DATE$
Valid Values:
Changes Take Effect: immediately

Specifies the file name pattern that Resource Manager will use when framing the file for Cisco UCM recording. The allowed substitutable strings are - $AGENTDN$: The DN where the call recording is initiated, $REFCI$: The x-refci parameter found in the From header, $DEVICE$: The x-nearenddevice parameter found in the From header, $DATE$: The current date in the YYYY-MM-DD format and $TIME$: The current time in the HH-MM-SS format.

service-type

Default Value:
Valid Values:
Changes Take Effect: immediately

Service Type. The value must be either voicexml, ccxml, conference or announcement.

sip.sessiontimer

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

SIP Session Timer Interval

toll-free-number

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

Tollfree number for this IVR Profile

VirtualReportingTag1

Default Value:
Valid Values:
Changes Take Effect: immediately

Parameter used for Virtual Reporting Object 1

VirtualReportingTag2

Default Value:
Valid Values:
Changes Take Effect: immediately

Parameter used for Virtual Reporting Object 2

gvp.log Section

- metricsfilter

metricsfilter

Default Value:
Valid Values:
Changes Take Effect: immediately

Allows the user to configure the metrics-filters to be sent to all the resources

gvp.policy Section

- announcement-allowed
- announcement-capability-requirement
- announcement-forbidden-respcode
- announcement-forbidden-set-alarm
- announcement-level2-burst-limit
- announcement-level3-burst-limit
- announcement-usage-limit
- announcement-usage-limit-exceeded-respcode
- announcement-usage-limit-exceeded-set-alarm
- announcement-usage-limit-per-session
- asr-reserve
- burst-allowed
- burst-set-alarm
- ccxml-capability-requirement
- ccxml-level2-burst-limit
- ccxml-level3-burst-limit
- ccxml-usage-limit
- ccxml-usage-limit-exceeded-alarm
- ccxml-usage-limit-exceeded-respcode
- ccxml-usage-limit-per-session
- conference-allowed
- conference-capability-requirement
- conference-forbidden-respcode
- conference-forbidden-set-alarm
- conference-level2-burst-limit
- conference-level3-burst-limit
- conference-usage-limit
- conference-usage-limit-exceeded-respcode
- conference-usage-limit-exceeded-set-alarm
- conference-usage-limit-per-session
- cpd-allowed
- cpd-capability-requirement
- cpd-forbidden-respcode
- cpd-forbidden-set-alarm
- cpd-level2-burst-limit
- cpd-level3-burst-limit
- cpd-usage-limit
- cpd-usage-limit-exceeded-respcode
- cpd-usage-limit-exceeded-set-alarm
- cpd-usage-limit-per-session
- cti-allowed
- dialing-rule-forbidden-respcode
- dialing-rule-forbidden-set-alarm
- disable-amr
- disable-amrwb
- disable-g729
- disable-video
- inbound-level2-burst-limit
- inbound-level3-burst-limit
- inbound-usage-limit
- inbound-usage-limit-exceeded-respcode
- inbound-usage-limit-exceeded-set-alarm
- level2-burst-limit
- level3-burst-limit
- max-subdialog-depth
- mcp-asr-usage-mode
- mcp-sendrecv-enabled
- msml-allowed
- msml-capability-requirement
- msml-forbidden-respcode
- msml-forbidden-set-alarm
- msml-level2-burst-limit
- msml-level3-burst-limit
- msml-usage-limit
- msml-usage-limit-exceeded-respcode
- msml-usage-limit-exceeded-set-alarm
- msml-usage-limit-per-session
- outbound-call-allowed
- outbound-call-forbidden-respcode
- outbound-call-forbidden-set-alarm
- outbound-level2-burst-limit
- outbound-level3-burst-limit
- outbound-usage-limit

- outbound-usage-limit-exceeded-respcode
- outbound-usage-limit-exceeded-set-alarm
- prediction-factor
- recordingclient-allowed
- recordingclient-capability-requirement
- recordingclient-forbidden-respcode
- recordingclient-forbidden-set-alarm
- recordingclient-level2-burst-limit
- recordingclient-level3-burst-limit
- recordingclient-usage-limit
- recordingclient-usage-limit-exceeded-respcode
- recordingclient-usage-limit-exceeded-set-alarm
- recordingclient-usage-limit-per-session
- recordingserver-allowed
- recordingserver-capability-requirement
- recordingserver-forbidden-respcode
- recordingserver-forbidden-set-alarm
- recordingserver-level2-burst-limit
- recordingserver-level3-burst-limit
- recordingserver-usage-limit
- recordingserver-usage-limit-exceeded-respcode
- recordingserver-usage-limit-exceeded-set-alarm
- recordingserver-usage-limit-per-session
- retry-on-speech-reserve-failure
- speech-reserve-failure-response
- transfer-allowed
- transfer-forbidden-respcode
- transfer-forbidden-set-alarm
- treatment-allowed
- treatment-capability-requirement
- treatment-forbidden-respcode
- treatment-forbidden-set-alarm
- treatment-level2-burst-limit
- treatment-level3-burst-limit
- treatment-usage-limit
- treatment-usage-limit-exceeded-respcode
- treatment-usage-limit-exceeded-set-alarm
- treatment-usage-limit-per-session
- tts-reserve
- usage-limit-exceeded-respcode
- usage-limit-exceeded-set-alarm
- usage-limits
- use-same-gateway
- voicexml-capability-requirement
- voicexml-dialog-allowed
- voicexml-dialog-forbidden-respcode
- voicexml-dialog-forbidden-set-alarm
- voicexml-level2-burst-limit
- voicexml-level3-burst-limit
- voicexml-usage-limit
- voicexml-usage-limit-exceeded-respcode
- voicexml-usage-limit-exceeded-set-alarm
- voicexml-usage-limit-per-session

announcement-allowed

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

Controls the usage of an announcement resource

announcement-capability-requirement

Default Value:
Valid Values:
Changes Take Effect: immediately

This parameter specifies the required capability for when the announcement service is invoked in the context of an application. The value of this parameter takes a format of: [cap_NameA]=[cap_ValueA1],...,[cap_ValueAm]; [cap_NameB]=[cap_ValueB1],...,[cap_ValueBn]; ; [cap_NameM]=[cap_ValueM1],...,[cap_ValueMi] The set of [cap_NameX] must be unique.

announcement-forbidden-respcode

Default Value: 403
Valid Values:
Changes Take Effect: immediately

Expects parameter value of the form sipcode;desc or just sipcode.

announcement-forbidden-set-alarm

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

If set to true, an alarm will be raised for the corresponding policy violation

announcement-level2-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

Announcement application level2 usage limit

announcement-level3-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

Announcement application level3 usage limit

announcement-usage-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

Announcement application usage limit

announcement-usage-limit-exceeded-respcode

Default Value: 480
Valid Values:
Changes Take Effect: immediately

Expects parameter value of the form sipcode;desc or just sipcode.

announcement-usage-limit-exceeded-set-alarm

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

If set to true, an alarm will be raised for the corresponding policy violation

announcement-usage-limit-per-session

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

Announcement application usage limit per call

asr-reserve

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

This configuration value specifies whether an MCP should pre-allocate ASR resource before accepting the call

burst-allowed

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

Controls whether burst usage for an application is allowed for various usage based policies

burst-set-alarm

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

If set to true, an alarm will be raised when usage limit is excceded and bursting is allowed

ccxml-capability-requirement

Default Value:
Valid Values:
Changes Take Effect: immediately

This parameter specifies the required capability for when the ccxml service is invoked in the context of an application. The value of this parameter takes a format of: [cap_NameA]=[cap_ValueA1],...,[cap_ValueAm]; [cap_NameB]=[cap_ValueB1],...,[cap_ValueBn]; ; [cap_NameM]=[cap_ValueM1],...,[cap_ValueMi] The set of [cap_NameX] must be unique.

ccxml-level2-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

CCXML application level2 usage limit

ccxml-level3-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

CCXML application level3 usage limit

ccxml-usage-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

CCXML application usage limit

ccxml-usage-limit-exceeded-alarm

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

If set to true, an alarm will be raised for the corresponding policy violation

ccxml-usage-limit-exceeded-respcode

Default Value: 480
Valid Values:
Changes Take Effect: immediately

Expects parameter value of the form sipcode;desc or just sipcode.

ccxml-usage-limit-per-session

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

CCXML application usage limit per call

conference-allowed

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

Controls whether the usage of a conference resource is allowed

conference-capability-requirement

Default Value:
Valid Values:
Changes Take Effect: immediately

This parameter specifies the required capability for when the conference service is invoked in the context of an application. The value of this parameter takes a format of: [cap_NameA]=[cap_ValueA1],...,[cap_ValueAm]; [cap_NameB]=[cap_ValueB1],...,[cap_ValueBn]; ; [cap_NameM]=[cap_ValueM1],...,[cap_ValueMi] The set of [cap_NameX] must be unique.

conference-forbidden-respcode

Default Value: 403
Valid Values:
Changes Take Effect: immediately

Expects parameter value of the form sipcode;desc or just sipcode.

conference-forbidden-set-alarm

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

If set to true, an alarm will be raised for the corresponding policy violation

conference-level2-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

Conference application level2 usage limit

conference-level3-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

Conference application level3 usage limit

conference-usage-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

Conference application usage limit

conference-usage-limit-exceeded-respcode

Default Value: 480
Valid Values:
Changes Take Effect: immediately

Expects parameter value of the form sipcode;desc or just sipcode.

conference-usage-limit-exceeded-set-alarm

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

If set to true, an alarm will be raised for the corresponding policy violation

conference-usage-limit-per-session

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

Conference application usage limit per call

cpd-allowed

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

Controls whether CPD service is allowed

cpd-capability-requirement

Default Value:
Valid Values:
Changes Take Effect: immediately

This parameter specifies the required capability for when the cpd service is invoked in the context of an application. The value of this parameter takes a format of: [cap_NameA]=[cap_ValueA1],...,[cap_ValueAm]; [cap_NameB]=[cap_ValueB1],...,[cap_ValueBn]; ; [cap_NameM]=[cap_ValueM1],...,[cap_ValueMi] The set of [cap_NameX] must be unique.

cpd-forbidden-respcode

Default Value: 403
Valid Values:
Changes Take Effect: immediately

Expects parameter value of the form sipcode;desc or just sipcode.

cpd-forbidden-set-alarm

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

If set to true, an alarm will be raised for the corresponding policy violation

cpd-level2-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

CPD application level2 usage limit

cpd-level3-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

CPD application level3 usage limit

cpd-usage-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

CPD application usage limit

cpd-usage-limit-exceeded-respcode

Default Value: 480
Valid Values:
Changes Take Effect: immediately

Expects parameter value of the form sipcode;desc or just sipcode.

cpd-usage-limit-exceeded-set-alarm

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

If set to true, an alarm will be raised for the corresponding policy violation

cpd-usage-limit-per-session

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

CPD application usage limit per call

cti-allowed

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

Controls whether CTI through CTI Connector and IVR Server is allowed. Applicable for CTI based on DN lookup case.

dialing-rule-forbidden-respcode

Default Value: 403
Valid Values:
Changes Take Effect: immediately

Expects parameter value of the form sipcode;desc or just sipcode.

dialing-rule-forbidden-set-alarm

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

If set to true, an alarm will be raised for the corresponding policy violation

disable-amr

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

Controls whether AMR-NB transcoding is enabled

disable-amrwb

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

Controls whether AMR-WB transcoding is enabled

disable-g729

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

Controls whether g729 transcoding is enabled

disable-video

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

Controls whether use of Video is enabled

inbound-level2-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

This parameter specifies the number of times an RM session can be concurrently in-use for an inbound call in the context of this IVRProfile for level2 burst

inbound-level3-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

This parameter specifies the number of times an RM session can be concurrently in-use for an inbound call in the context of this IVRProfile for level3 burst

inbound-usage-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

This parameter specifies the number of times an RM session can be concurrently in-use for an inbound call in the context of this IVRProfile

inbound-usage-limit-exceeded-respcode

Default Value: 480
Valid Values:
Changes Take Effect: immediately

Expects parameter value of the form sipcode;desc or just sipcode.

inbound-usage-limit-exceeded-set-alarm

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

If set to true, an alarm will be raised for the corresponding policy violation

level2-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

This parameter specifies the number of times an RM session can be concurrently in-use in the context of this IVRProfile for level2 burst

level3-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

This parameter specifies the number of times an RM session can be concurrently in-use in the context of this IVRProfile for level3 burst

max-subdialog-depth

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

This parameter limits the number of sub-dialogs in a VoiceXML call. RM simply passes this value to MCP in a Request-URI parameter.

mcp-asr-usage-mode

Default Value: per-call
Valid Values:
Changes Take Effect: immediately

When this parameter is set to per-call, there will be only one VRM session for the entire call which could have multiple recognition sessions. If the parameter value is set to per-utterance, a VRM session is opened for each recognition request. The VRM session is closed when the recognition request is completed successfully or unsuccessfully (such as no match). RM simply passes this value to MCP in a Request-URI parameter.

mcp-sendrecv-enabled

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

This configuration value specifies whether an MCP is allowed to perform <send> and <receive> extensions. The RM simply passes this value to the MCP in a Request-URI parameter.

msml-allowed

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

Controls whether MSML service is allowed

msml-capability-requirement

Default Value:
Valid Values:
Changes Take Effect: immediately

This parameter specifies the required capability for when the MSML service is invoked in the context of an application. The value of this parameter takes a format of: [cap_NameA]=[cap_ValueA1],...,[cap_ValueAm]; [cap_NameB]=[cap_ValueB1],...,[cap_ValueBn]; ; [cap_NameM]=[cap_ValueM1],...,[cap_ValueMi] The set of [cap_NameX] must be unique.

msml-forbidden-respcode

Default Value: 403
Valid Values:
Changes Take Effect: immediately

Expects parameter value of the form sipcode;desc or just sipcode.

msml-forbidden-set-alarm

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

If set to true, an alarm will be raised for the corresponding policy violation

msml-level2-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

level2 usage limit for MSML service-type

msml-level3-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

level3 usage limit for MSML service-type

msml-usage-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

usage limit for MSML service-type

msml-usage-limit-exceeded-respcode

Default Value: 480
Valid Values:
Changes Take Effect: immediately

Expects parameter value of the form sipcode;desc or just sipcode.

msml-usage-limit-exceeded-set-alarm

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

If set to true, an alarm will be raised for the corresponding policy violation

msml-usage-limit-per-session

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

usage limit per call for MSML service type

outbound-call-allowed

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

Controls whether the outbound call is allowed

outbound-call-forbidden-respcode

Default Value: 403
Valid Values:
Changes Take Effect: immediately

Expects parameter value of the form sipcode;desc or just sipcode.

outbound-call-forbidden-set-alarm

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

If set to true, an alarm will be raised for the corresponding policy violation

outbound-level2-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

This parameter specifies the number of times an RM session can be concurrently in-use for an outbound call in the context of this IVRProfile for level2 burst

outbound-level3-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

This parameter specifies the number of times an RM session can be concurrently in-use for an outbound call in the context of this IVRProfile for level3 burst

outbound-usage-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

This parameter specifies the number of times an RM session can be concurrently in-use for an outbound call in the context of this IVRProfile

outbound-usage-limit-exceeded-respcode

Default Value: 480
Valid Values:
Changes Take Effect: immediately

Expects parameter value of the form sipcode;desc or just sipcode.

outbound-usage-limit-exceeded-set-alarm

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

If set to true, an alarm will be raised for the corresponding policy violation

prediction-factor

Default Value: 1.0
Valid Values: Must be a numeric value either floating point or integer
Changes Take Effect: immediately

This parameter determines the ratio of engaging calls to predictive calls. It can be greater than 0.33 and less than or equal to 1. Default value is 1.0.

recordingclient-allowed

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

Controls whether Recording Client service is allowed

recordingclient-capability-requirement

Default Value:
Valid Values:
Changes Take Effect: immediately

This parameter specifies the required capability for when the Recording Client service is invoked in the context of an application. The value of this parameter takes a format of: [cap_NameA]=[cap_ValueA1],...,[cap_ValueAm]; [cap_NameB]=[cap_ValueB1],...,[cap_ValueBn]; ; [cap_NameM]=[cap_ValueM1],...,[cap_ValueMi] The set of [cap_NameX] must be unique.

recordingclient-forbidden-respcode

Default Value: 403
Valid Values:
Changes Take Effect: immediately

Expects parameter value of the form sipcode;desc or just sipcode.

recordingclient-forbidden-set-alarm

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

If set to true, an alarm will be raised for the corresponding policy violation

recordingclient-level2-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

level2 usage limit for Recording Client service-type

recordingclient-level3-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

level3 usage limit for Recording Client service-type

recordingclient-usage-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

usage limit for Recording Client service-type

recordingclient-usage-limit-exceeded-respcode

Default Value: 480
Valid Values:
Changes Take Effect: immediately

Expects parameter value of the form sipcode;desc or just sipcode.

recordingclient-usage-limit-exceeded-set-alarm

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

If set to true, an alarm will be raised for the corresponding policy violation

recordingclient-usage-limit-per-session

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

usage limit per call for Recording Client service type

recordingserver-allowed

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

Controls whether Recording Server service is allowed

recordingserver-capability-requirement

Default Value:
Valid Values:
Changes Take Effect: immediately

This parameter specifies the required capability for when the Recording Server service is invoked in the context of an application. The value of this parameter takes a format of: [cap_NameA]=[cap_ValueA1],...,[cap_ValueAm]; [cap_NameB]=[cap_ValueB1],...,[cap_ValueBn]; ; [cap_NameM]=[cap_ValueM1],...,[cap_ValueMi] The set of [cap_NameX] must be unique.

recordingserver-forbidden-respcode

Default Value: 403
Valid Values:
Changes Take Effect: immediately

Expects parameter value of the form sipcode;desc or just sipcode.

recordingserver-forbidden-set-alarm

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

If set to true, an alarm will be raised for the corresponding policy violation

recordingserver-level2-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

level2 usage limit for Recording Server service-type

recordingserver-level3-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

level3 usage limit for Recording Server service-type

recordingserver-usage-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

usage limit for Recording Server service-type

recordingserver-usage-limit-exceeded-respcode

Default Value: 480
Valid Values:
Changes Take Effect: immediately

Expects parameter value of the form sipcode;desc or just sipcode.

recordingserver-usage-limit-exceeded-set-alarm

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

If set to true, an alarm will be raised for the corresponding policy violation

recordingserver-usage-limit-per-session

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

usage limit per call for Recording Server service type

retry-on-speech-reserve-failure

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

This configuration value specifies whether RM should retry further resources when MCP sends ASR/TTS pre-allocation failure in response.

speech-reserve-failure-response

Default Value: 0
Valid Values:
Changes Take Effect: immediately

This configuration value specifies what response code RM should send if MCP sent ASR/TTS resource allocation failure and retry option is set to false in profile. The default value is 0 that signifies the MCP return code will not be overwritten. To overwrite MCP return code this parameter should be set to proper 4xx/5xx value.

transfer-allowed

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

Controls whether transfer is allowed

transfer-forbidden-respcode

Default Value: 403
Valid Values:

Changes Take Effect: immediately

Expects parameter value of the form sipcode;desc or just sipcode. Example - 403 or 403;This application does not allow call transfer

transfer-forbidden-set-alarm

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

If set to true, an alarm will be raised for the corresponding policy violation

treatment-allowed

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

Controls whether Treatment media service is allowed

treatment-capability-requirement

Default Value:
Valid Values:
Changes Take Effect: immediately

This parameter specifies the required capability for when the treatment service is invoked in the context of an application. The value of this parameter takes a format of: [cap_NameA]=[cap_ValueA1],...,[cap_ValueAm]; [cap_NameB]=[cap_ValueB1],...,[cap_ValueBn]; ; [cap_NameM]=[cap_ValueM1],...,[cap_ValueMi] The set of [cap_NameX] must be unique.

treatment-forbidden-respcode

Default Value: 403
Valid Values:
Changes Take Effect: immediately

Expects parameter value of the form sipcode;desc or just sipcode.

treatment-forbidden-set-alarm

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

If set to true, an alarm will be raised for the corresponding policy violation

treatment-level2-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

level2 usage limit for Treatment service-type

treatment-level3-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

level3 usage limit for Treatment service-type

treatment-usage-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

usage limit for Treatment media service-type

treatment-usage-limit-exceeded-respcode

Default Value: 480
Valid Values:
Changes Take Effect: immediately

Expects parameter value of the form sipcode;desc or just sipcode.

treatment-usage-limit-exceeded-set-alarm

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

If set to true, an alarm will be raised for the corresponding policy violation

treatment-usage-limit-per-session

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

usage limit per call for Treatment service type

tts-reserve

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

This configuration value specifies whether an MCP should pre-allocate TTS resource before accepting the call

usage-limit-exceeded-respcode

Default Value: 480
Valid Values:
Changes Take Effect: immediately

When a call is rejected due to the configuration value of one of: gvp.policy.usage-limits, or gvp.policy.outbound-usage-limit, or gvp.policy.inbound-usage-limit this is the SIP response code sent in the SIP response. Takes the form of [sipcode];[desc] or [sipcode], where [sipcode] is an number in the range of 400-699, and [desc] is any string

usage-limit-exceeded-set-alarm

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

If set to true, an alarm will be raised for the corresponding policy violation

usage-limits

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

This parameter specifies the number of times an RM session can be concurrently in-use in the context of this IVRProfile

use-same-gateway

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

This parameter is for Gateway Resource only.

voicexml-capability-requirement

Default Value:
Valid Values:
Changes Take Effect: immediately

This parameter specifies the required capability for when the voicexml service is invoked in the context of an application. The value of this parameter takes a format of: [cap_NameA]=[cap_ValueA1],...,[cap_ValueAm]; [cap_NameB]=[cap_ValueB1],...,[cap_ValueBn]; ; [cap_NameM]=[cap_ValueM1],...,[cap_ValueMi] The set of [cap_NameX] must be unique.

voicexml-dialog-allowed

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

Controls whether the usage of a voicexml resource is allowed

voicexml-dialog-forbidden-respcode

Default Value: 403
Valid Values:

Changes Take Effect: immediately

Expects parameter value of the form sipcode;desc or just sipcode.

voicexml-dialog-forbidden-set-alarm

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

If set to true, an alarm will be raised for the corresponding policy violation

voicexml-level2-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

Voicexml application level2 usage limit

voicexml-level3-burst-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

Voicexml application level3 usage limit

voicexml-usage-limit

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

Voicexml application usage limit

voicexml-usage-limit-exceeded-respcode

Default Value: 480
Valid Values:
Changes Take Effect: immediately

Expects parameter value of the form sipcode;desc or just sipcode.

voicexml-usage-limit-exceeded-set-alarm

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

If set to true, an alarm will be raised for the corresponding policy violation

voicexml-usage-limit-per-session

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: immediately

Voicexml application usage limit per call

gvp.policy.call-info Section

- rule-1
- rule-2

rule-1

Default Value:
Valid Values:
Changes Take Effect: immediately

The parameters within the gvp.policy.call-info sub-section for IVR Profile are used to specify the ANI-based rules to accept, reject, or script play for a call

rule-2

Default Value:
Valid Values:
Changes Take Effect: immediately

The parameters within the gvp.policy.call-info sub-section for IVR Profile are used to specify the ANI-based rules to accept, reject, or script play for a call

gvp.policy.dbmp Section

- rs.db.retention.cdr.default
- rs.db.retention.events.default
- rs.db.retention.latencies.daily.default
- rs.db.retention.latencies.hourly.default
- rs.db.retention.latencies.monthly.default
- rs.db.retention.latencies.weekly.default
- rs.db.retention.operations.30min.default
- rs.db.retention.operations.5min.default
- rs.db.retention.operations.daily.default
- rs.db.retention.operations.hourly.default
- rs.db.retention.operations.monthly.default
- rs.db.retention.operations.weekly.default
- rs.db.retention.sq.daily.default
- rs.db.retention.sq.failures.default
- rs.db.retention.sq.hourly.default
- rs.db.retention.sq.monthly.default
- rs.db.retention.sq.weekly.default
- rs.db.retention.var.30min.default
- rs.db.retention.var.5min.default
- rs.db.retention.var.daily.default
- rs.db.retention.var.hourly.default
- rs.db.retention.var.monthly.default
- rs.db.retention.var.weekly.default

rs.db.retention.cdr.default

Default Value: 30
Valid Values: An integer greater than 0, or 0 to use RS default
Changes Take Effect: immediately

The number of days for which Call Detail Records data will be retained in the database.

rs.db.retention.events.default

Default Value: 7
Valid Values: An integer greater than 0, or 0 to use RS default
Changes Take Effect: immediately

The number of days for which call log events (upstream logs) data will be retained in the database.

rs.db.retention.latencies.daily.default

Default Value: 90
Valid Values: An integer greater than 30
Changes Take Effect: immediately

The number of days for which daily latency histogram data will be retained in the database.

rs.db.retention.latencies.hourly.default

Default Value: 7
Valid Values: An integer greater than 0, or 0 to use RS default
Changes Take Effect: immediately

The number of days for which hourly latency histogram data will be retained in the database.

rs.db.retention.latencies.monthly.default

Default Value: 1095
Valid Values: An integer greater than 30
Changes Take Effect: immediately

The number of days for which monthly latency histogram data will be retained in the database.

rs.db.retention.latencies.weekly.default

Default Value: 364
Valid Values: An integer greater than 30
Changes Take Effect: immediately

The number of days for which weekly latency histogram data will be retained in the database.

rs.db.retention.operations.30min.default

Default Value: 7
Valid Values: An integer greater than 0, or 0 to use RS default
Changes Take Effect: immediately

The number of days for which 30-minute operational data will be retained in the database.

rs.db.retention.operations.5min.default

Default Value: 0
Valid Values: An integer greater than 0, or 0 to use RS default
Changes Take Effect: immediately

The number of days for which 5-minute operational data will be retained in the database.

rs.db.retention.operations.daily.default

Default Value: 90
Valid Values: An integer greater than 30
Changes Take Effect: immediately

The number of days for which daily operational data will be retained in the database.

rs.db.retention.operations.hourly.default

Default Value: 7
Valid Values: An integer greater than 0, or 0 to use RS default
Changes Take Effect: immediately

The number of days for which hourly operational data will be retained in the database.

rs.db.retention.operations.monthly.default

Default Value: 1095
Valid Values: An integer greater than 30
Changes Take Effect: immediately

The number of days for which monthly operational data will be retained in the database.

rs.db.retention.operations.weekly.default

Default Value: 364
Valid Values: An integer greater than 30
Changes Take Effect: immediately

The number of days for which weekly operational data will be retained in the database.

rs.db.retention.sq.daily.default

Default Value: 90
Valid Values: An integer greater than 30
Changes Take Effect: immediately

The number of days for which daily Service Quality summary data will be retained in the database.

rs.db.retention.sq.failures.default

Default Value: 365
Valid Values: An integer greater than 0, or 0 to use RS default
Changes Take Effect: immediately

The number of days for which Service Quality failure detail records will be retained in the database.

rs.db.retention.sq.hourly.default

Default Value: 7
Valid Values: An integer greater than 0, or 0 to use RS default
Changes Take Effect: immediately

The number of days for which hourly Service Quality summary data will be retained in the database.

rs.db.retention.sq.monthly.default

Default Value: 365
Valid Values: An integer greater than 30
Changes Take Effect: immediately

The number of days for which monthly Service Quality summary data will be retained in the database.

rs.db.retention.sq.weekly.default

Default Value: 180
Valid Values: An integer greater than 30
Changes Take Effect: immediately

The number of days for which weekly Service Quality summary data will be retained in the database.

rs.db.retention.var.30min.default

Default Value: 7
Valid Values: An integer greater than 0, or 0 to use RS default
Changes Take Effect: immediately

The number of days for which 30-minute Call Summary and IVR Action Summary data will be retained in the database.

rs.db.retention.var.5min.default

Default Value: 0
Valid Values: An integer greater than 0, or 0 to use RS default
Changes Take Effect: immediately

The number of days for which 5-minute Call Summary and IVR Action Summary data will be retained in the database.

rs.db.retention.var.daily.default

Default Value: 90
Valid Values: An integer greater than 30
Changes Take Effect: immediately

The number of days for which daily Call Summary and IVR Action Summary data will be retained in the database.

rs.db.retention.var.hourly.default

Default Value: 7
Valid Values: An integer greater than 0, or 0 to use RS default
Changes Take Effect: immediately

The number of days for which hourly Call Summary and IVR Action Summary data will be retained in the database.

rs.db.retention.var.monthly.default

Default Value: 1095
Valid Values: An integer greater than 30
Changes Take Effect: immediately

The number of days for which monthly Call Summary and IVR Action Summary data will be retained in the database.

rs.db.retention.var.weekly.default

Default Value: 364
Valid Values: An integer greater than 30

Changes Take Effect: immediately

The number of days for which weekly Call Summary and IVR Action Summary data will be retained in the database.

gvp.policy.dialing-rules Section

- rule-1
- rule-2

rule-1

Default Value:
Valid Values:
Changes Take Effect: immediately

The parameters within the gvp.policy.dialing-rules sub-section are used to specify dialing rules used to determine if an address made towards a GW is allowed

rule-2

Default Value:
Valid Values:
Changes Take Effect: immediately

The parameters within the gvp.policy.dialing-rules sub-section are used to specify dialing rules used to determine if an address made towards a GW is allowed

gvp.policy.speech-resources Section

- asr.defaultengine
- authorizedasrengines
- authorizedttsengines
- defaultlanguage
- nsssessionxml
- tts.defaultengine

asr.defaultengine

Default Value:
Valid Values:
Changes Take Effect: immediately

The engine specified here will be used to load a default engine when using the log metrics to ASR configuration. An application using a different name should override this using the Request URI configuration or asrengine property.

authorizedasrengines

Default Value:
Valid Values:
Changes Take Effect: immediately

This parameter represents the ":" delimited list of ASR resources that are authorized to be used by this profile

authorizedttsengines

Default Value:
Valid Values:
Changes Take Effect: immediately

This parameter represents the ":" delimited list of TTS resources that are authorized to be used by this profile

defaultlanguage

Default Value:
Valid Values:
Changes Take Effect: immediately

This parameter represents the default language for ASR/TTS

nsssessionxml

Default Value:
Valid Values:
Changes Take Effect: immediately

This parameter specifies the path of a session configuration file for the speech recognizer and synthesizer used by this application. When it is set, RM shall pass the value to MCP in a Request-URI parameter "gvp.config.vrm.nsssessionxml".

tts.defaultengine

Default Value:
Valid Values:
Changes Take Effect: immediately

The engine specified here will be used to load a default engine. An application using a different name should override this using the ttsengine property or the Request URI configuration.

gvp.policy.sqa Section

- error.notification.threshold

error.notification.threshold

Default Value: -1
Valid Values: An integer between 0 and 100 inclusive. Specify -1 to use RS' default setting.
Changes Take Effect: immediately

If the percentage of successful calls for an IVR Profile falls below this threshold during a service quality period, a notification is generated.

gvp.service-parameters Section

- cti.DefaultAgent
- cti.icm.enableBridgeXfer
- cti.icm.ScriptMapping
- cti.icm.ServiceID
- cti.TransferOnCTI
- recordingclient.audiosrc
- recordingclient.AWSAccessKeyId
- recordingclient.AWSAccessKeyId2
- recordingclient.AWSSecretAccessKey
- recordingclient.AWSSecretAccessKey2
- recordingclient.callrec_authorization
- recordingclient.callrec_dest
- recordingclient.httpauthorization
- recordingclient.httpauthorization2
- recordingclient.recdest
- recordingclient.recdest2
- recordingclient.recmediactl
- recordingclient.tonesilenceduration
- recordingclient.type
- recordingclient.type2
- voicexml.gvp.appmodule
- voicexml.gvpi.$adn-flag$
- voicexml.gvpi.$asrplatform$
- voicexml.gvpi.$asrwavfilelog$
- voicexml.gvpi.$badxmlpageposturl$
- voicexml.gvpi.$call-trace-url$
- voicexml.gvpi.$ccerror-telnum$
- voicexml.gvpi.$cpatimeout$
- voicexml.gvpi.$cti_endcall_on_agentleg_hup$
- voicexml.gvpi.$debug-url$
- voicexml.gvpi.$default-language$
- voicexml.gvpi.$dtmf_nomatch_utterance_enabled$
- voicexml.gvpi.$ivr-tmo$
- voicexml.gvpi.$outbound-call-limit$
- voicexml.gvpi.$record-pages$
- voicexml.gvpi.$rexfertimeout$
- voicexml.gvpi.$tntenable$
- voicexml.gvpi.$tntreclaimcode$
- voicexml.gvpi.$tntscript$
- voicexml.gvpi.$transactional-record$
- voicexml.gvpi.$transactional-record-posturl$
- voicexml.gvpi.$transfer-option$
- voicexml.gvpi.$transfer-type$
- voicexml.gvpi.$transferscript-url$
- voicexml.gvpi.$trap-url$
- voicexml.gvpi.$tts-gender$
- voicexml.gvpi.$tts-vendor$

cti.DefaultAgent

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

The default agent number for CTI transfer

cti.icm.enableBridgeXfer

Default Value: fixed,0

Valid Values:
Changes Take Effect: immediately

By enabling this parameter, the CTIC invokes Bridge Transfer to connect the caller to agent otherwise by default Blind Transfer is triggered. This feature is applicable only for Service Control Interface when CONNECT message is received with TransferHint flag set to false.

cti.icm.ScriptMapping

Default Value: fixed,TFN
Valid Values:
Changes Take Effect: immediately

This parameter indicates whether the ICM routing script should be chosen based on the TFN or the DNIS

cti.icm.ServiceID

Default Value: fixed,
Valid Values:
Changes Take Effect: immediately

The Service-ID configured in ICM for this IVR application

cti.TransferOnCTI

Default Value: fixed,no
Valid Values:
Changes Take Effect: immediately

CTI transfer option

recordingclient.audiosrc

Default Value:
Valid Values:
Changes Take Effect: immediately

The URI of a periodic audio tone to play during recording. If the URI is empty, no tone will be applied.

recordingclient.AWSAccessKeyId

Default Value:
Valid Values:
Changes Take Effect: immediately

This parameter specifies the AWS Access Key ID for recdest when the destination is Amazon S3.

recordingclient.AWSAccessKeyId2

Default Value:
Valid Values:
Changes Take Effect: immediately

This parameter specifies the AWS Access Key ID for recdest2 when the destination is Amazon S3.

recordingclient.AWSSecretAccessKey

Default Value:
Valid Values:
Changes Take Effect: immediately

This parameter specifies the AWS Secret Access Key for recdest when the destination is Amazon S3.

recordingclient.AWSSecretAccessKey2

Default Value:
Valid Values:
Changes Take Effect: immediately

This parameter specifies the AWS Secret Access Key for recdest2 when the destination is Amazon S3.

recordingclient.callrec_authorization

Default Value:
Valid Values:
Changes Take Effect: immediately

The authorization parameter for posting metadata. The format for specifying the authorization information is: username:password, where 'username' and 'password' are the credentials for accessing the web server.

recordingclient.callrec_dest

Default Value:
Valid Values:
Changes Take Effect: immediately

The URL for submitting Metadata as part of call recording.

recordingclient.httpauthorization

Default Value:
Valid Values:
Changes Take Effect: immediately

This parameter specifies the HTTP authorization information if "recdest" is specified to be an http:// destination (WebDAV). The format for specifying the authorization information is: username:password, where 'username' and 'password' are the credentials for accessing the web server.

recordingclient.httpauthorization2

Default Value:
Valid Values:
Changes Take Effect: immediately

This parameter specifies the HTTP authorization information if "recdest2" is specified to be an http:// destination (SpeechMiner). The format for specifying the authorization information is: username:password, where 'username' and 'password' are the credentials for accessing the web server.

recordingclient.recdest

Default Value: fixed,sip:$LocalIP$:5060
Valid Values:
Changes Take Effect: immediately

This parameter specifies one of the destinations for recording. The following types of destinations are allowed: - sip / sips URI. This will be used as the Request-URI address part of the outgoing recording server request. - file:// for local file recording. Must begin with file://. Path is relative to recording base path configured on the MCP, or can also be an absolute path location. - s3: for specifying an Amazon S3 storage bucket (must be accompanied by AWSAccessKeyId and AWSSecretAccessKey). - http:// or https:// for specifying a WebDAV storage location. Default value is the RM's address. However, the value of the "dest" parameter in the MSML request takes precedence over this IVR Profile parameter in the media server. When recdest / recdest2 are both configured, they must be both sip / sips, OR both one of the other possible destinations. Additional notes related to sip / sips destination: When recdest is set to RM (SIP AOR), MCP will use this in the Request-URI address part of the recording server request. RM will select the recording server resources based on load-balancing scheme configured in recording server LRGs. When recdest2 is configured, recdest should also be configured and these two parameters should be configured with AORs of two recording servers. Both recdest and recdest2 will be used by MCP in the Request-URI address part of the recording server request and in this case MCP will send two recording request to RM for the same recording (duplicate recording). RM will select recording server based on the Request-URI address. Please note that these recdest and recdest2 parameters should be configured for duplicate recording with third party recorders like zoom.

recordingclient.recdest2

Default Value: fixed,sip:$LocalIP$:5060
Valid Values:
Changes Take Effect: immediately

This parameter specifies a secondary/duplicate recording destination. The following types of destinations are allowed: - sip / sips URI. This will be used as the Request-URI address part of the outgoing recording server request. - file:// for local file recording. Must begin with file://. Path is relative to recording base path configured on the MCP, or can also be an absolute path location. - s3: for specifying an Amazon S3 storage bucket (must be accompanied by AWSAccessKeyId2 and AWSSecretAccessKey2). - http:// or https:// for specifying a SpeechMiner destination for analytics (requires call recording solution integration). Default value is the RM's address. However, the value of the "dest2" parameter in the MSML request takes precedence over this IVR Profile parameter in the media server. When recdest / recdest2 are both configured, they must be both sip / sips, OR both one of the other possible destinations. Additional notes related to sip / sips destination: If "recdest" and "recdest2" parameter are set to SIP AORs of recording servers, the MCP will use these AORs in RURI address part. When recdest2 is configured, recdest should also be configured and these two parameters should be configured with AORs of two recording servers. Both recdest and recdest2 will be used by MCP in the Request-URI address part of the recording server request and in this case MCP will send two recording request to RM for the same recording (duplicate recording). RM will select recording server based on the Request-URI address. Please note that these recdest and recdest2 parameters should be configured for duplicate recording with third party recorders like zoom

recordingclient.recmediactl

Default Value: fixed,2
Valid Values:
Changes Take Effect: immediately

Select the SIP session behavior of the media server in contacting the external recorder. If set to "Separate", separate SIP session (with single media line in the SDP) will be established for each of the recorded parties. If set to "Combined", 1 SIP session (with multiple media lines in the SDP) is established for the recorded parties in the same call recording session. Note that the URI specified by the "recmediactl" parameter in the MSML request takes precedence over this parameter.

recordingclient.tonesilenceduration

Default Value:
Valid Values:
Changes Take Effect: immediately

The duration of silence between audio tones when Periodic Audio Tone is in use in milliseconds.

recordingclient.type

Default Value:
Valid Values:
Changes Take Effect: immediately

The file type for http, S3 or file recording for recdest. Example formats: audio/wav, audio/wav;codec=ulaw, audio/mp3 . If left empty, the MCP will use a default configured type.

recordingclient.type2

Default Value:
Valid Values:
Changes Take Effect: immediately

The file type for http, S3 or file recording for recdest2. Example formats: audio/wav, audio/wav;codec=ulaw, audio/mp3 . If left empty, the MCP will use a default configured type.

voicexml.gvp.appmodule

Default Value: fixed,VXML-NG
Valid Values:
Changes Take Effect: immediately

Select the app module name

voicexml.gvpi.$adn-flag$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$asrplatform$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$asrwavfilelog$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$badxmlpageposturl$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$call-trace-url$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$ccerror-telnum$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$cpatimeout$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$cti_endcall_on_agentleg_hup$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$debug-url$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$default-language$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$dtmf_nomatch_utterance_enabled$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$ivr-tmo$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$outbound-call-limit$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$record-pages$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$rexfertimeout$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$tntenable$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$tntreclaimcode$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$tntscript$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$transactional-record$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$transactional-record-posturl$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$transfer-option$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$transfer-type$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$transferscript-url$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$trap-url$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$tts-gender$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

voicexml.gvpi.$tts-vendor$

Extension:DynamicPageList (DPL), version 2.01 : Warning: No results.

gvp.service-prerequisite Section

- alternatevoicexml
- announcement-url
- conference-id
- default-properties-page
- initial-page-url

alternatevoicexml

Default Value:
Valid Values:
Changes Take Effect: immediately

For VoiceXML IVR profile an alternate voicexml parameter is also supported that's used by MCP if the initial-page-url fails

announcement-url

Default Value:
Valid Values: The value should be a URL to the announcement audio file
Changes Take Effect: immediately

For announcement application, announcement-url is a mandatory parameter

conference-id

Default Value:
Valid Values: The value can be any string value
Changes Take Effect: immediately

For conference application, conference-id is mandatory parameter

default-properties-page

Default Value:
Valid Values:

Changes Take Effect: immediately

For voicexml service, this is the URL to a page containing the default properties and handlers

initial-page-url

Default Value:
Valid Values:
Changes Take Effect: immediately

Initial Page URL is a mandatory parameter for VoiceXML, and CCXML Voice Platform IVR Profile

log Section

- all
- check-point
- compatible-output-priority
- debug
- expire
- interaction
- keep-startup-file
- memory
- memory-storage-size
- message_format
- messagefile
- print-attributes
- segment
- spool
- standard
- time_convert
- time_format
- trace
- verbose

all

Default Value: ../logs/ResourceMgr

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
Changes Take Effect: immediately
Specifies the outputs to which an application sends all log events. The log output types must be separated by a comma when more than one output is configured.

check-point

Default Value: 1
Valid Values: 0 - 24
Changes Take Effect: immediately

Specifies, in hours, how often the application generates a check point log event, to divide the log into sections of equal time. By

default, the application generates this log event every hour. Setting the option to 0 prevents the generation of check-point events.

compatible-output-priority

Default Value: false
Valid Values: true, false
Changes Take Effect: immediately

Specifies whether the application uses 6.x output logic.

- **true** The log of the level specified by "Log Output Options" is sent to the specified output.
- **false** The log of the level specified by "Log Output Options" and higher levels is sent to the specified output.

debug

Default Value: ../logs/ResourceMgr

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends the log events of the Debug level and higher (that is, log events of the Standard, Interaction, Trace, and Debug levels). The log output types must be separated by a comma when more than one output is configured.

expire

Default Value: 20

Valid Values:

- **false** No expiration; all generated segments are stored.
- **[number] file or [number]** Sets the maximum number of log files to store. Specify a number from 1-1000.
- **[number] day** Sets the maximum number of days before log files are deleted. Specify a number from 1-100.
  Changes Take Effect: immediately
  Determines whether log files expire. If they do, sets the measurement for determining when they expire, along with the maximum number of files (segments) or days before the files are removed. This option is ignored if log output is not configured to be sent to a log file. Note: If the value of the option is set incorrectly -out of the range of valid values- it will be automatically reset to 10

interaction

Default Value: ../logs/ResourceMgr

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
Changes Take Effect: immediately
Specifies the outputs to which an application sends the log events of the Interaction level and higher (that is, log events of the Standard and Interaction levels). The log outputs must be separated by a comma when more than one output is configured.

keep-startup-file

Default Value: false

Valid Values:

- **false** No startup segment of the log is kept.
- **true** A startup segment of the log is kept. The size of the segment equals the value of the segment option.
- **[number] KB** Sets the maximum size, in kilobytes, for a startup segment of the log.
- **[number] MB** Sets the maximum size, in megabytes, for a startup segment of the log.
Changes Take Effect: After restart
Specifies whether a startup segment of the log, containing the initial T-Server configuration, is to be kept. If it is, this option can be set to true or to a specific size. If set to true, the size of the initial segment will be equal to the size of the regular log segment defined by the segment option. The value of this option will be ignored if segmentation is turned off (that is, if the segment option set to false).

memory

Default Value:
Valid Values: [string] (memory file name)
Changes Take Effect: immediately

Specifies the name of the file to which the application regularly prints a snapshot of the memory output, if it is configured to do this. The new snapshot overwrites the previously written data. If the application terminates abnormally, this file will contain the latest log messages. Memory output is not recommended for processors with a CPU frequency lower than 600 MHz.

memory-storage-size

Default Value:

Valid Values:

- **[number] KB or [number]** The size of the memory output, in kilobytes. The minimum value is 128 KB.
- **[number] MB** The size of the memory output, in megabytes. The maximum value is 64 MB
  Changes Take Effect: When memory output is created
  Specifies the buffer size for log output to the memory, if configured.

message_format

Default Value: short

Valid Values:

- **short** An application uses compressed headers when writing log records in its log file.
- **full** An application uses complete headers when writing log records in its log file.
  Changes Take Effect: immediately
  Specifies the format of log record headers that an application uses when writing logs in the log file. Using compressed log record headers improves application performance and reduces the log file's size. With the value set to short:
- A header of the log file or the log file segment contains information about the application (such as the application name, application type, host type, and time zone), whereas single log records within the file or segment omit this information.
- A log message priority is abbreviated to Std, Int, Trc, or Dbg, for Standard, Interaction, Trace, or Debug messages, respectively.
- The message ID does not contain the prefix GCTI or the application type ID.
  A log record in the full format looks like this:
  2002-05-07T18:11:38.196 Standard localhost cfg_dbserver GCTI-00-05060 Application started
  A log record in the short format looks like this:
  2002-05-07T18:15:33.952 Std 05060 Application started

messagefile

Default Value:
Valid Values: [string].lms (message file name)
Changes Take Effect: Immediately, if an application cannot find its *.lms file at startup

Specifies the file name for application-specific log events. The name must be valid for the operating system on which the application is running. The option value can also contain the absolute path to the application-specific *.lms file. Otherwise, an application looks for the file in its working directory.

print-attributes

Default Value: false
Valid Values: true, false
Changes Take Effect: immediately

Specifies whether the application attaches extended attributes, if any exist, to a log event that it sends to log output. Typically, log events of the Interaction log level and Audit-related log events contain extended attributes. Setting this option to true enables audit capabilities, but negatively affects performance. Genesys recommends enabling this option for Solution Control Server and Configuration Server when using audit tracking. For other applications, refer to Genesys 7.5 Combined Log Events Help to find out whether an application generates Interaction-level and Audit-related log events; if it does, enable the option only when testing new interaction scenarios.

- **true** Attaches extended attributes, if any exist, to a log event sent to log output.
- **false** Does not attach extended attributes to a log event sent to log output.

segment

Default Value: 10000

Valid Values:

- **false** No segmentation is allowed.
- **[number] KB or [number]** Sets the maximum segment size, in kilobytes. The minimum segment size is 100 KB.
- **[number] MB** Sets the maximum segment size, in megabytes.
- **[number] hr** Sets the number of hours for the segment to stay open. The minimum number is 1 hour.
  Changes Take Effect: immediately
  Specifies whether there is a segmentation limit for a log file. If there is, sets the mode of measurement, along with the maximum size. If the current log segment exceeds the size set by this option, the file is closed and a new one is created.

spool

Default Value:
Valid Values: [path] (the folder, with the full path to it)
Changes Take Effect: immediately

Specifies the folder, including full path to it, in which an application creates temporary files related to network log output. If you change the option value while the application is running, the change does not affect the currently open network output.

standard

Default Value: ../logs/ResourceMgr

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends the log events of the Standard level. The log output types must be separated by a comma when more than one output is configured.

time_convert

Default Value: local
Valid Values: local, utc
Changes Take Effect: immediately

Specifies the system in which an application calculates the log record time when generating a log file. The time is converted from the time in seconds since the Epoch (00:00:00 UTC, January 1, 1970).

- **Local Time (local)** The time of log record generation is expressed as a local time, based on the time zone and any seasonal adjustments. Time zone information of the application's host computer is used.
- **Coordinated Universal Time (utc)** The time of log record generation is expressed as Coordinated Universal Time (UTC).

time_format

Default Value: ISO8601
Valid Values: time, locale, ISO8601
Changes Take Effect: immediately

Specifies how to represent, in a log file, the time when an application generates log records.
A log record's time field in the ISO 8601 format looks like this:
2001-07-24T04:58:10.123

- **HH:MM:SS.sss (time)** The time string is formatted according to the HH:MM:SS.sss (hours, minutes, seconds, and milliseconds) format.
- **According to the system's locale (locale)** The time string is formatted according to the system's locale.
- **ISO 8601 format (ISO8601)** The date in the time string is formatted according to the ISO 8601 format. Fractional seconds are given in milliseconds.

trace

Default Value: ../logs/ResourceMgr

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends the log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels). The log outputs must be separated by a comma when more than one output is configured.

verbose

Default Value: standard
Valid Values: all, debug, trace, interaction, standard, none
Changes Take Effect: immediately

Determines whether a log output is created. If it is, specifies the minimum level of log events generated. The log events levels, starting with the highest priority level, are standard, interaction, trace, debug and all.

- **all** All log events (that is, log events of the Standard, Trace,Interaction, and Debug levels) are generated.
- **debug** The same as all.
- **trace** Log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels) are generated, but log events of the Debug level are not generated.
- **interaction** Log events of the Interaction level and higher (that is, log events of the Standard and Interaction levels) are generated, but log events of the Trace and Debug levels are not generated.
- **standard** Log events of the Standard level are generated, but log events of the Interaction, Trace, and Debug levels are not generated.
- **none** No log evenets are generated.

monitor Section

- optionsofflineresp
- sip.enable_dns_cache
- sip.localuser
- sip.logmsg.allowed
- sip.logmsg.maskoption
- sip.mtusize
- sip.preferred_ipversion
- sip.proxy.optionsinterval
- sip.proxy.release-recordingclient-session-on-fail
- sip.proxy.release-recordingserver-session-on-fail
- sip.proxy.releaseconfonfailure
- sip.proxy.unavailoptionsinterval
- sip.route.default.tcp
- sip.route.default.tcp.ipv6
- sip.route.default.tls
- sip.route.default.tls.ipv6
- sip.route.default.udp
- sip.route.default.udp.ipv6
- sip.tcp.portrange
- sip.tls.portrange
- sip.transport.0
- sip.transport.0.tos
- sip.transport.1
- sip.transport.1.tos
- sip.transport.2
- sip.transport.2.tos
- sip.transport.dnsharouting
- sip.transport.localaddress
- sip.transport.localaddress_ipv6
- sip.transport.localaddress.srv
- sip.transport.routefailovertime
- sip.transport.routerecoverytime
- sip.transport.setuptimer.tcp
- sip.transport.unavailablewakeup

optionsofflineresp

Default Value: 503
Valid Values:
Changes Take Effect: At start/restart

List of semi-colon separated SIP-OPTIONS response codes >=300 which can be used to mark a resource offline. If the response code received is not present in the list, then the resource will be considered online. Default is 503 which is the shutdown response code for OPTIONS by MCP

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

SIP user presented in OPTIONS requests. The specified text will be presented in the "From:" field of the form sip:user@host[:port]

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.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.optionsinterval

Default Value: 2000
Valid Values:
Changes Take Effect: After restart

Specified in milliseconds, this is the interval by which RM sends OPTIONS message to a healthy resource to determine if the resource is alive

sip.proxy.release-recordingclient-session-on-fail

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

Can be true of false. If true is specified and the resource that handles the Recording Client session went offline, then all associated Recording Client session calls are released and the new coming calls will be routed to the next available Recording Client resource. If false is specified, new calls that are joining the Recording Client session will receive an error until the Recording Client session is released, when the session timer expires.

sip.proxy.release-recordingserver-session-on-fail

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

Can be true of false. If true is specified and the resource that handles the Recording Server session went offline, then all associated Recording Server session calls are released and the new coming calls will be routed to the next available Recording Server resource. If false is specified, new calls that are joining the Recording Server session will receive an error until the Recording Server session is released, when the session timer expires.

sip.proxy.releaseconfonfailure

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

Can be true of false. If true is specified and the resource that handles the conference went offline, then all associated conference sessions are released and the new coming calls will be routed to the next available conference resource. If false is specified, new calls that are joining the conference will receive an error until the conference is released, when the session timer expires.

sip.proxy.unavailoptionsinterval

Default Value: 5000
Valid Values:
Changes Take Effect: After restart

Specified in milliseconds, this is the interval by which RM sends OPTIONS message to a dead resource to determine if the resource has become alive

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.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.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:5064
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:5064
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:5065 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.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 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.

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 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.

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).

mrcpv2pxy Section

default-resource-port-capacity

Default Value: 500
Valid Values:
Changes Take Effect: After restart

This parameter specifies the port capacity assigned to each Physical Resources, if they are not defined. Default value is 500.

enable_dns_cache

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

Specifies if MRCPv2Pxy should enable or disable the use of DNS cache for MRCPv2Pxy's application layer DNS resolutions. These resolutions are used to identify the source resource from where the SIP request is received. Enabling DNS cache increases MRCPv2Pxy's resilience towards network issues between MRCPv2Pxy 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

enable_mrcpv2_proxy

Default Value: 0
Valid Values:

Changes Take Effect: After restart

Determines whether this process should act as MRCPv2Proxy. Behaves as MRCPv2Proxy if set to 1; otherwise it behaves as Resource Manager

fips_enabled

Default Value: false
Valid Values: true, false
Changes Take Effect: After restart

Specifies whether to enable FIPS mode in MRCPv2Pxy. When FIPS mode is enabled, only FIPS 140-2 approved ciphers and algorithms can be used in SSL connections.

options_response_contenttype

Default Value: application/text
Valid Values:
Changes Take Effect: After restart

If rm.options_response_msg_body is defined, this string is returned by the MRCPv2Pxy as the "Content-type" header in the SIP response message.

options_response_msg_body

Default Value: v=0%0D%0Am=application 9 TCP/MRCPv2 1%0D%0Aa=resource:mrcpv2proxy%0D%0A
Valid Values:
Changes Take Effect: After restart

If defined, when the MRCPv2Pxy returns a response to a SIP OPTIONS message, this string is returned by the MRCPv2Pxy as the SIP response message body. Any hex-encoded characters in the string will first be decoded before being used. For example, string with multiple lines can be specified by: First Line%0D%0ASecond Line. This will result in %0D and %0A replaced by '\r' and '\n' respectively.

options-errresp-on-noresources

Default Value: true
Valid Values: true, false
Changes Take Effect: After restart

This parameter when set to true,MRCPv2Pxy sends error response to SIP OPTIONS when it detects all GVP resources are offline.

resolve-addr-for-aor-match

Default Value: false
Valid Values: true, false
Changes Take Effect: After restart

When this parameter when set to true, MRCPv2Pxy resolves hostname/FQDN for matching incoming resource AOR with configured resource AORs. Otherwise a direct string matching is performed.

resource-no-match-respcode

Default Value: 480
Valid Values:
Changes Take Effect: After restart

Expects parameter value of the form sipcode;desc or just sipcode.

resource-unavailable-respcode

Default Value: 480
Valid Values:
Changes Take Effect: After restart

Expects parameter value of the form sipcode;desc or just sipcode.

suspend-mode-respcode

Default Value: 503
Valid Values:
Changes Take Effect: After restart

When new session request comes and MRCPv2Pxy is in suspend mode, this SIP response code is returned. Expects parameter value of the form sipcode;desc or just sipcode.

OPM Section

- Transaction_dbid

Transaction_dbid

Default Value:
Valid Values:
Changes Take Effect: immediately

Allows the user to configure the transaction/list object DBID that is referenced during runtime in the context of this profile.

proxy Section

- sip.enable_dns_cache
- sip.localuser
- sip.logmsg.allowed
- sip.logmsg.maskoption
- sip.maxtcpconnections
- sip.maxtlsconnections
- sip.min_se
- sip.mtusize
- sip.preferred_ipversion
- sip.proxy.respaddr
- sip.route.default.tcp
- sip.route.default.tcp.ipv6
- sip.route.default.tls
- sip.route.default.tls.ipv6
- sip.route.default.udp
- sip.route.default.udp.ipv6
- sip.route.dest.0
- sip.route.dests
- sip.sessionexpires
- sip.tcp.portrange
- sip.threadpoolsize
- sip.threads
- sip.timer_C
- sip.timer_C1
- sip.tls.portrange
- sip.transport.0
- sip.transport.0.tos
- sip.transport.1
- sip.transport.1.tos
- sip.transport.2
- sip.transport.2.tos
- sip.transport.alarmtimer
- sip.transport.dnsharouting
- sip.transport.localaddress
- sip.transport.localaddress_ipv6
- sip.transport.localaddress.srv
- sip.transport.routefailovertime
- sip.transport.routerecoverytime
- sip.transport.setuptimer.tcp
- sip.transport.unavailablewakeup
- sip.udprecvbuffersize
- sip.udpsendbuffersize

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.

registrar Section

- sip.enable_dns_cache
- sip.localuser
- sip.logmsg.allowed
- sip.logmsg.maskoption
- sip.preferred_ipversion
- sip.registrar.domain
- sip.registrar.maxexpirytime
- sip.registrar.minexpirytime
- sip.route.default.tcp
- sip.route.default.tcp.ipv6
- sip.route.default.tls
- sip.route.default.tls.ipv6
- sip.route.default.udp
- sip.route.default.udp.ipv6
- sip.tcp.portrange
- sip.tls.portrange
- sip.transport.0
- sip.transport.0.tos
- sip.transport.1
- sip.transport.1.tos
- sip.transport.2
- sip.transport.2.tos
- sip.transport.dnsharouting
- sip.transport.localaddress
- sip.transport.localaddress_ipv6
- sip.transport.localaddress.srv
- sip.transport.routefailovertime
- sip.transport.routerecoverytime
- sip.transport.setuptimer.tcp
- sip.transport.unavailablewakeup

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

SIP user used by registrar in sending requests. The specified text will be presented in the "From:" field of the form sip:user@host[:port]</description>

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.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.registrar.domain

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

A comma-delimited list of domains accepted by this registrar. Only the host part of the strings defined by the domain entry of this configuration and request-uri of the REGISTER request will be compared. If this configuration value has empty value, comparison will be skipped. Otherwise, if a REGISTER request registers with a domain that is not in this list, the request will be rejected with a 404 Not Found.

sip.registrar.maxexpirytime

Default Value: 60
Valid Values:
Changes Take Effect: After restart

Defines the maximum expiry time (in seconds) of this registrar. If the client requests an expiry time longer than this value, this value will be used instead.

sip.registrar.minexpirytime

Default Value: 60
Valid Values:
Changes Take Effect: After restart

Defines the minimum expiry time (in seconds) of this registrar. If the client requests an expiry time less than this value, the request will be rejected with this value in the Min-Expires header.

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.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.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:5062
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:5062
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:5063 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.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 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.

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 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.

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).

rm Section

- conference-cleanup-timer
- conference-sip-error-respcode
- cti-unavailable-action
- cti-unavailable-respcode
- default-resource-port-capacity
- enable_dns_cache
- fips_enabled
- ignore-ruri-tenant-dbid
- options_response_contenttype
- options_response_msg_body
- options-errresp-on-noresources
- pass-capability-params-to-ctic
- pass-tenantid-parameter-to-gateway
- reject-on-geo-location-nomatch
- resolve-addr-for-aor-match
- resource-no-match-respcode
- resource-unavailable-respcode
- rewrite-referto-header
- sip-header-for-cti-dnis
- sip-header-for-dnis
- suspend-mode-respcode
- treat-campaign-as-conference
- voicexml-recording-allowed

conference-cleanup-timer

Default Value:
Valid Values: The value must be an integer
Changes Take Effect: After restart

If no calls are associated to the conference within the specified interval (in milliseconds), then the conference object will be cleared.

conference-sip-error-respcode

Default Value: 480
Valid Values:
Changes Take Effect: After restart

When conference call fails due to reaching maximum conference size, this SIP response code will be returned to the caller. Expects parameter value of the form sipcode;desc or just sipcode. Example - 480 or 480;Conference Capacity reached

cti-unavailable-action

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

On the initial INVITE, if CTI-C sends a specific 4xx/5xx SIP response code matching any of the codes specified in "cti-unavailable-respcode", then RM will assume that the CTI Server connectivity is broken. In that case RM will check this parameter "cti-unavailable-action", and if it is set RM will perform the action specified in this parameter. The possible values are: "answer", "reject", or "script;<service-type>;<url>"

cti-unavailable-respcode

Default Value: 404
Valid Values:
Changes Take Effect: After restart

On the initial INVITE, if CTI-C sends a specific 4xx/5xx SIP response code that matches any of the response codes specified in this parameter then RM will assume that the CTI Server connectivity is broken and it should not retry another CTI-C instance. Expects parameter value of the form sipcode1;sipcode2 etc.

default-resource-port-capacity

Default Value: 500
Valid Values:
Changes Take Effect: After restart

This parameter specifies the port capacity assigned to each Physical Resources, if they are not defined. Default value is 500.

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 for RM's application layer DNS resolutions. These resolutions are used to identify the source resource from where the SIP request is received; for ex: to identify gateway resource if VIA header contains FQDN instead of IP address 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

fips_enabled

Default Value: false
Valid Values: true, false
Changes Take Effect: After restart

Specifies whether to enable FIPS mode in RM. When FIPS mode is enabled, only FIPS 140-2 approved ciphers and algorithms can be used in SSL connections.

ignore-ruri-tenant-dbid

Default Value: false
Valid Values: true, false
Changes Take Effect: After restart

When this flag is set to true, RM will not use the tenant-dbid parameter received through the incoming INVITE RURI for identifying the tenant (incase of MSML calls).

options_response_contenttype

Default Value: application/text
Valid Values:
Changes Take Effect: After restart

If rm.options_response_msg_body is defined, this string is returned by the RM as the "Content-type" header in the SIP response message.

options_response_msg_body

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

If defined, when the RM returns a response to a SIP OPTIONS message, this string is returned by the RM as the SIP response message body. Any hex-encoded characters in the string will first be decoded before being used. For example, string with multiple lines can be specified by: First Line%0D%0ASecond Line. This will result in %0D and %0A replaced by '\r' and '\n' respectively.

options-errresp-on-noresources

Default Value: true
Valid Values: true, false
Changes Take Effect: After restart

This parameter when set to true,RM sends error response to SIP OPTIONS when it detects all GVP resources are offline.

pass-capability-params-to-ctic

Default Value: true
Valid Values: true, false
Changes Take Effect: After restart

When this parameter set to true and the target is CTI Connector, RM passes the capability parameters (specified by "gvp.rm.resource-req" prefix) in the request to CTI connector. Note that for any other type of resource, those parameters are not passed.

pass-tenantid-parameter-to-gateway

Default Value: true
Valid Values: true, false
Changes Take Effect: After restart

When this parameter is set to false, RM will not pass the tenant-id RURI parameter (specified by gvp-tenant-id) in the request to Gateway or external SIP service. Otherwise,RM will pass the tenant-id RURI parameter in the request to Gateway or external SIP service.

reject-on-geo-location-nomatch

Default Value: recordingclient,recordingserver
Valid Values:
Changes Take Effect: immediately

This parameter can be specified comma separated service type strings. RM rejects the request for non-matching geo-location while selecting LRGs for specified services.

resolve-addr-for-aor-match

Default Value: false
Valid Values: true, false
Changes Take Effect: After restart

When this parameter is set to true, RM resolves hostname/FQDN for matching incoming resource AOR with configured resource AORs. Otherwise a direct string matching is performed. Please note that it is important to set the port in SIPServer option sip-address-srv along with FQDN - <FQDN>:<Port>. Otherwise a mismatching of AORs might occur which could lead to RM not recognizing the gateway resource

resource-no-match-respcode

Default Value: 480
Valid Values:
Changes Take Effect: After restart

Expects parameter value of the form sipcode;desc or just sipcode.

resource-unavailable-respcode

Default Value: 480
Valid Values:
Changes Take Effect: After restart

Expects parameter value of the form sipcode;desc or just sipcode.

rewrite-referto-header

Default Value: true
Valid Values: true, false
Changes Take Effect: After restart

When this parameter set to true, RM rewrite host port in Refer-To header with request-uri's in Mid-dialog SIP REFER.

sip-header-for-cti-dnis

Default Value: request-uri
Valid Values: request-uri, to, history-info
Changes Take Effect: immediately

This parameter indicates which header the RM should retrieve the DNIS from(if P_Called_Party_ID header is not present), for the purpose of identifying an IVRProfile when the request is coming from CTI Connector

sip-header-for-dnis

Default Value: history-info
Valid Values: request-uri, to, history-info
Changes Take Effect: immediately

This parameter indicates the header the RM should retrieve the DNIS from(if P_Called_Party_ID header is not present), for the purpose of identifying an IVRProfile

suspend-mode-respcode

Default Value: 503
Valid Values:
Changes Take Effect: After restart

When new session request comes and RM is in suspend mode, this SIP response code is returned. Expects parameter value of the form sipcode;desc or just sipcode.

treat-campaign-as-conference

Default Value: true
Valid Values: true, false
Changes Take Effect: After restart

When this parameter set to true, RM routes MSML request with campaign id (like OCS campaign) as conference request.

voicexml-recording-allowed

Default Value: true
Valid Values: true, false
Changes Take Effect: After restart

When this parameter set to true, RM looks up a recording IVR profile provided that the relevant tenant policy parameters also allow the same. If set to false, this overrides the policy setting and does not do recording IVR profile mapping

snmp Section

- timeout

timeout

Default Value: 100
Valid Values: The parameter must be an integer value greater than zero.
Changes Take Effect: At start/restart

The maximum amount of time that SNMP can wait for a new task. This value is specified in milliseconds.

subscription Section

- notify-all-mcp-status
- notify-interval
- sip.enable_dns_cache
- sip.localuser
- sip.logmsg.allowed
- sip.logmsg.maskoption
- sip.mtusize
- sip.preferred_ipversion
- sip.route.default.tcp
- sip.route.default.tcp.ipv6
- sip.route.default.tls
- sip.route.default.tls.ipv6
- sip.route.default.udp
- sip.route.default.udp.ipv6
- sip.tcp.portrange
- sip.tls.portrange
- sip.transport.0
- sip.transport.0.tos
- sip.transport.1
- sip.transport.1.tos
- sip.transport.2
- sip.transport.2.tos
- sip.transport.dnsharouting
- sip.transport.localaddress
- sip.transport.localaddress_ipv6
- sip.transport.localaddress.srv
- sip.transport.routefailovertime
- sip.transport.routerecoverytime
- sip.transport.setuptimer.tcp
- sip.transport.unavailablewakeup
- subscription-duration

notify-all-mcp-status

Default Value: true
Valid Values: true, false
Changes Take Effect: After restart

When a resource status changes from online to offline or from offline to online RM will send sip Notify for all active subscriptions. By default, RM will include all the resource's current status in the sip Notify message. Configuring the parameter value to false will only include that particular resource in the sip Notify message.

notify-interval

Default Value: 5000
Valid Values:
Changes Take Effect: After restart

The interval that RM sends out NOTIFY message for the subscriptions. Notification should be time based and can be configured through the parameter subscription.notify-interval. This parameter accepts unsigned integer value including zero and the default is 5(s).

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

SIP user used by subscription in sending requests. The specified text will be presented in the "From:" field of the form sip:user@host[:port]</description>

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.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.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.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.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:5066
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:5066
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:5067 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.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 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.

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 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.

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).

subscription-duration

Default Value: 600
Valid Values:
Changes Take Effect: After restart

The subscription duration for the subscribe requests. If the Expires header is present then the minimum of subscription.subscription-duration and Expires value from the request is used as the subscription duration. However, if the Expires header specifies a value less than the allowed minimum (36) but greater than 0, then Resource Manager should use the allowed minimum (36) as the subscription duration.

Media Control Platform

Options for this component are contained in the following configuration sections:

- asr
- calllog
- callmgr
- conference
- cpa
- email
- ems
- fm
- log
- mpc
- mrcpv2client
- msml
- mtinternal
- mtmpc
- Netann
- remdial
- sessmgr
- sip
- stack
- tts
- vrm
- vrmrecorder
- vxmli

Tip

In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.

Power users: Download a CSV file containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
asr	defaultengine	default	Immediately/session
asr	delay_for_dtmf	250	Immediately
asr	load_once_per_call	1	Immediately/session
asr	log_metrics_to_asr	0	Immediately/session
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
asr	reserve	false	Immediately/session
calllog	directory	$InstallationRoot$/callrec/	Immediately/session
callmgr	enable_sip_response_in_transfer_metric	false	Immediately
callmgr	fips_enabled	false	At start/restart
callmgr	hrtimerresolution	4	At start/restart
callmgr	shutdown_time_limit	0	Immediately
callmgr	silent_shutdown	0	Immediately
callmgr	usehrtimerforregulartimer	false	At start/restart
conference	active_speaker_update_time	2000	At start/restart
conference	callrec_default_type		Immediately/session
conference	confdir	2	At start/restart
conference	gain_control_enabled	true	At start/restart
conference	highest_input	3	At start/restart
conference	initial_gain	0	At start/restart
conference	novideoimage	Genesys_Logo.jpg	Immediately/session
conference	record_chan1source	recorddnsays	Immediately/session
conference	record_chan2source	otherdnsays	Immediately/session
conference	record_otherdnhearstone	1	Immediately/session
conference	record_recorddnhearstone	1	Immediately/session
conference	silence_fill	0	At start/restart
conference	suppress_silence	0	At start/restart
conference	threadedoutputs	false	At start/restart
conference	video_mixer_layouts	1,dual-view|3,quad-view|5,multiple-5x1|6,multiple-3x3|10,multiple-4x4	Immediately/session
conference	video_output_algorithm	confrole	At start/restart
conference	video_output_type	single	Immediately/session
cpa	gateway.events	AMD CPT FAX PVD	Immediately/session
cpa	outbound.method	NONE	Immediately/session
cpa	outbound.native.ignoreconnectevent	false	Immediately/session
cpa	outbound.native.initialstate	preconnect	Immediately/session
email	fromAddr	nobody@example.com	At start/restart
email	smtpAddr	localhost	At start/restart
ems	dc.default.logfilter	0-2|*|*	At start/restart
ems	dc.default.metricsfilter	0-16,18,25,35,36,41,52-55,74,128,136-141	At start/restart
ems	dc.enableSQA	true	At start/restart
ems	dc.servicequality.AudioGapThreshold	2000	At start/restart
ems	dc.servicequality.CallAnswerThreshold	1500	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
ems	dc.servicequality.CallRejectThreshold	2000	At start/restart
ems	dc.servicequality.CumulativeResponse.threshold	2000	At start/restart
ems	dc.servicequality.FirstPromptInbound.threshold	1500	At start/restart
ems	dc.servicequality.FirstPromptOutbound.threshold	1500	At start/restart
ems	dc.servicequality.InboundRejectNetFailureCodes	decline	At start/restart
ems	dc.servicequality.InterPromptThreshold	4000	At start/restart
ems	dc.servicequality.OutboundRejectNetFailureCodes	busy|decline|fax|noanswer|hangup	
ems	logconfig.DATAC	0-2,4|*|*	Immediately
ems	logconfig.MFSINK	*|*|*	Immediately
ems	metricsconfig.DATAC	*	Immediately
ems	metricsconfig.MFSINK	0-16,18-41,43,52-56,72-74,76-81,127-129,130,132,134,135,136-1	Immediately
ems	ors.reportinginterval	60	At start/restart
ems	password		at start/restart
ems	rc.amq_connection_send_timeout	60	At start/restart
ems	rc.batch_size	500	At start/restart
ems	rc.cdr.batch_size	500	At start/restart
ems	rc.cdr.local_queue_max	1000000	At start/restart
ems	rc.cdr.local_queue_path	cdrQueue_mcp.db	At start/restart
ems	rc.cdr.max_throughput	0	At start/restart
ems	rc.certificate		at start/restart
ems	rc.keystore_certificate		at start/restart
ems	rc.keystore_password		at start/restart
ems	rc.local_queue_max	5000000	At start/restart
ems	rc.local_queue_path	reportingClientQueue.db	At start/restart
ems	rc.max_throughput	0	At start/restart
ems	rc.ors.local_queue_max	1000000	At start/restart
ems	rc.ors.local_queue_path	orsQueue_mcp.db	At start/restart
ems	rc.sqa.batch_size	1	At start/restart
ems	rc.sqa.local_queue_max	3000	At start/restart
ems	rc.sqa.local_queue_path	sqaQueue_mcp.db	At start/restart
ems	rc.truststore_certificate		at start/restart
fm	cachemaxentrycount	1000	At start/restart
fm	cachemaxentrysize	20000000	At start/restart
fm	cachemaxsize	200000000	At start/restart
fm	curlconnecttimeout	300	At start/restart
fm	curlredirect	1	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
fm	dns_cache_timeout	60	At start/restart
fm	enable100continue	0	At start/restart
fm	enabletcpkeepalive	1	At start/restart
fm	enabletcpnodelay	1	At start/restart
fm	enableuploadcontentrewind	1	At start/restart
fm	forbid_connection_reuse	0	At start/restart
fm	https_proxy		At start/restart
fm	http_proxy	localhost:3128	At start/restart
fm	interface		At start/restart
fm	localfile_maxage	10	At start/restart
fm	maxredirections	5	At start/restart
fm	no_cache_url_substring	cgi-bin,jsp,asp,?	At start/restart
fm	password		At start/restart
fm	portrange		At start/restart
fm	revalidatestaleresponse	1	At start/restart
fm	sleeptimems	10	At start/restart
fm	ssl_ca_info		At start/restart
fm	ssl_ca_path		At start/restart
fm	ssl_cert		At start/restart
fm	ssl_cert_type	PEM	At start/restart
fm	ssl_cipher_list		At start/restart
fm	ssl_crl_check_enabled	0	At start/restart
fm	ssl_crl_file_path		At start/restart
fm	ssl_key		At start/restart
fm	ssl_key_password		At start/restart
fm	ssl_key_type	PEM	At start/restart
fm	ssl_random_file		At start/restart
fm	ssl_verify_host	0	At start/restart
fm	ssl_verify_peer	0	At start/restart
fm	ssl_version	0	At start/restart
fm	tcpkeepaliveidle	60	At start/restart
fm	tcpkeepaliveinterval	60	At start/restart
log	all	../logs/MCP	Immediately
log	check-point	1	Immediately
log	compatible-output-priority	false	Immediately
log	debug	../logs/MCP	Immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
log	expire	10	Immediately
log	interaction	../logs/MCP	Immediately
log	keep-startup-file	true	After restart
log	mask_sensitive_data	false	Immediately
log	memory		Immediately
log	memory-storage-size		When memory output is created
log	messagefile		Immediately, if an application cannot find its *.lms file at startup
log	message_format	short	Immediately
log	print-attributes	false	Immediately
log	segment	10000	Immediately
log	spool		Immediately
log	standard	../logs/MCP_standard	Immediately
log	time_convert	local	Immediately
log	time_format	ISO8601	Immediately
log	trace	../logs/MCP	Immediately
log	verbose	interaction	Immediately
mpc	alarminterval	900000	At start/restart
mpc	amr.enable_dtx	1	At start/restart
mpc	amr.fmtp	octet-align=0 | octet-align=1	At start/restart
mpc	amr.maxptime	0	Immediately
mpc	amr.preferred_mode	15	Immediately
mpc	amr.ptime	20	Immediately
mpc	amrpayload	105	At start/restart
mpc	amrwb.enable_dtx	1	At start/restart
mpc	amrwb.fmtp	octet-align=0 | octet-align=1	At start/restart
mpc	amrwb.preferred_mode	15	Immediately
mpc	amr_wb.maxptime	0	Immediately
mpc	amr_wb.ptime	20	Immediately
mpc	amr_wbpayload	112	At start/restart
mpc	answerwithonecodec	0	Immediately
mpc	appendrejcodec	0	Immediately/session
mpc	asr.codec	pcmu telephone-event	At start/restart
mpc	asr.preferredipinterface	V4	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
mpc	asr.srtp.cryptomethods	AES_CM_128_HMAC_SHA1_80	At start/restart
mpc	asr.srtp.mode	none	At start/restart
mpc	asr.srtp.sessionparamsoffer	none	At start/restart
mpc	codec	pcmu pcma g722 opus g726 g729 gsm amr amr-wb h263 h263-1998 h264 vp8 telephone-event	Immediately/session
mpc	codecpref	r	Immediately/session
mpc	conference.allowloudestvideoecho	0	Immediately/session
mpc	cpa.busy	na_busy	At start/restart
mpc	cpa.carriermsg.0		Immediately
mpc	cpa.carriermsg.1		Immediately
mpc	cpa.carriermsg.2		Immediately
mpc	cpa.carriermsg.3		Immediately
mpc	cpa.carriermsg.4		Immediately
mpc	cpa.carriermsg.5		Immediately
mpc	cpa.carriermsg.6		Immediately
mpc	cpa.carriermsg.7		Immediately
mpc	cpa.carriermsg.8		Immediately
mpc	cpa.carriermsg.9		Immediately
mpc	cpa.carriermsg.readduration	60	Immediately
mpc	cpa.cm_enable_initial_tone_filter	true	At start/restart
mpc	cpa.cm_initial_silence_suppression_level	64	At start/restart
mpc	cpa.cm_match_percent	80	Immediately/session
mpc	cpa.custom1	none	At start/restart
mpc	cpa.custom2	none	At start/restart
mpc	cpa.custom3	none	At start/restart
mpc	cpa.custom4	none	At start/restart
mpc	cpa.enable_alternate_signals	false	At start/restart
mpc	cpa.enable_carrier_messages	false	Immediately/session
mpc	cpa.enable_log_param	false	At start/restart
mpc	cpa.enable_log_result	true	At start/restart
mpc	cpa.fastbusy	na_fastbusy	At start/restart
mpc	cpa.fax	standard_fax	At start/restart
mpc	cpa.faxdur	160	At start/restart
mpc	cpa.keptdur_before_statechange	0	At start/restart
mpc	cpa.maxbeepdettime	30000	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
mpc	cpa.maxpostconntime	20000	At start/restart
mpc	cpa.maxpreconntime	30000	At start/restart
mpc	cpa.maxrings	0	At start/restart
mpc	cpa.mintime_after_tone	200	At start/restart
mpc	cpa.nframes_cm_detection	50	At start/restart
mpc	cpa.no_ring_result	0	Immediately/session
mpc	cpa.postconnectresult.machine.list		Immediately/session
mpc	cpa.postconnsilduration	1000	Immediately/session
mpc	cpa.postconnsilresult	0	Immediately/session
mpc	cpa.preconnectresult.busy.list		Immediately/session
mpc	cpa.preconnectresult.custom1.list		Immediately/session
mpc	cpa.preconnectresult.custom2.list		Immediately/session
mpc	cpa.preconnectresult.custom3.list		Immediately/session
mpc	cpa.preconnectresult.custom4.list		Immediately/session
mpc	cpa.preconnectresult.fast_busy.list		Immediately/session
mpc	cpa.preconnectresult.sit_nocircuit.list		Immediately/session
mpc	cpa.preconnectresult.sit_operatorintercept.list		Immediately/session
mpc	cpa.preconnectresult.sit_reorder.list		Immediately/session
mpc	cpa.preconnectresult.sit_vacantcircuit.list		Immediately/session
mpc	cpa.preconn_tones_det_mode	0	At start/restart
mpc	cpa.priority_machine_machinegreetingdur	1500	At start/restart
mpc	cpa.priority_machine_maxvoicesigdur	600	At start/restart
mpc	cpa.priority_machine_voicepausedur	1100	At start/restart
mpc	cpa.priority_normal_machinegreetingdur	1800	At start/restart
mpc	cpa.priority_normal_maxvoicesigdur	800	At start/restart
mpc	cpa.priority_normal_voicepausedur	1000	At start/restart
mpc	cpa.priority_voice_machinegreetingdur	2000	At start/restart
mpc	cpa.priority_voice_maxvoicesigdur	1100	At start/restart
mpc	cpa.priority_voice_voicepausedur	850	At start/restart
mpc	cpa.ringback	na_ringback	At start/restart
mpc	cpa.sit_nocircuit	na_sit_nocircuit	At start/restart
mpc	cpa.sit_operatorintercept	na_sit_operatorintercept	At start/restart
mpc	cpa.sit_reorder	na_sit_reorder	At start/restart
mpc	cpa.sit_vacantcircuit	na_sit_vacantcircuit	At start/restart
mpc	cpa.tone1.segment1.f1max	0	At start/restart
mpc	cpa.tone1.segment1.f1min	0	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
mpc	cpa.tone1.segment1.f2max	0	At start/restart
mpc	cpa.tone1.segment1.f2min	0	At start/restart
mpc	cpa.tone1.segment1.offtimemax	0	At start/restart
mpc	cpa.tone1.segment1.offtimemin	0	At start/restart
mpc	cpa.tone1.segment1.ontimemax	20	At start/restart
mpc	cpa.tone1.segment1.ontimemin	20	At start/restart
mpc	cpa.tone1.segment2.f1max	0	At start/restart
mpc	cpa.tone1.segment2.f1min	0	At start/restart
mpc	cpa.tone1.segment2.f2max	0	At start/restart
mpc	cpa.tone1.segment2.f2min	0	At start/restart
mpc	cpa.tone1.segment2.offtimemax	0	At start/restart
mpc	cpa.tone1.segment2.offtimemin	0	At start/restart
mpc	cpa.tone1.segment2.ontimemax	20	At start/restart
mpc	cpa.tone1.segment2.ontimemin	20	At start/restart
mpc	cpa.tone1.segment3.f1max	0	At start/restart
mpc	cpa.tone1.segment3.f1min	0	At start/restart
mpc	cpa.tone1.segment3.f2max	0	At start/restart
mpc	cpa.tone1.segment3.f2min	0	At start/restart
mpc	cpa.tone1.segment3.offtimemax	0	At start/restart
mpc	cpa.tone1.segment3.offtimemin	0	At start/restart
mpc	cpa.tone1.segment3.ontimemax	20	At start/restart
mpc	cpa.tone1.segment3.ontimemin	20	At start/restart
mpc	cpa.tone10.segment1.f1max	0	At start/restart
mpc	cpa.tone10.segment1.f1min	0	At start/restart
mpc	cpa.tone10.segment1.f2max	0	At start/restart
mpc	cpa.tone10.segment1.f2min	0	At start/restart
mpc	cpa.tone10.segment1.offtimemax	0	At start/restart
mpc	cpa.tone10.segment1.offtimemin	0	At start/restart
mpc	cpa.tone10.segment1.ontimemax	20	At start/restart
mpc	cpa.tone10.segment1.ontimemin	20	At start/restart
mpc	cpa.tone10.segment2.f1max	0	At start/restart
mpc	cpa.tone10.segment2.f1min	0	At start/restart
mpc	cpa.tone10.segment2.f2max	0	At start/restart
mpc	cpa.tone10.segment2.f2min	0	At start/restart
mpc	cpa.tone10.segment2.offtimemax	0	At start/restart
mpc	cpa.tone10.segment2.offtimemin	0	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
mpc	cpa.tone10.segment2.ontimemax	20	At start/restart
mpc	cpa.tone10.segment2.ontimemin	20	At start/restart
mpc	cpa.tone10.segment3.f1max	0	At start/restart
mpc	cpa.tone10.segment3.f1min	0	At start/restart
mpc	cpa.tone10.segment3.f2max	0	At start/restart
mpc	cpa.tone10.segment3.f2min	0	At start/restart
mpc	cpa.tone10.segment3.offtimemax	0	At start/restart
mpc	cpa.tone10.segment3.offtimemin	0	At start/restart
mpc	cpa.tone10.segment3.ontimemax	20	At start/restart
mpc	cpa.tone10.segment3.ontimemin	20	At start/restart
mpc	cpa.tone2.segment1.f1max	0	At start/restart
mpc	cpa.tone2.segment1.f1min	0	At start/restart
mpc	cpa.tone2.segment1.f2max	0	At start/restart
mpc	cpa.tone2.segment1.f2min	0	At start/restart
mpc	cpa.tone2.segment1.offtimemax	0	At start/restart
mpc	cpa.tone2.segment1.offtimemin	0	At start/restart
mpc	cpa.tone2.segment1.ontimemax	20	At start/restart
mpc	cpa.tone2.segment1.ontimemin	20	At start/restart
mpc	cpa.tone2.segment2.f1max	0	At start/restart
mpc	cpa.tone2.segment2.f1min	0	At start/restart
mpc	cpa.tone2.segment2.f2max	0	At start/restart
mpc	cpa.tone2.segment2.f2min	0	At start/restart
mpc	cpa.tone2.segment2.offtimemax	0	At start/restart
mpc	cpa.tone2.segment2.offtimemin	0	At start/restart
mpc	cpa.tone2.segment2.ontimemax	20	At start/restart
mpc	cpa.tone2.segment2.ontimemin	20	At start/restart
mpc	cpa.tone2.segment3.f1max	0	At start/restart
mpc	cpa.tone2.segment3.f1min	0	At start/restart
mpc	cpa.tone2.segment3.f2max	0	At start/restart
mpc	cpa.tone2.segment3.f2min	0	At start/restart
mpc	cpa.tone2.segment3.offtimemax	0	At start/restart
mpc	cpa.tone2.segment3.offtimemin	0	At start/restart
mpc	cpa.tone2.segment3.ontimemax	20	At start/restart
mpc	cpa.tone2.segment3.ontimemin	20	At start/restart
mpc	cpa.tone3.segment1.f1max	0	At start/restart
mpc	cpa.tone3.segment1.f1min	0	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
mpc	cpa.tone3.segment1.f2max	0	At start/restart
mpc	cpa.tone3.segment1.f2min	0	At start/restart
mpc	cpa.tone3.segment1.offtimemax	0	At start/restart
mpc	cpa.tone3.segment1.offtimemin	0	At start/restart
mpc	cpa.tone3.segment1.ontimemax	20	At start/restart
mpc	cpa.tone3.segment1.ontimemin	20	At start/restart
mpc	cpa.tone3.segment2.f1max	0	At start/restart
mpc	cpa.tone3.segment2.f1min	0	At start/restart
mpc	cpa.tone3.segment2.f2max	0	At start/restart
mpc	cpa.tone3.segment2.f2min	0	At start/restart
mpc	cpa.tone3.segment2.offtimemax	0	At start/restart
mpc	cpa.tone3.segment2.offtimemin	0	At start/restart
mpc	cpa.tone3.segment2.ontimemax	20	At start/restart
mpc	cpa.tone3.segment2.ontimemin	20	At start/restart
mpc	cpa.tone3.segment3.f1max	0	At start/restart
mpc	cpa.tone3.segment3.f1min	0	At start/restart
mpc	cpa.tone3.segment3.f2max	0	At start/restart
mpc	cpa.tone3.segment3.f2min	0	At start/restart
mpc	cpa.tone3.segment3.offtimemax	0	At start/restart
mpc	cpa.tone3.segment3.offtimemin	0	At start/restart
mpc	cpa.tone3.segment3.ontimemax	20	At start/restart
mpc	cpa.tone3.segment3.ontimemin	20	At start/restart
mpc	cpa.tone4.segment1.f1max	0	At start/restart
mpc	cpa.tone4.segment1.f1min	0	At start/restart
mpc	cpa.tone4.segment1.f2max	0	At start/restart
mpc	cpa.tone4.segment1.f2min	0	At start/restart
mpc	cpa.tone4.segment1.offtimemax	0	At start/restart
mpc	cpa.tone4.segment1.offtimemin	0	At start/restart
mpc	cpa.tone4.segment1.ontimemax	20	At start/restart
mpc	cpa.tone4.segment1.ontimemin	20	At start/restart
mpc	cpa.tone4.segment2.f1max	0	At start/restart
mpc	cpa.tone4.segment2.f1min	0	At start/restart
mpc	cpa.tone4.segment2.f2max	0	At start/restart
mpc	cpa.tone4.segment2.f2min	0	At start/restart
mpc	cpa.tone4.segment2.offtimemax	0	At start/restart
mpc	cpa.tone4.segment2.offtimemin	0	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
mpc	cpa.tone4.segment2.ontimemax	20	At start/restart
mpc	cpa.tone4.segment2.ontimemin	20	At start/restart
mpc	cpa.tone4.segment3.f1max	0	At start/restart
mpc	cpa.tone4.segment3.f1min	0	At start/restart
mpc	cpa.tone4.segment3.f2max	0	At start/restart
mpc	cpa.tone4.segment3.f2min	0	At start/restart
mpc	cpa.tone4.segment3.offtimemax	0	At start/restart
mpc	cpa.tone4.segment3.offtimemin	0	At start/restart
mpc	cpa.tone4.segment3.ontimemax	20	At start/restart
mpc	cpa.tone4.segment3.ontimemin	20	At start/restart
mpc	cpa.tone5.segment1.f1max	0	At start/restart
mpc	cpa.tone5.segment1.f1min	0	At start/restart
mpc	cpa.tone5.segment1.f2max	0	At start/restart
mpc	cpa.tone5.segment1.f2min	0	At start/restart
mpc	cpa.tone5.segment1.offtimemax	0	At start/restart
mpc	cpa.tone5.segment1.offtimemin	0	At start/restart
mpc	cpa.tone5.segment1.ontimemax	20	At start/restart
mpc	cpa.tone5.segment1.ontimemin	20	At start/restart
mpc	cpa.tone5.segment2.f1max	0	At start/restart
mpc	cpa.tone5.segment2.f1min	0	At start/restart
mpc	cpa.tone5.segment2.f2max	0	At start/restart
mpc	cpa.tone5.segment2.f2min	0	At start/restart
mpc	cpa.tone5.segment2.offtimemax	0	At start/restart
mpc	cpa.tone5.segment2.offtimemin	0	At start/restart
mpc	cpa.tone5.segment2.ontimemax	20	At start/restart
mpc	cpa.tone5.segment2.ontimemin	20	At start/restart
mpc	cpa.tone5.segment3.f1max	0	At start/restart
mpc	cpa.tone5.segment3.f1min	0	At start/restart
mpc	cpa.tone5.segment3.f2max	0	At start/restart
mpc	cpa.tone5.segment3.f2min	0	At start/restart
mpc	cpa.tone5.segment3.offtimemax	0	At start/restart
mpc	cpa.tone5.segment3.offtimemin	0	At start/restart
mpc	cpa.tone5.segment3.ontimemax	20	At start/restart
mpc	cpa.tone5.segment3.ontimemin	20	At start/restart
mpc	cpa.tone6.segment1.f1max	0	At start/restart
mpc	cpa.tone6.segment1.f1min	0	At start/restart
Section	Option	Default	Changes Take Effect

Section	Option	Default	Changes Take Effect
mpc	cpa.tone6.segment1.f2max	0	At start/restart
mpc	cpa.tone6.segment1.f2min	0	At start/restart
mpc	cpa.tone6.segment1.offtimemax	0	At start/restart
mpc	cpa.tone6.segment1.offtimemin	0	At start/restart
mpc	cpa.tone6.segment1.ontimemax	20	At start/restart
mpc	cpa.tone6.segment1.ontimemin	20	At start/restart
mpc	cpa.tone6.segment2.f1max	0	At start/restart
mpc	cpa.tone6.segment2.f1min	0	At start/restart
mpc	cpa.tone6.segment2.f2max	0	At start/restart
mpc	cpa.tone6.segment2.f2min	0	At start/restart
mpc	cpa.tone6.segment2.offtimemax	0	At start/restart
mpc	cpa.tone6.segment2.offtimemin	0	At start/restart
mpc	cpa.tone6.segment2.ontimemax	20	At start/restart
mpc	cpa.tone6.segment2.ontimemin	20	At start/restart
mpc	cpa.tone6.segment3.f1max	0	At start/restart
mpc	cpa.tone6.segment3.f1min	0	At start/restart
mpc	cpa.tone6.segment3.f2max	0	At start/restart
mpc	cpa.tone6.segment3.f2min	0	At start/restart
mpc	cpa.tone6.segment3.offtimemax	0	At start/restart
mpc	cpa.tone6.segment3.offtimemin	0	At start/restart
mpc	cpa.tone6.segment3.ontimemax	20	At start/restart
mpc	cpa.tone6.segment3.ontimemin	20	At start/restart
mpc	cpa.tone7.segment1.f1max	0	At start/restart
mpc	cpa.tone7.segment1.f1min	0	At start/restart
mpc	cpa.tone7.segment1.f2max	0	At start/restart
mpc	cpa.tone7.segment1.f2min	0	At start/restart
mpc	cpa.tone7.segment1.offtimemax	0	At start/restart
mpc	cpa.tone7.segment1.offtimemin	0	At start/restart
mpc	cpa.tone7.segment1.ontimemax	20	At start/restart
mpc	cpa.tone7.segment1.ontimemin	20	At start/restart
mpc	cpa.tone7.segment2.f1max	0	At start/restart
mpc	cpa.tone7.segment2.f1min	0	At start/restart
mpc	cpa.tone7.segment2.f2max	0	At start/restart
mpc	cpa.tone7.segment2.f2min	0	At start/restart
mpc	cpa.tone7.segment2.offtimemax	0	At start/restart
mpc	cpa.tone7.segment2.offtimemin	0	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
mpc	cpa.tone7.segment2.ontimemax	20	At start/restart
mpc	cpa.tone7.segment2.ontimemin	20	At start/restart
mpc	cpa.tone7.segment3.f1max	0	At start/restart
mpc	cpa.tone7.segment3.f1min	0	At start/restart
mpc	cpa.tone7.segment3.f2max	0	At start/restart
mpc	cpa.tone7.segment3.f2min	0	At start/restart
mpc	cpa.tone7.segment3.offtimemax	0	At start/restart
mpc	cpa.tone7.segment3.offtimemin	0	At start/restart
mpc	cpa.tone7.segment3.ontimemax	20	At start/restart
mpc	cpa.tone7.segment3.ontimemin	20	At start/restart
mpc	cpa.tone8.segment1.f1max	0	At start/restart
mpc	cpa.tone8.segment1.f1min	0	At start/restart
mpc	cpa.tone8.segment1.f2max	0	At start/restart
mpc	cpa.tone8.segment1.f2min	0	At start/restart
mpc	cpa.tone8.segment1.offtimemax	0	At start/restart
mpc	cpa.tone8.segment1.offtimemin	0	At start/restart
mpc	cpa.tone8.segment1.ontimemax	20	At start/restart
mpc	cpa.tone8.segment1.ontimemin	20	At start/restart
mpc	cpa.tone8.segment2.f1max	0	At start/restart
mpc	cpa.tone8.segment2.f1min	0	At start/restart
mpc	cpa.tone8.segment2.f2max	0	At start/restart
mpc	cpa.tone8.segment2.f2min	0	At start/restart
mpc	cpa.tone8.segment2.offtimemax	0	At start/restart
mpc	cpa.tone8.segment2.offtimemin	0	At start/restart
mpc	cpa.tone8.segment2.ontimemax	20	At start/restart
mpc	cpa.tone8.segment2.ontimemin	20	At start/restart
mpc	cpa.tone8.segment3.f1max	0	At start/restart
mpc	cpa.tone8.segment3.f1min	0	At start/restart
mpc	cpa.tone8.segment3.f2max	0	At start/restart
mpc	cpa.tone8.segment3.f2min	0	At start/restart
mpc	cpa.tone8.segment3.offtimemax	0	At start/restart
mpc	cpa.tone8.segment3.offtimemin	0	At start/restart
mpc	cpa.tone8.segment3.ontimemax	20	At start/restart
mpc	cpa.tone8.segment3.ontimemin	20	At start/restart
mpc	cpa.tone9.segment1.f1max	0	At start/restart
mpc	cpa.tone9.segment1.f1min	0	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
mpc	cpa.tone9.segment1.f2max	0	At start/restart
mpc	cpa.tone9.segment1.f2min	0	At start/restart
mpc	cpa.tone9.segment1.offtimemax	0	At start/restart
mpc	cpa.tone9.segment1.offtimemin	0	At start/restart
mpc	cpa.tone9.segment1.ontimemax	20	At start/restart
mpc	cpa.tone9.segment1.ontimemin	20	At start/restart
mpc	cpa.tone9.segment2.f1max	0	At start/restart
mpc	cpa.tone9.segment2.f1min	0	At start/restart
mpc	cpa.tone9.segment2.f2max	0	At start/restart
mpc	cpa.tone9.segment2.f2min	0	At start/restart
mpc	cpa.tone9.segment2.offtimemax	20	At start/restart
mpc	cpa.tone9.segment2.offtimemin	0	At start/restart
mpc	cpa.tone9.segment2.ontimemax	20	At start/restart
mpc	cpa.tone9.segment2.ontimemin	20	At start/restart
mpc	cpa.tone9.segment3.f1max	0	At start/restart
mpc	cpa.tone9.segment3.f1min	0	At start/restart
mpc	cpa.tone9.segment3.f2max	0	At start/restart
mpc	cpa.tone9.segment3.f2min	0	At start/restart
mpc	cpa.tone9.segment3.offtimemax	0	At start/restart
mpc	cpa.tone9.segment3.offtimemin	0	At start/restart
mpc	cpa.tone9.segment3.ontimemax	20	At start/restart
mpc	cpa.tone9.segment3.ontimemin	20	At start/restart
mpc	cpa.voice_level_db	17.5	At start/restart
mpc	cpa.voice_range_db	25	At start/restart
mpc	ctrleventpoollowthreshold	50	At start/restart
mpc	ctrleventpoolthreshold	75	At start/restart
mpc	default_audio_format	ULAW	At start/restart
mpc	dsp.g726littleendian	0	Immediately/session
mpc	dsp.g729a	0	Immediately
mpc	dtmf.detectedge	0	At start/restart
mpc	dtmf.duration	200	At start/restart
mpc	dtmf.gap	100	At start/restart
mpc	dtmf.inband_amplitude	15000	At start/restart
mpc	dtmf.maxsilence	20	At start/restart
mpc	dtmf.minduration	0	At start/restart
mpc	dtmf.multidtmfonetimestamp	0	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
mpc	dtmf.pauseduration	200	At start/restart
mpc	dtmf.singlepacket	0	At start/restart
mpc	fcr.defaultdtmfhandling	as-is	Immediately/session
mpc	fcr.gain	0	At start/restart
mpc	font_paths_linux	/usr/share/fonts/default/ ghostscript	At start/restart
mpc	font_paths_win	C:/Windows/Fonts	At start/restart
mpc	g722.maxptime	0	Immediately
mpc	g722.ptime	0	Immediately
mpc	g726_32.maxptime	0	Immediately
mpc	g726_32.ptime	0	Immediately
mpc	g729.fmtp		At start/restart
mpc	g729.maxptime	0	Immediately
mpc	g729.ptime	0	Immediately
mpc	gsm.maxptime	0	immediately
mpc	gsm.ptime	0	immediately
mpc	h263.fmtp		At start/restart
mpc	h263_1998payload	99	At start/restart
mpc	h264.fmtp	profile=b; level=3.1; packetization-mode=*;|profile=cb; level=3.1; packetization-mode=*;|profile=m; level=3.1; packetization-mode=*;	At start/restart
mpc	h264.in_band_param_sets_only	0	At start/restart
mpc	h264payload	113	At start/restart
mpc	health.maxprocessingtime	600000	At start/restart
mpc	health.waittime	0	At start/restart
mpc	includeavpfinsdp	none	Immediately/session
mpc	maxmediathreads	16	At start/restart
mpc	maxrecordencryptedfilesize	120000000	At start/restart
mpc	maxrecordfilesize	0	Immediately/session
mpc	media.senddtmfdropaudio	1	At start/restart
mpc	mediamgr.audiobuffersize	102400	At start/restart
mpc	mediamgr.autorecordformatselect	1	At start/restart
mpc	mediamgr.CA_directory		Immediately/session
mpc	mediamgr.CA_file		Immediately/session
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
mpc	mediamgr.enableEODdoublecheck	1	At start/restart
mpc	mediamgr.h263overrideTR	1	At start/restart
mpc	mediamgr.hlsconsecutiveerrorsthreshold	5	Immediately
mpc	mediamgr.hlstotalerrorsthreshold	20	Immediately
mpc	mediamgr.ignore_cert_err	1	Immediately/session
mpc	mediamgr.isofilerecordheadersize	55000	At start/restart
mpc	mediamgr.maxcertificatecachesize	2000000	At start/restart
mpc	mediamgr.maxcertificatelength	5000	At start/restart
mpc	mediamgr.maxcertificatesperprofile	10	At start/restart
mpc	mediamgr.precacheprofileforcallrecording.0		At start/restart
mpc	mediamgr.precacheprofileforcallrecording.1		At start/restart
mpc	mediamgr.precacheprofileforcallrecording.2		At start/restart
mpc	mediamgr.precacheprofileforcallrecording.3		At start/restart
mpc	mediamgr.precacheprofileforcallrecording.4		At start/restart
mpc	mediamgr.precacheprofileforcallrecording.5		At start/restart
mpc	mediamgr.recordmp3audiobuffer	4000	At start/restart
mpc	mediamgr.recordrtphinttrack	0	At start/restart
mpc	mediamgr.recordwritetimeinterval	1000	At start/restart
mpc	mediamgr.rec_iframe_delay_threshold	160	At start/restart
mpc	mediamgr.rtsplowerbufferthreshold	100	At start/restart
mpc	mediamgr.rtsppause	1	At start/restart
mpc	mediamgr.rtspplayrange	1	At start/restart
mpc	mediamgr.rtspupperbufferthreshold	200	At start/restart
mpc	mediamgr.sharedhttpservers		At start/restart
mpc	mediamgr.strictsamplingrate	0	At start/restart
mpc	mediamgr.videobuffersize	256000	At start/restart
mpc	mediamgr.videofillingframeduration	1000	At start/restart
mpc	mediamgr.videofillingthreshold	2000	At start/restart
mpc	mixer.audiodelay_flush_all_threshold	500	At start/restart
mpc	mixer.audiodelay_flush_silence_threshold	100	At start/restart
mpc	mp3.bitrate	16	Immediately/session
mpc	mp3.compression_level_current_encoder	7	Immediately/session
mpc	mp3.interfrequency.encoding		At start/restart
mpc	mp3.samplingrate	32	Immediately/session
mpc	mp3.use_current_encoder	false	Immediately/session
mpc	mp3.use_integer_transcoder	false	Immediately/session
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
mpc	mp3.use_integer_transcoder_current_encoder	true	Immediately/session
mpc	numdispatchthreads	1	At start/restart
mpc	opus.apptype	voice	Immediately/session
mpc	opus.bitrate	0	Immediately/session
mpc	opus.complexity	10	Immediately/session
mpc	opus.fmtp	useinbandfec=1	At start/restart
mpc	opus.packetloss	20	Immediately/session
mpc	opuspayload	116	At start/restart
mpc	pcma.maxptime	0	Immediately
mpc	pcma.ptime	0	Immediately
mpc	pcmu.maxptime	0	Immediately
mpc	pcmu.ptime	0	Immediately
mpc	persistdympayfmtpair	1	Immediately
mpc	playcache.checkversiontime	300	Immediately/session
mpc	playcache.directory	$installationRoot$/cache/play	At start/restart
mpc	playcache.enable	1	Immediately/session
mpc	playcache.expiretime	24:00	At start/restart
mpc	playcache.maxsize	500	At start/restart
mpc	playremoteeodtimeout	10000	At start/restart
mpc	playremoteflushtimeout	10000	At start/restart
mpc	playsilencefill	160	At start/restart
mpc	preferredipinterface	V4	Immediately
mpc	record.allowsyncdiskwrite	0	Immediately/session
mpc	record.defaultdtmfhandling	as-is	Immediately/session
mpc	recordcachedir	$installationRoot$/cache/record	At start/restart
mpc	recordnumparallelpost	30	At start/restart
mpc	recordpostbacklogthreshold	25	At start/restart
mpc	recordpostinterval	15000	At start/restart
mpc	recordpostretrybackoff	120000	At start/restart
mpc	recordpostretrycount	3	At start/restart
mpc	refframereqonconnjoin	true	Immediately/session
mpc	rru.beginsilence	1000	At start/restart
mpc	rru.endsilence	3000	At start/restart
mpc	rtcp.tos	0	Immediately/session
mpc	rtcp.tos.video	0	Immediately/session
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
mpc	rtcpfeedback.audio	allow	Immediately/session
mpc	rtcpfeedback.video	allow	Immediately/session
mpc	rtp.activetimeout	0	At start/restart
mpc	rtp.audiobuffersize	50000	At start/restart
mpc	rtp.dejitter.delay	0	At start/restart
mpc	rtp.dejitter.timeout	200	At start/restart
mpc	rtp.dtmf.crlfenable	false	Immediately/session
mpc	rtp.dtmf.receive	SIPINFO INBAND	Immediately/session
mpc	rtp.dtmf.send	INBAND	Immediately/session
mpc	rtp.enablertcp	1	At start/restart
mpc	rtp.fixedsocketthreads	8	At start/restart
mpc	rtp.h264allowrfc3984stapa	1	At start/restart
mpc	rtp.inputmode	vad	At start/restart
mpc	rtp.localaddr	$LocalIP$	At start/restart
mpc	rtp.localaddrv6		At start/restart
mpc	rtp.maxrtppacketsize	0	At start/restart
mpc	rtp.multichantimeout	60000	At start/restart
mpc	rtp.overwritessrcandtimestamp	1	At start/restart
mpc	rtp.packetseq	0	At start/restart
mpc	rtp.portrange	20000-45000	At start/restart
mpc	rtp.prefilltime	200	At start/restart
mpc	rtp.request_iframe	1	Immediately/session
mpc	rtp.restrictsource	0	At start/restart
mpc	rtp.rfc2429maxpacketsize	1400	At start/restart
mpc	rtp.sendmode	vad	At start/restart
mpc	rtp.senduponrecv	0	At start/restart
mpc	rtp.source_buffer_video_data_size	0	Immediately/session
mpc	rtp.source_buffer_video_size	500	Immediately/session
mpc	rtp.statisticsinterval	300000	At start/restart
mpc	rtp.timeout	60000	At start/restart
mpc	rtp.tos	0	Immediately/session
mpc	rtp.tos.video	0	Immediately/session
mpc	rtp.video.udprecvbuffersize	60480	At start/restart
mpc	rtp.video.udpsendbuffersize	60480	At start/restart
mpc	rtp.videobuffersize	0	At start/restart
mpc	rtp.vp8maxpacketsize	1400	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
mpc	rtsp.connection.portrange	14000-15999	
mpc	rtsp.localaddr		At start/restart
mpc	rtsp.localaddrv6		At start/restart
mpc	rtsp.rtp.localaddr		At start/restart
mpc	rtsp.rtp.localaddrv6		At start/restart
mpc	rtsp.rtp.portrange		At start/restart
mpc	sdp.audiobandwidth		At start/restart
mpc	sdp.connection		At start/restart
mpc	sdp.map.origin.0		At start/restart
mpc	sdp.map.origin.0.confgain	100	At start/restart
mpc	sdp.map.origin.0.dtmftype	INBAND	At start/restart
mpc	sdp.map.origin.1		At start/restart
mpc	sdp.map.origin.1.confgain	100	At start/restart
mpc	sdp.map.origin.1.dtmftype	INBAND	At start/restart
mpc	sdp.map.origin.2		At start/restart
mpc	sdp.map.origin.2.confgain	100	At start/restart
mpc	sdp.map.origin.2.dtmftype	INBAND	At start/restart
mpc	sdp.map.origin.3		At start/restart
mpc	sdp.map.origin.3.confgain	100	At start/restart
mpc	sdp.map.origin.3.dtmftype	INBAND	At start/restart
mpc	sdp.map.origin.4		At start/restart
mpc	sdp.map.origin.4.confgain	100	At start/restart
mpc	sdp.map.origin.4.dtmftype	INBAND	At start/restart
mpc	sdp.map.origin.5		At start/restart
mpc	sdp.map.origin.5.confgain	100	At start/restart
mpc	sdp.map.origin.5.dtmftype	INBAND	At start/restart
mpc	sdp.map.origin.6		At start/restart
mpc	sdp.map.origin.6.confgain	100	At start/restart
mpc	sdp.map.origin.6.dtmftype	INBAND	At start/restart
mpc	sdp.map.origin.7		At start/restart
mpc	sdp.map.origin.7.confgain	100	At start/restart
mpc	sdp.map.origin.7.dtmftype	INBAND	At start/restart
mpc	sdp.map.origin.8		At start/restart
mpc	sdp.map.origin.8.confgain	100	At start/restart
mpc	sdp.map.origin.8.dtmftype	INBAND	At start/restart
mpc	sdp.map.origin.9		At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
mpc	sdp.map.origin.9.confgain	100	At start/restart
mpc	sdp.map.origin.9.dtmftype	INBAND	At start/restart
mpc	sdp.videobandwidth		At start/restart
mpc	srtp.cryptomethods	AES_CM_128_HMAC_SHA1_80	At start/restart
mpc	srtp.maxerror	5	At start/restart
mpc	srtp.mode	none	At start/restart
mpc	srtp.sessionparams	UNENCRYPTED_SRTP UNENCRYPTED_SRTCP UNAUTHENTICATED_SRTP	At start/restart
mpc	srtp.sessionparamsoffer		At start/restart
mpc	telephone_event.maxptime	0	Immediately
mpc	telephone_event.ptime	0	Immediately
mpc	telephone_eventpayload	101	At start/restart
mpc	tfcipayload	96	At start/restart
mpc	tiasfraction	100	At start/restart
mpc	transcoders	G722 GSM G726 G729 AMR AMR-WB MP3 OPUS H263 H264 VP8	At start/restart
mpc	transmitmultiplecodec	0	Immediately/session
mpc	tts.appendrejcodec	0	At start/restart
mpc	tts.codec	pcmu	Immediately
mpc	tts.preferredipinterface	V4	At start/restart
mpc	tts.srtp.cryptomethods	AES_CM_128_HMAC_SHA1_80	At start/restart
mpc	tts.srtp.mode	none	At start/restart
mpc	tts.srtp.sessionparamsoffer		At start/restart
mpc	validatemediatimers	1	At start/restart
mpc	videotranscoder.bitratecheckdelay	10000	At start/restart
mpc	videotranscoder.bitratechecktolerance	50	At start/restart
mpc	videotranscoder.checkbitrate	1	Immediately/session
mpc	videotranscoder.checkframerate	1	Immediately/session
mpc	videotranscoder.frameratechecktolerance	50	At start/restart
mpc	videotranscoder.h264.keyframeidrinterval	1	At start/restart
mpc	videotranscoder.h264.keyframeinterval	50	At start/restart
mpc	videotranscoder.h264.resolutions	SQCIF QCIF QVGA CIF VGA 4CIF SVGA 720P	At start/restart
mpc	videotranscoder.maxbitrate	500000	Immediately/session
mpc	videotranscoder.statsresetthreshold	60000	At start/restart
mpc	voipmetrics.enable	0	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
mpc	vp8.adaptive	true	At start/restart
mpc	vp8.defaultbitrate	0	At start/restart
mpc	vp8.defaultframerateden	1001	At start/restart
mpc	vp8.defaultframeratenum	30000	At start/restart
mpc	vp8.defaultresolution	CIF	At start/restart
mpc	vp8.maxkeyframeinterval	15	Immediately/session
mpc	vrmrecorder.codec	pcmu pcma g722 opus g726 g729 gsm amr amr-wb h263 h263-1998 h264 vp8 telephone-event	At start/restart
mpc	vrmrecorder.enable	true	At start/restart
mpc	vrmrecorder.preferredipinterface	V4	Immediately
mpc	vrmrecorder.srtp.cryptomethods	AES_CM_128_HMAC_SHA1_80	At start/restart
mpc	vrmrecorder.srtp.mode	none	At start/restart
mpc	vrmrecorder.srtp.sessionparamsoffer		At start/restart
mpc	widebandconferences	0	At start/restart
mrcpv2client	sip.transport.0	transport0 udp:any:7080	At start/restart
mrcpv2client	sip.transport.1	transport1 tcp:any:7080	At start/restart
mrcpv2client	sip.transport.2	transport2 tls:any:7081 type=TLSv1	At start/restart
mrcpv2client	sip.transport.localaddress		At start/restart
mrcpv2client	sip.transport.localaddress.srv	false	At start/restart
msml	beep.filename	file://$InstallationRoot$/audio/ulaw/default_audio/endofprompt.vox	Immediately
msml	beep.join.timelimit	5000	Immediately
msml	callrecording.dtmfhandling	as-is	Immediately/session
msml	clampdtmf.postsilencepackets	0	Immediately/session
msml	clampdtmf.presilencepackets	0	Immediately/session
msml	conference.participantjointimeout	120000	Immediately/session
msml	conference.passthrough_enabled	true	Immediately/session
msml	cpd.beeptimeout	30	Immediately
msml	cpd.postconnecttimeout	30	Immediately
msml	cpd.preconnecttimeout	30	Immediately
msml	cpd.record.basepath	file://$installationRoot$/record/	Immediately
msml	cpd.record.fileext	wav	Immediately
msml	defaultaudioext	.wav	Immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
msml	dialogend.silentfail	false	Immediately
msml	info.contenttypes	application/ vnd.radisys.msml+xml	Immediately
msml	play.basepath	file://$installationRoot$	Immediately
msml	play.fetchtimeout	25000	Immediately/session
msml	play.h263videoformat	QCIF=2	Immediately
msml	play.h264videoformat	0a=2,0b=2,0c=2,0d=2,14=2,15=2,16=2,1e=2	Immediately
msml	play.musicbasepath	file://$installationRoot$	Immediately
msml	play.preferredvideocontainer	avi	Immediately/session
msml	play.usedefaultsearchorder	true	Immediately
msml	record.amazonallowpublicaccess	false	Immediately/session
msml	record.amazonpostmode	http	Immediately/session
msml	record.amazonsignatureversion	V4	Immediately/session
msml	record.amazonsignedpayload	false	Immediately/session
msml	record.appenduniqueid	true	Immediately/session
msml	record.basepath	file://$installationRoot$	Immediately
msml	record.channels	2	Immediately/session
msml	record.channels2	2	Immediately/session
msml	record.deferredsink	true	Immediately
msml	record.filenametemplate	id	Immediately
msml	record.finalsilence	4	Immediately
msml	record.generatehash	false	Immediately/session
msml	record.irrecoverablerecordpostdir	$installationRoot$/cache/ record/failed	Immediately
msml	record.posttimeout	120000	Immediately/session
msml	record.updateheader	false	Immediately
msml	record.userecordcachedir	false	Immediately
mtinternal	enablertcp	0	At start/restart
mtinternal	max_concurrent_savedata	-1	At start/restart
mtinternal	receive_max_size	-1	At start/restart
mtinternal	receive_min_size	-1	At start/restart
mtinternal	receive_rate_alarm	500	At start/restart
mtinternal	receive_savedata		At start/restart
mtinternal	restrictsource	0	At start/restart
mtinternal	rtp.statisticsinterval	600000	At start/restart
mtinternal	transmit_max_size	160	At start/restart
mtinternal	transmit_min_size	160	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
mtinternal	transmit_rate	10	At start/restart
mtinternal	transmit_rate_alarm	500	At start/restart
mtinternal	transmit_savedata		At start/restart
mtmpc	conference.output_gain	100	At start/restart
Netann	annc.audiodefaultrepeat	forever	Immediately
Netann	annc.basepath	$installationRoot$	At start/restart
Netann	annc.defaultaudioext	.wav	Immediately
Netann	annc.fetchtimeout	25000	Immediately/session
Netann	annc.h263videoformat	QCIF=2	Immediately
Netann	annc.h264videoformat	0a=2,0b=2,0c=2,0d=2,14=2,15=2,16=2,1e=2	Immediately
Netann	annc.musicbasepath	$installationRoot$	Immediately
Netann	conference.recordmode	mixed	Immediately
Netann	record.appenduniqueid	true	Immediately/session
Netann	record.basepath	$InstallationRoot$/record	At start/restart
Netann	record.maxrecordsilence	0	Immediately
Netann	record.maxrecordtime	0	Immediately
Netann	sipinfonotifydtmf	Auto	At start/restart
remdial	maxcalls	500	At start/restart
remdial	maxclientsockets	64	At start/restart
remdial	port	6999	At start/restart
remdial	telnetmode	RAW	At start/restart
sessmgr	acceptcalltimeout	30000	At start/restart
sessmgr	alert_before_fetch	0	At start/restart
sessmgr	appmodules_linux	Remdial:RemoteDial Netann:Netann VXML3:VXML-NG MSML:MSML	At start/restart
sessmgr	appmodules_win	Remdial:RemoteDial Netann:Netann VXML3:VXML-NG MSML:MSML	At start/restart
sessmgr	default_init_url	file://$InstallationRoot$/samples/ulaw/helloworld.vxml	At start/restart
sessmgr	default_vxml_interpreter	VXML-NG	At start/restart
sessmgr	disconnect_cause.badfetch	17	At start/restart
sessmgr	disconnect_cause.decline	21	At start/restart
sessmgr	fcr_video_dir	IN	Immediately
sessmgr	init_accept_call_mode	DUPLEX	At start/restart
sessmgr	join_fallback	0	Immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
sessmgr	licensepoolsize.gvp_ports	max	At start/restart
sessmgr	licensepoolsize.gvp_tts_ports	max	At start/restart
sessmgr	maxincalltime	0	Immediately
sessmgr	mediaswitch_on_alert	0	Immediately
sessmgr	modules_linux	Remdial Netann VXML3 MSML	At start/restart
sessmgr	modules_win	Remdial Netann VXML3 MSML	At start/restart
sessmgr	mrt.sendsdpininvite	true	Immediately/session
sessmgr	MSML.MSML	msml	At start/restart
sessmgr	Netann.Netann	Netann	At start/restart
sessmgr	Remdial.RemoteDial	RemoteDial	At start/restart
sessmgr	VXML3.VXML-NG	vxmli-ng1	At start/restart
sip	attconfnetworktonetimeout	1000	At start/restart
sip	call_rate	0	At start/restart
sip	call_rate_period	0	At start/restart
sip	copyunknownheaders	1	At start/restart
sip	copyxgenesysheaders		At start/restart
sip	defaultblindxfer	REFER	At start/restart
sip	defaultbridgexfer	BRIDGE	At start/restart
sip	defaultconsultxfer	REFERJOIN	At start/restart
sip	defaultfrom		At start/restart
sip	defaultgw		At start/restart
sip	defaulthost		At start/restart
sip	deferoutalerting	0	At start/restart
sip	dnis_correlationid_length	0	At start/restart
sip	dnis_correlationid_offset	0	At start/restart
sip	dtmf.crlfenable	false	Immediately/session
sip	enablemaddr	true	At start/restart
sip	enablesendrecvevents	true	Immediately/session
sip	enabletfci	0	At start/restart
sip	enable_dns_cache	false	At start/restart
sip	handlesessionrefreshsdp	matchfull	Immediately/session
sip	hfdisctimer	5000	At start/restart
sip	hfprefix	!	At start/restart
sip	hfstopdial	!	At start/restart
sip	hftype	0	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
sip	in.bye.headers	Reason	At start/restart
sip	in.info.headers	*	At start/restart
sip	in.invite.headers	*	At start/restart
sip	in.invite.params	RequestURI	At start/restart
sip	info.contenttype	application/text	At start/restart
sip	localuser	Genesys	At start/restart
sip	logmsg.allowed	true	At start/restart
sip	logmsg.maskoption	0	At start/restart
sip	maxtcpaccepts	100	At start/restart
sip	maxtcpconnections	100	At start/restart
sip	maxtlsaccepts	100	At start/restart
sip	maxtlsconnections	100	At start/restart
sip	min_se	90	At start/restart
sip	mpc.copyheaders	X-Genesys-geo-location	At start/restart
sip	mtusize	1500	At start/restart
sip	out.info.headers	*	At start/restart
sip	out.invite.headers	*	At start/restart
sip	out.invite.params	RequestURI	At start/restart
sip	out.refer.headers	*	At start/restart
sip	out.refer.params	RequestURI	At start/restart
sip	outcalluseoriggw	1	At start/restart
sip	p-alcatel-csbu	fb=notransfer;dtmf_auto=dr	Immediately/session
sip	passertedidentity	1	Immediately/session
sip	pcalledpartyid	1	Immediately/session
sip	prack.support	0	At start/restart
sip	preferred_ipversion	ipv4	At start/restart
sip	referredby		At start/restart
sip	referxferhold	0	At start/restart
sip	referxfertryoutbound	0	At start/restart
sip	referxferwaitbye	0	At start/restart
sip	referxferwaitnotify	1	At start/restart
sip	registerexpiryadjustment	10	At start/restart
sip	registration		At start/restart
sip	route.default.tcp		At start/restart
sip	route.default.tls		At start/restart
sip	route.default.udp		At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
sip	route.dest.0		At start/restart
sip	route.dest.1		At start/restart
sip	route.dest.2		At start/restart
sip	route.dest.3		At start/restart
sip	route.dest.4		At start/restart
sip	route.dest.5		At start/restart
sip	routeset		At start/restart
sip	sdpansinprov	1	Immediately/session
sip	sdpwarningheaders	0	Immediately/session
sip	securerouteset		At start/restart
sip	sendalert	1	Immediately/session
sip	sessionexpires	1800	At start/restart
sip	sipinfoallowedcontenttypes		At start/restart
sip	tcp.portrange		At start/restart
sip	threadpoolsize	4	At start/restart
sip	threads	0	After restart
sip	timer.ci_proceeding	120000	At start/restart
sip	timer.provretransmit	60000	At start/restart
sip	timer_si	32000	At start/restart
sip	tls.portrange		At start/restart
sip	transfermethods	HKF REFER REFERJOIN MEDIAREDIRECT ATTCOURTESY ATTCONSULT ATTCONFERENCE ATTOOBCOURTESY ATTOOBCONSULT ATTOOBCONFERENCE NEC61ISDN	At start/restart
sip	transport.0	transport0 udp:any:5070	At start/restart
sip	transport.0.tos	0	At start/restart
sip	transport.1	transport1 tcp:any:5070	At start/restart
sip	transport.1.tos	0	At start/restart
sip	transport.2	transport2 tls:any:5071 cert=$InstallationRoot$/config/x509_certificate.pem key=$InstallationRoot$/config/x509_private_key.pem	At start/restart
sip	transport.2.tos	0	At start/restart
sip	transport.3		At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
sip	transport.3.tos	0	At start/restart
sip	transport.4		At start/restart
sip	transport.4.tos	0	At start/restart
sip	transport.5		At start/restart
sip	transport.5.tos	0	At start/restart
sip	transport.dnsharouting	false	At start/restart
sip	transport.localaddress		At start/restart
sip	transport.localaddress.srv	false	At start/restart
sip	transport.localaddress_ipv6		At start/restart
sip	transport.routefailovertime	5	At start/restart
sip	transport.routerecoverytime	30	At start/restart
sip	transport.setuptimer.tcp	30000	At start/restart
sip	transport.staticroutelist		At start/restart
sip	transport.unavailablewakeup	true	At start/restart
sip	userouteonrecording	true	Immediately/session
sip	voipmetrics.localhost	sip:$LocalIP$:5070	At start/restart
sip	voipmetrics.registration		At start/restart
sip	voipmetrics.remoteserver		At start/restart
sip	voipmetrics.routeset		At start/restart
sip	vxmlinvite	1	At start/restart
sip	warningheaders	0	Immediately/session
sip	xfer.copyheaders	*	Immediately
stack	connection.portrange	10000-11999	
stack	connection.timeout	10000	
stack	trace.debug	true	
tts	defaultengine	default	Immediately/session
tts	reserve	false	Immediately/session
vrm	client.dtmf.abnf_encoding_check	content	
vrm	client.dtmf.fetchtimeout	10000	
vrm	client.dtmf.maxage	-1	
vrm	client.dtmf.maxloopcount	1000	
vrm	client.dtmf.maxstale	-1	
vrm	client.grpc.credential		
vrm	client.grpc.init_worker_threads	5	At start/restart
vrm	client.grpc.init_worker_threads.tts	5	At start/restart
vrm	client.grpc.max_worker_threads	200	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
vrm	client.grpc.max_worker_threads.tts	350	At start/restart
vrm	client.grpc.sslroots	$InstallationRoot$/config/grpc_roots.pem	
vrm	client.grpc.timeout	10000	At start/restart
vrm	client.modules	MRCPV1 MRCPV2 MRCP_DTMFRECOGNIZER	
vrm	client.mrcpv1.sendtrapformrcprecogcompletioncause	004-006,009,010	Immediately
vrm	client.mrcpv1.sendtrapformrcprequestfailure		Immediately
vrm	client.mrcpv1.sendtrapformrcpresponsecode	405,407	Immediately
vrm	client.mrcpv1.sendtrapformrcpresponsefailure	MRCP-DEFINE-GRAMMAR MRCP-RECOGNIZE MRCP-SPEAK	Immediately
vrm	client.mrcpv1.sendtrapformrcpspeakcompletioncause	002,005	Immediately
vrm	client.mrcpv1.sendtrapforrtspresponsecode	405,454,500	Immediately
vrm	client.mrcpv2.earlynomatch	true	
vrm	client.mrcpv2.localaddr		At start/restart
vrm	client.mrcpv2.maxopensockets	256	
vrm	client.mrcpv2.portrange	12000-13999	
vrm	client.mrcpv2.prefix	mrcpv2client	
vrm	client.mrcpv2.proxy	false	At start/restart
vrm	client.mrcpv2.sendtrapformrcprecogcompletioncause	004-006,009,010,012,016	Immediately
vrm	client.mrcpv2.sendtrapformrcprequestfailure		Immediately
vrm	client.mrcpv2.sendtrapformrcpresponsecode	405,407	Immediately
vrm	client.mrcpv2.sendtrapformrcpresponsefailure	MRCP-DEFINE-GRAMMAR MRCP-RECOGNIZE MRCP-SPEAK	Immediately
vrm	client.mrcpv2.sendtrapformrcpspeakcompletioncause	002,005	Immediately
vrm	client.mrcpv2.sendtrapforsipresponsecode	400-513	Immediately
vrm	client.timeout	10000	
vrm	client.universals.uri	builtin:grammar/universals	
vrm	rtp.localaddr	$LocalIP$	At start/restart
vrm	rtp.localaddrv6		At start/restart
vrm	rtp.portrange	45536-65535	At start/restart
vrm	rtsp.localaddr	$LocalIP$	At start/restart
vrmrecorder	sip.localport	7090	At start/restart
vrmrecorder	sip.localsecureport	7091	At start/restart
vrmrecorder	sip.preferred_ipversion	ipv4	At start/restart
vrmrecorder	sip.routeset		At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
vrmrecorder	sip.secureroutеset		At start/restart
vrmrecorder	sip.transport.0	transport0 udp:any:7090	At start/restart
vrmrecorder	sip.transport.1	transport1 tcp:any:7090	At start/restart
vrmrecorder	sip.transport.2	transport2 tls:any:7091 TLSv1_2	At start/restart
vrmrecorder	sip.transport.dnsharouting	false	At start/restart
vrmrecorder	sip.transport.localaddress		At start/restart
vrmrecorder	sip.transport.localaddress.srv	false	At start/restart
vrmrecorder	sip.transport.localaddress_ipv6		At start/restart
vrmrecorder	sip.transport.staticroutelist		At start/restart
vrmrecorder	sip.transport.unavailablewakeup	true	At start/restart
vrmrecorder	toheadermode	toparams	Immediately/session
vrmrecorder	websocket.asio_worker_threads	3	At start/restart
vrmrecorder	websocket.buffer_size	200	Immediately
vrmrecorder	websocket.ssl_ca_file		Immediately
vrmrecorder	websocket.ssl_ca_path		Immediately
vrmrecorder	websocket.ssl_cert		Immediately
vrmrecorder	websocket.ssl_key		Immediately
vrmrecorder	websocket.ssl_verify_peer	0	Immediately
vrmrecorder	websocket.streaming_percentage	100	Immediately
vxmli	ac.allow_if_missing	true	At start/restart
vxmli	ac.allow_if_nomatch	false	At start/restart
vxmli	ac.enabled	true	At start/restart
vxmli	ac.use_platform_host_for_file_url	true	At start/restart
vxmli	asr.release_on_transfer	true	Immediately
vxmli	beep.uri	file://$InstallationRoot$/audio/ulaw/default_audio/endofprompt.vox	At start/restart
vxmli	break.strength.medium	500	At start/restart
vxmli	break.strength.strong	1000	At start/restart
vxmli	break.strength.weak	200	At start/restart
vxmli	break.strength.x-strong	2000	At start/restart
vxmli	break.strength.x-weak	50	At start/restart
vxmli	builtin_path	$InstallationRoot$/audio/ulaw/	At start/restart
vxmli	cache.document.max_count	50	At start/restart
vxmli	cache.document.max_entry_size	100000	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
vxmli	cache.document.max_size	1000000	At start/restart
vxmli	compiled_script_cache.enable	false	At start/restart
vxmli	compiled_script_cache.max_cached_scripts_count	10000	At start/restart
vxmli	compiled_script_cache.max_cached_script_size	100000	At start/restart
vxmli	compiled_script_cache.max_cache_size	2000000	At start/restart
vxmli	compiled_script_cache.min_cached_script_size	200	At start/restart
vxmli	conformance.disable_application_lastresult_extensions	false	At start/restart
vxmli	conformance.disallow_exec_content_within_prompts	false	At start/restart
vxmli	conformance.rfc5552_bye_reason	true	At start/restart
vxmli	conformance.strict_complete_timeout	true	
vxmli	conformance.strict_grammar_mode	false	At start/restart
vxmli	conformance.strict_tts_mode	false	At start/restart
vxmli	conformance.supported_builtin_dtmf	boolean digits currency date number phone time	At start/restart
vxmli	conformance.supported_builtin_voice	boolean digits currency date number phone time universals/Cancel universals/Exit universals/Help	At start/restart
vxmli	conformance.supported_grammar_languages	en-US	At start/restart
vxmli	conformance.supported_tts_languages	en-US	At start/restart
vxmli	consultationtransfer.result	true	At start/restart
vxmli	data.use_xerces_dom_parser	false	At start/restart
vxmli	data.xmlscript_path	$InstallationRoot$/script/	At start/restart
vxmli	debug.enabled	false	At start/restart
vxmli	debug.server.ip	default	At start/restart
vxmli	debug.server.port	27666	At start/restart
vxmli	debug.server.port.public	27666	At start/restart
vxmli	debug.server.tlscert	$InstallationRoot$/config/x509_certificate.pem	At start/restart
vxmli	debug.server.tlskey	$InstallationRoot$/config/x509_private_key.pem	At start/restart
vxmli	debug.server.tlspassword		At start/restart
vxmli	debug.server.tlsport	27668	At start/restart
vxmli	debug.server.tlsport.public	27668	At start/restart
vxmli	default.alternate_uri		At start/restart
vxmli	default.connecttimeout	30000	At start/restart
vxmli	default.xmllang	en-US	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
vxmli	defaults_vxml_url	file://$InstallationRoot$/config/defaults-ng.vxml	At start/restart
vxmli	detailed_fetch_error.enable	false	At start/restart
vxmli	directories.save_tempfiles	$InstallationRoot$/tmp/	At start/restart
vxmli	expose.nlsml.dom	false	At start/restart
vxmli	getinfo_pairs		Immediately
vxmli	grammar.builtin:dtmf/currency	dtmf/currency.grxml	At start/restart
vxmli	grammar.builtin:dtmf/date	dtmf/date.grxml	At start/restart
vxmli	grammar.builtin:dtmf/number	dtmf/number.grxml	At start/restart
vxmli	grammar.builtin:dtmf/phone	dtmf/phone.grxml	At start/restart
vxmli	grammar.builtin:dtmf/time	dtmf/time.grxml	At start/restart
vxmli	grammar.builtin_basepath_linux		At start/restart
vxmli	grammar.builtin_basepath_win		At start/restart
vxmli	grammar.builtin_baseurl		At start/restart
vxmli	grammar.mimetypes	application/srgs+xml|.grxml|application/srgs|.srgs|Media-Type|.grammar|application/x-abnf|.abnf	At start/restart
vxmli	grammars.cache_size	50000	At start/restart
vxmli	http.accept		At start/restart
vxmli	http.user_agent	NGi/$VERSION$	At start/restart
vxmli	http.version	1.1	At start/restart
vxmli	initial_request_enctype	application/x-www-form-urlencoded	At start/restart
vxmli	initial_request_fetchtimeout	30000	At start/restart
vxmli	initial_request_maxage	-1	At start/restart
vxmli	initial_request_maxstale	-1	At start/restart
vxmli	initial_request_method	GET	At start/restart
vxmli	inlinegrammar_by_url	false	At start/restart
vxmli	jsruntime_size	64	At start/restart
vxmli	jsstack_size	16384	At start/restart
vxmli	legacy.simple_dtmf_grammars	false	
vxmli	local.webserver.basepath_linux		At start/restart
vxmli	local.webserver.basepath_win		At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
vxmli	local.webserver.baseurl		At start/restart
vxmli	logdir	$InstallationRoot$/logs/	At start/restart
vxmli	maintainer.email_subject	Message from GVP to Application Maintainer	At start/restart
vxmli	maintainer.enabled	false	Immediately
vxmli	maintainer.log_message.on_error	true	At start/restart
vxmli	max_application_logfile_size	524288000	At start/restart
vxmli	max_loop_count	1000	At start/restart
vxmli	max_num_documents	5000	At start/restart
vxmli	max_num_sessions	10000	At start/restart
vxmli	max_runtime_error	1000	At start/restart
vxmli	max_scripturl_length	16384	At start/restart
vxmli	max_script_time	2000	At start/restart
vxmli	max_size.script_file	0	At start/restart
vxmli	max_size.vxml_page	0	At start/restart
vxmli	max_size.xml_data	0	At start/restart
vxmli	max_subdialog_depth	50	At start/restart
vxmli	messaging.enabled	true	
vxmli	num_session_processing_threads	8	At start/restart
vxmli	oem_namespace	http://www.genesyslab.com/2006/vxml21-extension http://www.voicegenie.com/2006/vxml21-extension	At start/restart
vxmli	performjsgc_on_subdialogreturn	false	At start/restart
vxmli	recording.basepath	$InstallationRoot$/record	At start/restart
vxmli	recordutterance.path	$InstallationRoot$/utterance	At start/restart
vxmli	savetmpfiles.max_bytes	100000000	At start/restart
vxmli	script_max_loop	1000000	At start/restart
vxmli	session_vars	session.connection.local.uri|LOCALURI|1|session.connection.remote	At start/restart
vxmli	tmpdir	$InstallationRoot$/tmp/	At start/restart
vxmli	transfer.allowed	true	At start/restart
vxmli	tts.defaultengine	default	Immediately
vxmli	universals.cancel	builtin:grammar/universals/Cancel	At start/restart
vxmli	universals.exit	builtin:grammar/universals/Exit	At start/restart
vxmli	universals.help	builtin:grammar/universals/Help	At start/restart
vxmli	universals_path_linux		At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
vxmli	universals_path_win		At start/restart
vxmli	userdata.convert_name_to_lowercase	false	Immediately/session
vxmli	userdata.prefix	X-Genesys-	At start/restart
vxmli	use_isdn_mapping	0	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

mtinternal Section

- enablertcp
- max_concurrent_savedata
- receive_max_size
- receive_min_size
- receive_rate_alarm
- receive_savedata
- restrictsource
- rtp.statisticsinterval
- transmit_max_size
- transmit_min_size
- transmit_rate
- transmit_rate_alarm
- transmit_savedata

enablertcp

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

Specifies whether to transmit RTCP packets.

max_concurrent_savedata

Default Value: -1
Valid Values: mtinternal.max_concurrent_savedata must be an integer that is greater or equal to -1 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

If specified as an integer n, and mtinternal.transmit_savedata or mtinternal.receive_savedata is enabled, then only a maximum of n concurrent files will be open for writing data. Default value is -1, which would place no limit.

receive_max_size

Default Value: -1
Valid Values: mtinternal.receive_max_size must be an integer that is greater or equal to -1 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

Defines the maximum packet sample size that will be notified to the receiver. Note that this number is applied to all codecs with fixed frame size. It will be rounded down to the nearest multiple of the codec frame size. This parameter will be disabled when variable frame size codec is used. Set to -1 to disable the limit.

receive_min_size

Default Value: -1
Valid Values: mtinternal.receive_min_size must be an integer that is greater or equal to -1 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

Defines the minimum packet sample size that will be notified to the receiver. Note that this number is applied to all codecs with fixed frame size. It will be rounded down to the nearest multiple of the codec frame size. This parameter will be disabled when variable frame size codec is used. Set to -1 to disable the limit.

receive_rate_alarm

Default Value: 500
Valid Values: mtinternal.receive_rate_alarm 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

If greater than 0, minor alarm is generated if the transmission rate of incoming packets is slower the real time by the specified delay in milliseconds. This alarm will be disabled if variable frame size codec is used for received packets.

receive_savedata

Default Value:
Valid Values: mtinternal.receive_savedata must be a valid path
Changes Take Effect: At start/restart

If specified, received data is saved under the directory.

restrictsource

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

Specifies whether to allow dropping packets from other sources (filtering).

rtp.statisticsinterval

Default Value: 600000
Valid Values: Possible values are integers from 0 to 3600000 inclusive.
Changes Take Effect: At start/restart

Specifies the interval (in ms) at which statistics logging in the RTP layer will be logged. Setting this value to 0 will disable the statistics logging. If enabled, will log when an RTP connection is destroyed, regardless of interval.

transmit_max_size

Default Value: 160
Valid Values: mtinternal.transmit_max_size must be an integer that is greater or equal to -1 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

Defines the maximum data size in bytes that can be sent. Note that this number is applied to all codecs with fixed frame size. It will be rounded down to the nearest multiple of the codec frame size. This parameter will be disabled when variable frame size codec is used. Set to -1 to disable the limit.

transmit_min_size

Default Value: 160
Valid Values: mtinternal.transmit_min_size must be an integer that is greater or equal to -1 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

Defines the minimum data size in bytes that can be sent. Note that this number is applied to all codecs with fixed frame size. It will be rounded down to the nearest multiple of the codec frame size. This parameter will be disabled when variable frame size codec is used. Set to -1 to disable the limit.

transmit_rate

Default Value: 10
Valid Values: The maximum transmission rate 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

Specifies the transmission rate limit as a multiple of realtime. A value of 1 means realtime, 2 means 2 times realtime and so on. Set to 0 for no limit.

transmit_rate_alarm

Default Value: 500
Valid Values: mtinternal.transmit_rate_alarm 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

If greater than 0, minor alarm is generated if the transmission rate of outgoing packets is slower the real time by the specified delay in milliseconds. This alarm will be disabled if variable frame size codec is used for transmitted packets.

transmit_savedata

Default Value:
Valid Values: mtinternal.transmit_savedata must be a valid path
Changes Take Effect: At start/restart

If specified, utterance is saved under the directory.

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 bypass-resource-list 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.securerouteset=<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

asr Section

defaultengine

Default Value: default
Valid Values: The engine name must be a string.
Changes Take Effect: Immediately/session

The engine specified here will be used to load a default engine when using the log metrics to ASR configuration. An application using a different name should override this using the Request URI configuration or asrengine property.

delay_for_dtmf

Default Value: 250
Valid Values: asr.delay_for_dtmf should 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: Immediately

The amount of delay, in milliseconds, for starting the next ASR recognition after the last DTMF input from the previous field.

load_once_per_call

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

When this parameter is set to Enable, there will be only one VRM session for the entire call which could have multiple recognition sessions. If the parameter value is set to Disable, a VRM session is opened for each recognition request. The VRM session is closed when the recognition request is completed successfully or unsuccessfully (such as no match). As a result, there could be multiple VRM sessions in a call. Having multiple VRM sessions in a call could make the ASR server license

usage more efficient. However, this configuration could have the following consequences:
1. There will be longer delays on speech barge in.
2. The save utterance data could be deleted by some recognizer servers after each VRM session. In that case, the VoiceXML application cannot refer to the saved utterance file after the recognition session.
Note: for ASR engines such as Google Speech-to-Text that need to open a VRM session for each recognition request, this option will be diasbled automatically.

log_metrics_to_asr

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

This parameter is only for ScanSoft Open Speech Recognizer. When set to Enable the MCP will log certain call metrics including Call Starts and Call Ends to the OSR server for the purposes of tuning

reserve

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

When set to true, the MCP will attempt to reserve an ASR resource prior to accepting the call. This resource will be available until an explicit release of the resource, or until the end of the call. The call will be rejected if the resource is not successfully reserved.

calllog Section

- directory

directory

Default Value: $InstallationRoot$/callrec/
Valid Values: Path to the full call recording directory
Changes Take Effect: Immediately/session

Specifies the default full call recording file path if it is not specified in the VXML page.

callmgr Section

- enable_sip_response_in_transfer_metric
- fips_enabled
- hrtimerresolution
- shutdown_time_limit
- silent_shutdown
- usehrtimerforregulartimer

enable_sip_response_in_transfer_metric

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

Specifies whether or not the SIP response code is appended in the transfer_result metrics. In case the SIP response code is not available and this parameter is enabled, 'N/A' is appended in the metrics.

fips_enabled

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

Specifies whether to enable FIPS mode in MCP. When FIPS mode is enabled, only FIPS 140-2 approved ciphers and algorithms can be used in SSL connections.

hrtimerresolution

Default Value: 4
Valid Values: A valid resolution should be an integer from 1 to 20 inclusive
Changes Take Effect: At start/restart

Sets the resolution of the high resolution system timer in msec.

shutdown_time_limit

Default Value: 0

Valid Values: An integer greater or equal to 0.
Changes Take Effect: Immediately

Max time in minutes MCP will wait to upload all reporting data and/or recorded files. Setting this parameter to 0 disables the waiting and MCP will shutdown even with reporting data and/or recoded files still to be uploaded (default).

silent_shutdown

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

Specifies whether or not to shutdown silently, i.e. no core or logs during shutdown. This parameter works only on Linux.

usehrtimerforregulartimer

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

Specifies whether or not the high resolution timer should be used for all timers. This is a Windows only configuration. Enabling this configuration will improve the regularity of media transmissions from a conference, but overall capacity of the MCP will be affected.

conference Section

- active_speaker_update_time
- callrec_default_type
- confdir
- gain_control_enabled
- highest_input
- initial_gain
- novideoimage
- record_chan1source
- record_chan2source
- record_otherdnhearstone
- record_recorddnhearstone
- silence_fill
- suppress_silence
- threadedoutputs
- video_mixer_layouts
- video_output_algorithm
- video_output_type

active_speaker_update_time

Default Value: 2000
Valid Values: conference.active_speaker_update_time must 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

The conference active speaker is updated periodically to the currently loudest input. The input with the highest average audio level during the update period is selected as the loudest. This parameter sets the time period (in msec) for this function. The default value is 2000.

callrec_default_type

Default Value:
Valid Values: Please specify a valid audio codec.
Changes Take Effect: Immediately/session

The default recording type for MSML conference recording. Example formats: audio/wav, audio/wav;codec=ulaw, audio/mp3 . If left empty, the MCP will use wave file with the default platform codec.

confdir

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

Default conference direction of the participant. 0 - Talk only 1 - Listen only 2 - Duplex

gain_control_enabled

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

When gain control is enabled, various configurations used to set gain levels will be respected fully. When gain control is disabled, gains of 0 will result in muted streams, while gains greater than 0, will result in streams that remain at their current level.

highest_input

Default Value: 3
Valid Values: The number must 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

This value will determined the number of highest inputs used for mixing output. If 0 is set, all inputs will be used. This parameter applies to both MSML and NETANN conferences. However, if MSML defines its own highest-input value through 'n-loudest' parameter, it will replace your set value in conference.highest_input parameter.

initial_gain

Default Value: 0
Valid Values: The number must 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

Gain in db when talking to the conference.

novideoimage

Default Value: Genesys_Logo.jpg
Valid Values: Please specify a valid path to an image file, check description for further details.
Changes Take Effect: Immediately/session

Specifies the jpeg file to use for the image to be displayed in video mixed conferences for participants that do not provide video input. Setting this parameter to blank will disable the no video image feature. This parameter is only active when the conference.video_output_type parameter is set to "mixed".

The file must be in the installation root video directory or a sub-directory of this.

A directory can be specified (for example "images/filename.jpg"), and the path will be taken relative to the installation root video directory."

record_chan1source

Default Value: recorddnsays
Valid Values: Choose between: recorddnsays or otherdnhears
Changes Take Effect: Immediately/session

Specifies the source to use for Call Recording channel 1. Setting this to recorddnsays selects the audio input of the record dn (or the first conference participant), setting to otherdnhears selects the conference audio output of the other dn (or second conference participant). The primary purpose is to control whether the repeating conference tone is included in the recorded audio of the record dn. If set to recorddnsays the tone will not be recorded, setting to otherdnhears will cause the tone to be recorded. The default valuse is recorddnsays.

record_chan2source

Default Value: otherdnsays
Valid Values: Choose between: otherdnsays or recorddnhears
Changes Take Effect: Immediately/session

Specifies the source to use for Call Recording channel 2. Setting this to otherdnsays selects the audio input of the other dn (or the second conference participant), setting to recordndhears selects the conference audio output of the record dn (or the first conference participant). The primary purpose is to control whether the repeating conference tone is included in the recorded audio of the other dn. If set to otherdnsays the tone will not be recorded, setting to recorddnhears will cause the tone to be recorded. The default valuse is otherdnsays.

record_otherdnhearstone

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

Specifies whether the other dn (or the second conference participant), hears the repeating tone that indicates the call is being recorded. The default value is Yes.

record_recorddnhearstone

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

Specifies whether the record dn (or the first conference participant), hears the repeating tone that indicates the call is being recorded. The default value is Yes.

silence_fill

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

Whether to silence fill the output when no data.

suppress_silence

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

Whether to suppress silence on input.

threadedoutputs

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

Enable threaded transcoding to conference outputs. Enabling this option can result in conferences that make better use of the available processors on a system.

video_mixer_layouts

Default Value: 1,dual-view|3,quad-view|5,multiple-5x1|6,multiple-3x3|10,multiple-4x4
Valid Values: A list of layouts separated by "|". Please check parameter description for more details.
Changes Take Effect: Immediately/session

Specifies the layouts that will be used by the conference video mixer when the layouts to use are not specified by the application. This parameter is only active when the conference.video_output_type parameter is set to "mixed".

This parameter has the following format:
n1,layout1|n2,layout2|n3,layout3...
where each "n,layout" pair, "layout" specifies the layout name to use when the number of conference participants is greater than or equal to "n" and less than the "n" value of any other pair.

The following layouts as described in ITEF document "draft-ietf-mediactrl-mixer-control-package" are supported:
single-view: displays the video from one participant
dual-view: displays two participants horizontally arranged
dual-view-crop: same as dual-view but video streams are cropped so as to fully fill the frame
dual-view-2x1: displays participants vertically arranged
dual-view-2x1-crop: same as dual-view-2x1 but video streams are cropped so as to fully fill the frame
quad-view: displays four participants in a 2x2 grid
multiple-5x1: displays five participants arranged along the right side and bottom, with the current active speaker displayed in a larger frame at the top left
multiple-3x3: displays 9 participants in a 3x3 grid
multiple-4x4: displays 16 participants in a 4x4 grid

For example: "1,dual-view|3,multiple-5x1", would select the dual-view layout when the number of participants is less than 3, and the multiple-5x1 layout for 3 or more participants.

If this parameter is not included or set to "", the following default value will be used:
1,dual-view|3,quad-view|5,multiple-5x1|6,multiple-3x3|10,multiple-4x4

video_output_algorithm

Default Value: confrole
Valid Values: Choose between: confrole, fixed, loudest or none
Changes Take Effect: At start/restart

Specifies how the conference chooses the video output. Note if "Select the first conference participant" is selected, the first participant should provide video input. Otherwise no video will be seen for the conference. This parameter is active only when conference.video_output_type is set to single. confrole - Select video feeds by participants' conference roles. fixed - Select the first conference participant. loudest - Select the loudest participant. none - Disable video.

video_output_type

Default Value: single
Valid Values: Choose between: single or mixed
Changes Take Effect: Immediately/session

Specifies the type of video output for conferences. If set to "single", a single stream output is enabled, where the video stream from one conference participant is sent to each conference participant. If set to "mixed", a video mixed output is enabled, where the video streams from multiple conference participants are combined into one frame and sent to each participant.

Note, if this parameter is set to "mixed" the conference.video_output_algorithm configuration parameter will not be used. Similarly, the control of video_output_algorithm by the application will be ignored.

cpa Section

- gateway.events
- outbound.method
- outbound.native.ignoreconnectevent
- outbound.native.initialstate

gateway.events

Default Value: AMD CPT FAX PVD
Valid Values: Any combination of: AMD, CPT, FAX, PVD and PTT
Changes Take Effect: Immediately/session

The supported Gateway CPA events. The ones listed here will be requested to the Gateway.

outbound.method

Default Value: NONE
Valid Values: Choose between: PSTNC, NATIVE or NONE
Changes Take Effect: Immediately/session

This configuration option controls the Call Progress Analysis method used when MCP initiates outbound calls for bridge transfers and "remdial" requests . If 'NONE' is selected, no methods will be supported. NOTE: that this option does not apply to SSG (Supplementary Services Gateway) or OCS (Outbound Contact Server) initiated calls. PSTNC - CPA using PSTN Connector NATIVE - CPA using Native CPA NONE - Disable CPA for the outbound calls

outbound.native.ignoreconnectevent

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

When native CPA is used for outbound calls (for bridge transfers and "remdial" requests), this option specifies whether the CPA algorithm should ignore or handle the call connect event. If not ignored, the native CPA algorithm will switch to the postconnect state when received the call connect event. This option can be used for fine tuning the CPA detection algorithm to improve accuracy and applies only if the outbound.native.initialstate option is set to preconnect. NOTE: this option does not apply to SSG (Supplementary Services Gateway) or OCS (Outbound Contact Server) initiated calls.

outbound.native.initialstate

Default Value: preconnect
Valid Values: Choose between: preconnect or postconnect
Changes Take Effect: Immediately/session

When native CPA is used for outbound calls (for bridge transfers and "remdial" requests), this option specifies the initial CPA state. NOTE: this option does not apply to SSG (Supplementary Services Gateway) or OCS (Outbound Contact Server) initiated calls. preconnect - detection will start as soon as the call is initiated, and detection of preconnect and postconnect events will be enabled. postconnect - detection will start when the call is connected, and only detection of postconnect events will be enabled.

email Section

- fromAddr
- smtpAddr

fromAddr

Default Value: nobody@example.com
Valid Values: Please specify a valid email address.
Changes Take Effect: At start/restart

On Windows, this is the "From" header for maintainer e-mails. On Linux, it appears as the first line of the message body.

smtpAddr

Default Value: localhost
Valid Values: Please specify a valid SMTP server address.
Changes Take Effect: At start/restart

SMTP server address for sending maintainer e-mails

ems Section

- dc.default.logfilter
- dc.default.metricsfilter
- dc.enableSQA
- dc.servicequality.AudioGap.threshold
- dc.servicequality.CallAnswer.threshold
- dc.servicequality.CallReject.threshold
- dc.servicequality.CumulativeResponse.threshold
- dc.servicequality.FirstPromptInbound.threshold
- dc.servicequality.FirstPromptOutbound.threshold
- dc.servicequality.InboundRejectNoFailureCodes
- dc.servicequality.InterPrompt.threshold
- dc.servicequality.OutboundRejectNoFailureCodes
- logconfig.DATAC
- logconfig.MFSINK
- metricsconfig.DATAC
- metricsconfig.MFSINK
- ors.reportinginterval
- password
- rc.amq_connection_send_timeout
- rc.batch_size
- rc.cdr.batch_size
- rc.cdr.local_queue_max
- rc.cdr.local_queue_path
- rc.cdr.max_throughput
- rc.certificate
- rc.keystore_certificate
- rc.keystore_password
- rc.local_queue_max
- rc.local_queue_path
- rc.max_throughput
- rc.ors.local_queue_max
- rc.ors.local_queue_path
- rc.sqa.batch_size
- rc.sqa.local_queue_max
- rc.sqa.local_queue_path
- rc.truststore_certificate

dc.default.logfilter

Default Value: 0-2|*|*
Valid Values: Pipe delimited ranges for log levels, module IDs and specifier IDs. Ranges can be comma separated integers or range of integers or '*'.
Changes Take Effect: At start/restart

Specifies the filter for logs to be delivered "upstream" to the Reporting Server for Call Events reporting. The format is 'levels|moduleIDs|specifierIDs' (repeated if necessary). The values between the pipes can be in the format: 'm-n,o,p' (ie "0-4, 5,6"). The wildcard character '*' can also be used to indicate all valid numbers. Example: '*|*|*' indicates that all log messages should be sent to the sink. Alternatively, '0,1|0-10|*|4|*|*' inidcates that CRITICAL(0) and ERROR(1) level messages with module IDs in the range 0-10 wil be sent to the sink; and all INFO(4) level messages will be sent as well.

dc.default.metricsfilter

Default Value: 0-16,18,25,35,36,41,52-55,74,128,136-141
Valid Values: Comma separated list of metric values or ranges. A metric value must be between 0 and 159 inclusive. The values '*' and blank are also allowed.

Changes Take Effect: At start/restart

Specifies the default filter for metrics to be delivered "upstream" to the Reporting Server for Call Events reporting. '*' indicates that all metrics will be sent to the sink. Alternatively, '5-10,50-55,70,71' indicates that metrics with IDs 5,6,7,8,9,10,50,51,52,53,54,55,70 and 71 will be sent to the Reporting Server. This filter will be used unless the default has been overridden in the tenant or IVR Application profile to which the given call has been associated.

dc.enableSQA

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

This flag determines if the Data Collection Sink is configured to perform Service Quality analysis.

dc.servicequality.AudioGap.threshold

Default Value: 2000
Valid Values: An integer greater than 0.
Changes Take Effect: At start/restart

This parameter indicates the largest acceptable audio gap (in ms) that the platform can have while playing back audio to the user.

dc.servicequality.CallAnswer.threshold

Default Value: 1500
Valid Values: An integer greater than 0.
Changes Take Effect: At start/restart

This parameter indicates the maximum acceptable time (in ms) that the platform can take to answer a call.

dc.servicequality.CallReject.threshold

Default Value: 2000
Valid Values: An integer greater than 0.
Changes Take Effect: At start/restart

This parameter indicates the maximum acceptable time (in ms) that the platform can take to reject a call.

dc.servicequality.CumulativeResponse.threshold

Default Value: 2000
Valid Values: An integer greater than 0.
Changes Take Effect: At start/restart

This parameter indicates the maximum acceptable time (in ms) that the platform can take to play a prompt following user interaction.

dc.servicequality.FirstPromptInbound.threshold

Default Value: 1500
Valid Values: An integer greater than 0.
Changes Take Effect: At start/restart

This parameter indicates the maximum acceptable time (in ms) that the platform can take to play the first prompt on an inbound call.

dc.servicequality.FirstPromptOutbound.threshold

Default Value: 1500
Valid Values: An integer greater than 0.
Changes Take Effect: At start/restart

This parameter indicates the maximum acceptable time (in ms) that the platform can take to play the first prompt on an outbound call.

dc.servicequality.InboundRejectNoFailureCodes

Default Value: decline
Valid Values: This is a '|' delimited list.
Changes Take Effect: At start/restart

This parameter specifies incall_reject reason codes which should not be flagged as call failures.

dc.servicequality.InterPrompt.threshold

Default Value: 4000
Valid Values: An integer greater than 0.
Changes Take Effect: At start/restart

This parameter indicates the maximum acceptable time (in ms) that the platform can take to play a prompt after a previous prompt when no user interaction has taken place inbetween the 2 prompts.

dc.servicequality.OutboundRejectNoFailureCodes

Default Value: busy|decline|fax|noanswer|hangup
Valid Values: This is a '|' delimited list.
Changes Take Effect:

This parameter specifies outcall_reject reason codes which should not be flagged as call failures.

logconfig.DATAC

Default Value: 0-2,4|*|*
Valid Values: Pipe delimited ranges for log levels, module IDs and specifier IDs. Ranges can be comma separated integers or range of integers or '*'.
Changes Take Effect: Immediately

Controls the log messages that are sent to the Data Collection sink. The format is 'levels|moduleIDs|specifierIDs' (repeated if necessary). The values between the pipes can be in the format: 'm-n,o,p' (ie "0-4, 5,6"). The wildcard character '*' can also be used to indicate all valid numbers. Example: '*|*|*' indicates that all log messages should be sent to the sink. Alternatively, '0,1|0-10|*|4|*|*' inidcates that CRITICAL(0) and ERROR(1) level messages with module IDs in the range 0-10 wil be sent to the sink; and all INFO(4) level messages will be sent as well.

logconfig.MFSINK

Default Value: *|*|*
Valid Values: Pipe delimited ranges for log levels, module IDs and specifier IDs. Ranges can be comma separated integers or range of integers or '*'.
Changes Take Effect: Immediately

Controls the log messages that are sent to the MF sink. The format is 'levels|moduleIDs|specifierIDs' (repeated if necessary). The values between the pipes can be in the format: 'm-n,o,p' (ie "0-4, 5,6"). The wildcard character '*' can also be used to indicate all valid numbers. Example: '*|*|*' indicates that all log messages should be sent to the sink. Alternatively, '0,1|0-10|*|4|*|*' inidcates that CRITICAL(0) and ERROR(1) level messages with module IDs in the range 0-10 wil be sent to the sink; and all INFO(4) level messages will be sent as well.

metricsconfig.DATAC

Default Value: *
Valid Values: Comma separated list of metric values or ranges. A metric value must be between 0 and 141 inclusive. The values '*' and blank are also allowed.
Changes Take Effect: Immediately

Specifies the metrics that are delivered to the Data Collection sink. '*' indicates that all metrics will be sent to the sink. Alternatively, '5-10,50-55,70,71' indicates that metrics with IDs 5,6,7,8,9,10,50,51,52,53,54,55,70 and 71 will be sent to the Data Collection sink.

metricsconfig.MFSINK

Default Value: 0-16,18-41,43,52-56,72-74,76-81,127-129,130,132,134,135,136-141,146-159
Valid Values: Comma separated list of metric values or ranges. A metric value must be between 0 and 159 inclusive. The values '*' and blank are also allowed.
Changes Take Effect: Immediately

Specifies the metrics that are delivered to the MF Sink. '*' indicates that all metrics will be sent to the sink. Alternatively, '5-10,50-55,70,71' indicates that metrics with IDs 5,6,7,8,9,10,50,51,52,53,54,55,70 and 71 will be sent to the MF sink.

ors.reportinginterval

Default Value: 60
Valid Values: An integer between 1-299 inclusive.
Changes Take Effect: At start/restart

Interval (seconds) accumulated operational reports are submitted to the Reporting Server

password

Default Value:
Valid Values: KeyStore Password
Changes Take Effect: at start/restart

The password for Reporting Client keyStore. Required to connect to the Reporting Server (ActiveMQ) over TLS.

rc.amq_connection_send_timeout

Default Value: 60
Valid Values: An integer greater than or equal to 45.
Changes Take Effect: At start/restart

This option specifies the maximum time in seconds to wait for ActiveMQ Producer Send Message response.

rc.batch_size

Default Value: 500
Valid Values: An integer between 1-5000 inclusive.
Changes Take Effect: At start/restart

The number of upstream log events queued up by the reporting client before sending them up to the reporting server. A higher batch size (e.g. 50 records) may improve performance at the cost of sending upstream data less frequently.

rc.cdr.batch_size

Default Value: 500
Valid Values: An integer between 1-5000 inclusive.
Changes Take Effect: At start/restart

The number of CDR messages queued up by the reporting client before sending them up to the reporting server. A higher batch size (e.g. 50 records) may improve performance at the cost of sending CDR data less frequently.

rc.cdr.local_queue_max

Default Value: 1000000
Valid Values: An integer greater or equal to -1.
Changes Take Effect: At start/restart

This option specifies the maximum number of data items to the local database for CDR reporting. Queuing to the local database will occur either when the Reporting Server is unavailable, or when data is being provided to the Client faster than the Server can consume it. A value of -1 indicates an "unlimited" number of records will be allowed. A value of 0 indicates that no records will be persisted locally and data will be discarded if the RS is unavailable.

rc.cdr.local_queue_path

Default Value: cdrQueue_mcp.db
Valid Values: Path to the DB file.
Changes Take Effect: At start/restart

The full path of the local database file used to locally persist data for CDRs.

rc.cdr.max_throughput

Default Value: 0

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

This option specifies the maximum rate at which CDR data, in bytes per second, is sent to the Reporting Server. A value of 0 (default) indicates that CDR data will be sent as quickly as possible.

rc.certificate

Default Value:
Valid Values: File path
Changes Take Effect: at start/restart

The file name of the TLS certificate in "PEM" format. Required to connect to the Reporting Server (ActiveMQ) over TLS.

rc.keystore_certificate

Default Value:
Valid Values: File path
Changes Take Effect: at start/restart
Introduced: 9.0.010.72

The file name of the TLS KeyStore certificate in "PEM" format. Required to connect to the Reporting Server (ActiveMQ) over TLS.

rc.keystore_password

Default Value:
Valid Values: KeyStore Password
Changes Take Effect: at start/restart
Introduced: 9.0.010.72

The password for Reporting Client keyStore. Required to connect to the Reporting Server (ActiveMQ) over TLS.

rc.local_queue_max

Default Value: 5000000
Valid Values: An integer greater or equal to -1.
Changes Take Effect: At start/restart

This option specifies the maximum number of data items to the local database for Upstream Logging. Queuing to the local database will occur either when the Reporting Server is unavailable, or when data is being provided to the Client faster than the Server can consume it. A value of -1 indicates an "unlimited" number of records will be allowed. A value of 0 indicates that no records will be persisted locally and data will be discarded if the RS is unavailable.

rc.local_queue_path

Default Value: reportingClientQueue.db
Valid Values: Path to the DB file.
Changes Take Effect: At start/restart

The full path of the local database file used to locally persist data for upstream logging to the GVP Reporting Client.

rc.max_throughput

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

This option specifies the maximum rate at which Upstream Logging data, in bytes per second, is sent to the Reporting Server. A value of 0 (default) indicates that Upstream Logging data will be sent as quickly as possible.

rc.ors.local_queue_max

Default Value: 1000000
Valid Values: An integer greater or equal to -1.
Changes Take Effect: At start/restart

This option specifies the maximum number of data items to the local database for Operational Reporting. Queuing to the local database will occur either when the Reporting Server is unavailable, or when data is being provided to the Client fdaster than the Server can consume it. A value of -1 indicates an "unlimited" number of records will be allowed. A value of 0 indicates that no records will be persisted locally and data will be discarded if the RS is unavailable.

rc.ors.local_queue_path

Default Value: orsQueue_mcp.db
Valid Values: Path to the DB file.
Changes Take Effect: At start/restart

The full path of the local database file used to locally persist data for Operational Reporting.

rc.sqa.batch_size

Default Value: 1
Valid Values: An integer between 1-5000 inclusive.
Changes Take Effect: At start/restart

The number of SQA messages queued up by the reporting client before sending them up to the reporting server. For SQA messages, this option has little effect.

rc.sqa.local_queue_max

Default Value: 3000
Valid Values: An integer greater or equal to -1.
Changes Take Effect: At start/restart

This option specifies the maximum number of data items to the local database file for SQA reporting. Queuing to the local database will occur either when the Reporting Server is unavailable, or when data is being provided to the Client fdaster than the Server can consume it. A value of -1 indicates an "unlimited" number of records will be allowed. A value of 0 indicates that no records will be persisted locally and data will be discarded if the RS is unavailable.

rc.sqa.local_queue_path

Default Value: sqaQueue_mcp.db
Valid Values: Path to the DB file.
Changes Take Effect: At start/restart

The full path of the local database file used to locally persist data for SQA dats.

rc.truststore_certificate

Default Value:
Valid Values: File path
Changes Take Effect: at start/restart
Introduced: 9.0.010.72

The file name of the TLS TrustStore certificate in "PEM" format. Required to connect to the Reporting Server (ActiveMQ) over TLS.

fm Section

- cachemaxentrycount
- cachemaxentrysize
- cachemaxsize
- curlconnecttimeout
- curlredirect
- dns_cache_timeout
- enable100continue
- enabletcpkeepalive
- enabletcpnodelay
- enableuploadcontentrewind
- forbid_connection_reuse
- http_proxy
- https_proxy
- interface
- localfile_maxage
- maxredirections
- no_cache_url_substring
- password
- portrange
- revalidatestaleresponse
- sleeptimems
- ssl_ca_info
- ssl_ca_path
- ssl_cert
- ssl_cert_type
- ssl_cipher_list
- ssl_crl_check_enabled
- ssl_crl_file_path
- ssl_key
- ssl_key_password
- ssl_key_type
- ssl_random_file
- ssl_verify_host
- ssl_verify_peer
- ssl_version
- tcpkeepaliveidle
- tcpkeepaliveinterval

cachemaxentrycount

Default Value: 1000
Valid Values: Must be an integer greater than or equal to 0.
Changes Take Effect: At start/restart

The maximum number of cache entries that can be stored in the cache.

cachemaxentrysize

Default Value: 20000000
Valid Values: Must be an integer greater than or equal to 0.
Changes Take Effect: At start/restart

The maximum size of each cache entry in bytes.

cachemaxsize

Default Value: 200000000
Valid Values: Must be an integer greater than or equal to 0.
Changes Take Effect: At start/restart

The maximum total size of the cache in bytes.

curlconnecttimeout

Default Value: 300
Valid Values: An positive integer less than equal to 65535.
Changes Take Effect: At start/restart

Specifies the maximum time in seconds that is allowed for the connection phase to the server. This value applies only to the connection phase; it has no effect once the connection is made. Note: For Netann calls, the parameter annc.fetchtimeout has a maximum value of 25 seconds. This can limit the maximum value for curlconnecttimeout. For example, if annc.fetchtimeout is set to 25 seconds and curlconnecttimeout is set to 30 seconds, the call will terminate as soon as the annc.fetchtimeout timer expires. Similarly, for VXML calls, parameters sessmgr.acceptcalltimeout and vxmli.initial_request_fetchtimeout might limit the maximum value for curlconnecttimeout.

curlredirect

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

Enable or disable libcurl redirect. If it is disabled, FM will perform redirections whenever necessary.

dns_cache_timeout

Default Value: 60
Valid Values: Must be a numeric value greater or equal to -1.
Changes Take Effect: At start/restart

This parameter sets the DNS cache timeout in seconds. Name resolved will be kept in memory and used for this number of seconds. Set to zero to completely disable caching, or set to -1 to make the cached entries remain forever. Note that DNS entries have a "TTL" property but libcurl doesn't use that. This DNS cache timeout is entirely speculative that a name will resolve to the same address for a certain small amount of time into the future.

enable100continue

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

Enable or disable the "Expect: 100-continue" header in HTTP 1.1 requests.

enabletcpkeepalive

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

If set to 1, TCP keepalive probes will be sent. The delay and frequency of these probes can be controlled by [fm].tcpkeepaliveidle and [fm].tcpkeepaliveinterval configuration options.

enabletcpnodelay

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

The purpose of this parameter is to try to minimize the number of small packets on the network (where "small packets" means TCP segments less than the Maximum Segment Size (MSS) for the network). If set to 1, small data segments are sent without delay (that is, without waiting for acknowledgement from a peer). Nagle algorithm will be disabled.

enableuploadcontentrewind

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

Enable or disable rewind of uploaded contet by libcurl during PUT requests. The rewind is necessary if the content needs to be resent due to a redirection. If it is disabled, libcurl will not be able to rewind the content and therefore, it won't be able to resend it.

forbid_connection_reuse

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

If set to 1, libcurl will explicitly close the connection when done with the transfer. Normally, libcurl keeps all connections alive when done with one transfer in case a succeeding one follows that can re-use them. This option should be used with caution and only if you understand what it does as it can seriously impact performance. Set to 0 to have libcurl keep the connection open for possible later re-use (default behavior).

http_proxy

Default Value: localhost:3128
Valid Values: Speficy a valid HTTP proxy address.
Changes Take Effect: At start/restart

The HTTP proxy to be used for HTTP requests.

https_proxy

Default Value:
Valid Values: Speficy a valid HTTPS proxy address.
Changes Take Effect: At start/restart

The HTTPS proxy to be used for HTTPS requests.

interface

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

This sets the network interface IP address to be used for outgoing HTTP requests. If this parameter is empty, it will automatically select the network interface to be used. If the Squid HTTP proxy is used, it has to be configured to accept HTTP requests from the interface specified. Otherwise, Squid by default would only accept HTTP requests from the localhost.

localfile_maxage

Default Value: 10
Valid Values: A number between 0 and 86400 inclusive.
Changes Take Effect: At start/restart

Maxage for cached local files in seconds. Caching of local files can be turned off by setting this to 0.

maxredirections

Default Value: 5
Valid Values: Must be an integer from 0 to 99 inclusive.
Changes Take Effect: At start/restart

The maximum number of times to follow the Location: header in the HTTP response. Set to 0 to disable HTTP redirection.

no_cache_url_substring

Default Value: cgi-bin,jsp,asp,?
Valid Values: Specify a comma-separated list of strings.
Changes Take Effect: At start/restart

If a URL contains any one of the sub-strings in this comma-delimited list, it will not be cached.

password

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

The password required to use the ssl_key.

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 port range to be used for HTTP requests. If this parameter is not specified, MCP will let the OS choose the local port.

revalidatestaleresponse

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

Specifies whether or not revalidate only stale response or any response with "must-revalidate" directive. Setting this parameter to 0 will cause revalidation of all responses that contains "must-revalidate" directive and if the parameter is 1 - only stale responses will be revalidated.

sleeptimems

Default Value: 10
Valid Values: Must be an non-negative integer.
Changes Take Effect: At start/restart

The amount of time in ms to sleep between gathering data during a fetch. It is recommended to keep this at the default of 10ms to not needlessly process data, but can be reduced if fetches take too long.

ssl_ca_info

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

The file name holding one or more certificates to verify the peer with.

ssl_ca_path

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

The path holding multiple CA certificates to verify the peer with. The certificate directory must be prepared using the openssl c_rehash utility.

ssl_cert

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

The file name of your certificate. The default format is "PEM" and can be changed with the configuration parameter ssl_cert_type

ssl_cert_type

Default Value: PEM

Valid Values: Choose between: PEM or DER
Changes Take Effect: At start/restart

The format of the certificate.

ssl_cipher_list

Default Value:
Valid Values: Can be an empty string or a colon-separated list of SSL ciphers.
Changes Take Effect: At start/restart

The list of ciphers to use for the SSL connection. The list must be syntactically correct, it consists of one or more cipher strings separated by colons. Commas or spaces are also acceptable separators but colons are normally used, , - and + can be used as operators. Valid examples of cipher lists include 'RC4-SHA', 'SHA1+DES', 'TLSv1' and 'DEFAULT'. More details about cipher lists can be found on this URL: http://www.openssl.org/docs/apps/ciphers.html.

ssl_crl_check_enabled

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

Whether or not to enable CRL validation. When this option is set, ssl_verify_peer should be set along with ssl_crl_file_path.

ssl_crl_file_path

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

The file name holding one or more certificates of CRL.

ssl_key

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

The file name of the private key. The default format for the key is "PEM" and may be changed by the parameter ssl_key_type.

ssl_key_password

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

The password required to use the ssl_key.

ssl_key_type

Default Value: PEM
Valid Values: Choose between: PEM or DER
Changes Take Effect: At start/restart

The format of the private key.

ssl_random_file

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

The path to a file which is read from to seed the random engine for SSL.

ssl_verify_host

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

Specifies how the Common name from the peer certificate should be verified during the SSL handshake: 0 - Do not verify 1 - Check existence only 2 - Ensure that it matches the provided hostname

ssl_verify_peer

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

Whether or not to verify the peer's certificate. When this option is set, one of ssl_ca_info or ssl_ca_path should be set.

ssl_version

Default Value: 0
Valid Values: Choose between: 0, 1, 3, 4, 5 or 6.
Changes Take Effect: At start/restart

Sets what version of SSL to attempt to use. By default, the SSL library will automatically detect the correct version. This parameter can be used to override this automatic detection, for situations where the wrong version is chosen. Note that SSLv2 is no longer supported. 0 - Self discover remote SSL protocol version 1 - Force TLSv1.x 3 - Force SSLv3 4 - Force TLSv1.0 5 - Force TLSv1.1 6 - Force TLSv1.2

tcpkeepaliveidle

Default Value: 60
Valid Values: An integer greater than 0.
Changes Take Effect: At start/restart

The amount of delay, in seconds, that libcurl will wait while the connection is idle before sending keepalive probes.

tcpkeepaliveinterval

Default Value: 60
Valid Values: An integer greater than 0.
Changes Take Effect: At start/restart

The amount of interval, in seconds, that libcurl will wait before sending another keepalive probe after a previously unanswered one.

log Section

- all
- check-point
- compatible-output-priority
- debug
- expire
- interaction
- keep-startup-file
- mask_sensitive_data
- memory
- memory-storage-size
- message_format
- messagefile
- print-attributes
- segment
- spool
- standard
- time_convert
- time_format
- trace
- verbose

all

Default Value: ../logs/MCP

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
Changes Take Effect: Immediately
Specifies the outputs to which an application sends all log events. The log output types must be separated by a comma when more than one output is configured.

check-point

Default Value: 1
Valid Values: 0 - 24
Changes Take Effect: Immediately

Specifies, in hours, how often the application generates a check point log event, to divide the log into sections of equal time. By

default, the application generates this log event every hour. Setting the option to 0 prevents the generation of check-point events.

compatible-output-priority

Default Value: false

Valid Values:

- **true** The log of the level specified by "Log Output Options" is sent to the specified output.
- **false** The log of the level specified by "Log Output Options" and higher levels is sent to the specified output.
Changes Take Effect: Immediately
Specifies whether the application uses 6.x output logic.

debug

Default Value: ../logs/MCP

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
Changes Take Effect: Immediately
Specifies the outputs to which an application sends the log events of the Debug level and higher (that is, log events of the Standard, Interaction, Trace, and Debug levels). The log output types must be separated by a comma when more than one output is configured.

expire

Default Value: 10

Valid Values:

- **false** No expiration; all generated segments are stored.
- **[number] file or [number]** Sets the maximum number of log files to store. Specify a number from 1-1000.
- **[number] day** Sets the maximum number of days before log files are deleted. Specify a number from 1-100. Note: If an option's value is set incorrectly-out of the range of valid values - it will be automatically reset to 10.
Changes Take Effect: Immediately
Determines whether log files expire. If they do, sets the measurement for determining when they expire, along with the maximum number of files (segments) or days before the files are removed.

interaction

Default Value: ../logs/MCP

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: Immediately
  Specifies the outputs to which an application sends the log events of the Interaction level and higher (that is, log events of the Standard and Interaction levels). The log outputs must be separated by a comma when more than one output is configured.

keep-startup-file

Default Value: true

Valid Values:

- **false** No startup segment of the log is kept.
- **true** A startup segment of the log is kept. The size of the segment equals the value of the segment option.
- **[number] KB** Sets the maximum size, in kilobytes, for a startup segment of the log.
- **[number] MB** Sets the maximum size, in megabytes, for a startup segment of the log.
  Changes Take Effect: After restart
  Specifies whether a startup segment of the log, containing the initial configuration, is to be kept. If it is, this option can be set to true or to a specific size. If set to true, the size of the initial segment will be equal to the size of the regular log segment defined by the segment option. The value of this option will be ignored if segmentation is turned off (that is, if the segment option set to false).

mask_sensitive_data

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

When set to true and the logging level is set to trace/all or debug, user input sensitive data are replaced with "****" in log messages. When set to false, no masking is applied to log.

memory

Default Value:
Valid Values: [string] (memory file name)

Changes Take Effect: Immediately

Specifies the name of the file to which the application regularly prints a snapshot of the memory output, if it is configured to do this. The new snapshot overwrites the previously written data. If the application terminates abnormally, this file will contain the latest log messages. Memory output is not recommended for processors with a CPU frequency lower than 600 MHz.

memory-storage-size

Default Value:

Valid Values:

- **[number] KB or [number]** The size of the memory output, in kilobytes. The minimum value is 128 KB.
- **[number] MB** The size of the memory output, in megabytes. The maximum value is 64 MB
Changes Take Effect: When memory output is created
Specifies the buffer size for log output to the memory, if configured.

message_format

Default Value: short

Valid Values:

- **short** An application uses compressed headers when writing log records in its log file.
- **full** An application uses complete headers when writing log records in its log file.
Changes Take Effect: Immediately
Specifies the format of log record headers that an application uses when writing logs in the log file. Using compressed log record headers improves application performance and reduces the log file's size. With the value set to short:

- A header of the log file or the log file segment contains information about the application (such as the application name, application type, host type, and time zone), whereas single log records within the file or segment omit this information.
- A log message priority is abbreviated to Std, Int, Trc, or Dbg, for Standard, Interaction, Trace, or Debug messages, respectively.
- The message ID does not contain the prefix GCTI or the application type ID.
A log record in the full format looks like this:
2002-05-07T18:11:38.196 Standard localhost cfg_dbserver GCTI-00-05060 Application started
A log record in the short format looks like this:
2002-05-07T18:15:33.952 Std 05060 Application started

messagefile

Default Value:
Valid Values: [string].lms (message file name)
Changes Take Effect: Immediately, if an application cannot find its *.lms file at startup

Specifies the file name for application-specific log events. The name must be valid for the operating system on which the application is running. The option value can also contain the absolute path to the application-specific *.lms file. Otherwise, an application looks for the file in its working directory.

print-attributes

Default Value: false

Valid Values:

- **true** Attaches extended attributes, if any exist, to a log event sent to log output.
- **false** Does not attach extended attributes to a log event sent to log output.
  Changes Take Effect: Immediately
  Specifies whether the application attaches extended attributes, if any exist, to a log event that it sends to log output. Typically, log events of the Interaction log level and Audit-related log events contain extended attributes. Setting this option to true enables audit capabilities, but negatively affects performance. Genesys recommends enabling this option for Solution Control Server and Configuration Server when using audit tracking. For other applications, refer to Genesys 7.5 Combined Log Events Help to find out whether an application generates Interaction-level and Audit-related log events; if it does, enable the option only when testing new interaction scenarios.

segment

Default Value: 10000

Valid Values:

- **false** No segmentation is allowed.
- **[number] KB or [number]** Sets the maximum segment size, in kilobytes. The minimum segment size is 100 KB.
- **[number] MB** Sets the maximum segment size, in megabytes.
- **[number] hr** Sets the number of hours for the segment to stay open. The minimum number is 1 hour.
  Changes Take Effect: Immediately
  Specifies whether there is a segmentation limit for a log file. If there is, sets the mode of measurement, along with the maximum size. If the current log segment exceeds the size set by this option, the file is closed and a new one is created.

spool

Default Value:
Valid Values: [path] (the folder, with the full path to it)
Changes Take Effect: Immediately

Specifies the folder, including full path to it, in which an application creates temporary files related to network log output. If you change the option value while the application is running, the change does not affect the currently open network output.

standard

Default Value: ../logs/MCP_standard

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message

Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.

- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
Changes Take Effect: Immediately
Specifies the outputs to which an application sends the log events of the Standard level. The log output types must be separated by a comma when more than one output is configured.

time_convert

Default Value: local

Valid Values:

- **local** The time of log record generation is expressed as a local time, based on the time zone and any seasonal adjustments. Time zone information of the application's host computer is used.
- **utc** The time of log record generation is expressed as Coordinated Universal Time (UTC).
Changes Take Effect: Immediately
Specifies the system in which an application calculates the log record time when generating a log file. The time is converted from the time in seconds since the Epoch (00:00:00 UTC, January 1, 1970).

time_format

Default Value: ISO8601

Valid Values:

- **time** The time string is formatted according to the HH:MM:SS.sss (hours, minutes, seconds, and milliseconds) format.
- **locale** The time string is formatted according to the system's locale.
- **ISO8601** The date in the time string is formatted according to the ISO 8601 format. Fractional seconds are given in milliseconds.
Changes Take Effect: Immediately
Specifies how to represent, in a log file, the time when an application generates log records.
A log record's time field in the ISO 8601 format looks like this:
2001-07-24T04:58:10.123

trace

Default Value: ../logs/MCP

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output

enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.

- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
Changes Take Effect: Immediately
Specifies the outputs to which an application sends the log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels). The log outputs must be separated by a comma when more than one output is configured.

verbose

Default Value: interaction

Valid Values:

- **all** All log events (that is, log events of the Standard, Trace,Interaction, and Debug levels) are generated.
- **debug** The same as all.
- **trace** Log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels) are generated, but log events of the Debug level are not generated.
- **interaction** Log events of the Interaction level and higher (that is, log events of the Standard and Interaction levels) are generated, but log events of the Trace and Debug levels are not generated.
- **standard** Log events of the Standard level are generated, but log events of the Interaction, Trace, and Debug levels are not generated.
- **none** No output is produced.
Changes Take Effect: Immediately
Determines whether a log output is created. If it is, specifies the minimum level of log events generated. The log events levels, starting with the highest priority level, are Standard, Interaction, Trace, and Debug.

mpc Section

- alarminterval
- amr_wb.maxptime
- amr_wb.ptime
- amr_wbpayload
- amr.enable_dtx
- amr.fmtp
- amr.maxptime
- amr.preferred_mode
- amr.ptime
- amrpayload
- amrwb.enable_dtx
- amrwb.fmtp
- amrwb.preferred_mode
- answerwithonecodec
- appendrejcodec
- asr.codec
- asr.preferredipinterface
- asr.srtp.cryptomethods
- asr.srtp.mode
- asr.srtp.sessionparamsoffer
- codec
- codecpref
- conference.allowloudestvideoecho
- cpa.busy
- cpa.carriermsg.0
- cpa.carriermsg.1
- cpa.carriermsg.2
- cpa.carriermsg.3
- cpa.carriermsg.4
- cpa.carriermsg.5
- cpa.carriermsg.6
- cpa.carriermsg.7
- cpa.carriermsg.8
- cpa.carriermsg.9
- cpa.carriermsg.readduration
- cpa.cm_enable_initial_tone_filter
- cpa.cm_initial_silence_suppression_level
- cpa.cm_match_percent
- cpa.custom1
- cpa.custom2
- cpa.custom3
- cpa.custom4
- cpa.enable_alternate_signals
- cpa.enable_carrier_messages
- cpa.enable_log_param
- cpa.enable_log_result
- cpa.fastbusy
- cpa.fax
- cpa.faxdur
- cpa.keptdur_before_statechange
- cpa.maxbeepdettime
- cpa.maxpostconntime
- cpa.maxpreconntime
- cpa.maxrings
- cpa.mintime_after_tone
- cpa.nframes_cm_detection
- cpa.no_ring_result
- cpa.postconnectresult.machine.list
- cpa.postconnsilduration
- cpa.postconnsilresult
- cpa.preconn_tones_det_mode
- cpa.preconnectresult.busy.list
- cpa.preconnectresult.custom1.list
- cpa.preconnectresult.custom2.list
- cpa.preconnectresult.custom3.list
- cpa.preconnectresult.custom4.list
- cpa.preconnectresult.fast_busy.list
- cpa.preconnectresult.sit_nocircuit.list
- cpa.preconnectresult.sit_operatorintercept.l
- cpa.preconnectresult.sit_reorder.list
- cpa.preconnectresult.sit_vacantcircuit.list
- cpa.priority_machine_machinegreetingdur
- cpa.priority_machine_maxvoicesigdur
- cpa.priority_machine_voicepausedur
- cpa.priority_normal_machinegreetingdur
- cpa.priority_normal_maxvoicesigdur
- cpa.priority_normal_voicepausedur
- cpa.priority_voice_machinegreetingdur
- cpa.priority_voice_maxvoicesigdur
- cpa.priority_voice_voicepausedur
- cpa.ringback
- cpa.sit_nocircuit
- cpa.sit_operatorintercept
- cpa.sit_reorder
- cpa.sit_vacantcircuit
- cpa.tone1.segment1.f1max
- cpa.tone1.segment1.f1min
- cpa.tone1.segment1.f2max
- cpa.tone1.segment1.f2min
- cpa.tone1.segment1.offtimemax

- cpa.tone1.segment1.offtimemin
- cpa.tone1.segment1.ontimemax
- cpa.tone1.segment1.ontimemin
- cpa.tone1.segment2.f1max
- cpa.tone1.segment2.f1min
- cpa.tone1.segment2.f2max
- cpa.tone1.segment2.f2min
- cpa.tone1.segment2.offtimemax
- cpa.tone1.segment2.offtimemin
- cpa.tone1.segment2.ontimemax
- cpa.tone1.segment2.ontimemin
- cpa.tone1.segment3.f1max
- cpa.tone1.segment3.f1min
- cpa.tone1.segment3.f2max
- cpa.tone1.segment3.f2min
- cpa.tone1.segment3.offtimemax
- cpa.tone1.segment3.offtimemin
- cpa.tone1.segment3.ontimemax
- cpa.tone1.segment3.ontimemin
- cpa.tone10.segment1.f1max
- cpa.tone10.segment1.f1min
- cpa.tone10.segment1.f2max
- cpa.tone10.segment1.f2min
- cpa.tone10.segment1.offtimemax
- cpa.tone10.segment1.offtimemin
- cpa.tone10.segment1.ontimemax
- cpa.tone10.segment1.ontimemin
- cpa.tone10.segment2.f1max
- cpa.tone10.segment2.f1min
- cpa.tone10.segment2.f2max
- cpa.tone10.segment2.f2min
- cpa.tone10.segment2.offtimemax
- cpa.tone10.segment2.offtimemin
- cpa.tone10.segment2.ontimemax
- cpa.tone10.segment2.ontimemin
- cpa.tone10.segment3.f1max
- cpa.tone10.segment3.f1min
- cpa.tone10.segment3.f2max
- cpa.tone10.segment3.f2min
- cpa.tone10.segment3.offtimemax
- cpa.tone10.segment3.offtimemin
- cpa.tone10.segment3.ontimemax
- cpa.tone10.segment3.ontimemin
- cpa.tone2.segment1.f1max
- cpa.tone2.segment1.f1min
- cpa.tone2.segment1.f2max
- cpa.tone2.segment1.f2min
- cpa.tone2.segment1.offtimemax
- cpa.tone2.segment1.offtimemin
- cpa.tone2.segment1.ontimemax
- cpa.tone2.segment1.ontimemin
- cpa.tone2.segment2.f1max
- cpa.tone2.segment2.f1min
- cpa.tone2.segment2.f2max
- cpa.tone2.segment2.f2min
- cpa.tone2.segment2.offtimemax
- cpa.tone2.segment2.offtimemin
- cpa.tone2.segment2.ontimemax
- cpa.tone2.segment2.ontimemin
- cpa.tone2.segment3.f1max
- cpa.tone2.segment3.f1min
- cpa.tone2.segment3.f2max
- cpa.tone2.segment3.f2min
- cpa.tone2.segment3.offtimemax
- cpa.tone2.segment3.offtimemin
- cpa.tone2.segment3.ontimemax
- cpa.tone2.segment3.ontimemin
- cpa.tone3.segment1.f1max
- cpa.tone3.segment1.f1min
- cpa.tone3.segment1.f2max
- cpa.tone3.segment1.f2min
- cpa.tone3.segment1.offtimemax
- cpa.tone3.segment1.offtimemin
- cpa.tone3.segment1.ontimemax
- cpa.tone3.segment1.ontimemin
- cpa.tone3.segment2.f1max
- cpa.tone3.segment2.f1min
- cpa.tone3.segment2.f2max
- cpa.tone3.segment2.f2min
- cpa.tone3.segment2.offtimemax
- cpa.tone3.segment2.offtimemin
- cpa.tone3.segment2.ontimemax
- cpa.tone3.segment2.ontimemin
- cpa.tone3.segment3.f1max
- cpa.tone3.segment3.f1min
- cpa.tone3.segment3.f2max
- cpa.tone3.segment3.f2min
- cpa.tone3.segment3.offtimemax
- cpa.tone3.segment3.offtimemin
- cpa.tone3.segment3.ontimemax
- cpa.tone3.segment3.ontimemin
- cpa.tone4.segment1.f1max
- cpa.tone4.segment1.f1min
- cpa.tone4.segment1.f2max
- cpa.tone4.segment1.f2min
- cpa.tone4.segment1.offtimemax
- cpa.tone4.segment1.offtimemin
- cpa.tone4.segment1.ontimemax
- cpa.tone4.segment1.ontimemin
- cpa.tone4.segment2.f1max
- cpa.tone4.segment2.f1min
- cpa.tone4.segment2.f2max
- cpa.tone4.segment2.f2min
- cpa.tone4.segment2.offtimemax
- cpa.tone4.segment2.offtimemin

- cpa.tone4.segment2.ontimemax
- cpa.tone4.segment2.ontimemin
- cpa.tone4.segment3.f1max
- cpa.tone4.segment3.f1min
- cpa.tone4.segment3.f2max
- cpa.tone4.segment3.f2min
- cpa.tone4.segment3.offtimemax
- cpa.tone4.segment3.offtimemin
- cpa.tone4.segment3.ontimemax
- cpa.tone4.segment3.ontimemin
- cpa.tone5.segment1.f1max
- cpa.tone5.segment1.f1min
- cpa.tone5.segment1.f2max
- cpa.tone5.segment1.f2min
- cpa.tone5.segment1.offtimemax
- cpa.tone5.segment1.offtimemin
- cpa.tone5.segment1.ontimemax
- cpa.tone5.segment1.ontimemin
- cpa.tone5.segment2.f1max
- cpa.tone5.segment2.f1min
- cpa.tone5.segment2.f2max
- cpa.tone5.segment2.f2min
- cpa.tone5.segment2.offtimemax
- cpa.tone5.segment2.offtimemin
- cpa.tone5.segment2.ontimemax
- cpa.tone5.segment2.ontimemin
- cpa.tone5.segment3.f1max
- cpa.tone5.segment3.f1min
- cpa.tone5.segment3.f2max
- cpa.tone5.segment3.f2min
- cpa.tone5.segment3.offtimemax
- cpa.tone5.segment3.offtimemin
- cpa.tone5.segment3.ontimemax
- cpa.tone5.segment3.ontimemin
- cpa.tone6.segment1.f1max
- cpa.tone6.segment1.f1min
- cpa.tone6.segment1.f2max
- cpa.tone6.segment1.f2min
- cpa.tone6.segment1.offtimemax
- cpa.tone6.segment1.offtimemin
- cpa.tone6.segment1.ontimemax
- cpa.tone6.segment1.ontimemin
- cpa.tone6.segment2.f1max
- cpa.tone6.segment2.f1min
- cpa.tone6.segment2.f2max
- cpa.tone6.segment2.f2min
- cpa.tone6.segment2.offtimemax
- cpa.tone6.segment2.offtimemin
- cpa.tone6.segment2.ontimemax
- cpa.tone6.segment2.ontimemin
- cpa.tone6.segment3.f1max
- cpa.tone6.segment3.f1min
- cpa.tone6.segment3.f2max
- cpa.tone6.segment3.f2min
- cpa.tone6.segment3.offtimemax
- cpa.tone6.segment3.offtimemin
- cpa.tone6.segment3.ontimemax
- cpa.tone6.segment3.ontimemin
- cpa.tone7.segment1.f1max
- cpa.tone7.segment1.f1min
- cpa.tone7.segment1.f2max
- cpa.tone7.segment1.f2min
- cpa.tone7.segment1.offtimemax
- cpa.tone7.segment1.offtimemin
- cpa.tone7.segment1.ontimemax
- cpa.tone7.segment1.ontimemin
- cpa.tone7.segment2.f1max
- cpa.tone7.segment2.f1min
- cpa.tone7.segment2.f2max
- cpa.tone7.segment2.f2min
- cpa.tone7.segment2.offtimemax
- cpa.tone7.segment2.offtimemin
- cpa.tone7.segment2.ontimemax
- cpa.tone7.segment2.ontimemin
- cpa.tone7.segment3.f1max
- cpa.tone7.segment3.f1min
- cpa.tone7.segment3.f2max
- cpa.tone7.segment3.f2min
- cpa.tone7.segment3.offtimemax
- cpa.tone7.segment3.offtimemin
- cpa.tone7.segment3.ontimemax
- cpa.tone7.segment3.ontimemin
- cpa.tone8.segment1.f1max
- cpa.tone8.segment1.f1min
- cpa.tone8.segment1.f2max
- cpa.tone8.segment1.f2min
- cpa.tone8.segment1.offtimemax
- cpa.tone8.segment1.offtimemin
- cpa.tone8.segment1.ontimemax
- cpa.tone8.segment1.ontimemin
- cpa.tone8.segment2.f1max
- cpa.tone8.segment2.f1min
- cpa.tone8.segment2.f2max
- cpa.tone8.segment2.f2min
- cpa.tone8.segment2.offtimemax
- cpa.tone8.segment2.offtimemin
- cpa.tone8.segment2.ontimemax
- cpa.tone8.segment2.ontimemin
- cpa.tone8.segment3.f1max
- cpa.tone8.segment3.f1min
- cpa.tone8.segment3.f2max
- cpa.tone8.segment3.f2min
- cpa.tone8.segment3.offtimemax
- cpa.tone8.segment3.offtimemin
- cpa.tone8.segment3.ontimemax

- cpa.tone8.segment3.ontimemin
- cpa.tone9.segment1.f1max
- cpa.tone9.segment1.f1min
- cpa.tone9.segment1.f2max
- cpa.tone9.segment1.f2min
- cpa.tone9.segment1.offtimemax
- cpa.tone9.segment1.offtimemin
- cpa.tone9.segment1.ontimemax
- cpa.tone9.segment1.ontimemin
- cpa.tone9.segment2.f1max
- cpa.tone9.segment2.f1min
- cpa.tone9.segment2.f2max
- cpa.tone9.segment2.f2min
- cpa.tone9.segment2.offtimemax
- cpa.tone9.segment2.offtimemin
- cpa.tone9.segment2.ontimemax
- cpa.tone9.segment2.ontimemin
- cpa.tone9.segment3.f1max
- cpa.tone9.segment3.f1min
- cpa.tone9.segment3.f2max
- cpa.tone9.segment3.f2min
- cpa.tone9.segment3.offtimemax
- cpa.tone9.segment3.offtimemin
- cpa.tone9.segment3.ontimemax
- cpa.tone9.segment3.ontimemin
- cpa.voice_level_db
- cpa.voice_range_db
- ctrleventpoollowthreshold
- ctrleventpoolthreshold
- default_audio_format
- dsp.g726littleendian
- dsp.g729a
- dtmf.detectedge
- dtmf.duration
- dtmf.gap
- dtmf.inband_amplitude
- dtmf.maxsilence
- dtmf.minduration
- dtmf.multidtmfonetimestamp
- dtmf.pauseduration
- dtmf.singlepacket
- fcr.defaultdtmfhandling
- fcr.gain
- font_paths_linux
- font_paths_win
- g722.maxptime
- g722.ptime
- g726_32.maxptime
- g726_32.ptime
- g729.fmtp
- g729.maxptime
- g729.ptime
- gsm.maxptime
- gsm.ptime
- h263_1998payload
- h263.fmtp
- h264.fmtp
- h264.in_band_param_sets_only
- h264payload
- health.maxprocessingtime
- health.waittime
- includeavpfinsdp
- maxmediathreads
- maxrecordencryptedfilesize
- maxrecordfilesize
- media.senddtmfdropaudio
- mediamgr.audiobuffersize
- mediamgr.autorecordformatselect
- mediamgr.CA_directory
- mediamgr.CA_file
- mediamgr.enableEODdoublecheck
- mediamgr.h263overrideTR
- mediamgr.hlsconsecutiveerrorsthreshold
- mediamgr.hlstotalerrorsthreshold
- mediamgr.ignore_cert_err
- mediamgr.isofilerecordheadersize
- mediamgr.maxcertificatecachesize
- mediamgr.maxcertificatelength
- mediamgr.maxcertificatesperprofile
- mediamgr.precacheprofileforcallrecording.0
- mediamgr.precacheprofileforcallrecording.1
- mediamgr.precacheprofileforcallrecording.2
- mediamgr.precacheprofileforcallrecording.3
- mediamgr.precacheprofileforcallrecording.4
- mediamgr.precacheprofileforcallrecording.5
- mediamgr.rec_iframe_delay_threshold
- mediamgr.recordmp3audiobuffer
- mediamgr.recordrtphinttrack
- mediamgr.recordwritetimeinterval
- mediamgr.rtsplowerbufferthreshold
- mediamgr.rtsppause
- mediamgr.rtspplayrange
- mediamgr.rtspupperbufferthreshold
- mediamgr.sharedhttpservers
- mediamgr.strictsamplingrate
- mediamgr.videobuffersize
- mediamgr.videofillingframeduration
- mediamgr.videofillingthreshold
- mixer.audiodelay_flush_all_threshold
- mixer.audiodelay_flush_silence_threshold
- mp3.bitrate
- mp3.compression_level_current_encoder
- mp3.interfrequency.encoding
- mp3.samplingrate
- mp3.use_current_encoder

- mp3.use_integer_transcoder
- mp3.use_integer_transcoder_current_encoder
- numdispatchthreads
- opus.apptype
- opus.bitrate
- opus.complexity
- opus.fmtp
- opus.packetloss
- opuspayload
- pcma.maxptime
- pcma.ptime
- pcmu.maxptime
- pcmu.ptime
- persistdympayfmtpair
- playcache.checkversiontime
- playcache.directory
- playcache.enable
- playcache.expiretime
- playcache.maxsize
- playremoteeodtimeout
- playremoteflushtimeout
- playsilencefill
- preferredipinterface
- record.allowsyncdiskwrite
- record.defaultdtmfhandling
- recordcachedir
- recordnumparallelpost
- recordpostbacklogthreshold
- recordpostinterval
- recordpostretrybackoff
- recordpostretrycount
- refframereqonconnjoin
- rru.beginsilence
- rru.endsilence
- rtcp.tos
- rtcp.tos.video
- rtcpfeedback.audio
- rtcpfeedback.video
- rtp.activetimeout
- rtp.audiobuffersize
- rtp.dejitter.delay
- rtp.dejitter.timeout
- rtp.dtmf.crlfenable
- rtp.dtmf.receive
- rtp.dtmf.send
- rtp.enablertcp
- rtp.fixedsocketthreads
- rtp.h264allowrfc3984stapa
- rtp.inputmode
- rtp.localaddr
- rtp.localaddrv6
- rtp.maxrtppacketsize
- rtp.multichantimeout
- rtp.overwritessrcandtimestamp
- rtp.packetseq
- rtp.portrange
- rtp.prefilltime
- rtp.request_iframe
- rtp.restrictsource
- rtp.rfc2429maxpacketsize
- rtp.sendmode
- rtp.senduponrecv
- rtp.source_buffer_video_data_size
- rtp.source_buffer_video_size
- rtp.statisticsinterval
- rtp.timeout
- rtp.tos
- rtp.tos.video
- rtp.video.udprecvbuffersize
- rtp.video.udpsendbuffersize
- rtp.videobuffersize
- rtp.vp8maxpacketsize
- rtsp.connection.portrange
- rtsp.localaddr
- rtsp.localaddrv6
- rtsp.rtp.localaddr
- rtsp.rtp.localaddrv6
- rtsp.rtp.portrange
- sdp.audiobandwidth
- sdp.connection
- sdp.map.origin.0
- sdp.map.origin.0.confgain
- sdp.map.origin.0.dtmftype
- sdp.map.origin.1
- sdp.map.origin.1.confgain
- sdp.map.origin.1.dtmftype
- sdp.map.origin.2
- sdp.map.origin.2.confgain
- sdp.map.origin.2.dtmftype
- sdp.map.origin.3
- sdp.map.origin.3.confgain
- sdp.map.origin.3.dtmftype
- sdp.map.origin.4
- sdp.map.origin.4.confgain
- sdp.map.origin.4.dtmftype
- sdp.map.origin.5
- sdp.map.origin.5.confgain
- sdp.map.origin.5.dtmftype
- sdp.map.origin.6
- sdp.map.origin.6.confgain
- sdp.map.origin.6.dtmftype
- sdp.map.origin.7
- sdp.map.origin.7.confgain
- sdp.map.origin.7.dtmftype
- sdp.map.origin.8

- sdp.map.origin.8.confgain
- sdp.map.origin.8.dtmftype
- sdp.map.origin.9
- sdp.map.origin.9.confgain
- sdp.map.origin.9.dtmftype
- sdp.videobandwidth
- srtp.cryptomethods
- srtp.maxerror
- srtp.mode
- srtp.sessionparams
- srtp.sessionparamsoffer
- telephone_event.maxptime
- telephone_event.ptime
- telephone_eventpayload
- tfcipayload
- tiasfraction
- transcoders
- transmitmultiplecodec
- tts.appendrejcodec
- tts.codec
- tts.preferredipinterface
- tts.srtp.cryptomethods
- tts.srtp.mode
- tts.srtp.sessionparamsoffer
- validatemediatimers
- videotranscoder.bitratecheckdelay
- videotranscoder.bitratechecktolerance
- videotranscoder.checkbitrate
- videotranscoder.checkframerate
- videotranscoder.frameratechecktolerance
- videotranscoder.h264.keyframeidrinterval
- videotranscoder.h264.keyframeinterval
- videotranscoder.h264.resolutions
- videotranscoder.maxbitrate
- videotranscoder.statsresetthreshold
- voipmetrics.enable
- vp8.adaptive
- vp8.defaultbitrate
- vp8.defaultframerateden
- vp8.defaultframeratenum
- vp8.defaultresolution
- vp8.maxkeyframeinterval
- vrmrecorder.codec
- vrmrecorder.enable
- vrmrecorder.preferredipinterface
- vrmrecorder.srtp.cryptomethods
- vrmrecorder.srtp.mode
- vrmrecorder.srtp.sessionparamsoffer
- widebandconferences

Tip

The following descriptions were generated by dynamic query and include cached results that may be up to one day old. Click here to refresh the query.

alarminterval

Default Value: 900000
Valid Values: mpc.alarminterval 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 sending failure alarm notifications. An initial alarm is generated on the first failure and if the 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 15 minutes(900000 milli seconds), which means that we would send failure alarm notification for the first failure and then send another alarm notification after 15 minutes. This process is repeated until the root cause for the failure has been rectified.

>> Back to Top

amr_wb.maxptime

Default Value: 0
Valid Values: Choose between: 0, 20, 40, 60, 80 or 100.
Changes Take Effect: Immediately

If the MCP is offering the SDP, or answering the SDP where the offer does not have the maxptime, the maxptime attribute will be set according to this configuration. If this configuration does not exist, or is disabled (0), the maxptime attribute will not be sent unless the SDP offer had the maxptime attribute. In the case where other codecs in the SDP also specify maxptime, the configuration of the codec listed before this codec will take precedence.

>> Back to Top

amr_wb.ptime

Default Value: 20
Valid Values: Choose between: 0, 20, 40, 60, 80 or 100.
Changes Take Effect: Immediately

If the MCP is offering the SDP or answering the SDP where the offer does not have the ptime, the ptime attribute will be set according to this configuration. This configuration is also used as the transmission rate of this codec when the remote SDP does not specify the ptime attribute. Note that transmission rate will default to 20ms if this configuration is disabled. If disabled (0), ptime attribute will not be sent unless the SDP offer had the ptime attribute. In the case where the other codecs in the SDP also specify the configured ptime, the configuration of the codec listed before this codec will take precedence.

>> Back to Top

amr_wbpayload

Default Value: 112
Valid Values: A valid AMR-WB Payload can only be an integer from 96 to 127 inclusive
Changes Take Effect: At start/restart

Default payload type number to use for the AMR-WB codec

>> Back to Top

amr.enable_dtx

Default Value: 1

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

This parameter controls whether the AMR transcoder will generate comfort noise frames when transcoding data to AMR format for which the voice activity detector indicates no speech.

>> Back to Top

amr.fmtp

Default Value: octet-align=0 | octet-align=1
Valid Values: <parameter=value>[|<parameter=value>]*
Changes Take Effect: At start/restart

Specifies the AMR SDP RTP payload configurations offered and accepted by the MCP. Set to one or more fmtp text values separated by the '|' character. The fmtp text is the same as would appear in the SDP negotiation (see RFC 4867). Each "|" separated value configures an AMR payload type. There are two fmtp parameters that can be set for each payload type, octet-align and mode-set.

Setting octet-align=0 or octet-align=1 disables or enables octet align mode for the payload.

Setting mode-set restricts the AMR modes for the payload. For example, setting "mode-set=0,1" only allows modes 0 and 1. If mode-set is not set, all modes are allowed unless the mode-set is restricted by the remote end. Valid modes are inclusively 0 to 7.

For example, setting this parameter to "octet-align=1" enables one payload type with octet aligned mode enabled and any mode allowed, and setting it to "octet-align=0 | octet-align=1" enables two payload types, one with bandwidth efficient mode enabled and any mode allowed, and one with octet aligned enabled and any mode allowed.

Note, the mode-set parameter can cause transcoding to be required. For example, if a prompt to be played is in AMR format mode 5, but only mode 0 is allowed in the payload, a transcoder will be invoked to transcode from AMR mode 5 to AMR mode 0.

Some AMR implementations may specify a fmtp options that are not actually activated for the payload. To work around this, the mpc.amr.fmtp can be set to "*". For this setting, all fmtp content in an SDP offer will be ignored and "octet-align=0" will be returned in the SDP answer. Similarly, an offer for this configuration will be set to "octet-align=0", and all fmtp content in the answer will be ignored.

>> Back to Top

amr.maxptime

Default Value: 0
Valid Values: Choose between: 0, 20, 40, 60, 80 or 100.
Changes Take Effect: Immediately

If the MCP is offering the SDP, or answering the SDP where the offer does not have the maxptime, the maxptime attribute will be set according to this configuration. If this configuration does not exist, or is disabled (0), the maxptime attribute will not be sent unless the SDP offer had the maxptime attribute. In the case where other codecs in the SDP also specify maxptime, the configuration of the codec listed before this codec will take precedence.

>> Back to Top

amr.preferred_mode

Default Value: 15
Valid Values: Choose between: 0, 1, 2, 3, 4, 5, 6, 7 or 15 (Disable)
Changes Take Effect: Immediately

Specifies the AMR Preferred Codec Mode. This is the value that the MCP sends to the remote end as the preferred mode for AMR data sent to the MCP.

>> Back to Top

amr.ptime

Default Value: 20
Valid Values: Choose between: 0, 20, 40, 60, 80 or 100.
Changes Take Effect: Immediately

If the MCP is offering the SDP or answering the SDP where the offer does not have the ptime, the ptime attribute will be set according to this configuration. This configuration is also used as the transmission rate of this codec when the remote SDP does not specify the ptime attribute. Note that transmission rate will default to 20ms if this configuration is disabled. If disabled (0), ptime attribute will not be sent unless the SDP offer had the ptime attribute. In the case where the other codecs in the SDP also specify the configured ptime, the configuration of the codec listed before this codec will take precedence.

>> Back to Top

amrpayload

Default Value: 105
Valid Values: A valid AMR Payload can only be an integer from 96 to 127 inclusive
Changes Take Effect: At start/restart

Default payload type number to use for the AMR codec

>> Back to Top

amrwb.enable_dtx

Default Value: 1
Valid Values: Choose between: 0 or 1

Changes Take Effect: At start/restart

This parameter controls whether the AMR-WB transcoder will generate comfort noise frames when transcoding data to AMR-WB format for which the voice activity detector indicates no speech.

>> Back to Top

amrwb.fmtp

Default Value: octet-align=0 | octet-align=1
Valid Values: <parameter=value>[|<parameter=value>]*
Changes Take Effect: At start/restart

Specifies the AMR-WB SDP RTP payload configurations offered and accepted by the MCP. Set to one or more fmtp text values separated by the '|' character. The fmtp text is the same as would appear in the SDP negotiation (see RFC 4867). Each "|" separated value configures an AMR-WB payload type. There are two fmtp parameters that can be set for each payload type, octet-align and mode-set.

Setting octet-align=0 or octet-align=1 disables or enables octet align mode for the payload.

Setting mode-set restricts the AMR-WB modes for the payload. For example, setting "mode-set=0,1" only allows modes 0 and 1. If mode-set is not set, all modes are allowed unless the mode-set is restricted by the remote end. Valid modes are inclusively 0 to 8.

For example, setting this parameter to "octet-align=1" enables one payload type with octet aligned mode enabled and any mode allowed, and setting it to "octet-align=0 | octet-align=1" enables two payload types, one with bandwidth efficient mode enabled and any mode allowed, and one with octet aligned enabled and any mode allowed.

Note, the mode-set parameter can cause transcoding to be required. For example, if a prompt to be played is in AMR-WB format mode 5, but only mode 0 is allowed in the payload, a transcoder will be invoked to transcode from AMR-WB mode 5 to AMR-WB mode 0.

Some AMR-WB implementations may specify a fmtp options that are not actually activated for the payload. To work around this, the mpc.amrwb.fmtp can be set to "*". For this setting, all fmtp content in an SDP offer will be ignored and "octet-align=0" will be returned in the SDP answer. Similarly, an offer for this configuration will be set to "octet-align=0", and all fmtp content in the answer will be ignored.

>> Back to Top

amrwb.preferred_mode

Default Value: 15
Valid Values: Choose between: 0, 1, 2, 3, 4, 5, 6, 7 or 15 (Disable)
Changes Take Effect: Immediately

Specifies the AMR-WB Preferred Codec Mode. This is the value that the MCP sends to the remote end as the preferred mode for AMR-WB data sent to the MCP.

>> Back to Top

answerwithonecodec

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

When an SDP offer contains more than one codec per media line, this can be used to limit the codecs in the answer to one (the most preferred) when enabled. If disabled (the default), all the negotiated codecs will be returned in the answer.

>> Back to Top

appendrejcodec

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

When set to Enable, the MCP will advertise all supported codecs when generating an SDP answer or SDP offer. Even if codecs are rejected or not presented in the caller's SDP, the MCP will still support receiving these codecs. The MCP will not send for those SDPs unless a payload is presented by the caller.

>> Back to Top

asr.codec

Default Value: pcmu telephone-event
Valid Values: Choose between: "pcmu telephone-event", "pcma telephone-event", "g722 telephone-event", "g726 telephone-event", "g729 telephone-event", "gsm telephone-event", "amr telephone-event", "amr-wb telephone-event" or "tfci telephone-event".
Changes Take Effect: At start/restart

Specifies the MRCP ASR codec to be used.

>> Back to Top

asr.preferredipinterface

Default Value: V4
Valid Values: Choose between: V4 or V6
Changes Take Effect: At start/restart

Specifies the preferred IP interface to use (IPv4 or IPv6) for MRCP ASR when performing SDP negotiation. In particular, this will be used to set the root connection attribute in SDP answers, and set the connection attribute in SDP offers.

>> Back to Top

asr.srtp.cryptomethods

Default Value: AES_CM_128_HMAC_SHA1_80
Valid Values: Any combination of: "AES_CM_128_HMAC_SHA1_80" and "AES_CM_128_HMAC_SHA1_32". Or "none".
Changes Take Effect: At start/restart

List of crypto suites corresponding to advertised capabilities offered by the MCP to the MRCP ASR server using SDP. See RFC4568 for the description of the suites. Methods can only contain alphanumeric characters.

>> Back to Top

asr.srtp.mode

Default Value: none
Valid Values: none: No SRTP supported: the MCP will ignore the crypto. offer: SRTP supported in outgoing SDP offers. If the other side ignores SRTP, the MCP will fall back to non SRTP mode. offer_strict: Same as offer, however if the other side doesn't use SRTP, negotiation will fail.
Changes Take Effect: At start/restart

Specifies the srtp mode for the MCP to use for MRCP ASR sessions.

>> Back to Top

asr.srtp.sessionparamsoffer

Default Value: none
Valid Values: Any combination of: "UNENCRYPTED_SRTP", "UNENCRYPTED_SRTCP" and "UNAUTHENTICATED_SRTP". Or "none".
Changes Take Effect: At start/restart

List of session parameters that the MCP will include in its SDP offers to the MRCP ASR server. See RFC4568 for their description. Note that RFC4568 doesn't allow unauthenticated srtcp.

>> Back to Top

codec

Default Value: pcmu pcma g722 opus g726 g729 gsm amr amr-wb h263 h263-1998 h264 vp8 telephone-event
Valid Values: Any combination of: pcmu, pcma, g722, opus, g726, g729, gsm, amr, amr-wb, tfci,

h263, h263-1998, h264, vp8 or telephone-event.
Changes Take Effect: Immediately/session

List of codec corresponding to advertised capabilities offered by the MCP using SDP. The offered codec list will control the codecs that are offered by the MCP to the remote party for media sent from the remote party to Genesys. The order of the codecs will determine the order in SDP offer presented by the MCP. telephone-event is mandatory if RFC2833 DTMF relay is required. If the telephone-event is not set then the mpc.rtp.dtmf.send and mpc.rtp.dtmf.receive will control the DTMF relay method.

>> Back to Top

codecpref

Default Value: r
Valid Values: Choose between: r or l
Changes Take Effect: Immediately/session

Specifies whether remote or local preferences will be used to interpret the accept codec list. If remote preferences are used, then the effective accept list will be the format list offered by the remote entity, filtered to include only those entries also on the locally configured list. If local preferences are used, then the local accept list will be used, but only including those capabilities offered by the remote entity. The "mpc.codecpref" parameter will be used to control this, and can be set to either Remote or Local; the default value will be Remote. r - Remote l - Local

>> Back to Top

conference.allowloudestvideoecho

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

Only applicable if the conference.video_output_algorithm is loudest or confrole where it falls back to the loudest. This parameter controls who the loudest speaker will see as the video. If true, the loudest speaker will see oneself. If false, the loudest spaker will see the previously selected video who was not oneself (if no previous, then no video).

>> Back to Top

cpa.busy

Default Value: na_busy
Valid Values: Any combination of: "na_ringback", "na_busy", "na_fastbusy", "na_sit_nocircuit", "na_sit_vacantcircuit", "na_sit_operatorintercept", "na_sit_reorder", "standard_fax", "tone1", "tone2", "tone3", "tone4", "tone5", "tone6", "tone7", "tone8", "tone9" and "tone10". Or "none".
Changes Take Effect: At start/restart

Specifies tones for CPA's busy pattern. Default tone value is builtin North American busy (NA busy). Value "Disable" disables busy detection. Valid tones include builtins and Custom tone 1 to Custom tone 10.

The builtin North American busy has three segments. All segments are the same and are defined as follows:
Segment 1: f1=460-500(Hz), f2=600-640(Hz), ontime=360-640(ms), offtime=360-640(ms)
Segment 2: f1=460-500(Hz), f2=600-640(Hz), ontime=360-640(ms), offtime=360-640(ms)
Segment 3: f1=460-500(Hz), f2=600-640(Hz), ontime=360-640(ms), offtime=360-640(ms)

>> Back to Top

cpa.carriermsg.0

Default Value:
Valid Values: Can be an empty string or a valid path to a carrier message file.
Changes Take Effect: Immediately

Specifies full path for the file with carrier message. Path requires a schema of file://, http:// or https://. Examples: cpa.carriermsg.0 = file://E:\cpatest\carrierMsg\cm_NotInUse_Operator1.pcm16 cpa.carriermsg.0 = file:///opt/msg/cm_NotInUse_Operator1.pcm16 cpa.carriermsg.0 = http://localhost/cm_NotInUse_Operator1.wav You can configure as many as 100 carrier messages. The limitation of 100 messages is due to performance.

>> Back to Top

cpa.carriermsg.1

Default Value:
Valid Values: Can be an empty string or a valid path to a carrier message file.
Changes Take Effect: Immediately

Specifies full path for the file with carrier message. Path requires a schema of file://, http:// or https://. Examples: cpa.carriermsg.1 = file://E:\cpatest\carrierMsg\cm_NotInUse_Operator1.pcm16 cpa.carriermsg.1 = file:///opt/msg/cm_NotInUse_Operator1.pcm16 cpa.carriermsg.1 = http://localhost/cm_NotInUse_Operator1.wav You can configure as many as 100 carrier messages. The limitation of 100 messages is due to performance.

>> Back to Top

cpa.carriermsg.2

Default Value:
Valid Values: Can be an empty string or a valid path to a carrier message file.
Changes Take Effect: Immediately

Specifies full path for the file with carrier message. Path requires a schema of file://, http:// or https://. Examples: cpa.carriermsg.2 = file://E:\cpatest\carrierMsg\cm_NotInUse_Operator1.pcm16 cpa.carriermsg.2 = file:///opt/msg/cm_NotInUse_Operator1.pcm16 cpa.carriermsg.2 = http://localhost/cm_NotInUse_Operator1.wav You can configure as many as 100 carrier messages. The limitation of 100 messages is due to performance.

>> Back to Top

cpa.carriermsg.3

Default Value:
Valid Values: Can be an empty string or a valid path to a carrier message file.
Changes Take Effect: Immediately

Specifies full path for the file with carrier message. Path requires a schema of file://, http:// or https://. Examples: cpa.carriermsg.3 = file://E:\cpatest\carrierMsg\cm_NotInUse_Operator1.pcm16 cpa.carriermsg.3 = file:///opt/msg/cm_NotInUse_Operator1.pcm16 cpa.carriermsg.3 = http://localhost/cm_NotInUse_Operator1.wav You can configure as many as 100 carrier messages. The limitation of 100 messages is due to performance.

>> Back to Top

cpa.carriermsg.4

Default Value:
Valid Values: Can be an empty string or a valid path to a carrier message file.
Changes Take Effect: Immediately

Specifies full path for the file with carrier message. Path requires a schema of file://, http:// or https://. Examples: cpa.carriermsg.4 = file://E:\cpatest\carrierMsg\cm_NotInUse_Operator1.pcm16 cpa.carriermsg.4 = file:///opt/msg/cm_NotInUse_Operator1.pcm16 cpa.carriermsg.4 = http://localhost/cm_NotInUse_Operator1.wav You can configure as many as 100 carrier messages. The limitation of 100 messages is due to performance.

>> Back to Top

cpa.carriermsg.5

Default Value:
Valid Values: Can be an empty string or a valid path to a carrier message file.
Changes Take Effect: Immediately

Specifies full path for the file with carrier message. Path requires a schema of file://, http:// or https://. Examples: cpa.carriermsg.5 = file://E:\cpatest\carrierMsg\cm_NotInUse_Operator1.pcm16 cpa.carriermsg.5 = file:///opt/msg/cm_NotInUse_Operator1.pcm16 cpa.carriermsg.5 = http://localhost/cm_NotInUse_Operator1.wav You can configure as many as 100 carrier messages. The limitation of 100 messages is due to performance.

>> Back to Top

cpa.carriermsg.6

Default Value:
Valid Values: Can be an empty string or a valid path to a carrier message file.
Changes Take Effect: Immediately

Specifies full path for the file with carrier message. Path requires a schema of file://, http:// or https://. Examples: cpa.carriermsg.6 = file://E:\cpatest\carrierMsg\cm_NotInUse_Operator1.pcm16 cpa.carriermsg.6 = file:///opt/msg/cm_NotInUse_Operator1.pcm16 cpa.carriermsg.6 = http://localhost/cm_NotInUse_Operator1.wav You can configure as many as 100 carrier messages. The limitation of 100 messages is due to performance.

>> Back to Top

cpa.carriermsg.7

Default Value:
Valid Values: Can be an empty string or a valid path to a carrier message file.
Changes Take Effect: Immediately

Specifies full path for the file with carrier message. Path requires a schema of file://, http:// or https://. Examples: cpa.carriermsg.7 = file://E:\cpatest\carrierMsg\cm_NotInUse_Operator1.pcm16 cpa.carriermsg.7 = file:///opt/msg/cm_NotInUse_Operator1.pcm16 cpa.carriermsg.7 = http://localhost/cm_NotInUse_Operator1.wav You can configure as many as 100 carrier messages. The limitation of 100 messages is due to performance.

>> Back to Top

cpa.carriermsg.8

Default Value:
Valid Values: Can be an empty string or a valid path to a carrier message file.
Changes Take Effect: Immediately

Specifies full path for the file with carrier message. Path requires a schema of file://, http:// or https://. Examples: cpa.carriermsg.8 = file://E:\cpatest\carrierMsg\cm_NotInUse_Operator1.pcm16 cpa.carriermsg.8 = file:///opt/msg/cm_NotInUse_Operator1.pcm16 cpa.carriermsg.8 = http://localhost/cm_NotInUse_Operator1.wav You can configure as many as 100 carrier messages. The limitation of 100 messages is due to performance.

>> Back to Top

cpa.carriermsg.9

Default Value:
Valid Values: Can be an empty string or a valid path to a carrier message file.
Changes Take Effect: Immediately

Specifies full path for the file with carrier message. Path requires a schema of file://, http:// or https://. Examples: cpa.carriermsg.9 = file://E:\cpatest\carrierMsg\cm_NotInUse_Operator1.pcm16 cpa.carriermsg.9 = file:///opt/msg/cm_NotInUse_Operator1.pcm16 cpa.carriermsg.9 = http://localhost/cm_NotInUse_Operator1.wav You can configure as many as 100 carrier messages. The limitation of 100 messages is due to performance.

>> Back to Top

cpa.carriermsg.readduration

Default Value: 60
Valid Values: The number must be a non-negative integer, greater than or equal to 60 and less than or equal to 300
Changes Take Effect: Immediately

Specifies the read duration. This is how many seconds we read from a carrier message file until we stop reading that file. This prevents MCP from reading carrier message files if they span far too long. Very long carrier message files can impact matching accuracy.

This parameter does not govern HTTP request timeouts.

A maximum read duration of 300 seconds for optimal matching accuracy and performance is enforced. A minimum of 60 seconds is required.

Do not rely on this parameter to precisely measure how long to read each file. Always ensure that the read duration is longer than your longest carrier message file.

After changing this parameter, the coefficients for all the carrier message will be recalculated again. Please give it some time to recalculate before attempting to make a call after changing this parameter.

>> Back to Top

cpa.cm_enable_initial_tone_filter

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

Tone filter for suppressing generic single tone at the beginning of the incoming frames for carrier message detection. The suppression starts when 10 consecutive frames (400msec) of a given frequency is detected. There is no limit for tone duration, so both continuous and intermittent tone (like ring tones) are suppressed.

>> Back to Top

cpa.cm_initial_silence_suppression_level

Default Value: 64
Valid Values: A valid suppression level must be in the range 0-100 inclusive.
Changes Take Effect: At start/restart

Specifies the initial level needed for silence suppression in carrier messages detection. Common range for this parameter is 40 to 100. Increasing the value of this parameter results in high energy noise getting suppressed.

>> Back to Top

cpa.cm_match_percent

Default Value: 80
Valid Values: A valid matching percent should be in the range 40-80 inclusive.
Changes Take Effect: Immediately/session

Specifies matching percent for carrier messages detection. Common range for this parameter is 70 to 80. Increasing this value, the matching is favoured; decreasing the value, the matching is restricted.

>> Back to Top

cpa.custom1

Default Value: none
Valid Values: Any combination of: "na_ringback", "na_busy", "na_fastbusy", "na_sit_nocircuit", "na_sit_vacantcircuit", "na_sit_operatorintercept", "na_sit_reorder", "standard_fax", "tone1", "tone2", "tone3", "tone4", "tone5", "tone6", "tone7", "tone8", "tone9" and "tone10". Or "none".
Changes Take Effect: At start/restart

Specifies tones for CPA's custom 1 pattern. Default tone value is "Disable" which disables custom 1 detection. Valid tones include builtins and Custom tone 1 to Custom tone 10.

>> Back to Top

cpa.custom2

Default Value: none
Valid Values: Any combination of: "na_ringback", "na_busy", "na_fastbusy", "na_sit_nocircuit", "na_sit_vacantcircuit", "na_sit_operatorintercept", "na_sit_reorder", "standard_fax", "tone1", "tone2", "tone3", "tone4", "tone5", "tone6", "tone7", "tone8", "tone9" and "tone10". Or "none".
Changes Take Effect: At start/restart

Specifies tones for CPA's custom 2 pattern. Default tone value is "Disable" which disables custom 2 detection. Valid tones include builtins and Custom tone 1 to Custom tone 10.

>> Back to Top

cpa.custom3

Default Value: none
Valid Values: Any combination of: "na_ringback", "na_busy", "na_fastbusy", "na_sit_nocircuit", "na_sit_vacantcircuit", "na_sit_operatorintercept", "na_sit_reorder", "standard_fax", "tone1", "tone2", "tone3", "tone4", "tone5", "tone6", "tone7", "tone8", "tone9" and "tone10". Or "none".
Changes Take Effect: At start/restart

Specifies tones for CPA's custom 3 pattern. Default tone value is "Disable" which disables custom 3 detection. Valid tones include builtins and Custom tone 1 to Custom tone 10.

>> Back to Top

cpa.custom4

Default Value: none
Valid Values: Any combination of: "na_ringback", "na_busy", "na_fastbusy", "na_sit_nocircuit", "na_sit_vacantcircuit", "na_sit_operatorintercept", "na_sit_reorder", "standard_fax", "tone1", "tone2", "tone3", "tone4", "tone5", "tone6", "tone7", "tone8", "tone9" and "tone10". Or "none".
Changes Take Effect: At start/restart

Specifies tones for CPA's custom 4 pattern. Default tone value is "Disable" which disables custom 4 detection. Valid tones include builtins and Custom tone 1 to Custom tone 10.

>> Back to Top

cpa.enable_alternate_signals

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

Enable CPA alternate signals checking. This parameter should be turned on when we have SIT tone coming right after ring tone, without any silence or with very small silence (less than 100 msec). This parameter also good for cases when voice is coming right after SIT tone with small silence in between.

>> Back to Top

cpa.enable_carrier_messages

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

Enables/ disables carrier messages detection.

>> Back to Top

cpa.enable_log_param

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

Enable CPA configuration parameters logging

>> Back to Top

cpa.enable_log_result

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

Enable CPA result logging

>> Back to Top

cpa.fastbusy

Default Value: na_fastbusy
Valid Values: Any combination of: "na_ringback", "na_busy", "na_fastbusy", "na_sit_nocircuit", "na_sit_vacantcircuit", "na_sit_operatorintercept", "na_sit_reorder", "standard_fax", "tone1", "tone2", "tone3", "tone4", "tone5", "tone6", "tone7", "tone8", "tone9" and "tone10". Or "none".
Changes Take Effect: At start/restart

Specifies tones for CPA's fast busy pattern. Default tone value is builtin North American fast busy (NA fast busy). Value "Disable" disables fast busy detection. Valid tones include builtins and Custom tone 1 to Custom tone 10.

The builtin North American fast busy has three segments. All segments are the same and are defined as follows:
Segment 1: f1=460-500(Hz), f2=600-640(Hz), ontime=160-320(ms), offtime=180-320(ms)
Segment 2: f1=460-500(Hz), f2=600-640(Hz), ontime=160-320(ms), offtime=180-320(ms)
Segment 3: f1=460-500(Hz), f2=600-640(Hz), ontime=160-320(ms), offtime=180-320(ms)

>> Back to Top

cpa.fax

Default Value: standard_fax
Valid Values: Any combination of: "na_ringback", "na_busy", "na_fastbusy", "na_sit_nocircuit", "na_sit_vacantcircuit", "na_sit_operatorintercept", "na_sit_reorder", "standard_fax", "tone1", "tone2", "tone3", "tone4", "tone5", "tone6", "tone7", "tone8", "tone9" and "tone10". Or "none".
Changes Take Effect: At start/restart

Specifies tones for CPA's fax pattern. Default tone value is builtin standard fax (Standard fax). Value "Disable" disables fax detection. Valid tones include builtins and Custom tone 1 to Custom tone 10.

The builtin standard fax has only one segment and is defined as follows:
Segment 1: f1=2090-2110(Hz), f2=0-0(Hz), ontime=cpa.faxdur(ms), offtime=n/a

>> Back to Top

cpa.faxdur

Default Value: 160
Valid Values: A valid fax duration must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies fax duration (msec) for CPA. Fax signal must be greater than or equal to this length to be detected.

>> Back to Top

cpa.keptdur_before_statechange

Default Value: 0
Valid Values: A valid duration kept upon state modification must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum most recent buffer duration (msec) to be kept when CPA is requested to move from one state to another.

>> Back to Top

cpa.maxbeepdettime

Default Value: 30000
Valid Values: A valid beepdetect time must be a numeric not less than 20
Changes Take Effect: At start/restart

Specifies maximum duration (msec) for CPA beep detection state before a timeout event is thrown.

>> Back to Top

cpa.maxpostconntime

Default Value: 20000
Valid Values: A valid postconnect time must be a numeric not less than 20
Changes Take Effect: At start/restart

Specifies maximum duration (msec) for CPA postconnect state before a timeout event is thrown.

>> Back to Top

cpa.maxpreconntime

Default Value: 30000
Valid Values: A valid preconnect time must be a numeric not less than 20
Changes Take Effect: At start/restart

Specifies maximum duration (msec) for CPA preconnect state before a timeout event is thrown.

>> Back to Top

cpa.maxrings

Default Value: 0
Valid Values: A valid maximum ringback must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum ringbacks before a no answer event is thrown by CPA. Zero disables ringback count.

>> Back to Top

cpa.mintime_after_tone

Default Value: 200
Valid Values: A valid integer number between 40 and 400, inclusive of both numbers.
Changes Take Effect: At start/restart

Specifies the minimum idle time to wait (in milli seconds) following a detected tone signal before confirming it. In some situations, a SIT tone could almost immediately be followed by a connect event, ending the preconnect state and the SIT detection. In such situations, a shorter value for this parameter, say 100 ms, may be needed to wrap up SIT detection before the connect event.

>> Back to Top

cpa.nframes_cm_detection

Default Value: 50
Valid Values: A valid number of frames must be in the range 25-100 inclusive.
Changes Take Effect: At start/restart

Specifies the number of frames needed for carrier messages detection. Increasing the number of frames improves precision of the matching process but delays time to result.

>> Back to Top

cpa.no_ring_result

Default Value: 0
Valid Values: Choose between: 0, 2, 15, 16, 17 or 18.
Changes Take Effect: Immediately/session

This parameter specifies CPA result if no ringback is detected before postconnect event arrives. Default is none, that is, no CPA result returned. 0 - none 2 - busy 15 - human 16 - machine 17 - fax 18 - no_media

>> Back to Top

cpa.postconnectresult.machine.list

Default Value:
Valid Values: Can be an empty string or a space separated list of numbers ranging from 0 to 100.
Changes Take Effect: Immediately/session

Specifies list of carrier message files associated with result machine in postconnect mode. The list is a sequence of integer number equal to the index of carrier message previously specified. Example: cpa.postconnectresult.machine.list = 0 10 It means that if incoming message matches with carriermsg.0 or carriermsg.10, then CPA outputs result = machine

>> Back to Top

cpa.postconnsilduration

Default Value: 1000
Valid Values: A valid value must be in the range 200-3000 inclusive
Changes Take Effect: Immediately/session

Specifies the duration of silence that may trigger a configurable CPD result immediately after the postconnent event arrives. The default value is 1000 milliseconds. The range is between 200 and 3000 milliseconds. This parameter does not take effect until mpc.cpa.postconnsilresult is set to a value other than none (0).

>> Back to Top

cpa.postconnsilresult

Default Value: 0
Valid Values: Choose between: 0, 2, 15, 16, 17 or 18.
Changes Take Effect: Immediately/session

Specifies CPA result if a period of silence, which is configurable through mpc.cpa.postconnsilduration, is detected immediately after postconnect event arrives. The default option is none (0), that is, no CPA result returned. 0 - none 2 - busy 15 - human 16 - machine 17 - fax 18 - no_media

>> Back to Top

cpa.preconn_tones_det_mode

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

Specifies the mode for the detection of preconnect tones. By default, the preconnect tones will only be detected in preconnect state. Optionally, the detection can be configured to operate in preconnect and postconnect state. 0 - Preconnect state only 1 - Preconnect and postconnect state NOTE: This option only applies to tones, carrier message detection (Voiceprint) during preconnect phase is not affected, that is, by setting this option to 1 (Preconnect and postconnect state) will not make MCP detect carrier messages at postconnect phase.

>> Back to Top

cpa.preconnectresult.busy.list

Default Value:
Valid Values: Can be an empty string or a space separated list of numbers ranging from 0 to 100.
Changes Take Effect: Immediately/session

Specifies list of carrier message files associated with result busy in preconnect mode. The list is a sequence of integer number equal to the index of carrier message previously specified. Example: cpa.preconnectresult.busy.list = 0 2 4 It means that if incoming message matches with carriermsg.0, carriermsg.2 or carriermsg.4 then CPA outputs result = busy.

>> Back to Top

cpa.preconnectresult.custom1.list

Default Value:
Valid Values: Can be an empty string or a space separated list of numbers ranging from 0 to 100.

Changes Take Effect: Immediately/session

Specifies list of carrier message files associated with result custom1 in preconnect mode. The list is a sequence of integer number equal to the index of carrier message previously specified. Example: cpa.preconnectresult.custom1.list = 0 2 4 It means that if incoming message matches with carriermsg.0, carriermsg.2 or carriermsg.4 then CPA outputs result = sit.custom1.

>> Back to Top

cpa.preconnectresult.custom2.list

Default Value:
Valid Values: Can be an empty string or a space separated list of numbers ranging from 0 to 100.
Changes Take Effect: Immediately/session

Specifies list of carrier message files associated with result custom2 in preconnect mode. The list is a sequence of integer number equal to the index of carrier message previously specified. Example: cpa.preconnectresult.custom2.list = 1 3 5 It means that if incoming message matches with carriermsg.1, carriermsg.3 or carriermsg.5 then CPA outputs result = sit.custom2.

>> Back to Top

cpa.preconnectresult.custom3.list

Default Value:
Valid Values: Can be an empty string or a space separated list of numbers ranging from 0 to 100.
Changes Take Effect: Immediately/session

Specifies list of carrier message files associated with result custom3 in preconnect mode. The list is a sequence of integer number equal to the index of carrier message previously specified. Example: cpa.preconnectresult.custom3.list = 0 2 4 It means that if incoming message matches with carriermsg.0, carriermsg.2 or carriermsg.4 then CPA outputs result = sit.custom3.

>> Back to Top

cpa.preconnectresult.custom4.list

Default Value:
Valid Values: Can be an empty string or a space separated list of numbers ranging from 0 to 100.
Changes Take Effect: Immediately/session

Specifies list of carrier message files associated with result custom4 in preconnect mode. The list is a sequence of integer number equal to the index of carrier message previously specified. Example: cpa.preconnectresult.custom4.list = 0 2 4 It means that if incoming message matches with carriermsg.0, carriermsg.2 or carriermsg.4 then CPA outputs result = sit.custom4.

>> Back to Top

cpa.preconnectresult.fast_busy.list

Default Value:
Valid Values: Can be an empty string or a space separated list of numbers ranging from 0 to 100.
Changes Take Effect: Immediately/session

Specifies list of carrier message files associated with result fast busy in preconnect mode. The list is a sequence of integer number equal to the index of carrier message previously specified. Example: cpa.preconnectresult.fast_busy.list = 0 2 4 It means that if incoming message matches with carriermsg.0, carriermsg.2 or carriermsg.4 then CPA outputs result = busy.

>> Back to Top

cpa.preconnectresult.sit_nocircuit.list

Default Value:
Valid Values: Can be an empty string or a space separated list of numbers ranging from 0 to 100.
Changes Take Effect: Immediately/session

Specifies list of carrier message files associated with result sit_nocircuit in preconnect mode. The list is a sequence of integer number equal to the index of carrier message previously specified. Example: cpa.preconnectresult.sit_nocircuit.list = 0 2 4 It means that if incoming message matches with carriermsg.0, carriermsg.2 or carriermsg.4 then CPA outputs result = sit.nocircuit.

>> Back to Top

cpa.preconnectresult.sit_operatorintercept.list

Default Value:
Valid Values: Can be an empty string or a space separated list of numbers ranging from 0 to 100.
Changes Take Effect: Immediately/session

Specifies list of carrier message files associated with result sit_operatorintercept in preconnect mode. The list is a sequence of integer number equal to the index of carrier message previously specified. Example: cpa.preconnectresult.sit_operatorintercept.list = 0 2 4 It means that if incoming message matches with carriermsg.0, carriermsg.2 or carriermsg.4 then CPA outputs result = sit.operatorintercept.

>> Back to Top

cpa.preconnectresult.sit_reorder.list

Default Value:
Valid Values: Can be an empty string or a space separated list of numbers ranging from 0 to 100.

Changes Take Effect: Immediately/session

Specifies list of carrier message files associated with result sit_reorder in preconnect mode. The list is a sequence of integer number equal to the index of carrier message previously specified. Example: cpa.preconnectresult.sit_reorder.list = 0 2 4 It means that if incoming message matches with carriermsg.0, carriermsg.2 or carriermsg.4 then CPA outputs result defined = sit.reorder.

>> Back to Top

cpa.preconnectresult.sit_vacantcircuit.list

Default Value:
Valid Values: Can be an empty string or a space separated list of numbers ranging from 0 to 100.
Changes Take Effect: Immediately/session

Specifies list of carrier message files associated with result sit_vacantcircuit in preconnect mode. The list is a sequence of integer number equal to the index of carrier message previously specified. Example: cpa.preconnectresult.sit_vacantcircuit.list = 0 2 4 It means that if incoming message matches with carriermsg.0, carriermsg.2 or carriermsg.4 then CPA outputs result = sit.vacantcircuit.

>> Back to Top

cpa.priority_machine_machinegreetingdur

Default Value: 1500
Valid Values: A valid machine-favored machine greeting duration must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies machine-favored machine greeting duration (msec) for CPA.

>> Back to Top

cpa.priority_machine_maxvoicesigdur

Default Value: 600
Valid Values: A valid machine-favored maximum voice signal duration must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies machine-favored maximum voice signal duration (msec) for CPA.

>> Back to Top

cpa.priority_machine_voicepausedur

Default Value: 1100

Valid Values: A valid machine-favored voice pause duration must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies machine-favored voice pause duration (msec) for CPA.

>> Back to Top

cpa.priority_normal_machinegreetingdur

Default Value: 1800
Valid Values: A valid normal machine greeting duration must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies normal machine greeting duration (msec) for CPA.

>> Back to Top

cpa.priority_normal_maxvoicesigdur

Default Value: 800
Valid Values: A valid normal maximum voice signal duration must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies normal maximum voice signal duration (msec) for CPA.

>> Back to Top

cpa.priority_normal_voicepausedur

Default Value: 1000
Valid Values: A valid normal voice pause duration must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies normal voice pause duration (msec) for CPA.

>> Back to Top

cpa.priority_voice_machinegreetingdur

Default Value: 2000
Valid Values: A valid voice-favored machine greeting duration must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies voice-favored machine greeting duration (msec) for CPA.

>> Back to Top

cpa.priority_voice_maxvoicesigdur

Default Value: 1100
Valid Values: A valid voice-favored maximum voice signal duration must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies voice-favored maximum voice signal duration (msec) for CPA.

>> Back to Top

cpa.priority_voice_voicepausedur

Default Value: 850
Valid Values: A valid voice-favored voice pause duration must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies voice-favored voice pause duration (msec) for CPA.

>> Back to Top

cpa.ringback

Default Value: na_ringback
Valid Values: Any combination of: "na_ringback", "na_busy", "na_fastbusy", "na_sit_nocircuit", "na_sit_vacantcircuit", "na_sit_operatorintercept", "na_sit_reorder", "standard_fax", "tone1", "tone2", "tone3", "tone4", "tone5", "tone6", "tone7", "tone8", "tone9" and "tone10". Or "none".
Changes Take Effect: At start/restart

Each of the result pattern types ringback, busy, fax, sit nocircuit, sit reorder, sit operatorintercept, sit vacantcircuit, custom1, custom2, custom3, and custom4, has a configuration parameter that sets the list of one or more tone definition names that are mapped to the type. Some pattern types have default tone settings. Specifying "Disable" for a pattern type will disable detection of the type.

The list of tone definition names consist of a set of builtin standard tones and a number of configured custom tones. The builtin tones include NA ringback (North American ringback), NA busy, NA fast busy, Standard fax, NA SIT no circuit, NA SIT vacant circuit, NA SIT operator intercept, NA SIT reorder. Configuration for up to 10 custom tones, named Custom tone 1 through Custom tone 10, each containing one to three segments is supported.

The configuration for each segment includes frequency range for one or two frequencies, on time range, off time range. Specifying zero to min and max for f1 and f2 implicitly disables the segment. Specifying f2 values implicitly enables a second frequency for the segment. Specifying segment2 values implicitly enables a second segment for the tone and so on for segment3. Any not set tone parameters will default to null/disabled values.

In this case, cpa.ringback then specifies tones for CPA's ringback type. Default tone value is builtin

North American ringback (NA ringback). Value "Disable" disables ringback detection. Valid tones include builtins and Custom tone 1 to Custom tone 10.

The builtin North American ringback is composed of three different ringback tones. Each of them has only one segment and is defined as follows:
NA RINGBACK 1: f1=420-445(Hz), f2=475-500(Hz), ontime=720-1280(ms), offtime=1440-2560(ms)
NA RINGBACK 2: f1=420-445(Hz), f2=475-500(Hz), ontime=720-1280(ms), offtime=2160-3840(ms)
NA RINGBACK 3: f1=420-445(Hz), f2=475-500(Hz), ontime=1440-2560(ms), offtime=2880-5120(ms)

>> Back to Top

cpa.sit_nocircuit

Default Value: na_sit_nocircuit
Valid Values: Any combination of: "na_ringback", "na_busy", "na_fastbusy", "na_sit_nocircuit", "na_sit_vacantcircuit", "na_sit_operatorintercept", "na_sit_reorder", "standard_fax", "tone1", "tone2", "tone3", "tone4", "tone5", "tone6", "tone7", "tone8", "tone9" and "tone10". Or "none".
Changes Take Effect: At start/restart

Specifies tones for CPA's SIT no circuit pattern. Default tone value is builtin North American SIT no circuit (NA SIT nocircuit). Value "Disable" disables SIT no circuit detection. Valid tones include builtins and Custom tone 1 to Custom tone 10.

The builtin North American sit no circuit has three segments. Each segment is defined as follows:
Segment 1: f1=950-1020(Hz), f2=0-0(Hz), ontime=320-440(ms), offtime=0-60(ms)
Segment 2: f1=1400-1450(Hz), f2=0-0(Hz), ontime=320-440(ms), offtime=0-60(ms)
Segment 3: f1=1740-1850(Hz), f2=0-0(Hz), ontime=320-440(ms), offtime=0-100(ms)

>> Back to Top

cpa.sit_operatorintercept

Default Value: na_sit_operatorintercept
Valid Values: Any combination of: "na_ringback", "na_busy", "na_fastbusy", "na_sit_nocircuit", "na_sit_vacantcircuit", "na_sit_operatorintercept", "na_sit_reorder", "standard_fax", "tone1", "tone2", "tone3", "tone4", "tone5", "tone6", "tone7", "tone8", "tone9" and "tone10". Or "none".
Changes Take Effect: At start/restart

Specifies tones for CPA's SIT operator intercept pattern. Default tone value is builtin North American SIT operator intercept (NA SIT operator intercept). Value "Disable" disables SIT operator intercept detection. Valid tones include builtins and Custom tone 1 to Custom tone 10.

The builtin North American sit operator intercept has three segments. Each segment is defined as follows:
Segment 1: f1=874-955(Hz), f2=0-0(Hz), ontime=160-300(ms), offtime=0-60(ms)
Segment 2: f1=1310-1430(Hz), f2=0-0(Hz), ontime=160-300(ms), offtime=0-60(ms)
Segment 3: f1=1740-1850(Hz), f2=0-0(Hz), ontime=320-440(ms), offtime=0-100(ms)

>> Back to Top

cpa.sit_reorder

Default Value: na_sit_reorder
Valid Values: Any combination of: "na_ringback", "na_busy", "na_fastbusy", "na_sit_nocircuit", "na_sit_vacantcircuit", "na_sit_operatorintercept", "na_sit_reorder", "standard_fax", "tone1", "tone2", "tone3", "tone4", "tone5", "tone6", "tone7", "tone8", "tone9" and "tone10". Or "none".
Changes Take Effect: At start/restart

Specifies tones for CPA's SIT reorder pattern. Default tone value is builtin North American SIT reorder (NA SIT reorder). Value "Disable" disables SIT reorder detection. Valid tones include builtins and Custom tone 1 to Custom tone 10.

The builtin North American sit reorder has three segments. Each segment is defined as follows:
Segment 1: f1=874-955(Hz), f2=0-0(Hz), ontime=160-300(ms), offtime=0-60(ms)
Segment 2: f1=1400-1450(Hz), f2=0-0(Hz), ontime=320-440(ms), offtime=0-60(ms)
Segment 3: f1=1740-1850(Hz), f2=0-0(Hz), ontime=320-440(ms), offtime=0-100(ms)

>> Back to Top

cpa.sit_vacantcircuit

Default Value: na_sit_vacantcircuit
Valid Values: Any combination of: "na_ringback", "na_busy", "na_fastbusy", "na_sit_nocircuit", "na_sit_vacantcircuit", "na_sit_operatorintercept", "na_sit_reorder", "standard_fax", "tone1", "tone2", "tone3", "tone4", "tone5", "tone6", "tone7", "tone8", "tone9" and "tone10". Or "none".
Changes Take Effect: At start/restart

Specifies tones for CPA's SIT vacant circuit pattern. Default tone value is builtin North American SIT vacant circuit (NA SIT vacantcircuit). Value "Disable" disables SIT vacant circuit detection. Valid tones include builtins and Custom tone 1 to Custom tone 10.

The builtin North American sit vacant circuit has three segments. Each segment is defined as follows:
Segment 1: f1=950-1020(Hz), f2=0-0(Hz), ontime=320-440(ms), offtime=0-60(ms)
Segment 2: f1=1310-1430(Hz), f2=0-0(Hz), ontime=160-300(ms), offtime=0-60(ms)
Segment 3: f1=1740-1850(Hz), f2=0-0(Hz), ontime=320-440(ms), offtime=0-100(ms)

>> Back to Top

cpa.tone1.segment1.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 1 of tone 1 (Hz) for CPA.

>> Back to Top

cpa.tone1.segment1.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 1 of tone 1 (Hz) for CPA.

>> Back to Top

cpa.tone1.segment1.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 1 of tone 1 (Hz) for CPA.

>> Back to Top

cpa.tone1.segment1.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 1 of tone 1 (Hz) for CPA.

>> Back to Top

cpa.tone1.segment1.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 1 of tone 1 (msec) for CPA.

>> Back to Top

cpa.tone1.segment1.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 1 of tone 1 (msec) for CPA.

>> Back to Top

cpa.tone1.segment1.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 1 of tone 1 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone1.segment1.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 1 of tone 1 (msec) for CPA.

>> Back to Top

cpa.tone1.segment2.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 2 of tone 1 (Hz) for CPA.

>> Back to Top

cpa.tone1.segment2.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 2 of tone 1 (Hz) for CPA.

>> Back to Top

cpa.tone1.segment2.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 2 of tone 1 (Hz) for CPA.

>> Back to Top

cpa.tone1.segment2.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 2 of tone 1 (Hz) for CPA.

>> Back to Top

cpa.tone1.segment2.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 2 of tone 1 (msec) for CPA.

>> Back to Top

cpa.tone1.segment2.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 2 of tone 1 (msec) for CPA.

>> Back to Top

cpa.tone1.segment2.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 2 of tone 1 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone1.segment2.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 2 of tone 1 (msec) for CPA.

>> Back to Top

cpa.tone1.segment3.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 3 of tone 1 (Hz) for CPA.

>> Back to Top

cpa.tone1.segment3.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 3 of tone 1 (Hz) for CPA.

>> Back to Top

cpa.tone1.segment3.f2max

Default Value: 0

Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 3 of tone 1 (Hz) for CPA.

>> Back to Top

cpa.tone1.segment3.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 3 of tone 1 (Hz) for CPA.

>> Back to Top

cpa.tone1.segment3.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 3 of tone 1 (msec) for CPA.

>> Back to Top

cpa.tone1.segment3.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 3 of tone 1 (msec) for CPA.

>> Back to Top

cpa.tone1.segment3.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 3 of tone 1 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime

will be matched.

>> Back to Top

cpa.tone1.segment3.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 3 of tone 1 (msec) for CPA.

>> Back to Top

cpa.tone10.segment1.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 1 of tone 10 (Hz) for CPA.

>> Back to Top

cpa.tone10.segment1.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 1 of tone 10 (Hz) for CPA.

>> Back to Top

cpa.tone10.segment1.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 1 of tone 10 (Hz) for CPA.

>> Back to Top

cpa.tone10.segment1.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 1 of tone 10 (Hz) for CPA.

>> Back to Top

cpa.tone10.segment1.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 1 of tone 10 (msec) for CPA.

>> Back to Top

cpa.tone10.segment1.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 1 of tone 10 (msec) for CPA.

>> Back to Top

cpa.tone10.segment1.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 1 of tone 10 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone10.segment1.ontimemin

Default Value: 20

Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 1 of tone 10 (msec) for CPA.

>> Back to Top

cpa.tone10.segment2.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 2 of tone 10 (Hz) for CPA.

>> Back to Top

cpa.tone10.segment2.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 2 of tone 10 (Hz) for CPA.

>> Back to Top

cpa.tone10.segment2.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 2 of tone 10 (Hz) for CPA.

>> Back to Top

cpa.tone10.segment2.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 2 of tone 10 (Hz) for CPA.

>> Back to Top

cpa.tone10.segment2.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 2 of tone 10 (msec) for CPA.

>> Back to Top

cpa.tone10.segment2.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 2 of tone 10 (msec) for CPA.

>> Back to Top

cpa.tone10.segment2.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 2 of tone 10 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone10.segment2.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 2 of tone 10 (msec) for CPA.

>> Back to Top

cpa.tone10.segment3.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 3 of tone 10 (Hz) for CPA.

>> Back to Top

cpa.tone10.segment3.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 3 of tone 10 (Hz) for CPA.

>> Back to Top

cpa.tone10.segment3.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 3 of tone 10 (Hz) for CPA.

>> Back to Top

cpa.tone10.segment3.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 3 of tone 10 (Hz) for CPA.

>> Back to Top

cpa.tone10.segment3.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 3 of tone 10 (msec) for CPA.

>> Back to Top

cpa.tone10.segment3.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 3 of tone 10 (msec) for CPA.

>> Back to Top

cpa.tone10.segment3.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 3 of tone 10 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone10.segment3.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 3 of tone 10 (msec) for CPA.

>> Back to Top

cpa.tone2.segment1.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 1 of tone 2 (Hz) for CPA.

>> Back to Top

cpa.tone2.segment1.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 1 of tone 2 (Hz) for CPA.

>> Back to Top

cpa.tone2.segment1.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 1 of tone 2 (Hz) for CPA.

>> Back to Top

cpa.tone2.segment1.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 1 of tone 2 (Hz) for CPA.

>> Back to Top

cpa.tone2.segment1.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 1 of tone 2 (msec) for CPA.

>> Back to Top

cpa.tone2.segment1.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 1 of tone 2 (msec) for CPA.

>> Back to Top

cpa.tone2.segment1.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 1 of tone 2 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone2.segment1.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 1 of tone 2 (msec) for CPA.

>> Back to Top

cpa.tone2.segment2.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 2 of tone 2 (Hz) for CPA.

>> Back to Top

cpa.tone2.segment2.f1min

Default Value: 0

Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 2 of tone 2 (Hz) for CPA.

>> Back to Top

cpa.tone2.segment2.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 2 of tone 2 (Hz) for CPA.

>> Back to Top

cpa.tone2.segment2.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 2 of tone 2 (Hz) for CPA.

>> Back to Top

cpa.tone2.segment2.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 2 of tone 2 (msec) for CPA.

>> Back to Top

cpa.tone2.segment2.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 2 of tone 2 (msec) for CPA.

>> Back to Top

cpa.tone2.segment2.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 2 of tone 2 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone2.segment2.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 2 of tone 2 (msec) for CPA.

>> Back to Top

cpa.tone2.segment3.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 3 of tone 2 (Hz) for CPA.

>> Back to Top

cpa.tone2.segment3.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 3 of tone 2 (Hz) for CPA.

>> Back to Top

cpa.tone2.segment3.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 3 of tone 2 (Hz) for CPA.

>> Back to Top

cpa.tone2.segment3.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 3 of tone 2 (Hz) for CPA.

>> Back to Top

cpa.tone2.segment3.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 3 of tone 2 (msec) for CPA.

>> Back to Top

cpa.tone2.segment3.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 3 of tone 2 (msec) for CPA.

>> Back to Top

cpa.tone2.segment3.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 3 of tone 2 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone2.segment3.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 3 of tone 2 (msec) for CPA.

>> Back to Top

cpa.tone3.segment1.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 1 of tone 3 (Hz) for CPA.

>> Back to Top

cpa.tone3.segment1.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 1 of tone 3 (Hz) for CPA.

>> Back to Top

cpa.tone3.segment1.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 1 of tone 3 (Hz) for CPA.

>> Back to Top

cpa.tone3.segment1.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 1 of tone 3 (Hz) for CPA.

>> Back to Top

cpa.tone3.segment1.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 1 of tone 3 (msec) for CPA.

>> Back to Top

cpa.tone3.segment1.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 1 of tone 3 (msec) for CPA.

>> Back to Top

cpa.tone3.segment1.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 1 of tone 3 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone3.segment1.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 1 of tone 3 (msec) for CPA.

>> Back to Top

cpa.tone3.segment2.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 2 of tone 3 (Hz) for CPA.

>> Back to Top

cpa.tone3.segment2.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 2 of tone 3 (Hz) for CPA.

>> Back to Top

cpa.tone3.segment2.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 2 of tone 3 (Hz) for CPA.

>> Back to Top

cpa.tone3.segment2.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 2 of tone 3 (Hz) for CPA.

>> Back to Top

cpa.tone3.segment2.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 2 of tone 3 (msec) for CPA.

>> Back to Top

cpa.tone3.segment2.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 2 of tone 3 (msec) for CPA.

>> Back to Top

cpa.tone3.segment2.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 2 of tone 3 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone3.segment2.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 2 of tone 3 (msec) for CPA.

>> Back to Top

cpa.tone3.segment3.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 3 of tone 3 (Hz) for CPA.

>> Back to Top

cpa.tone3.segment3.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 3 of tone 3 (Hz) for CPA.

>> Back to Top

cpa.tone3.segment3.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 3 of tone 3 (Hz) for CPA.

>> Back to Top

cpa.tone3.segment3.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 3 of tone 3 (Hz) for CPA.

>> Back to Top

cpa.tone3.segment3.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 3 of tone 3 (msec) for CPA.

>> Back to Top

cpa.tone3.segment3.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 3 of tone 3 (msec) for CPA.

>> Back to Top

cpa.tone3.segment3.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 3 of tone 3 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone3.segment3.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 3 of tone 3 (msec) for CPA.

>> Back to Top

cpa.tone4.segment1.f1max

Default Value: 0

Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 1 of tone 4 (Hz) for CPA.

>> Back to Top

cpa.tone4.segment1.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 1 of tone 4 (Hz) for CPA.

>> Back to Top

cpa.tone4.segment1.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 1 of tone 4 (Hz) for CPA.

>> Back to Top

cpa.tone4.segment1.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 1 of tone 4 (Hz) for CPA.

>> Back to Top

cpa.tone4.segment1.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 1 of tone 4 (msec) for CPA.

>> Back to Top

cpa.tone4.segment1.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 1 of tone 4 (msec) for CPA.

>> Back to Top

cpa.tone4.segment1.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 1 of tone 4 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone4.segment1.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 1 of tone 4 (msec) for CPA.

>> Back to Top

cpa.tone4.segment2.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 2 of tone 4 (Hz) for CPA.

>> Back to Top

cpa.tone4.segment2.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 2 of tone 4 (Hz) for CPA.

>> Back to Top

cpa.tone4.segment2.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 2 of tone 4 (Hz) for CPA.

>> Back to Top

cpa.tone4.segment2.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 2 of tone 4 (Hz) for CPA.

>> Back to Top

cpa.tone4.segment2.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 2 of tone 4 (msec) for CPA.

>> Back to Top

cpa.tone4.segment2.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 2 of tone 4 (msec) for CPA.

>> Back to Top

cpa.tone4.segment2.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 2 of tone 4 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone4.segment2.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 2 of tone 4 (msec) for CPA.

>> Back to Top

cpa.tone4.segment3.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 3 of tone 4 (Hz) for CPA.

>> Back to Top

cpa.tone4.segment3.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 3 of tone 4 (Hz) for CPA.

>> Back to Top

cpa.tone4.segment3.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 3 of tone 4 (Hz) for CPA.

>> Back to Top

cpa.tone4.segment3.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 3 of tone 4 (Hz) for CPA.

>> Back to Top

cpa.tone4.segment3.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 3 of tone 4 (msec) for CPA.

>> Back to Top

cpa.tone4.segment3.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 3 of tone 4 (msec) for CPA.

>> Back to Top

cpa.tone4.segment3.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 3 of tone 4 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone4.segment3.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 3 of tone 4 (msec) for CPA.

>> Back to Top

cpa.tone5.segment1.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 1 of tone 5 (Hz) for CPA.

>> Back to Top

cpa.tone5.segment1.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 1 of tone 5 (Hz) for CPA.

>> Back to Top

cpa.tone5.segment1.f2max

Default Value: 0

Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 1 of tone 5 (Hz) for CPA.

>> Back to Top

cpa.tone5.segment1.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 1 of tone 5 (Hz) for CPA.

>> Back to Top

cpa.tone5.segment1.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 1 of tone 5 (msec) for CPA.

>> Back to Top

cpa.tone5.segment1.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 1 of tone 5 (msec) for CPA.

>> Back to Top

cpa.tone5.segment1.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 1 of tone 5 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime

will be matched.

>> Back to Top

cpa.tone5.segment1.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 1 of tone 5 (msec) for CPA.

>> Back to Top

cpa.tone5.segment2.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 2 of tone 5 (Hz) for CPA.

>> Back to Top

cpa.tone5.segment2.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 2 of tone 5 (Hz) for CPA.

>> Back to Top

cpa.tone5.segment2.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 2 of tone 5 (Hz) for CPA.

>> Back to Top

cpa.tone5.segment2.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 2 of tone 5 (Hz) for CPA.

>> Back to Top

cpa.tone5.segment2.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 2 of tone 5 (msec) for CPA.

>> Back to Top

cpa.tone5.segment2.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 2 of tone 5 (msec) for CPA.

>> Back to Top

cpa.tone5.segment2.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 2 of tone 5 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone5.segment2.ontimemin

Default Value: 20

Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 2 of tone 5 (msec) for CPA.

>> Back to Top

cpa.tone5.segment3.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 3 of tone 5 (Hz) for CPA.

>> Back to Top

cpa.tone5.segment3.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 3 of tone 5 (Hz) for CPA.

>> Back to Top

cpa.tone5.segment3.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 3 of tone 5 (Hz) for CPA.

>> Back to Top

cpa.tone5.segment3.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 3 of tone 5 (Hz) for CPA.

>> Back to Top

cpa.tone5.segment3.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 3 of tone 5 (msec) for CPA.

>> Back to Top

cpa.tone5.segment3.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 3 of tone 5 (msec) for CPA.

>> Back to Top

cpa.tone5.segment3.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 3 of tone 5 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone5.segment3.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 3 of tone 5 (msec) for CPA.

>> Back to Top

cpa.tone6.segment1.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 1 of tone 6 (Hz) for CPA.

>> Back to Top

cpa.tone6.segment1.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 1 of tone 6 (Hz) for CPA.

>> Back to Top

cpa.tone6.segment1.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 1 of tone 6 (Hz) for CPA.

>> Back to Top

cpa.tone6.segment1.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 1 of tone 6 (Hz) for CPA.

>> Back to Top

cpa.tone6.segment1.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 1 of tone 6 (msec) for CPA.

>> Back to Top

cpa.tone6.segment1.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 1 of tone 6 (msec) for CPA.

>> Back to Top

cpa.tone6.segment1.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 1 of tone 6 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone6.segment1.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 1 of tone 6 (msec) for CPA.

>> Back to Top

cpa.tone6.segment2.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 2 of tone 6 (Hz) for CPA.

>> Back to Top

cpa.tone6.segment2.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 2 of tone 6 (Hz) for CPA.

>> Back to Top

cpa.tone6.segment2.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 2 of tone 6 (Hz) for CPA.

>> Back to Top

cpa.tone6.segment2.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 2 of tone 6 (Hz) for CPA.

>> Back to Top

cpa.tone6.segment2.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 2 of tone 6 (msec) for CPA.

>> Back to Top

cpa.tone6.segment2.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 2 of tone 6 (msec) for CPA.

>> Back to Top

cpa.tone6.segment2.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 2 of tone 6 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone6.segment2.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 2 of tone 6 (msec) for CPA.

>> Back to Top

cpa.tone6.segment3.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 3 of tone 6 (Hz) for CPA.

>> Back to Top

cpa.tone6.segment3.f1min

Default Value: 0

Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 3 of tone 6 (Hz) for CPA.

>> Back to Top

cpa.tone6.segment3.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 3 of tone 6 (Hz) for CPA.

>> Back to Top

cpa.tone6.segment3.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 3 of tone 6 (Hz) for CPA.

>> Back to Top

cpa.tone6.segment3.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 3 of tone 6 (msec) for CPA.

>> Back to Top

cpa.tone6.segment3.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 3 of tone 6 (msec) for CPA.

>> Back to Top

cpa.tone6.segment3.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 3 of tone 6 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone6.segment3.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 3 of tone 6 (msec) for CPA.

>> Back to Top

cpa.tone7.segment1.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 1 of tone 7 (Hz) for CPA.

>> Back to Top

cpa.tone7.segment1.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 1 of tone 7 (Hz) for CPA.

>> Back to Top

cpa.tone7.segment1.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 1 of tone 7 (Hz) for CPA.

>> Back to Top

cpa.tone7.segment1.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 1 of tone 7 (Hz) for CPA.

>> Back to Top

cpa.tone7.segment1.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 1 of tone 7 (msec) for CPA.

>> Back to Top

cpa.tone7.segment1.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 1 of tone 7 (msec) for CPA.

>> Back to Top

cpa.tone7.segment1.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 1 of tone 7 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone7.segment1.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 1 of tone 7 (msec) for CPA.

>> Back to Top

cpa.tone7.segment2.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 2 of tone 7 (Hz) for CPA.

>> Back to Top

cpa.tone7.segment2.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 2 of tone 7 (Hz) for CPA.

>> Back to Top

cpa.tone7.segment2.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 2 of tone 7 (Hz) for CPA.

>> Back to Top

cpa.tone7.segment2.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 2 of tone 7 (Hz) for CPA.

>> Back to Top

cpa.tone7.segment2.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 2 of tone 7 (msec) for CPA.

>> Back to Top

cpa.tone7.segment2.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 2 of tone 7 (msec) for CPA.

>> Back to Top

cpa.tone7.segment2.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 2 of tone 7 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone7.segment2.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 2 of tone 7 (msec) for CPA.

>> Back to Top

cpa.tone7.segment3.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 3 of tone 7 (Hz) for CPA.

>> Back to Top

cpa.tone7.segment3.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 3 of tone 7 (Hz) for CPA.

>> Back to Top

cpa.tone7.segment3.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 3 of tone 7 (Hz) for CPA.

>> Back to Top

cpa.tone7.segment3.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 3 of tone 7 (Hz) for CPA.

>> Back to Top

cpa.tone7.segment3.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 3 of tone 7 (msec) for CPA.

>> Back to Top

cpa.tone7.segment3.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 3 of tone 7 (msec) for CPA.

>> Back to Top

cpa.tone7.segment3.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 3 of tone 7 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone7.segment3.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 3 of tone 7 (msec) for CPA.

>> Back to Top

cpa.tone8.segment1.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 1 of tone 8 (Hz) for CPA.

>> Back to Top

cpa.tone8.segment1.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 1 of tone 8 (Hz) for CPA.

>> Back to Top

cpa.tone8.segment1.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 1 of tone 8 (Hz) for CPA.

>> Back to Top

cpa.tone8.segment1.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 1 of tone 8 (Hz) for CPA.

>> Back to Top

cpa.tone8.segment1.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 1 of tone 8 (msec) for CPA.

>> Back to Top

cpa.tone8.segment1.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 1 of tone 8 (msec) for CPA.

>> Back to Top

cpa.tone8.segment1.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 1 of tone 8 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone8.segment1.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 1 of tone 8 (msec) for CPA.

>> Back to Top

cpa.tone8.segment2.f1max

Default Value: 0

Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 2 of tone 8 (Hz) for CPA.

>> Back to Top

cpa.tone8.segment2.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 2 of tone 8 (Hz) for CPA.

>> Back to Top

cpa.tone8.segment2.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 2 of tone 8 (Hz) for CPA.

>> Back to Top

cpa.tone8.segment2.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 2 of tone 8 (Hz) for CPA.

>> Back to Top

cpa.tone8.segment2.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 2 of tone 8 (msec) for CPA.

>> Back to Top

cpa.tone8.segment2.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 2 of tone 8 (msec) for CPA.

>> Back to Top

cpa.tone8.segment2.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 2 of tone 8 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone8.segment2.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 2 of tone 8 (msec) for CPA.

>> Back to Top

cpa.tone8.segment3.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 3 of tone 8 (Hz) for CPA.

>> Back to Top

cpa.tone8.segment3.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 3 of tone 8 (Hz) for CPA.

>> Back to Top

cpa.tone8.segment3.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 3 of tone 8 (Hz) for CPA.

>> Back to Top

cpa.tone8.segment3.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 3 of tone 8 (Hz) for CPA.

>> Back to Top

cpa.tone8.segment3.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 3 of tone 8 (msec) for CPA.

>> Back to Top

cpa.tone8.segment3.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 3 of tone 8 (msec) for CPA.

>> Back to Top

cpa.tone8.segment3.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 3 of tone 8 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone8.segment3.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 3 of tone 8 (msec) for CPA.

>> Back to Top

cpa.tone9.segment1.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 1 of tone 9 (Hz) for CPA.

>> Back to Top

cpa.tone9.segment1.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 1 of tone 9 (Hz) for CPA.

>> Back to Top

cpa.tone9.segment1.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 1 of tone 9 (Hz) for CPA.

>> Back to Top

cpa.tone9.segment1.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 1 of tone 9 (Hz) for CPA.

>> Back to Top

cpa.tone9.segment1.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 1 of tone 9 (msec) for CPA.

>> Back to Top

cpa.tone9.segment1.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 1 of tone 9 (msec) for CPA.

>> Back to Top

cpa.tone9.segment1.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 1 of tone 9 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone9.segment1.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 1 of tone 9 (msec) for CPA.

>> Back to Top

cpa.tone9.segment2.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 2 of tone 9 (Hz) for CPA.

>> Back to Top

cpa.tone9.segment2.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 2 of tone 9 (Hz) for CPA.

>> Back to Top

cpa.tone9.segment2.f2max

Default Value: 0

Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 2 of tone 9 (Hz) for CPA.

>> Back to Top

cpa.tone9.segment2.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 2 of tone 9 (Hz) for CPA.

>> Back to Top

cpa.tone9.segment2.offtimemax

Default Value: 20
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 2 of tone 9 (msec) for CPA.

>> Back to Top

cpa.tone9.segment2.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 2 of tone 9 (msec) for CPA.

>> Back to Top

cpa.tone9.segment2.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 2 of tone 9 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime

will be matched.

>> Back to Top

cpa.tone9.segment2.ontimemin

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 2 of tone 9 (msec) for CPA.

>> Back to Top

cpa.tone9.segment3.f1max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 1 of segment 3 of tone 9 (Hz) for CPA.

>> Back to Top

cpa.tone9.segment3.f1min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 1 of segment 3 of tone 9 (Hz) for CPA.

>> Back to Top

cpa.tone9.segment3.f2max

Default Value: 0
Valid Values: A valid maximum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum frequency 2 of segment 3 of tone 9 (Hz) for CPA.

>> Back to Top

cpa.tone9.segment3.f2min

Default Value: 0
Valid Values: A valid minimum frequency must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum frequency 2 of segment 3 of tone 9 (Hz) for CPA.

>> Back to Top

cpa.tone9.segment3.offtimemax

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies maximum offtime of segment 3 of tone 9 (msec) for CPA.

>> Back to Top

cpa.tone9.segment3.offtimemin

Default Value: 0
Valid Values: A valid offtime must be a non-negative numeric
Changes Take Effect: At start/restart

Specifies minimum offtime of segment 3 of tone 9 (msec) for CPA.

>> Back to Top

cpa.tone9.segment3.ontimemax

Default Value: 20
Valid Values: A valid ontimemin must be a greater than or equal to 0 numeric
Changes Take Effect: At start/restart

Specifies maximum ontime of segment 3 of tone 9 (msec) for CPA. Setting the value to zero disables checking the ontime against a maximum value, so that any time greater than the minimum ontime will be matched.

>> Back to Top

cpa.tone9.segment3.ontimemin

Default Value: 20

Valid Values: A valid ontimemin must be a greater than or equal to 20 numeric
Changes Take Effect: At start/restart

Specifies minimum ontime of segment 3 of tone 9 (msec) for CPA.

>> Back to Top

cpa.voice_level_db

Default Value: 17.5
Valid Values: A valid voice level must be a number greater than or equal to one
Changes Take Effect: At start/restart

Specifies the active voice signal level (in dB relative to the maximum) for CPA. By default, this value is set to 70% of the default value of Voice range (dB); that is 17.5 dB. The valid range is 1 dB to Voice range (dB) inclusive. If the value is greater than Voice range (dB), it will be set to Voice range (dB).

>> Back to Top

cpa.voice_range_db

Default Value: 25
Valid Values: A valid voice range must be an integer greater than zero
Changes Take Effect: At start/restart

Specifies the minimum signal to noise ratio (or dynamic range) for the CPA signal (in dB). If the difference between the minimum and maximum signal level is less than this threshold, the entire signal is considered to be noise.

>> Back to Top

ctrleventpoollowthreshold

Default Value: 50
Valid Values: A valid value for the ctrleventpoollowthreshold is greater than or equal to 0 and less than or equal to 100.
Changes Take Effect: At start/restart

Once the mpc.ctrleventpoolthreshold value is reached for an individual event pool, the number of used events in that pool must drop below the low threshold value before calls can be accepted. Only enabled if mpc.ctrleventpoolthreshold is non-zero. The value is in percentage (%).

>> Back to Top

ctrleventpoolthreshold

Default Value: 75
Valid Values: A valid value for the ctrleventpoolthreshold is greater than or equal to 0 and less than or equal to 100.
Changes Take Effect: At start/restart

Specified a threshold for the percentage (%) of events in an individual media event pool can be reached before the MCP will start rejecting calls. Once reached, the number of used events must drop below the percentage specified in mpc.ctrleventpoollowthreshold before calls will be accepted again. When set to 0, this functionality is disabled.

>> Back to Top

default_audio_format

Default Value: ULAW
Valid Values: Choose between: ULAW or ALAW
Changes Take Effect: At start/restart

Default audio format used by the MCP

>> Back to Top

dsp.g726littleendian

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

This parameter specifies whether input/output of the G.726 data is in big-endian or in little-endian order. In addition to determining the order of the generated G.726 data, the incoming G.726 data order is assumed to be in the order specified by this parameter. 0 - Big-Endian 1 - Little-Endian

>> Back to Top

dsp.g729a

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

Specifies whether to use G.729 Annex A for G.729 transcoding.

>> Back to Top

dtmf.detectedge

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

Specifies whether a DTMF will be recognized on the "rising" edge (1st RFC2833 packet), or on the "falling" edge (when any of the following event happens: 1st RFC2833 packet with "E" bit set, upon receipt of a RTP packet that is not for the same DTMF event, or after the maximum silence gap timeout.

>> Back to Top

dtmf.duration

Default Value: 200
Valid Values: Possible values are integers from 10 to 1000 inclusive
Changes Take Effect: At start/restart

Specifies the duration (in milliseconds) of outgoing RFC2833 DTMF packets. Default value is 200.

>> Back to Top

dtmf.gap

Default Value: 100
Valid Values: Possible values are integers from 10 to 1000 inclusive.
Changes Take Effect: At start/restart

Specifies the gap between an outgoing RFC2833 DTMF packet and the following outgoing packet in milliseconds.

>> Back to Top

dtmf.inband_amplitude

Default Value: 15000
Valid Values: Possible values are integers from 0 to 32,767 inclusive.
Changes Take Effect: At start/restart

Specifies the amplitude for inband dtmf generator. The higher the the value, the greater the output amplitude in terms of dB. The default value of 15000 gives approximately -20dB while 3000 gives approximately -35dB for example.

>> Back to Top

dtmf.maxsilence

Default Value: 20
Valid Values: mpc.dtmf.maxsilence must be an integer that is at least equal to 0 and less than or equal to 120.
Changes Take Effect: At start/restart

The maximum silence permitted between same inband DTMF tones in ms to be considered no longer part of the same DTMF.

>> Back to Top

dtmf.minduration

Default Value: 0
Valid Values: mpc.dtmf.minduration 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

Specifies the minimum duration of DTMF events in ms (either inband or RFC2833) required before a DTMF is detected by the dialog. Must be greater than or equal to 0ms.

>> Back to Top

dtmf.multidtmfonetimestamp

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

Specifies whether the RFC2833 packets of multiple DTMFs will have the same timestamp. If it is true, the End bit is used to differentiate the DTMFs.

>> Back to Top

dtmf.pauseduration

Default Value: 200
Valid Values: Possible values are integers from 10 to 1000 inclusive
Changes Take Effect: At start/restart

Specifies the duration (in milliseconds) for the duration of a pause ('p') DTMF.

>> Back to Top

dtmf.singlepacket

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

When set to Disable, outgoing DTMF are represented by multiple (depends on mpc.dtmf.duration) RFC2833 packets followed by 3 RFC2833 packets with the End bit set. When set to Enable, outgoing DTMF are represented by a single RFC2833 packet with the End bit set.

>> Back to Top

fcr.defaultdtmfhandling

Default Value: as-is
Valid Values: as-is: (default) Record everything as-is from the RTP stream. Inband DTMFs will be recorded, but RFC2833 digits will not no-digits: Strip out all DTMF digits. This includes inband or RFC2833. NOTE: When telephone-event is negotiated on the call, if inband audio DTMFs are received, they will not be removed from the recording. all-digits: Record all DTMF digits, including inband, and generate audio for RFC2833 digits
Changes Take Effect: Immediately/session

Specifies the recording behavior for DTMFs in a Full Call Recording.

>> Back to Top

fcr.gain

Default Value: 0
Valid Values: The number must be an integer from -30 to 30 inclusive
Changes Take Effect: At start/restart

Gain (in dB from -30 to 30) applied to audio used in Full Call Recording (both input from the caller and output to the caller) from call participants.

>> Back to Top

font_paths_linux

Default Value: /usr/share/fonts/default/ghostscript
Valid Values: Please specify a valid '|' separated list of font folder paths.
Changes Take Effect: At start/restart

List of paths of font directories on a Linux MCP system, separated by the delimiter '|'. This information is used by the Video Text Overlay feature. All the font files are scanned at start-up, and their font name to file name mapping information is cached for fast look-up later. An empty value will disable the feature. The special value "default" can be used for the builtin default value.

>> Back to Top

font_paths_win

Default Value: C:/Windows/Fonts
Valid Values: Please specify a valid '|' separated list of font folder paths.
Changes Take Effect: At start/restart

List of paths of font directories on a Windows MCP system, separated by the delimiter '|'. This information is used by the Video Text Overlay feature. All the font files are scanned at start-up, and their font name to file name mapping information is cached for fast look-up later. An empty value will disable the feature. The special value "default" can be used for the builtin default value.

>> Back to Top

g722.maxptime

Default Value: 0
Valid Values: Choose between: 0, 10, 20, 30, 40, 60, 80 or 100.
Changes Take Effect: Immediately

If the MCP is offering the SDP, or answering the SDP where the offer does not have the maxptime, the maxptime attribute will be set according to this configuration. If this configuration does not exist, or is disabled (0), the maxptime attribute will not be sent unless the SDP offer had the maxptime attribute. In the case where other codecs in the SDP also specify maxptime, the configuration of the codec listed before this codec will take precedence.

>> Back to Top

g722.ptime

Default Value: 0
Valid Values: Choose between: 0, 10, 20, 30, 40, 60, 80 or 100.
Changes Take Effect: Immediately

If the MCP is offering the SDP or answering the SDP where the offer does not have the ptime, the ptime attribute will be set according to this configuration. This configuration is also used as the transmission rate of this codec when the remote SDP does not specify the ptime attribute. Note that transmission rate will default to 20ms if this configuration is disabled. If disabled (0), ptime attribute will not be sent unless the SDP offer had the ptime attribute. In the case where the other codecs in the SDP also specify the configured ptime, the configuration of the codec listed before this codec will take precedence.

>> Back to Top

g726_32.maxptime

Default Value: 0
Valid Values: Choose between: 0, 10, 20, 30, 40 or 60.
Changes Take Effect: Immediately

If the MCP is offering the SDP, or answering the SDP where the offer does not have the maxptime, the maxptime attribute will be set according to this configuration. If this configuration does not exist, or is disabled (0), the maxptime attribute will not be sent unless the SDP offer had the maxptime attribute. In the case where other codecs in the SDP also specify maxptime, the configuration of the codec listed before this codec will take precedence.

>> Back to Top

g726_32.ptime

Default Value: 0
Valid Values: Choose between: 0, 10, 20, 30, 40 or 60.
Changes Take Effect: Immediately

If the MCP is offering the SDP or answering the SDP where the offer does not have the ptime, the ptime attribute will be set according to this configuration. This configuration is also used as the transmission rate of this codec when the remote SDP does not specify the ptime attribute. Note that transmission rate will default to 20ms if this configuration is disabled. If disabled (0), ptime attribute will not be sent unless the SDP offer had the ptime attribute. In the case where the other codecs in the SDP also specify the configured ptime, the configuration of the codec listed before this codec will take precedence.

>> Back to Top

g729.fmtp

Default Value:
Valid Values: Can be an empty string or choose between: "annexb=yes" or "annexb=no"
Changes Take Effect: At start/restart

Specifies the default G729 fmtp option string used by the platform when initiating SDP offer or answering SDP offer. When initiating SDP offer, if No fmtp is selected, fmtp attribute line for G729 will not be present in SDP offered by the platform. If annexb enabled is selected, fmtp attribute line for G729 will be present as "annexb=yes". If annexb disabled is selected, fmtp attribute line for G729 will be shown as "annexb=no". When answering to an SDP offer with a valid G729 fmtp line, this parameter has no effect and the platform will reply to the offer with the same fmtp line. When answering to an SDP offer without an fmtp line or with an invalid G729 fmtp line, the platform will reply to the offer using this configuration value with the same rule as initiating SDP offer.

>> Back to Top

g729.maxptime

Default Value: 0
Valid Values: Choose between: 0, 10, 20, 30, 40, 60, 80 or 100.
Changes Take Effect: Immediately

If the MCP is offering the SDP, or answering the SDP where the offer does not have the maxptime, the maxptime attribute will be set according to this configuration. If this configuration does not exist, or is disabled (0), the maxptime attribute will not be sent unless the SDP offer had the maxptime attribute. In the case where other codecs in the SDP also specify maxptime, the configuration of the codec listed before this codec will take precedence.

>> Back to Top

g729.ptime

Default Value: 0
Valid Values: Choose between: 0, 10, 20, 30, 40, 60, 80 or 100.
Changes Take Effect: Immediately

If the MCP is offering the SDP or answering the SDP where the offer does not have the ptime, the ptime attribute will be set according to this configuration. This configuration is also used as the transmission rate of this codec when the remote SDP does not specify the ptime attribute. Note that transmission rate will default to 20ms if this configuration is disabled. If disabled (0), ptime attribute will not be sent unless the SDP offer had the ptime attribute. In the case where the other codecs in the SDP also specify the configured ptime, the configuration of the codec listed before this codec will take precedence.

>> Back to Top

gsm.maxptime

Default Value: 0
Valid Values: Choose between: 0, 20, 40, 60, 80 or 100.
Changes Take Effect: immediately

If the MCP is offering the SDP, or answering the SDP where the offer does not have the maxptime, the maxptime attribute will be set according to this configuration. If this configuration does not exist, or is disabled (0), the maxptime attribute will not be sent unless the SDP offer had the maxptime attribute. In the case where other codecs in the SDP also specify maxptime, the configuration of the codec listed before this codec will take precedence.

>> Back to Top

gsm.ptime

Default Value: 0

Valid Values: Choose between: 0, 20, 40, 60, 80 or 100.
Changes Take Effect: immediately

If the MCP is offering the SDP or answering the SDP where the offer does not have the ptime, the ptime attribute will be set according to this configuration. This configuration is also used as the transmission rate of this codec when the remote SDP does not specify the ptime attribute. Note that transmission rate will default to 20ms if this configuration is disabled. If disabled (0), ptime attribute will not be sent unless the SDP offer had the ptime attribute. In the case where the other codecs in the SDP also specify the configured ptime, the configuration of the codec listed before this codec will take precedence.

>> Back to Top

h263_1998payload

Default Value: 99
Valid Values: A valid H263-1998 payload can only be an integer from 96 to 127 inclusive
Changes Take Effect: At start/restart

Default payload type number to use for the H263-1998 codec

>> Back to Top

h263.fmtp

Default Value:
Valid Values: <token>[;<token>...][|<token>[;<token>...]...]
Changes Take Effect: At start/restart

Specifies the SDP fmtp line offered and accepted by MCP for H263 and H263-1998. The value is in the format: <token>[;<token>...][|<token>[;<token>...]...] Note that the list of tokens are grouped by separating them by a vertical bar - each group of tokens represent a separate SDP fmtp line. When more than 1 fmtp's are specified, H263-1998 negotiation will use all of the fmtp's as the local fmtp (for example offer generation will generate 3 payloads for 3 fmtp's). For H263, only the first fmtp will be used as the local fmtp.

Following tokens are accepted: profile=<profile> level=<level> SQCIF=<mpi> QCIF=<mpi> CIF=<mpi> CIF4=<mpi> CIF16=<mpi> CUSTOM=<max width>,<max height>,<mpi> F=1 I=1 J=1 T=1 K=1 N=1 P=1

profile - Profile from 0 to 8 can be specified. level - Level from 10 to 70 are supported. SQCIF - Specifies 128 x 96 video resolution with fps @ 30000 / (1001 * mpi) QCIF - Specifies 176 x 144 video resolution with fps @ 30000 / (1001 * mpi) CIF - Specifies 352 x 288 video resolution with fps @ 30000 / (1001 * mpi) CIF4 - Specifies 704 x 480 video resolution with fps @ 30000 / (1001 * mpi) CIF16 - Specifies 1408 x 1152 video resolution with fps @ 30000 / (1001 * mpi) CUSTOM - Specifies custom video resolution with fps @ 30000 / (1001 * mpi) F=1 - Specifies that annex F (from ITU-T Recommendation H.263, January 2005) is supported. I=1 - Specifies that annex I (from ITU-T Recommendation H.263, January 2005) is supported. J=1 - Specifies that annex J (from ITU-T Recommendation H.263, January 2005) is supported. T=1 - Specifies that annex T (from ITU-T

Recommendation H.263, January 2005) is supported. K=1 - Specifies that annex K (from ITU-T Recommendation H.263, January 2005) is supported. Not supported when H263 transcoding is enabled. N=1 - Specifies that annex N (from ITU-T Recommendation H.263, January 2005) is supported. Not supported when H263 transcoding is enabled. P=1 - Specifies that annex P (from ITU-T Recommendation H.263, January 2005) is supported.

Please see RFC4629 for more details.

If H263 transcoding is enabled for the session, the fmtp containing the following tokens will not be offered and also not accepted by MCP: - profile value other than 0 - K=1 - N=1

If H263 transcoding is enabled and h263.fmtp is not specified, the following fmtp value will be set by default: profile=0;level=70|profile=0;level=70;F=1;I=1;J=1;T=1;P=1 If H263 transcoding is disabled and h263.fmtp is not specified, no fmtp will be generated in the offer and all fmtp's will be accepted by MCP. If H263 transcoding is disabled and h263.fmtp is not specified, fmtp negotiation will be done without the transcoding restrictions imposed on the allowed tokens.

>> Back to Top

h264.fmtp

Default Value: profile=b; level=3.1; packetization-mode=*;|profile=cb; level=3.1; packetization-mode=*;|profile=m; level=3.1; packetization-mode=*;
Valid Values: Please check the parameter description.
Changes Take Effect: At start/restart

Specifies the H264 SDP profile, level and packetization mode offered and accepted by the MCP. Set to one or more fmtp text values separated by the '|' character. One fmtp text is in the form of "profile=X; level=Y; packetization-mode=Z;".

X is an element of the set {*, b, cb, m, e, h, h10, h10i, h42, h42i, h44, h44i, c44i} specifying the H264 profile offered and accepted by the MCP. In the set, * is used as the wildcard to allow the MCP to offer and accept any valid profile. The rest of the set are profiles defined by H264 whose full name are (in respective order as the aforementioned set): {baseline, constrained baseline, main, extended, high, high 10, high 10 intra, high 4:2:2, high 4:2:2 intra, high 4:4:4, high 4:4:4 intra, cavlc 4:4:4 intra}. Invalid profile value will be replaced with * (wildcard).

Y is an element of the set {*, 1, 1b, 1.1, 1.2, 1.3, 2, 2.1, 2.2, 3, 3.1, 3.2, 4, 4.1, 4.2, 5, 5.1} specifying the H264 level of the corresponding profiles offered and accepted by the MCP. In the set, * is used as the wildcard to allow MCP to offer and accept any valid level for its corresponding profile. The rest of the set are levels defined by H264. Invalid level value will be replaced with * (wildcard).

Z is an element of the set {*, 0, 1} specifying the H264 packetization mode offered and accepted by the MCP. Similar to the others, * is used as the wildcard to allow the MCP to offer and accept any valid packetization mode. 0 refers to single NALU packetization mode while 1 demands non-interleaved packetization capability. The MCP does not support interleaved packetization mode, as well as, any value other than stated. Invalid packetization-mode value will be replaced with 0 (single NALU).

During SDP negotiation, each fmtp text value without wildcard will be translated to one H264 media fmtp line while those with wildcard will be translated to one or more H264 media fmtp line equivalent to the wildcard.
For example, profile=b; level=1.1; packetization-mode=* which is the first part of the default will be

translated to two H264 media fmtp lines of profile-level-id=42000B; packetization-mode=0; and profile-level-id=42000B; packetization-mode=1;. Note that profile "b" is equivalent to 66 in decimal or 42 in hexadecimal and level "1.1" is equivalent to level 11 in decimal or level 0B in hexadecimal.
According to RFC3984, the use of profile-level-id and packetization-mode during capability exchange must be negotiated symmetrically except the level part can be downgraded. For example, the MCP is configured with h264.fmtp="profile=b; level=1; packetization-mode=1;" and it receives an offer with H264 media fmtp line of profile-level-id=420033; packetization-mode=1; which is equivalent to h264.fmtp="profile=b; level=5.1; packetization-mode=1". In this case, the profile and packetization-mode of the platform and the offer are symmetric but the level parts are not. This offer will be accepted by the MCP with level downgrade in its response, e.g. "profile-level-id=42000A; packetization-mode=1". The offerer when receiving the response will know that the answerer has accepted the offer but the level must be downgraded and the offerer will have to produce the H264 content accordingly when proceeding with this response.
Another example, the MCP is configured with h264.fmtp="profile=b; level=5.1; packetization-mode=1" and it receives an offer with H264 media fmtp line of profile-level-id-42000A; packetization-mode=1; which is equivalent to h264.fmtp="profile=b; level=1; packetization-mode=1". In this case, the profile and packetization-mode of the platform and the offer are symmetric but the level parts are not. This offer will still be accepted by the MCP without level downgrade in its response, e.g. "profile-level-id=42000A; packetization-mode=1;". The MCP accepts the offer because it is configured with a higher level which is capable of processing any lower level. The offerer will receive the response that the MCP has accepted the offer.

H264 transcoder does not support extended and advanced 4:4:4 profiles. Consequently, if H264 transcoding is enabled for the session, the fmtp containing one of the following profiles (whether enumerated by * or explicitly configured) will not be offered and also not accepted during the SDP negotiation: {e, h44, h44i, c44i}

>> Back to Top

h264.in_band_param_sets_only

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

This parameter specifies the utilization of sprop-parameter-sets attributes of the initial SDP offered to MCP. It does not; however, apply to any SDP offered by MCP as MCP does not send any sprop-parameter-sets in its SDP offering to another party.
When set to Disable (default), if any profile-level-id plus packetization-mode in the initial offered SDP is accepted by MCP without level downgrade, MCP will utilize the H264 parameter sets value provided by sprop-parameter-sets attributes if present and valid. Refer to H264 FMTP for more detail on how profile-level-id and packetization-mode are negotiated.
When set to Enable, MPC will not utilize any H264 parameter sets value provided by sprop-parameter-sets attributes in the offered SDP. Attribute in-band-parameter-sets=1 will be included in the response SDP for any H264 media line to explicitly declare that only parameter sets received via RTP will be utilized and that implicitly forces the offerer to include all parameter sets within RTP packets.

>> Back to Top

h264payload

Default Value: 113
Valid Values: A valid H264 payload can only be an integer from 96 to 127 inclusive
Changes Take Effect: At start/restart

Default payload type number to use for the H264 codec

>> Back to Top

health.maxprocessingtime

Default Value: 600000
Valid Values: mpc.health.maxprocessingtime must be an integer no less than 0.
Changes Take Effect: At start/restart

Specifies the maximum processimg time of media thread in milliseconds. If a media thread is processing a media object more than the maximum processing time, meaning the thread may fall into an inifinite loop or deadlock, MCP will be terminated. Default value is 600000. If it is set to 0, MCP will not check processing time at all.

>> Back to Top

health.waittime

Default Value: 0
Valid Values: mpc.health.waittime must be an integer no less than 0.
Changes Take Effect: At start/restart

Specifies the wait time in milliseconds for Health Thread to check the health of media threads periodically. It is reasonable to set health.waittime smaller than health.maxprocessingtime. Default value is 0, meaning MCP will not perform health check. Note: do not enable health check unless it is really necessary, e.g. MCP has to restart in order to recover from a stuck situation.

>> Back to Top

includeavpfinsdp

Default Value: none
Valid Values: Choose between: "none", "audio", "video" or "audioandvideo".
Changes Take Effect: Immediately/session

Sets if the MCP will include SAVPF / AVPF instead of SAVP / AVP in SDP. If set to "none" (default), SAVP / AVP will be used. If set to "audio", only audio will have SAVPF / AVPF. If set to "video", only video will have SAVPF / AVPF. If set to "audioandvideo", both audio and video will have SAVPF / AVPF.

>> Back to Top

maxmediathreads

Default Value: 16
Valid Values: mpc.maxmediathreads must be an integer greater than 0 and less than or equal to 100
Changes Take Effect: At start/restart

Specifies the maximum number of media threads that can be created within MPC. Default value is 16. It is highly recommended to use the default setting.

>> Back to Top

maxrecordencryptedfilesize

Default Value: 120000000
Valid Values: mpc.maxrecordencryptedfilesize 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

When encrypting of recorded media files is enabled, this parameter specifies the maximum file size. Encrypted recordings will stop when this limit (bytes) is exceeded. If encryption is enabled for a recording, the media is kept in memory and only written to disk at the end of the recording. This parameter limits the amount of memory that can be used for one recording. The default value of 120 MByte, is large enough to store 2 hours for 2 channels each at 64 Kbits/sec. Value of 0 disables this limit.

>> Back to Top

maxrecordfilesize

Default Value: 0
Valid Values: mpc.maxrecordfilesize is greater than or equal to 0 and less than or equal to 4000000000.
Changes Take Effect: Immediately/session

All recordings (regular and FCR) will stop when this limit (bytes) is exceeded. Note that the recorded file will usually exceed this limit by a few hundred bytes depending on the codec and the container chosen. Value of 0 disables this limit.

>> Back to Top

media.senddtmfdropaudio

Default Value: 1

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

Specifies the behavior of dtmf transmission when there are overlapping dtmf events and audio data. When the value is set to Enable, audio whose timestamp overlaps with dtmf will be dropped. When the value is set to Disable, audio timestamp shifting will be invoked to avoid overlapping.

>> Back to Top

mediamgr.audiobuffersize

Default Value: 102400
Valid Values: Possible values are integer values greater than or equal to 1024 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

Specifies the audio buffer size for the non-TTS source (in bytes). Default value is 102400.

>> Back to Top

mediamgr.autorecordformatselect

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

This parameter can enable a mode where regular recording or FCR encoding format is determined based on the incoming content format and the formats supported by the container. Note that auto detection only applies for the cases where the recording MIME string specifies only the container and not the codec/videocodec parameter. For example, if recording MIME is specified as "video/x-avi" without the videocodec parameter and if the incoming stream is H264, the resulting recording file will be an AVI with the H264 format. If this parameter was disabled, specifying "video/x-avi" would always result in AVI with the H263 format being recorded (since H263 is the default format for AVI).

>> Back to Top

mediamgr.CA_directory

Default Value:
Valid Values: Can be an empty string or a valid path to the Certificate Authority folder.
Changes Take Effect: Immediately/session

Path to the Certificate Authority folder for MSML file-based call recording. This parameter has lower priority than CA_file and if file is set directory is not used.

>> Back to Top

mediamgr.CA_file

Default Value:
Valid Values: Can be an empty string or a valid path to the Certificate Authority certificate file.
Changes Take Effect: Immediately/session

Path to the Certificate Authority certificate file for MSML file-based call recording. This parameter has higher priority than CA_directory.

>> Back to Top

mediamgr.enableEODdoublecheck

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

Enables END of DATA double check. This is needed for the files created by GVPi that are written in shorter temporary files.

>> Back to Top

mediamgr.h263overrideTR

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

This parameter is for video recording with H263 and H263-1998 video codec. Whenever video/audio out-of-sync happens in recorded files, enabling this parameter may solve the issue. By default the MCP uses an inherent property available in each H263 video sample called Temporal Reference to determine timing between each video sample in a recording session. Video/audio out-of-sync in recorded files, however, may occur if the Temporal References in the video frames are incorrect. Setting this parameter to Enable will allow the MCP to correct Temporal Reference and try to synchronize video and audio during recording sessions. Setting this parameter to Disable will keep the Temporal Reference intact.

>> Back to Top

mediamgr.hlsconsecutiveerrorsthreshold

Default Value: 5
Valid Values: Must be an integer of value equal to 0 to indicate no limit, or any value greater or equal to 1 to impose a limit.
Changes Take Effect: Immediately

Specifies the number of HTTP Live Streaming (HLS) segment fetching errors allowed to happen consecutively before giving up the fetching process. If the value is equal to 0, than MCP will try to fetch the segments until there are segments to be fetched, or until there is still content in the buffer to be played.

>> Back to Top

mediamgr.hlstotalerrorsthreshold

Default Value: 20
Valid Values: Must be an integer of value equal to 0 to indicate no limit, or any value greater or equal to 1 to impose a limit.
Changes Take Effect: Immediately

Specifies the total number of HTTP Live Streaming (HLS) segment errors allowed to happen before giving up the fetching process. This value must be equal or greater than the specified by the parameter mediamgr.hlsallowedconsecutiveerrors. If the value is equal to 0, than MCP will try to fetch the segments until there are segments to be fetched, or until there is still content in the buffer to be played. The following chart exemplifies how both thresholds work: | Segment# | Fetch result | Cons. Counter | Total Counter | | 1 | Good | 0 | 0 | | 2 | Fail | 1 | 1 | | 3 | Fail | 2 | 2 | | 4 | Good | 0 | 2 | | 5 | Fail | 1 | 3 |

>> Back to Top

mediamgr.ignore_cert_err

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

Specifies whether to ignore certificate verification errors and continue encrypting the media for MSML file-based call recording.

>> Back to Top

mediamgr.isofilerecordheadersize

Default Value: 55000
Valid Values: mpc.mediamgr.isofilerecordheadersize 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

The header of ISO file container grows as the content of the file grows. The MCP will reserve the header size to harddrive before recording media of an ongoing session. The MCP will actually record header at the end of the session and harddrive operations may be required if the reserved header size is not enough to accommodate the actual header size.

>> Back to Top

mediamgr.maxcertificatecachesize

Default Value: 2000000
Valid Values: mpc.mediamgr.maxcertificatecachesize must be an integer that is greater than or equal to 20000 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

This parameter sets the maximum size of the cached memory in bytes to store certificates for MSML recordings.

>> Back to Top

mediamgr.maxcertificatelength

Default Value: 5000
Valid Values: mpc.mediamgr.maxcertificatelength must be an integer that is greater than or equal to 1 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

This parameter sets the maximum length in characters of one certificate for MSML file-based call recording. If certificate will be longer than this length it will not be used for encryption of MSML recording.

>> Back to Top

mediamgr.maxcertificatesperprofile

Default Value: 10
Valid Values: mpc.mediamgr.maxcertificatesperprofile must be an integer that is greater than or equal to 1 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

This parameter sets the maximum number of certificates for MSML file-based call recording per IVR profile.

>> Back to Top

mediamgr.precacheprofileforcallrecording.0

Default Value:
Valid Values: Can be an empty string or a stringin the format: "[TENANT_NAME].IVR_PROFILE_NAME".

Changes Take Effect: At start/restart

IVR profile information for pre-caching of encryption related parameters for call recording. If not specified, the encryption parameters will be cached when the profile is first accessed. The format of the profile information should strictly follow "[TENANT_NAME].IVR_PROFILE_NAME".

>> Back to Top

mediamgr.precacheprofileforcallrecording.1

Default Value:
Valid Values: Can be an empty string or a stringin the format: "[TENANT_NAME].IVR_PROFILE_NAME".
Changes Take Effect: At start/restart

IVR profile information for pre-caching of encryption related parameters for call recording. If not specified, the encryption parameters will be cached when the profile is first accessed. The format of the profile information should strictly follow "[TENANT_NAME].IVR_PROFILE_NAME".

>> Back to Top

mediamgr.precacheprofileforcallrecording.2

Default Value:
Valid Values: Can be an empty string or a stringin the format: "[TENANT_NAME].IVR_PROFILE_NAME".
Changes Take Effect: At start/restart

IVR profile information for pre-caching of encryption related parameters for call recording. If not specified, the encryption parameters will be cached when the profile is first accessed. The format of the profile information should strictly follow "[TENANT_NAME].IVR_PROFILE_NAME".

>> Back to Top

mediamgr.precacheprofileforcallrecording.3

Default Value:
Valid Values: Can be an empty string or a stringin the format: "[TENANT_NAME].IVR_PROFILE_NAME".
Changes Take Effect: At start/restart

IVR profile information for pre-caching of encryption related parameters for call recording. If not specified, the encryption parameters will be cached when the profile is first accessed. The format of the profile information should strictly follow "[TENANT_NAME].IVR_PROFILE_NAME".

>> Back to Top

mediamgr.precacheprofileforcallrecording.4

Default Value:
Valid Values: Can be an empty string or a stringin the format: "[TENANT_NAME].IVR_PROFILE_NAME".
Changes Take Effect: At start/restart

IVR profile information for pre-caching of encryption related parameters for call recording. If not specified, the encryption parameters will be cached when the profile is first accessed. The format of the profile information should strictly follow "[TENANT_NAME].IVR_PROFILE_NAME".

>> Back to Top

mediamgr.precacheprofileforcallrecording.5

Default Value:
Valid Values: Can be an empty string or a stringin the format: "[TENANT_NAME].IVR_PROFILE_NAME".
Changes Take Effect: At start/restart

IVR profile information for pre-caching of encryption related parameters for call recording. If not specified, the encryption parameters will be cached when the profile is first accessed. The format of the profile information should strictly follow "[TENANT_NAME].IVR_PROFILE_NAME". If additional profiles are wanted, new parameters with an incremental number at the end need to be added.

>> Back to Top

mediamgr.rec_iframe_delay_threshold

Default Value: 160
Valid Values: mpc.mediamgr.rec_iframe_delay_threshold must be an integer at least equal to -1 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

This parameter is for video recording with audio and video. When starting a recorder, a few initial video frames may be dropped as the first self-referencing intra frame is not received for some reasons. As a result, audio duration received prior to receiving the next self-referencing video frame may be too long and it makes audio and video get out-of-sync. This parameter limits how long in milliseconds the audio is allowed in this situation without having to do video filling. The value of -1 will disable this feature.

>> Back to Top

mediamgr.recordmp3audiobuffer

Default Value: 4000
Valid Values: mpc.mediamgr.recordmp3audiobuffer must be an integer that is greater than or equal

to 2000.
Changes Take Effect: At start/restart

Specifies the duration of the audio buffer in milliseconds for MP3 recording.

>> Back to Top

mediamgr.recordrtphinttrack

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

For ISO file container, recording a hint track for a media track into a recording file allows the file to be streamed when placed on a streaming server.

>> Back to Top

mediamgr.recordwritetimeinterval

Default Value: 1000
Valid Values: mpc.mediamgr.recordwritetimeinterval must be an integer equal to 0, or greater than or equal to 1000 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

This parameter sets the time period in milliseconds for the periodic writing of recording data to a file and must be an integer equal to 0, or greater than or equal to 1000. If time interval is set to 0 it means that time driven recording is disabled.

>> Back to Top

mediamgr.rtsplowerbufferthreshold

Default Value: 100
Valid Values: mpc.mediamgr.rtsplowerbufferthreshold 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

If mpc.media.rtsppause is set to 1, and RTP streaming has been paused. PLAY will be sent to resume RTP streaming if the packet buffer size has reduced to the lower threshold. Default value is 100 packets. The lower threshold must be smaller than the upper threshold. This value can be overridden using the RTSP URL parameter "vg-rtsp-lowerbufferthreshold".

>> Back to Top

mediamgr.rtsppause

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

Select the option based on RTSP server support for PAUSE. This value can be overridden using the RTSP URL parameter "vg-rtspserver-pause". 0 - PAUSE is not supported by the RTSP server 1 - PAUSE is supported by the RTSP server

>> Back to Top

mediamgr.rtspplayrange

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

Select the option based on RTSP server support for the Range parameter in a PLAY request. This value can be overridden using the RTSP URL parameter "vg-rtspserver-playrange". 0 - PLAY is not supported by the RTSP server 1 - PLAY is supported by the RTSP server

>> Back to Top

mediamgr.rtspupperbufferthreshold

Default Value: 200
Valid Values: mpc.mediamgr.rtspupperbufferthreshold 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

If mpc.media.rtsppause is set to 1, PAUSE will be sent to stop RTP streaming when the packet buffer size has reached the upper threshold. Default value is 200 packets. This value can be overridden using the RTSP URL parameter "vg-rtsp-upperbufferthreshold".

>> Back to Top

mediamgr.sharedhttpservers

Default Value:
Valid Values: Can be an empty string or a list of space separated network addresses.
Changes Take Effect: At start/restart

Specifies the live HTTP server addresses (without port) delimited by space - address can be a hostname, IPv4, or IPv6 address.
e.g. genesyslab.com [fe80:0:0:0:200:f8ff:fe21:67cf] 192.168.0.101 dummyhost 192.168.0.102

3ffe:1900:4545:3:200:f8ff:fe21:67cf
If HTTP URL play request has streaming turned on and the URL address is one of the addresses specified by this configuration, the HTTP URL will be played in live HTTP streaming mode.
In live HTTP streaming mode, multiple sessions specifying the same URL will play from the same HTTP stream, and newly starting sessions will start playing from the currently arriving media.

>> Back to Top

mediamgr.strictsamplingrate

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

The sampling rate that is officially supported for audio is 8000 Hz and video is 90000 Hz. Some media files may indicate a different sampling rate than what supported and trying to play those files may result in bad media quality. If this parameter is set to Enable, media files indicating any sampling rate other than officially supported will not be played. If this parameter is set to Disable, media files indicating any sampling rate other than supported will still be attempted to play by MCP but without guarantee quality.

>> Back to Top

mediamgr.videobuffersize

Default Value: 256000
Valid Values: Possible values are integer values greater than or equal to 8000 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

Specifies the video buffer size for non-TTS source (in bytes). This value should be sufficient for buffering up to 1 second of all supported modes of H263 and H264 video stream. Refer to the appropriate specification, e.g. ITU-T H.263 for H.263 and ITU-T H.264 for H.264, and GVP User Guide to determine the size to set to avoid overrunning the video buffer.

>> Back to Top

mediamgr.videofillingframeduration

Default Value: 1000
Valid Values: mpc.mediamgr.videofillingframeduration must be an integer that is greater than 32 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

This parameter is for video recording with audio and video. It is used when video filling happens, e.g. the total duration of video frames dropped exceeds mpc.mediamgr.rec_iframe_delay_threshold. When doing video filling, the duration of between the first and second recorded video frame will be stretched so that synchronization between audio and video is maintained. This parameter limits how long the duration in milliseconds between two video frames can be stretched and guides the recorder to regenerate more than one video frame until it completes video filling duration. Note that the value of this parameter should not exceed that of mpc.mediamgr.maxdurationpervidframe. Half the value of mpc.mediamgr.maxdurationpervidframe is recommended and is set as the default.

>> Back to Top

mediamgr.videofillingthreshold

Default Value: 2000
Valid Values: mpc.mediamgr.videofillingthreshold must be a postive integer that is 0 or greater and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

This parameter is for video recording. It is used to decide when to trigger video filling; i.e., when the interval between the current and the last frame exceeds this threshold, video filling will be done on the next I-frame for this gap, with a new frame being created for each "videofillingframeduration". This parameter is in milliseconds, and this feature can be disabled by setting this to 0 or a large value.

>> Back to Top

mixer.audiodelay_flush_all_threshold

Default Value: 500
Valid Values: mpc.mixer.audiodelay_flush_all_threshold must be an integer that is at least 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

Specifies the maximum difference between the current and expected packet time stamps when mixer flushes all buffered packets. The units are in milliseconds. Default value is 500. Setting to zero disables flushing.

>> Back to Top

mixer.audiodelay_flush_silence_threshold

Default Value: 100
Valid Values: mpc.mixer.audiodelay_flush_silence_threshold must be an integer that is at least 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

Specifies the maximum difference between the current and expected silent packet time stamps when mixer flushes silent buffered packets. The units are in milliseconds. Default value is 100. Setting to zero disables flushing.

>> Back to Top

mp3.bitrate

Default Value: 16
Valid Values: Choose between: 8, 16, 24, 32, 48, 64, 96, 128, 160, 192, 256 or 320.
Changes Take Effect: Immediately/session

This specifies the MP3 encoding bitrate in Kbits/Second, which will determine the quality and size of a recorded MP3 file. Beware that bitrates above 160 kbps are not supported when sampling rate is less than 32 KHz, i.e., 16 KHz, as per MPEG 2 Layer 3 standard. 8 kbps bitrate is supported only for mono MP3 recording (for GIR only). Note that integer transcoding is not supported for bitrates lower than 32 kbps. For bitrates lower than 32 kbps, the sampling rate will be forced to 16 KHz, and MPEG 2 Layer 3 will be used.

>> Back to Top

mp3.compression_level_current_encoder

Default Value: 7
Valid Values: A number between 1 and 9 inclusive.
Changes Take Effect: Immediately/session

This parameter can be used to specify the quality level of the mp3 file from the current encoder, with 1 the highest and 9 the lowest quality. This parameter takes effect only when [mpc].mp3.use_current_encoder is true.

>> Back to Top

mp3.interfrequency.encoding

Default Value:
Valid Values: Can be an empty string or one of the following: 8 or 16.
Changes Take Effect: At start/restart

This can be used to specify the intermediate PCM16 format frequency as 8 or 16 KHz for MP3 encoding. By default, when this value is empty, the most suitable frequency based on the input format will be selected, except in the case of Call Recording, which would pick 8KHz by default.

>> Back to Top

mp3.samplingrate

Default Value: 32
Valid Values: Choose between: 16, 32 or 48.
Changes Take Effect: Immediately/session

This specifies the MP3 sampling rate used in encoding, in KHz. MPEG 1 Layer 3 standard is used for encoding when the sampling rate is 32 KHz or higher, while MPEG 2 Layer 3 standard is used when it is lower. Beware that 16 KHz is not supported when MP3 integer transcoder option is enabled. 48 KHz is not supported during MSML call recording.

>> Back to Top

mp3.use_current_encoder

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

This parameter can be used to specify whether to use the current encoder for Stereo MP3 Encoding or not. If not, the Legacy version will be used.

>> Back to Top

mp3.use_integer_transcoder

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

This can be used to specify the type of MP3 transcoder. When set to false, a floating point implementation is used; else if set to true, an integer implementation is used.

>> Back to Top

mp3.use_integer_transcoder_current_encoder

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

This parameter can be used to specify the type of the current MP3 transcoder. When set to true, an integer implementation is used. If set to false, a floating point implementation is used. This parameter takes effect only when [mpc].mp3.use_current_encoder is true.

>> Back to Top

numdispatchthreads

Default Value: 1
Valid Values: mpc.numdispatchthreads must be an integer greater than 0 and less than or equal to 32
Changes Take Effect: At start/restart

Specifies the number of media dispatching threads.

>> Back to Top

opus.apptype

Default Value: voice
Valid Values: voice: VoIP Application that mostly uses speech. It may alter the output sound to make it more intelligible. audio: Application that uses music and speech. It provides lower coding delay.
Changes Take Effect: Immediately/session

Used to indicate the intended application type to the Opus encoder.

>> Back to Top

opus.bitrate

Default Value: 0
Valid Values: A number 0 for Opus default, or 6 to 510 for bitrate in kbps
Changes Take Effect: Immediately/session

This specifies the Opus maximum encoding bitrate in Kbits/second, or 0 to use Opus codec default (which is 12 kbps for NB codecs). Per RFC 6716, recommended values are 8-12 kbps for NB speech and 16-20 kbps for WB speech.

>> Back to Top

opus.complexity

Default Value: 10
Valid Values: A number between 0 and 10 inclusive.
Changes Take Effect: Immediately/session

Specifies Opus encoder's computational complexity. The range is 0 to 10, inclusive. The higher the value, the higher the complexity and the audio quality.

>> Back to Top

opus.fmtp

Default Value: useinbandfec=1
Valid Values: [useinbandfec=(0|1)] [; maxaveragebitrate=(6000-510000)]
Changes Take Effect: At start/restart

Specifies the default OPUS fmtp option string used by the platform when initiating SDP offer or

answering SDP offer. If the fmtp parameter is empty, the fmtp attribute line for OPUS will not be present in SDP offered by the platform.
The supported fmtp parameters are:
"useinbandfec" specifies whether MCP will take advantage of Opus in-band FEC or not. Opus in-band FEC helps mitigate errors when unstable transmissions occur. Possible values for "useinbandfec" are 1 and 0. If no value is specified, then in-band FEC will not be applied. For better error recovering results, the corresponding "maxaveragebitrate" should be set to a higher value, e.g. 48000.
"maxaveragebitrate" specifies the maximum average bitrate. Sending out this ftmp serves as a mandate to the remote end to not send a stream with average birate higher than the "maxaveragebitrate" value, as it might overload our network and/or receiver. Possible values for "maxaveragebitrate" are any integer in the range from 6000 to 510000 inclusive. If no value is specified, the bitrate will be automatically decided by MCP according to the audio source.
Unsupported fmtp parameters: usedtx; cbr; stereo; sprop-stereo; maxplaybackrate; sprop-maxcapturerate.

>> Back to Top

opus.packetloss

Default Value: 20
Valid Values: A number between 0 and 100 inclusive.
Changes Take Effect: Immediately/session

Used to indicate the expected packet loss percentage to the Opus encoder. The range is 0 to 100, inclusive. Higher values will give progressively more loss resistant behavior, at the expense of quality at a given bitrate in the lossless case, but greater quality under loss. The default value is 20, implying 20 percent packet loss is expected.

>> Back to Top

opuspayload

Default Value: 116
Valid Values: A valid Opus payload can only be an integer from 96 to 127 inclusive
Changes Take Effect: At start/restart

Default payload type number to use for the Opus codec

>> Back to Top

pcma.maxptime

Default Value: 0
Valid Values: Choose between: 0, 10, 20, 30, 40, 60, 80 or 100.
Changes Take Effect: Immediately

If the MCP is offering the SDP, or answering the SDP where the offer does not have the maxptime, the maxptime attribute will be set according to this configuration. If this configuration does not exist, or is disabled (0), the maxptime attribute will not be sent unless the SDP offer had the maxptime attribute. In the case where other codecs in the SDP also specify maxptime, the configuration of the codec listed before this codec will take precedence.

>> Back to Top

pcma.ptime

Default Value: 0
Valid Values: Choose between: 0, 10, 20, 30, 40, 60, 80 or 100.
Changes Take Effect: Immediately

If the MCP is offering the SDP or answering the SDP where the offer does not have the ptime, the ptime attribute will be set according to this configuration. This configuration is also used as the transmission rate of this codec when the remote SDP does not specify the ptime attribute. Note that transmission rate will default to 20ms if this configuration is disabled. If disabled (0), ptime attribute will not be sent unless the SDP offer had the ptime attribute. In the case where the other codecs in the SDP also specify the configured ptime, the configuration of the codec listed before this codec will take precedence.

>> Back to Top

pcmu.maxptime

Default Value: 0
Valid Values: Choose between: 0, 10, 20, 30, 40, 60, 80 or 100.
Changes Take Effect: Immediately

If the MCP is offering the SDP, or answering the SDP where the offer does not have the maxptime, the maxptime attribute will be set according to this configuration. If this configuration does not exist, or is disabled (0), the maxptime attribute will not be sent unless the SDP offer had the maxptime attribute. In the case where other codecs in the SDP also specify maxptime, the configuration of the codec listed before this codec will take precedence.

>> Back to Top

pcmu.ptime

Default Value: 0
Valid Values: Choose between: 0, 10, 20, 30, 40, 60, 80 or 100.
Changes Take Effect: Immediately

If the MCP is offering the SDP or answering the SDP where the offer does not have the ptime, the ptime attribute will be set according to this configuration. This configuration is also used as the transmission rate of this codec when the remote SDP does not specify the ptime attribute. Note that transmission rate will default to 20ms if this configuration is disabled. If disabled (0), ptime attribute will not be sent unless the SDP offer had the ptime attribute. In the case where the other codecs in the SDP also specify the configured ptime, the configuration of the codec listed before this codec will take precedence.

>> Back to Top

persistdympayfmtpair

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

With regards to RFC3264, a history of mappings from payload to format per m-line should be maintained for a session. This is to ensure a dynamic payload assigned to a particular format per m-line will not be reused for a different format when given a reINVITE and asked for an offer. When enabled, the aforementioned behavior will be performed. Note that a given reINVITE with an offer will be responded with regards to, if any, the given dynamic payloads, not the maintained payloads, due to backward-compatibility. When disabled, the legacy GVP method, where history is not remembered, will be used.

>> Back to Top

playcache.checkversiontime

Default Value: 300
Valid Values: The parameter must be set to integer of value 0 or greater.
Changes Take Effect: Immediately/session

This parameter sets the time period for checking that the source media of a cache entry has changed. This parameter does not apply to http://, https://, and file:// URL types, see note below.

When a entry in the cache is played, the source media will be checked for change if it has not been checked within this time period. If source media has been found to change the cache file(s) will be recreated using the changed media. Setting the value to zero will cause a check to be performed for every play. The value is set in seconds. The default value is 300.

For http://, https://, and file:// URL types, the checking of the source media for changes is handled by the fetching module so this parameter does not apply. For these URL types, if the media content provided by the fetching module changes it will be used on the next play. An exception to this is that for file:// URL types, this parameter does not apply if the prompt is played using the MSML <play> tag with precheck disabled.

>> Back to Top

playcache.directory

Default Value: $installationRoot$/cache/play
Valid Values: The parameter must be set to a directory path.
Changes Take Effect: At start/restart

This parameter sets the root directory of the play cache.

>> Back to Top

playcache.enable

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

This parameter enables the use of the play cache for media playing. When enabled, media played from http://, file://, rtsp://, and qtmf:// URL types will utilize the play cache. When transcoding is required to play the audio or video media from a source URL to an endpoint with particular audio and or video codecs settings, the play cache will save the transcoded media to audio and or video track file(s), and the media will be played from these track files the next time the URL is played to an endpoint with the same (or compatible) codecs settings. The play cache is enabled by default.

>> Back to Top

playcache.expiretime

Default Value: 24:00
Valid Values: The parameter must be set to format hours:minutes or hours, where hours and minutes are numeric values
Changes Take Effect: At start/restart

This parameter sets expire time for media URL entries in the play cache. If the amount of time since an entry for a media URL has been played exceeds this time, the entry will be deleted from the play cache. The format is hours:minutes or hours. Setting the value to zero disables deleting based on expire time. The default value is 24:00.

>> Back to Top

playcache.maxsize

Default Value: 500
Valid Values: The parameter must be set to integer greater than or equal to zero.
Changes Take Effect: At start/restart

This parameter sets the maximum disk space for the play cache. If the amount of disk space used by the play cache exceeds this value, cache entries will be deleted, starting with the least recently played. The value is set in MBytes. Setting the value to zero disables deleting based on disk spaced used. The default value is 500.

>> Back to Top

playremoteeodtimeout

Default Value: 10000
Valid Values: mpc.playremoteeodtimeout must be an integer greater than 0
Changes Take Effect: At start/restart

Specifies the duration in milliseconds to wait for remote buffer end of data callback. Playback by platform may involve data buffering locally and remotely, e.g. MCP as the local entity and PSTN-C as the remote one. After the local entity sends its very last packet to the remote, an EOD request will be issued to the remote entity where it will have to respond when its very last packet has been played. If there is no reply from the remote within this period, the local entity will issue a timeout on waiting and proceed.

>> Back to Top

playremoteflushtimeout

Default Value: 10000
Valid Values: mpc.playremoteflushtimeout must be an integer greater than 0
Changes Take Effect: At start/restart

Specifies the duration in milliseconds to wait for remote buffer flush callback. Playback by platform may involve data buffering locally and remotely, e.g. MCP as the local entity and PSTN-C as the remote one. After the local entity flushes its buffer, a flush request will be issued to the remote entity where it will have to respond. If there is no reply from the remote within this period, the local entity will issue a timeout on waiting and proceed.

>> Back to Top

playsilencefill

Default Value: 160
Valid Values: mpc.playsilencefill must be an integer that is greater than or equal to 0 and less than or equal to 1000.
Changes Take Effect: At start/restart

Specifies the amount of silence fill in milliseconds to add at the end of prompt play. Default is 160. Setting to zero disables play silence fill.

>> Back to Top

preferredipinterface

Default Value: V4
Valid Values: Choose between: V4 or V6
Changes Take Effect: Immediately

Specifies the preferred IP interface to use (IPv4 or IPv6) when performing SDP negotiation. In particular, this will be used to set the root connection attribute in SDP answers, and set the connection attribute in SDP offers.

>> Back to Top

record.allowsyncdiskwrite

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

Specifies whether synchronous write during recording is allowed.

>> Back to Top

record.defaultdtmfhandling

Default Value: as-is
Valid Values: as-is: (default) Record everything as-is from the RTP stream. Inband DTMFs will be recorded, but RFC2833 digits will not no-digits: Strip out all DTMF digits. This includes inband or RFC2833. NOTE: When telephone-event is negotiated on the call, if inband audio DTMFs are received, they will not be removed from the recording. all-digits: Record all DTMF digits, including inband, and generate audio for RFC2833 digits
Changes Take Effect: Immediately/session

Specifies the recording behavior for DTMFs in a Simple Recording.

>> Back to Top

recordcachedir

Default Value: $installationRoot$/cache/record
Valid Values: The parameter must be set to a directory path.
Changes Take Effect: At start/restart

This parameter sets the temporary recording cache directory in case of MSML call recording. Once the recording completes the the recording files are removed from the cache directory after successfully placing them at the final recording destination.

>> Back to Top

recordnumparallelpost

Default Value: 30
Valid Values: mpc.recordnumparallelpost 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

While doing MSML call recording the recordings are added to a list if they need to be posted to Amazon S3, Call Recording API, HTTP/HTTPS or SpeechMiner. A separate posting thread wakes up from time to time and works on the list of recordings to be posted. This parameter specifies the max. number of active (post in progress) post attempts in the system at any given time. The default value is 30, which means 30 active record posts can exist in the system at a given time. Setting this parameter to 0 disables recordings from being posted/moved to final destination and the recording files remain in the record cache directory forever.

>> Back to Top

recordpostbacklogthreshold

Default Value: 25
Valid Values: mpc.recordpostbacklogthreshold must be an integer that is greater than or equal to 1 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

While doing MSML call recording the recordings are added to a list if they need to be posted to Amazon S3, Call Recording API, HTTP/HTTPS or SpeechMiner. A separate posting thread wakes up from time to time and works on the list of recordings to be posted. If due to any reason the posting thread lags behind, then we send an alarm notification as soon as the post backlog reaches or exceeds the threshold limit specified by this parameter. We send another alarm notification when the post backlog is below the configured threshold. The default value is 25, which means that we send an alarm when the post backlog reaches or exceeds 25 posts.

>> Back to Top

recordpostinterval

Default Value: 15000
Valid Values: mpc.recordpostinterval must be an integer that is greater than or equal to 1 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

While doing MSML call recording the recordings are added to a list if they need to be posted to Amazon S3, Call Recording API, HTTP/HTTPS or SpeechMiner. A separate record posting thread wakes up from time to time and works on the list of records to be posted. This parameter specifies the time gap between consecutive processing attempts by this thread. The unit for this parameter is milliseconds and the default value is 15 seconds (15000 milliseconds).

>> Back to Top

recordpostretrybackoff

Default Value: 120000

Valid Values: mpc.recordpostretrybackoff 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

While doing MSML call recording the recordings are added to a list if they need to be posted to Amazon S3, Call Recording API, HTTP/HTTPS or SpeechMiner. A separate posting thread wakes up from time to time and works on the list of recordings to be posted. This parameter specifies the backoff period between consecutive post retry attempts. This only applies to recording entries whose posting failed the first time and needs to be retried again. The unit for this parameter is milliseconds and the default value is 120 seconds (120000 milliseconds), which means that the posting thread would attempt post retries once every 2 minutes approximately. Setting this parameter to 0 causes all retry attempts to occur at the same time without any wait period.

>> Back to Top

recordpostretrycount

Default Value: 3
Valid Values: mpc.recordpostretrycount 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

While doing MSML call recording the recordings are added to a list if they need to be posted to Amazon S3, Call Recording API, HTTP/HTTPS or SpeechMiner. A separate posting thread wakes up from time to time and works on the list of recordings to be posted. This parameter specifies the max. number of retry attempts made for failed posting attempts. After the specified number of attempts the failing recording is removed from the list of recordings to be posted and is never retried again. The default value is 3, which means failed post attempts would be retried a maximum of 3 times. Setting this parameter to 0 disables any retry attempts for posts having recoverable errors.

>> Back to Top

refframereqonconnjoin

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

Enables requesting of intra-frames when there is a join or a bridge between connections / calls.

>> Back to Top

rru.beginsilence

Default Value: 1000
Valid Values: The value must be an integer from 0 to 10000 inclusive
Changes Take Effect: At start/restart

Specifies the amount of begin silence in milliseconds to insert for RRU. Default is 1000.

>> Back to Top

rru.endsilence

Default Value: 3000
Valid Values: The value must be an integer from 0 to 10000 inclusive
Changes Take Effect: At start/restart

Specifies the amount of end silence in milliseconds to insert for RRU. Default is 3000.

>> Back to Top

rtcp.tos

Default Value: 0
Valid Values: Possible values are integers from 0 to 255 inclusive.
Changes Take Effect: Immediately/session

Specifies the IP Differentiated Services Field (also known as ToS) to set in all outgoing audio RTCP packets. 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.

>> Back to Top

rtcp.tos.video

Default Value: 0
Valid Values: Possible values are integers from 0 to 255 inclusive.
Changes Take Effect: Immediately/session

Specifies the IP Differentiated Services Field (also known as ToS) to set in all outgoing video RTCP packets. 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.

>> Back to Top

rtcpfeedback.audio

Default Value: allow
Valid Values: Choose between: "force", "allow" or "disable".
Changes Take Effect: Immediately/session

Sets the behavior for RTCP feedback. If set to "allow" (default) the MCP will be enabled to send Generic NACK messages as per RFC 4585 Section 6.2.1 when the far end sends SAVPF or AVPF in SDP. If set to "force", the MCP will enable these messages independent of SDP. If set to "disable", the MCP will disable these messages independent of SDP. This configuration parameter covers audio.

>> Back to Top

rtcpfeedback.video

Default Value: allow
Valid Values: Choose between: "force", "allow" or "disable".
Changes Take Effect: Immediately/session

Sets the behavior for RTCP feedback. If set to "allow" (default) the MCP will be enabled to send Generic NACK messages as per RFC 4585 Section 6.2.1 and RTCP PLI as per RFC 4584 section 6.3.1, when the far end sends SAVPF or AVPF in SDP. If set to "force", the MCP will enable these messages independent of SDP. If set to "disable", the MCP will disable these messages independent of SDP. This configuration parameter covers video.

>> Back to Top

rtp.activetimeout

Default Value: 0
Valid Values: mpc.rtp.activetimeout should be an integer 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

MPC will not send the first outgoing RTP packet until it received an incoming RTP packet or the RTP active timeout is reached. This value is time in milliseconds. Default to 0, in which RTP packets will be transmitted immediately.

>> Back to Top

rtp.audiobuffersize

Default Value: 50000
Valid Values: mpc.rtp.audiobuffersize 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

Specifies the size of the buffer used for sending audio RTP data in bytes. If 0 is specified, buffer size will be initially set to 120000, and will be increased automatically if more space is needed.

>> Back to Top

rtp.dejitter.delay

Default Value: 0
Valid Values: rtp.dejitter.delay must be an integer that is greater than or equal to 0 and less than or equal to 10000.
Changes Take Effect: At start/restart

Specifies the total duration (in milliseconds) of RTP packets to buffer for the inter-arrival dejittering purpose. This will translate to an initial delay before the packets are dispatched internally for further processing. 0 disables the inter-arrival jitter removal functionality.

>> Back to Top

rtp.dejitter.timeout

Default Value: 200
Valid Values: rtp.dejitter.timeout must be an integer that is greater than or equal to 1 and less than or equal to 1000.
Changes Take Effect: At start/restart

Controls how long the buffered RTP packet will wait for the missing RTP (in milliseconds). If timeout occurs, the dispatch process is initiated regardless of the missing packet.

>> Back to Top

rtp.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

>> Back to Top

rtp.dtmf.receive

Default Value: SIPINFO INBAND
Valid Values: Any combination of: SIPINFO and INBAND. Or "none".
Changes Take Effect: Immediately/session

Specifies the allowable ways to receive DTMF in an RTP session if telephone-event (RFC2833) is not negotiated in SDP. Allowable values are to support DTMFs relayed over SIP INFO messages and/or over INBAND audio DTMFs. The default selection is to enable both, however inband DTMF will not be supported if telephone-event is negotiated. SIP INFO will be supported if selected here whether or not telephone-event is negotiated. If support neither is selected on it's own will result in neither being supported. SIPINFO - Support DTMFs relayed over SIP INFO messages INBAND - Support inband audio DTMFs none - Support neither

>> Back to Top

rtp.dtmf.send

Default Value: INBAND
Valid Values: Choose between: SIPINFO or INBAND.
Changes Take Effect: Immediately/session

Specifies the allowable ways to send DTMF in an RTP session if telephone-event (RFC2833) is not negotiated. SIPINFO - Support sending DTMFs over SIP INFO messages INBAND - Support sending inband audio DTMFs

>> Back to Top

rtp.enablertcp

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

Specifies whether to transmit RTCP packets.

>> Back to Top

rtp.fixedsocketthreads

Default Value: 8
Valid Values: Possible values are integers from 0 to 100 inclusive.
Changes Take Effect: At start/restart

Specifies the fixed number of RTP socket threads. Fixed number of RTP socket threads specified by this parameter will be allocated at the start-up time, and no new RTP threads will be created during run-time. If set to 0: 1 RTP thread will be created at start-up time, and new RTP threads will be created in proportion to the number of open sockets during run-time. Setting this parameter to 0 is not recommended. Instead this parameter should be set in proportion to the number of CPU cores in the system.

>> Back to Top

rtp.h264allowrfc3984stapa

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

Specifies whether RFC3984 single-time aggregation packet type A (STAPA) can be used when non-interleaved packetization mode is negotiated. When non-interleaved mode is negotiated as the packet transport mode, single NAL unit, STAPA and fragmentation type A packets will be sent by default. Alternatively, this configuration, when set to Disable, can allow only single NAL unit and fragmentation type A packets to be used.

>> Back to Top

rtp.inputmode

Default Value: vad
Valid Values: Choose between: "continuous" or "vad"
Changes Take Effect: At start/restart

Specifies the input mode of incoming RTP streams: continuous - Continuous input; vad - VAD input.

>> Back to Top

rtp.localaddr

Default Value: $LocalIP$
Valid Values: Can be an empty string or a valid IPv4 address.
Changes Take Effect: At start/restart

mpc.rtp.localaddr provides configurability of the connection part (IPv4) of SDP messages sent by the MCP.
If this parameter is not specified, then the IP Address of the local system will be used.

>> Back to Top

rtp.localaddrv6

Default Value:
Valid Values: Can be an empty string or a valid IPv6 address.
Changes Take Effect: At start/restart

mpc.rtp.localaddr provides configurability of the connection part (IPv6) of SDP messages sent by the MCP.
If this parameter is not specified, then the IP Address of the local system will be used.

>> Back to Top

rtp.maxrtppacketsize

Default Value: 0
Valid Values: mpc.rtp.maxrtppacketsize 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

Specifies the maximum size of RTP packets that are sent from the platform in bytes. This also controls the maximum size of the SRTP packets being sent. If 0 is specified, there is no limit - unless internal buffer specified by rtp.audiobuffersize or rtp.videobuffersize runs out of space. Note that for SRTP, huge packet sizes (above 80KB which is greater than the typical 1500 MTU limit) may cause SRTP encryption errors before being sent out. If the problem is encountered for very large video packets, it can be worked around by negotiating lower level/bitrate or by leveraging codec specific transport mechanisms (e.g. packetization-mode=1 SDP fmtp for H264).

>> Back to Top

rtp.multichantimeout

Default Value: 60000
Valid Values: mpc.rtp.multichantimeout 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

Specifies the RTP timeout value in milliseconds for multichannel recordings. A RTP stream will be considered inactive if there has been no activity for the timeout period. A value of 0 disables this timeout. Default value is 60000.

>> Back to Top

rtp.overwritessrcandtimestamp

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

Set to Enable to have the SSRC and timestamp of outgoing RTP packets overwritten during a media bridge. Setting to Disable would result in legacy VG Platform behavior. Setting to Enable is required for SRTP operations, and with certain devices that have problems with receiving inconsistent SSRC and timestamp information.

>> Back to Top

rtp.packetseq

Default Value: 0
Valid Values: mpc.rtp.packetseq 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

Specifies the sequence number for the first outgoing RTP packet. IF set to 0, the first sequence number will be randomly generated for each RTP stream. Default value is 0.

>> Back to Top

rtp.portrange

Default Value: 20000-45000
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

Specifies the RTP ports to be used by MPC.

>> Back to Top

rtp.prefilltime

Default Value: 200
Valid Values: Possible values are integers from 100 to 1000 inclusive.
Changes Take Effect: At start/restart

Specifies the time (milliseconds) limit in which the pre-fill amount needs to be sent out by. If the value is M milliseconds and the pre-fill amount is N milliseconds, then the RTP packets will be sent out at (N/M) times the real-time rate for M milliseconds. When in faster than realtime and N/M results in less than double the real-time rate, N/M will be set to double the real-time rate. Possible values are 100 to 1000, inclusive. Default value is 200.

>> Back to Top

rtp.request_iframe

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

Allows/disallows requesting of video intra-frames. Intra-frames require more bandwith, but improve video quality.

>> Back to Top

rtp.restrictsource

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

Specifies whether to allow dropping packets from other sources (filtering).

>> Back to Top

rtp.rfc2429maxpacketsize

Default Value: 1400
Valid Values: mpc.rtp.rfc2429maxpacketsize 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

Specifies the maximum RTP packet size for RFC2429 packets in bytes. Specifies the maximum RTP packet size for H263 RFC2429 packets in bytes. Any packet that exceeds the limit will be broken down into smaller packets. This parameter is used to prevent the OS from sending fragmented UDP packets, which may not be supported by some devices.
Default value is 1400. Set to 0 to disable the limit.

>> Back to Top

rtp.sendmode

Default Value: vad
Valid Values: Choose between: "continuous" or "vad"
Changes Take Effect: At start/restart

Specifies the output mode of outgoing RTP streams: continuous - Continuous output; vad - VAD output.

>> Back to Top

rtp.senduponrecv

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

Specifies whether defer sending of RTP packets until valid RTP packets are received.

>> Back to Top

rtp.source_buffer_video_data_size

Default Value: 0
Valid Values: rtp.source_buffer_video_data_size must be an integer that is greater than or equal to 0 and less than or equal to 50000000.
Changes Take Effect: Immediately/session

Specifies the maximum amount of video media data (in bytes) that the RTP source buffer can contain. If set to zero, the value will be determined automatically based on the video bitrate.

If video conferencing with video_output_type set to mixed is to be utilized, the platform will buffer the last video IFrame and subsequent packets received for each conference participant. This parameter determines the amount of video data that can be buffered.

The default value zero is correct for most applications.

>> Back to Top

rtp.source_buffer_video_size

Default Value: 500
Valid Values: rtp.source_buffer_video_size must be an integer that is greater than or equal to 200 and less than or equal to 2000.
Changes Take Effect: Immediately/session

Specifies the maximum number of packets that the RTP source video buffer can contain. The default value 500 is correct for most applications.

If video conferencing with video_output_type set to mixed is to be utilized, the platform will buffer the last video IFrame and subsequent packets received for each conference participant. This parameter sets the number of packets that can be buffered. It should be set to the maximum expected input IFrame interval (in packet count) plus 20. For example, if a device will be connected that sends an IFrame every 600 packets, the value should be set to 620.

>> Back to Top

rtp.statisticsinterval

Default Value: 300000
Valid Values: Possible values are integers from 0 to 3600000 inclusive.
Changes Take Effect: At start/restart

Specifies the interval (in ms) at which statistics logging in the RTP layer will be logged. Setting this value to 0 will disable the statistics logging. If enabled, will log when an RTP connection is destroyed, regardless of interval.

>> Back to Top

rtp.timeout

Default Value: 60000
Valid Values: mpc.rtp.timeout 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

Specifies the RTP timeout value in milliseconds. A RTP stream will be considered inactive if there has been no activity for the timeout period. A value of 0 disables this timeout. Default value is 60000.

>> Back to Top

rtp.tos

Default Value: 0
Valid Values: Possible values are integers from 0 to 255 inclusive.
Changes Take Effect: Immediately/session

Specifies the IP Differentiated Services Field (also known as ToS) to set in all outgoing audio RTP packets. 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.

>> Back to Top

rtp.tos.video

Default Value: 0
Valid Values: Possible values are integers from 0 to 255 inclusive.
Changes Take Effect: Immediately/session

Specifies the IP Differentiated Services Field (also known as ToS) to set in all outgoing video RTP packets. 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.

>> Back to Top

rtp.video.udprecvbuffersize

Default Value: 60480
Valid Values: mpc.rtp.udpbuffersize 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

Specifies the size of the receive buffer for video RTP UDP sockets in bytes. Default value is 60480. If set to zero the buffer size will be set to the default for the operating system.

>> Back to Top

rtp.video.udpsendbuffersize

Default Value: 60480
Valid Values: rtp.video.udpsendbuffersize 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

Specifies the size of the send buffer for video RTP UDP sockets in bytes. Default value is 60480. If set to zero the buffer size will be set to the default for the operating system.

>> Back to Top

rtp.videobuffersize

Default Value: 0
Valid Values: mpc.rtp.videobuffersize 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

Specifies the size of the buffer used for sending RTP video data in bytes. This value should be sufficient for buffering up to 1 second of all supported modes of H263 and H264 video stream. Refer to the appropriate specification, e.g. ITU-T H.263 for H.263 and ITU-T H.264 for H.264, and GVP User Guide to determine the size to set to avoid overrunning the video buffer. If 0 is specified, buffer size will be initially set to 120000, and will be increased automatically if more space is needed.

>> Back to Top

rtp.vp8maxpacketsize

Default Value: 1400
Valid Values: mpc.rtp.vp8maxpacketsize 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

Specifies the maximum RTP packet size for VP8 packets in bytes. Any VP8 packet that exceeds the limit will be broken down into smaller packets. This parameter is used to prevent the OS from sending fragmented UDP packets, which may not be supported by some devices.
Default value is 1400. Set to 0 to disable the limit.

>> Back to Top

rtsp.connection.portrange

Default Value: 14000-15999
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:

Specifies the available ports to receive RTSP messages from RTSP servers.

>> Back to Top

rtsp.localaddr

Default Value:
Valid Values: Can be an empty string or a valid IPv4 address.
Changes Take Effect: At start/restart

Specifies the IPv4 interface to receive RTSP messages from RTSP servers. If this parameter is not specified, then the IP Address of the local system will be used. Note that most RTSP servers require this parameter and [mpc]rtsp.rtp.localaddr to be configured identically.

>> Back to Top

rtsp.localaddrv6

Default Value:
Valid Values: Can be an empty string or a valid IPv6 address.
Changes Take Effect: At start/restart

Specifies the IPv6 interface to receive RTSP messages from RTSP servers. If this parameter is not specified, then the IP Address of the local system will be used. Note that most RTSP servers require this parameter and [mpc]rtsp.rtp.localaddrv6 to be configured identically.

>> Back to Top

rtsp.rtp.localaddr

Default Value:
Valid Values: Can be an empty string or a valid IPv4 address.
Changes Take Effect: At start/restart

Specifies the interface to receive RTP media from RTSP servers. If this parameter is not specified, then the value in [mpc]rtp.localaddr will be used. Note that most RTSP servers require this parameter and [mpc]rtsp.localaddr to be configured identically.

>> Back to Top

rtsp.rtp.localaddrv6

Default Value:
Valid Values: Can be an empty string or a valid IPv6 address.
Changes Take Effect: At start/restart

Specifies the IPv6 interface to receive RTP media from RTSP servers. If this parameter is not specified, then the value in [mpc]rtp.localaddrv6 will be used. Note that most RTSP servers require this parameter and [mpc]rtsp.localaddrv6 to be configured identically.

>> Back to Top

rtsp.rtp.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

Specifies the available ports to receive RTP media from RTSP servers. If this parameter is not specified, then the value in [mpc]rtp.portange will be used.

>> Back to Top

sdp.audiobandwidth

Default Value:
Valid Values: A valid bandwidth as specified in RFC4566.
Changes Take Effect: At start/restart

Specifies the value of the bandwidth attribute as specified in RFC4566. If not empty, this value will be added to the bandwidth attribute for the audio media description in offerring SDP

>> Back to Top

sdp.connection

Default Value:
Valid Values: IN (IP4|IP6) <connection-address>
Changes Take Effect: At start/restart

Specifies the connection value of outgoing SDP content for a call. Format is defined at RFC4566. It is indepedent of [mpc] rtp.localaddr, which sets the IP address on the platform to be used. This parameter should only be used if the you wish to send an IP address in SDP that is different from the IP address that will be used in [mpc] rtp.localaddr. Setting it to an empty string disables used of this parameter. Possible use cases include when the MCP has a private IP address and a public IP address, and the SDP needs to contain the public IP address.

Examples of possible values include:
- IN IP4 127.0.0.1
- IN IP6 ::1

>> Back to Top

sdp.map.origin.0

Default Value:
Valid Values: A valid string must be of the format <FQDN or IP>/[session name content]
Changes Take Effect: At start/restart

Specifies the origin to match in the SDP. If origin specified by this parameter matches the SDP, the DTMF type specified by mpc.sdp.map.origin.0.dtmftype and the confgain specified by mpc.sdp.map.origin.0.confgain is used. Possible value is "<origin address>/<session name>". Where <origin address> is either a fully qualtified domain name or a dotted IP address. This value is matched against the address part of the "o=" line. Note, the value should be set to either the fully qualified domain name or a dotted IP address, depending on which form the end point sends in the SDP. If the end point may send either form then two mpc.sdp.map.origin.0 entries can be used, one set to the fully qualified domain name form and one set to the dotted IP address form. Where <session name> is the prefix or the entire content of the SDP "s=" (after the "s=" part) line to match. For example if the value is set to "192.168.0.1/phone-call", it will match on 192.168.0.1 in the address part of the "o=" line and require that the "s=" line start with "s=phone-call". If the <session name> is an empty string, it will match any "s=" line content. If both <origin address> and <session name> matches "o=" and "s=" respectively, then it is considered a match.

>> Back to Top

sdp.map.origin.0.confgain

Default Value: 100
Valid Values: mpc.sdp.map.origin.0.confgain must be an integer that is greater than or equal to 0 and less than or equal to 1000.
Changes Take Effect: At start/restart

Specifies the input gain factor to apply for the SDP matching connection when joining the conference. The connection's SDP must match the mpc.sdp.map.origin.0 configuration. The value is specified in percentage. 100 will denote no change. 30 will denote a new input volume of 30% of the original volume into the conference. 200 will denote a new input volume twice as high as the original volume.

>> Back to Top

sdp.map.origin.0.dtmftype

Default Value: INBAND
Valid Values: Choose between: SIPINFO or INBAND.
Changes Take Effect: At start/restart

Specifies the DTMF type to use when mpc.sdp.map.origin.0 matches. This is regardless of whether telephone-event is negotiated or not, and also overrides the mpc.rtp.dtmf.send configuration. SIPINFO - Support sending DTMFs over SIP INFO messages INBAND - Support sending inband audio DTMFs

>> Back to Top

sdp.map.origin.1

Default Value:
Valid Values: A valid string must be of the format <FQDN or IP>/[session name content]
Changes Take Effect: At start/restart

Specifies the origin to match in the SDP. If origin specified by this parameter matches the SDP, the DTMF type specified by mpc.sdp.map.origin.1.dtmftype and the confgain specified by mpc.sdp.map.origin.1.confgain is used. Possible value is "<origin address>/<session name>". Where <origin address> is either a fully qualtified domain name or a dotted IP address. This value is matched against the address part of the "o=" line. Note, the value should be set to either the fully qualified domain name or a dotted IP address, depending on which form the end point sends in the SDP. If the end point may send either form then two mpc.sdp.map.origin.1 entries can be used, one set to the fully qualified domain name form and one set to the dotted IP address form. Where <session name> is the prefix or the entire content of the SDP "s=" (after the "s=" part) line to match. For example if the value is set to "192.168.0.1/phone-call", it will match on 192.168.0.1 in the address part of the "o=" line and require that the "s=" line start with "s=phone-call". If the <session name> is an empty string, it will match any "s=" line content. If both <origin address> and <session name> matches "o=" and "s=" respectively, then it is considered a match.

>> Back to Top

sdp.map.origin.1.confgain

Default Value: 100
Valid Values: mpc.sdp.map.origin.1.confgain must be an integer that is greater than or equal to 0 and less than or equal to 1000.
Changes Take Effect: At start/restart

Specifies the input gain factor to apply for the SDP matching connection when joining the conference. The connection's SDP must match the mpc.sdp.map.origin.1 configuration. The value is specified in percentage. 100 will denote no change. 30 will denote a new input volume of 30% of the original volume into the conference. 200 will denote a new input volume twice as high as the original volume.

>> Back to Top

sdp.map.origin.1.dtmftype

Default Value: INBAND
Valid Values: Choose between: SIPINFO or INBAND.
Changes Take Effect: At start/restart

Specifies the DTMF type to use when mpc.sdp.map.origin.1 matches. This is regardless of whether telephone-event is negotiated or not, and also overrides the mpc.rtp.dtmf.send configuration. SIPINFO - Support sending DTMFs over SIP INFO messages INBAND - Support sending inband audio DTMFs

>> Back to Top

sdp.map.origin.2

Default Value:
Valid Values: A valid string must be of the format <FQDN or IP>/[session name content]
Changes Take Effect: At start/restart

Specifies the origin to match in the SDP. If origin specified by this parameter matches the SDP, the DTMF type specified by mpc.sdp.map.origin.2.dtmftype and the confgain specified by mpc.sdp.map.origin.2.confgain is used. Possible value is "<origin address>/<session name>". Where <origin address> is either a fully qualtified domain name or a dotted IP address. This value is matched against the address part of the "o=" line. Note, the value should be set to either the fully qualified domain name or a dotted IP address, depending on which form the end point sends in the SDP. If the end point may send either form then two mpc.sdp.map.origin.2 entries can be used, one set to the fully qualified domain name form and one set to the dotted IP address form. Where <session name> is the prefix or the entire content of the SDP "s=" (after the "s=" part) line to match. For example if the value is set to "192.168.0.1/phone-call", it will match on 192.168.0.1 in the address part of the "o=" line and require that the "s=" line start with "s=phone-call". If the <session name> is an empty string, it will match any "s=" line content. If both <origin address> and <session name> matches "o=" and "s=" respectively, then it is considered a match.

>> Back to Top

sdp.map.origin.2.confgain

Default Value: 100
Valid Values: mpc.sdp.map.origin.2.confgain must be an integer that is greater than or equal to 0 and less than or equal to 1000.
Changes Take Effect: At start/restart

Specifies the input gain factor to apply for the SDP matching connection when joining the conference. The connection's SDP must match the mpc.sdp.map.origin.2 configuration. The value is specified in percentage. 100 will denote no change. 30 will denote a new input volume of 30% of the original volume into the conference. 200 will denote a new input volume twice as high as the original volume.

>> Back to Top

sdp.map.origin.2.dtmftype

Default Value: INBAND
Valid Values: Choose between: SIPINFO or INBAND.
Changes Take Effect: At start/restart

Specifies the DTMF type to use when mpc.sdp.map.origin.2 matches. This is regardless of whether telephone-event is negotiated or not, and also overrides the mpc.rtp.dtmf.send configuration. SIPINFO - Support sending DTMFs over SIP INFO messages INBAND - Support sending inband audio DTMFs

>> Back to Top

sdp.map.origin.3

Default Value:
Valid Values: A valid string must be of the format <FQDN or IP>/[session name content]
Changes Take Effect: At start/restart

Specifies the origin to match in the SDP. If origin specified by this parameter matches the SDP, the DTMF type specified by mpc.sdp.map.origin.3.dtmftype and the confgain specified by mpc.sdp.map.origin.3.confgain is used. Possible value is "<origin address>/<session name>". Where <origin address> is either a fully qualtified domain name or a dotted IP address. This value is matched against the address part of the "o=" line. Note, the value should be set to either the fully qualified domain name or a dotted IP address, depending on which form the end point sends in the SDP. If the end point may send either form then two mpc.sdp.map.origin.3 entries can be used, one set to the fully qualified domain name form and one set to the dotted IP address form. Where <session name> is the prefix or the entire content of the SDP "s=" (after the "s=" part) line to match. For example if the value is set to "192.168.0.1/phone-call", it will match on 192.168.0.1 in the address part of the "o=" line and require that the "s=" line start with "s=phone-call". If the <session name> is an empty string, it will match any "s=" line content. If both <origin address> and <session name> matches "o=" and "s=" respectively, then it is considered a match.

>> Back to Top

sdp.map.origin.3.confgain

Default Value: 100
Valid Values: mpc.sdp.map.origin.3.confgain must be an integer that is greater than or equal to 0 and less than or equal to 1000.
Changes Take Effect: At start/restart

Specifies the input gain factor to apply for the SDP matching connection when joining the conference. The connection's SDP must match the mpc.sdp.map.origin.3 configuration. The value is specified in percentage. 100 will denote no change. 30 will denote a new input volume of 30% of the original volume into the conference. 200 will denote a new input volume twice as high as the original volume.

>> Back to Top

sdp.map.origin.3.dtmftype

Default Value: INBAND
Valid Values: Choose between: SIPINFO or INBAND.
Changes Take Effect: At start/restart

Specifies the DTMF type to use when mpc.sdp.map.origin.3 matches. This is regardless of whether telephone-event is negotiated or not, and also overrides the mpc.rtp.dtmf.send configuration. SIPINFO - Support sending DTMFs over SIP INFO messages INBAND - Support sending inband audio DTMFs

>> Back to Top

sdp.map.origin.4

Default Value:
Valid Values: A valid string must be of the format <FQDN or IP>/[session name content]
Changes Take Effect: At start/restart

Specifies the origin to match in the SDP. If origin specified by this parameter matches the SDP, the DTMF type specified by mpc.sdp.map.origin.4.dtmftype and the confgain specified by mpc.sdp.map.origin.4.confgain is used. Possible value is "<origin address>/<session name>". Where <origin address> is either a fully qualtified domain name or a dotted IP address. This value is matched against the address part of the "o=" line. Note, the value should be set to either the fully qualified domain name or a dotted IP address, depending on which form the end point sends in the SDP. If the end point may send either form then two mpc.sdp.map.origin.4 entries can be used, one set to the fully qualified domain name form and one set to the dotted IP address form. Where <session name> is the prefix or the entire content of the SDP "s=" (after the "s=" part) line to match. For example if the value is set to "192.168.0.1/phone-call", it will match on 192.168.0.1 in the address part of the "o=" line and require that the "s=" line start with "s=phone-call". If the <session name> is an empty string, it will match any "s=" line content. If both <origin address> and <session name> matches "o=" and "s=" respectively, then it is considered a match.

>> Back to Top

sdp.map.origin.4.confgain

Default Value: 100
Valid Values: mpc.sdp.map.origin.4.confgain must be an integer that is greater than or equal to 0 and less than or equal to 1000.
Changes Take Effect: At start/restart

Specifies the input gain factor to apply for the SDP matching connection when joining the conference. The connection's SDP must match the mpc.sdp.map.origin.4 configuration. The value is specified in percentage. 100 will denote no change. 30 will denote a new input volume of 30% of the original volume into the conference. 200 will denote a new input volume twice as high as the original volume.

>> Back to Top

sdp.map.origin.4.dtmftype

Default Value: INBAND
Valid Values: Choose between: SIPINFO or INBAND.
Changes Take Effect: At start/restart

Specifies the DTMF type to use when mpc.sdp.map.origin.4 matches. This is regardless of whether telephone-event is negotiated or not, and also overrides the mpc.rtp.dtmf.send configuration. SIPINFO - Support sending DTMFs over SIP INFO messages INBAND - Support sending inband audio DTMFs

>> Back to Top

sdp.map.origin.5

Default Value:
Valid Values: A valid string must be of the format <FQDN or IP>/[session name content]
Changes Take Effect: At start/restart

Specifies the origin to match in the SDP. If origin specified by this parameter matches the SDP, the DTMF type specified by mpc.sdp.map.origin.5.dtmftype and the confgain specified by mpc.sdp.map.origin.5.confgain is used. Possible value is "<origin address>/<session name>". Where <origin address> is either a fully qualtified domain name or a dotted IP address. This value is matched against the address part of the "o=" line. Note, the value should be set to either the fully qualified domain name or a dotted IP address, depending on which form the end point sends in the SDP. If the end point may send either form then two mpc.sdp.map.origin.5 entries can be used, one set to the fully qualified domain name form and one set to the dotted IP address form. Where <session name> is the prefix or the entire content of the SDP "s=" (after the "s=" part) line to match. For example if the value is set to "192.168.0.1/phone-call", it will match on 192.168.0.1 in the address part of the "o=" line and require that the "s=" line start with "s=phone-call". If the <session name> is an empty string, it will match any "s=" line content. If both <origin address> and <session name> matches "o=" and "s=" respectively, then it is considered a match.

>> Back to Top

sdp.map.origin.5.confgain

Default Value: 100
Valid Values: mpc.sdp.map.origin.5.confgain must be an integer that is greater than or equal to 0 and less than or equal to 1000.
Changes Take Effect: At start/restart

Specifies the input gain factor to apply for the SDP matching connection when joining the conference. The connection's SDP must match the mpc.sdp.map.origin.5 configuration. The value is specified in percentage. 100 will denote no change. 30 will denote a new input volume of 30% of the original volume into the conference. 200 will denote a new input volume twice as high as the original volume.

>> Back to Top

sdp.map.origin.5.dtmftype

Default Value: INBAND
Valid Values: Choose between: SIPINFO or INBAND.
Changes Take Effect: At start/restart

Specifies the DTMF type to use when mpc.sdp.map.origin.5 matches. This is regardless of whether telephone-event is negotiated or not, and also overrides the mpc.rtp.dtmf.send configuration. SIPINFO - Support sending DTMFs over SIP INFO messages INBAND - Support sending inband audio DTMFs

>> Back to Top

sdp.map.origin.6

Default Value:
Valid Values: A valid string must be of the format <FQDN or IP>/[session name content]
Changes Take Effect: At start/restart

Specifies the origin to match in the SDP. If origin specified by this parameter matches the SDP, the DTMF type specified by mpc.sdp.map.origin.6.dtmftype and the confgain specified by mpc.sdp.map.origin.6.confgain is used. Possible value is "<origin address>/<session name>". Where <origin address> is either a fully qualtified domain name or a dotted IP address. This value is matched against the address part of the "o=" line. Note, the value should be set to either the fully qualified domain name or a dotted IP address, depending on which form the end point sends in the SDP. If the end point may send either form then two mpc.sdp.map.origin.6 entries can be used, one set to the fully qualified domain name form and one set to the dotted IP address form. Where <session name> is the prefix or the entire content of the SDP "s=" (after the "s=" part) line to match. For example if the value is set to "192.168.0.1/phone-call", it will match on 192.168.0.1 in the address part of the "o=" line and require that the "s=" line start with "s=phone-call". If the <session name> is an empty string, it will match any "s=" line content. If both <origin address> and <session name> matches "o=" and "s=" respectively, then it is considered a match.

>> Back to Top

sdp.map.origin.6.confgain

Default Value: 100
Valid Values: mpc.sdp.map.origin.6.confgain must be an integer that is greater than or equal to 0 and less than or equal to 1000.
Changes Take Effect: At start/restart

Specifies the input gain factor to apply for the SDP matching connection when joining the conference. The connection's SDP must match the mpc.sdp.map.origin.6 configuration. The value is specified in percentage. 100 will denote no change. 30 will denote a new input volume of 30% of the original volume into the conference. 200 will denote a new input volume twice as high as the original volume.

>> Back to Top

sdp.map.origin.6.dtmftype

Default Value: INBAND
Valid Values: Choose between: SIPINFO or INBAND.
Changes Take Effect: At start/restart

Specifies the DTMF type to use when mpc.sdp.map.origin.6 matches. This is regardless of whether telephone-event is negotiated or not, and also overrides the mpc.rtp.dtmf.send configuration. SIPINFO - Support sending DTMFs over SIP INFO messages INBAND - Support sending inband audio DTMFs

>> Back to Top

sdp.map.origin.7

Default Value:
Valid Values: A valid string must be of the format <FQDN or IP>/[session name content]
Changes Take Effect: At start/restart

Specifies the origin to match in the SDP. If origin specified by this parameter matches the SDP, the DTMF type specified by mpc.sdp.map.origin.7.dtmftype and the confgain specified by mpc.sdp.map.origin.7.confgain is used. Possible value is "<origin address>/<session name>". Where <origin address> is either a fully qualtified domain name or a dotted IP address. This value is matched against the address part of the "o=" line. Note, the value should be set to either the fully qualified domain name or a dotted IP address, depending on which form the end point sends in the SDP. If the end point may send either form then two mpc.sdp.map.origin.7 entries can be used, one set to the fully qualified domain name form and one set to the dotted IP address form. Where <session name> is the prefix or the entire content of the SDP "s=" (after the "s=" part) line to match. For example if the value is set to "192.168.0.1/phone-call", it will match on 192.168.0.1 in the address part of the "o=" line and require that the "s=" line start with "s=phone-call". If the <session name> is an empty string, it will match any "s=" line content. If both <origin address> and <session name> matches "o=" and "s=" respectively, then it is considered a match.

>> Back to Top

sdp.map.origin.7.confgain

Default Value: 100
Valid Values: mpc.sdp.map.origin.7.confgain must be an integer that is greater than or equal to 0 and less than or equal to 1000.
Changes Take Effect: At start/restart

Specifies the input gain factor to apply for the SDP matching connection when joining the conference. The connection's SDP must match the mpc.sdp.map.origin.7 configuration. The value is specified in percentage. 100 will denote no change. 30 will denote a new input volume of 30% of the original volume into the conference. 200 will denote a new input volume twice as high as the original volume.

>> Back to Top

sdp.map.origin.7.dtmftype

Default Value: INBAND
Valid Values: Choose between: SIPINFO or INBAND.
Changes Take Effect: At start/restart

Specifies the DTMF type to use when mpc.sdp.map.origin.7 matches. This is regardless of whether telephone-event is negotiated or not, and also overrides the mpc.rtp.dtmf.send configuration. SIPINFO - Support sending DTMFs over SIP INFO messages INBAND - Support sending inband audio DTMFs

>> Back to Top

sdp.map.origin.8

Default Value:
Valid Values: A valid string must be of the format <FQDN or IP>/[session name content]
Changes Take Effect: At start/restart

Specifies the origin to match in the SDP. If origin specified by this parameter matches the SDP, the DTMF type specified by mpc.sdp.map.origin.8.dtmftype and the confgain specified by mpc.sdp.map.origin.8.confgain is used. Possible value is "<origin address>/<session name>". Where <origin address> is either a fully qualtified domain name or a dotted IP address. This value is matched against the address part of the "o=" line. Note, the value should be set to either the fully qualified domain name or a dotted IP address, depending on which form the end point sends in the SDP. If the end point may send either form then two mpc.sdp.map.origin.8 entries can be used, one set to the fully qualified domain name form and one set to the dotted IP address form. Where <session name> is the prefix or the entire content of the SDP "s=" (after the "s=" part) line to match. For example if the value is set to "192.168.0.1/phone-call", it will match on 192.168.0.1 in the address part of the "o=" line and require that the "s=" line start with "s=phone-call". If the <session name> is an empty string, it will match any "s=" line content. If both <origin address> and <session name> matches "o=" and "s=" respectively, then it is considered a match.

>> Back to Top

sdp.map.origin.8.confgain

Default Value: 100
Valid Values: mpc.sdp.map.origin.8.confgain must be an integer that is greater than or equal to 0 and less than or equal to 1000.
Changes Take Effect: At start/restart

Specifies the input gain factor to apply for the SDP matching connection when joining the conference. The connection's SDP must match the mpc.sdp.map.origin.8 configuration. The value is specified in percentage. 100 will denote no change. 30 will denote a new input volume of 30% of the original volume into the conference. 200 will denote a new input volume twice as high as the original volume.

>> Back to Top

sdp.map.origin.8.dtmftype

Default Value: INBAND
Valid Values: Choose between: SIPINFO or INBAND.
Changes Take Effect: At start/restart

Specifies the DTMF type to use when mpc.sdp.map.origin.8 matches. This is regardless of whether telephone-event is negotiated or not, and also overrides the mpc.rtp.dtmf.send configuration. SIPINFO - Support sending DTMFs over SIP INFO messages INBAND - Support sending inband audio DTMFs

>> Back to Top

sdp.map.origin.9

Default Value:
Valid Values: A valid string must be of the format <FQDN or IP>/[session name content]
Changes Take Effect: At start/restart

Specifies the origin to match in the SDP. If origin specified by this parameter matches the SDP, the DTMF type specified by mpc.sdp.map.origin.9.dtmftype and the confgain specified by mpc.sdp.map.origin.9.confgain is used. Possible value is "<origin address>/<session name>". Where <origin address> is either a fully qualtified domain name or a dotted IP address. This value is matched against the address part of the "o=" line. Note, the value should be set to either the fully qualified domain name or a dotted IP address, depending on which form the end point sends in the SDP. If the end point may send either form then two mpc.sdp.map.origin.9 entries can be used, one set to the fully qualified domain name form and one set to the dotted IP address form. Where <session name> is the prefix or the entire content of the SDP "s=" (after the "s=" part) line to match. For example if the value is set to "192.168.0.1/phone-call", it will match on 192.168.0.1 in the address part of the "o=" line and require that the "s=" line start with "s=phone-call". If the <session name> is an empty string, it will match any "s=" line content. If both <origin address> and <session name> matches "o=" and "s=" respectively, then it is considered a match.

>> Back to Top

sdp.map.origin.9.confgain

Default Value: 100
Valid Values: mpc.sdp.map.origin.9.confgain must be an integer that is greater than or equal to 0 and less than or equal to 1000.
Changes Take Effect: At start/restart

Specifies the input gain factor to apply for the SDP matching connection when joining the conference. The connection's SDP must match the mpc.sdp.map.origin.9 configuration. The value is specified in percentage. 100 will denote no change. 30 will denote a new input volume of 30% of the original volume into the conference. 200 will denote a new input volume twice as high as the original volume.

>> Back to Top

sdp.map.origin.9.dtmftype

Default Value: INBAND
Valid Values: Choose between: SIPINFO or INBAND.
Changes Take Effect: At start/restart

Specifies the DTMF type to use when mpc.sdp.map.origin.9 matches. This is regardless of whether telephone-event is negotiated or not, and also overrides the mpc.rtp.dtmf.send configuration. SIPINFO - Support sending DTMFs over SIP INFO messages INBAND - Support sending inband audio DTMFs

>> Back to Top

sdp.videobandwidth

Default Value:
Valid Values: A valid bandwidth as specified in RFC4566.
Changes Take Effect: At start/restart

Specifies the value of the bandwidth attribute as specified in RFC4566. If not empty, this value will be added to the bandwidth attribute for the video media description in offerring SDP

>> Back to Top

srtp.cryptomethods

Default Value: AES_CM_128_HMAC_SHA1_80
Valid Values: Any combination of: "AES_CM_128_HMAC_SHA1_80" and "AES_CM_128_HMAC_SHA1_32". Or "none".
Changes Take Effect: At start/restart

List of crypto suites corresponding to advertised capabilities offered by the MCP using SDP. See RFC4568 for the description of the suites.

>> Back to Top

srtp.maxerror

Default Value: 5
Valid Values: mpc.srtp.maxerror must be an integer that is greater than or equal to 1 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

Specifies the tolerance for SRTP errors in transmission and receiving of packets. When the number of errors is greater than this value, a call may be terminated.

>> Back to Top

srtp.mode

Default Value: none
Valid Values: none: No SRTP supported: the MCP will ignore the crypto. accept_only: SRTP supported for SDP offers sent to the MCP, no outgoing offers will add SRTP to m-lines that did not previously contain it. offer: SRTP supported for SDP offers received by the MCP and will be including in outgoing SDP offers. If the other side ignores SRTP, the MCP will fall back to non SRTP mode. If a previously negotiated m-line is used in a reoffer, or the far end requests an offer, and that m-line did not have SRTP negotiated, SRTP will NOT be added. If the far end reoffers and adds SRTP to a previously

negotiated m-line, SRTP WILL be negotiated. offer_strict: Same as offer, however if the other side doesn't use SRTP, negotiation will fail. offer_selectable: Same as offer except - if an offer has two media lines that are the same except that one has crypto, only the one with crypto will be accepted. In its own offer, two media lines will be offered for each media type, one with crypto and the other without. If both media lines are accepted, all RTP will be sent and received only through the crypto line.
Changes Take Effect: At start/restart

Specifies the srtp mode for the MCP

>> Back to Top

srtp.sessionparams

Default Value: UNENCRYPTED_SRTP UNENCRYPTED_SRTCP UNAUTHENTICATED_SRTP
Valid Values: Any combination of: "UNENCRYPTED_SRTP", "UNENCRYPTED_SRTCP" and "UNAUTHENTICATED_SRTP". Or "none".
Changes Take Effect: At start/restart

List of session parameters that the MCP is willing to accept. See RFC4568 for their description. Note that RFC4568 doesn't allow unauthenticated srtcp.

>> Back to Top

srtp.sessionparamsoffer

Default Value:
Valid Values: Any combination of: "UNENCRYPTED_SRTP", "UNENCRYPTED_SRTCP" and "UNAUTHENTICATED_SRTP". Or "none".
Changes Take Effect: At start/restart

List of session parameters that the MCP will include in its SDP offers. See RFC4568 for their description. Note that RFC4568 doesn't allow unauthenticated srtcp.

>> Back to Top

telephone_event.maxptime

Default Value: 0
Valid Values: Choose between: 0, 10, 20, 30, 40, 60, 80 or 100.
Changes Take Effect: Immediately

If the MCP is offering the SDP, or answering the SDP where the offer does not have the maxptime, the maxptime attribute will be set according to this configuration. If this configuration does not exist, or is disabled (0), the maxptime attribute will not be sent unless the SDP offer had the maxptime attribute. In the case where other codecs in the SDP also specify maxptime, the configuration of the codec listed before this codec will take precedence.

>> Back to Top

telephone_event.ptime

Default Value: 0
Valid Values: Choose between: 0, 10, 20, 30, 40, 60, 80 or 100.
Changes Take Effect: Immediately

If the MCP is offering the SDP or answering the SDP where the offer does not have the ptime, the ptime attribute will be set according to this configuration. This configuration is also used as the transmission rate of this codec when the remote SDP does not specify the ptime attribute. Note that transmission rate will default to 20ms if this configuration is disabled. If disabled (0), ptime attribute will not be sent unless the SDP offer had the ptime attribute. In the case where the other codecs in the SDP also specify the configured ptime, the configuration of the codec listed before this codec will take precedence.

>> Back to Top

telephone_eventpayload

Default Value: 101
Valid Values: A valid telephone-event payload can only be an integer from 96 to 127 inclusive
Changes Take Effect: At start/restart

Default telephone-event payload to use by the MCP if none are specified

>> Back to Top

tfcipayload

Default Value: 96
Valid Values: A valid tfci payload can only be an integer from 96 to 127 inclusive
Changes Take Effect: At start/restart

Default payload type number to use for tfci

>> Back to Top

tiasfraction

Default Value: 100
Valid Values: tiasfraction is a percentage (out of 100) that must be an integer of value 0 or greater.
Changes Take Effect: At start/restart

When the TIAS bandwidth parameter is specified on incoming SDP, mpc.tiasfraction specifies the percentage of the TIAS bitrate that the MPC will try to achieve on the outbound media stream. If tiasfraction is 100 (default) then the MPC will try to limit the media bitrate to TIAS. In some cases it might go slightly over the TIAS limit (by perhaps one or two percent), so for safety it might be better to specify a tiasfraction value somewhat less than 100. It is possible to specify a tiasfraction greater than 100, but this is not recommended.

>> Back to Top

transcoders

Default Value: G722 GSM G726 G729 AMR AMR-WB MP3 OPUS H263 H264 VP8
Valid Values: Any combination of: G722, GSM, G726, G729, AMR, AMR-WB, MP3, OPUS, H263, H264 and VP8. Or "none".
Changes Take Effect: At start/restart

Specifies the list of transcoders to be used by MPC. Add H263 to allow video transcoding involving H263 codec: - H263 transcoding to/from H264 (note: H264 also has to be enabled). - H263 resolution downscaling. - H263 frame rate throttling. - H263 bit rate throttling. - H263 conference video mixing. - Textoverlay on H263 video Add H264 to allow video transcoding involving H264 codec: - H264 transcoding to/from H263 (note: H263 also has to be enabled). - H264 resolution downscaling. - H264 frame rate throttling. - H264 bit rate throttling. - H264 conference video mixing. - Textoverlay on H264 video Add VP8 to allow video transcoding involving VP8 codec Set to "none" in order to disable all transcoders.

>> Back to Top

transmitmultiplecodec

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

When media negotiation returns more than one supported codecs, this parameter specifies whether to allow transmission of all supported codecs, or restrict transmission to only one codec. If set to Enable, more than one codec can be transmitted. If set to Disable, only the codec at the top of the negotiated codec list will be transmitted. Note that for SIP devices that support multiple codecs, this parameter must be set to Disable for full call recording to work.

>> Back to Top

tts.appendrejcodec

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

When set to Enable, the MCP will advertise all supported codecs when generating an SDP offer to the MRCP TTS. Even if codecs are rejected or not presented in the caller's SDP, the MCP will still support receiving these codecs. The MCP will not send for those SDPs unless a payload is presented by the caller.

>> Back to Top

tts.codec

Default Value: pcmu
Valid Values: Any combination of: pcmu, pcma, g722, g726, g729, gsm, amr, amr-wb and tfci.
Changes Take Effect: Immediately

List of codec corresponding to advertised capabilities offered by the MCP to the MRCP TTS server using SDP. The offered codec list will control the codecs that are offered by the MCP to the remote party for media sent from the remote party to Genesys.

>> Back to Top

tts.preferredipinterface

Default Value: V4
Valid Values: Choose between: V4 or V6
Changes Take Effect: At start/restart

Specifies the preferred IP interface to use (IPv4 or IPv6) for MRCP TTS when performing SDP negotiation. In particular, this will be used to set the root connection attribute in SDP answers, and set the connection attribute in SDP offers.

>> Back to Top

tts.srtp.cryptomethods

Default Value: AES_CM_128_HMAC_SHA1_80
Valid Values: Any combination of: "AES_CM_128_HMAC_SHA1_80" and "AES_CM_128_HMAC_SHA1_32". Or "none".
Changes Take Effect: At start/restart

List of crypto suites corresponding to advertised capabilities offered by the MCP to the MRCP TTS server using SDP. See RFC4568 for the description of the suites.

>> Back to Top

tts.srtp.mode

Default Value: none
Valid Values: none: No SRTP supported: the MCP will ignore the crypto. offer: SRTP supported in outgoing SDP offers. If the other side ignores SRTP, the MCP will fall back to non SRTP mode. offer_strict: Same as offer, however if the other side doesn't use SRTP, negotiation will fail.
Changes Take Effect: At start/restart

Specifies the srtp mode for the MCP to use for MRCP TTS sessions

>> Back to Top

tts.srtp.sessionparamsoffer

Default Value:
Valid Values: Any combination of: "UNENCRYPTED_SRTP", "UNENCRYPTED_SRTCP" and "UNAUTHENTICATED_SRTP". Or "none".
Changes Take Effect: At start/restart

List of session parameters that the MCP will include in its SDP offers to the MRCP TTS server. See RFC4568 for their description. Note that RFC4568 doesn't allow unauthenticated srtcp.

>> Back to Top

validatemediatimers

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

When enabled, all media thread timers would be validated. This is useful for scenario where clock skew prevents media threads from waking up at regular intervals.

>> Back to Top

videotranscoder.bitratecheckdelay

Default Value: 10000
Valid Values: A valid value should be an integer greater or equal to 0
Changes Take Effect: At start/restart

This parameter specifies the bit rate check delay when bit rate check is enabled for video transcoding. Bit rate checking will start after the milliseconds specified by this parameter elapses.

>> Back to Top

videotranscoder.bitratechecktolerance

Default Value: 50
Valid Values: A valid value should be an integer greater or equal to 0
Changes Take Effect: At start/restart

This parameter specifies the bit rate check tolerance when bit rate check is enabled for video transcoding. Bit rate checking will allow the bit rate to go over the maximum by the percentage specified by this parameter.

>> Back to Top

videotranscoder.checkbitrate

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

When set to true and the transcoder for the incoming video format is enabled, video transcoding will be triggered when bit rate exceeds the maximum bit rate. When false, it will not.

>> Back to Top

videotranscoder.checkframerate

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

When set to true and the transcoder for the incoming video format is enabled, video transcoding will be triggered when frame rate exceeds the maximum frame rate. When false, it will not.

>> Back to Top

videotranscoder.frameratechecktolerance

Default Value: 50
Valid Values: A valid value should be an integer greater or equal to 0
Changes Take Effect: At start/restart

This parameter specifies the frame rate check tolerance when frame rate check is enabled for video transcoding. Frame rate checking will allow the frame rate to go over the maximum by the percentage specified by this parameter.

>> Back to Top

videotranscoder.h264.keyframeidrinterval

Default Value: 1
Valid Values: A number between 0 and 2147483647 inclusive.
Changes Take Effect: At start/restart

This parameter specifies the IDR frame generation frequency of the H264 transcoder. IDR frame is one of types of i-frames in H264. For example, if 2 is specified, every other i-frame generated will be an IDR frame.

>> Back to Top

videotranscoder.h264.keyframeinterval

Default Value: 50
Valid Values: A number between 0 and 2147483647 inclusive.
Changes Take Effect: At start/restart

This parameter specifies the i-frame generation frequency of the H264 transcoder. For example, if 50 is specified, an i-frame will be generated per every 50 frames.

>> Back to Top

videotranscoder.h264.resolutions

Default Value: SQCIF QCIF QVGA CIF VGA 4CIF SVGA 720P
Valid Values: Any combination of: SQCIF, QCIF, QVGA, CIF, VGA, 4CIF, SVGA, 720P and custom resolution "WidthxHeight".
Changes Take Effect: At start/restart

This parameter specifies the list of H264 encodable resolutions when H264 transcoding is applied. If empty, defaults to "SQCIF QCIF QVGA CIF VGA 4CIF SVGA 720P". ITU-T H264 Recommendation document Table A.6 specifies the list of resolution/frame rate/bit rate limits per level. If the resolution needs to be downscaled because of the level requirement, the resolution closest downward in this list will be selected. Format: <resolution> <resolution> [<resolution> ...] Where <resolution> is <width>x<height> or one of the following keywords - SQCIF - Sub-QCIF resolution (128x96) QCIF - QCIF resolution (176x144) QVGA - QVGA resolution (320x240) CIF - CIF resolution (352x288) VGA - VGA resolution (640x480) 4CIF - 4CIF resolution (704x576) SVGA - SVGA resolution (800x600) 720P - 720P HD resolution (1280x720) When <width>x<height> syntax is used, the resolution must be less than or equal to 720P HD resolution. WARNING: MCP will fail to start if invalid resolution is specified.

>> Back to Top

videotranscoder.maxbitrate

Default Value: 500000
Valid Values: A valid value should be an integer greater or equal to 0
Changes Take Effect: Immediately/session

This parameter specifies maximum bit rate used for encoding when video transcoding is active. 0 indicates that there is no maximum imposed. If not 0, video transcoded output encoding bit rate is set to the minimum of the maximum allowed bitrate of the receiver and the value specified by this parameter.

>> Back to Top

videotranscoder.statsresetthreshold

Default Value: 60000
Valid Values: A number between 1000 and 2147483647 inclusive.
Changes Take Effect: At start/restart

This parameter specifies the accumulated duration (in milliseconds) threshold at which to trigger resetting of frame rate/bit rate statistics. For example, if set to 60000, the cumulative duration used for calculating frame rate/bit rate is reset approximately every 60 seconds. The statistics is used for checking and triggering video transcoding when frame rate/bit rate exceeds the required maximum. Lower value makes the transcoding trigger more sensitive to sudden bursts that exceeds the required maximum.

>> Back to Top

voipmetrics.enable

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

When enabled, MCP will collect several metrics defined in RFC 3611 for each audio session. The metrics can be divided into local and remote. For local metrics, MCP collects some of them by exchanging RTCP messages between itself and the remote party while some are calculated locally from ongoing activities. For remote metrics, the remote party, if supporting RFC 3611, will report MCP about its metrics periodically and MCP will record them whenever it receives an update.

At the end of each audio session, MCP users also have an option to publish the local and remote metrics to a destination. Refer to voipmetrics.* configuration under sip section for more information.

>> Back to Top

vp8.adaptive

Default Value: true
Valid Values: The value must be a boolean of either true or false.
Changes Take Effect: At start/restart

This parameter specifies the adaptivity of the VP8 encoder behaviour, and thus the determinism of its output. In adaptive mode (the default) the encoder will adapt to environmental conditions to provide the best overall user experience. Non-adaptive mode will result in the same output everytime, but will not adapt to environmental situations.

>> Back to Top

vp8.defaultbitrate

Default Value: 0
Valid Values: The bitrate value must be an integer of value 0 or greater.
Changes Take Effect: At start/restart

This parameter specifies the output bitrate in bits/sec for transcoding to the VP8 format. If set to 0 the default bitrate of the VP8 encoder will be used.
WARNING: MCP will fail to start if an invalid value is specified.

>> Back to Top

vp8.defaultframerateden

Default Value: 1001
Valid Values: The framerate numerator value must be 1 or greater.
Changes Take Effect: At start/restart

This parameter specifies the output framerate denominator for transcoding to the VP8 format. The framerate numerator and denominator values are combined to determine the framerate (e.g. 30000/1001 gives 29.97 frames/sec).
WARNING: MCP will fail to start if an invalid value is specified.

>> Back to Top

vp8.defaultframeratenum

Default Value: 30000
Valid Values: The framerate numerator value must be 1 or greater.
Changes Take Effect: At start/restart

This parameter specifies the output framerate numerator for transcoding to the VP8 format. The framerate numerator and denominator values are combined to determine the framerate (e.g. 30000/1001 gives 29.97 frames/sec).
WARNING: MCP will fail to start if an invalid value is specified.

>> Back to Top

vp8.defaultresolution

Default Value: CIF
Valid Values: Choose between: SQCIF, QCIF, QVGA, CIF, VGA, 4CIF, SVGA, 720P or custom resolution "WidthxHeight".
Changes Take Effect: At start/restart

This parameter specifies the output resolution for transcoding to the VP8 format.

The value is specified by a keyword or width and height value as follows:
SQCIF - Sub-QCIF resolution (128x96)
QCIF - QCIF resolution (176x144)
QVGA - QVGA resolution (320x240)
CIF - CIF resolution (352x288)
VGA - VGA resolution (640x480)
4CIF - 4CIF resolution (704x576)
SVGA - SVGA resolution (800x600)
720P - 720P HD resolution (1280x720)
WidthxHeight - specifies a custom width and height

When WidthxHeight syntax is used, the resolution must be less than or equal to 720P HD resolution.
WARNING: MCP will fail to start if invalid resolution is specified.

>> Back to Top

vp8.maxkeyframeinterval

Default Value: 15
Valid Values: The value must be nonnegative.
Changes Take Effect: Immediately/session

This parameter, expressed as a number of frames, forces the encoder to code a keyframe if the last keyframe was vp8.maxkeyframeinterval frames ago. A value of 0 or 1 implies all frames will be keyframes.

>> Back to Top

vrmrecorder.codec

Default Value: pcmu pcma g722 opus g726 g729 gsm amr amr-wb h263 h263-1998 h264 vp8 telephone-event
Valid Values: Any combination of: pcmu, pcma, g722, opus, g726, g729, gsm, amr, amr-wb, h263, h263-1998, h264, vp8, or telephone-event.
Changes Take Effect: At start/restart

Specifies a list of codecs supported by MCP for VRM recorder. This option is used to limit supported codecs on the RTP streams sent to the recorder. It is similar to the main "codec" parameter, except in this case, the codecs and order in the offer are dictated by the codecs negotiated on the inbound call legs. By restricting the codecs in this list, a streaming issue on recorder streams caused by lack of transcoding support could be avoided, where the recorder sends a SIP session refresh with an SDP that changes the codec priority order from the original MCP offer.

>> Back to Top

vrmrecorder.enable

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

When set to true, the vrmrecorder for the CRQM feature will be enabled. When false, or not set, it will not be loaded.

>> Back to Top

vrmrecorder.preferredipinterface

Default Value: V4
Valid Values: Choose between: V4 or V6
Changes Take Effect: Immediately

Specifies the preferred IP interface to use (IPv4 or IPv6) when performing SDP negotiation (CRQM related). In particular, this will be used to set the root connection attribute in SDP answers, and set the connection attribute in SDP offers.

>> Back to Top

vrmrecorder.srtp.cryptomethods

Default Value: AES_CM_128_HMAC_SHA1_80
Valid Values: Any combination of: "AES_CM_128_HMAC_SHA1_80" and "AES_CM_128_HMAC_SHA1_32". Or "none".
Changes Take Effect: At start/restart

List of crypto suites corresponding to advertised capabilities offered by the MCP to a recording server using SDP. See RFC4568 for the description of the suites.

>> Back to Top

vrmrecorder.srtp.mode

Default Value: none
Valid Values: none: No SRTP supported: the MCP will ignore the crypto. offer: SRTP supported in outgoing SDP offers. If the other side ignores SRTP, the MCP will fall back to non SRTP mode. offer_strict: Same as offer, however if the other side doesn't use SRTP, negotiation will fail. offer_selectable: Same as offer except - two media lines will be offered for each media type, one with crypto and the other without. If both media lines are accepted, all RTP will be sent and received only through the crypto line.
Changes Take Effect: At start/restart

Specifies the srtp mode for the MCP to use for recording sessions

>> Back to Top

vrmrecorder.srtp.sessionparamsoffer

Default Value:
Valid Values: Any combination of: "UNENCRYPTED_SRTP", "UNENCRYPTED_SRTCP" and "UNAUTHENTICATED_SRTP". Or "none".
Changes Take Effect: At start/restart

List of session parameters that the MCP will include in its SDP offers to a recording server. See RFC4568 for their description. Note that RFC4568 doesn't allow unauthenticated srtcp.

>> Back to Top

widebandconferences

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

When enabled and the conference's initial audio requirements are unknown, MCP will mix the conference's audio in wideband. This will generally increase conference sound quality at the cost of increased CPU usage.

>> Back to Top

mrcpv2client Section

- sip.transport.0
- sip.transport.1
- sip.transport.2
- sip.transport.localaddress
- sip.transport.localaddress.srv

sip.transport.0

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

The SIP UDP Transport used by the MRCPV2 Client. Format: sip.transport.x = transport_name type:ip:port

where: transport_name is any string type is udp/tcp/tls ip is the IP address of the network interface that accepts incoming SIP messages port is the port number where SIP stack accepts incoming SIP messages
If ip is an IPv6 address, [] must be used. To define a transport to listen to all IPv4 interfaces, use "any" or "any4" for ip. To define a transport to listen to all IPv6 interfaces, use "any6" for ip. Remarks: The default transport is the smallest non-empty ID. If all transport.x values are empty, UDP, TCP, and TLS transports will all be enabled and respectively listen from ports 5060, 5060, and 5061 on any network interface. TLS transport will use the certificate, x509_certificate.pem, and key, x509_private_key.pem, in the config directory. UDP will be the default transport.

sip.transport.1

Default Value: transport1 tcp:any:7080
Valid Values: <transport_name> <type>:<ip-address>:<port> [parameters]
Changes Take Effect: At start/restart

The SIP TCP Transport used by the MRCPV2 Client. Format: sip.transport.x = transport_name type:ip:port

where: transport_name is any string type is udp/tcp/tls ip is the IP address of the network interface that accepts incoming SIP messages port is the port number where SIP stack accepts incoming SIP messages
If ip is an IPv6 address, [] must be used.
To define a transport to listen to all IPv4 interfaces, use "any" or "any4" for ip. To define a transport to listen to all IPv6 interfaces, use "any6" for ip. Remarks: The default transport is the smallest non-

empty ID. If all transport.x values are empty, UDP, TCP, and TLS transports will all be enabled and respectively listen from ports 5060, 5060, and 5061 on any network interface. TLS transport will use the certificate, x509_certificate.pem, and key, x509_private_key.pem, in the config directory. UDP will be the default transport.

sip.transport.2

Default Value: transport2 tls:any:7081 type=TLSv1
Valid Values: <transport_name> <type>:<ip-address>:<port> [parameters]
Changes Take Effect: At start/restart

The SIP TLS Transport used by the MRCPV2 Client. Format: sip.transport.x = transport_name type:ip:port [parameters]

where: transport_name is any string type is udp/tcp/tls ip is the IP address of the network interface that accepts incoming SIP messages port is the port number where SIP stack accepts incoming SIP messages [parameters] defines any extra SIP transport parameters. Note that this is for LMSIP2.

If ip is an IPv6 address, [] must be used. To define a transport to listen to all IPv4 interfaces, use "any" or "any4" for ip. To define a transport to listen to all IPv6 interfaces, use "any6" for ip. Example:
cert=[cert path and filename] Applicable to SIPS only and mandatory if using SIPS. The path and the filename of the TLS certificate to be used.
key=[key path and filename] Applicable to SIPS only and mandatory if using SIPS. The path and the filename of the TLS key to be used.
type=[Type of secure transport] Applicable to SIPS only and is optional. The type of secure transport to be used and value can be TLSv1_2, TLSv1_1, TLSv1, SSLv3, or SSLv23. The default value is TLSv1. Note that SSLv2 is no longer supported.
password=[password] Applicable to SIPS only and is optional. The password associated with the certificate and key pair. Required only if key file is password protected.
cafile=[CA cert path and filename] Mandatory for TLS mutual authentication. The path and the filename of the certificate to be used for verifying the peer. The same certificate specified in cert=[cert path and filename] parameter can be used as the value here if using only 1 certificate is preferred.
verifypeer=true Mandatory for TLS mutual authentication. This parameter turns on the TLS mutual authentication.
verifydepth=[max depth for the certificate chain verification] Applicable only to TLS mutual authentication. This parameter sets the maximum depth for the certificate chain verification. For the default Genesys certificate provided, the recommended value is 1.
tls-cipher-list=[List of ciphers that are applicable for the socket] Applicable only to TLS socket - both server and client sockets. This parameter allows selecting a list of cipher suites used in TLS. This option is transfered to a third-party library and describes a possible set of cipher suites. Refer to https://www.openssl.org/docs/man1.0.2/man1/ciphers.html for Cipher list format. Default is ALL:!EXPORT:!LOW:!aNULL:!eNULL:!SSLv2 Remarks: The default transport is the smallest non-empty ID. If all transport.x values are empty, UDP, TCP, and TLS transports will all be enabled and respectively listen from ports 5060, 5060, and 5061 on any network interface. TLS transport will use the certificate, x509_certificate.pem, and key, x509_private_key.pem, in the config directory. UDP will be the default transport. Note: The max path length supported for certificate and key file is 259 characters.

sip.transport.localaddress

Default Value:
Valid Values: Specify a valid IP address, hostname or domain name
Changes Take Effect: At start/restart

If specified, the sent-by field of the Via header and the hostport part of the Contact header in the outgoing SIP message will be set to this value if a IPv4 transport is used. The value must be a hostname or domain name if [sip].transport.localaddress.srv is set to true, otherwise when [sip].transport.localaddress.srv is set to false an IP address or hostname can be used for the value. If left empty the outgoing transport's actual IP and port will be used for the Via header and the Contact header. Note that if the domain name used in the SRV record query is specified, mrcpv2client.sip.transport.localaddress.srv must be set to true to prevent the port part being automatically generated by the SIP stack.

sip.transport.localaddress.srv

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

Specifies whether the mrcpv2client.transport.localaddress contains an SRV domain name. If set to true, port part will not be automatically generated by the SIP stack. Otherwise, the outgoing transport's port will used together with the hostname specified by the mrcpv2client.sip.transport.localaddress.

msml Section

- beep.filename
- beep.join.timelimit
- callrecording.dtmfhandling
- clampdtmf.postsilencepackets
- clampdtmf.presilencepackets
- conference.participantjointimeout
- conference.passthrough_enabled
- cpd.beeptimeout
- cpd.postconnecttimeout
- cpd.preconnecttimeout
- cpd.record.basepath
- cpd.record.fileext
- defaultaudioext
- dialogend.silentfail
- info.contenttypes
- play.basepath
- play.fetchtimeout
- play.h263videoformat
- play.h264videoformat
- play.musicbasepath
- play.preferredvideocontainer
- play.usedefaultsearchorder
- record.amazonallowpublicaccess
- record.amazonpostmode
- record.amazonsignatureversion
- record.amazonsignedpayload
- record.appenduniqueid
- record.basepath
- record.channels
- record.channels2
- record.deferredsink
- record.filenametemplate
- record.finalsilence
- record.generatehash
- record.irrecoverablerecordpostdir
- record.posttimeout
- record.updateheader
- record.userecordcachedir

beep.filename

Default Value: file://$InstallationRoot$/audio/ulaw/default_audio/endofprompt.vox
Valid Values: Please specify a valid path to the file
Changes Take Effect: Immediately

This parameter is used to specify the filename for the 'beep' before doing the <join> operation or in place of the "$beep$" in a play element.. Will be limited by the msml.beep.join.timelimit configuration.

beep.join.timelimit

Default Value: 5000
Valid Values: Must be an integer greater than 0 and less than or equal to 10000.
Changes Take Effect: Immediately

The timelimit for the audible "beep" when played during a <join> element. Units are in milliseconds.

callrecording.dtmfhandling

Default Value: as-is
Valid Values: as-is: (default) Record everything as-is from the RTP stream. Inband DTMFs will be recorded, but RFC2833 digits will not. no-digits: Strip out all DTMF digits. This includes inband or RFC2833. NOTE: When telephone-event is negotiated on the call, if inband audio DTMFs are received, they will not be removed from the recording. all-digits: Record all DTMF digits, including inband, and generate audio for RFC2833 digits.
Changes Take Effect: Immediately/session

Specifies the recording behavior for DTMFs in MSML Call Recording.

clampdtmf.postsilencepackets

Default Value: 0
Valid Values: Must be an integer greater than or equal to 0.
Changes Take Effect: Immediately/session

Specifies the number of audio packets that will be replaced with silence after a clamped DTMF. This can be used in the case where DTMF tone appears after DTMF RFC2833 event.

clampdtmf.presilencepackets

Default Value: 0
Valid Values: Must be an integer 0 to 50 inclusive.
Changes Take Effect: Immediately/session

Specifies the number of audio packets that will be replaced with silence before a clamped DTMF. This can be used in the case where DTMF tone appears before DTMF RFC2833 event, which may happen when SIP gateway converts DTMF tones to DTMF RFC2833 event. Note the bigger number is set, the more audio delays will be introduced in a conference.

conference.participantjointimeout

Default Value: 120000
Valid Values: Must be an integer greater than or equal to 0 and less than or equal to the maximum integer as defined by Genesys Administrator.
Changes Take Effect: Immediately/session

Time a conference that is set to delete when no media will wait until a partipant joins before it decides to self terminate. In extreme scenarios, this prevents a leak from occurring. Default is 2 minutes (120000 ms). Units are in ms. Set to 0 to disable.

conference.passthrough_enabled

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

Used to avoid double transcoding when 2 participants with lossy audio codecs is being recorded by MCP. Pass through is established only if Codecs and other media capabilities match on both sides and the Mixer is not used for modifying the signal. If true, this capability is enable.

cpd.beeptimeout

Default Value: 30
Valid Values: Must be an integer greater than or equal to 0 and less than 60.
Changes Take Effect: Immediately

CPD Beep Timeout in seconds. When not set in the <cpd> element attributes, this value will be used as the default beep timeout. Set to 0 to disable.

cpd.postconnecttimeout

Default Value: 30
Valid Values: Must be an integer greater than or equal to 0 and less than 60.
Changes Take Effect: Immediately

CPD Post-connect Timeout in seconds. When not set in the <cpd> element attributes, this value will be used as the default post-connect timeout. Set to 0 to disable.

cpd.preconnecttimeout

Default Value: 30
Valid Values: Must be an integer greater than or equal to 0 and less than 60.
Changes Take Effect: Immediately

CPD Pre-connect Timeout in seconds. When not set in the <cpd> element attributes, this value will be used as the default pre-connect timeout. Set to 0 to disable.

cpd.record.basepath

Default Value: file://$installationRoot$/record/
Valid Values: Please specify a valid path.

Changes Take Effect: Immediately

Path pointing to the root directory for CPD recording.

cpd.record.fileext

Default Value: wav
Valid Values: Please specify a valid audio file extention.
Changes Take Effect: Immediately

Specifies the file extension for CPD recording. Will be used to determine the MIME-type of the file, and the extension used.

defaultaudioext

Default Value: .wav
Valid Values: Speficy a valid audio file extension.
Changes Take Effect: Immediately

Specifies the default file extension of audio files to be used in play prompt or recording.

dialogend.silentfail

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

Set the default behavior for dialogend with regards to silently failing if the dialog cannot be found. When true, and a dialog to end cannot be found, the dialogend will not fail. When false, the dialogend request will fail if the dialog cannot be found.

info.contenttypes

Default Value: application/vnd.radisys.msml+xml
Valid Values: A valid content type can only contain alphanumeric characters, and '/' or '\'
Changes Take Effect: Immediately

Content types in a SIP INFO messages that are allowed for the MSML AppModule. Only the defined content types are processed, others are ignored. If left empty, the default value is "application/vnd.radisys.msml+xml". Specifying "*" would mean that any value is permitted. This is a space delimited list of values.

play.basepath

Default Value: file://$installationRoot$
Valid Values: Please specify a valid path.
Changes Take Effect: Immediately

Path pointing to the root directory of prompt media.

play.fetchtimeout

Default Value: 25000
Valid Values: Must be an integer greater than or equal to 5000 and less than or equal to 25000.
Changes Take Effect: Immediately/session

Sets the fetch timeout (in ms) for an MSML play.

play.h263videoformat

Default Value: QCIF=2
Valid Values: Specify a comma-separated list of H.263 video formats.
Changes Take Effect: Immediately

A comma-separated list of H.263 video formats that are used for selecting H.263 video files to play.

play.h264videoformat

Default Value: 0a=2,0b=2,0c=2,0d=2,14=2,15=2,16=2,1e=2
Valid Values: Specify a comma-separated list of H.264 video formats.
Changes Take Effect: Immediately

A comma-separated list of H.264 video formats that are used for selecting H.264 video files to play. The video format is in the form of "byte_value=mpi" where byte value is the last byte of the profile-level-id, and mpi is the minimum picture interval. The last byte of the profile-level-id in the negotiated SDP is matched against the desired minimum picture interval specified in this configuration parameter. MCP shall select the prompt file with filename ending as profile-level-id=matched_minimum_picture_interval to play. If the last byte of profile-level-id of the negotiated SDP is not found in this configuration parameter list, no file will be played. For example, if this configuration parameter has value 0a=2, and if negotiated SDP for H.264 codec has specified profile-level-id as 42e00a, then MCP shall look for prompt file name ending with H264_42e00a=2.

play.musicbasepath

Default Value: file://$installationRoot$

Valid Values: Please specify a valid path.
Changes Take Effect: Immediately

Path pointing to the root directory of music prompt.

play.preferredvideocontainer

Default Value: avi
Valid Values: Can only be 3gp or avi.
Changes Take Effect: Immediately/session

When an extension is not present in the MSML play request, precheck is enabled, and the user negotiates a video codec, this configuration will be used to determine which container will be attempted.

play.usedefaultsearchorder

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

Specifies the audio file search order for MSML prompt announcement. The default search order is <ID>/<format>.<ext> followed by <ID>_<format>.<ext>. If this option is set to true, the default order will be used. If this is set to false, the search order will be reversed.

record.amazonallowpublicaccess

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

Specifies the access permissions for the recording file uploaded to Amazon s3 during MSML call recording. When set to 'false', MCP would restrict access to the uploaded file to the s3 bucket owner only and when set to 'true', MCP would allow public download access to the uploaded recording file. Note that if both primary recording destination(recdest) and secondary recording destination(recdest2) are configured to use s3 URI format(s3:bucketname) then MCP would grant the same access permissions(depending upon the configuration value of this parameter) to the two recording files uploaded to Amazon s3.

record.amazonpostmode

Default Value: http
Valid Values: Choose between: http or https
Changes Take Effect: Immediately/session

This parameter specifies the mode to be used for uploading recording files to Amazon s3 during MSML call recording. When set to 'https', MCP would use 'HTTPS' protocol for uploading the recording files to Amazon s3 and when set to 'http', MCP would use 'HTTP' protocol. The default mode is 'HTTP'. Note that if both primary recording destination(recdest) and secondary recording destination(recdest2) are configured to use s3 URI format(s3:bucketname) then MCP would use either 'HTTP' or 'HTTPS'(depending upon the configuration value of this parameter) for uploading the two recording files to Amazon s3.

record.amazonsignatureversion

Default Value: V4
Valid Values: Choose between: V2 or V4
Changes Take Effect: Immediately/session

Specifies the Amazon method to generate the authentication signature on GET and PUT requests during record upload. When set to 'V2' the Amazon 'AWS' algorithm will be used to authenticate the requests. This version was deprecated by Amazon somewhere around the year 2014, and all locations deployed after this date no longer accepts this authentication version. When set to 'V4' the Amazon 'AWS4-HMAC-SHA256' algorithm will be used to authenticate the requests. This is currently the official method for authentication, it introduces more security and is accepted in all regions.

The 'V4' authentication algorithm has some new requirements, one of them is the bucket location (or region), this information was not previously needed and therefore MCP didn't care about it. Two methods were introduced in order for MCP to get the bucket's location: (1) Automatic method, where MCP uses an Amazon service to get the information, This method does not require additional input from the customer and is backward compatible; (2) Manual method, where the customer provides the bucket's location using the IVR-Profile through the new parameters recordingclient.AWSRegion and recordingclient.AWSRegion2;

The automatic method (1) is the default method, as it does not require any further configuration or additional input from the customers. The manual method (2) will be used only as an alternative when the automatic method is not being able to properly get the bucket location.

record.amazonsignedpayload

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

Specifies if the payload will be signed with the V4 signature. This provides added security but MCP needs to read the entire payload, so it will impact the performance. This only applies if the V4 signature is enabled through the parameter [msml].record.amazonsignatureversion. When set to 'true', MCP will calculate the Hash SHA256 of the Amazon POST payloads, and use the result to create the signature. When set to 'false', MCP won't calculate the payload hash.

record.appenduniqueid

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

When set to true, if an MSML Dialog Recording (i.e. recording from the record tag in MSML Dialog Base Package) is requested, record destinations that do not have an extension specified will have a unique identifier included as part of recorded file name. When set to false, no unique identifier will be included in the final file name.

If a directory is specified, a unique indentifier will always be used, independent of this configuration.

If the attribute "gvp:appenduniqueid" is specified in the record element, that value will take precedence over the configured value.

record.basepath

Default Value: file://$installationRoot$
Valid Values: Please specify a valid path.
Changes Take Effect: Immediately

Path pointing to the root directory for recording media.

record.channels

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

This parameter specifies the number of channels for MSML recording to dest(1- mono, 2- stereo). Default value is 2 (stereo).

record.channels2

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

This parameter specifies the number of channels for MSML recording to dest2(1- mono, 2- stereo). Default value is 2 (stereo).

record.deferredsink

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

When set to true the Recorder will act as deferred sink during MSML call recording. This means that the Recorder would use its own thread for writing media data to recording file and is more robust to any disk IO issues which arise during writing of the media data to the file. When set to false the Recorder would not be a deferred sink and would use the source thread for writing the media data to the file.

record.filenametemplate

Default Value: $id$
Valid Values: Please specify a valid template following the instructions in the description.
Changes Take Effect: Immediately

This parameter specifies the default template for generating MSML recording (aka GIR-Recording) and IVR-Recording file names.

For MSML recording (GIR-Recording): - Any gvp:param present in the template may be replaced by its value if specified using MSML. - Some possible template parameters: $id$, $dateTime$, $MCPDateTime$, $dnis$, $recordDN$, $ani$, $callUuid$, $sipsAppName$, $connId$, $record$, $dest$, $dest2$, $type$, $type2$, $channels$, $channels2$, $AWSRegion$, $AWSRegion2$, $callrec_dest$, $audiosrc$, $tonesilenceduration$, and any other gvp:param present in MSML. - Example: The template $id$_$record$_$MCPDateTime$ produces the file name "basicrecid12345_source_2013-09-13_08-10-15_*.*" where $id$ is specified as "basicrecid12345", $record$ is specified as "source" using MSML gvp:param and $MCPDateTime$ enables insertion of MCP local time.

For IVR-Recording: - Some of the parameters passed in the INVITE RURI are accepted. - Possible template parameters: $id$, $dateTime$, $MCPDateTime$, $dnis$, $recordDN$, $ani$, $callUuid$ and $sipsAppName$. - The $id$ template is equivalent to $callUuid$_$dateTime$ template. The date and time used is in UTC mode retrieved from the MCP machine. - Example: The template $callUuid$_$MCPDateTime$ produces the file name "SDFGTRE3456YHBVFT543_2018-04-26_13-33-46_*.*" where "SDFGTRE3456YHBVFT543" is the SIP header XGENESYSCALLUUID value and $MCPDateTime$ enables insertion of MCP local time.

Notes: - The template $dateTime$ is replaced by the UTC time, and $MCPDateTime$ is replaced by the local time from the MCP machine. - There is a 260 character limit (including directory names and extension) for the recording file name on Windows. - Parameters are case sensitive.

record.finalsilence

Default Value: 4
Valid Values: Must be an integer greater than or equal to 0 and less than or equal to 10000.
Changes Take Effect: Immediately

The default final silence duration in seconds that can be detected in a recording to terminate the recording.

record.generatehash

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

Specifies if MCP should generate the SHA256 hash of the recorded files. The generated hash is used to sign the payloads in case amazon posts are configured to use V4 signature, and it will also be added to the HTCC metadata. When set to 'true', MCP will generate the SHA256 hash of the recorded files. When set to 'false', MCP won't generate the recorded files hash.

record.irrecoverablerecordpostdir

Default Value: $installationRoot$/cache/record/failed
Valid Values: Please specify a valid path.
Changes Take Effect: Immediately

While doing MSML call recording the recordings are added to a list if they need to be posted to Amazon S3, Call Recording API, HTTP/HTTPS or SpeechMiner. A separate posting thread wakes up from time to time and works on the list of recordings to be posted. This parameter specifies the directory for storing recording files which encounter irrecoverable errors during the post attempts.

record.posttimeout

Default Value: 120000
Valid Values: msml.record.posttimeout must be an integer that is greater than or equal to 1 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: Immediately/session

The post timeout for recordings which need to be posted to Amazon S3, Call Recording API, HTTP/HTTPS or SpeechMiner. Once this timeout expires the post attempt would be treated as one which encountered recoverable error and would be retried. The default value of this parameter is 120 sec (120000 milli seconds).

record.updateheader

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

When set to true the recording file header will be updated on disk during MSML call recording. When set to false the recording file header will not be updated on disk during the recording and the header updation will be performed(if needed) while trying to place the recording file at its final destination.

record.userecordcachedir

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

When set to true, record cache dir(specified using config parameter mpc.recordcachedir) is used for FILE based MSML call recording. Once the recording completes, the recording file is moved from the record cache dir to the final recording destination. When set to false, record cache dir is not used for FILE based MSML call recording and the recording file is directly created at the final recording destination. Note that the value of this configuration parameter is ignored and the behavior for 'true' is used if HTCC post is desired.

mtinternal Section

enablertcp

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

Specifies whether to transmit RTCP packets.

max_concurrent_savedata

Default Value: -1
Valid Values: mtinternal.max_concurrent_savedata must be an integer that is greater or equal to -1 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

If specified as an integer n, and mtinternal.transmit_savedata or mtinternal.receive_savedata is enabled, then only a maximum of n concurrent files will be open for writing data. Default value is -1, which would place no limit.

receive_max_size

Default Value: -1
Valid Values: mtinternal.receive_max_size must be an integer that is greater or equal to -1 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

Defines the maximum packet sample size that will be notified to the receiver. Note that this number is applied to all codecs with fixed frame size. It will be rounded down to the nearest multiple of the codec frame size. This parameter will be disabled when variable frame size codec is used. Set to -1 to disable the limit.

receive_min_size

Default Value: -1
Valid Values: mtinternal.receive_min_size must be an integer that is greater or equal to -1 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

Defines the minimum packet sample size that will be notified to the receiver. Note that this number is applied to all codecs with fixed frame size. It will be rounded down to the nearest multiple of the codec frame size. This parameter will be disabled when variable frame size codec is used. Set to -1 to disable the limit.

receive_rate_alarm

Default Value: 500
Valid Values: mtinternal.receive_rate_alarm 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

If greater than 0, minor alarm is generated if the transmission rate of incoming packets is slower the real time by the specified delay in milliseconds. This alarm will be disabled if variable frame size codec is used for received packets.

receive_savedata

Default Value:
Valid Values: mtinternal.receive_savedata must be a valid path
Changes Take Effect: At start/restart

If specified, received data is saved under the directory.

restrictsource

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

Specifies whether to allow dropping packets from other sources (filtering).

rtp.statisticsinterval

Default Value: 600000
Valid Values: Possible values are integers from 0 to 3600000 inclusive.
Changes Take Effect: At start/restart

Specifies the interval (in ms) at which statistics logging in the RTP layer will be logged. Setting this value to 0 will disable the statistics logging. If enabled, will log when an RTP connection is destroyed, regardless of interval.

transmit_max_size

Default Value: 160
Valid Values: mtinternal.transmit_max_size must be an integer that is greater or equal to -1 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

Defines the maximum data size in bytes that can be sent. Note that this number is applied to all codecs with fixed frame size. It will be rounded down to the nearest multiple of the codec frame size. This parameter will be disabled when variable frame size codec is used. Set to -1 to disable the limit.

transmit_min_size

Default Value: 160
Valid Values: mtinternal.transmit_min_size must be an integer that is greater or equal to -1 and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: At start/restart

Defines the minimum data size in bytes that can be sent. Note that this number is applied to all codecs with fixed frame size. It will be rounded down to the nearest multiple of the codec frame size. This parameter will be disabled when variable frame size codec is used. Set to -1 to disable the limit.

transmit_rate

Default Value: 10
Valid Values: The maximum transmission rate 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

Specifies the transmission rate limit as a multiple of realtime. A value of 1 means realtime, 2 means 2 times realtime and so on. Set to 0 for no limit.

transmit_rate_alarm

Default Value: 500
Valid Values: mtinternal.transmit_rate_alarm 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

If greater than 0, minor alarm is generated if the transmission rate of outgoing packets is slower the real time by the specified delay in milliseconds. This alarm will be disabled if variable frame size codec is used for transmitted packets.

transmit_savedata

Default Value:
Valid Values: mtinternal.transmit_savedata must be a valid path
Changes Take Effect: At start/restart

If specified, utterance is saved under the directory.

mtmpc Section

- conference.output_gain

conference.output_gain

Default Value: 100
Valid Values: mtmpc.conference.output_gain must be an integer at least equal 0 and less than or equal to 1000
Changes Take Effect: At start/restart

Specifies the gain applied to the output of a conference in decibels. Default value is 100.

Netann Section

- annc.audiodefaultrepeat
- annc.basepath
- annc.defaultaudioext
- annc.fetchtimeout
- annc.h263videoformat
- annc.h264videoformat
- annc.musicbasepath
- conference.recordmode
- record.appenduniqueid
- record.basepath
- record.maxrecordsilence
- record.maxrecordtime
- sipinfonotifydtmf

annc.audiodefaultrepeat

Default Value: forever
Valid Values: Speficy a positive integer number. Or "forever" for endless repeat times.
Changes Take Effect: Immediately

Specifies the default repeat times to be used for Netann announcement playback, not applicable to DTMF prompts.

annc.basepath

Default Value: $installationRoot$
Valid Values: Please specify a valid path.
Changes Take Effect: At start/restart

Path pointing to the root directory of prompt media.

annc.defaultaudioext

Default Value: .wav
Valid Values: Speficy a valid audio file extension.
Changes Take Effect: Immediately

Specifies the default file extension of audio files to be used for Netann announcement playback.

annc.fetchtimeout

Default Value: 25000
Valid Values: Must be an integer greater than or equal to 5000 and less than or equal to 25000.
Changes Take Effect: Immediately/session

Sets the fetch timeout (in ms) for a Play Announcement.

annc.h263videoformat

Default Value: QCIF=2
Valid Values: Speficy a comma-separated list of H.263 video formats.
Changes Take Effect: Immediately

A comma-separated list of H.263 video formats that are used for selecting H.263 video files to play. Examples of H.263 video formats are SQCIF=1 to 6, QCIF=1 to 6, CIF=1 to 6, CIF4=1 to 6, and CIF16=1 to 6.

annc.h264videoformat

Default Value: 0a=2,0b=2,0c=2,0d=2,14=2,15=2,16=2,1e=2
Valid Values: Speficy a comma-separated list of H.264 video formats.
Changes Take Effect: Immediately

A comma-separated list of H.264 video formats that are used for selecting H.264 video files to play. The video format is in the form of "byte_value=mpi" where byte value is the last byte of the profile-level-id, and mpi is the minimum picture interval. The last byte of the profile-level-id in the negotiated SDP is matched against the desired minimum picture interval specified in this configuration parameter. MCP shall select the prompt file with filename ending as profile-level-id=matched_minimum_picture_interval to play. If the last byte of profile-level-id of the negotiated SDP is not found in this configuration parameter list, no file will be played. For example, if this configuration parameter has value 0a=2, and if negotiated SDP for H.264 codec has specified profile-level-id as 42e00a, then MCP shall look for prompt file name ending with H264_42e00a=2.

annc.musicbasepath

Default Value: $installationRoot$
Valid Values: Please specify a valid path.
Changes Take Effect: Immediately

Path pointing to the root directory of music prompts.

conference.recordmode

Default Value: mixed
Valid Values: Choose between: mixed, multich, pcap or multich-pcap.
Changes Take Effect: Immediately

When recording is enabled in a conference, this option specifies the recording mode. mixed - The recorded file format will be specified by request, with audio from all participants mixed into a single file. multich - A WAV file with multiple audio channels will be used, with audio from only first two participants recorded in 2 channels. pcap - The recorded file format is pcap. One file will be created for each participant. multich-pcap - The recorded file format is pcap. One file will be created for the conference. Only the first two participants will be recorded into the file.

record.appenduniqueid

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

When set to true, if a Netann Recording is requested, record destinations that do not have an extension specified will have a unique identifier included as part of recorded file name. When set to false, no unique identifier will be included in the final file name.

PCAP recordings will still have _(recording number).pcap appended at the end of the file.

If a directory is specified, a unique indentifier will always be used, independent of this configuration.

record.basepath

Default Value: $InstallationRoot$/record
Valid Values: Please specify a valid path.
Changes Take Effect: At start/restart

Path pointing to the root directory of the recorded file.

record.maxrecordsilence

Default Value: 0
Valid Values: Speficy a positive integer number.
Changes Take Effect: Immediately

Defines the maximum amount of silence in seconds allowed during a recording. If the value is set to 0, silence detection is not used.

record.maxrecordtime

Default Value: 0
Valid Values: Speficy a positive integer number.
Changes Take Effect: Immediately

Defines the maximum recording time in seconds. The default value 0 means that the recording time is unlimited

sipinfonotifydtmf

Default Value: Auto
Valid Values: Choose between: Auto, True or False
Changes Take Effect: At start/restart

Specify when recieving a DTMF, whether to always send, never send, or to depend on the Allow header of incoming INVITEs for prompt announcement services. Auto - Depends on Allow Header True - Always Send False - Never Send

remdial Section

- maxcalls
- maxclientsockets
- port
- telnetmode

maxcalls

Default Value: 500
Valid Values: The number should be an integer 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

Maximum number of concurrent remdial calls

maxclientsockets

Default Value: 64
Valid Values: The number should be an integer 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

Max number of remdial clients allowed

port

Default Value: 6999
Valid Values: The port number must be an integer from 1030 to 65535 inclusive
Changes Take Effect: At start/restart

Remdial port

telnetmode

Default Value: RAW

Valid Values: Choose between: RAW or NORMAL
Changes Take Effect: At start/restart

Remdial telnet mode. If set to RAW, remdial will buffer data until it receives a carriage return. If set to NORMAL, Remdial will expect the that the full request was sent all at once. RAW is the recommendation configuration since it will support most telnet clients. The default Windows telnet client will only work if this configuration is set to RAW. NORMAL will provide a performance boost if the client sends the full request all at once. Most Linux and Solaris clients, along with PuTTy on Windows, will work with this configuration.

sessmgr Section

- acceptcalltimeout
- alert_before_fetch
- appmodules_linux
- appmodules_win
- default_init_url
- default_vxml_interpreter
- disconnect_cause.badfetch
- disconnect_cause.decline
- fcr_video_dir
- init_accept_call_mode
- join_fallback
- licensepoolsize.gvp_ports
- licensepoolsize.gvp_tts_ports
- maxincalltime
- mediaswitch_on_alert
- modules_linux
- modules_win
- mrt.sendsdpininvite
- MSML.MSML
- Netann.Netann
- Remdial.RemoteDial
- VXML3.VXML-NG

acceptcalltimeout

Default Value: 30000
Valid Values: sessmgr.acceptcalltimeout must be an integer 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

Accept call timeout in milliseconds. After alerting is issued, if the application module does not accept the inbound call within the timeout, the call will be disconnected. The timeout is set to 30000 milliseconds by default.

alert_before_fetch

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

Issues alerting message to phone network before the page is successfully fetched. When it is set to 1, Composer debugging with the NGI will not work. It is because NGI will not be able to attach the SIP headers to the 18x response.

appmodules_linux

Default Value: Remdial:RemoteDial Netann:Netann VXML3:VXML-NG MSML:MSML
Valid Values: Any combination of: Remdial:RemoteDial, Netann:Netann, VXML3:VXML-NG and MSML:MSML.
Changes Take Effect: At start/restart

This specifies the list of names of app modules to be initialized on startup for the Linux platform. Each possible value is made up of <Module_Name>:<App_Module_Name>. <Module_Name> specifies the module containing <App_Module_Name>. ":" is the delimiter used below.

To enable VoiceXML Applications on Linux, VXML3:VXML-NG must be set, and [sessmgr] modules_linux needs to have VXML3 set. To disable VoiceXML Applications on Linux, VXML3:VXML-NG must not be set, and [sessmgr] modules_linux needs to not have VXML3 set.

appmodules_win

Default Value: Remdial:RemoteDial Netann:Netann VXML3:VXML-NG MSML:MSML
Valid Values: Any combination of: Remdial:RemoteDial, Netann:Netann, VXML3:VXML-NG and MSML:MSML.
Changes Take Effect: At start/restart

This specifies the list of names of app modules to be initialized on startup for the Windows platform. Each possible value is made up of <Module_Name>:<App_Module_Name>. <Module_Name> specifies the module containing <App_Module_Name>. ":" is the delimiter used below.

To enable VoiceXML Applications on Windows, VXML3:VXML-NG must be set, and [sessmgr] modules_win needs to have VXML3 set. To disable VoiceXML Applications on Windows, VXML3:VXML-NG must not be set, and [sessmgr] modules_win needs to not have VXML3 set.

default_init_url

Default Value: file://$InstallationRoot$/samples/ulaw/helloworld.vxml
Valid Values: Please specify a valid URL to a VoiceXML page
Changes Take Effect: At start/restart

Specifies the URL to the initial VoiceXML page if one isn't specified in the incoming SIP request.

default_vxml_interpreter

Default Value: VXML-NG
Valid Values: VXML-NG or VXML-LGVP
Changes Take Effect: At start/restart

Specifies which VoiceXML Interpreter is used to handle calls that do not specify the VoiceXML

Interpreter. VXML-NG - Next Generation VoiceXML Interpreter VXML-LGVP - Legacy GVP VoiceXML Interpreter

disconnect_cause.badfetch

Default Value: 17
Valid Values: The sessmgr.disconnect_cause.badfetch must 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

This parameter is used to specify the ISDN disconnect cause code if the initial page fetch failed for some reason

disconnect_cause.decline

Default Value: 21
Valid Values: The sessmgr.disconnect_cause.decline must 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

This parameter is used to specify the ISDN disconnect cause code if the MCP has chosen to decline the call

fcr_video_dir

Default Value: IN
Valid Values: Choose between: IN or OUT
Changes Take Effect: Immediately

This specifies which video stream will be recorded during an FCR operation. It can be the video from the user or the video played to the user. IN - FCR records the video from the user OUT - FCR records the video played to the user

init_accept_call_mode

Default Value: DUPLEX
Valid Values: Choose between: INBOUND, OUTBOUND, DUPLEX or DISABLE
Changes Take Effect: At start/restart

This specifies the AcceptCallMode when the MCP starts up. INBOUND - Accept only inbound call OUTBOUND - Accept only outbound call DUPLEX - Accept both inbound and outbound calls DISABLE - Do not accept calls

join_fallback

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

This determines whether to fall back on MediaRedirect/Bridged transfer if CallJoin fails. 0 - No fall back 1 - Falls back to MediaRedirect if supported. Otherwise, to Bridged transfer

licensepoolsize.gvp_ports

Default Value: max
Valid Values: max or a number
Changes Take Effect: At start/restart

License pool size for voice port usage, value should be max or a numeric number. MCP would attempt to acquire voice ports from the Genesys License Server up to the pool size specified value. For max. value, MCP would try to acquire the max. allowed voice port licenses as the Genesys License Server could provide.

licensepoolsize.gvp_tts_ports

Default Value: max
Valid Values: max or a number
Changes Take Effect: At start/restart

License pool size for TTS port usage, value should be max or a numeric number. MCP would attempt to acquire TTS ports from the Genesys License Server up to the pool size specified value. For max. value, MCP would try to acquire the max. allowed TTS port licenses as the Genesys License Server could provide.

maxincalltime

Default Value: 0
Valid Values: Time must be an non-negative integer value and less than or equal to the maximum integer as defined by the Genesys Administrator Help.
Changes Take Effect: Immediately

This specifies the maximum call time for inbound calls in seconds. When the timer expires, the inbound call will be disconnected. Set to 0 to disable the timer.

mediaswitch_on_alert

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

Specifies when media switching should occur in a call transfer, when the transfer "connectwhen" attribute is set to "immediate". When this parameter is set to Enable, media switching would occur when call alerting started on the outbound call. Otherwise, media switching would occur as soon as the outbound call is initiated.

modules_linux

Default Value: Remdial Netann VXML3 MSML
Valid Values: Any combination of: Remdial, Netann, VXML3 and MSML.
Changes Take Effect: At start/restart

This specifies the list of MCP Application Modules to be loaded, in the order defined, for the Linux platform. The modules correspond to dynamic link libraries that are named libAPP<module name>.so.

To enable VoiceXML Applications on Linux, VXML3 must be set, and [sessmgr] appmodules_linux needs to have VXML3:VXML-NG set. To disable VoiceXML Applications on Linux, VXML3 must not be set, and [sessmgr] appmodules_linux needs to not have VXML3:VXML-NG set.

modules_win

Default Value: Remdial Netann VXML3 MSML
Valid Values: Any combination of: Remdial, Netann, VXML3 and MSML.
Changes Take Effect: At start/restart

This specifies the list of MCP Application Modules to be loaded, in the order defined, for the Windows platform. The modules correspond to dynamic link libraries that are named libAPP<module name>.dll.

To enable VoiceXML Applications on Windows, VXML3 must be set, and [sessmgr] appmodules_win needs to have VXML3:VXML-NG set. To disable VoiceXML Applications on Windows, VXML3 must not be set, and [sessmgr] appmodules_win needs to not have VXML3:VXML-NG set.

mrt.sendsdpininvite

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

When enabled, for a Media Redirect call that has 'connectwhen' specified as "answered", the MCP will send the caller's last SDP to the callee both in a reINVITE and in an ACK. When disabled, the reINVITE to the callee will not contain any SDP.

MSML.MSML

Default Value: msml
Valid Values: A valid name can only contain characters and numerics.
Changes Take Effect: At start/restart

Name of MSML Instance

Netann.Netann

Default Value: Netann
Valid Values: A valid name can only contain characters and numerics.
Changes Take Effect: At start/restart

Name of Netann Instance

Remdial.RemoteDial

Default Value: RemoteDial
Valid Values: A valid name can only contain characters and numerics.
Changes Take Effect: At start/restart

Name of Remdial Instance

VXML3.VXML-NG

Default Value: vxmli-ng1
Valid Values: A valid name can only contain characters and numerics.
Changes Take Effect: At start/restart

Name of the NGI app module instance

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 bypass-resource-list 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.securerouteset=<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

stack Section

- connection.portrange
- connection.timeout
- trace.debug

connection.portrange

Default Value: 10000-11999
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:

The port range of RTSP stack used by MRCPv1 client.

connection.timeout

Default Value: 10000
Valid Values: A number between 1 and 60000 inclusive.
Changes Take Effect:

The connection timeout for SRM MRCPv1 and MRCPv2 Stack to establish a TCP connection to the server. The value must be integer values in milliseconds.

trace.debug

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

Whether to enable the stack debug message

tts Section

- defaultengine
- reserve

defaultengine

Default Value: default
Valid Values: The engine name must be a string.
Changes Take Effect: Immediately/session

The engine specified here will be used to load a default engine. An application using a different name should override this using the ttsengine property or the Request URI configuration.

reserve

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

When set to true, the MCP will attempt to reserve a TTS resource prior to accepting the call. This resource will be available until an explicit release of the resource, or until the end of the call. The call will be rejected if the resource is not successfully reserved.

vrm Section

- client.dtmf.abnf_encoding_check
- client.dtmf.fetchtimeout
- client.dtmf.maxage
- client.dtmf.maxloopcount
- client.dtmf.maxstale
- client.grpc.credential
- client.grpc.init_worker_threads
- client.grpc.init_worker_threads.tts
- client.grpc.max_worker_threads
- client.grpc.max_worker_threads.tts
- client.grpc.sslroots
- client.grpc.timeout
- client.modules
- client.mrcpv1.sendtrapformrcprecogcompletioncause
- client.mrcpv1.sendtrapformrcprequestfailure
- client.mrcpv1.sendtrapformrcpresponsecode
- client.mrcpv1.sendtrapformrcpresponsefailure
- client.mrcpv1.sendtrapformrcpspeakcompletioncause
- client.mrcpv1.sendtrapforrtspresponsecode
- client.mrcpv2.earlynomatch
- client.mrcpv2.localaddr
- client.mrcpv2.maxopensocket
- client.mrcpv2.portrange
- client.mrcpv2.prefix
- client.mrcpv2.proxy
- client.mrcpv2.sendtrapformrcprecogcompletioncause
- client.mrcpv2.sendtrapformrcprequestfailur
- client.mrcpv2.sendtrapformrcpresponsecod
- client.mrcpv2.sendtrapformrcpresponsefailu
- client.mrcpv2.sendtrapformrcpspeakcomple
- client.mrcpv2.sendtrapforsipresponsecode
- client.timeout
- client.universals.uri
- rtp.localaddr
- rtp.localaddrv6
- rtp.portrange
- rtsp.localaddr

client.dtmf.abnf_encoding_check

Default Value: content
Valid Values: Choose between: content, attribute or none
Changes Take Effect:

Method for checking ABNF grammar encoding: Selecting content, the entire grammar content will be checked to confirm it is UTF-8 encoded. Selecting attribute, only the encoding field in the self-identifying header will be checked to confirm the grammar is UTF-8 encoded. If the encoding field is absent, the content check method will be used. Selecting none, the encoding will not be checked.

client.dtmf.fetchtimeout

Default Value: 10000
Valid Values: A number between 1 and 86400000 inclusive.
Changes Take Effect:

Timeout in milliseconds that a native DTMF recognizer needs to complete for an external grammar fetching.

client.dtmf.maxage

Default Value: -1
Valid Values: A number between -1 and 86400000 inclusive.
Changes Take Effect:

Maxage in milliseconds that a native DTMF recognizer will use for an external grammar fetching. A value of -1 indicates to use the server's maxage value.

client.dtmf.maxloopcount

Default Value: 1000
Valid Values: A number between 100 and 86400000 inclusive.
Changes Take Effect:

Maximum number of loops that is allowed in evaluating a DTMF grammar.

client.dtmf.maxstale

Default Value: -1
Valid Values: A number between -1 and 86400000 inclusive.
Changes Take Effect:

Maxstale in milliseconds that a native DTMF recognizer will use for an external grammar fetching. A value of -1 indicates to use the server's maxstale value.

client.grpc.credential

Default Value:
Valid Values: Path to the Google Speech-to-Text or Text-to-Speech credential file
Changes Take Effect:

This parameter specifies the path to the Google Speech-to-Text or Text-to-Speech credential file.

client.grpc.init_worker_threads

Default Value: 5
Valid Values: An integer greater than or equal to 0

Changes Take Effect: At start/restart

This parameter specifies the initial number of GRPC client worker threads for ASR. More threads will be created as necessary up to "max_worker_threads".

client.grpc.init_worker_threads.tts

Default Value: 5
Valid Values: An integer greater than or equal to 0
Changes Take Effect: At start/restart

This parameter specifies the initial number of GRPC client worker threads for TTS. More threads will be created as necessary up to "max_worker_threads.tts".

client.grpc.max_worker_threads

Default Value: 200
Valid Values: A number between 1 and 500 inclusive.
Changes Take Effect: At start/restart

This parameter specifies the maximum number of GRPC client worker threads that would be created for ASR. If more threads are required by additional GRPC/GSR sessions, those GRPC sessions will fail.

client.grpc.max_worker_threads.tts

Default Value: 350
Valid Values: A number between 1 and 500 inclusive.
Changes Take Effect: At start/restart

This parameter specifies the maximum number of GRPC client worker threads that would be created for ASR. If more threads are required by additional GRPC/GTTS sessions, those GRPC sessions will fail.

client.grpc.sslroots

Default Value: $InstallationRoot$/config/grpc_roots.pem
Valid Values: Path to the GRPC SSL roots certificate
Changes Take Effect:

This parameter specifies the path to the GRPC SSL roots certificate, which can be downloaded from https://github.com/grpc/grpc/raw/master/etc/roots.pem.

client.grpc.timeout

Default Value: 10000
Valid Values: A number between 1 and 60000 inclusive.
Changes Take Effect: At start/restart

Timeout value to wait for a response from the server. The value is in milliseconds.

client.modules

Default Value: MRCPV1 MRCPV2 MRCP_DTMFRECOGNIZER
Valid Values: Any combination of: MRCPV1, MRCPV2, MRCP_DTMFRECOGNIZER and GRPC
Changes Take Effect:

This parameter lists the SRM MRCP client protocol modules as well as GRPC modules installed in the platform. MRCPV1 - Enable MRCPv1 MRCPV2 - Enable MRCPv2 MRCP_DTMFRECOGNIZER - Enable on-board DTMF Recognizer GRPC - Enable Google Speech-to-Text or Text-to-Speech using GRPC

client.mrcpv1.sendtrapformrcprecogcompletioncause

Default Value: 004-006,009,010
Valid Values: A comma separated list of values and/or ranges.
Changes Take Effect: Immediately

Send traps when receiving one of the completion-causes in the MRCP RECOGINTION-COMPLETE event. Refer to the MRCPv1 specification for the completion cause codes and their corresponding descriptions.

client.mrcpv1.sendtrapformrcprequestfailure

Default Value:
Valid Values: Any combination of: RTSP-DESCRIBE, RTSP-SETUP, RTSP-TEARDOWN, MRCP-SET-PARAMS, MRCP-DEFINE-GRAMMAR, MRCP-RECOGNIZE, MRCP-RECOGNITION-START-TIMER, MRCP-SPEAK and MRCP-STOP
Changes Take Effect: Immediately

Sends traps when one of the following requests fails to send: RTSP-DESCRIBE RTSP-SETUP RTSP-TEARDOWN MRCP-SET-PARAMS MRCP-DEFINE-GRAMMAR MRCP-RECOGNIZE MRCP-RECOGNITION-START-TIMER MRCP-SPEAK MRCP-STOP

client.mrcpv1.sendtrapformrcpresponsecode

Default Value: 405,407

Valid Values: A comma separated list of values and/or ranges.
Changes Take Effect: Immediately

Send traps when receiving one of the response codes in the MRCP request's reply. Refer to the MRCPv1 specification for the response codes and their corresponding descriptions.

client.mrcpv1.sendtrapformrcpresponsefailure

Default Value: MRCP-DEFINE-GRAMMAR MRCP-RECOGNIZE MRCP-SPEAK
Valid Values: Any combination of: RTSP-DESCRIBE, RTSP-SETUP, RTSP-TEARDOWN, MRCP-SET-PARAMS, MRCP-DEFINE-GRAMMAR, MRCP-RECOGNIZE, MRCP-RECOGNITION-START-TIMER, MRCP-SPEAK and MRCP-STOP
Changes Take Effect: Immediately

Sends traps when receiving error response codes for these responses. The error response codes are configured in "Send Trap For MRCPv1 Response Codes": RTSP-DESCRIBE RTSP-SETUP RTSP-TEARDOWN MRCP-SET-PARAMS MRCP-DEFINE-GRAMMAR MRCP-RECOGNIZE MRCP-RECOGNITION-START-TIMER MRCP-SPEAK MRCP-STOP

client.mrcpv1.sendtrapformrcpspeakcompletioncause

Default Value: 002,005
Valid Values: A comma separated list of values and/or ranges.
Changes Take Effect: Immediately

Send traps when receiving one of the completion-causes in the MRCP SPEAK-COMPLETE event. Refer to the MRCPv1 specification for the completion cause codes and their corresponding descriptions.

client.mrcpv1.sendtrapforrtspresponsecode

Default Value: 405,454,500
Valid Values: A comma separated list of values and/or ranges.
Changes Take Effect: Immediately

Send traps when receiving one of the response codes in the RTSP request's reply. Refer to the RTSP specification for the response codes and their corresponding descriptions.

client.mrcpv2.earlynomatch

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

The TRUE value of this parameter tells the MRCPv2 server MUST not wait for the end of speech before processing the collected speech to match active grammars.

client.mrcpv2.localaddr

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

Specifies the network interface (IP address) to be used by MRCPv2 stack. If this parameter is not specified, the OS will choose an interface.

client.mrcpv2.maxopensocket

Default Value: 256
Valid Values: A number between 1 and 1024 inclusive.
Changes Take Effect:

The parameter specifies the maximum allowed sockets opened for MRCPv2 sessions.

client.mrcpv2.portrange

Default Value: 12000-13999
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:

The port range of MRCPv2 stack.

client.mrcpv2.prefix

Default Value: mrcpv2client
Valid Values: Any non-empty string
Changes Take Effect:

The value is used by the SIP stack to choose the SIP port for SRM MRCPv2 client.

client.mrcpv2.proxy

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

Specifies whether to consider the MRCPv2 resources added in the connection tab of MCP should be treated as MRCPv2 proxy, When the MRCPv2 proxy is enabled, MCP will pass through the authorization header and the engine name as X-Genesys headers to MRCPv2 proxy server.

client.mrcpv2.sendtrapformrcprecogcompletioncause

Default Value: 004-006,009,010,012,016
Valid Values: A comma separated list of values and/or ranges.
Changes Take Effect: Immediately

Sends traps when receiving one of the completion-causes in the MRCP RECOGINTION-COMPLETE event. Refer to the MRCPv2 specification for the completion cause codes and their corresponding descriptions.

client.mrcpv2.sendtrapformrcprequestfailure

Default Value:
Valid Values: Any combination of SIP-OPTIONS, SIP-INVITE, SIP-BYE, MRCP-SET-PARAMS, MRCP-DEFINE-GRAMMAR, MRCP-RECOGNIZE, MRCP-START-INPUT-TIMER, MRCP-SPEAK and MRCP-STOP
Changes Take Effect: Immediately

Sends traps when one of the following requests fails to send: SIP-OPTIONS SIP-INVITE SIP-BYE MRCP-SET-PARAMS MRCP-DEFINE-GRAMMAR MRCP-RECOGNIZE MRCP-START-INPUT-TIMER MRCP-SPEAK MRCP-STOP

client.mrcpv2.sendtrapformrcpresponsecode

Default Value: 405,407
Valid Values: A comma separated list of values and/or ranges.
Changes Take Effect: Immediately

Sends traps when receiving one of the response codes in the MRCP request's reply. Refer to the MRCPv2 specification for the response codes and their corresponding descriptions.

client.mrcpv2.sendtrapformrcpresponsefailure

Default Value: MRCP-DEFINE-GRAMMAR MRCP-RECOGNIZE MRCP-SPEAK
Valid Values: Any combination of SIP-OPTIONS, SIP-INVITE, SIP-BYE, MRCP-SET-PARAMS, MRCP-DEFINE-GRAMMAR, MRCP-RECOGNIZE, MRCP-START-INPUT-TIMER, MRCP-SPEAK and MRCP-STOP
Changes Take Effect: Immediately

Sends traps when receiving error response codes for these responses. The error response codes are configured in "Send Trap For MRCPv2 Response Codes": SIP-OPTIONS SIP-INVITE SIP-BYE MRCP-SET-

PARAMS MRCP-DEFINE-GRAMMAR MRCP-RECOGNIZE MRCP-START-INPUT-TIMER MRCP-SPEAK MRCP-STOP

client.mrcpv2.sendtrapformrcpspeakcompletioncause

Default Value: 002,005
Valid Values: A comma separated list of values and/or ranges.
Changes Take Effect: Immediately

Send traps when receiving one of the completion-causes in the MRCP SPEAK-COMPLETE event. Refer to the MRCPv2 specification for the completion cause codes and their corresponding descriptions.

client.mrcpv2.sendtrapforsipresponsecode

Default Value: 400-513
Valid Values: A comma separated list of values and/or ranges.
Changes Take Effect: Immediately

Sends traps when receiving one of the response codes in the SIP response. Refer to the SIP specification for the response codes and their corresponding descriptions.

client.timeout

Default Value: 10000
Valid Values: A number between 1 and 60000 inclusive.
Changes Take Effect:

Timeout value to wait for response. The value must be integer values in milliseconds.

client.universals.uri

Default Value: builtin:grammar/universals
Valid Values: URI to universals grammars.
Changes Take Effect:

This gives the URI convention that the NextGen VXMLI uses to specify the universals grammars. The default value should be set to: client.universals.uri = builtin:grammar/universals

rtp.localaddr

Default Value: $LocalIP$
Valid Values: IPv4 Address

Changes Take Effect: At start/restart

Specifies the IPv4 interface to be used by RTP streams to and from speech resources. If this parameter is not specified, then the value will be auto-configured.

rtp.localaddrv6

Default Value:
Valid Values: IPv6 Address
Changes Take Effect: At start/restart

Specifies the IPv6 interface to be used by RTP streams to and from speech resources. If this parameter is not specified, then the value will be auto-configured.

rtp.portrange

Default Value: 45536-65535
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

Specifies the ports to be used by RTP streams to and from speech resources. If this parameter is not specified, then the value will be auto-configured.

rtsp.localaddr

Default Value: $LocalIP$
Valid Values: IP Address
Changes Take Effect: At start/restart

Specifies the interface to be used by RTSP streams to and from speech resources. If this parameter is not specified, then the value will be auto-configured.

vrmrecorder Section

sip.localport

Default Value: 7090
Valid Values: The port number must be from 1030 to 65535 inclusive
Changes Take Effect: At start/restart

The Local Non-secure SIP Port used by the VRMRecorder Client when SIP UDP and SIP TCP are used.

sip.localsecureport

Default Value: 7091
Valid Values: The port number must be from 1030 to 65535 inclusive
Changes Take Effect: At start/restart

The Local Secure SIP Port used by the VRMRecorder Client when SIP TLS is used.

sip.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 by the VRMRecorder. 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, the other version will be used. Valid values are "ipv4" and "ipv6".

sip.routeset

Default Value:
Valid Values: A valid routeset must have the format as specified in [sip] routeset description
Changes Take Effect: At start/restart

Defines a route set for non-secure SIP connections to third party recorders by the VRMRecorder client. If defined, this route set will be inserted as the ROUTE header for all VRMRecorder SIP sessions. This will force the MCP to send the SIP messages via this defined route set. Please see "[sip] routeset" for format and other descriptions. The typical value for this would be the Resource Manager (RM) address, as all recorder requests go through the RM.

sip.securerouteset

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

Defines a route set for secure SIP connections to third party recorders. The URI for secure connections 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 VRMRecorder secure SIP sessions. This will force the MCP to send the secure SIP messages via this defined route set. Please see "[sip] securerouteset" for format and other descriptions. The typical value for this would be the Resource Manager (RM)'s secure address, as all recorder requests go through the RM.

sip.transport.0

Default Value: transport0 udp:any:7090
Valid Values: <transport_name> <type>:<ip-address>:<port> [parameters]
Changes Take Effect: At start/restart

The SIP UDP Transport used by the VRMRecorder Client. Format: sip.transport.x = transport_name type:ip:port

where: transport_name is any string type is udp/tcp/tls ip is the IP address of the network interface that accepts incoming SIP messages port is the port number where SIP stack accepts incoming SIP messages
If ip is an IPv6 address, [] must be used. To define a transport to listen to all IPv4 interfaces, use "any" or "any4" for ip. To define a transport to listen to all IPv6 interfaces, use "any6" for ip. Remarks: The default transport is the smallest non-empty ID. If all transport.x values are empty, UDP, TCP, and TLS

transports will all be enabled and respectively listen from ports 5060, 5060, and 5061 on any network interface. TLS transport will use the certificate, x509_certificate.pem, and key, x509_private_key.pem, in the config directory. UDP will be the default transport.

sip.transport.1

Default Value: transport1 tcp:any:7090
Valid Values: <transport_name> <type>:<ip-address>:<port> [parameters]
Changes Take Effect: At start/restart

The SIP TCP Transport used by the VRMRecorder Client. Format: sip.transport.x = transport_name type:ip:port

where: transport_name is any string type is udp/tcp/tls ip is the IP address of the network interface that accepts incoming SIP messages port is the port number where SIP stack accepts incoming SIP messages
If ip is an IPv6 address, [] must be used.
To define a transport to listen to all IPv4 interfaces, use "any" or "any4" for ip. To define a transport to listen to all IPv6 interfaces, use "any6" for ip. Remarks: The default transport is the smallest non-empty ID. If all transport.x values are empty, UDP, TCP, and TLS transports will all be enabled and respectively listen from ports 5060, 5060, and 5061 on any network interface. TLS transport will use the certificate, x509_certificate.pem, and key, x509_private_key.pem, in the config directory. UDP will be the default transport.

sip.transport.2

Default Value: transport2 tls:any:7091 TLSv1_2
Valid Values: <transport_name> <type>:<ip-address>:<port> [parameters]
Changes Take Effect: At start/restart

The SIP TLS Transport used by the VRMRecorder Client. Format: sip.transport.x = transport_name type:ip:port [parameters]

where: transport_name is any string type is udp/tcp/tls ip is the IP address of the network interface that accepts incoming SIP messages port is the port number where SIP stack accepts incoming SIP messages [parameters] defines any extra SIP transport parameters. Note that this is for LMSIP2.

If ip is an IPv6 address, [] must be used. To define a transport to listen to all IPv4 interfaces, use "any" or "any4" for ip. To define a transport to listen to all IPv6 interfaces, use "any6" for ip. Example:
cert=[cert path and filename] Applicable to SIPS only and mandatory if using SIPS. The path and the filename of the TLS certificate to be used.
key=[key path and filename] Applicable to SIPS only and mandatory if using SIPS. The path and the filename of the TLS key to be used.
type=[Type of secure transport] Applicable to SIPS only and is optional. The type of secure transport to be used and value can be TLSv1_2, TLSv1_1, TLSv1, SSLv3, or SSLv23. The default value is TLSv1. Note that SSLv2 is no longer supported.
password=[password] Applicable to SIPS only and is optional. The password associated with the certificate and key pair. Required only if key file is password protected.
cafile=[CA cert path and filename] Mandatory for TLS mutual authentication. The path and the

filename of the certificate to be used for verifying the peer. The same certificate specified in cert=[cert path and filename] parameter can be used as the value here if using only 1 certificate is preferred.
verifypeer=true Mandatory for TLS mutual authentication. This parameter turns on the TLS mutual authentication.
verifydepth=[max depth for the certificate chain verification] Applicable only to TLS mutual authentication. This parameter sets the maximum depth for the certificate chain verification. For the default Genesys certificate provided, the recommended value is 1.
tls-cipher-list=[List of ciphers that are applicable for the socket] Applicable only to TLS socket - both server and client sockets. This parameter allows selecting a list of cipher suites used in TLS. This option is transfered to a third-party library and describes a possible set of cipher suites. Refer to https://www.openssl.org/docs/man1.0.2/man1/ciphers.html for Cipher list format. Default is ALL:!EXPORT:!LOW:!aNULL:!eNULL:!SSLv2 Remarks: The default transport is the smallest non-empty ID. If all transport.x values are empty, UDP, TCP, and TLS transports will all be enabled and respectively listen from ports 5060, 5060, and 5061 on any network interface. TLS transport will use the certificate, x509_certificate.pem, and key, x509_private_key.pem, in the config directory. UDP will be the default transport. Note: The max path length supported for certificate and key file is 259 characters.

sip.transport.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.

sip.transport.localaddress

Default Value:
Valid Values: Specify a valid IP Address, hostname or domain name
Changes Take Effect: At start/restart

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

sip.transport.localaddress.srv

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

Specifies whether the mrcpv2client.transport.localaddress contains an SRV domain name. If set to true, port part will not be automatically generated by the SIP stack. Otherwise, the outgoing transport's port will used together with the hostname specified by the vrmrecorder.sip.transport.localaddress.

sip.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.

sip.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).

toheadermode

Default Value: toparams
Valid Values: Choose between: legacy, uriparams, toparams or bothtoanduriparams
Changes Take Effect: Immediately/session

The To Header Mode for Third Party Call Recording. If set to "legacy", the MCP will copy the Request URI of the INVITE request into the To Header, identical to pre-GVP 8.5.0 behavior. If set to "uriparams", the Request URI parameters will be included in the Request URI part of the To Header. If set to "toparams", the Request URI parameters will be included in the To params of the To Header. If set to "bothtoanduriparams", the Request URI parameters will be included in both the Request URI part of the To Header and the To params of the To Header.

websocket.asio_worker_threads

Default Value: 3
Valid Values: Any positive integer value.
Changes Take Effect: At start/restart

Number of threads used to handle WebSocket connections.

websocket.buffer_size

Default Value: 200
Valid Values: A number between 0 and 5000 inclusive, incremented by 20.
Changes Take Effect: Immediately

The duration of audio data (in milliseconds) that will be buffered before delivering it to the server. Must be an integer in the range of 0 to 5000 milliseconds. The value must be a multiple of 20, which is tipically the size of a single packet, otherwise, it will be rounded down. Buffering will be disabled if value is set to 0. Default value is 200 milliseconds.

websocket.ssl_ca_file

Default Value:
Valid Values: Can be an empty string or a valid file name.
Changes Take Effect: Immediately

The file name holding one or more certificates to verify the peer with.

websocket.ssl_ca_path

Default Value:

Valid Values: Can be an empty string or a valid folder path.
Changes Take Effect: Immediately

The path holding multiple CA certificates to verify the peer with. The certificate directory must be prepared using the openssl c_rehash utility.

websocket.ssl_cert

Default Value:
Valid Values: Can be an empty string or a valid file name.
Changes Take Effect: Immediately

The file name of your certificate. The file format must be "PEM".

websocket.ssl_key

Default Value:
Valid Values: Can be an empty string or a valid file name.
Changes Take Effect: Immediately

The file name of the private key. The file format must be "PEM".

websocket.ssl_verify_peer

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

Whether or not to verify the peer's certificate. When this option is set, one of ssl_ca_file or ssl_ca_path should be set.

websocket.streaming_percentage

Default Value: 100
Valid Values: A number between 0 and 100 inclusive.
Changes Take Effect: Immediately

MCP runs an algorithm for every call to verify if it can or cannot be streamed, the algorithm will be based on the percetage provided in this parameter. Therefore, setting the parameter to 100 means that all calls will be streamed, and setting it to 0, means that no calls will be streamed. Default value is 100 percent.

vxmli Section

- ac.allow_if_missing
- ac.allow_if_nomatch
- ac.enabled
- ac.use_platform_host_for_file_url
- asr.release_on_transfer
- beep.uri
- break.strength.medium
- break.strength.strong
- break.strength.weak
- break.strength.x-strong
- break.strength.x-weak
- builtin_path
- cache.document.max_count
- cache.document.max_entry_size
- cache.document.max_size
- compiled_script_cache.enable
- compiled_script_cache.max_cache_size
- compiled_script_cache.max_cached_script_size
- compiled_script_cache.max_cached_scripts_count
- compiled_script_cache.min_cached_script_size
- conformance.disable_application_lastresult_extensions
- conformance.disallow_exec_content_within_prompts
- conformance.rfc5552_bye_reason
- conformance.strict_complete_timeout
- conformance.strict_grammar_mode
- conformance.strict_tts_mode
- conformance.supported_builtin_dtmf
- conformance.supported_builtin_voice
- conformance.supported_grammar_languages
- conformance.supported_tts_languages
- consultationtransfer.result
- data.use_xerces_dom_parser
- data.xmlscript_path
- debug.enabled
- debug.server.ip
- debug.server.port
- debug.server.port.public
- debug.server.tlscert
- debug.server.tlskey
- debug.server.tlspassword
- debug.server.tlsport
- debug.server.tlsport.public
- default.alternate_uri
- default.connecttimeout
- default.xmllang
- defaults_vxml_url
- detailed_fetch_error.enable
- directories.save_tempfiles
- exposevxml.dom
- getinfo_pairs
- grammar.builtin_basepath_linux
- grammar.builtin_basepath_win
- grammar.builtin_baseurl
- grammar.builtin:dtmf/currency
- grammar.builtin:dtmf/date
- grammar.builtin:dtmf/number
- grammar.builtin:dtmf/phone
- grammar.builtin:dtmf/time
- grammar.mimetypes
- grammars.cache_size
- http.accept
- http.user_agent
- http.version
- initial_request_enctype
- initial_request_fetchtimeout
- initial_request_maxage
- initial_request_maxstale
- initial_request_method
- inlinegrammar_by_url
- jsruntime_size
- jsstack_size
- legacy.simple_dtmf_grammars
- local.webserver.basepath_linux
- local.webserver.basepath_win
- local.webserver.baseurl
- logdir
- maintainer.email_subject
- maintainer.enabled
- maintainer.log_message.on_error
- max_application_logfile_size
- max_loop_count
- max_num_documents
- max_num_sessions
- max_runtime_error
- max_script_time
- max_scripturl_length
- max_size.script_file
- max_size.vxml_page
- max_size.xml_data

- max_subdialog_depth
- messaging.enabled
- num_session_processing_threads
- oem_namespace
- performjsgc_on_subdialogreturn
- recording.basepath
- recordutterance.path
- savetmpfiles.max_bytes
- script_max_loop
- session_vars
- tmpdir
- transfer.allowed
- tts.defaultengine
- universals_path_linux
- universals_path_win
- universals.cancel
- universals.exit
- universals.help
- use_isdn_mapping
- userdata.convert_name_to_lowercase
- userdata.prefix

ac.allow_if_missing

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

Used for data. Determines the behaviour when fetched XML data does not contain any access-control processing instructions. This parameter only has an effect if ac.enabled is set to true. A value of true means to allow access to XML data if access-control directive is missing. A value of false means to disallow access to XML data if access-control directive is missing.

ac.allow_if_nomatch

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

Used by the data tag. This determines the behaviour of access-control when the host machine does not appear in any access-control directive. This parameter only has an effect if ac.enabled is set to true.

ac.enabled

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

Controls support for access-control when using the data tag

ac.use_platform_host_for_file_url

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

Used for the data element. It determines the behaviour when the VoiceXML page accessing the XML data is a file URI. When set to true it will force access-control to use the hostname of the platform when verifying access-control instructions. When set to false, access will be allowed if VoiceXML page is a file URI.

asr.release_on_transfer

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

If the value is true, all open ASR engines will be released upon a successful transfer (where no speech grammars are loaded). If the value is false, no open ASR engines will be released upon a successful transfer.

beep.uri

Default Value: file://$InstallationRoot$/audio/ulaw/default_audio/endofprompt.vox
Valid Values: Please specify a valid URI to the beep file.
Changes Take Effect: At start/restart

The URI (can be either file:// or http://) of the beep file to be played when beep="true" in the record tag.

break.strength.medium

Default Value: 500
Valid Values: A number between 1 and 1000000 inclusive.
Changes Take Effect: At start/restart

Specifies the time in milliseconds that the Interpreter should use when encountering a break with the specified strength. This value will be ignored if the break is rendered by a TTS service.

break.strength.strong

Default Value: 1000
Valid Values: A number between 1 and 1000000 inclusive.

Changes Take Effect: At start/restart

Specifies the time in milliseconds that the Interpreter should use when encountering a break with the specified strength. This value will be ignored if the break is rendered by a TTS service.

break.strength.weak

Default Value: 200
Valid Values: A number between 1 and 1000000 inclusive.
Changes Take Effect: At start/restart

Specifies the time in milliseconds that the Interpreter should use when encountering a break with the specified strength. This value will be ignored if the break is rendered by a TTS service.

break.strength.x-strong

Default Value: 2000
Valid Values: A number between 1 and 1000000 inclusive.
Changes Take Effect: At start/restart

Specifies the time in milliseconds that the Interpreter should use when encountering a break with the specified strength. This value will be ignored if the break is rendered by a TTS service.

break.strength.x-weak

Default Value: 50
Valid Values: A number between 1 and 1000000 inclusive.
Changes Take Effect: At start/restart

Specifies the time in milliseconds that the Interpreter should use when encountering a break with the specified strength. This value will be ignored if the break is rendered by a TTS service.

builtin_path

Default Value: $InstallationRoot$/audio/ulaw/
Valid Values: Please specify a valid file system path.
Changes Take Effect: At start/restart

This parameter indicates the main path to search for builtin audio files

cache.document.max_count

Default Value: 50
Valid Values: Must be an integer greater than or equal to 0.
Changes Take Effect: At start/restart

The maximum number of documents that may be cached concurrently.

cache.document.max_entry_size

Default Value: 100000
Valid Values: Must be an integer greater than or equal to 0.
Changes Take Effect: At start/restart

The maximum size of each cached document in bytes.

cache.document.max_size

Default Value: 1000000
Valid Values: Must be an integer greater than or equal to 0.
Changes Take Effect: At start/restart

The maximum size, in bytes, of all concurrently cached documents.

compiled_script_cache.enable

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

Used to enabled ECMAScript caching in the VoiceXML interpreter.

compiled_script_cache.max_cache_size

Default Value: 2000000
Valid Values: A number between 0 and 50000000 inclusive.
Changes Take Effect: At start/restart

The maximum size, in bytes, of all concurrently cached scripts.

compiled_script_cache.max_cached_script_size

Default Value: 100000
Valid Values: A number between 0 and 1000000000 inclusive.Note that if minimum script size given by complied_script_cache.min_cached_script_size is set to a non-zero value then max size specified by this configuration parameter should be greater than the minimum script size for the script to be cached successfully.
Changes Take Effect: At start/restart

The maximum size, in bytes, of a script to be cached.

compiled_script_cache.max_cached_scripts_count

Default Value: 10000
Valid Values: A number between 0 and 1000000 inclusive.
Changes Take Effect: At start/restart

The maximum number of scripts that may be cached concurrently.

compiled_script_cache.min_cached_script_size

Default Value: 200
Valid Values: A number between 0 and 1000000000 inclusive.
Changes Take Effect: At start/restart

The minimum size, in bytes, of a script to be cached.

conformance.disable_application_lastresult_extensions

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

When set to true, none of the additional extension properties of the application.lastresult$ object are set when a result is exposed.

conformance.disallow_exec_content_within_prompts

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

When set to true, executable content is not permitted inside foreach, when the foreach is inside a prompt.

conformance.rfc5552_bye_reason

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

Indicates whether the interpreter will conform to RFC5552, in terms of including reason= in the body of the SIP BYE message. When it is set to false, the message will not have the __reason entry.

conformance.strict_complete_timeout

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

When set to true, the interpreter will calculate the maximum of the completetimeout and incompletetimeout values as the value for the incompletetimeout.

conformance.strict_grammar_mode

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

Indicates whether the interpreter will follow the VoiceXML specification strictly when handling the grammar element. Specifically, when set to false it will NOT ignore the mode attribute for an external grammar.

conformance.strict_tts_mode

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

Indicates whether the Interpreter will be strict in conformance of the tts mode. The TTS language will be checked against the list specified in conformance.supported_tts_languages.

conformance.supported_builtin_dtmf

Default Value: boolean digits currency date number phone time
Valid Values: Can be an empty string or a space separated list of dtmf build-in grammars.
Changes Take Effect: At start/restart

Indicates the platform supported dtmf built-in grammars when strict grammar mode is enabled. This is a space delimited list.

conformance.supported_builtin_voice

Default Value: boolean digits currency date number phone time universals/Cancel universals/Exit universals/Help
Valid Values: Can be an empty string or a space separated list of voice build-in grammars.
Changes Take Effect: At start/restart

Indicates the platform supported voice built-in grammars when strict grammar mode is enabled. This is a space delimited list.

conformance.supported_grammar_languages

Default Value: en-US
Valid Values: A space separated list of language codes.
Changes Take Effect: At start/restart

Indicates the grammar languages supported. Note that this is only meaningful when conformance.strict_grammar_mode is enabled.

conformance.supported_tts_languages

Default Value: en-US
Valid Values: A space separated list of language codes.
Changes Take Effect: At start/restart

Indicates the tts languages supported. This is a '|' delimited list.

consultationtransfer.result

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

Specifies whether consultation transfer result would be exposed to parent page during multiphase transfer.

data.use_xerces_dom_parser

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

Choose the XML DOM parser for data tag. Setting this to true is to choose Xerces XML parser; else XML for script is used.

data.xmlscript_path

Default Value: $InstallationRoot$/script/
Valid Values: Please specify a valid path to a folder.
Changes Take Effect: At start/restart

The path of the java script files which are required if XML for script is used for the XML DOM parser. The names of the XML DOM parsing script files are xmlsax.js and xmlw3dom.js, and they should exist in this path

debug.enabled

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

Enable real time debugging for the platform.

debug.server.ip

Default Value: default
Valid Values: Please specify a valid IP address.
Changes Take Effect: At start/restart

The IP address that the debugging client should use to connect to the platform. The platform reports this value to the debugging client via SIP 18x response. A value of "default" means that the platform will determine the IP address programmatically.

debug.server.port

Default Value: 27666
Valid Values: An integer between 1025 and 65535 inclusive. or 0 to disable this port
Changes Take Effect: At start/restart

The TCP port that the platform will accept socket connections from the debugging client. Setting to 0 will disable this port.

debug.server.port.public

Default Value: 27666
Valid Values: An integer between 1025 and 65535 inclusive.
Changes Take Effect: At start/restart

The TCP port that the debugging client should use to connect to the platform. The platform reports this value to the debugging client via SIP 18x response. This value is publicly exposed and may be different from debug.server.port if a firewall separates the platform and the debugging client.

debug.server.tlscert

Default Value: $InstallationRoot$/config/x509_certificate.pem
Valid Values: Please specify a valid path to the TLS Certificate.
Changes Take Effect: At start/restart

The path and file name of the TLS Certificate. This is required to establish a TLS connection between the debugging client and the platform.

debug.server.tlskey

Default Value: $InstallationRoot$/config/x509_private_key.pem
Valid Values: Please specify a valid path to the TLS Key.
Changes Take Effect: At start/restart

The path and file name of the TLS Key. This is required to establish a TLS connection between the debugging client and the platform.

debug.server.tlspassword

Default Value:
Valid Values: Please specify TLS Key password.
Changes Take Effect: At start/restart

The password required to use the TLS Key, if the TLS Key is password protected.

debug.server.tlsport

Default Value: 27668
Valid Values: An integer between 1025 and 65535 inclusive, or 0 to disable the port.
Changes Take Effect: At start/restart

The TLS port that the platform will accept socket connections from the debugging clients. Setting to 0 will disable this port.

debug.server.tlsport.public

Default Value: 27668
Valid Values: An integer between 1025 and 65535 inclusive.
Changes Take Effect: At start/restart

The TLS port that the debugging clients should use to connect to the platform. The platform reports this value to the debugging client via SIP 18x response. This value is publicly exposed and may be different from debug.server.tlsport if a firewall separates the platform and the debugging clients.

default.alternate_uri

Default Value:
Valid Values: Please specify a valid URI address.
Changes Take Effect: At start/restart

The value to use for an alternate URI when the main one can not be fetched.

default.connecttimeout

Default Value: 30000
Valid Values: A number between 0 and 1000000 inclusive.
Changes Take Effect: At start/restart

The default value to use for a transfer's connecttimeout attribute if not provided. Applies to bridge or consultation transfers. Specified in milliseconds.

default.xmllang

Default Value: en-US

Valid Values: A valid language code.
Changes Take Effect: At start/restart

The default value to use for xml:lang when it is not provided in the document.

defaults_vxml_url

Default Value: file://$InstallationRoot$/config/defaults-ng.vxml
Valid Values: Please specify a valid path to a VoiceXML file.
Changes Take Effect: At start/restart

This parameter specifies the defaults.vxml path if a default root page is not specified in the DNIS-URL mapping.

detailed_fetch_error.enable

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

Specifies whether a more detailed fetch error should be generated. If enabled, a different error id and trap is generated for fetching errors of type 4xx, all other fetching errors will be handled as usual. In addition, the CallId is included to all fetching error log message.

directories.save_tempfiles

Default Value: $InstallationRoot$/tmp/
Valid Values: Please specify a valid path.
Changes Take Effect: At start/restart

The directory in which to save tempfiles.

expose.nlsml.dom

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

Instructs the interpreter whether to expose the NLSML result from the recognizer as a DOM object in application.lastresult$.xmlresult. A value of true means to expose NLSML result from recognizer. A value of false means not to expose NLSML result from recognizer. When this feature is enabled, it may consume large amount of CPU and memory resource if the application has application.lastresult$ as namelist value in various VoiceXML tags, such as <return> in a subdialog.

getinfo_pairs

Default Value:
Valid Values: Can be an empty string or a comma separated list of <param>=<value> items.
Changes Take Effect: Immediately

It is used to set up the valid input parameter and its value for function _VGGetInfo(parameter) / _GetInfo(parameter). The list is comma-delimited, and each item in the list must be in the format <param>=<value>, for example hostaddr=www.genesyslab.com,company=genesys.

grammar.builtin_basepath_linux

Default Value:
Valid Values: Please specify a valid Linux folder path.
Changes Take Effect: At start/restart

Builtin grammar base path. This parameter is effective when parameter inlinegrammar_by_url is set to false.

grammar.builtin_basepath_win

Default Value:
Valid Values: Please specify a valid Windows folder path.
Changes Take Effect: At start/restart

Builtin grammar base path. This parameter is effective when parameter inlinegrammar_by_url is set to false.

grammar.builtin_baseurl

Default Value:
Valid Values: Please specify a valid URL address.
Changes Take Effect: At start/restart

The base URL to be used when exposing builtin dtmf grammars as a URL to be fetched by an offboard speech engine. This parameter is effective only when parameter inlinegrammar_by_url is set to true.

grammar.builtin:dtmf/currency

Default Value: dtmf/currency.grxml
Valid Values: please specify a relative path to the builtin currency grammar file.

Changes Take Effect: At start/restart

Builtin currency grammar path relative to grammar.builtin_basepath_win or grammar.builtin_basepath_linux or grammar.builtin_baseurl.

grammar.builtin:dtmf/date

Default Value: dtmf/date.grxml
Valid Values: please specify a relative path to the builtin date grammar file.
Changes Take Effect: At start/restart

Builtin date grammar path relative to grammar.builtin_basepath_win or grammar.builtin_basepath_linux or grammar.builtin_baseurl.

grammar.builtin:dtmf/number

Default Value: dtmf/number.grxml
Valid Values: please specify a relative path to the builtin number grammar file.
Changes Take Effect: At start/restart

Builtin number grammar path relative to grammar.builtin_basepath_win or grammar.builtin_basepath_linux or grammar.builtin_baseurl.

grammar.builtin:dtmf/phone

Default Value: dtmf/phone.grxml
Valid Values: please specify a relative path to the builtin phone grammar file.
Changes Take Effect: At start/restart

Builtin phone grammar path relative to grammar.builtin_basepath_win or grammar.builtin_basepath_linux or grammar.builtin_baseurl.

grammar.builtin:dtmf/time

Default Value: dtmf/time.grxml
Valid Values: please specify a relative path to the builtin time grammar file.
Changes Take Effect: At start/restart

Builtin time grammar path relative to grammar.builtin_basepath_win or grammar.builtin_basepath_linux or grammar.builtin_baseurl.

grammar.mimetypes

Default Value: application/srgs+xml|.grxml|application/srgs|.srgs|Media-Type|.grammar|application/x-abnf|.abnf
Valid Values: Can be an empty string or a '|' separated list of mime types.
Changes Take Effect: At start/restart

When vxmli.inlinegrammar_by_url is enabled, the interpreter exposes inline grammars as external grammars for an offboard speech engines as a URL reference, by a locally configured web server. This parameter defines the mappings between the media type of the grammars to the file extension of the exposed URL. The web server should be configured with the same mapping so that the media type of the grammar is exposed correctly to the speech engines. When vxmli.inlinegrammar_by_url is disabled, the interpreter exposes the inline grammar directly in the MRCP request. The mimetypes defined in this parameter are used to verify the type attribute specified in the grammar element.

grammars.cache_size

Default Value: 50000
Valid Values: A number between 1 and 1000000 inclusive.
Changes Take Effect: At start/restart

The amount of memory to allocate for caching grammars. This is slightly more than 100 bytes per grammar.

http.accept

Default Value:
Valid Values: Can be an empty string or a list of mime types according to the HTTP specification.
Changes Take Effect: At start/restart

Specifies the acceptable mime types for fetched resources. If left to empty, it takes on a value of "*/*"

http.user_agent

Default Value: NGi/$VERSION$
Valid Values: Specify a valid HTTP user agent.
Changes Take Effect: At start/restart

Specifies the HTTP user agent to use when fetching resources. If $VERSION$ is contained in the value, it will be replaced with the actual GVP product version info.

http.version

Default Value: 1.1
Valid Values: Choose between: 1.0 or 1.1
Changes Take Effect: At start/restart

Specifies the http version to use when fetching resources. Specify 1.0 or 1.1. Default value is 1.1.

initial_request_enctype

Default Value: application/x-www-form-urlencoded
Valid Values: Please specify a valid HTTP encoding type.
Changes Take Effect: At start/restart

The HTTP encoding type to use for the initial request when the request method is POST

initial_request_fetchtimeout

Default Value: 30000
Valid Values: A number between 0 and 1000000 inclusive.
Changes Take Effect: At start/restart

The fetch timeout (in ms) of the initial VXML document. If document fetch is not completed within this time, the fetch is considered to have failed and the call will be rejected. If value is set to 0, the parameter will be ignored and 60000 will be used instead.

initial_request_maxage

Default Value: -1
Valid Values: An integer greater or equal to -1
Changes Take Effect: At start/restart

Specifies the maximum age (in ms) of content that the VXML document is willing to use. -1 if undefined. The document is not willing to use stale content, unless initial_request_maxstale is defined. Note that since the initial page fetch always include the session id, it is nearly impossible to have this option be meaningful for the initial page. It is, however, meaningful for the initial root page.

initial_request_maxstale

Default Value: -1
Valid Values: An integer between -1 and 1000000 inclusive.
Changes Take Effect: At start/restart

Specifies the maximum amount of time (in ms) past content expiration that the VXML document is willing to accept. -1 if undefined.

initial_request_method

Default Value: GET
Valid Values: Choose between: GET or POST
Changes Take Effect: At start/restart

The HTTP method to use for the initial request

inlinegrammar_by_url

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

If this is enabled, NGI hosts inline grammars using the local web server and passes the grammar URL to the MRCP server. This allows NGI to share the same grammar URL among multiple recognitions to optimize loading of grammar. If this is disabled, NGI passes the inline grammar directly to the MRCP server in the MRCP request.

jsruntime_size

Default Value: 64
Valid Values: A number between 1 and 64 inclusive.
Changes Take Effect: At start/restart

Specifies the size of each JavaScript Engine Runtime in MB.

jsstack_size

Default Value: 16384
Valid Values: A number between 1 and 2097152 inclusive.
Changes Take Effect: At start/restart

Specifies the stack size of each JavaScript Engine context in byte.

legacy.simple_dtmf_grammars

Default Value: false

Valid Values: Choose between: true or false
Changes Take Effect:

When set to true this parameter tells the interpreter to support certain inline legacy DTMF grammars that do not follow proper ABNF syntax.

local.webserver.basepath_linux

Default Value:
Valid Values: Please specify a valid Linux folder path.
Changes Take Effect: At start/restart

This is the path on the local file system where the interpreter writes the inline grammar files, so that the onboard web server can expose the grammar as a URL to an offboard speech engine.

local.webserver.basepath_win

Default Value:
Valid Values: Please specify a valid Windows folder path.
Changes Take Effect: At start/restart

This is the path on the local file system where the interpreter writes the inline grammar files, so that the onboard web server can expose the grammar as a URL to an offboard speech engine.

local.webserver.baseurl

Default Value:
Valid Values: Please specify a valid URL.
Changes Take Effect: At start/restart

This is the base URL to be used when exposing inline grammars as a URL to be fetched by an offboard speech engine.

logdir

Default Value: $InstallationRoot$/logs/
Valid Values: please specify a valid folder path.
Changes Take Effect: At start/restart

The directory for logs created from the log element with destination file.

maintainer.email_subject

Default Value: Message from GVP to Application Maintainer
Valid Values: Please specify an email address.
Changes Take Effect: At start/restart

The text to use as the subject for Maintainer Email messages.

maintainer.enabled

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

If true, the maintainer email feature is enabled. Otherwise, it is disabled.

maintainer.log_message.on_error

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

Controls whether the Interpreter will create a log message for the maintainer package automatically, when an error is thrown. A value of true means message is logged on errors. A value of false means no message is logged on errors.

max_application_logfile_size

Default Value: 524288000
Valid Values: A number between 0 and 2147483647 inclusive.
Changes Take Effect: At start/restart

The maximum size in bytes of an application log file which can be logged by using the log element with dest value set to file.

max_loop_count

Default Value: 1000
Valid Values: A number between 0 and 1000000 inclusive.
Changes Take Effect: At start/restart

Maximum number of runtime loops is allowed between waiting states in an application execution. The runtime loop count will be increased when any form item, event handler and an iteration of the foreach element is executed. And the counter will be reset at a waiting state (e.g. waiting for user input, recording and transferring call).

max_num_documents

Default Value: 5000
Valid Values: A number between 1 and 1000000 inclusive.
Changes Take Effect: At start/restart

This parameter specifies the maximum number of cacheable documents

max_num_sessions

Default Value: 10000
Valid Values: A number between 1 and 1000000 inclusive.
Changes Take Effect: At start/restart

The maximum number of permitted concurrent sessions

max_runtime_error

Default Value: 1000
Valid Values: A number between 0 and 100000 inclusive.
Changes Take Effect: At start/restart

Maximum number of runtime application errors is allowed. The runtime error count will be increased when any application run time error is encountered.

max_script_time

Default Value: 2000
Valid Values: A number between 0 and 10000000 inclusive.
Changes Take Effect: At start/restart

Maximum duration in millisecond is allowed for each script or ECMAScript expression execution.

max_scripturl_length

Default Value: 16384
Valid Values: A number between 0 and 65000 inclusive.
Changes Take Effect: At start/restart

When the scripturl length exceeds the above value, MCP will throw sematic error while processing the script tag. There will be no limit when it's set to 0.

max_size.script_file

Default Value: 0
Valid Values: A number between 1000 and 1000000000 inclusive. Or 0 to disable the limit.
Changes Take Effect: At start/restart

Maximum Size allowed in bytes of the script file. If the limit is exceeded, it will result in a badfetch.

max_size.vxml_page

Default Value: 0
Valid Values: A number between 1000 and 1000000000 inclusive. Or 0 to disable the limit.
Changes Take Effect: At start/restart

Maximum Size allowed in bytes of the VXML Document. If the limit is exceeded, it will result in a badfetch.

max_size.xml_data

Default Value: 0
Valid Values: A number between 1000 and 1000000000 inclusive. Or 0 to disable the limit.
Changes Take Effect: At start/restart

Maximum Size allowed in bytes of the XML/JSON data. If the limit is exceeded, it will result in a badfetch.

max_subdialog_depth

Default Value: 50
Valid Values: A number between 1 and 1000 inclusive.
Changes Take Effect: At start/restart

Maximum depth of subdialogs allowed in a VXML session. The subdialog depth increments when a subdialog is entered, and the depth decrements when a subdialog is returned.

messaging.enabled

Default Value: true

Valid Values: Choose between: true or false
Changes Take Effect:

When set to true the send and receive tags function as normal. Otherwise, these tags are not permitted in VoiceXML pages.

num_session_processing_threads

Default Value: 8
Valid Values: A number between 0 and 1000 inclusive.
Changes Take Effect: At start/restart

The total number of VXML page execution threads to create.

oem_namespace

Default Value: http://www.genesyslab.com/2006/vxml21-extension http://www.voicegenie.com/2006/vxml21-extension
Valid Values: Can be an empty string or a space separated list of XML-namespace extentions.
Changes Take Effect: At start/restart

This defines the XML-namespace the applications must use for the non-standard, extension features. Each extension XML attribute/element must be defined in this namespace.

performjsgc_on_subdialogreturn

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

Specifies whether to perform JavaScript Engine garbage collection during subdialog return.

recording.basepath

Default Value: $InstallationRoot$/record
Valid Values: Please specify a valid file system path.
Changes Take Effect: At start/restart

This parameter indicates the base path where the dest/destexpr/filename/filenameexpr attributes of record are based upon.

recordutterance.path

Default Value: $InstallationRoot$/utterance
Valid Values: Please specify a valid file system path.
Changes Take Effect: At start/restart

This parameter indicates the parent directory where all the recorded utterance files are saved, when the user has specified the sub-directory name using com.voicegenie.utterancedest or vg:utterancedest.

savetmpfiles.max_bytes

Default Value: 100000000
Valid Values: A number between 0 and 2000000000 inclusive.
Changes Take Effect: At start/restart

Maximum bytes allowed for the total saved temp files per session. If the limit is exceeded, savetmpfiles will be disabled for the applicable session.

script_max_loop

Default Value: 1000000
Valid Values: A number between 0 and 10000000 inclusive.
Changes Take Effect: At start/restart

Maximum number of loops is allowed in each script or ECMAScript expression execution. The loop counter will be increased by 1 when a script branches backward during execution and when a function returns.

session_vars

Default Value:
session.connection.local.uri|LOCALURI|1|session.connection.remote.uri|REMOTEURI|1|session.connection.originator
Valid Values: <session-variable>|<variable-name>|(0|1|2|3)[|<session-variable>|<variable-name>|(0|1|2|3)]*
Changes Take Effect: At start/restart

Each session variable entry is composed of three components. The first component is the session variable name as exposed within VoiceXML. The second component is the variable name sent back from the Call Manager. The third component indicates either whether the session variable will be included in the request for the initial page URL (0 = do not include, 1 = include in GET, 2 = include in POST, 3 = include in GET and POST), or the type of array of the session variable (6 = associative array, 7 = array specific for draft-burke). This is a '|' delimited list. Besides the default variables, session.connection.protocol.sip.body (session.connection.protocol.sip.body|Sip.Body|0) contains string in initial SIP INVITE body. For INVITE without body, the variable is 'undefined'. The variable session.connection.record (session.connection.record|Record.Status|0) will hold the status of only IVR-Recording, it does not apply for FCR nor the recordings initiated using record tag in VXML.

tmpdir

Default Value: $InstallationRoot$/tmp/
Valid Values: please specify a valid folder path.
Changes Take Effect: At start/restart

Temp directory that exists on the platform

transfer.allowed

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

Indicates whether transfers should be permitted

tts.defaultengine

Default Value: default
Valid Values: The engine name must be a string.
Changes Take Effect: Immediately

The engine specified here will be used as the default TTS engine. An application using a different name should override this using the Request URI configuration or the ttsengine property.

universals_path_linux

Default Value:
Valid Values: Please specify a valid Linux file system path.
Changes Take Effect: At start/restart

The path on the local file system where the universal grammar files are stored.

universals_path_win

Default Value:
Valid Values: Please specify a valid Windows file system path.
Changes Take Effect: At start/restart

The path on the local file system where the universal grammar files are stored.

universals.cancel

Default Value: builtin:grammar/universals/Cancel
Valid Values: A location or URL of the universal cancel grammar.
Changes Take Effect: At start/restart

This parameter specifies the universal cancel grammar used by the platform

universals.exit

Default Value: builtin:grammar/universals/Exit
Valid Values: A location or URL of the universal exit grammar.
Changes Take Effect: At start/restart

This parameter specifies the universal exit grammar used by the platform

universals.help

Default Value: builtin:grammar/universals/Help
Valid Values: A location or URL of the universal help grammar.
Changes Take Effect: At start/restart

This parameter specifies the universal help grammar used by the platform

use_isdn_mapping

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

This parameter controls whether the disconnected return status of the outbound leg should be derived from ISDN code or internal disconnect reason. 0: uses internal disconnect reason
1: uses ISDN code

userdata.convert_name_to_lowercase

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

Whether or not to convert the userdata name to lower case.

userdata.prefix

Default Value: X-Genesys-
Valid Values: Please specify a valid SIP header prefix.
Changes Take Effect: At start/restart

This is a string that, when used as a prefix in a SIP header, identifies userdata variables.

Reporting Server

Options for this component are contained in the following configuration sections:

- activemqtlsKeyStore
- activemqtlsTrustStore
- agentx
- cdr
- dbmp
- https
- https_key
- imdb
- latency
- log
- messaging
- persistence
- reporting
- schedule
- snmp
- sqa

Tip

In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.

Power users: Download a CSV file containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
activemqtlsKeyStore	activemq.tlsKeyStore	keystore.ks	at start/restart
activemqtlsKeyStore	password		at start/restart
activemqtlsTrustStore	activemq.tlsTrustStore	client.ks	at start/restart
activemqtlsTrustStore	password		at start/restart
agentx	connection_delay_sec	60	at start/restart
agentx	max_connection_attempt	-1	at start/restart
cdr	call-timeout	180	at start/restart
cdr	db-maintenance-batch-size	5	at start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
cdr	max-page-count	10	at start/restart
cdr	max-page-size	100	at start/restart
cdr	media-service-cdrs.reduce	true	at start/restart
cdr	or-call-counting.enable	true	at start/restart
dbmp	rs.db.retention.cdr.default	30	immediately
dbmp	rs.db.retention.events.default	7	immediately
dbmp	rs.db.retention.latencies.daily.default	90	immediately
dbmp	rs.db.retention.latencies.hourly.default	7	immediately
dbmp	rs.db.retention.latencies.monthly.default	1095	immediately
dbmp	rs.db.retention.latencies.weekly.default	364	immediately
dbmp	rs.db.retention.operations.30min.default	7	immediately
dbmp	rs.db.retention.operations.5min.default	1	immediately
dbmp	rs.db.retention.operations.daily.default	90	immediately
dbmp	rs.db.retention.operations.hourly.default	7	immediately
dbmp	rs.db.retention.operations.monthly.default	1095	immediately
dbmp	rs.db.retention.operations.weekly.default	364	immediately
dbmp	rs.db.retention.sq.daily.default	90	immediately
dbmp	rs.db.retention.sq.failures.default	365	immediately
dbmp	rs.db.retention.sq.hourly.default	7	immediately
dbmp	rs.db.retention.sq.monthly.default	365	immediately
dbmp	rs.db.retention.sq.weekly.default	180	immediately
dbmp	rs.db.retention.var.30min.default	7	immediately
dbmp	rs.db.retention.var.5min.default	1	immediately
dbmp	rs.db.retention.var.daily.default	90	immediately
dbmp	rs.db.retention.var.hourly.default	7	immediately
dbmp	rs.db.retention.var.monthly.default	1095	immediately
dbmp	rs.db.retention.var.weekly.default	364	immediately
https	https.certificate.algorithm	SunX509	at start/restart
https	https.client.authentication	none	at start/restart
https	https.connector.type	2	at start/restart
https	https.keystore.path	${user.home}/.keystore	at start/restart
https	https.keystore.type	JKS	at start/restart
https	https.protocol	TLS	at start/restart
https	https.random.algorithm		at start/restart
https	https.security.provider		at start/restart
https	password		at start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
https_key	password		at start/restart
imdb	imdb-max-cdr-queries	3	at start/restart
imdb	imdb-query-lock-timeout	1000	at start/restart
latency	threshold.asr_input_response	2000	at start/restart
latency	threshold.audio_fetch	1000	at start/restart
latency	threshold.call_answer	2000	at start/restart
latency	threshold.call_reject	2000	at start/restart
latency	threshold.cumulative_response	2000	at start/restart
latency	threshold.data_fetch	2000	at start/restart
latency	threshold.dtmf_input_response	2000	at start/restart
latency	threshold.grammar_fetch	1000	at start/restart
latency	threshold.inbound_first_prompt	2000	at start/restart
latency	threshold.initial_response	4000	at start/restart
latency	threshold.interprompt	2000	at start/restart
latency	threshold.java_script_execution	50	at start/restart
latency	threshold.java_script_fetch	1000	at start/restart
latency	threshold.mrcp_asr_session_establish	100	at start/restart
latency	threshold.mrcp_asr_set_params	100	at start/restart
latency	threshold.mrcp_asr_stop	100	at start/restart
latency	threshold.mrcp_define_grammar	500	at start/restart
latency	threshold.mrcp_recognize	500	at start/restart
latency	threshold.mrcp_speak	100	at start/restart
latency	threshold.mrcp_tts_session_establish	100	at start/restart
latency	threshold.mrcp_tts_set_params	100	at start/restart
latency	threshold.mrcp_tts_stop	100	at start/restart
latency	threshold.noinput_response	2000	at start/restart
latency	threshold.outbound_first_prompt	2000	at start/restart
latency	threshold.page_compile	100	at start/restart
latency	threshold.page_fetch	1500	at start/restart
latency	threshold.recording_response	2000	at start/restart
latency	threshold.transfer_response	2000	at start/restart
log	all		immediately
log	debug	logs/rs.log	immediately
log	expire	false	immediately
log	interaction		immediately
log	message_format	full	immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
log	segment	10MB	immediately
log	standard	stdout	immediately
log	time_format	time	immediately
log	trace		immediately
log	verbose	trace	immediately
messaging	activemq.connectionMode	0	at start/restart
messaging	activemq.dataDirectory	data/activemq	at start/restart
messaging	activemq.diskStoreUsageLimit	256 gb	at start/restart
messaging	activemq.needClientAuth	false	at start/restart
messaging	activemq.serverIP		At start/restart
messaging	activemq.tlsKeyStore	keystore.ks	at start/restart
messaging	activemq.tlsPort	61617	at start/restart
messaging	activemq.tlsServerIP		At start/restart
messaging	activemq.tlsTrusStorePassword		at start/restart
messaging	activemq.tlsTrustStore	client.ks	at start/restart
messaging	activemq.useJmx	false	at start/restart
messaging	password		at start/restart
messaging	port	61616	at start/restart
messaging	tlsKeyStorePassword		at start/restart
persistence	hibernate.remote.database		at start/restart
persistence	hibernate.remote.dialect		at start/restart
persistence	hibernate.remote.driver		at start/restart
persistence	hibernate.remote.url		at start/restart
persistence	hibernate.remote.user		at start/restart
persistence	password		at start/restart
persistence	rs.histonly.enabled	false	at start/restart
persistence	rs.nodb.enabled	false	at start/restart
persistence	rs.storage.metricsfilter	*	at start/restart
reporting	binding.address		at start/restart
reporting	db.query.timeout.max	60	immediately
reporting	hostname		at start/restart
reporting	password		at start/restart
reporting	port	8080	at start/restart
reporting	protocol	http	at start/restart
reporting	response.header	X-Frame-Options: DENY	at start/restart
reporting	response.header.landingpage	X-Frame-Options: DENY	at start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
reporting	retrieveMultipleObjectsTimeoutValue	180000	at start/restart
reporting	rs.query.limit.30min	336	immediately
reporting	rs.query.limit.5min	288	immediately
reporting	rs.query.limit.day	92	immediately
reporting	rs.query.limit.hour	168	immediately
reporting	rs.query.limit.month	36	immediately
reporting	rs.query.limit.week	53	immediately
reporting	rs.summarization.buffer	60	at start/restart
reporting	usehostname-in-ruri	false	at start/restart
reporting	username		at start/restart
schedule	quartz.rs.calltimeout	0 50 * * * ?	at start/restart
schedule	quartz.rs.dbMaintenancePeriod	0 30 1 * * ?	at start/restart
schedule	quartz.rs.dbPartitioningPeriod	0 0 0/1 * * ?	at start/restart
schedule	quartz.rs.or.counting	0 40 * * * ?	at start/restart
schedule	quartz.var.summarization	300000	at start/restart
snmp	bulk.size	50	
snmp	polling.interval	60	
snmp	timeout	30000	immediately
sqa	error.notification.threshold	95	immediately
sqa	monitor.min.alert.number	100	immediately
sqa	monitor.min.latency.warn.number	100	immediately
sqa	service.quality.period	900	At start/restart
sqa	stat.update.interval	900	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

activemqtlsKeyStore Section

- activemq.tlsKeyStore
- password

activemq.tlsKeyStore

Default Value: keystore.ks
Valid Values: Path to the keystore file
Changes Take Effect: at start/restart

Path to the Java keystore file containing the cryptographic key and trusted certificate entries needed by the ActiveMQ broker for TLS/SSL support.

password

Default Value:
Valid Values: ActiveMQ broker keystore password
Changes Take Effect: at start/restart

The password needed to open the keystore used by the ActiveMQ broker.

activemqtlsTrustStore Section

- activemq.tlsTrustStore
- password

activemq.tlsTrustStore

Default Value: client.ks
Valid Values: Path to the TrustStore file
Changes Take Effect: at start/restart

Path to the Java TrustStore file containing the trusted certificate entries needed by the ActiveMQ broker for TLS/SSL support.

password

Default Value:
Valid Values: ActiveMQ broker TrustStore password
Changes Take Effect: at start/restart

The password needed to open the TrustStore used by the ActiveMQ broker.

agentx Section

connection_delay_sec

Default Value: 60
Valid Values: An integer greater than 0
Changes Take Effect: at start/restart

The number of SECONDS to wait between each reconnection attempt to SNMP Master Agent.

max_connection_attempt

Default Value: -1
Valid Values: An integer greater than 0
Changes Take Effect: at start/restart

The maximum connection attempts to be made by the SNMP Subagent to SNMP Master Agent. Value if not set or value lesser than or equal to 0 means no limit on number of attempts.

cdr Section

- call-timeout
- db-maintenance-batch-size
- max-page-count
- max-page-size
- media-service-cdrs.reduce
- or-call-counting.enable

call-timeout

Default Value: 180
Valid Values: An integer from 1 - 1440 inclusive
Changes Take Effect: at start/restart

Specifies the amount of time, in minutes, until a call is considered 'timed out' from the perspective of VAR and CDR reporting

db-maintenance-batch-size

Default Value: 5
Valid Values: An integer from 1 - 1440 inclusive
Changes Take Effect: at start/restart

Specifies the maximum duration, in minutes, to process in a batch for services that support batch purging

max-page-count

Default Value: 10
Valid Values: An integer from 1 - 100 inclusive
Changes Take Effect: at start/restart

The maximum number of pages that will be returned in any given CDR or Call Events report request

max-page-size

Default Value: 100

Valid Values: An integer from 1 - 10000 inclusive
Changes Take Effect: at start/restart

The maximum number of records per page that will be returned in any given CDR or Call Events report request

media-service-cdrs.reduce

Default Value: true
Valid Values:
Changes Take Effect: at start/restart

When this option is set to true the following CDRs will not be stored to the remote database: Any RM CDR or MCP CDR with media service type set to: media, cpd, record or conference.

or-call-counting.enable

Default Value: true
Valid Values:
Changes Take Effect: at start/restart

When this option is set to true the RS will calculate peaks and arrivals for MCP VXML calls and MCP Treatment calls (without VXML).

dbmp Section

- rs.db.retention.cdr.default
- rs.db.retention.events.default
- rs.db.retention.latencies.daily.default
- rs.db.retention.latencies.hourly.default
- rs.db.retention.latencies.monthly.default
- rs.db.retention.latencies.weekly.default
- rs.db.retention.operations.30min.default
- rs.db.retention.operations.5min.default
- rs.db.retention.operations.daily.default
- rs.db.retention.operations.hourly.default
- rs.db.retention.operations.monthly.default
- rs.db.retention.operations.weekly.default
- rs.db.retention.sq.daily.default
- rs.db.retention.sq.failures.default
- rs.db.retention.sq.hourly.default
- rs.db.retention.sq.monthly.default
- rs.db.retention.sq.weekly.default
- rs.db.retention.var.30min.default
- rs.db.retention.var.5min.default
- rs.db.retention.var.daily.default
- rs.db.retention.var.hourly.default
- rs.db.retention.var.monthly.default
- rs.db.retention.var.weekly.default

rs.db.retention.cdr.default

Default Value: 30
Valid Values: An integer greater than 0
Changes Take Effect: immediately

The number of days for which Call Detail Records data will be retained in the database.

rs.db.retention.events.default

Default Value: 7
Valid Values: An integer greater than 0
Changes Take Effect: immediately

The number of days for which call log events (upstream logs) data will be retained in the database.

rs.db.retention.latencies.daily.default

Default Value: 90
Valid Values: An integer greater than 30
Changes Take Effect: immediately

The number of days for which daily latency histogram data will be retained in the database.

rs.db.retention.latencies.hourly.default

Default Value: 7
Valid Values: An integer greater than 0
Changes Take Effect: immediately

The number of days for which hourly latency histogram data will be retained in the database.

rs.db.retention.latencies.monthly.default

Default Value: 1095
Valid Values: An integer greater than 30
Changes Take Effect: immediately

The number of days for which monthly latency histogram data will be retained in the database.

rs.db.retention.latencies.weekly.default

Default Value: 364
Valid Values: An integer greater than 30
Changes Take Effect: immediately

The number of days for which weekly latency histogram data will be retained in the database.

rs.db.retention.operations.30min.default

Default Value: 7
Valid Values: An integer greater than 0
Changes Take Effect: immediately

The number of days for which 30-minute operational data will be retained in the database.

rs.db.retention.operations.5min.default

Default Value: 1
Valid Values: An integer greater than 0
Changes Take Effect: immediately

The number of days for which 5-minute operational data will be retained in the database.

rs.db.retention.operations.daily.default

Default Value: 90
Valid Values: An integer greater than 30
Changes Take Effect: immediately

The number of days for which daily operational data will be retained in the database.

rs.db.retention.operations.hourly.default

Default Value: 7
Valid Values: An integer greater than 0
Changes Take Effect: immediately

The number of days for which hourly operational data will be retained in the database.

rs.db.retention.operations.monthly.default

Default Value: 1095
Valid Values: An integer greater than 30
Changes Take Effect: immediately

The number of days for which monthly operational data will be retained in the database.

rs.db.retention.operations.weekly.default

Default Value: 364
Valid Values: An integer greater than 30
Changes Take Effect: immediately

The number of days for which weekly operational data will be retained in the database.

rs.db.retention.sq.daily.default

Default Value: 90
Valid Values: An integer greater than 30
Changes Take Effect: immediately

The number of days for which daily Service Quality summary data will be retained in the database.

rs.db.retention.sq.failures.default

Default Value: 365
Valid Values: An integer greater than 0
Changes Take Effect: immediately

The number of days for which Service Quality failure detail records will be retained in the database.

rs.db.retention.sq.hourly.default

Default Value: 7
Valid Values: An integer greater than 0
Changes Take Effect: immediately

The number of days for which hourly Service Quality summary data will be retained in the database.

rs.db.retention.sq.monthly.default

Default Value: 365
Valid Values: An integer greater than 30
Changes Take Effect: immediately

The number of days for which monthly Service Quality summary data will be retained in the database.

rs.db.retention.sq.weekly.default

Default Value: 180
Valid Values: An integer greater than 30
Changes Take Effect: immediately

The number of days for which weekly Service Quality summary data will be retained in the database.

rs.db.retention.var.30min.default

Default Value: 7
Valid Values: An integer greater than 0
Changes Take Effect: immediately

The number of days for which 30-minute Call Summary and IVR Action Summary data will be retained in the database.

rs.db.retention.var.5min.default

Default Value: 1
Valid Values: An integer greater than 0
Changes Take Effect: immediately

The number of days for which 5-minute Call Summary and IVR Action Summary data will be retained in the database.

rs.db.retention.var.daily.default

Default Value: 90
Valid Values: An integer greater than 30
Changes Take Effect: immediately

The number of days for which daily Call Summary and IVR Action Summary data will be retained in the database.

rs.db.retention.var.hourly.default

Default Value: 7
Valid Values: An integer greater than 0
Changes Take Effect: immediately

The number of days for which hourly Call Summary and IVR Action Summary data will be retained in the database.

rs.db.retention.var.monthly.default

Default Value: 1095
Valid Values: An integer greater than 30
Changes Take Effect: immediately

The number of days for which monthly Call Summary and IVR Action Summary data will be retained in the database.

rs.db.retention.var.weekly.default

Default Value: 364
Valid Values: An integer greater than 30

Changes Take Effect: immediately

The number of days for which weekly Call Summary and IVR Action Summary data will be retained in the database.

https Section

- https.certificate.algorithm
- https.client.authentication
- https.connector.type
- https.keystore.path
- https.keystore.type
- https.protocol
- https.random.algorithm
- https.security.provider
- password

https.certificate.algorithm

Default Value: SunX509
Valid Values: Name of HTTPS algorithm
Changes Take Effect: at start/restart

The SSL algorithm used for the configured keystore.

https.client.authentication

Default Value: none

Valid Values:
none
No certificate request, so client-side authentication is disabled.

required
A certificate is requested and the server will require a valid, non-empty certificate response to establish the connection. (Only works for BIO connector type).

preferred
A certificate is requested, but the server will still establish the connection if the certificate response is empty.

Changes Take Effect: at start/restart

HTTPS client authentication requirements.

https.connector.type

Default Value: 2

Valid Values:

NIO
: Non-blocking NIO connector (Refer to Jetty's JavaDoc for class org.mortbay.jetty.security.SslSelectChannelConnector for more information).

BIO
: Blocking BIO connector (Refer to Jetty's JavaDoc for class org.mortbay.jetty.security.SslSocketConnector for more information).

Changes Take Effect: at start/restart

The type of Jetty connector to use

https.keystore.path

Default Value: ${user.home}/.keystore
Valid Values: A directory path
Changes Take Effect: at start/restart

The path to the keystore file, which will be used for all the HTTPS connectors.

https.keystore.type

Default Value: JKS
Valid Values: A HTTPS keystore type
Changes Take Effect: at start/restart

The type of keystore, which defines the file format that the security implementation supports.

https.protocol

Default Value: TLS

Valid Values:

SSL
Supports some version of SSL.

SSLv2
Supports SSL version 2 or higher.

SSLv3
Supports SSL version 3; may support other versions.

TLS
Supports some versions of TLS.

TLSv1
Supports TLS version 1; may support other versions.

Changes Take Effect: at start/restart

The cryptographic protocol to use.

https.random.algorithm

Default Value:
Valid Values: Name of the RNG (Random Number Generator) algorithm
Changes Take Effect: at start/restart

Refer to the JDK JavaDoc for class java.security.SecureRandom for more information.

https.security.provider

Default Value:
Valid Values: Name of Java security provider
Changes Take Effect: at start/restart

Refer to the JDK JavaDoc for class java.security.Provider for more information.

password

Default Value:
Valid Values: A string
Changes Take Effect: at start/restart

The password for the keystore file.

https_key Section

- password

password

Default Value:
Valid Values: A string
Changes Take Effect: at start/restart

The optional key password for the HTTPS configuration.

imdb Section

- imdb-max-cdr-queries
- imdb-query-lock-timeout

imdb-max-cdr-queries

Default Value: 3
Valid Values: An integer from 1 - 15 inclusive
Changes Take Effect: at start/restart

The maximum number of concurrently executed RM, MCP, CCP CDR in-progress queries

imdb-query-lock-timeout

Default Value: 1000
Valid Values: An integer from 100 - 5000 inclusive
Changes Take Effect: at start/restart

The max time the real-time query would wait to acquire the lock against underlying in-memory storage in milliseconds

latency Section

threshold.asr_input_response

Default Value: 2000
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.audio_fetch

Default Value: 1000
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.call_answer

Default Value: 2000
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.call_reject

Default Value: 2000
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.cumulative_response

Default Value: 2000
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.data_fetch

Default Value: 2000
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.dtmf_input_response

Default Value: 2000

Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.grammar_fetch

Default Value: 1000
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.inbound_first_prompt

Default Value: 2000
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.initial_response

Default Value: 4000
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.interprompt

Default Value: 2000
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.java_script_execution

Default Value: 50
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.java_script_fetch

Default Value: 1000
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.mrcp_asr_session_establish

Default Value: 100
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.mrcp_asr_set_params

Default Value: 100
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.mrcp_asr_stop

Default Value: 100
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.mrcp_define_grammar

Default Value: 500
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.mrcp_recognize

Default Value: 500
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.mrcp_speak

Default Value: 100
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.mrcp_tts_session_establish

Default Value: 100

Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.mrcp_tts_set_params

Default Value: 100
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.mrcp_tts_stop

Default Value: 100
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.noinput_response

Default Value: 2000
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.outbound_first_prompt

Default Value: 2000
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.page_compile

Default Value: 100
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.page_fetch

Default Value: 1500
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.recording_response

Default Value: 2000
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

threshold.transfer_response

Default Value: 2000
Valid Values: The format is as follows: (threshold)
Changes Take Effect: at start/restart

This parameter defines the latency threshold (milliseconds) and percentile (%) for a given latency. For every Service Quality period the Reporting Server will calculate the actual latency associated with the specified percentile. If that number exceeds the threshold specified here, an error is logged.

log Section

- all
- debug
- expire
- interaction
- message_format
- segment
- standard
- time_format
- trace
- verbose

all

Default Value:

Valid Values:

stdout
Log events are sent to the Standard output (stdout).

stderr
Log events are sent to the Standard error output (stderr).

network
Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.

[filename]
Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

Changes Take Effect: immediately

Specifies the outputs to which an application sends all log events. The log output types must be separated by a comma when more than one output is configured.

debug

Default Value: logs/rs.log

Valid Values:

stdout

Log events are sent to the Standard output (stdout).

stderr

Log events are sent to the Standard error output (stderr).

network

Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.

[filename]

Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

Changes Take Effect: immediately

Specifies the outputs to which an application sends the log events of the Debug level and higher (that is, log events of the Standard, Interaction, Trace, and Debug levels). The log output types must be separated by a comma when more than one output is configured.

expire

Default Value: false

Valid Values:

false

No expiration; all generated segments are stored.

[number]

Sets the maximum number of log files to store. Specify a number from 1-100.

Changes Take Effect: immediately

Determines whether log files expire. If they do, sets the measurement for determining when they expire, along with the maximum number of files (segments) or days before the files are removed.

interaction

Default Value:

Valid Values:

stdout
: Log events are sent to the Standard output (stdout).

stderr
: Log events are sent to the Standard error output (stderr).

network
: Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.

[filename]
: Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

Changes Take Effect: immediately

Specifies the outputs to which an application sends the log events of the Interaction level and higher (that is, log events of the Standard and Interaction levels). The log outputs must be separated by a comma when more than one output is configured.

message_format

Default Value: full

Valid Values:

Compressed Headers
: An application uses compressed headers when writing log records in its log file.

A log record in the short format looks like this:
2002-05-07T18:15:33.952 Std 05060 Application started

Complete Headers

An application uses complete headers when writing log records in its log file. A log record in the full format looks like:
2002-05-07T18:11:38.196 Standard localhost cfg_dbserver GCTI-00-05060 Application started

Changes Take Effect: immediately

Specifies the format of log record headers that an application uses when writing logs in the log file. Using compressed log record headers improves application performance and reduces the log file's size.

segment

Default Value: 10MB

Valid Values:

false

This setting will cause RS to use a segment size of 10MB

[number] KB or [number]

Sets the maximum segment size, in kilobytes.

[number] MB

Sets the maximum segment size, in megabytes.

Changes Take Effect: immediately

Specifies the segmentation limit for a log file. Sets the mode of measurement, along with the maximum size. If the current log segment exceeds the size set by this option, the file is closed and a new one is created.

standard

Default Value: stdout

Valid Values:

stdout
Log events are sent to the Standard output (stdout).

stderr
Log events are sent to the Standard error output (stderr).

network
Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.

[filename]
Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

Changes Take Effect: immediately

Specifies the outputs to which an application sends the log events of the Standard level. The log output types must be separated by a comma when more than one output is configured.

time_format

Default Value: time

Valid Values:
time (HH:MM:SS.sss)
The time string is formatted according to HH:mm:ss.SSS.

locale (dd/MM/yyyy hh:mm:ss aaa)
The time string is formatted according to the system's locale. With format: dd/MM/yyyy hh:mm:ss aaa

ISO8601 (yyyy-MM-dd'T'HH:mm:ss.SSSZ)
The date in the time string is formatted according to the ISO 8601 format: yyyy-MM-dd'T'HH:mm:ss.SSSZ

Changes Take Effect: immediately

Specifies how to represent, in a log file, the time when an application generates log records.

trace

Default Value:

Valid Values:

stdout
Log events are sent to the Standard output (stdout).

stderr
Log events are sent to the Standard error output (stderr).

network
Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.

[filename]
Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

Changes Take Effect: immediately

Specifies the outputs to which an application sends the log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels). The log outputs must be separated by a comma when more than one output is configured.

verbose

Default Value: trace

Valid Values:

all
All log events (that is, log events of the Standard, Trace,Interaction, and Debug levels) are generated.

debug
The same as all.

trace
Log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels) are generated, but log events of the Debug level are not generated.

interaction
Interaction level is not mapped and will have the same effect as none.

standard
Log events of the Standard level are generated, but log events of the Interaction, Trace, and Debug levels are not generated.

none
No output is produced.

Changes Take Effect: immediately

Determines whether a log output is created. If it is, specifies the minimum level of log events generated. The log events levels, starting with the highest priority level, are Standard, Interaction, Trace, and Debug.

messaging Section

- activemq.connectionMode
- activemq.dataDirectory
- activemq.diskStoreUsageLimit
- activemq.needClientAuth
- activemq.serverIP
- activemq.tlsKeyStore
- activemq.tlsPort
- activemq.tlsServerIP
- activemq.tlsTrusStorePassword
- activemq.tlsTrustStore
- activemq.useJmx
- password
- port
- tlsKeyStorePassword

activemq.connectionMode

Default Value: 0
Valid Values: An integer equal to 0, 1 or 2
Changes Take Effect: at start/restart

The type of connectors to enable on the ActiveMQ broker. The choices are a) unencrypted only, b) SSL only, or c) SSL for new clients and unencrypted support for older clients that do not support SSL.

activemq.dataDirectory

Default Value: data/activemq
Valid Values: A directory path
Changes Take Effect: at start/restart

The full path of the directory that ActiveMQ uses for persistent queuing

activemq.diskStoreUsageLimit

Default Value: 256 gb
Valid Values: An integer followed by a measurement unit (b, kb, mb, gb).
Changes Take Effect: at start/restart

Limit of disk storage for messages handled by the ActiveMQ broker.

activemq.needClientAuth

Default Value: false
Valid Values: ActiveMQ broker need Client Authentication
Changes Take Effect: at start/restart

if the parameter value is true then which instructs the broker to check connecting client certificates and allow access only to those that are found in the truststore by the ActiveMQ broker.

activemq.serverIP

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

IP Address for the listening port used by the ActiveMQ broker (unencrypted connector).

activemq.tlsKeyStore

Default Value: keystore.ks
Valid Values: Path to the keystore file
Changes Take Effect: at start/restart

Path to the Java keystore file containing the cryptographic key and trusted certificate entries needed by the ActiveMQ broker for TLS/SSL support.

activemq.tlsPort

Default Value: 61617
Valid Values: An integer greater than 0
Changes Take Effect: at start/restart

The SSL listening port for the ActiveMQ JMS broker that receives incoming data from Reporting Clients.

activemq.tlsServerIP

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

IP Address for the TLS (encrypted) listening port used by the ActiveMQ broker.

activemq.tlsTrusStorePassword

Default Value:
Valid Values: ActiveMQ broker TrustStore password
Changes Take Effect: at start/restart

The password needed to open the TrustStore used by the ActiveMQ broker.

activemq.tlsTrustStore

Default Value: client.ks
Valid Values: Path to the TrustStore file
Changes Take Effect: at start/restart

Path to the Java TrustStore file containing the trusted certificate entries needed by the ActiveMQ broker for TLS/SSL support.

activemq.useJmx

Default Value: false
Valid Values: true or false
Changes Take Effect: at start/restart

JMX Monitoring can be enabled for monitoring ActiveMQ message queues

password

Default Value:
Valid Values: ActiveMQ broker keystore password
Changes Take Effect: at start/restart
Discontinued: 9.0.010.62 (renamed as tlskeystorepassword)

The password needed to open the keystore used by the ActiveMQ broker.

As a part of Mutual TLS feature support, password has been renamed as tlsKeyStorePassword

port

Default Value: 61616
Valid Values: An integer greater than 0
Changes Take Effect: at start/restart

The listening port for the ActiveMQ JMS broker that receives incoming data from Reporting Clients.

tlsKeyStorePassword

Default Value:
Valid Values: ActiveMQ broker keystore password
Changes Take Effect: at start/restart
Introduced: 9.0.010.62 (renamed from password)

The password needed to open the keystore used by the ActiveMQ broker.

As a part of Mutual TLS feature support, password has been renamed as tlsKeyStorePassword.

persistence Section

- hibernate.remote.database
- hibernate.remote.dialect
- hibernate.remote.driver
- hibernate.remote.url
- hibernate.remote.user
- password
- rs.histonly.enabled
- rs.nodb.enabled
- rs.storage.metricsfilter

hibernate.remote.database

Default Value:
Valid Values: A Database Name
Changes Take Effect: at start/restart

The name of remote database that will be used for RS. Used to help construct the JDBC connection URL.

hibernate.remote.dialect

Default Value:
Valid Values: MS SQL DB Dialect or Oracle DB Dialect
Changes Take Effect: at start/restart

The dialect Hibernate should use when interacting with the database

hibernate.remote.driver

Default Value:
Valid Values: MS SQL DB Datasource or Oracle DB Datasource
Changes Take Effect: at start/restart

SQL Driver Hibernate should use when interacting with the database

hibernate.remote.url

Default Value:

Valid Values: A JDBC URL
Changes Take Effect: at start/restart

The JDBC URL that RS should use to connect with the database. For Oracle, the final URL is constructed by appending a colon plus the hibernate.remote.database string to this option's value. For SQL Server, the final URL is constructed by appending ';databasename=' plus the hibernate.remote.database string to this option's value. The JDBC connection URL will equal the hibernate.remote.url string if the hibernate.remote.database parameter is set to empty.

hibernate.remote.user

Default Value:
Valid Values: User Name
Changes Take Effect: at start/restart

The user name that RS should use to connect the the remote database

password

Default Value:
Valid Values: User Password
Changes Take Effect: at start/restart

The password that RS should use to connect the the remote database

rs.histonly.enabled

Default Value: false
Valid Values: Enable HIST-Only Mode
Changes Take Effect: at start/restart

Configures the RS to run in HIST-Only Mode. The RS will never write to the remote database, but will continue to support historical report queries. The HIST-Only RS does not support writing CDR, OR, SQA, or log data. It does not support data summarization or data purging. It does not support real-time (RT) call reports.

rs.nodb.enabled

Default Value: false
Valid Values: This option controls 'no DB' mode. In 'no DB' mode, the RS functions without a remote DB, however only a limited number of reporting services are available.
Changes Take Effect: at start/restart

Enables the 'no DB' feature for running the RS without a remote DB.

rs.storage.metricsfilter

Default Value: *
Valid Values: This option controls the metrics that should be persisted to the database backend.
Changes Take Effect: at start/restart

RS uses the string provided to filter metrics before saving to the database. The string uses the same format as in Reporting Client, such as 0-16,18,25,35,36,41,52-55,74,128,136-141. The default value is "*". When the parameter is missing, the default value will be assumed and all metrics received will be saved to the database.

reporting Section

- binding.address
- db.query.timeout.max
- hostname
- password
- port
- protocol
- response.header
- response.header.landingpage
- retrieveMultipleObjectsTimeoutValue
- rs.query.limit.30min
- rs.query.limit.5min
- rs.query.limit.day
- rs.query.limit.hour
- rs.query.limit.month
- rs.query.limit.week
- rs.summarization.buffer
- usehostname-in-ruri
- username

binding.address

Default Value:
Valid Values: An IP address.
Changes Take Effect: at start/restart

The interface IP address that should be used for binding the RS service.

db.query.timeout.max

Default Value: 60
Valid Values: An integer greater than 0, less than 65535
Changes Take Effect: immediately

This parameter only controls the database query sent from RS to database server. The HTTP query on RS reporting would have longer timeout when it involves more than one database query.

hostname

Default Value:
Valid Values: A hostname or fully qualified domain name.
Changes Take Effect: at start/restart

The hostname that should be used for accessing RS.

password

Default Value:
Valid Values: A string
Changes Take Effect: at start/restart

The password for RS to perform basic HTTP authentication.

port

Default Value: 8080
Valid Values: An integer greater than 0
Changes Take Effect: at start/restart

The port on which the RS receives reporting requests.

protocol

Default Value: http
Valid Values: An integer greater than 0
Changes Take Effect: at start/restart

The type of communication protocol that RS uses to service reporting requests.

response.header

Default Value: X-Frame-Options: DENY
Valid Values: A string
Changes Take Effect: at start/restart

The custom response header to be added to all page response.

response.header.landingpage

Default Value: X-Frame-Options: DENY
Valid Values: A string
Changes Take Effect: at start/restart

The custom response header to be added to the landing page response.

retrieveMultipleObjectsTimeoutValue

Default Value: 180000
Valid Values: long value greater than or equal to 60000
Changes Take Effect: at start/restart

This parameter can be used to know the maximum amount of time, in milliseconds, that the RS will wait to retrieve all the configurations from the Configuration Server and cache the configurations locally.

rs.query.limit.30min

Default Value: 336
Valid Values: An integer greater than 0
Changes Take Effect: immediately

The maximum number of 30-minute periods that are included in any report with granularity of 30-minute.

rs.query.limit.5min

Default Value: 288
Valid Values: An integer greater than 0
Changes Take Effect: immediately

The maximum number of 5-minute periods that are included in any report with granularity of 5-minutes.

rs.query.limit.day

Default Value: 92
Valid Values: An integer greater than 0
Changes Take Effect: immediately

The maximum number of days that are included in any report with granularity of day.

rs.query.limit.hour

Default Value: 168
Valid Values: An integer greater than 0
Changes Take Effect: immediately

The maximum number of hours that are included in any report with granularity of hour.

rs.query.limit.month

Default Value: 36
Valid Values: An integer greater than 0
Changes Take Effect: immediately

The maximum number of months that are included in any report with granularity of month.

rs.query.limit.week

Default Value: 53
Valid Values: An integer greater than 0
Changes Take Effect: immediately

The maximum number of weeks that are included in any report with granularity of week.

rs.summarization.buffer

Default Value: 60
Valid Values: An integer from 0 and 44640 inclusive.
Changes Take Effect: at start/restart

The buffer time in minutes from now. The summarization job will only summarize records written before that time.

usehostname-in-ruri

Default Value: false
Valid Values:
Changes Take Effect: at start/restart

When this parameter is true GAX uses hostname in the request-uri to connect to Reporting Server.

username

Default Value:
Valid Values: A string
Changes Take Effect: at start/restart

The username for RS to perform basic HTTP authentication.

schedule Section

quartz.rs.calltimeout

Default Value: 0 50 * * * ?
Valid Values: Refer to CronExpression JavaDoc (http://www.quartz-scheduler.org) for more details about cron expression
Changes Take Effect: at start/restart

The CRON schedule that Quartz should use to execute the Call Timeout Process. This process is responsible for timing out RM/MCP/CCP and VAR Call Data Records.

quartz.rs.dbMaintenancePeriod

Default Value: 0 30 1 * * ?
Valid Values: Refer to CronExpression JavaDoc (http://www.quartz-scheduler.org) for more details about cron expression
Changes Take Effect: at start/restart

The CRON schedule that Quartz should use to purge old data according to each application's data retention policy.

quartz.rs.dbPartitioningPeriod

Default Value: 0 0 0/1 * * ?
Valid Values: Refer to CronExpression JavaDoc (http://www.quartz-scheduler.org) for more details about cron expression
Changes Take Effect: at start/restart

The CRON schedule that Quartz should use to run partition archiving job.

quartz.rs.or.counting

Default Value: 0 40 * * * ?
Valid Values: Refer to CronExpression JavaDoc (http://www.quartz-scheduler.org) for more details about cron expression
Changes Take Effect: at start/restart

The CRON schedule that Quartz should use to run the MCP VXML OR counting job process.

quartz.var.summarization

Default Value: 300000
Valid Values: An integer from 60000 and 86400000 inclusive.
Changes Take Effect: at start/restart

The schedule that Quartz should use to update VAR summary statistics. This schedule is expressed in milliseconds. For example, by default the VAR Update Process will run every 300 seconds (5 minutes).

snmp Section

- bulk.size
- polling.interval
- timeout

bulk.size

Default Value: 50
Valid Values: An integer greater than 0
Changes Take Effect:

The maximum number of entries that will be retrieved by a single SNMP GetBulk request. Note that this setting maybe be overriden by client configuration and packet size limit.

polling.interval

Default Value: 60
Valid Values: An integer greater than 0
Changes Take Effect:

The interval between each SNMP request to a specific component.

timeout

Default Value: 30000
Valid Values: An integer greater or equal to 1000
Changes Take Effect: immediately

The maximum amount of time the SNMP query will wait to receive the response from the SNMP Agent.

sqa Section

- error.notification.threshold
- monitor.min.alert.number
- monitor.min.latency.warn.number
- service.quality.period
- stat.update.interval

error.notification.threshold

Default Value: 95
Valid Values: An integer between 1 and 100 inclusive
Changes Take Effect: immediately

If the percentage of successful calls falls below this threshold during a service quality period, a notification is generated.

monitor.min.alert.number

Default Value: 100
Valid Values: An integer greater than 0
Changes Take Effect: immediately

The minimum number of calls that need to be recorded before the service quality notification is issued at the critical level.

monitor.min.latency.warn.number

Default Value: 100
Valid Values: An integer greater than 0
Changes Take Effect: immediately

The minimum number of latency measurements that need to be recorded before a warning is logged indicating that the latency measurements have exceeded the configured threshold for the update period.

service.quality.period

Default Value: 900
Valid Values: An integer equal to 300, 600, 900, 1200, 1800, or 3600.
Changes Take Effect: At start/restart

This parameter indicates the interval (in seconds) at which service quality data will be forwarded to the RS from the MCP relative to the beginning of the hour. MCP components must be restarted to refresh their version of this parameter if it is updated.

stat.update.interval

Default Value: 900
Valid Values: An integer equal to 300, 600, 900, 1200, 1800, or 3600.
Changes Take Effect: At start/restart

This parameter defines the period of time, in seconds, between statistic updates, and is relative to the beginning of the hour, rather than the MCP client start time. MCP components must be restarted to refresh their version of this parameter if it is updated.

Speech-Related Components

These components provide the interface to third-party speech servers that deliver speech recognition and text-to-speech services for VoiceXML. GVP uses the Media Resource Control Protocol to communicate with these services. The MCP includes client interfaces for MRCPv1 and MRCPv2. These clients are capable of load-balancing across pools of speech servers, and service monitoring of speech servers for availability purposes. GVP also includes an MRCPv1 proxy that provides global load balancing, peak reporting, and other services.

- MRCP Proxy

    MRCP Proxy is an integral component that interfaces with the MRCP, Management Framework, and Operational Reporting API. The MRCP Proxy can be placed between the Media Control Platforms and the MRCPv1 resources within a GVP deployment. Deploying the MRCP Proxy enables ASR/TTS usage reporting data to be sent to the Reporting Server.

    For more information about the MRCP Proxy application, see MRCP Proxy in the *GVP Deployment Guide*. For various MRCP Proxy configuration options, see MRCP Proxy Options in this document.

- MRCPv1/v2 Services

GVP provides transparent access to MRCP services from VoiceXML. GVP will acquire and releases ASR and TTS sessions as required for proper execution of a VoiceXML applications. Text to Speech services render audio streams from text, allowing playback of dynamic text for which pre-recorded prompts may be difficult or impossible to provide. Text rendering can be controlled using the Speech Synthesis Markup Language (SSML), and can support multiple languages.

Speech Recognition services can process caller audio and, and using either pre-defined context free grammars or natural language models, return an interpretation of what the caller said. Speech recognition services support the Speech Recognition Grammar Specification (SRGS) for grammar specification, and the Natural Language Semantic Markup Language (NLSML) specification for describing the results of a recognition.

MRCP Proxy

Options for this component are contained in the following configuration sections:

- ems
- log
- snmp
- stack
- vrmproxy

Tip

In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.

Power users: Download a CSV file containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
ems	logconfig.MFSINK	*	immediately
ems	metricsconfig.MFSINK	*	immediately
ems	ors.reportinginterval	60	At start/restart
ems	rc.amq_connection_send_timeout	60	At start/restart
ems	rc.cdr.batch_size	500	At start/restart
ems	rc.cdr.local_queue_max	-1	At start/restart
ems	rc.cdr.local_queue_path	cdrQueue_rm.db	At start/restart
ems	rc.certificate		at start/restart
ems	rc.keystore_certificate		at start/restart
ems	rc.keystore_password		at start/restart
ems	rc.ors.batch_size	500	At start/restart
ems	rc.ors.local_queue_max	-1	At start/restart
ems	rc.ors.local_queue_path	orsQueue_rm.db	At start/restart
ems	rc.truststore_certificate		at start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
log	all	../logs/MRCPProxy	immediately
log	check-point	1	immediately
log	compatible-output-priority	false	immediately
log	debug	../logs/MRCPProxy	immediately
log	expire	20	immediately
log	interaction	../logs/MRCPProxy	immediately
log	keep-startup-file	false	After restart
log	memory		immediately
log	memory-storage-size		When memory output is created
log	messagefile		Immediately, if an application cannot find its *.lms file at startup
log	message_format	short	immediately
log	print-attributes	false	immediately
log	segment	10000	immediately
log	spool		immediately
log	standard	../logs/MRCPProxy	immediately
log	time_convert	local	immediately
log	time_format	ISO8601	immediately
log	trace	../logs/MRCPProxy	immediately
log	verbose	standard	immediately
snmp	timeout	100	At start/restart
stack	connection.portrange	10000-11999	At start/restart
stack	connection.timeout	10000	At start/restart
stack	trace.debug	true	At start/restart
vrmproxy	disconnect_ping_timeout	true	Immediately
vrmproxy	fips_enabled	false	After restart
vrmproxy	ping_alarm_threshold	3	Immediately
vrmproxy	resource_alarm_threshold	30	Immediately
vrmproxy	timeout.back_in_service	10000	Immediately
vrmproxy	timeout.barge_in_occurred	10000	Immediately
vrmproxy	timeout.check_avail_res	30000	Immediately
vrmproxy	timeout.clean_loop	60000	Immediately
vrmproxy	timeout.close_session	10000	Immediately
vrmproxy	timeout.control	10000	Immediately
vrmproxy	timeout.define_grammar	10000	Immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
vrmproxy	timeout.get_params	10000	Immediately
vrmproxy	timeout.get_result	10000	Immediately
vrmproxy	timeout.get_server_info	10000	Immediately
vrmproxy	timeout.max_idle	180000	Immediately
vrmproxy	timeout.open_session	10000	Immediately
vrmproxy	timeout.pause	10000	Immediately
vrmproxy	timeout.recognize	10000	Immediately
vrmproxy	timeout.recog_start_timers	10000	Immediately
vrmproxy	timeout.reconnect_interval	10000	Immediately
vrmproxy	timeout.resume	10000	Immediately
vrmproxy	timeout.set_params	10000	Immediately
vrmproxy	timeout.speak	10000	Immediately
vrmproxy	timeout.stop	10000	Immediately
vrmproxy	uri	rtsp://localhost:16000/mrcpproxy	After restart
Section	Option	Default	Changes Take Effect

ems Section

- logconfig.MFSINK
- metricsconfig.MFSINK
- ors.reportinginterval
- rc.amq_connection_send_timeout
- rc.cdr.batch_size
- rc.cdr.local_queue_max
- rc.cdr.local_queue_path
- rc.certificate
- rc.keystore_certificate
- rc.keystore_password
- rc.ors.batch_size
- rc.ors.local_queue_max
- rc.ors.local_queue_path
- rc.truststore_certificate

logconfig.MFSINK

Default Value: *
Valid Values: Pipe delimited ranges for log levels, module IDs and specifier IDs. Ranges can be comma separated integers or range of integers or '*'.
Changes Take Effect: immediately

Controls the log messages that are sent to the MF sink. The format is 'levels

metricsconfig.MFSINK

Default Value: *
Valid Values: Comma separated list of metric values or ranges. A metric value must be between 0 and 141 inclusive. The values '*' and blank are also allowed.
Changes Take Effect: immediately

Specifies the metrics that are delivered to the MF Sink. '*' indicates that all metrics will be sent to the sink. Alternatively, '5-10,50-55,70,71' indicates that metrics with IDs 5,6,7,8,9,10,50,51,52,53,54,55,70 and 71 will be sent to the MF sink.

ors.reportinginterval

Default Value: 60
Valid Values: An integer between 1-299 inclusive.
Changes Take Effect: At start/restart

Interval (seconds) accumulated operational reports are submitted to the Reporting Server

rc.amq_connection_send_timeout

Default Value: 60
Valid Values: An integer greater than or equal to 45.
Changes Take Effect: At start/restart

This option specifies the maximum time in seconds to wait for ActiveMQ Producer Send Message response.

rc.cdr.batch_size

Default Value: 500
Valid Values: An integer between 1-5000 inclusive.
Changes Take Effect: At start/restart

The number of CDR messages queued up by the reporting client before sending them up to the reporting server. A higher batch size (e.g. 50 records) will lessen bandwidth constraints, at the cost of making sending CDR data at larger intervals.

rc.cdr.local_queue_max

Default Value: -1
Valid Values: An integer greater or equal to -1.
Changes Take Effect: At start/restart

This option specifies the maximum number of data items to the local database for CDR reporting. Queuing to the local database will occur either when the Reporting Server is unavailable, or when data is being provided to the Client faster than the Server can consume it. This value defaults to -1 indicating an "unlimited" number of records will be allowed. A value of 0 indicates that no records will be persisted locally and data will be discarded if the RS is unavailable.

rc.cdr.local_queue_path

Default Value: cdrQueue_rm.db
Valid Values: Path to the DB file.
Changes Take Effect: At start/restart

The full path of the local database file used to locally persist data for CDRs.

rc.certificate

Default Value:
Valid Values: File path
Changes Take Effect: at start/restart

The file name of the TLS certificate in "PEM" format. Required to connect to the Reporting Server (ActiveMQ) over TLS.

rc.keystore_certificate

Default Value:
Valid Values: File path
Changes Take Effect: at start/restart

The file name of the TLS KeyStore certificate in "PEM" format. Required to connect to the Reporting Server (ActiveMQ) over TLS.

rc.keystore_password

Default Value:
Valid Values: KeyStore Password
Changes Take Effect: at start/restart

The password for Reporting Client keyStore. Required to connect to the Reporting Server (ActiveMQ) over TLS.

rc.ors.batch_size

Default Value: 500
Valid Values: An integer between 1-5000 inclusive.
Changes Take Effect: At start/restart

The number of OR messages queued up by the reporting client before sending them up to the reporting server.

rc.ors.local_queue_max

Default Value: -1
Valid Values: An integer greater or equal to -1.
Changes Take Effect: At start/restart

This option specifies the maximum number of data items to the local database for Operational Reporting. Queuing to the local database will occur either when the Reporting Server is unavailable, or when data is being provided to the Client fdaster than the Server can consume it. This value defaults to -1 indicating an "unlimited" number of records will be allowed. A value of 0 indicates that no records will be persisted locally and data will be discarded if the RS is unavailable.

rc.ors.local_queue_path

Default Value: orsQueue_rm.db
Valid Values: Path to the DB file.
Changes Take Effect: At start/restart

The full path of the local database file used to locally persist data for Operational Reporting.

rc.truststore_certificate

Default Value:
Valid Values: File path
Changes Take Effect: at start/restart

The file name of the TLS TrustStore certificate in "PEM" format. Required to connect to the Reporting Server (ActiveMQ) over TLS.

log Section

- all
- check-point
- compatible-output-priority
- debug
- expire
- interaction
- keep-startup-file
- memory
- memory-storage-size
- message_format
- messagefile
- print-attributes
- segment
- spool
- standard
- time_convert
- time_format
- trace
- verbose

all

Default Value: ../logs/MRCPProxy

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends all log events. The log output types must be separated by a comma when more than one output is configured.

check-point

Default Value: 1
Valid Values: 0 - 24
Changes Take Effect: immediately

Specifies, in hours, how often the application generates a check point log event, to divide the log into sections of equal time. By

default, the application generates this log event every hour. Setting the option to 0 prevents the generation of check-point events.

compatible-output-priority

Default Value: false
Valid Values: true, false
Changes Take Effect: immediately

Specifies whether the application uses 6.x output logic.

- **true** The log of the level specified by "Log Output Options" is sent to the specified output.
- **false** The log of the level specified by "Log Output Options" and higher levels is sent to the specified output.

debug

Default Value: ../logs/MRCPProxy

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
Changes Take Effect: immediately
Specifies the outputs to which an application sends the log events of the Debug level and higher (that is, log events of the Standard, Interaction, Trace, and Debug levels). The log output types must be separated by a comma when more than one output is configured.

expire

Default Value: 20

Valid Values:

- **false** No expiration; all generated segments are stored.
- **[number] file or [number]** Sets the maximum number of log files to store. Specify a number from 1-1000.
- **[number] day** Sets the maximum number of days before log files are deleted. Specify a number from 1-100.
Changes Take Effect: immediately
Determines whether log files expire. If they do, sets the measurement for determining when they expire, along with the maximum number of files (segments) or days before the files are removed. This option is ignored if log output is not configured to be sent to a log file. Note: If the value of the option is set incorrectly - out of the range of valid values- it will be automatically reset to 10

interaction

Default Value: ../logs/MRCPProxy

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
Changes Take Effect: immediately
Specifies the outputs to which an application sends the log events of the Interaction level and higher (that is, log events of the Standard and Interaction levels). The log outputs must be separated by a comma when more than one output is configured.

keep-startup-file

Default Value: false

Valid Values:

- **false** No startup segment of the log is kept.
- **true** A startup segment of the log is kept. The size of the segment equals the value of the segment option.
- **[number] KB** Sets the maximum size, in kilobytes, for a startup segment of the log.
- **[number] MB** Sets the maximum size, in megabytes, for a startup segment of the log.
Changes Take Effect: After restart
Specifies whether a startup segment of the log, containing the initial T-Server configuration, is to be kept. If it is, this option can be set to true or to a specific size. If set to true, the size of the initial segment will be equal to the size of the regular log segment defined by the segment option. The value of this option will be ignored if segmentation is turned off (that is, if the segment option set to false).

memory

Default Value:
Valid Values: [string] (memory file name)
Changes Take Effect: immediately

Specifies the name of the file to which the application regularly prints a snapshot of the memory output, if it is configured to do this. The new snapshot overwrites the previously written data. If the application terminates abnormally, this file will contain the latest log messages. Memory output is not recommended for processors with a CPU frequency lower than 600 MHz.

memory-storage-size

Default Value:

Valid Values:

- **[number] KB or [number]** The size of the memory output, in kilobytes. The minimum value is 128 KB.
- **[number] MB** The size of the memory output, in megabytes. The maximum value is 64 MB
  Changes Take Effect: When memory output is created
  Specifies the buffer size for log output to the memory, if configured.

message_format

Default Value: short

Valid Values:

- **short** An application uses compressed headers when writing log records in its log file.
- **full** An application uses complete headers when writing log records in its log file.
  Changes Take Effect: immediately
  Specifies the format of log record headers that an application uses when writing logs in the log file. Using compressed log record headers improves application performance and reduces the log file's size. With the value set to short:
- A header of the log file or the log file segment contains information about the application (such as the application name, application type, host type, and time zone), whereas single log records within the file or segment omit this information.
- A log message priority is abbreviated to Std, Int, Trc, or Dbg, for Standard, Interaction, Trace, or Debug messages, respectively.
- The message ID does not contain the prefix GCTI or the application type ID.
  A log record in the full format looks like this:
  2002-05-07T18:11:38.196 Standard localhost cfg_dbserver GCTI-00-05060 Application started
  A log record in the short format looks like this:
  2002-05-07T18:15:33.952 Std 05060 Application started

messagefile

Default Value:
Valid Values: [string].lms (message file name)
Changes Take Effect: Immediately, if an application cannot find its *.lms file at startup

Specifies the file name for application-specific log events. The name must be valid for the operating system on which the application is running. The option value can also contain the absolute path to the application-specific *.lms file. Otherwise, an application looks for the file in its working directory.

print-attributes

Default Value: false
Valid Values: true, false
Changes Take Effect: immediately

Specifies whether the application attaches extended attributes, if any exist, to a log event that it sends to log output. Typically, log events of the Interaction log level and Audit-related log events contain extended attributes. Setting this option to true enables audit capabilities, but negatively affects performance. Genesys recommends enabling this option for Solution Control Server and Configuration Server when using audit tracking. For other applications, refer to Genesys 7.5 Combined Log Events Help to find out whether an application generates Interaction-level and Audit-related log events; if it does, enable the option only when testing new interaction scenarios.

- **true** Attaches extended attributes, if any exist, to a log event sent to log output.
- **false** Does not attach extended attributes to a log event sent to log output.

segment

Default Value: 10000

Valid Values:

- **false** No segmentation is allowed.
- **[number] KB or [number]** Sets the maximum segment size, in kilobytes. The minimum segment size is 100 KB.
- **[number] MB** Sets the maximum segment size, in megabytes.
- **[number] hr** Sets the number of hours for the segment to stay open. The minimum number is 1 hour.
  Changes Take Effect: immediately
  Specifies whether there is a segmentation limit for a log file. If there is, sets the mode of measurement, along with the maximum size. If the current log segment exceeds the size set by this option, the file is closed and a new one is created.

spool

Default Value:
Valid Values: [path] (the folder, with the full path to it)
Changes Take Effect: immediately

Specifies the folder, including full path to it, in which an application creates temporary files related to network log output. If you change the option value while the application is running, the change does not affect the currently open network output.

standard

Default Value: ../logs/MRCPProxy

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends the log events of the Standard level. The log output types must be separated by a comma when more than one output is configured.

time_convert

Default Value: local
Valid Values: local, utc
Changes Take Effect: immediately

Specifies the system in which an application calculates the log record time when generating a log file. The time is converted from the time in seconds since the Epoch (00:00:00 UTC, January 1, 1970).

- **Local Time (local)** The time of log record generation is expressed as a local time, based on the time zone and any seasonal adjustments. Time zone information of the application's host computer is used.
- **Coordinated Universal Time (utc)** The time of log record generation is expressed as Coordinated Universal Time (UTC).

time_format

Default Value: ISO8601
Valid Values: time, locale, ISO8601
Changes Take Effect: immediately

Specifies how to represent, in a log file, the time when an application generates log records.
A log record's time field in the ISO 8601 format looks like this:
2001-07-24T04:58:10.123

- **HH:MM:SS.sss (time)** The time string is formatted according to the HH:MM:SS.sss (hours, minutes, seconds, and milliseconds) format.
- **According to the system's locale (locale)** The time string is formatted according to the system's locale.
- **ISO 8601 format (ISO8601)** The date in the time string is formatted according to the ISO 8601 format. Fractional seconds are given in milliseconds.

trace

Default Value: ../logs/MRCPProxy

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends the log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels). The log outputs must be separated by a comma when more than one output is configured.

verbose

Default Value: standard
Valid Values: all, debug, trace, interaction, standard, none
Changes Take Effect: immediately

Determines whether a log output is created. If it is, specifies the minimum level of log events generated. The log events levels, starting with the highest priority level, are standard, interaction, trace, debug and all.

- **all** All log events (that is, log events of the Standard, Trace,Interaction, and Debug levels) are generated.
- **debug** The same as all.
- **trace** Log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels) are generated, but log events of the Debug level are not generated.
- **interaction** Log events of the Interaction level and higher (that is, log events of the Standard and Interaction levels) are generated, but log events of the Trace and Debug levels are not generated.
- **standard** Log events of the Standard level are generated, but log events of the Interaction, Trace, and Debug levels are not generated.
- **none** No log evenets are generated.

snmp Section

- timeout

timeout

Default Value: 100
Valid Values: The parameter must be an integer value greater than zero.
Changes Take Effect: At start/restart

The maximum amount of time that SNMP can wait for a new task. This value is specified in milliseconds.

stack Section

- connection.portrange
- connection.timeout
- trace.debug

connection.portrange

Default Value: 10000-11999
Valid Values:
Changes Take Effect: At start/restart

The port range of RTSP stack used by MRCPv1 client.

connection.timeout

Default Value: 10000
Valid Values:
Changes Take Effect: At start/restart

The connection timeout for SRM MRCPv1 and MRCPv2 Stack to establish a TCP connection to the server. The value must be integer values in milliseconds.

trace.debug

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

Whether to enable the stack debug message

vrmproxy Section

- disconnect_ping_timeout
- fips_enabled
- ping_alarm_threshold
- resource_alarm_threshold
- timeout.back_in_service
- timeout.barge_in_occurred
- timeout.check_avail_res
- timeout.clean_loop
- timeout.close_session
- timeout.control
- timeout.define_grammar
- timeout.get_params
- timeout.get_result
- timeout.get_server_info
- timeout.max_idle
- timeout.open_session
- timeout.pause
- timeout.recog_start_timers
- timeout.recognize
- timeout.reconnect_interval
- timeout.resume
- timeout.set_params
- timeout.speak
- timeout.stop
- uri

disconnect_ping_timeout

Default Value: true
Valid Values: true, false
Changes Take Effect: Immediately

Specifies whether or not to disconnect the resource when ping timeout occurs. MRCP Proxy will reconnect the resource immediately. This procedure provides a method to repair the stale connection.

fips_enabled

Default Value: false
Valid Values: true, false
Changes Take Effect: After restart

Specifies whether to enable FIPS mode in MRCP Proxy. When FIPS mode is enabled, only FIPS 140-2 approved ciphers and algorithms can be used in SSL connections.

ping_alarm_threshold

Default Value: 3

Valid Values:
Changes Take Effect: Immediately

Specifies the alarm threshold of continuous ping failures. When the number of continuous ping failures for a resource is equal to or greater than the threshold, an alarm will be raised. Default is 3 times.

resource_alarm_threshold

Default Value: 30
Valid Values:
Changes Take Effect: Immediately

Specifies the unavailable resource alarm threshold in percentage. Default is 30 percent.

timeout.back_in_service

Default Value: 10000
Valid Values:
Changes Take Effect: Immediately

Timeout in milliseconds for a server to be put back in service after it encounters errors such as timeout or TCP connection error.

timeout.barge_in_occurred

Default Value: 10000
Valid Values:
Changes Take Effect: Immediately

Timeout of BARGE-IN-OCCURRED in milliseconds.

timeout.check_avail_res

Default Value: 30000
Valid Values:
Changes Take Effect: Immediately

Timeout in milliseconds to check available resources. If the unavailable resource alarm threshold is reached, an alarm will be raised.

timeout.clean_loop

Default Value: 60000
Valid Values:
Changes Take Effect: Immediately

Interval to clean idle sessions as determined by timeout.max_idle parameter.

timeout.close_session

Default Value: 10000
Valid Values:
Changes Take Effect: Immediately

Timeout of Close-Session request in milliseconds.

timeout.control

Default Value: 10000
Valid Values:
Changes Take Effect: Immediately

Timeout of CONTROL message in milliseconds.

timeout.define_grammar

Default Value: 10000
Valid Values:
Changes Take Effect: Immediately

Timeout of DEFINE-GRAMMAR message in milliseconds.

timeout.get_params

Default Value: 10000
Valid Values:
Changes Take Effect: Immediately

Timeout of GET-PARAMS message in milliseconds.

timeout.get_result

Default Value: 10000
Valid Values:
Changes Take Effect: Immediately

Timeout of GET-RESULT message in milliseconds.

timeout.get_server_info

Default Value: 10000
Valid Values:
Changes Take Effect: Immediately

Timeout of to get a response for Get-Server-Info request (Ping) in milliseconds.

timeout.max_idle

Default Value: 180000
Valid Values:
Changes Take Effect: Immediately

Max session idle time in milliseconds. Sessions exceeding this idle time will be terminated.

timeout.open_session

Default Value: 10000
Valid Values:
Changes Take Effect: Immediately

Timeout of Open-Session in milliseconds.

timeout.pause

Default Value: 10000
Valid Values:
Changes Take Effect: Immediately

Timeout of PAUSE message in milliseconds.

timeout.recog_start_timers

Default Value: 10000
Valid Values:
Changes Take Effect: Immediately

Timeout of RECOGNITION-START-TIMERS message in milliseconds.

timeout.recognize

Default Value: 10000
Valid Values:
Changes Take Effect: Immediately

Timeout of RECOGNIZE message in milliseconds.

timeout.reconnect_interval

Default Value: 10000
Valid Values:
Changes Take Effect: Immediately

If TCP connection is not yet established with the MRCP server, interval in milliseconds to try reconnecting.

timeout.resume

Default Value: 10000
Valid Values:
Changes Take Effect: Immediately

Timeout of RESUME message in milliseconds.

timeout.set_params

Default Value: 10000
Valid Values:
Changes Take Effect: Immediately

Timeout of SET-PARAMS message in milliseconds.

timeout.speak

Default Value: 10000
Valid Values:
Changes Take Effect: Immediately

Timeout of SPEAK message in milliseconds.

timeout.stop

Default Value: 10000
Valid Values:
Changes Take Effect: Immediately

Timeout of STOP message in milliseconds.

uri

Default Value: rtsp://localhost:16000/mrcpproxy
Valid Values:
Changes Take Effect: After restart

This parameter specifies the full RTSP URI the MRCPv1 clients should use for contacting this proxy. The MRCP Proxy will listen for TCP connections at the port specified by the URI. If port is not specified in the URI, default port 16000 will be assumed. For deployments where MRCP Proxy is in a separate box from the MCP, the default value must be changed with the the IP of the MRCP Proxy.

MRCPv1_ASR

Options for this component are contained in the following configuration sections:

- provision

Tip

In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.

Power users: **Download a CSV file** containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
provision	vrm.client.ConnectPerSetup	false	At start/restart
provision	vrm.client.DisableHotWord	true	
provision	vrm.client.DisablePing	false	At start/restart
provision	vrm.client.EventLoggingEngine	nrec	At start/restart
provision	vrm.client.HotKeyBasePath	/mcp/$AppName$/grammar/common/hotkey	At start/restart
provision	vrm.client.IBMHotWord	false	At start/restart
provision	vrm.client.NoDuplicatedGramURI	true	At start/restart
provision	vrm.client.resource.name		At start/restart
provision	vrm.client.resource.type	ASR	At start/restart
provision	vrm.client.resource.uri		At start/restart
provision	vrm.client.SendLoggingTag	true	At start/restart
provision	vrm.client.SendSilence	false	At start/restart
provision	vrm.client.SendSWMSParams	true	At start/restart
provision	vrm.client.TelispeechRecognitionBargein	false	At start/restart
provision	vrm.client.TransportProtocol	MRCPv1	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
provision	vrm.proxy.ping_interval	30000	Immediately
Section	**Option**	**Default**	**Changes Take Effect**

provision Section

- vrm.client.ConnectPerSetup
- vrm.client.DisableHotWord
- vrm.client.DisablePing
- vrm.client.EventLoggingEngine
- vrm.client.HotKeyBasePath
- vrm.client.IBMHotWord
- vrm.client.NoDuplicatedGramURI
- vrm.client.resource.name
- vrm.client.resource.type
- vrm.client.resource.uri
- vrm.client.SendLoggingTag
- vrm.client.SendSilence
- vrm.client.SendSWMSParams
- vrm.client.TelispeechRecognitionBargein
- vrm.client.TransportProtocol
- vrm.proxy.ping_interval

vrm.client.ConnectPerSetup

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

When this option is set to true the SRM Client will create a new connection to the ASR or TTS server per MRCP session setup.

vrm.client.DisableHotWord

Default Value: true
Valid Values:
Changes Take Effect:

Setting this parameter, the platform will treat recognition based barge-in as speech based barge-in. This parameter should be set to true to all the ASR server that does not support recognition based barge-in

vrm.client.DisablePing

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

When this option is set to true the MRCPv1 Client will not ping the MRCPv1 server.

vrm.client.EventLoggingEngine

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

The name of the ASR engine and reporting tool for telephony event logging and reporting.

vrm.client.HotKeyBasePath

Default Value: /mcp/$AppName$/grammar/common/hotkey
Valid Values:
Changes Take Effect: At start/restart

The HTTP fetchable location for the hotkey grammars. The value of this parameter is concatenated with the IP address of the Media Control Platform to form a fetchable location for hotkey grammars.

vrm.client.IBMHotWord

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

This enables hotword recognition for the IBM Speech Server when bargein type is specified as hotword. Otherwise, normal speech recognition is performed.

vrm.client.NoDuplicatedGramURI

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

To workaround the problem for some engines that cannot accept duplicated URI in the same recognition session.

vrm.client.resource.name

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

This parameter specifies the name of resource name. Some common names are NUANCE, REALSPEAK

vrm.client.resource.type

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

This parameter specifies the speech resource type.

vrm.client.resource.uri

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

This parameter specifies the URI to the speech resource, e.g. rtsp://<MRCP server IP>:<port>/media/speechrecognizer. Please consult your MRCP vendor documentation for appropriate setting.

vrm.client.SendLoggingTag

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

When this option is set to true the SRM Client will set the logging-tag parameter in the first SET-PARAMS method to the unique Call ID of the call.

vrm.client.SendSilence

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

If set to true, the MCP will send silence audio to the MRCP server during a recognition session pause period. Otherwise, the MCP will not send any audio during a recognition session pause period.

vrm.client.SendSWMSParams

Default Value: true
Valid Values:

Changes Take Effect: At start/restart

When this is set, the SRM client will send the SWMS parameters using the SWMS 3.0 convention.

vrm.client.TelispeechRecognitionBargein

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

Set to true to support Telisma bargein recognition capability.

vrm.client.TransportProtocol

Default Value: MRCPv1
Valid Values:
Changes Take Effect: At start/restart

This parameter specifies the MRCP protocol used by the Speech Resource.

vrm.proxy.ping_interval

Default Value: 30000
Valid Values:
Changes Take Effect: Immediately

This parameter specifies the ping interval in milliseconds for the MRCP Proxy to ping the speech resource. This parameter is only used by the MRCP proxy.

MRCPv1_TTS

Options for this component are contained in the following configuration sections:

- provision

Tip

In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.

Power users: Download a CSV file containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
provision	vrm.client.ConnectPerSetup	false	At start/restart
provision	vrm.client.DisablePing	false	At start/restart
provision	vrm.client.NoSpeechLanguageHeader	false	At start/restart
provision	vrm.client.resource.name		At start/restart
provision	vrm.client.resource.type	TTS	At start/restart
provision	vrm.client.resource.uri		At start/restart
provision	vrm.client.SendLoggingTag	true	At start/restart
provision	vrm.client.SpeechMarkerEncoding	UTF-8	At start/restart
provision	vrm.client.TransportProtocol	MRCPv1	At start/restart
provision	vrm.client.TTSInsertVoiceTag	false	At start/restart
provision	vrm.proxy.ping_interval	30000	Immediately
Section	**Option**	**Default**	**Changes Take Effect**

provision Section

vrm.client.ConnectPerSetup

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

When this option is set to true the SRM Client will create a new connection to the ASR or TTS server per MRCP session setup.

vrm.client.DisablePing

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

When this option is set to true the MRCPv1 Client will not ping the MRCPv1 server.

vrm.client.NoSpeechLanguageHeader

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

When this parameter is set to true, the SRM Client will not send the Speech-Language header in MRCP SET-PARAMS and SPEAK requests in a TTS session. Without the Speech-Language header, some MRCP TTS servers is able to use its default language when the application specified language is absent.

vrm.client.resource.name

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

This parameter specifies the name of resource name. Some common names are SPEECHWORKS, REALSPEAK

vrm.client.resource.type

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

This parameter specifies the speech resource type.

vrm.client.resource.uri

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

This parameter specifies the URI to the speech resource, e.g. rtsp://<MRCP server IP>:<port>/media/speechsynthesizer. Please consult your MRCP vendor documentation for appropriate setting.

vrm.client.SendLoggingTag

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

When this option is set to true the SRM Client will set the logging-tag parameter in the first SET-PARAMS method to the unique Call ID of the call.

vrm.client.SpeechMarkerEncoding

Default Value: UTF-8
Valid Values:
Changes Take Effect: At start/restart

If a TTS MRCP server does not have the content-encoding header to specify the Speech Marker name encoding in a SPEECH-MARKER event, the SRM client will use the value specified by this parameter as the encoding of the Speech Marker name.

vrm.client.TransportProtocol

Default Value: MRCPv1
Valid Values:
Changes Take Effect: At start/restart

This parameter specifies the MRCP protocol used by the Speech Resource.

vrm.client.TTSInsertVoiceTag

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

When this option is set to true, the SRM Client will use the voice name defined in the TTSENGINE property to tell the TTS engine what voice to use.

vrm.proxy.ping_interval

Default Value: 30000
Valid Values:
Changes Take Effect: Immediately

This parameter specifies the ping interval in milliseconds for the MRCP Proxy to ping the speech resource. This parameter is only used by the MRCP proxy.

MRCPv2_ASR

Options for this component are contained in the following configuration sections:

- provision

> ## Tip
>
> In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.
>
> **Power users: Download a CSV file** containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
provision	vrm.client.ConfidenceScale	100	At start/restart
provision	vrm.client.ConnectPerSetup	true	At start/restart
provision	vrm.client.DisableHotWord	false	
provision	vrm.client.EventLoggingEngine	mrec	At start/restart
provision	vrm.client.HotKeyBasePath	/mcp/$AppName$/grammar/common/hotkey	At start/restart
provision	vrm.client.IBMHotWord	false	At start/restart
provision	vrm.client.NoDuplicatedGramURI	true	At start/restart
provision	vrm.client.resource.name		At start/restart
provision	vrm.client.resource.type	ASR	At start/restart
provision	vrm.client.resource.uri		At start/restart
provision	vrm.client.SendLoggingTag	true	At start/restart
provision	vrm.client.SendSessionXML	false	At start/restart
provision	vrm.client.SendSilence	false	At start/restart
provision	vrm.client.SendSWMSParams	true	At start/restart
provision	vrm.client.SrtpLifetime	48	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
provision	vrm.client.TelispeechRecognitionBargein	false	At start/restart
provision	vrm.client.TlsCertificateKey	$InstallationRoot$/config/x509_certificate.pem	At start/restart
provision	vrm.client.TlsPassword		At start/restart
provision	vrm.client.TlsPrivateKey	$InstallationRoot$/config/x509_private_key.pem	At start/restart
provision	vrm.client.TlsProtocolType	TLSv1	At start/restart
provision	vrm.client.TransportProtocol	MRCPv2	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

provision Section

- vrm.client.ConfidenceScale
- vrm.client.ConnectPerSetup
- vrm.client.DisableHotWord
- vrm.client.EventLoggingEngine
- vrm.client.HotKeyBasePath
- vrm.client.IBMHotWord
- vrm.client.NoDuplicatedGramURI
- vrm.client.resource.name
- vrm.client.resource.type
- vrm.client.resource.uri
- vrm.client.SendLoggingTag
- vrm.client.SendSessionXML
- vrm.client.SendSilence
- vrm.client.SendSWMSParams
- vrm.client.SrtpLifetime
- vrm.client.TelispeechRecognitionBargein
- vrm.client.TlsCertificateKey
- vrm.client.TlsPassword
- vrm.client.TlsPrivateKey
- vrm.client.TlsProtocolType
- vrm.client.TransportProtocol

vrm.client.ConfidenceScale

Default Value: 100
Valid Values:
Changes Take Effect: At start/restart

This defines the range of the confidence value of the recognition results.

vrm.client.ConnectPerSetup

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

When this option is set to true the SRM Client will create a new connection to the ASR or TTS server per MRCP session setup.

vrm.client.DisableHotWord

Default Value: false
Valid Values:
Changes Take Effect:

Setting this parameter, the platform will treat recognition based barge-in as speech based barge-in. This parameter should be set to true to all the ASR server that does not support recognition based barge-in

vrm.client.EventLoggingEngine

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

The name of the ASR engine and reporting tool for telephony event logging and reporting.

vrm.client.HotKeyBasePath

Default Value: /mcp/$AppName$/grammar/common/hotkey
Valid Values:
Changes Take Effect: At start/restart

The HTTP fetchable location for the hotkey grammars. The value of this parameter is concatenated with the IP address of the Media Control Platform to form a fetchable location for hotkey grammars.

vrm.client.IBMHotWord

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

This enables hotword recognition for the IBM Speech Server when bargein type is specified as hotword. Otherwise, normal speech recognition is performed.

vrm.client.NoDuplicatedGramURI

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

To workaround the problem for some engines that cannot accept duplicated URI in the same recognition session.

vrm.client.resource.name

Default Value:

Valid Values:
Changes Take Effect: At start/restart

This parameter specifies the name of resource name. Some common names are NUANCE, REALSPEAK

vrm.client.resource.type

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

This parameter specifies the speech resource type.

vrm.client.resource.uri

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

This parameter specifies the URI to the speech resource, e.g. sip:mresources@<MRCP server IP>:<port>. Please consult your MRCP vendor documentation for appropriate setting.

vrm.client.SendLoggingTag

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

When this option is set to true the SRM Client will set the logging-tag parameter in the first SET-PARAMS method to the unique Call ID of the call.

vrm.client.SendSessionXML

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

When this is set, the SRM client will send the specified session.xml contents to the MRCP server. Note, this should not be set to true to any MRCP server other than the Nuance Speech Server 6.1 or later.

vrm.client.SendSilence

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

If set to true, the MCP will send silence audio to the MRCP server during a recognition session pause period. Otherwise, the MCP will not send any audio during a recognition session pause period.

vrm.client.SendSWMSParams

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

When this is set, the SRM client will send the SWMS parameters using the SWMS 3.0 convention.

vrm.client.SrtpLifetime

Default Value: 48
Valid Values: Must be 48
Changes Take Effect: At start/restart

This parameter specifies the SRTP packets lifetime maximum. 48 is the value once supported by Nuance Speech Server 5.0.2.

vrm.client.TelispeechRecognitionBargein

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

Set to true to support Telisma bargein recognition capability.

vrm.client.TlsCertificateKey

Default Value: $InstallationRoot$/config/x509_certificate.pem
Valid Values:
Changes Take Effect: At start/restart

This parameter specifies the path to TLS Certificate Key. Make sure you acquire the key and from the MRCPv2 server vendor. Place them in the places specified by this parameter in the corresponding resources.

vrm.client.TlsPassword

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

If the TLS certificate key and Private key are password protected, this parameter can be used to specify the password. An empty value of this parameter means no password is required

vrm.client.TlsPrivateKey

Default Value: $InstallationRoot$/config/x509_private_key.pem
Valid Values:
Changes Take Effect: At start/restart

This parameter specifies the path to TLS Private Key. Make sure you acquire the key and from the MRCPv2 server vendor. Place them in the places specified by this parameter in the corresponding resources.

vrm.client.TlsProtocolType

Default Value: TLSv1
Valid Values:
Changes Take Effect: At start/restart

This parameter specifies the TLS Protocol Type.

vrm.client.TransportProtocol

Default Value: MRCPv2
Valid Values:
Changes Take Effect: At start/restart

This parameter specifies the MRCP protocol used by the Speech Resource.

MRCPv2_TTS

Options for this component are contained in the following configuration sections:

- provision

Tip

In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.

Power users: Download a CSV file containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
provision	vrm.client.ConnectPerSetup	true	
provision	vrm.client.NoSpeechLanguageHeader	false	At start/restart
provision	vrm.client.resource.name		At start/restart
provision	vrm.client.resource.type	TTS	At start/restart
provision	vrm.client.resource.uri		At start/restart
provision	vrm.client.SendLoggingTag	true	
provision	vrm.client.SendSessionXML	false	At start/restart
provision	vrm.client.SpeechMarkerEncoding	UTF-8	At start/restart
provision	vrm.client.SrtpLifetime	48	At start/restart
provision	vrm.client.TlsCertificateKey	$InstallationRoot$/config/x509_certificate.pem	At start/restart
provision	vrm.client.TlsPassword		At start/restart
provision	vrm.client.TlsPrivateKey	$InstallationRoot$/config/x509_private_key.pem	At start/restart
provision	vrm.client.TlsProtocolType	TLSv1	At start/restart
provision	vrm.client.TransportProtocol	MRCPv2	At start/restart
provision	vrm.client.TTSInsertVoiceTag	false	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

provision Section

- vrm.client.ConnectPerSetup
- vrm.client.NoSpeechLanguageHeader
- vrm.client.resource.name
- vrm.client.resource.type
- vrm.client.resource.uri
- vrm.client.SendLoggingTag
- vrm.client.SendSessionXML
- vrm.client.SpeechMarkerEncoding
- vrm.client.SrtpLifetime
- vrm.client.TlsCertificateKey
- vrm.client.TlsPassword
- vrm.client.TlsPrivateKey
- vrm.client.TlsProtocolType
- vrm.client.TransportProtocol
- vrm.client.TTSInsertVoiceTag

vrm.client.ConnectPerSetup

Default Value: true
Valid Values:
Changes Take Effect:

When this option is set to true the SRM Client will create a new connection to the ASR or TTS server per MRCP session setup.

vrm.client.NoSpeechLanguageHeader

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

When this parameter is set to true, the SRM Client will not send the Speech-Language header in MRCP SET-PARAMS and SPEAK requests in a TTS session. Without the Speech-Language header, some MRCP TTS servers is able to use its default language when the application specified language is absent.

vrm.client.resource.name

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

This parameter specifies the name of resource name. Some common names are SPEECHWORKS, REALSPEAK

vrm.client.resource.type

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

This parameter specifies the speech resource type.

vrm.client.resource.uri

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

This parameter specifies the URI to the speech resource, e.g. sip:mresources@<MRCP server IP>:<port>. Please consult your MRCP vendor documentation for appropriate setting.

vrm.client.SendLoggingTag

Default Value: true
Valid Values:
Changes Take Effect:

When this option is set to true the SRM Client will set the logging-tag parameter in the first SET-PARAMS method to the unique Call ID of the call.

vrm.client.SendSessionXML

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

When this is set, the SRM client will send the specified session.xml contents to the MRCP server. Note, this should not be set to true to any MRCP server other than the Nuance Speech Server 6.1 or later.

vrm.client.SpeechMarkerEncoding

Default Value: UTF-8
Valid Values:

Changes Take Effect: At start/restart

If a TTS MRCP server does not have the content-encoding header to specify the Speech Marker name encoding in a SPEECH-MARKER event, the SRM client will use the value specified by this parameter as the encoding of the Speech Marker name.

vrm.client.SrtpLifetime

Default Value: 48
Valid Values: Must be 48
Changes Take Effect: At start/restart

This parameter specifies the SRTP packets lifetime maximum. 48 is the value once supported by Nuance Speech Server 5.0.2.

vrm.client.TlsCertificateKey

Default Value: $InstallationRoot$/config/x509_certificate.pem
Valid Values:
Changes Take Effect: At start/restart

This parameter specifies the path to TLS Certificate Key. Make sure you acquire the key and from the MRCPv2 server vendor. Place them in the places specified by this parameter in the corresponding resources.

vrm.client.TlsPassword

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

If the TLS certificate key and Private key are password protected, this parameter can be used to specify the password. An empty value of this parameter means no password is required

vrm.client.TlsPrivateKey

Default Value: $InstallationRoot$/config/x509_private_key.pem
Valid Values:
Changes Take Effect: At start/restart

This parameter specifies the path to TLS Private Key. Make sure you acquire the key and from the MRCPv2 server vendor. Place them in the places specified by this parameter in the corresponding resources.

vrm.client.TlsProtocolType

Default Value: TLSv1
Valid Values:
Changes Take Effect: At start/restart

This parameter specifies the TLS Protocol Type.

vrm.client.TransportProtocol

Default Value: MRCPv2
Valid Values:
Changes Take Effect: At start/restart

This parameter specifies the MRCP protocol used by the Speech Resource.

vrm.client.TTSInsertVoiceTag

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

When this option is set to true, the SRM Client will use the voice name defined in the TTSENGINE property to tell the TTS engine what voice to use.

Connectors

The GVP 8.5 deployment supports the following connectors:

- CTI Connector

  The CTI Connector acts as a SIP B2B UA to provide a SIP interface to the GVP components. It communicates with CTI by using the following protocols and interfaces:

  - ML over TCP/IP with Genesys IVR Server
  - GED-125 interface over TCP/IP with Cisco ICM.

  The CTI Connector acts as a border element within GVP, interfacing with the CTI network on one side, and through the Resource Manager, interacts with the Media Control Platform on the other side.

  For more information about the CTI Connector, see CTI Connector in the *GVP Deployment Guide*. For the CTI Connector configuration options, see CTI Connector Options in this document.

- UCM Connector

  The UCM Connector is a stand alone component, which acts as a gateway between Cisco T-Servers (a Genesys component) and switches, and GVP to provide media services.

  Cisco T-Server communicates with Cisco switches by using CP4SM (a Genesys proprietary protocol) rather than the SIP communication protocol. The UCM Connector performs the translation between CP4SM messages and SIP events.

  For more information about the UCM Connector, see Connector Overview in the *Genesys Media Server Deployment Guide*. For the UCM Connector configuration options, see UCM Connector Options in this document.

- PSTN Connector

  The PSTN Connector is a stand-alone component that provides connectivity to traditional telephony networks and equipment, such as a private branch exchange (PBX) or automatic call distribution (ACD). Used for existing deployments that use Dialogic TDM cards; the PSTN Connector provides seamless integration and migration to the IP-based GVP 8.5 architecture.

For more information about the PSTN Connector, see PSTN Connector in the *GVP Deployment Guide*. For the PSTN Connector configuration options, see PSTN Connector Options in this document.

CTI Connector

Options for this component are contained in the following configuration sections:

- CTIC
- ems
- ICMC
- IServer_Sample
- IVRSC
- log
- mediacontroller
- sip
- Tenant1

Tip

In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.

Power users: Download a CSV file containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
CTIC	copy-originatingleg-headers	X-Genesys-GVP-Session-Data	After restart
CTIC	CTIFramework	IVRServerClient	After restart
CTIC	DefaultDNIS		After restart
CTIC	disable_cdr	false	After restart
CTIC	fips_enabled	False	After restart
CTIC	GetDNISFromIServer	false	After restart
CTIC	IVRPortBaseIndex	-1	After restart
CTIC	MaxIVRPorts	2000	After restart
ems	logconfig.MFSINK	• |*|*	immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
ems	logconfig.TRAPSINK	• |*|*	At start/restart
ems	trace_flag	FALSE	immediately
ICMC	CancelResponseTimeoutMSec	2500	After restart
ICMC	ConnectMsgTimeoutMSec	3500	After restart
ICMC	DNISIndicator		After restart
ICMC	eccSessionIdVarName	userSessionId	At start/restart
ICMC	eccvariablelist	userSessionId:5000	At start/restart
ICMC	enablePreRouting	false	After restart
ICMC	ICMInterface	0	After restart
ICMC	ICMUnavailableAction	hangup	At start/restart
ICMC	NewCallTimeoutMsec	1500	After restart
ICMC	RunScriptResultTimeoutMsec	2500	After restart
ICMC	SessionIdleTimeoutMSec	120000	After restart
ICMC	TransferOnDialogFailure	false	At start/restart
ICMC	translation-routed-call	false	After restart
ICMC	TrunkGroupID	0	After restart
IServer_Sample	cafile		After restart
IServer_Sample	certificate		After restart
IServer_Sample	clientname		After restart
IServer_Sample	enablekeepalivereq	0	After restart
IServer_Sample	iserveraddr		After restart
IServer_Sample	iserversocket		After restart
IServer_Sample	IVRSCClientPortRange		After restart
IServer_Sample	keepalivereqinterval	5	After restart
IServer_Sample	keepaliveresptimeout	3	After restart
IServer_Sample	key		After restart
IServer_Sample	noofkeepalivereqtosendinfailurecase	3	After restart
IServer_Sample	password		After restart
IServer_Sample	secured	false	After restart
IServer_Sample	type		After restart
IServer_Sample	verifydepth	1	After restart
IServer_Sample	verifypeer	false	After restart
IVRSC	customeriserverslist	IServer_Sample;	After restart
IVRSC	fetchscriptidfromurs	0	After restart
IVRSC	scriptidkeyname		After restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
log	all	../logs/CTIConnector	immediately
log	check-point	1	immediately
log	compatible-output-priority	false	immediately
log	debug	../logs/CTIConnector	immediately
log	expire	20	immediately
log	interaction	../logs/CTIConnector	immediately
log	keep-startup-file	false	After restart
log	memory		immediately
log	messagefile		Immediately, if an application cannot find its *.lms file at startup
log	message_format	short	immediately
log	print-attributes	false	immediately
log	segment	10000	immediately
log	spool		immediately
log	standard	../logs/CTIConnector	immediately
log	time_convert	local	immediately
log	time_format	time	immediately
log	trace	../logs/CTIConnector	immediately
log	verbose	standard	immediately
mediacontroller	codec_check_exclusion.payloads	13	immediately
mediacontroller	sdp.defaultipversion	true	immediately
mediacontroller	sdp.localhost	$LocalIP$	immediately
mediacontroller	sdp.localhost.ipv6	$LocalIPv6$	immediately
mediacontroller	suppress_bye_after_refer	false	immediately
sip	localuser	CTIConnector	At start/restart
sip	mtusize	1500	After restart
sip	tcp.portrange		At start/restart
sip	tls.portrange		At start/restart
sip	transport.0	transport0 udp:any:5080	At start/restart
sip	transport.1	transport1 tcp:any:5080	At start/restart
sip	transport.2	transport2 tls:any:5081 cert=$InstallationRoot$/config/x509_certificate.pem key=$InstallationRoot$/config/x509_private_key.pem	At start/restart
sip	transport.localaddress		At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
sip	transport.localaddress.srv	false	At start/restart
sip	transport.localaddress_ipv6		At start/restart
sip	transport.routefailovertime	5	At start/restart
sip	transport.routerecoverytime	30	At start/restart
sip	transport.staticroutelist		At start/restart
sip	transport.unavailablewakeup	true	At start/restart
Tenant1	Ports	9000	After restart
Tenant1	TenantName		After restart
Section	**Option**	**Default**	**Changes Take Effect**

CTIC Section

- copy-originatingleg-headers
- CTIFramework
- DefaultDNIS
- disable_cdr
- fips_enabled
- GetDNISFromIServer
- IVRPortBaseIndex
- MaxIVRPorts

copy-originatingleg-headers

Default Value: X-Genesys-GVP-Session-Data
Valid Values:
Changes Take Effect: After restart

The CTI Connector shall copy all headers matching the configured list of prefixes on to other call legs towards MCP and agent

CTIFramework

Default Value: IVRServerClient
Valid Values: IVRServerClient, CiscoICMClient
Changes Take Effect: After restart

This parameter indicates which CTI Framework to be used by CTI Connector for CTI functionalities.

DefaultDNIS

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

The value of this parameter defines Default DNIS, incase I-Server does not send DNIS.

disable_cdr

Default Value: false

Valid Values: true, false
Changes Take Effect: After restart

This Parameter is included to Disable/Enable the CRD feature from CTI-C

fips_enabled

Default Value: False
Valid Values: True, False
Changes Take Effect: After restart

Specifies whether to enable FIPS mode in CTI Connector. When FIPS mode is enabled, only FIPS 140-2 approved ciphers and algorithms can be used in SSL connections.

GetDNISFromIServer

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

The value of this parameter indicates whether CTIConnector needs to get the DNIS value from IVR Server.

IVRPortBaseIndex

Default Value: -1
Valid Values:
Changes Take Effect: After restart

CTI Connector would use this parameter as starting IVRport number and it would increment the IVRPort by (1). If this parameter is set to (-1) CTIC will not generate IVR Port rather it will take the port base on DNIndicator.

MaxIVRPorts

Default Value: 2000
Valid Values:
Changes Take Effect: After restart

CTI Connector would use this parameter as upper bound to generate IVRPort number.

ems Section

- logconfig.MFSINK
- logconfig.TRAPSINK
- trace_flag

logconfig.MFSINK

Default Value:

- |*|*

Valid Values: Pipe delimited ranges for log levels, module IDs and specifier IDs. Ranges can be comma separated integers or range of integers or '*'.
Changes Take Effect: immediately

Controls the log messages that are sent to the MF sink. The format is 'levels|moduleIDs|specifierIDs' (repeated if necessary). The values between the pipes can be in the format: 'm-n,o,p' (ie "0-4, 5,6"). The wildcard character '*' can also be used to indicate all valid numbers. Example: '*|*|*' indicates that all log messages should be sent to the sink. Alternatively, '0,1|0-10|*|4|*|*' indicates that CRITICAL(0) and ERROR(1) level messages with module IDs in the range 0-10 will be sent to the sink; and all INFO(4) level messages will be sent as well.

logconfig.TRAPSINK

Default Value:

- |*|*

Valid Values:
Changes Take Effect: At start/restart

Specifies the metrics that are delivered to the SNMP Trap Sink.

trace_flag

Default Value: FALSE
Valid Values: FALSE, TRUE
Changes Take Effect: immediately

Flag specifying whether debug level logging is enabled. When enabled (flag is set to TRUE), debug level logs will be processed and filtered like other log levels. When the flag is set to FALSE, debug level log messages will never be processed.

ICMC Section

- CancelResponseTimeoutMSec
- ConnectMsgTimeoutMSec
- DNISIndicator
- eccSessionIdVarName
- eccvariablelist
- enablePreRouting
- ICMInterface
- ICMUnavailableAction
- NewCallTimeoutMsec
- RunScriptResultTimeoutMsec
- SessionIdleTimeoutMSec
- TransferOnDialogFailure
- translation-routed-call
- TrunkGroupID

CancelResponseTimeoutMSec

Default Value: 2500
Valid Values:
Changes Take Effect: After restart

CTI Connector waits for the (CONNECT/RELEASE) response to CancelResponse message from ICM for the specified time. If no response is received with in the configured time then CTIConnector shall clear the call.

ConnectMsgTimeoutMSec

Default Value: 3500
Valid Values:
Changes Take Effect: After restart

CTI Connector waits for the (CONNECT_TO_RESOURCE/CONNECT/RELEASE) response from ICM for the specified time. If no response is received with in the configured time then CTIConnector shall clear the call.

DNISIndicator

Default Value:
Valid Values: sid, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10
Changes Take Effect: After restart

This parameter value indicates which field fron RUN_SCRIPT_REQ message should be used for fetching the DNIS value.

eccSessionIdVarName

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

CTI Connector shall take the SessionId and send it to ICM through this variable. Example : userECCVar1 The variable name configured here ("userECCVar1" in the example) should be specified in the ECC Variables list. If not, the SessionId will not be sent in the NEW_CALL message. By default, it will be set to "userSessionId" and the SessionId will be sent through userSessionId. If it is empty, the SessionId will not be sent in the NEW_CALL message.

eccvariablelist

Default Value: userSessionId:5000
Valid Values:
Changes Take Effect: At start/restart

CTI Connector shall take the configured list of ECC variable names and register it with ICM through initial REGISTER_VARIABLES message. The ECC variable names along with their tag values should be separated by comma. The ECC variable may be specified without a tag, in which case, CTIC will generate a tag for it. Example: userECCVar1:5010,userECCVar2,userECCVar3:5011 Default value is userSessionId:5000

enablePreRouting

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

This parameter should be set to true when call is pre-routed to ICM (for Network VRU deployment type 2/3/7/8/). In this case the CTI Connector sends REQUEST_INSTRUCTION message for establishing the call with ICM.

ICMInterface

Default Value: 0
Valid Values: 0, 1
Changes Take Effect: After restart

This parameter indicates about the interface that CTIC shall use to communicate with ICM. By default

CTIConnector shall use the Service Control Interface to communicate with ICM.

ICMUnavailableAction

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

This parameter describes action to take when the ICM connection break during a call . When action is 'transfer' CTIC transfers the call using REFER to the destination specified in the "cti.FailoverNumber" in IVR profile.

NewCallTimeoutMsec

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

CTI Connector waits for the (RUN_SCRIPT_REQ/CONNECT/RELEASE) response to NEW_CALL message from ICM for the specified time. If no response is received with in the configured time then CTIConnector shall clear the call.

RunScriptResultTimeoutMsec

Default Value: 2500
Valid Values:
Changes Take Effect: After restart

CTI Connector waits for the (RUN_SCRIPT_REQ/CONNECT/RELEASE) response to Run Script Result message from ICM for the specified time. If no response is received with in the configured time then CTIConnector shall clear the call.

SessionIdleTimeoutMSec

Default Value: 120000
Valid Values:
Changes Take Effect: After restart

Maximum time the call will be kept active in CTIConnector, after the timeout CTIConnector will clear the call.

TransferOnDialogFailure

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

This parameter describes action to take when the ICM responds with DIALOGUE_FAILURE_EVENT for RUN_SCRIPT_RESULT . When it is set to 'true' CTIC transfers the call using REFER to the destination specified in the "cti.FailoverNumber" in IVR profile.

translation-routed-call

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

This parameter value indicates CTIC whether the incoming is translation routed or normal call. The default value for this parameter is false.This should be set to true for Type 8 Network VRU deployment.

TrunkGroupID

Default Value: 0
Valid Values:
Changes Take Effect: After restart

The Trunk Group ID information is sent to ICM for every call through VRU-PG for ICM reporting purpose

IServer_Sample Section

- cafile
- certificate
- clientname
- enablekeepalivereq
- iserveraddr
- iserversocket
- IVRSCClientPortRange
- keepalivereqinterval
- keepaliveresptimeout
- key
- noofkeepalivereqtosendinfailurecase
- password
- secured
- type
- verifydepth
- verifypeer

cafile

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

The path and the filename of the certificate to be used for verifying the peer.

certificate

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

The path and the filename of the TLS certificate.

clientname

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

The IVR Group Name on the CME

enablekeepalivereq

Default Value: 0
Valid Values:
Changes Take Effect: After restart

To Enable the KeepAlive Request from IVR-SC (Heartbeat IVR-SC -> IVR-Server)

iserveraddr

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

The IP Address of the IVR Server machine

iserversocket

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

The gli_server_address port on the IVR Server. Usually the port is 9090

IVRSCClientPortRange

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

This parameter defines CTI Connector TCP port range used for communication with IVR Server. The lower and upper limit is 1030 and 65535 respectively. If value is not specified then CTI Connector will let OS choose the local port value. For example : 7775-7780

keepalivereqinterval

Default Value: 5
Valid Values:
Changes Take Effect: After restart

The KeepAlive Request Interval

keepaliveresptimeout

Default Value: 3
Valid Values:
Changes Take Effect: After restart

KeepAlive Response Timeout

key

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

The path and the filename of the TLS key to be used.

noofkeepalivereqtosendinfailurecase

Default Value: 3
Valid Values:
Changes Take Effect: After restart

Number of request to be sent to IVR-Server before being marrked as unavailable

password

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

The password associated with the certificate and key pair. Required only if key file is password protected.

secured

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

Enable the TLS connection request from cticonnector (CTIConnector -> IVR-Server)

type

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

TLS version to used for connection.

verifydepth

Default Value: 1
Valid Values:
Changes Take Effect: After restart

This parameter sets the maximum depth for the certificate chain verification.

verifypeer

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

This parameter turns on peer certificate verification.

IVRSC Section

- customeriserverslist
- fetchscriptidfromurs
- scriptidkeyname

customeriserverslist

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

Lists all the IVR Servers. The IVRServer in customeriserverlist should be separated by semicolon (";").

fetchscriptidfromurs

Default Value: 0
Valid Values:
Changes Take Effect: After restart

For fetching the user defined key value from framework Default is set to 0

scriptidkeyname

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

Key name which is configured in Framework side and which will be used in UdataGet message by IVR Server Cleint.Applicable only when IVR Server Mode set to 'Behind the Switch' Mode.

log Section

- all
- check-point
- compatible-output-priority
- debug
- expire
- interaction
- keep-startup-file
- memory
- message_format
- messagefile
- print-attributes
- segment
- spool
- standard
- time_convert
- time_format
- trace
- verbose

all

Default Value: ../logs/CTIConnector

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends all log events. The log output types must be separated by a comma when more than one output is configured.

check-point

Default Value: 1
Valid Values: 0 - 24
Changes Take Effect: immediately

Specifies, in hours, how often the application generates a check point log event, to divide the log into sections of equal time. By default, the application generates this log event every hour. Setting the option to 0 prevents the generation of check-point events.

compatible-output-priority

Default Value: false

Valid Values:

- **true** The log of the level specified by "Log Output Options" is sent to the specified output.
- **false** The log of the level specified by "Log Output Options" and higher levels is sent to the specified output.
Changes Take Effect: immediately
Specifies whether the application uses 6.x output logic.

debug

Default Value: ../logs/CTIConnector

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
Changes Take Effect: immediately
Specifies the outputs to which an application sends the log events of the Debug level and higher (that is, log events of the Standard, Interaction, Trace, and Debug levels). The log output types must be separated by a comma when more than one output is configured.

expire

Default Value: 20

Valid Values:

- **false** No expiration; all generated segments are stored.
- **[number] file or [number]** Sets the maximum number of log files to store. Specify a number from 1-1000.
- **[number] day** Sets the maximum number of days before log files are deleted. Specify a number from 1-100.
Changes Take Effect: immediately
Determines whether log files expire. If they do, sets the measurement for determining when they expire, along with the maximum number of files (segments) or days before the files are removed. This option is ignored if log output is not configured to be sent to a log file. Note: If the value of the option is set incorrectly -out of the range of valid values- it will be automatically reset to 10

interaction

Default Value: ../logs/CTIConnector

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends the log events of the Interaction level and higher (that is, log events of the Standard and Interaction levels). The log outputs must be separated by a comma when more than one output is configured.

keep-startup-file

Default Value: false

Valid Values:

- **false** No startup segment of the log is kept.
- **true** A startup segment of the log is kept. The size of the segment equals the value of the segment option.
- **[number] KB** Sets the maximum size, in kilobytes, for a startup segment of the log.
- **[number] MB** Sets the maximum size, in megabytes, for a startup segment of the log.
  Changes Take Effect: After restart
  Specifies whether a startup segment of the log, containing the initial T-Server configuration, is to be kept. If it is, this option can be set to true or to a specific size. If set to true, the size of the initial segment will be equal to the size of the regular log segment defined by the segment option. The value of this option will be ignored if segmentation is turned off (that is, if the segment option set to false).

memory

Default Value:
Valid Values: [string] (memory file name)
Changes Take Effect: immediately

Specifies the name of the file to which the application regularly prints a snapshot of the memory output, if it is configured to do this. The new snapshot overwrites the previously written data. If the application terminates abnormally, this file will contain the latest log messages. Memory output is not recommended for processors with a CPU frequency lower than 600 MHz.

message_format

Default Value: short

Valid Values:

- **short** An application uses compressed headers when writing log records in its log file.
- **full** An application uses complete headers when writing log records in its log file.
  Changes Take Effect: immediately
  Specifies the format of log record headers that an application uses when writing logs in the log file. Using compressed log record headers improves application performance and reduces the log file's size. With the value set to short:
- A header of the log file or the log file segment contains information about the application (such as the application name, application type, host type, and time zone), whereas single log records within the file or segment omit this information.
- A log message priority is abbreviated to Std, Int, Trc, or Dbg, for Standard, Interaction, Trace, or Debug messages, respectively.
- The message ID does not contain the prefix GCTI or the application type ID.
  A log record in the full format looks like this:
  2002-05-07T18:11:38.196 Standard localhost cfg_dbserver GCTI-00-05060 Application started
  A log record in the short format looks like this:
  2002-05-07T18:15:33.952 Std 05060 Application started

messagefile

Default Value:
Valid Values: [string].lms (message file name)
Changes Take Effect: Immediately, if an application cannot find its *.lms file at startup

Specifies the file name for application-specific log events. The name must be valid for the operating system on which the application is running. The option value can also contain the absolute path to the application-specific *.lms file. Otherwise, an application looks for the file in its working directory.

print-attributes

Default Value: false
Valid Values: true, false
Changes Take Effect: immediately

Specifies whether the application attaches extended attributes, if any exist, to a log event that it sends to log output. Typically, log events of the Interaction log level and Audit-related log events contain extended attributes. Setting this option to true enables audit capabilities, but negatively affects performance. Genesys recommends enabling this option for Solution Control Server and Configuration Server when using audit tracking. For other applications, refer to Genesys 7.5 Combined Log Events Help to find out whether an application generates Interaction-level and Audit-related log events; if it does, enable the option only when testing new interaction scenarios.

- **true** Attaches extended attributes, if any exist, to a log event sent to log output.
- **false** Does not attach extended attributes to a log event sent to log output.

segment

Default Value: 10000

Valid Values:

- **false** No segmentation is allowed.
- **[number] KB or [number]** Sets the maximum segment size, in kilobytes. The minimum segment size is 100 KB.
- **[number] MB** Sets the maximum segment size, in megabytes.
- **[number] hr** Sets the number of hours for the segment to stay open. The minimum number is 1 hour.
Changes Take Effect: immediately
Specifies whether there is a segmentation limit for a log file. If there is, sets the mode of measurement, along with the maximum size. If the current log segment exceeds the size set by this option, the file is closed and a new one is created.

spool

Default Value:
Valid Values: [path] (the folder, with the full path to it)
Changes Take Effect: immediately

Specifies the folder, including full path to it, in which an application creates temporary files related to network log output. If you change the option value while the application is running, the change does not affect the currently open network output.

standard

Default Value: ../logs/CTIConnector

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
Changes Take Effect: immediately
Specifies the outputs to which an application sends the log events of the Standard level. The log output types must be separated by a comma when more than one output is configured.

time_convert

Default Value: local
Valid Values: local, utc
Changes Take Effect: immediately

Specifies the system in which an application calculates the log record time when generating a log file. The time is converted from the time in seconds since the Epoch (00:00:00 UTC, January 1, 1970).

- **Local Time (local)** The time of log record generation is expressed as a local time, based on the time zone and any seasonal adjustments. Time zone information of the application's host computer is used.
- **Coordinated Universal Time (utc)** The time of log record generation is expressed as Coordinated Universal Time (UTC).

time_format

Default Value: time
Valid Values: time, locale, ISO8601
Changes Take Effect: immediately

Specifies how to represent, in a log file, the time when an application generates log records.
A log record's time field in the ISO 8601 format looks like this:
2001-07-24T04:58:10.123

- **HH:MM:SS.sss (time)** The time string is formatted according to the HH:MM:SS.sss (hours, minutes, seconds, and milliseconds) format.
- **According to the system's locale (locale)** The time string is formatted according to the system's locale.
- **ISO 8601 format (ISO8601)** The date in the time string is formatted according to the ISO 8601 format. Fractional seconds are given in milliseconds.

trace

Default Value: ../logs/CTIConnector

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends the log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels). The log outputs must be separated by a comma when more than one output is configured.

verbose

Default Value: standard

Valid Values:

- **all** All log events (that is, log events of the Standard, Trace,Interaction, and Debug levels) are generated.

- **debug** The same as all.
- **trace** Log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels) are generated, but log events of the Debug level are not generated.
- **interaction** Log events of the Interaction level and higher (that is, log events of the Standard and Interaction levels) are generated, but log events of the Trace and Debug levels are not generated.
- **standard** Log events of the Standard level are generated, but log events of the Interaction, Trace, and Debug levels are not generated.
- **none** No output is produced.
  Changes Take Effect: immediately
  Determines whether a log output is created. If it is, specifies the minimum level of log events generated. The log events levels, starting with the highest priority level, are Standard, Interaction, Trace, and Debug.

mediacontroller Section

- codec_check_exclusion.payloads
- sdp.defaultipversion
- sdp.localhost
- sdp.localhost.ipv6
- suppress_bye_after_refer

codec_check_exclusion.payloads

Default Value: 13
Valid Values:
Changes Take Effect: immediately

A list of space delimited payloads that will be excluded during codec checking for join result determination.

sdp.defaultipversion

Default Value: true
Valid Values: ipv4, ipv6
Changes Take Effect: immediately

Default IP version to be used in SDP message, apply to initiated SDP offer to unjoined endpoint. Valid values are "ipv4" or "ipv6".

sdp.localhost

Default Value: $LocalIP$
Valid Values:
Changes Take Effect: immediately

The local host IPv4 address (only the host part) that will be used in SDP.

sdp.localhost.ipv6

Default Value: $LocalIPv6$

Valid Values:
Changes Take Effect: immediately

The local host IPv6 address (only the host part) that will be used in SDP.

suppress_bye_after_refer

Default Value: false

Valid Values:

- **1** Enable suppression
- **0** Disable suppression
  Changes Take Effect: immediately
  Suppress BYE after successful REFER. Turn on this feature if the call flow expects to receive BYE, this will avoid BYE messages from both direction.

session

This section contains no public options.

sip Section

- localuser
- mtusize
- tcp.portrange
- tls.portrange
- transport.0
- transport.1
- transport.2
- transport.localaddress
- transport.localaddress_ipv6
- transport.localaddress.srv
- transport.routefailovertime
- transport.routerecoverytime
- transport.staticroutelist
- transport.unavailablewakeup

localuser

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

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

mtusize

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

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

tcp.portrange

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

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

tls.portrange

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

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

transport.0

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

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

where transport_name is any string; type is udp/tcp/tls; ip is the IP address of the network interface that accepts incoming SIP messages; To define a transport to listen to all IPv4 interfaces, use "any" or "any4" for ip. To define a transport to listen to all IPv6 interfaces, use "any6" for ip. port is the port number where SIP stack accepts incoming SIP messages;
[parameters] defines any extra SIP transport parameters.

Example:
cert=[cert path and filename] Applicable to SIPS only and mandatory if using SIPS. The path and the filename of the TLS certificate to be used key=[key path and filename] Applicable to SIPS only and mandatory if using SIPS. The path and the filename of the TLS key to be used. type=[Type of secure transport] Applicable to SIPS only and is optional. The type of secure transport to be used and value can be TLSv1, SSLv3, SSLv23, TLSv1_1, TLSv1_2. Default to TLSv1_2. Note that SSLv2 is no longer supported. password=[password] Applicable to SIPS only and is optional. The password associated with the certificate and key pair. Required only if key file is password protected. cafile=[CA cert path and filename] Mandatory for TLS mutual authentication. The path and the filename of the certificate to be used for verifying the peer. The same certificate specified in cert=[cert path and filename] parameter can be used as the value here if using only 1 certificate is preferred. verifypeer=true Mandatory for TLS mutual authentication. This parameter turns on the TLS mutual authentication. verifydepth=[max depth for the certificate chain verification] Applicable only to TLS mutual authentication. This parameter sets the maximum depth for the certificate chain verification. For the default Genesys certificate provided, the recommended value is 1.

transport.1

Default Value: transport1 tcp:any:5080

Valid Values:
Changes Take Effect: At start/restart

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

where transport_name is any string; type is udp/tcp/tls; ip is the IP address of the network interface that accepts incoming SIP messages; To define a transport to listen to all IPv4 interfaces, use "any" or "any4" for ip. To define a transport to listen to all IPv6 interfaces, use "any6" for ip. port is the port number where SIP stack accepts incoming SIP messages;
[parameters] defines any extra SIP transport parameters.

Example:
cert=[cert path and filename] Applicable to SIPS only and mandatory if using SIPS. The path and the filename of the TLS certificate to be used key=[key path and filename] Applicable to SIPS only and mandatory if using SIPS. The path and the filename of the TLS key to be used. type=[Type of secure transport] Applicable to SIPS only and is optional. The type of secure transport to be used and value can be TLSv1, SSLv3, SSLv23, TLSv1_1, TLSv1_2. Default to TLSv1_2. Note that SSLv2 is no longer supported. password=[password] Applicable to SIPS only and is optional. The password associated with the certificate and key pair. Required only if key file is password protected. cafile=[CA cert path and filename] Mandatory for TLS mutual authentication. The path and the filename of the certificate to be used for verifying the peer. The same certificate specified in cert=[cert path and filename] parameter can be used as the value here if using only 1 certificate is preferred. verifypeer=true Mandatory for TLS mutual authentication. This parameter turns on the TLS mutual authentication. verifydepth=[max depth for the certificate chain verification] Applicable only to TLS mutual authentication. This parameter sets the maximum depth for the certificate chain verification. For the default Genesys certificate provided, the recommended value is 1.

transport.2

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

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

where transport_name is any string; type is udp/tcp/tls; ip is the IP address of the network interface that accepts incoming SIP messages; To define a transport to listen to all IPv4 interfaces, use "any" or "any4" for ip. To define a transport to listen to all IPv6 interfaces, use "any6" for ip. port is the port number where SIP stack accepts incoming SIP messages;
[parameters] defines any extra SIP transport parameters.

Example:
cert=[cert path and filename] Applicable to SIPS only and mandatory if using SIPS. The path and the filename of the TLS certificate to be used key=[key path and filename] Applicable to SIPS only and mandatory if using SIPS. The path and the filename of the TLS key to be used. type=[Type of secure transport] Applicable to SIPS only and is optional. The type of secure transport to be used and value

can be TLSv1, SSLv3, SSLv23, TLSv1_1, TLSv1_2. Default to TLSv1_2. Note that SSLv2 is no longer supported. password=[password] Applicable to SIPS only and is optional. The password associated with the certificate and key pair. Required only if key file is password protected. cafile=[CA cert path and filename] Mandatory for TLS mutual authentication. The path and the filename of the certificate to be used for verifying the peer. The same certificate specified in cert=[cert path and filename] parameter can be used as the value here if using only 1 certificate is preferred. verifypeer=true Mandatory for TLS mutual authentication. This parameter turns on the TLS mutual authentication. verifydepth=[max depth for the certificate chain verification] Applicable only to TLS mutual authentication. This parameter sets the maximum depth for the certificate chain verification. For the default Genesys certificate provided, the recommended value is 1.

transport.localaddress

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

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

transport.localaddress_ipv6

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

If specified, the sent-by field of the Via header and the hostport part of the Contact header in the outgoing SIP message will be set to this value if a IPv6 transport is used. The value must be a hostname or domain name. If left empty the outgoing transport's actual IP and port will be used for the Via header and the Contact header. Note that if the domain name used in the SRV record query is specified, sip.transport.localaddress.srv must be set to true to prevent the port part being automatically generated by the SIP stack.

transport.localaddress.srv

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

Specifies whether the sip.transport.localaddress contains an SRV domain name. If set to true, port part will not be automatically generated by the SIP stack. Otherwise, the outgoing transport's port will used together with the hostname specified by the sip.transport.localaddress.

transport.routefailovertime

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

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

transport.routerecoverytime

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

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

transport.staticroutelist

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

Specifies a list of static routes. Each route group is separated by |. Each static route group is a list of IP addresses separated by comma. Within the route group, each IP address could substitute each other as an alternate route destination if sending a SIP request to one of the IP address fails. For example, 10.0.0.1,10.0.0.2|10.0.10.1,10.0.10.2 specified two static route groups, and each group specified two routes that are alternative to each other. Default value is an empty list.

transport.unavailablewakeup

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

Specifies whether unavailable route destinations can be made active if needed before the route recover timer expires. The unavailable destinations would be made active only when all destinations corresponding to a static route group or DNS SRV domain are unavailable. This parameter is applicable when SIP stack is running under HA mode (Static route list or DNS SRV routing).

Tenant1 Section

- Ports
- TenantName

Ports

Default Value: 9000
Valid Values:
Changes Take Effect: After restart

List of listener port numbers separated by comma on which CTIConnector waits for TCP connection from Cisco VRU-PG. Optionally the Trunk Group IDs supported by the PIMs can also be configured here. The Trunk Group IDs can be listed for a particular PIM separated by &. For example: 6000:1&2,7000,8000:3&4 In the above example 6000 supports Trunk Group IDs 1 and 2, 7000 does not specify the TG IDs it supports and 8000 supports TGIDs 3 and 4. Note: 1) Valid range for TG IDs is 0-65535. 2) Same TG IDs should not be mentioned by more than one PIM. TG IDs should be unique across all the PIMs. 3) The value mentioned as the default TrunkGroupID under ICMC section should not be specified by any of the PIMs as a supported TG.

TenantName

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

This parameter specifies the name of the Tenant.

UCM Connector

Options for this component are contained in the following configuration sections:

- ems
- log
- sip
- TServer
- UCMC

Tip

In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.

Power users: **Download a CSV file** containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
ems	logconfig.MFSINK	•	immediately
ems	logconfig.TRAPSINK •		At start/restart
ems	trace_flag	FALSE	immediately
log	all	../logs/UCMConnector	immediately
log	check-point	1	immediately
log	compatible-output-priority	false	immediately
log	debug	../logs/UCMConnector	immediately
log	expire	20	immediately
log	interaction	../logs/UCMConnector	immediately
log	keep-startup-file	false	After restart
log	memory		immediately
log	messagefile		Immediately, if an
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
			application cannot find its *.lms file at startup
log	message_format	short	immediately
log	print-attributes	false	immediately
log	segment	10000	immediately
log	spool		immediately
log	standard	../logs/UCMConnector	immediately
log	time_convert	local	immediately
log	time_format	time	immediately
log	trace	../logs/UCMConnector	immediately
log	verbose	standard	immediately
sip	localuser	UCMConnector	At start/restart
sip	mtusize	1500	After restart
sip	tcp.portrange		At start/restart
sip	tls.portrange		At start/restart
sip	transport.0	transport0 udp:any:5080	At start/restart
sip	transport.1	transport1 tcp:any:5080	At start/restart
sip	transport.2	transport2 tls:any:5081 cert=$InstallationRoot$/config/x509_certificate.pem key=$InstallationRoot$/config/x509_private_key.pem	At start/restart
sip	transport.localaddress		At start/restart
sip	transport.localaddress.srv	false	At start/restart
sip	transport.localaddress_ipv6		At start/restart
sip	transport.routefailovertime	5	At start/restart
sip	transport.routerecoverytime	30	At start/restart
sip	transport.staticroutelist		At start/restart
TServer	smloc	SM	After restart
TServer	TServerAddress		After restart
TServer	TSvrConnectionRetryCount	10	After restart
TServer	UCMCClientPortRange		After restart
UCMC	fips_enabled	False	After restart
UCMC	NotifyGMSDTMF	false	After restart
UCMC	RMAddress		After restart
UCMC	UseSecureSIP	false	After restart
Section	**Option**	**Default**	**Changes Take Effect**

ems Section

- logconfig.MFSINK
- logconfig.TRAPSINK
- trace_flag

logconfig.MFSINK

Default Value:

-

Valid Values: Pipe delimited ranges for log levels, module IDs and specifier IDs. Ranges can be comma separated integers or range of integers or '*'.
Changes Take Effect: immediately

Controls the log messages that are sent to the MF sink. The format is 'levels

logconfig.TRAPSINK

Default Value:

-

Valid Values:
Changes Take Effect: At start/restart

Specifies the metrics that are delivered to the SNMP Trap Sink.

trace_flag

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

Flag specifying whether debug level logging is enabled. When enabled (flag is set to TRUE), debug level logs will be processed and filtered like other log levels. When the flag is set to FALSE, debug level log messages will never be processed.

log Section

- all
- check-point
- compatible-output-priority
- debug
- expire
- interaction
- keep-startup-file
- memory
- message_format
- messagefile
- print-attributes
- segment
- spool
- standard
- time_convert
- time_format
- trace
- verbose

all

Default Value: ../logs/UCMConnector

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends all log events. The log output types must be separated by a comma when more than one output is configured.

check-point

Default Value: 1
Valid Values: 0 - 24
Changes Take Effect: immediately

Specifies, in hours, how often the application generates a check point log event, to divide the log into sections of equal time. By default, the application generates this log event every hour. Setting the option to 0 prevents the generation of check-point events.

compatible-output-priority

Default Value: false

Valid Values:

- **true** The log of the level specified by "Log Output Options" is sent to the specified output.
- **false** The log of the level specified by "Log Output Options" and higher levels is sent to the specified output.
Changes Take Effect: immediately
Specifies whether the application uses 6.x output logic.

debug

Default Value: ../logs/UCMConnector

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
Changes Take Effect: immediately
Specifies the outputs to which an application sends the log events of the Debug level and higher (that is, log events of the Standard, Interaction, Trace, and Debug levels). The log output types must be separated by a comma when more than one output is configured.

expire

Default Value: 20

Valid Values:

- **false** No expiration; all generated segments are stored.
- **[number] file or [number]** Sets the maximum number of log files to store. Specify a number from 1-100.
- **[number] day** Sets the maximum number of days before log files are deleted. Specify a number from 1-100.
Changes Take Effect: immediately
Determines whether log files expire. If they do, sets the measurement for determining when they expire, along with the maximum number of files (segments) or days before the files are removed.

interaction

Default Value: ../logs/UCMConnector

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends the log events of the Interaction level and higher (that is, log events of the Standard and Interaction levels). The log outputs must be separated by a comma when more than one output is configured.

keep-startup-file

Default Value: false

Valid Values:

- **false** No startup segment of the log is kept.
- **true** A startup segment of the log is kept. The size of the segment equals the value of the segment option.
- **[number] KB** Sets the maximum size, in kilobytes, for a startup segment of the log.
- **[number] MB** Sets the maximum size, in megabytes, for a startup segment of the log.
  Changes Take Effect: After restart
  Specifies whether a startup segment of the log, containing the initial T-Server configuration, is to be kept. If it is, this option can be set to true or to a specific size. If set to true, the size of the initial segment will be equal to the size of the regular log segment defined by the segment option. The value of this option will be ignored if segmentation is turned off (that is, if the segment option set to false).

memory

Default Value:
Valid Values: [string] (memory file name)
Changes Take Effect: immediately

Specifies the name of the file to which the application regularly prints a snapshot of the memory output, if it is configured to do this. The new snapshot overwrites the previously written data. If the application terminates abnormally, this file will contain the latest log messages. Memory output is not recommended for processors with a CPU frequency lower than 600 MHz.

message_format

Default Value: short

Valid Values:

- **short** An application uses compressed headers when writing log records in its log file.

- **full** An application uses complete headers when writing log records in its log file.
  Changes Take Effect: immediately
  Specifies the format of log record headers that an application uses when writing logs in the log file. Using compressed log record headers improves application performance and reduces the log file's size. With the value set to short:
- A header of the log file or the log file segment contains information about the application (such as the application name, application type, host type, and time zone), whereas single log records within the file or segment omit this information.
- A log message priority is abbreviated to Std, Int, Trc, or Dbg, for Standard, Interaction, Trace, or Debug messages, respectively.
- The message ID does not contain the prefix GCTI or the application type ID.
  A log record in the full format looks like this:
  2002-05-07T18:11:38.196 Standard localhost cfg_dbserver GCTI-00-05060 Application started
  A log record in the short format looks like this:
  2002-05-07T18:15:33.952 Std 05060 Application started

messagefile

Default Value:
Valid Values: [string].lms (message file name)
Changes Take Effect: Immediately, if an application cannot find its *.lms file at startup

Specifies the file name for application-specific log events. The name must be valid for the operating system on which the application is running. The option value can also contain the absolute path to the application-specific *.lms file. Otherwise, an application looks for the file in its working directory.

print-attributes

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

Specifies whether the application attaches extended attributes, if any exist, to a log event that it sends to log output. Typically, log events of the Interaction log level and Audit-related log events contain extended attributes. Setting this option to true enables audit capabilities, but negatively affects performance. Genesys recommends enabling this option for Solution Control Server and Configuration Server when using audit tracking. For other applications, refer to Genesys 7.5 Combined Log Events Help to find out whether an application generates Interaction-level and Audit-related log events; if it does, enable the option only when testing new interaction scenarios.

- **true** Attaches extended attributes, if any exist, to a log event sent to log output.
- **false** Does not attach extended attributes to a log event sent to log output.

segment

Default Value: 10000

Valid Values:

- **false** No segmentation is allowed.

- **[number] KB or [number]** Sets the maximum segment size, in kilobytes. The minimum segment size is 100 KB.
- **[number] MB** Sets the maximum segment size, in megabytes.
- **[number] hr** Sets the number of hours for the segment to stay open. The minimum number is 1 hour.
  Changes Take Effect: immediately
  Specifies whether there is a segmentation limit for a log file. If there is, sets the mode of measurement, along with the maximum size. If the current log segment exceeds the size set by this option, the file is closed and a new one is created.

spool

Default Value:
Valid Values: [path] (the folder, with the full path to it)
Changes Take Effect: immediately

Specifies the folder, including full path to it, in which an application creates temporary files related to network log output. If you change the option value while the application is running, the change does not affect the currently open network output.

standard

Default Value: ../logs/UCMConnector

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends the log events of the Standard level. The log output types must be separated by a comma when more than one output is configured.

time_convert

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

Specifies the system in which an application calculates the log record time when generating a log file. The time is converted from the time in seconds since the Epoch (00:00:00 UTC, January 1, 1970).

- **Local Time (local)** The time of log record generation is expressed as a local time, based on the time zone and any seasonal adjustments. Time zone information of the application's host computer is used.

- **Coordinated Universal Time (utc)** The time of log record generation is expressed as Coordinated Universal Time (UTC).

time_format

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

Specifies how to represent, in a log file, the time when an application generates log records.
A log record's time field in the ISO 8601 format looks like this:
2001-07-24T04:58:10.123

- **HH:MM:SS.sss (time)** The time string is formatted according to the HH:MM:SS.sss (hours, minutes, seconds, and milliseconds) format.
- **According to the system's locale (locale)** The time string is formatted according to the system's locale.
- **ISO 8601 format (ISO8601)** The date in the time string is formatted according to the ISO 8601 format. Fractional seconds are given in milliseconds.

trace

Default Value: ../logs/UCMConnector

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends the log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels). The log outputs must be separated by a comma when more than one output is configured.

verbose

Default Value: standard

Valid Values:

- **all** All log events (that is, log events of the Standard, Trace,Interaction, and Debug levels) are generated.
- **debug** The same as all.

- **trace** Log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels) are generated, but log events of the Debug level are not generated.
- **interaction** Log events of the Interaction level and higher (that is, log events of the Standard and Interaction levels) are generated, but log events of the Trace and Debug levels are not generated.
- **standard** Log events of the Standard level are generated, but log events of the Interaction, Trace, and Debug levels are not generated.
- **none** No output is produced.
  Changes Take Effect: immediately
  Determines whether a log output is created. If it is, specifies the minimum level of log events generated. The log events levels, starting with the highest priority level, are Standard, Interaction, Trace, and Debug.

sip Section

localuser

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

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

mtusize

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

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

tcp.portrange

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

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

tls.portrange

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

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

transport.0

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

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

where transport_name is any string; type is udp/tcp/tls; ip is the IP address of the network interface that accepts incoming SIP messages; 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, 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

Default Value: transport1 tcp:any:5080
Valid Values:

Changes Take Effect: At start/restart

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

where transport_name is any string; type is udp/tcp/tls; ip is the IP address of the network interface that accepts incoming SIP messages; 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, 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

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

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

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

Default Value: 5
Valid Values: Any integer in the range 1-32
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: Any integer in the range 1-600
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.staticroutelist

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

Specifies a list of static routes. Each route group is separated by |. Each static route group is a list of IP addresses separated by comma. Within the route group, each IP address could substitute each other as an alternate route destination if sending a SIP request to one of the IP address fails. For example, 10.0.0.1,10.0.0.2|10.0.10.1,10.0.10.2 specified two static route groups, and each group specified two routes that are alternative to each other. Default value is an empty list.

TServer Section

- smloc
- TServerAddress
- TSvrConnectionRetryCount
- UCMCClientPortRange

smloc

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

UCMC loc

TServerAddress

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

IP Address and port information of the Cisco T-Server.(Eg: 10.10.10.10:5060)

TSvrConnectionRetryCount

Default Value: 10
Valid Values:
Changes Take Effect: After restart

This paramter describes that on connection loss, how many times UCM-C should retry the connection to T-Server before it goes to sleep for configured time

UCMCClientPortRange

Default Value:
Valid Values:

Changes Take Effect: After restart

The local client side TCP port range to be used for CP4SM transport with CISCO T-Server. If this parameter is not specified, UCMC will let the OS choose the local port. The port range MUST BE within the range of 1030-65535. Eg: 1050-1070

UCMC Section

fips_enabled

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

This specifies whether to enable FIPS mode in UCMC. When FIPS mode is enabled, only FIPS 140-2 approved ciphers and algorithms can be used in SSL connections.

NotifyGMSDTMF

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

This parameter specfies whether to enable the DTMF collection from GMS and notify it to CUCM TServer.

RMAddress

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

IP Address and port information of the Resource Manager.(Eg: 10.10.10.10:5060)

UseSecureSIP

Default Value: false

Valid Values:
Changes Take Effect: After restart

This parameter specifies whether to use SIP over TLS instead of SIP. If this parameter is set to true, the RMAddress parameter name may need to be changed to point to the SIPS port of RM

PSTN Connector

Options for this component are contained in the following configuration sections:

- DialogicManager
- DialogicManager_CPD
- DialogicManager_Route1
- ems
- GatewayManager
- log
- MediaManager
- PSTNConnector
- TalkerManager
- TalkerManager_Route1

> ## Tip
> In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.
>
> **Power users: Download a CSV file** containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
DialogicManager	CheckFirmwareStateBeforeMediaOps	True	After restart
DialogicManager	CpaFailTimeMsec	4000	After restart
DialogicManager	CpaMaxInterRingMsec	8000	After restart
DialogicManager	CpaMinRingMsec	1900	After restart
DialogicManager	CpaOption	0	After restart
DialogicManager	CpaPamdOption	2	After restart
DialogicManager	CpaQualTemplates	0	After restart
DialogicManager	CpaStartDelayMsec	250	After restart
DialogicManager	DefaultDNIS	NoDNIS	After restart
DialogicManager	DisableCustomTones	0	After restart
DialogicManager	MinDownLoadSize	32768	After restart
DialogicManager	RingbackFile		After restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
DialogicManager	TMgrVoxIndexFile	TMGRVOXI.VAP	After restart
DialogicManager	TMgrVoxIndexFileAlaw	TMGRVOXI_ALAW.VAP	After restart
DialogicManager_CPD	BackupTServerAddress		After restart
DialogicManager_CPD	BackupTServerPort	0	After restart
DialogicManager_CPD	CPDCallsByTServer	0	After restart
DialogicManager_CPD	CPDFAX2AsAM	0	After restart
DialogicManager_CPD	CPDOffHookDelayMsec	100	After restart
DialogicManager_CPD	CPDPostConnectPriority	TServer	After restart
DialogicManager_CPD	CPDPreConnectPriority	TServer	After restart
DialogicManager_CPD	CPDTServerCallClear	0	After restart
DialogicManager_CPD	CPDTServerConnTimeoutMsec	20000	After restart
DialogicManager_CPD	CPDWaitOffHook	0	After restart
DialogicManager_CPD	PrimaryTServerAddress		After restart
DialogicManager_CPD	PrimaryTServerPort	0	After restart
DialogicManager_Route1	CPDBasedDial	0	After restart
DialogicManager_Route1	Describe	Inbound Route	After restart
DialogicManager_Route1	DialPrefix	1	After restart
DialogicManager_Route1	DirNumbers		After restart
DialogicManager_Route1	IsdnNumberingPlan	0x01	After restart
DialogicManager_Route1	IsdnNumberingType	0x02	After restart
DialogicManager_Route1	IsdnTableFile		After restart
DialogicManager_Route1	MaxDialDigits	7	After restart
DialogicManager_Route1	MediaVoxResourceBoard	0	After restart
DialogicManager_Route1	NetType	0	After restart
DialogicManager_Route1	NewCallConfirmationType	0	After restart
DialogicManager_Route1	OverlapRcvAniDnisLen	0	After restart
DialogicManager_Route1	OverlapReceiveEnabled	0	After restart
DialogicManager_Route1	Ports		After restart
DialogicManager_Route1	Signaling		After restart
DialogicManager_Route1	T1rbAniDnisDelim	•	After restart
DialogicManager_Route1	T1rbAniDnisOrder	1	After restart
DialogicManager_Route1	T1rbProtocolFile	pdk_dmv	After restart
DialogicManager_Route1	T1rbRemoveAniDnisDelim	1	After restart
DialogicManager_Route1	TBCTType		After restart
DialogicManager_Route1	Type		After restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
ems	logconfig.MFSINK •	|*|*	immediately
ems	logconfig.TRAPSINK •	|*|*	At start/restart
GatewayManager	LocalSIPPort	5170	After restart
GatewayManager	SessionTimerSE	1800	After restart
GatewayManager	SessionTimerSupport	true	After restart
GatewayManager	TNZXferPrehangupWaitTime	4000	After restart
GatewayManager	UserAgentAddr		After restart
GatewayManager	UserAgentPort		After restart
log	all	../logs/PSTNConnector	immediately
log	debug	../logs/PSTNConnector	immediately
log	expire	7 day	immediately
log	interaction	../logs/PSTNConnector	immediately
log	segment	10000	immediately
log	standard	../logs/PSTNConnector	immediately
log	time_convert	local	immediately
log	trace	../logs/PSTNConnector	immediately
log	verbose	standard	immediately
MediaManager	DTMFSinglePacket	true	After restart
MediaManager	rtpdejitterdelay	0	At start/restart
MediaManager	RtpDTMFPayloadType	101	After restart
MediaManager	RtpLocalCodecType		After restart
MediaManager	rtprecvaudiobuffersize	0	At start/restart
PSTNConnector	BoardType	DialogicManager	After restart
TalkerManager	AckMsgFax	0	After restart
TalkerManager	AckMsgTDD	0	After restart
TalkerManager	EnableTDD	0	After restart
TalkerManager	HangUpAfterBlindXfer	1	After restart
TalkerManager	MinDownLoadSize	8192	After restart
TalkerManager	RetryAllocResource	0	After restart
TalkerManager	TimeReconfigMFCMsec	0	After restart
TalkerManager	WaitAnswer2DTMF	1	After restart
TalkerManager	WaitFreeStatusDialOutMsec	0	After restart
TalkerManager_Route1	Describe	Inbound Route	After restart
Section	**Option**	**Default**	**Changes Take Effect**

log Section

- all
- debug
- expire
- interaction
- segment
- standard
- time_convert
- trace
- verbose

all

Default Value: ../logs/PSTNConnector

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
Changes Take Effect: immediately
Specifies the outputs to which an application sends all log events. The log output types must be separated by a comma when more than one output is configured.

debug

Default Value: ../logs/PSTNConnector

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.

- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
Changes Take Effect: immediately
Specifies the outputs to which an application sends the log events of the Debug level and higher (that is, log events of the Standard, Interaction, Trace, and Debug levels). The log output types must be separated by a comma when more than one output is configured.

expire

Default Value: 7 day

Valid Values:

- **false** No expiration; all generated segments are stored.
- **[number] file or [number]** Sets the maximum number of log files to store. Specify a number from 1-100.
- **[number] day** Sets the maximum number of days before log files are deleted. Specify a number from 1-100.
Changes Take Effect: immediately
Determines whether log files expire. If they do, sets the measurement for determining when they expire, along with the maximum number of files (segments) or days before the files are removed.

interaction

Default Value: ../logs/PSTNConnector

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
Changes Take Effect: immediately
Specifies the outputs to which an application sends the log events of the Interaction level and higher (that is, log events of the Standard and Interaction levels). The log outputs must be separated by a comma when more than one output is configured.

segment

Default Value: 10000

Valid Values:

- **false** No segmentation is allowed.
- **[number] KB or [number]** Sets the maximum segment size, in kilobytes. The minimum segment size is 100 KB.
- **[number] MB** Sets the maximum segment size, in megabytes.
- **[number] hr** Sets the number of hours for the segment to stay open. The minimum number is 1 hour.
Changes Take Effect: immediately
Specifies whether there is a segmentation limit for a log file. If there is, sets the mode of measurement, along with the maximum size. If the current log segment exceeds the size set by this option, the file is closed and a new one is created.

standard

Default Value: ../logs/PSTNConnector

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
Changes Take Effect: immediately
Specifies the outputs to which an application sends the log events of the Standard level. The log output types must be separated by a comma when more than one output is configured.

time_convert

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

Specifies the system in which an application calculates the log record time when generating a log file. The time is converted from the time in seconds since the Epoch (00:00:00 UTC, January 1, 1970).

- **Local Time (local)** The time of log record generation is expressed as a local time, based on the time zone and any seasonal adjustments. Time zone information of the application's host computer is used.
- **Coordinated Universal Time (utc)** The time of log record generation is expressed as Coordinated Universal Time (UTC).

trace

Default Value: ../logs/PSTNConnector

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends the log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels). The log outputs must be separated by a comma when more than one output is configured.

verbose

Default Value: standard

Valid Values:

- **all** All log events (that is, log events of the Standard, Trace,Interaction, and Debug levels) are generated.
- **debug** The same as all.
- **trace** Log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels) are generated, but log events of the Debug level are not generated.
- **interaction** Log events of the Interaction level and higher (that is, log events of the Standard and Interaction levels) are generated, but log events of the Trace and Debug levels are not generated.
- **standard** Log events of the Standard level are generated, but log events of the Interaction, Trace, and Debug levels are not generated.
- **none** No output is produced.
  Changes Take Effect: immediately
  Determines whether a log output is created. If it is, specifies the minimum level of log events generated. The log events levels, starting with the highest priority level, are Standard, Interaction, Trace, and Debug.

ems Section

logconfig.MFSINK

Default Value:

- |*|*

Valid Values: Pipe delimited ranges for log levels, module IDs and specifier IDs. Ranges can be comma separated integers or range of integers or '*'.
Changes Take Effect: immediately

Controls the log messages that are sent to the MF sink. The format is 'levels|moduleIDs|specifierIDs' (repeated if necessary). The values between the pipes can be in the format: 'm-n,o,p' (ie "0-4, 5,6"). The wildcard character '*' can also be used to indicate all valid numbers. Example: '*|*|*' indicates that all log messages should be sent to the sink. Alternatively, '0,1|0-10|*|4|*|*' indicates that CRITICAL(0) and ERROR(1) level messages with module IDs in the range 0-10 will be sent to the sink; and all INFO(4) level messages will be sent as well.

logconfig.TRAPSINK

Default Value:

- |*|*

Valid Values:
Changes Take Effect: At start/restart

Specifies the metrics that are delivered to the SNMP Trap Sink.

TalkerManager_Route1 Section

- Describe

Describe

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

Describes whether the route is Inbound or Outbound

TalkerManager Section

- AckMsgFax
- AckMsgTDD
- EnableTDD
- HangUpAfterBlindXfer
- MinDownLoadSize
- RetryAllocResource
- TimeReconfigMFCMsec
- WaitAnswer2DTMF
- WaitFreeStatusDialOutMsec

AckMsgFax

Default Value: 0
Valid Values:
Changes Take Effect: After restart

Send ACK or NAK responses for each SIP INFO received in Fax operation.

AckMsgTDD

Default Value: 0
Valid Values:
Changes Take Effect: After restart

Send ACK or NAK responses for each SIP INFO received in TDD operation.

EnableTDD

Default Value: 0
Valid Values:
Changes Take Effect: After restart

Calls generated from TDD equipments will be accepted.

HangUpAfterBlindXfer

Default Value: 1
Valid Values:

Changes Take Effect: After restart

Hangup call after blind transfer.

MinDownLoadSize

Default Value: 8192
Valid Values:
Changes Take Effect: After restart

MinDownLoadSize in bytes

RetryAllocResource

Default Value: 0
Valid Values:
Changes Take Effect: After restart

Number of retries for waiting resources (-1==Forever, 0==Skip, 'n'==n_times).

TimeReconfigMFCMsec

Default Value: 0
Valid Values:
Changes Take Effect: After restart

Time Reconfiguration MFC (msec)

WaitAnswer2DTMF

Default Value: 1
Valid Values:
Changes Take Effect: After restart

Wait answer result before dialing DTMF.

WaitFreeStatusDialOutMsec

Default Value: 0
Valid Values:
Changes Take Effect: After restart

Wait time for free status of dialout channel (msec)

DialogicManager_Route1 Section

- CPDBasedDial
- Describe
- DialPrefix
- DirNumbers
- IsdnNumberingPlan
- IsdnNumberingType
- IsdnTableFile
- MaxDialDigits
- MediaVoxResourceBoard
- NetType
- NewCallConfirmationType
- OverlapRcvAniDnisLen
- OverlapReceiveEnabled
- Ports
- Signaling
- T1rbAniDnisDelim
- T1rbAniDnisOrder
- T1rbProtocolFile
- T1rbRemoveAniDnisDelim
- TBCTType
- Type

CPDBasedDial

Default Value: 0
Valid Values:
Changes Take Effect: After restart

Indicates whether to use the Genesys CPD Library for detecting the CPD results. If the value is set to False, then PSTN Connector shall use the Dialogic otherwise uses the Genesys CPD Library.

Describe

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

Describes whether the route is Inbound or Outbound

DialPrefix

Default Value: 1
Valid Values:
Changes Take Effect: After restart

If call is not in the home NPA then platform will prepend this to the number to be dialed. Only used when Network Type=PSTN

DirNumbers

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

DN range for the route. Specify DNs separated by dash or commas. E.g. 101-110,115,120-130. This parameter is applicable in case when Genesys CPD libraray is used for CPA analysis

IsdnNumberingPlan

Default Value: 0x01
Valid Values:
Changes Take Effect: After restart

Used for outbound ISDN routes to determine the encoding of the Calling/Called Party IE Numbering Plan in the outgoing Setup. 0x00 - Unknown (Dialogic UNKNOWN_NUMB_PLAN) 0x01 - ISDN E.164 (Dialogic ISDN_NUMB_PLAN) 0x02 - Telephony E.163 (Dialogic TELEPHONY_NUMB_PLAN) 0x09 - Private (Dialogic PRIVATE_NUMB_PLAN)

IsdnNumberingType

Default Value: 0x02
Valid Values:
Changes Take Effect: After restart

Used for outbound ISDN routes to determine the encoding of the Calling/Called Party IE Numbering Type in the outgoing Setup. 0x00-Unknown (Dialogic EN_BLOC_NUMBER) 0x01-International Number (Dialogic INTL_NUMBER) 0x02-National Number (Dialogic NAT_NUMBER) 0x04-Subscriber Number (Dialogic LOC_NUMBER)

IsdnTableFile

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

Point to URL containing ISDN table data

MaxDialDigits

Default Value: 7
Valid Values:
Changes Take Effect: After restart

Indicates the number of digits that should be dialed out. If Network Type=PSTN, then this value must be 7, 10, or 11. If Network Type=Enterprise, then this can have any value. If value is zero then there is no max. If missing or invalid value is given, then default is 7

MediaVoxResourceBoard

Default Value: 0
Valid Values:
Changes Take Effect: After restart

This parameter is applicable for JCT boards configured for T1/E1-ISDN or E1-CAS. Specifies which board should be used for CSP. If zero value is specified, then this field defaults to the same board as the network port. Any other value indicates the board number to use for CSP resources. For ISDN and E1-CAS JCT boards, a different board must be configured for CSP than the network port. Note: The value should be a single value, not a comma separated list. Routes with this parameter should be on a single board. For example, do not use Ports=1:1-4, 2:3-5.

NetType

Default Value: 0
Valid Values:
Changes Take Effect: After restart

Indicates what type of telephony network the route is connected to. PSTN,0;Enterprise (PBX/ACD),1

NewCallConfirmationType

Default Value: 0
Valid Values:
Changes Take Effect: After restart

This parameter applies to both inbound and outbound call and the value must be set to AfterAnswer when using groundstart protocol, otherwise select the default value BeforeAnswer. For inbound call, when it is set to AfterAnswer, the call is accepted and answered first and then DNIS digits are collected where as in the default case (value is BeforeAnswer), the ANI/DNIS are collected first before answering the call.For outbound call, when it is set to AfterAnswer, the CPA detection is started right after making the call where as in the default case (value is BeforeAnswer), the CPA detection is started after the call is connected.

OverlapRcvAniDnisLen

Default Value: 0
Valid Values:
Changes Take Effect: After restart

Max digits to receive (ANI + DNIS + delimiters) in overlap receive mode

OverlapReceiveEnabled

Default Value: 0
Valid Values:
Changes Take Effect: After restart

Enable overlap receive for ISDN

Ports

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

Indicates the ports for this route. Format is Card:PortRange[,Card:PortRange...]. For example: 1:1-30 or 1:1-15,2:16-30

Signaling

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

Select the Route Signaling type. T1-ISDN (PRI),0;Analog,1;E1-ISDN (PRI),2;T1-RobbedBit,3;E1-CAS,4

T1rbAniDnisDelim

Default Value:

-

Valid Values:
Changes Take Effect: After restart

The character(e.g. * or #) which separates ANI from DNIS in the incoming call data and default value is *

T1rbAniDnisOrder

Default Value: 1
Valid Values:
Changes Take Effect: After restart

Indicates the way ANI/DNIS is given by T1. Ignored if signalling protocol is not T1-RobbedBit.No ANI/DNIS,0;DNIS only,1;DNIS followed by ANI,2;ANI followed by DNIS,3

T1rbProtocolFile

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

Mandatory for T1-RobbedBit signaling. Indicates Dilaogic T1 configuration file to use. Examples: us_mf_loop_io = For loopback testing; us_mf_io = Generic US T1 Robbed Bit

T1rbRemoveAniDnisDelim

Default Value: 1
Valid Values:
Changes Take Effect: After restart

Indicates if ANI/DNIS deliminators should be removed. Ignored if signalling protocol is not T1-RobbedBit

TBCTType

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

Indicates the type of Two Channel Transfer: NortelRLT, ECTexplicit, ECTexplicit_NZ, ECTexplicit_UK, ECTexplicit_AUS

Type

Default Value:

Valid Values:
Changes Take Effect: After restart

Call direction of Route. Inbound - can handle Inbound calls only; Outbound - can handle Outbound calls only; Inbound & Outbound - can handle both Inbound & Outbound calls (It is supported only on ISDN)

DialogicManager_CPD Section

BackupTServerAddress

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

Specifies the IP address of the backup T-Server.

BackupTServerPort

Default Value: 0
Valid Values:
Changes Take Effect: After restart

Specifies the port of the backup T-Server.

CPDCallsByTServer

Default Value: 0
Valid Values:
Changes Take Effect: After restart

If checked, the CPD library will make outbound calls using TServer (not Dialogic).

CPDFAX2AsAM

Default Value: 0
Valid Values:
Changes Take Effect: After restart

Indicates if CPD library should accept FAX2 tone as Answering machine.

CPDOffHookDelayMsec

Default Value: 100
Valid Values:
Changes Take Effect: After restart

This parameter is used only if the parameter CPD Calls Made by TServer is selected.Specifies the off-hook delay in milliseconds. A negative value specifies to go off-hook first, wait for the specified time, and then dial a number. A positive value specifies to dial first, wait for the specified time, and then set the channel off-hook.

CPDPostConnectPriority

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

Indicates if priority should be given to TServer or Dialogic, in case of conflicting CPD results: TServer,Dialogic

CPDPreConnectPriority

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

Decides the priority between T-Server or Dialogic for Pre-connect CPD events

CPDTServerCallClear

Default Value: 0
Valid Values:
Changes Take Effect: After restart

Specifies whether outgoing calls are to be cleared by T-Server.

CPDTServerConnTimeoutMsec

Default Value: 20000
Valid Values:
Changes Take Effect: After restart

Specifies the dialer reconnect timeout for T-Server in milliseconds.

CPDWaitOffHook

Default Value: 0
Valid Values:
Changes Take Effect: After restart

This parameter is used only if the parameter CPD Offhook Delay has a negative value. If this parameter is selected, the CPD library waits for the off-hook confirmation event from T-Server before dialing.

PrimaryTServerAddress

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

Specifies the IP address of the primary T-Server.

PrimaryTServerPort

Default Value: 0
Valid Values:
Changes Take Effect: After restart

Specifies the port number of the primary T-Server.

DialogicManager Section

- CheckFirmwareStateBeforeMediaOps
- CpaFailTimeMsec
- CpaMaxInterRingMsec
- CpaMinRingMsec
- CpaOption
- CpaPamdOption
- CpaQualTemplates
- CpaStartDelayMsec
- DefaultDNIS
- DisableCustomTones
- MinDownLoadSize
- RingbackFile
- TMgrVoxIndexFile
- TMgrVoxIndexFileAlaw

CheckFirmwareStateBeforeMediaOps

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

This parameter will determine whether the dialogic firmware state should be checked before media operations.

CpaFailTimeMsec

Default Value: 4000
Valid Values:
Changes Take Effect: After restart

Maximum time to wait for Answering machine detection. Units in Miliseconds

CpaMaxInterRingMsec

Default Value: 8000
Valid Values:
Changes Take Effect: After restart

Max time to wait between consecutive ringback before deciding connected. Units in 10ms

CpaMinRingMsec

Default Value: 1900
Valid Values:
Changes Take Effect: After restart

Minimum Ring duration for answering machine detection. Units in 10ms

CpaOption

Default Value: 0
Valid Values:
Changes Take Effect: After restart

Choose Customer enabled CPA Parameters

CpaPamdOption

Default Value: 2
Valid Values:
Changes Take Effect: After restart

List of supported Answering Machine detection options

CpaQualTemplates

Default Value: 0
Valid Values:
Changes Take Effect: After restart

Qualification Template for AM Detection

CpaStartDelayMsec

Default Value: 250
Valid Values:
Changes Take Effect: After restart

Time to wait after dialing before starting cadence or frequency or positive voice detection. Units in Miliseconds.

DefaultDNIS

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

This value used in case of behind-the-switch setup when DNIS information is not available and based on this value the TG DN for RM should be configured for SIP in order to route the call to RM

DisableCustomTones

Default Value: 0
Valid Values:
Changes Take Effect: After restart

This parameter will determine whether custom tones will be deleted unconditionally before doing CPA

MinDownLoadSize

Default Value: 32768
Valid Values:
Changes Take Effect: After restart

MinDownLoadSize in bytes

RingbackFile

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

File used to play ringback tone instead of Index File Name. File format is 8Khz PCM and Mu-law or A-law depending on region. The file must contain a single ring with the desired trailing silence.

TMgrVoxIndexFile

Default Value: TMGRVOXI.VAP
Valid Values:
Changes Take Effect: After restart

File used for playing ringback (ulaw format)

TMgrVoxIndexFileAlaw

Default Value: TMGRVOXI_ALAW.VAP
Valid Values:
Changes Take Effect: After restart

File used for playing ringback (alaw format)

GatewayManager Section

LocalSIPPort

Default Value: 5170
Valid Values:
Changes Take Effect: After restart

Specifies local SIP Port Number to be used by PSTN Connector for SIP Communication

SessionTimerSE

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

The time interval in seconds which a call session must be refreshed, otherwise the session expires.

SessionTimerSupport

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

Controls whether Session Timer support is enabled for a call session

TNZXferPrehangupWaitTime

Default Value: 4000
Valid Values:
Changes Take Effect: After restart

Time to wait before hangup after receving the successful response for dialing digits

UserAgentAddr

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

When PSTN Connector receives a TDM call, this is the destination to which it will send the SIP call. Usually this would be the SIP Server IP Address

UserAgentPort

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

The destination Port Number for PSTN Connector on the SIP side. This would be SIP Server Port Number

PSTNConnector Section

BoardType

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

Type of the hardware used by PSTN Connector to interface with the TDM network

MediaManager Section

- DTMFSinglePacket
- rtpdejitterdelay
- RtpDTMFPayloadType
- RtpLocalCodecType
- rtprecvaudiobuffersize

DTMFSinglePacket

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

Specifies whether to send a single RFC2833 packet for every DTMF digit recognized at the Dialogic side. If this is set to false, then PSTNC tries to send 8 packets corresponding to 1280 ticks

rtpdejitterdelay

Default Value: 0
Valid Values: rtpdejitterdelay must be an integer that is greater than or equal to 0 and less than or equal to 10000.
Changes Take Effect: At start/restart

Specifies the total duration (in milliseconds) of RTP packets to buffer for the inter-arrival dejittering purpose. This will translate to an initial delay before the packets are dispatched internally for further processing. 0 disables the inter-arrival jitter removal functionality.

RtpDTMFPayloadType

Default Value: 101
Valid Values:
Changes Take Effect: After restart

The payload/encoding type of DTMF packets 96, 97, 98, 99, 100, etc

RtpLocalCodecType

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

Local Codec number to be used in RTP values are 0 - Mu law, 8 - A law

rtprecvaudiobuffersize

Default Value: 0
Valid Values: rtprecvaudiobuffersize 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

Specifies the buffer size used for the RTP packet reordering feature and audio packets. This optional feature provides support for receiving RTP packets out of order and reordering them before further processing. If enabled, the suggested normal value is 1000. Note that if rtpdejitterdelay is non-zero, and the resulting jitter buffer size to accommodate the delay is greater than the size defined by this configuration, the size will be set to the greater value specified by the rtpdejitterdelay. Setting the buffer size to 0 and rtpdejitterdelay to 0 disables the RTP packet reordering feature for audio. Note that if the selected buffer size is non-zero but too small (say less than 200), the packet may not fit and be dispatched immediately without the re-ordering.

Others

- Policy Server

  The Policy Server implements various call handling and validation policies to ensure that system configuration and usages are within the boundaries defined for the deployment. For example, the PS allows allocation of dialed numbers to be validated across multiple tenants, while respecting tenant security. Note that most GVP deployments no longer require the PS, as the functionality is available in other ways.

  For more information about the Policy Server application, see Policy Server in the *GVP Deployment Guide*. For the Policy Server configuration options, see Policy Server Options in this document.

- **Reporting Plugin for GAX**

  The GVP Reporting Plugin for GAX provides a user interface to the GVP reporting capability. It allows the user to generate call detail reports, operational reports such as resource usage peaks, and service quality reports.

  For the GVP Reporting Plugin for GAX configuration options, see Reporting Plugin for GAX Options in this document.

- Call Control Platform

  The Call Control Platform (CCP) provides a platform that can execute Call Control XML (CCXML) applications. CCXML allows one to define an event-based application for controlling the call flow between a SIP network and a media processing platform. The applications can make use of MCP media services such as conferencing, announcement and VoiceXML dialogs.

  For more information about the Call Control Platform application, see Call Control Platform in the *GVP Deployment Guide*. For the Call Control Platform configuration options, see Call Control Platform Options in this document.

- Supplementary Services Gateway

  The Supplementary Services Gateway (SSG) provides an HTTP-based interface for processing lists of outbound calls. It is intended for use by those who have built their own outbound-calling infrastructure, or who have simple outbound calling needs. For a complete outbound campaign solution, please see the Genesys Outbound Calling solution.

For more information about the Supplementary Services Gateway application, see Supplementary Services Gateway in the *GVP Deployment Guide*. For the Supplementary Services Gateway configuration options, see Supplementary Services Gateway Options in this document.

- **Third Party Call Recorder**

  The RM and MCP provides media handling services in support of integration to third party voice recording systems. Voice media from a call is replicated and forwarded to the third party recording system for actual recording.

  For the Third Party Call Recorder configuration options, see Third Party Call Recorder Options in this document.

Policy Server

Options for this component are contained in the following configuration sections:

- agentx
- https
- https_key
- log
- reporting

Tip

In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.

Power users: Download a CSV file containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
agentx	connection_delay_sec	60	at start/restart
agentx	max_connection_attempt	-1	at start/restart
https	https.certificate.algorithm	SunX509	at start/restart
https	https.client.authentication	none	at start/restart
https	https.connector.type	2	at start/restart
https	https.keystore.path	${user.home}/.keystore	at start/restart
https	https.keystore.type	JKS	at start/restart
https	https.protocol	TLS	at start/restart
https	https.random.algorithm		at start/restart
https	https.security.provider		at start/restart
https	password		at start/restart
https_key	password		at start/restart
log	all		immediately
log	debug	logs/ps.log	immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
log	expire	false	immediately
log	interaction		immediately
log	message_format	full	immediately
log	segment	10MB	immediately
log	standard	stdout	immediately
log	time_format	time	immediately
log	trace		immediately
log	verbose	trace	immediately
reporting	binding.address		at start/restart
reporting	did.max_overlaps	10	at start/restart
reporting	hostname		at start/restart
reporting	password		at start/restart
reporting	port	8090	at start/restart
reporting	protocol	http	at start/restart
reporting	username		at start/restart
Section	**Option**	**Default**	**Changes Take Effect**

agentx Section

- connection_delay_sec
- max_connection_attempt

connection_delay_sec

Default Value: 60
Valid Values: An integer greater than 0
Changes Take Effect: at start/restart

The number of SECONDS to wait between each reconnection attempt to SNMP Master Agent.

max_connection_attempt

Default Value: -1
Valid Values: An integer greater than 0
Changes Take Effect: at start/restart

The maximum connection attempts to be made by the SNMP Subagent to SNMP Master Agent. Value if not set or value lesser than or equal to 0 means no limit on number of attempts.

https Section

- https.certificate.algorithm
- https.client.authentication
- https.connector.type
- https.keystore.path
- https.keystore.type
- https.protocol
- https.random.algorithm
- https.security.provider
- password

https.certificate.algorithm

Default Value: SunX509
Valid Values: Name of HTTPS algorithm
Changes Take Effect: at start/restart

The SSL algorithm used for the configured keystore.

https.client.authentication

Default Value: none

Valid Values:

none
No certificate request, so client-side authentication is disabled.

required
A certificate is requested and the server will require a valid, non-empty certificate response to establish the connection. (Only works for BIO connector type).

preferred
A certificate is requested, but the server will still establish the connection if the certificate response is empty.

Changes Take Effect: at start/restart

HTTPS client authentication requirements.

https.connector.type

Default Value: 2

Valid Values:

NIO
: Non-blocking NIO connector (Refer to Jetty's JavaDoc for class org.mortbay.jetty.security.SslSelectChannelConnector for more information).

BIO
: Blocking BIO connector (Refer to Jetty's JavaDoc for class org.mortbay.jetty.security.SslSocketConnector for more information).

Changes Take Effect: at start/restart

The type of Jetty connector to use

https.keystore.path

Default Value: ${user.home}/.keystore
Valid Values: A directory path
Changes Take Effect: at start/restart

The path to the keystore file, which will be used for all the HTTPS connectors.

https.keystore.type

Default Value: JKS
Valid Values: A HTTPS keystore type
Changes Take Effect: at start/restart

The type of keystore, which defines the file format that the security implementation supports.

https.protocol

Default Value: TLS

Valid Values:

SSL
Supports some version of SSL.

SSLv2
Supports SSL version 2 or higher.

SSLv3
Supports SSL version 3; may support other versions.

TLS
Supports some versions of TLS.

TLSv1
Supports TLS version 1; may support other versions.

Changes Take Effect: at start/restart

The cryptographic protocol to use.

https.random.algorithm

Default Value:
Valid Values: Name of the RNG (Random Number Generator) algorithm
Changes Take Effect: at start/restart

Refer to the JDK JavaDoc for class java.security.SecureRandom for more information.

https.security.provider

Default Value:
Valid Values: Name of Java security provider
Changes Take Effect: at start/restart

Refer to the JDK JavaDoc for class java.security.Provider for more information.

password

Default Value:
Valid Values: A string
Changes Take Effect: at start/restart

The password for the keystore file.

https_key Section

- password

password

Default Value:
Valid Values: A string
Changes Take Effect: at start/restart

The optional key password for the HTTPS configuration.

log Section

- all
- debug
- expire
- interaction
- message_format
- segment
- standard
- time_format
- trace
- verbose

all

Default Value:

Valid Values:

stdout

Log events are sent to the Standard output (stdout).

stderr

Log events are sent to the Standard error output (stderr).

network

Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.

[filename]

Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

Changes Take Effect: immediately

Specifies the outputs to which an application sends all log events. The log output types must be separated by a comma when more than one output is configured.

debug

Default Value: logs/ps.log

Valid Values:
stdout
Log events are sent to the Standard output (stdout).

stderr
Log events are sent to the Standard error output (stderr).

network
Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.

[filename]
Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

Changes Take Effect: immediately

Specifies the outputs to which an application sends the log events of the Debug level and higher (that is, log events of the Standard, Interaction, Trace, and Debug levels). The log output types must be separated by a comma when more than one output is configured.

expire

Default Value: false

Valid Values:
false
No expiration; all generated segments are stored.

[number]
Sets the maximum number of log files to store. Specify a number from 1-100.

Changes Take Effect: immediately

Determines whether log files expire. If they do, sets the measurement for determining when they expire, along with the maximum number of files (segments) or days before the files are removed.

interaction

Default Value:

Valid Values:

stdout
: Log events are sent to the Standard output (stdout).

stderr
: Log events are sent to the Standard error output (stderr).

network
: Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.

[filename]
: Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

Changes Take Effect: immediately

Specifies the outputs to which an application sends the log events of the Interaction level and higher (that is, log events of the Standard and Interaction levels). The log outputs must be separated by a comma when more than one output is configured.

message_format

Default Value: full

Valid Values:

Compressed Headers
: An application uses compressed headers when writing log records in its log file.

A log record in the short format looks like this:
2002-05-07T18:15:33.952 Std 05060 Application started

Complete Headers

An application uses complete headers when writing log records in its log file.
A log record in the full format looks like:
2002-05-07T18:11:38.196 Standard localhost cfg_dbserver GCTI-00-05060 Application started

Changes Take Effect: immediately

Specifies the format of log record headers that an application uses when writing logs in the log file. Using compressed log record headers improves application performance and reduces the log file's size.

segment

Default Value: 10MB

Valid Values:

false

This setting will cause PS to use a segment size of 10MB

[number] KB or [number]

Sets the maximum segment size, in kilobytes.

[number] MB

Sets the maximum segment size, in megabytes.

Changes Take Effect: immediately

Specifies the segmentation limit for a log file. Sets the mode of measurement, along with the maximum size. If the current log segment exceeds the size set by this option, the file is closed and a new one is created.

standard

Default Value: stdout

Valid Values:

stdout
Log events are sent to the Standard output (stdout).

stderr
Log events are sent to the Standard error output (stderr).

network
Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.

[filename]
Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

Changes Take Effect: immediately

Specifies the outputs to which an application sends the log events of the Standard level. The log output types must be separated by a comma when more than one output is configured.

time_format

Default Value: time

Valid Values:
time (HH:MM:SS.sss)
The time string is formatted according to HH:mm:ss.SSS.

locale (dd/MM/yyyy hh:mm:ss aaa)
The time string is formatted according to the system's locale. With format: dd/MM/yyyy hh:mm:ss aaa

ISO8601 (yyyy-MM-dd'T'HH:mm:ss.SSSZ)
The date in the time string is formatted according to the ISO 8601 format: yyyy-MM-dd'T'HH:mm:ss.SSSZ

Changes Take Effect: immediately

Specifies how to represent, in a log file, the time when an application generates log records.

trace

Default Value:

Valid Values:

stdout
: Log events are sent to the Standard output (stdout).

stderr
: Log events are sent to the Standard error output (stderr).

network
: Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.

[filename]
: Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

Changes Take Effect: immediately

Specifies the outputs to which an application sends the log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels). The log outputs must be separated by a comma when more than one output is configured.

verbose

Default Value: trace

Valid Values:

all
: All log events (that is, log events of the Standard, Trace,Interaction, and Debug levels) are generated.

debug
The same as all.

trace
Log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels) are generated, but log events of the Debug level are not generated.

interaction
Interaction level is not mapped and will have the same effect as none.

standard
Log events of the Standard level are generated, but log events of the Interaction, Trace, and Debug levels are not generated.

none
No output is produced.

Changes Take Effect: immediately

Determines whether a log output is created. If it is, specifies the minimum level of log events generated. The log events levels, starting with the highest priority level, are Standard, Interaction, Trace, and Debug.

reporting Section

- binding.address
- did.max_overlaps
- hostname
- password
- port
- protocol
- username

binding.address

Default Value:
Valid Values: An IP address.
Changes Take Effect: at start/restart

The interface IP address that should be used for binding the PS service.

did.max_overlaps

Default Value: 10
Valid Values: An integer greater than 1
Changes Take Effect: at start/restart

The maximum number of overlaps that can be returned from a DID overlap query.

hostname

Default Value:
Valid Values: A hostname or fully qualified domain name.
Changes Take Effect: at start/restart

The hostname that should be used for accessing PS.

password

Default Value:
Valid Values: A string

Changes Take Effect: at start/restart

The password for PS to perform basic HTTP authentication.

port

Default Value: 8090
Valid Values: An integer greater than 0
Changes Take Effect: at start/restart

The port on which the PS receives reporting requests.

protocol

Default Value: http
Valid Values: An integer greater than 0
Changes Take Effect: at start/restart

The type of communication protocol that PS uses to service reporting requests.

username

Default Value:
Valid Values: A string
Changes Take Effect: at start/restart

The username for PS to perform basic HTTP authentication.

Reporting Plugin for GAX

Options for this component are contained in the following configuration sections:

- gvp-rpt

Tip

In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.

Power users: **Download a CSV file** containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
gvp-rpt	chartDisable	false	Immediately
gvp-rpt	httpTimeout	60	After restart
gvp-rpt	lgrResetTime	720	After restart
Section	**Option**	**Default**	**Changes Take Effect**

gvp-rpt Section

- chartDisable
- httpTimeout
- lgrResetTime

chartDisable

Default Value: false
Valid Values: true, false
Changes Take Effect: Immediately

When set to true, chart rendering in OR/Last IVR Action/SQ Call Summary reports will be disabled.

httpTimeout

Default Value: 60
Valid Values: A positive integer.
Changes Take Effect: After restart

The timeout value until a HTTP connection is etablished with a Reporting Server. A value of zero means the timeout is not used.

Timeout in seconds.

lgrResetTime

Default Value: 720
Valid Values: A positive integer.
Changes Take Effect: After restart

When the last good Reporting Server(RS) is a read-only RS, the Plug-in will reset the last good RS to the primary RS after the reset time passes. When the value is set to 0, the last good RS is reset immediately.

The time value is in minutes.

Call Control Platform

Options for this component are contained in the following configuration sections:

- ccpccxml
- ccxmli
- ems
- fm
- log
- mediacontroller
- session
- sip
- snmp

Tip

In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.

Power users: Download a CSV file containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
ccpccxml	defaultmaxage	60	immediately
ccpccxml	defaultmaxstale	0	immediately
ccpccxml	default_uri	file://$InstallationRoot$/config/default.ccxml	immediately
ccpccxml	fips_enabled	false	At start/restart
ccpccxml	shutdown_grace_period	7200	immediately
ccpccxml	sip.send_progressing	0	immediately
ccxmli	basichttp.recv.accessuri	ipv4	immediately
ccxmli	basichttp.recv.host		immediately
ccxmli	basichttp.recv.host.ipv6		immediately
ccxmli	basichttp.recv.path	/ccxml/basichttp	immediately
ccxmli	basichttp.recv.port	4892	immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
ccxmli	basichttp.recv.show_error_body	false	immediately
ccxmli	basichttp.send.timeout	15000	immediately
ccxmli	createsession.recv.accessuri	ipv4	immediately
ccxmli	createsession.recv.host		immediately
ccxmli	createsession.recv.host.ipv6		immediately
ccxmli	createsession.recv.path	/ccxml/createsession	immediately
ccxmli	createsession.recv.port	4892	immediately
ccxmli	createsession.recv.show_error_body	false	immediately
ccxmli	debug_data.dir	$InstallationRoot$/debugdata	immediately
ccxmli	debug_data.dir_levels	0	immediately
ccxmli	debug_data.file_levels	0	immediately
ccxmli	default_caller_id	sip:ccxml@localhost	immediately
ccxmli	fetch.timeout	30	immediately
ccxmli	inactive_session_kill_timeout	7200	immediately
ccxmli	kill_by_other	true	immediately
ccxmli	max_conf_per_session	100	immediately
ccxmli	max_conn_per_session	100	immediately
ccxmli	max_dialog_per_session	100	immediately
ccxmli	max_internal_loop_count	200	immediately
ccxmli	max_num_documents	6000	immediately
ccxmli	max_num_sessions	6000	immediately
ccxmli	num_session_processing_threads	5	immediately
ccxmli	platform.save_ccxml_files	false	immediately
ccxmli	platform.save_script_files	false	immediately
ccxmli	ssl	false	At start/restart
ccxmli	ssl.recv.cert_file		At start/restart
ccxmli	ssl.recv.password		At start/restart
ccxmli	ssl.recv.private_key_file		At start/restart
ccxmli	ssl.recv.protocol_type	TLSv1	At start/restart
ccxmli	trace_flag	true	immediately
ems	dc.default.logfilter	0-2|*|*	At start/restart
ems	dc.default.metricsfilter	1001,1009,1012-1013,1031,1050-1052,1058-1059	At start/restart
ems	logconfig.DATAC	0-2|*|*	immediately
ems	logconfig.MFSINK	• |*|*	immediately
ems	metricsconfig.DATAC	•	immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
ems	metricsconfig.MFSINK	1000-1001,1003-1005,1007-1016,1019-1021,1024,1027-1036,103	Immediately
ems	ors.reportinginterval	60	At start/restart
ems	rc.amq_connection_send_timeout	60	At start/restart
ems	rc.batch_size	500	At start/restart
ems	rc.cdr.batch_size	500	At start/restart
ems	rc.cdr.local_queue_max	1000000	At start/restart
ems	rc.cdr.local_queue_path	$InstallationRoot$/config/cdrQueue_ccp.db	At start/restart
ems	rc.cdr.max_throughput	0	At start/restart
ems	rc.certificate		at start/restart
ems	rc.local_queue_max	5000000	At start/restart
ems	rc.local_queue_path	$InstallationRoot$/config/upstreamQueue_CCP.db	At start/restart
ems	rc.max_throughput	0	At start/restart
ems	rc.ors.local_queue_max	1000000	At start/restart
ems	rc.ors.local_queue_path	$InstallationRoot$/config/orsQueue_ccp.db	At start/restart
fm	cachemaxentrycount	1000	At start/restart
fm	cachemaxentrysize	100000	At start/restart
fm	cachemaxsize	10000000	At start/restart
fm	enable100continue	0	At start/restart
fm	https_proxy		At start/restart
fm	http_proxy	localhost:3128	At start/restart
fm	interface		At start/restart
fm	localfile_maxage	10	At start/restart
fm	maxredirections	5	At start/restart
fm	no_cache_url_substring	cgi-bin,jsp,asp,?	At start/restart
fm	portrange		At start/restart
fm	ssl_ca_info		At start/restart
fm	ssl_ca_path		At start/restart
fm	ssl_cert		At start/restart
fm	ssl_cert_type	PEM	At start/restart
fm	ssl_cipher_list		At start/restart
fm	ssl_key		At start/restart
fm	ssl_key_password		At start/restart
fm	ssl_key_type	PEM	At start/restart
fm	ssl_random_file		At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
fm	ssl_verify_host	0	At start/restart
fm	ssl_verify_peer	0	At start/restart
fm	ssl_version	0	At start/restart
log	all	../logs/ccp	immediately
log	check-point	1	immediately
log	compatible-output-priority	false	immediately
log	debug	../logs/ccp	immediately
log	expire	10	immediately
log	interaction	../logs/ccp	immediately
log	keep-startup-file	true	After restart
log	memory		immediately
log	memory-storage-size		When memory output is created
log	messagefile		Immediately, if an application cannot find its *.lms file at startup
log	message_format	short	immediately
log	print-attributes	false	immediately
log	segment	10000	immediately
log	spool		immediately
log	standard	../logs/ccp_standard	immediately
log	time_convert	local	immediately
log	time_format	ISO8601	immediately
log	trace	../logs/ccp	immediately
log	verbose	interaction	immediately
mediacontroller	allow_dialog_transfer	1	immediately
mediacontroller	bridge_server	$LocalIP$:5060	immediately
mediacontroller	bridge_server.defaultmaxsize	4	immediately
mediacontroller	bridge_server.defaultreserve	4	immediately
mediacontroller	bridge_server.profile	Default Conference	immediately
mediacontroller	bridge_sips_server	$LocalIP$:5061	immediately
mediacontroller	codec_check_exclusion.payloads	13	immediately
mediacontroller	conference.defaultreserve	8	immediately
mediacontroller	defaultrejectcode	480	immediately
mediacontroller	full_audio_codec	0|pcmu|audio/basic|8000|1 8|pcma|audio/x-alaw-basic|8000|1	immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
		9|g722|audio/ g722|8000|1 23|g726-16|audio/ g726-16|8000|1 22|g726-16|audio/ g726-16|8000|1 2|g726-32|audio/ g726|8000|1 125&	
mediacontroller	full_video_codec	34|h263|video/ H263|90000|1 99|h263-1998|video/ H263-1998|90000|1 113|H264|video/ H264|90000|1	immediately
mediacontroller	inbound_allowed_media	dynamic	immediately
mediacontroller	sdp.defaultipversion	true	immediately
mediacontroller	sdp.localhost	$LocalIP$	immediately
mediacontroller	sdp.localhost.ipv6	$LocalIPv6$	immediately
mediacontroller	sip.allowedunknownheaders		immediately
mediacontroller	sipproxy	$LocalIP$:5060	immediately
mediacontroller	sipsecure	0	immediately
mediacontroller	sipsproxy	$LocalIP$:5061	immediately
session	copy_unknown_headers	true	immediately
sip	copyunknownheaders	1	At start/restart
sip	localuser	Genesys	At start/restart
sip	maxtcpconnections	100	At start/restart
sip	maxtlsconnections	100	At start/restart
sip	min_se	90	At start/restart
sip	mtusize	1500	At start/restart
sip	OPTIONS.header.Accept	application/sdp	immediately
sip	OPTIONS.header.Accept-Encoding		immediately
sip	OPTIONS.header.Accept-Language	en	immediately
sip	OPTIONS.header.Allow	INVITE,ACK,CANCEL,BYE,OPTIONS,INFO	immediately
sip	OPTIONS.header.Supported		immediately
sip	prack.support	0	At start/restart
sip	preferred_ipversion	ipv4	At start/restart
sip	registerexpiryadjustment	10	At start/restart
sip	route.default.tcp		At start/restart
sip	route.default.tcp.ipv6		At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
sip	route.default.tls		At start/restart
sip	route.default.tls.ipv6		At start/restart
sip	route.default.udp		At start/restart
sip	route.default.udp.ipv6		At start/restart
sip	route.dest.0		At start/restart
sip	route.dest.1		At start/restart
sip	route.dest.2		At start/restart
sip	route.dest.3		At start/restart
sip	route.dest.4		At start/restart
sip	route.dest.5		At start/restart
sip	routeset		At start/restart
sip	securerouteset		At start/restart
sip	sessionexpires	1800	At start/restart
sip	tcp.portrange		At start/restart
sip	threadpoolsize	4	At start/restart
sip	threads	0	After restart
sip	timer.ci_proceeding	120000	At start/restart
sip	tls.portrange		At start/restart
sip	transport.0	transport0 udp:any:5068	At start/restart
sip	transport.0.tos	0	At start/restart
sip	transport.1	transport1 tcp:any:5068	At start/restart
sip	transport.1.tos	0	At start/restart
sip	transport.2	transport2 tls:any:5069 cert=$InstallationRoot$/config/x509_certificate.pem key=$InstallationRoot$/config/x509_private_key.pem	At start/restart
sip	transport.2.tos	0	At start/restart
sip	transport.3		At start/restart
sip	transport.3.tos	0	At start/restart
sip	transport.4		At start/restart
sip	transport.4.tos	0	At start/restart
sip	transport.5		At start/restart
sip	transport.5.tos	0	At start/restart
sip	transport.dnsharouting	false	At start/restart
sip	transport.localaddress		At start/restart
sip	transport.localaddress.srv	false	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
sip	transport.localaddress_ipv6		At start/restart
sip	transport.staticroutelist		At start/restart
snmp	timeout	100	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

ccpccxml Section

- default_uri
- defaultmaxage
- defaultmaxstale
- fips_enabled
- shutdown_grace_period
- sip.send_progressing

default_uri

Default Value: file://$InstallationRoot$/config/default.ccxml
Valid Values:
Changes Take Effect: immediately

Specifies the URI for the default CCXML application

defaultmaxage

Default Value: 60
Valid Values: From 30 to 180 inclusive (in seconds)
Changes Take Effect: immediately

Default Maxage for fetching an initial CCXML page

defaultmaxstale

Default Value: 0
Valid Values: From 0 to 180 inclusive (in seconds)
Changes Take Effect: immediately

Default Maxstale for fetching an initial CCXML page

fips_enabled

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

Specifies whether to enable FIPS mode in CCP. When FIPS mode is enabled, only FIPS 140-2 approved ciphers and algorithms can be used in SSL connections.

shutdown_grace_period

Default Value: 7200
Valid Values: From 0 to 65535 inclusive (in seconds)
Changes Take Effect: immediately

The amount of time (in seconds) sessions are given to terminate after Graceful Stop is selected. Once this grace period is exceeded, sessions are killed by ccxml.kill.unconditional events.

sip.send_progressing

Default Value: 0
Valid Values: 1, 0
Changes Take Effect: immediately

Determines whether 180 SIP response is sent on <accept> tag for all incoming calls.
0 - 180 response is sent when <send> is called
1 - 180 response is sent immediately after sending 100 Trying

ccxmli Section

basichttp.recv.accessuri

Default Value: ipv4
Valid Values: ipv4, ipv6
Changes Take Effect: immediately

Preferred IP version to be used in basichttp access uri "session.ioprocessors["basichttp"]". Valid values are "ipv4" and "ipv6".

basichttp.recv.host

Default Value:
Valid Values:
Changes Take Effect: immediately

The IPv4 address or hostname on which the Basic HTTP Event I/O Processor will be listening for HTTP requests on IPv4 network interface. If the value is an empty string, the system listen on all available IPv4 network interface. If hostname is specified, the first IPv4 address in the resolved list will be used.

Note: Genesys recommends setting the same value on 'ccxmli.createsession.recv.host'.

basichttp.recv.host.ipv6

Default Value:
Valid Values:
Changes Take Effect: immediately

The IPv6 address or hostname on which the Basic HTTP Event I/O Processor will be listening for HTTP requests on IPv6 network interface. If the value is an empty string, the system listen on all available IPv6 network interface. If hostname is specified, the first IPv6 address in the resolved list will be used.

basichttp.recv.path

Default Value: /ccxml/basichttp
Valid Values:
Changes Take Effect: immediately

The access path for the Basic HTTP Event I/O Processor.

basichttp.recv.port

Default Value: 4892
Valid Values:
Changes Take Effect: immediately

The port on which the Basic HTTP Event I/O Processor will be listening for HTTP requests.

basichttp.recv.show_error_body

Default Value: false
Valid Values: true, false
Changes Take Effect: immediately

When set to TRUE, a descriptive text will be returned in the response body when an HTTP failure response is given for a request to the Basic HTTP Event I/O Processor.

basichttp.send.timeout

Default Value: 15000
Valid Values:
Changes Take Effect: immediately

The HTTP response timeout (in milliseconds) value for an event sent to another platform via HTTP.

createsession.recv.accessuri

Default Value: ipv4
Valid Values: ipv4, ipv6
Changes Take Effect: immediately

Preferred IP version to be used in createsession access uri "session.ioprocessors["createsession"]". Valid values are "ipv4" and "ipv6".

createsession.recv.host

Default Value:
Valid Values:
Changes Take Effect: immediately

The IPv4 address or hostname on which the Session Creation Event I/O Processor will be listening for HTTP requests on IPv4 network interface. If the value is an empty string, the system listen on all available IPv4 network interface. If hostname is specified, the first IPv4 address in the resolved list will be used. Note: Genesys recommends setting the same value on 'ccxmli.basichttp.recv.host'.

createsession.recv.host.ipv6

Default Value:
Valid Values:
Changes Take Effect: immediately

The IPv6 address or hostname on which the Session Creation Event I/O Processor will be listening for HTTP requests on IPv6 network interface. If the value is an empty string, the system listen on all available IPv6 network interface. If hostname is specified, the first IPv6 address in the resolved list will be used.

createsession.recv.path

Default Value: /ccxml/createsession
Valid Values:
Changes Take Effect: immediately

The access path for the Session Creation Event I/O Processor.

createsession.recv.port

Default Value: 4892
Valid Values: A valid value is an integer from 1025 to 65535 inclusive.
Changes Take Effect: immediately

The port on which the Session Creation Event I/O Processor will be listening for HTTP requests.

createsession.recv.show_error_body

Default Value: false
Valid Values: true, false
Changes Take Effect: immediately

When set to TRUE, a descriptive text will be returned in the response body when an HTTP failure response is given for a request to the Session Creation Event I/O Processor.

debug_data.dir

Default Value: $InstallationRoot$/debugdata
Valid Values:
Changes Take Effect: immediately

Debug Data Directory

debug_data.dir_levels

Default Value: 0
Valid Values:
Changes Take Effect: immediately

The nesting depth of debug data sub-folders. For example, if the session id is "1234" and directory nesting is set to 2, a file called "debug.dat" will be saved as <ccxmli.debug_data.dir>/1/2/1234/debug.dat. When set to 0, no nesting occurs. Directory nesting can be enabled when there's a need to retain debug data for a lot of sessions, to decrease the number of sub-directories each directory will have.

debug_data.file_levels

Default Value: 0
Valid Values:
Changes Take Effect: immediately

The nesting depth of debug data files. For example, if the session id is "1234" and file nesting is set to 2, a file called "debug.dat" will be saved as <ccxmli.debug_data.dir>/1234/d/e/debug.dat. When set to 0, no nesting occurs. File nesting can be enabled when there's a need to retain debug data for a lot of files, to decrease the number of files each directory will have.

default_caller_id

Default Value: sip:ccxml@localhost
Valid Values:
Changes Take Effect: immediately

Default CallerID

fetch.timeout

Default Value: 30
Valid Values:
Changes Take Effect: immediately

The default timeout interval (in seconds) for the initial page fetch completion for new CCXML session to complete.

inactive_session_kill_timeout

Default Value: 7200
Valid Values:
Changes Take Effect: immediately

The amount of time (in seconds) that a session may idle without owning any connections or dialogs and without removing any "external" events from its event queue (An external event is an event that does not have an eventsourcetype of ccxml and an eventsource that is the current session's id). If the limit is reached, then ccxml.kill is sent to the session. If the limit value is not configured or is set to 0, then no limit is placed on the idle time.

kill_by_other

Default Value: true
Valid Values: true, false
Changes Take Effect: immediately

If set to True, allow Process to be killed by external entity.

max_conf_per_session

Default Value: 100
Valid Values: A valid value is an integer from 1 to 100000 inclusive.
Changes Take Effect: immediately

Max Conf per session

max_conn_per_session

Default Value: 100
Valid Values: A valid value is an integer from 1 to 100000 inclusive.
Changes Take Effect: immediately

Max Connections per session

max_dialog_per_session

Default Value: 100
Valid Values: A valid value is an integer from 1 to 100000 inclusive.
Changes Take Effect: immediately

Max dialogs per session

max_internal_loop_count

Default Value: 200
Valid Values:
Changes Take Effect: immediately

The number of times a session iterates through an <eventprocessor> loop without removing an "external" event from its event queue (An external event is an event that does not have an eventsourcetype of ccxml and an eventsource that is the current session's id.) or without the session's event queue being empty after processing an event. If the limit is reached, then ccxml.kill.unconditional is sent to the session. If the limit value is not configured or set to 0 then no limit is placed on the event processing.

max_num_documents

Default Value: 6000
Valid Values: A valid value is an integer from 1 to 100000 inclusive.
Changes Take Effect: immediately

Max number of documents

max_num_sessions

Default Value: 6000
Valid Values: A valid value is an integer from 1 to 100000 inclusive.
Changes Take Effect: immediately

Max number of sessions

num_session_processing_threads

Default Value: 5
Valid Values: A valid value is an integer from 1 to 5 inclusive.
Changes Take Effect: immediately

Numbers of threads per session

platform.save_ccxml_files

Default Value: false
Valid Values: true, false
Changes Take Effect: immediately

When set to True, fetch request/response/data for each fetched CCXML page will be saved.

platform.save_script_files

Default Value: false
Valid Values: true, false
Changes Take Effect: immediately

When set to True, fetch request/response/data for each fetched ECMAScript file will be saved.

ssl

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

Use SSL to receive CreateSession and BasicHTTP requests

ssl.recv.cert_file

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

The path and the filename of the SSL certificate to be used for createsession and BasicHTTP.

ssl.recv.password

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

The password associated with the certificate and key pair. Required only if key file is password protected.

ssl.recv.private_key_file

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

The path and the filename of the SSL key to be used for createsession and BasicHTTP.

ssl.recv.protocol_type

Default Value: TLSv1
Valid Values: TLSv1, SSLv2, SSLv3, SSLv23
Changes Take Effect: At start/restart

- The type of secure transport to be used and valid values are:
- **SSLv2** A TLS/SSL connection established with these methods will only understand the SSLv2 protocol. This server will only understand SSLv2 client hello messages.
- **SSLv3** A TLS/SSL connection established with these methods will only understand the SSLv3 protocol. This server will only understand SSLv3 client hello messages. This especially means, that it will not understand SSLv2 client hello messages which are widely used for compatibility reasons.
- **TLSv1** A TLS/SSL connection established with these methods will only understand the TLSv1 protocol. This server will only understand TLSv1 client hello messages. This especially means, that it will not understand

SSLv2 client hello messages which are widely used for compatibility reasons.

- **SSLv23** A TLS/SSL connection established with these methods will understand the SSLv2, SSLv3, and TLSv1 protocol. This server will understand SSLv2, SSLv3, and TLSv1 client hello messages. This is the best choice when compatibility is a concern.

trace_flag

Default Value: true
Valid Values: true, false
Changes Take Effect: immediately

Trace flag.

ems Section

- dc.default.logfilter
- dc.default.metricsfilter
- logconfig.DATAC
- logconfig.MFSINK
- metricsconfig.DATAC
- metricsconfig.MFSINK
- ors.reportinginterval
- rc.amq_connection_send_timeout
- rc.batch_size
- rc.cdr.batch_size
- rc.cdr.local_queue_max
- rc.cdr.local_queue_path
- rc.cdr.max_throughput
- rc.certificate
- rc.local_queue_max
- rc.local_queue_path
- rc.max_throughput
- rc.ors.local_queue_max
- rc.ors.local_queue_path

dc.default.logfilter

Default Value: 0-2|*|*
Valid Values: Pipe delimited ranges for log levels, module IDs and specifier IDs. Ranges can be comma separated integers or range of integers or '*'.
Changes Take Effect: At start/restart

Specifies the filter for logs to be delivered "upstream" to the Reporting Server for Call Events reporting. The format is 'levels|moduleIDs|specifierIDs' (repeated if necessary). The values between the pipes can be in the format: 'm-n,o,p' (ie "0-4, 5,6"). The wildcard character '*' can also be used to indicate all valid numbers. Example: '*|*|*' indicates that all log messages should be sent to the sink. Alternatively, '0,1|0-10|*|4|*|*' inidcates that CRITICAL(0) and ERROR(1) level messages with module IDs in the range 0-10 wil be sent to the sink; and all INFO(4) level messages will be sent as well.

dc.default.metricsfilter

Default Value: 1001,1009,1012-1013,1031,1050,1052,1058-1059
Valid Values: Comma separated list of metric values or ranges. A metric value must be between 0 and 141 inclusive. The values '*' and blank are also allowed.
Changes Take Effect: At start/restart

Specifies the default filter for metrics to be delivered "upstream" to the Reporting Server for Call Events reporting. '*' indicates that all metrics will be sent to the sink. Alternatively, '5-10,50-55,70,71' indicates that metrics with IDs 5,6,7,8,9,10,50,51,52,53,54,55,70 and 71 will be sent to the MF sink. This filter will be used unless the default has been overridden in the tenant or IVR Application profile to which the given call has been associated.

logconfig.DATAC

Default Value: 0-2|*|*
Valid Values: Pipe delimited ranges for log levels, module IDs and specifier IDs. Ranges can be comma separated integers or range of integers or '*'.
Changes Take Effect: immediately

Controls the log messages that are sent to the MF sink. The format is 'levels|moduleIDs|specifierIDs' (repeated if necessary). The values between the pipes can be in the format: 'm-n,o,p' (ie "0-4, 5,6"). The wildcard character '*' can also be used to indicate all valid numbers. Example: '*|*|*' indicates that all log messages should be sent to the sink. Alternatively, '0,1|0-10|*|4|*|*' inidcates that CRITICAL(0) and ERROR(1) level messages with module IDs in the range 0-10 wil be sent to the sink; and all INFO(4) level messages will be sent as well.

logconfig.MFSINK

Default Value:

- |*|*

Valid Values: Pipe delimited ranges for log levels, module IDs and specifier IDs. Ranges can be comma separated integers or range of integers or '*'.
Changes Take Effect: immediately

Controls the log messages that are sent to the MF sink. The format is 'levels|moduleIDs|specifierIDs' (repeated if necessary). The values between the pipes can be in the format: 'm-n,o,p' (ie "0-4, 5,6"). The wildcard character '*' can also be used to indicate all valid numbers. Example: '*|*|*' indicates that all log messages should be sent to the sink. Alternatively, '0,1|0-10|*|4|*|*' inidcates that CRITICAL(0) and ERROR(1) level messages with module IDs in the range 0-10 wil be sent to the sink; and all INFO(4) level messages will be sent as well.

metricsconfig.DATAC

Default Value:

-

Valid Values: Comma separated list of metric values or ranges. A metric value must be between 0 and 141 inclusive. The values '*' and blank are also allowed.
Changes Take Effect: immediately

Specifies the metrics that are delivered to the Data Collection Sink. '*' indicates that all metrics will be sent to the sink. Alternatively, '5-10,50-55,70,71' indicates that metrics with IDs 5,6,7,8,9,10,50,51,52,53,54,55,70 and 71 will be sent to the MF sink.

metricsconfig.MFSINK

Default Value:
1000-1001,1003-1005,1007-1016,1019-1021,1024,1027-1036,1039-1045,1048-1050,1052-1054,1056,1058-1062
Valid Values: Comma separated list of metric values or ranges. A CCP metric value must be between 1000 and 1063 inclusive. The values '*' and blank are also allowed.
Changes Take Effect: immediately

Specifies the metrics that are delivered to the MF Sink. '*' indicates that all metrics will be sent to the sink. Alternatively, '5-10,50-55,70,71' indicates that metrics with IDs 5,6,7,8,9,10,50,51,52,53,54,55,70 and 71 will be sent to the MF sink.

ors.reportinginterval

Default Value: 60
Valid Values: An integer between 1-299 inclusive.
Changes Take Effect: At start/restart

Interval (seconds) accumulated operational reports are submitted to the Reporting Server

rc.amq_connection_send_timeout

Default Value: 60
Valid Values: An integer greater than or equal to 45.
Changes Take Effect: At start/restart

This option specifies the maximum time in seconds to wait for ActiveMQ Producer Send Message response.

rc.batch_size

Default Value: 500
Valid Values: An integer between 1-5000 inclusive.
Changes Take Effect: At start/restart

The number of upstream messages queued up by the reporting client before sending them up to the reporting server. A higher batch size (e.g. 50 records) will lessen bandwidth constraints, at the cost of making sending data at larger intervals.

rc.cdr.batch_size

Default Value: 500
Valid Values: An integer between 1-5000 inclusive.

Changes Take Effect: At start/restart

The number of CDR messages queued up by the reporting client before sending them up to the reporting server. A higher batch size (e.g. 50 records) will lessen bandwidth constraints, at the cost of making sending CDR data at larger intervals.

rc.cdr.local_queue_max

Default Value: 1000000
Valid Values: An integer greater or equal to -1.
Changes Take Effect: At start/restart

This option specifies the maximum number of data items to the local database for CDR reporting. Queuing to the local database will occur either when the Reporting Server is unavailable, or when data is being provided to the Client faster than the Server can consume it. A value of -1 indicates an "unlimited" number of records will be allowed. A value of 0 indicates that no records will be persisted locally and data will be discarded if the RS is unavailable.

rc.cdr.local_queue_path

Default Value: $InstallationRoot$/config/cdrQueue_ccp.db
Valid Values: Path to the DB file.
Changes Take Effect: At start/restart

The full path of the local database file used to locally persist data for CDRs.

rc.cdr.max_throughput

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

This option specifies the maximum rate at which CDR data, in bytes per second, is sent to the Reporting Server. A value of 0 (default) indicates that CDR data will be sent as quickly as possible.

rc.certificate

Default Value:
Valid Values: File path
Changes Take Effect: at start/restart

The file name of the TLS certificate in "PEM" format. Required to connect to the Reporting Server (ActiveMQ) over TLS.

rc.local_queue_max

Default Value: 5000000
Valid Values: An integer greater or equal to -1.
Changes Take Effect: At start/restart

This option specifies the maximum number of data items to the local database for Upstream Logging. Queuing to the local database will occur either when the Reporting Server is unavailable, or when data is being provided to the Client faster than the Server can consume it. A value of -1 indicates an "unlimited" number of records will be allowed. A value of 0 indicates that no records will be persisted locally and data will be discarded if the RS is unavailable.

rc.local_queue_path

Default Value: $InstallationRoot$/config/upstreamQueue_CCP.db
Valid Values: Path to the DB file.
Changes Take Effect: At start/restart

The full path of the local database file used to locally persist data for upstream logging to the GVP Reporting Client.

rc.max_throughput

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

This option specifies the maximum rate at which Upstream Logging data, in bytes per second, is sent to the Reporting Server. A value of 0 (default) indicates that Upstream Logging data will be sent as quickly as possible.

rc.ors.local_queue_max

Default Value: 1000000
Valid Values: An integer greater or equal to -1.
Changes Take Effect: At start/restart

This option specifies the maximum number of data items to the local database for Operational Reporting. Queuing to the local database will occur either when the Reporting Server is unavailable, or when data is being provided to the Client fdaster than the Server can consume it. A value of -1 indicates an "unlimited" number of records will be allowed. A value of 0 indicates that no records will be persisted locally and data will be discarded if the RS is unavailable.

rc.ors.local_queue_path

Default Value: $InstallationRoot$/config/orsQueue_ccp.db
Valid Values: Path to the DB file.
Changes Take Effect: At start/restart

The full path of the local database file used to locally persist data for Operational Reporting.

fm Section

- cachemaxentrycount
- cachemaxentrysize
- cachemaxsize
- enable100continue
- http_proxy
- https_proxy
- interface
- localfile_maxage
- maxredirections
- no_cache_url_substring
- portrange
- ssl_ca_info
- ssl_ca_path
- ssl_cert
- ssl_cert_type
- ssl_cipher_list
- ssl_key
- ssl_key_password
- ssl_key_type
- ssl_random_file
- ssl_verify_host
- ssl_verify_peer
- ssl_version

cachemaxentrycount

Default Value: 1000
Valid Values: Must be an integer greater than or equal to 0.
Changes Take Effect: At start/restart

The maximum number of cache entries that can be stored in the cache.

cachemaxentrysize

Default Value: 100000
Valid Values: Must be an integer greater than or equal to 0.
Changes Take Effect: At start/restart

The maximum size of each cache entry in bytes.

cachemaxsize

Default Value: 10000000
Valid Values: Must be an integer greater than or equal to 0.
Changes Take Effect: At start/restart

The maximum total size of the cache in bytes.

enable100continue

Default Value: 0
Valid Values:
Changes Take Effect: At start/restart

Enable or disable the "Expect: 100-continue" header in HTTP 1.1 requests.

http_proxy

Default Value: localhost:3128
Valid Values:
Changes Take Effect: At start/restart

The HTTP proxy to be used for HTTP requests.

https_proxy

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

The HTTPS proxy to be used for HTTPS requests.

interface

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

This sets the network interface IP address to be used for outgoing HTTP requests. If this parameter is empty, it will automatically select the network interface to be used. If the Squid HTTP proxy is used, it has to be configured to accept HTTP requests from the interface specified. Otherwise, Squid by default would only accept HTTP requests from the localhost.

localfile_maxage

Default Value: 10
Valid Values:

Changes Take Effect: At start/restart

Maxage for cached local file in seconds. Caching of local file can be turned off by setting this to 0.

maxredirections

Default Value: 5
Valid Values: Must be an integer greater than or equal to 0, and less than 99.
Changes Take Effect: At start/restart

The maximum number of times to follow the Location: header in the HTTP response. Set to 0 to disable HTTP redirection.

no_cache_url_substring

Default Value: cgi-bin,jsp,asp,?
Valid Values:
Changes Take Effect: At start/restart

If a URL contains any one of the sub-strings in this comma-delimited list, it will not be cached.

portrange

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

The local port range to be used for HTTP requests. If this parameter is not specified, CCP will let the OS choose the local port.

ssl_ca_info

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

The file name holding one or more certificates to verify the peer with.

ssl_ca_path

Default Value:

Valid Values:
Changes Take Effect: At start/restart

The path holding multiple CA certificates to verify the peer with. The certificate directory must be prepared using the openssl c_rehash utility.

ssl_cert

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

The file name of your certificate. The default format is "PEM" and can be changed with the configuration parameter ssl_cert_type

ssl_cert_type

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

The format of the certificate.

ssl_cipher_list

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

The list of ciphers to use for the SSL connection. The list must be syntactically correct, it consists of one or more cipher strings separated by colons. Commas or spaces are also acceptable separators but colons are normally used, , - and + can be used as operators. Valid examples of cipher lists include 'RC4-SHA', 'SHA1+DES', 'TLSv1' and 'DEFAULT'. More details about cipher lists can be found on this URL: http://www.openssl.org/docs/apps/ciphers.html.

ssl_key

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

The file name of the private key. The default format for the key is "PEM" and may be changed by the parameter ssl_key_type.

ssl_key_password

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

The password required to use the ssl_key.

ssl_key_type

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

The format of the private key.

ssl_random_file

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

The path to a file which is read from to seed the random engine for SSL.

ssl_verify_host

Default Value: 0
Valid Values:
Changes Take Effect: At start/restart

Specifies how the Common name from the peer certificate should be verified during the SSL handshake

ssl_verify_peer

Default Value: 0
Valid Values:
Changes Take Effect: At start/restart

Whether or not to verify the peer's certificate. When this option is set, one of ssl_ca_info or ssl_ca_path should be set.

ssl_version

Default Value: 0
Valid Values:
Changes Take Effect: At start/restart

Set what version of SSL to attempt to use. By default, the SSL library will automatically detect the correct version. This parameter can be used to override this automatic detection, for situations where the wrong version is chosen.

log Section

- all
- check-point
- compatible-output-priority
- debug
- expire
- interaction
- keep-startup-file
- memory
- memory-storage-size
- message_format
- messagefile
- print-attributes
- segment
- spool
- standard
- time_convert
- time_format
- trace
- verbose

all

Default Value: ../logs/ccp

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application’s working directory.
Changes Take Effect: immediately
Specifies the outputs to which an application sends all log events. The log output types must be separated by a comma when more than one output is configured.

check-point

Default Value: 1
Valid Values: 0 - 24
Changes Take Effect: immediately

Specifies, in hours, how often the application generates a check point log event, to divide the log into sections of equal time. By

default, the application generates this log event every hour. Setting the option to 0 prevents the generation of check-point events.

compatible-output-priority

Default Value: false

Valid Values:

- **true** The log of the level specified by "Log Output Options" is sent to the specified output.
- **false** The log of the level specified by "Log Output Options" and higher levels is sent to the specified output.
Changes Take Effect: immediately
Specifies whether the application uses 6.x output logic.

debug

Default Value: ../logs/ccp

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
Changes Take Effect: immediately
Specifies the outputs to which an application sends the log events of the Debug level and higher (that is, log events of the Standard, Interaction, Trace, and Debug levels). The log output types must be separated by a comma when more than one output is configured.

expire

Default Value: 10

Valid Values:

- **false** No expiration; all generated segments are stored.
- **[number] file or [number]** Sets the maximum number of log files to store. Specify a number from 1-100.
- **[number] day** Sets the maximum number of days before log files are deleted. Specify a number from 1-100.
Changes Take Effect: immediately
Determines whether log files expire. If they do, sets the measurement for determining when they expire, along with the maximum number of files (segments) or days before the files are removed.

interaction

Default Value: ../logs/ccp

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
Changes Take Effect: immediately
Specifies the outputs to which an application sends the log events of the Debug level and higher (that is, log events of the Standard, Interaction, Trace, and Debug levels). The log output types must be separated by a comma when more than one output is configured.

keep-startup-file

Default Value: true

Valid Values:

- **false** No startup segment of the log is kept.
- **true** A startup segment of the log is kept. The size of the segment equals the value of the segment option.
- **[number] KB** Sets the maximum size, in kilobytes, for a startup segment of the log.
- **[number] MB** Sets the maximum size, in megabytes, for a startup segment of the log.
Changes Take Effect: After restart
Specifies whether a startup segment of the log, containing the initial configuration, is to be kept. If it is, this option can be set to true or to a specific size. If set to true, the size of the initial segment will be equal to the size of the regular log segment defined by the segment option. The value of this option will be ignored if segmentation is turned off (that is, if the segment option set to false).

memory

Default Value:
Valid Values: [string] (memory file name)
Changes Take Effect: immediately

Specifies the name of the file to which the application regularly prints a snapshot of the memory output, if it is configured to do this. The new snapshot overwrites the previously written data. If the application terminates abnormally, this file will contain the latest log messages. Memory output is not recommended for processors with a CPU frequency lower than 600 MHz.

memory-storage-size

Default Value:

Valid Values:

- **[number] KB or [number]** The size of the memory output, in kilobytes. The minimum value is 128 KB.
- **[number] MB** The size of the memory output, in megabytes. The maximum value is 64 MB
  Changes Take Effect: When memory output is created
  Specifies the buffer size for log output to the memory, if configured.

message_format

Default Value: short

Valid Values:

- **short** An application uses compressed headers when writing log records in its log file.
- **full** An application uses complete headers when writing log records in its log file.
  Changes Take Effect: immediately
  Specifies the format of log record headers that an application uses when writing logs in the log file. Using compressed log record headers improves application performance and reduces the log file's size. With the value set to short:
- A header of the log file or the log file segment contains information about the application (such as the application name, application type, host type, and time zone), whereas single log records within the file or segment omit this information.
- A log message priority is abbreviated to Std, Int, Trc, or Dbg, for Standard, Interaction, Trace, or Debug messages, respectively.
- The message ID does not contain the prefix GCTI or the application type ID.
  A log record in the full format looks like this:
  2002-05-07T18:11:38.196 Standard localhost cfg_dbserver GCTI-00-05060 Application started
  A log record in the short format looks like this:
  2002-05-07T18:15:33.952 Std 05060 Application started

messagefile

Default Value:
Valid Values: [string].lms (message file name)
Changes Take Effect: Immediately, if an application cannot find its *.lms file at startup

Specifies the file name for application-specific log events. The name must be valid for the operating system on which the application is running. The option value can also contain the absolute path to the application-specific *.lms file. Otherwise, an application looks for the file in its working directory.

print-attributes

Default Value: false

Valid Values:

- **true** Attaches extended attributes, if any exist, to a log event sent to log output.
- **false** Does not attach extended attributes to a log event sent to log output.
  Changes Take Effect: immediately
  Specifies whether the application attaches extended attributes, if any exist, to a log event that it sends to log output. Typically, log events of the Interaction log level and Audit-related log events contain extended

attributes. Setting this option to true enables audit capabilities, but negatively affects performance. Genesys recommends enabling this option for Solution Control Server and Configuration Server when using audit tracking. For other applications, refer to Genesys 7.5 Combined Log Events Help to find out whether an application generates Interaction-level and Audit-related log events; if it does, enable the option only when testing new interaction scenarios.

segment

Default Value: 10000

Valid Values:

- **false** No segmentation is allowed.
- **[number] KB or [number]** Sets the maximum segment size, in kilobytes. The minimum segment size is 100 KB.
- **[number] MB** Sets the maximum segment size, in megabytes.
- **[number] hr** Sets the number of hours for the segment to stay open. The minimum number is 1 hour.
  Changes Take Effect: immediately
  Specifies whether there is a segmentation limit for a log file. If there is, sets the mode of measurement, along with the maximum size. If the current log segment exceeds the size set by this option, the file is closed and a new one is created.

spool

Default Value:
Valid Values: [path] (the folder, with the full path to it)
Changes Take Effect: immediately

Specifies the folder, including full path to it, in which an application creates temporary files related to network log output. If you change the option value while the application is running, the change does not affect the currently open network output.

standard

Default Value: ../logs/ccp_standard

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends the log events of the Debug level and higher (that is, log events of the Standard, Interaction, Trace, and Debug levels). The log output types must be separated by a

comma when more than one output is configured.

time_convert

Default Value: local

Valid Values:

- **local** The time of log record generation is expressed as a local time, based on the time zone and any seasonal adjustments. Time zone information of the application's host computer is used.
- **utc** The time of log record generation is expressed as Coordinated Universal Time (UTC).
Changes Take Effect: immediately
Specifies the system in which an application calculates the log record time when generating a log file. The time is converted from the time in seconds since the Epoch (00:00:00 UTC, January 1, 1970).

time_format

Default Value: ISO8601

Valid Values:

- **time** The time string is formatted according to the HH:MM:SS.sss (hours, minutes, seconds, and milliseconds) format.
- **locale** The time string is formatted according to the system's locale.
- **ISO8601** The date in the time string is formatted according to the ISO 8601 format. Fractional seconds are given in milliseconds.
Changes Take Effect: immediately
Specifies how to represent, in a log file, the time when an application generates log records.
A log record's time field in the ISO 8601 format looks like this:
2001-07-24T04:58:10.123

trace

Default Value: ../logs/ccp

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application’s working directory.
Changes Take Effect: immediately
Specifies the outputs to which an application sends the log events of the Debug level and higher (that is, log events of the Standard, Interaction, Trace, and Debug levels). The log output types must be separated by a

comma when more than one output is configured.

verbose

Default Value: interaction

Valid Values:

- **all** All log events (that is, log events of the Standard, Trace,Interaction, and Debug levels) are generated.
- **debug** The same as all.
- **trace** Log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels) are generated, but log events of the Debug level are not generated.
- **interaction** Log events of the Interaction level and higher (that is, log events of the Standard and Interaction levels) are generated, but log events of the Trace and Debug levels are not generated.
- **standard** Log events of the Standard level are generated, but log events of the Interaction, Trace, and Debug levels are not generated.
- **none** No output is produced.
  Changes Take Effect: immediately
  Determines whether a log output is created. If it is, specifies the minimum level of log events generated. The log events levels, starting with the highest priority level, are Standard, Interaction, Trace, and Debug.

mediacontroller Section

- allow_dialog_transfer
- bridge_server
- bridge_server.defaultmaxsize
- bridge_server.defaultreserve
- bridge_server.profile
- bridge_sips_server
- codec_check_exclusion.payloads
- conference.defaultreserve
- defaultrejectcode
- full_audio_codec
- full_video_codec
- inbound_allowed_media
- sdp.defaultipversion
- sdp.localhost
- sdp.localhost.ipv6
- sip.allowedunknownheaders
- sipproxy
- sipsecure
- sipsproxy

allow_dialog_transfer

Default Value: 1

Valid Values:

- **true** Enable transfers through dialog
- **false** Disable transfers through dialog
Changes Take Effect: immediately
Allows SIP dialog transfer. If this parameter is set to false, all incoming SIP REFER will be automatically rejected with SIP 403. Otherwise, the request will be forward to the CCXML application.

bridge_server

Default Value: $LocalIP$:5060
Valid Values: A valid IP address:Port can only contain alphanumeric characters, '.', '-', ':', ' ','/' and '\' characters
Changes Take Effect: immediately

The address of SIP Bridge Server for use when the two end-points cannot be joined due to media bridging limitations.
Bridge Server must be able to

- send media to multiple end-points
- send and receive from distinct end-points and
- have transcoding capability.

bridge_server.defaultmaxsize

Default Value: 4
Valid Values: From 1 to 1000 inclusive
Changes Take Effect: immediately

This controls the confmaxsize URI parameter when conference is set up in the bridge server.

bridge_server.defaultreserve

Default Value: 4
Valid Values: From 1 to 1000 inclusive
Changes Take Effect: immediately

This controls the confreserve URI parameter when conference is set up in the bridge server.

bridge_server.profile

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

The name of device profile to use with the configured Bridge Server.

bridge_sips_server

Default Value: $LocalIP$:5061
Valid Values: A valid IP address:Port can only contain alphanumeric characters, '.', '-', ':', ' ','/' and '\' characters
Changes Take Effect: immediately

The address of SIP secure Bridge Server for use when the two end-points cannot be joined due to media bridging limitations.
Bridge Server must be able to

- send media to multiple end-points
- send and receive from distinct end-points and
- have transcoding capability.

codec_check_exclusion.payloads

Default Value: 13
Valid Values:
Changes Take Effect: immediately

A list of space delimited payloads that will be excluded during codec checking for join result determination.

conference.defaultreserve

Default Value: 8
Valid Values:
Changes Take Effect: immediately

Default URI confreserve parameter for conference server if requested reserve size is not defined

defaultrejectcode

Default Value: 480
Valid Values:
Changes Take Effect: immediately

Specifies the default SIP Response code to use when an incoming call is rejected by the application

full_audio_codec

Default Value: 0|pcmu|audio/basic|8000|1 8|pcma|audio/x-alaw-basic|8000|1 9|g722|audio/g722|8000|1 23|g726-16|audio/g726-16|8000|1 22|g726-16|audio/g726-16|8000|1 2|g726-32|audio/g726|8000|1 125|g726-40|audio/g726-40|8000|1 18|g729|audio/g729|8000|1 3|gsm|audio/x-gsm|8000|1 105|AMR|audio/AMR|8000|1 112|AMR-WB|audio/AMR-WB|16000|1 101|telephone-event|none|8000|1
Valid Values:
Changes Take Effect: immediately

This defines the audio codecs that get set in the SDP in an initial offer with no media bridge. Codec entry has to be in the format of: payload|name|mime|rate|#channels. Each codec entry is separated by a whitespace.

full_video_codec

Default Value: 34|h263|video/H263|90000|1 99|h263-1998|video/H263-1998|90000|1 113|H264|video/H264|90000|1
Valid Values:
Changes Take Effect: immediately

This defines the video codecs that get set in the SDP in an initial offer with no media bridge. Codec entry has to be in the format of: payload|name|mime|rate|#channels. Each codec entry is separated by a whitespace.

inbound_allowed_media

Default Value: dynamic
Valid Values: Must be one of the following:

- **dynamic**
- **audio video**
- **audio**
- **video**
Changes Take Effect: immediately
The default allowed media types for an inbound call. All inbound calls will be limited to this set of media types in terms of SDP exchange. If set to dynamic, media type is determined from the capability SDP of the inbound call (if capability SDP is not available, it defaults to audio and video).

sdp.defaultipversion

Default Value: true
Valid Values: ipv4, ipv6
Changes Take Effect: immediately

Default IP version to be used in SDP message, apply to initiated SDP offer to unjoined endpoint. Valid values are "ipv4" or "ipv6".

sdp.localhost

Default Value: $LocalIP$
Valid Values:
Changes Take Effect: immediately

The local host IPv4 address (only the host part) that will be used in SDP.

sdp.localhost.ipv6

Default Value: $LocalIPv6$
Valid Values:
Changes Take Effect: immediately

The local host IPv6 address (only the host part) that will be used in SDP.

sip.allowedunknownheaders

Default Value:

-

Valid Values:
Changes Take Effect: immediately

This parameter takes a space delimited list of acceptable unknown header list. Unknown headers received from SIP messages that are not part of this list will be ignored. It will not be accessable from the application. Specifying a wilcard (*) means all unknown headers are allowed.

sipproxy

Default Value: $LocalIP$:5060
Valid Values: A valid IP address:Port can only contain alphanumeric characters, '.', '-', ':', ' ','/' and '\' characters
Changes Take Effect: immediately

The address of SIP Proxy for outbound SIP requests. Should be specified like 10.10.30.205:5070

sipsecure

Default Value: 0

Valid Values:

- **true** Using SIP Secure protocol
- **false** Not using SIP Secure protocol
  Changes Take Effect: immediately
  If this flag is set to true, all the outbound sip requests would be in SIP secure protocol. Note, the hints attribute of the CCXML elements that initiates an out bound request can over write this configuration.

sipsproxy

Default Value: $LocalIP$:5061
Valid Values: A valid IP address:Port can only contain alphanumeric characters, '.', '-', ':', ' ','/' and '\' characters
Changes Take Effect: immediately

The address of SIP Secure Proxy for outbound SIP requests. Should be specified like 10.10.30.205:5071

session Section

- copy_unknown_headers

copy_unknown_headers

Default Value: true
Valid Values: true, false
Changes Take Effect: immediately

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. When the flag is set to true, unknown Headers will be copied, and if the flag is set to false, unknown headers will not be copied.

sip Section

- copyunknownheaders
- localuser
- maxtcpconnections
- maxtlsconnections
- min_se
- mtusize
- OPTIONS.header.Accept
- OPTIONS.header.Accept-Encoding
- OPTIONS.header.Accept-Language
- OPTIONS.header.Allow
- OPTIONS.header.Supported
- prack.support
- preferred_ipversion
- registerexpiryadjustment
- route.default.tcp
- route.default.tcp.ipv6
- route.default.tls
- route.default.tls.ipv6
- route.default.udp
- route.default.udp.ipv6
- route.dest.0
- route.dest.1
- route.dest.2
- route.dest.3
- route.dest.4
- route.dest.5
- routeset
- securerouteset
- sessionexpires
- tcp.portrange
- threadpoolsize
- threads
- timer.ci_proceeding
- tls.portrange
- 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.staticroutelist

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

snmp Section

- timeout

timeout

Default Value: 100
Valid Values: The parameter must be an integer value greater than zero.
Changes Take Effect: At start/restart

The maximum amount of time that SNMP can wait for a new task. This value is specified in milliseconds.

Supplementary Services Gateway

Options for this component are contained in the following configuration sections:

- Common
- ems
- fm
- HTTP
- log
- SSG
- Tenant1

Tip

In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.

Power users: Download a CSV file containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
Common	enable-ipv6	1	At start/restart
ems	logconfig.MFSINK	• |*|*	immediately
ems	logconfig.TRAPSINK •	|*|*	At start/restart
fm	http_proxy		At start/restart
fm	request_wait_time	5000	At start/restart
HTTP	CertFile	$InstallationRoot$/config/ x509_certificate.pem	After restart
HTTP	CertKeyFile	$InstallationRoot$/config/ x509_private_key.pem	After restart
HTTP	CertPassword		After restart
HTTP	HTTPDefaultPage	SSG	After restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
HTTP	HTTPPort	9800	After restart
HTTP	HTTPSPort	9801	After restart
HTTP	ResponseHeaders	X-Frame-Options:DENY	After restart
HTTP	TLSType	SSLv23	After restart
log	all	../logs/SSG	immediately
log	debug	../logs/SSG	immediately
log	expire	7 day	immediately
log	interaction	../logs/SSG	immediately
log	segment	10000	immediately
log	standard	../logs/SSG	immediately
log	time_convert	local	immediately
log	trace	../logs/SSG	immediately
log	verbose	standard	immediately
SSG	CleanIntervalSecs	180	After restart
SSG	ClientPortToTServer		After restart
SSG	ConnRetryIntervalSecs	120	After restart
SSG	fips_enabled	False	After restart
SSG	InitiatedCallRetryFlag	1	After restart
SSG	MaxAttemptsLimit	25	After restart
SSG	MaxDBConnPoolSize	7	After restart
SSG	MinDBConnPoolSize	3	After restart
SSG	pacing.BatchLimit	TotalPorts	After restart
SSG	pacing.caps.CallRequestsPerSecond	30	After restart
SSG	pacing.EqualPriorityToNewAndOld	false	After restart
SSG	pacing.NextRetryIntervalSecs	10	After restart
SSG	pacing.PortLoadFactor	100	After restart
SSG	pacing.QLowWatermark	25	After restart
SSG	pacing.SlotCalculation	Proportionate	After restart
SSG	PAssertedIdentityUsage	0	After restart
SSG	RegRetryIntervalSecs	120	After restart
SSG	ReqAccOnResourceDNErrTimeoutSecs	900	After restart
SSG	ReqAccOnSIPSConnErrTimeoutSecs	900	After restart
SSG	TimeToLiveLimitMins	1440	After restart
Tenant1	AccessGroup		After restart
Tenant1	DialPrefix		After restart
Tenant1	RPDN		After restart
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
Tenant1	TGDN		After restart
Section	**Option**	**Default**	**Changes Take Effect**

Common Section

- enable-ipv6

enable-ipv6

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

T-library configuration parameter to enable SSG using IPv6 for connecting with SIP-Server

ems Section

- logconfig.MFSINK
- logconfig.TRAPSINK

logconfig.MFSINK

Default Value:

- |*|*

Valid Values: Pipe delimited ranges for log levels, module IDs and specifier IDs. Ranges can be comma separated integers or range of integers or '*'.
Changes Take Effect: immediately

Controls the log messages that are sent to the MF sink. The format is 'levels|moduleIDs|specifierIDs' (repeated if necessary). The values between the pipes can be in the format: 'm-n,o,p' (ie "0-4, 5,6"). The wildcard character '*' can also be used to indicate all valid numbers. Example: '*|*|*' indicates that all log messages should be sent to the sink. Alternatively, '0,1|0-10|*|4|*|*' indicates that CRITICAL(0) and ERROR(1) level messages with module IDs in the range 0-10 will be sent to the sink; and all INFO(4) level messages will be sent as well.

logconfig.TRAPSINK

Default Value:

- |*|*

Valid Values:
Changes Take Effect: At start/restart

Specifies the metrics that are delivered to the SNMP Trap Sink.

fm Section

http_proxy

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

The HTTP proxy to be used for HTTP requests

request_wait_time

Default Value: 5000
Valid Values:
Changes Take Effect: At start/restart

Controls Fetching module Request wait time. Specified in milli-seconds

HTTP Section

- CertFile
- CertKeyFile
- CertPassword
- HTTPDefaultPage
- HTTPPort
- HTTPSPort
- ResponseHeaders
- TLSType

CertFile

Default Value: $InstallationRoot$/config/x509_certificate.pem
Valid Values:
Changes Take Effect: After restart

Name of the HTTPS Server Certificate file.

CertKeyFile

Default Value: $InstallationRoot$/config/x509_private_key.pem
Valid Values:
Changes Take Effect: After restart

Name of the HTTPS Server Certificate Key file.

CertPassword

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

Password for accessing the HTTP Server Certificate Key File.

HTTPDefaultPage

Default Value: SSG
Valid Values:

Changes Take Effect: After restart

Default HTTP Page, being used by SSG for storing the outbound requests.

HTTPPort

Default Value: 9800
Valid Values:
Changes Take Effect: After restart

Describes the port on which HTTP requests can be received from client applications.

HTTPSPort

Default Value: 9801
Valid Values:
Changes Take Effect: After restart

Describes the port on which HTTPS requests can be received from client applications.

ResponseHeaders

Default Value: X-Frame-Options:DENY
Valid Values:
Changes Take Effect: After restart

Specifies any custom HTTP headers that need to be included in HTTP responses sent by SSG. These are sent for all HTTP responses by SSG(both for Root page access and TriggerAction requests). Format for specification is Header1:Value1|Header2:Value2. The Value part may also contain : and | characters in which case they must be escaped with a backward slash (eg: Header1:Value1-\|Value2 will be considered as Header1: Value1-|Value2. If unescaped, then the header will be Header1:Value1-). Default value will be set to X-Frame-Options:DENY

TLSType

Default Value: SSLv23
Valid Values: SSLv23, SSLv3, SSLv2, TLSv1
Changes Take Effect: After restart

Name of the secure protocol with version information.

log Section

- all
- debug
- expire
- interaction
- segment
- standard
- time_convert
- trace
- verbose

all

Default Value: ../logs/SSG

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends all log events. The log output types must be separated by a comma when more than one output is configured.

debug

Default Value: ../logs/SSG

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.

- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends the log events of the Debug level and higher (that is, log events of the Standard, Interaction, Trace, and Debug levels). The log output types must be separated by a comma when more than one output is configured.

expire

Default Value: 7 day

Valid Values:

- **false** No expiration; all generated segments are stored.
- **[number] file or [number]** Sets the maximum number of log files to store. Specify a number from 1-1000.
- **[number] day** Sets the maximum number of days before log files are deleted. Specify a number from 1-100.
  Changes Take Effect: immediately
  Determines whether log files expire. If they do, sets the measurement for determining when they expire, along with the maximum number of files (segments) or days before the files are removed. This option is ignored if log output is not configured to be sent to a log file. Note: If the value of the option is set incorrectly -out of the range of valid values- it will be automatically reset to 10

interaction

Default Value: ../logs/SSG

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends the log events of the Interaction level and higher (that is, log events of the Standard and Interaction levels). The log outputs must be separated by a comma when more than one output is configured.

segment

Default Value: 10000

Valid Values:

- **false** No segmentation is allowed.
- **[number] KB or [number]** Sets the maximum segment size, in kilobytes. The minimum segment size is 100 KB.
- **[number] MB** Sets the maximum segment size, in megabytes.
- **[number] hr** Sets the number of hours for the segment to stay open. The minimum number is 1 hour.
  Changes Take Effect: immediately
  Specifies whether there is a segmentation limit for a log file. If there is, sets the mode of measurement, along with the maximum size. If the current log segment exceeds the size set by this option, the file is closed and a new one is created.

standard

Default Value: ../logs/SSG

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends the log events of the Standard level. The log output types must be separated by a comma when more than one output is configured.

time_convert

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

Specifies the system in which an application calculates the log record time when generating a log file. The time is converted from the time in seconds since the Epoch (00:00:00 UTC, January 1, 1970).

- **Local Time (local)** The time of log record generation is expressed as a local time, based on the time zone and any seasonal adjustments. Time zone information of the application's host computer is used.
- **Coordinated Universal Time (utc)** The time of log record generation is expressed as Coordinated Universal Time (UTC).

trace

Default Value: ../logs/SSG

Valid Values:

- **stdout** Log events are sent to the Standard output (stdout).
- **stderr** Log events are sent to the Standard error output (stderr).
- **network** Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- **memory** Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- **[filename]** Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.
  Changes Take Effect: immediately
  Specifies the outputs to which an application sends the log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels). The log outputs must be separated by a comma when more than one output is configured.

verbose

Default Value: standard

Valid Values:

- **all** All log events (that is, log events of the Standard, Trace,Interaction, and Debug levels) are generated.
- **debug** The same as all.
- **trace** Log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels) are generated, but log events of the Debug level are not generated.
- **interaction** Log events of the Interaction level and higher (that is, log events of the Standard and Interaction levels) are generated, but log events of the Trace and Debug levels are not generated.
- **standard** Log events of the Standard level are generated, but log events of the Interaction, Trace, and Debug levels are not generated.
- **none** No output is produced.
  Changes Take Effect: immediately
  Determines whether a log output is created. If it is, specifies the minimum level of log events generated. The log events levels, starting with the highest priority level, are Standard, Interaction, Trace, and Debug.

PageCollector Section

No public options in this section.

SSG Section

CleanIntervalSecs

Default Value: 180
Valid Values:
Changes Take Effect: After restart

Interval in seconds that determines how frequently SSG removes expired or completed requests from the DB.

ClientPortToTServer

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

The local client side TCP port to be used for T-Lib transport. If this parameter is not specified, SSG will let the OS choose the local port.

ConnRetryIntervalSecs

Default Value: 120
Valid Values:
Changes Take Effect: After restart

SSG attempts to re-connect to SIP Server in case of connection failure with SIP Server continuously in this interval.

fips_enabled

Default Value: False
Valid Values: True, False
Changes Take Effect: After restart

Specifies whether to enable FIPS mode in SSG. When FIPS mode is enabled, only FIPS 140-2 approved ciphers and algorithms can be used in SSL connections.

InitiatedCallRetryFlag

Default Value: 1
Valid Values: 0, 1, 2, 3
Changes Take Effect: After restart

This parameter specifies how to process the requests present in the DB when SSG comes up. If the parameter value is set to 0 (zero), SSG deems all the initiated requests during SSG startup as failures and invokes notification URL for these requests. If it is set to 1, then SSG retries those requests. If the value is set to 2, then SSG deletes requests which are new and initiated. If the value is set to 3, then SSG deletes all the database requests

MaxAttemptsLimit

Default Value: 25
Valid Values:
Changes Take Effect: After restart

The maximum attempts allowed (as system-wide upper limit) for outbound call requests from customer application.

MaxDBConnPoolSize

Default Value: 7
Valid Values:
Changes Take Effect: After restart

The maximum number of database connections kept alive for use in SSG.

MinDBConnPoolSize

Default Value: 3
Valid Values:
Changes Take Effect: After restart

The minimum number of database connections kept alive for use in SSG.

pacing.BatchLimit

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

Total Number of requests, being fetched from DB in to the memory queue for processing in each cycle. If 'TotalPorts' is configured, SSG uses GVP total port capacity as obtained from SIP-S EventResourceInfo as the batch limit. if 'AvailPorts' is configured, SSG uses current available port capacity as obtained from SIP-S EventResourceInfo as the batch limit. Otherwise,user can configure any integer value as string, which will used as the fetching limit.

pacing.caps.CallRequestsPerSecond

Default Value: 30
Valid Values:
Changes Take Effect: After restart

This parameter controls the maximum calls per second that SSG shall initiate via SIP Server

pacing.EqualPriorityToNewAndOld

Default Value: false
Valid Values: true, false
Changes Take Effect: After restart

In each fetch cycle from db, SSG gives equal priority to New and Old records if flag is set to true. Otherwise, New and Old records are not differentiated. If this option is set to true, increased DB fetches may result in some performance degardation.

pacing.NextRetryIntervalSecs

Default Value: 10
Valid Values:
Changes Take Effect: After restart

This parameter dicates after how many seconds the call will be retried when temporary internal errors occur.

pacing.PortLoadFactor

Default Value: 100
Valid Values:
Changes Take Effect: After restart

This parameter dictates how many outbound calls are inititated by SSG at a time. This is a % of the current GVP available port capacity.

pacing.QLowWatermark

Default Value: 25
Valid Values:
Changes Take Effect: After restart

When In-Memory queue falls below this pre-defined % of total Batch Limit, SSG activates next fetching cycle.

pacing.SlotCalculation

Default Value: Proportionate
Valid Values: Proportionate, Equal
Changes Take Effect: After restart

This parameter dictates how many records are allotted for an application in each database dip in every fetch cycle. If 'Proportionate' is configured, BatchLimit is divided among applications in the same ratio as their pending requests. if 'Equal' is configured, BatchLimit is divided equally among applications.

PAssertedIdentityUsage

Default Value: 0
Valid Values:
Changes Take Effect: After restart

SSG includes this parameter under SIP_HEADERS extension in TMakePredictiveCall. This parameter can be set to 0,1 or 2 values. Setting it to '0' makes SSG not to include the parameter as extension parameter. Setting it to '1' makes SSG map ANI AS-IS to this parameter and include in the SIP_HEADERS extension. Setting it to '2' makes SSG extract the user part of the ANI and map it to this extension parameter.

RegRetryIntervalSecs

Default Value: 120
Valid Values:
Changes Take Effect: After restart

SSG attempts to re-register the Resource DN in case of registraion failure with SIP Server continuously in this interval.

ReqAccOnResourceDNErrTimeoutSecs

Default Value: 900
Valid Values:
Changes Take Effect: After restart

SSG rejects new requests from tenant applications if SSG fails to register Resource DN with SIP Server after the above time-out.

ReqAccOnSIPSConnErrTimeoutSecs

Default Value: 900
Valid Values:
Changes Take Effect: After restart

SSG rejects new requests from tenant applications if SSG fails to connect to SIP Server after the above time-out.

TimeToLiveLimitMins

Default Value: 1440
Valid Values:
Changes Take Effect: After restart

The maximum duration allowed (as system-wide upper limit) for outbound call requests from customer application.

Tenant1 Section

AccessGroup

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

The Access Group controls enabling of Digest Authentication for a tenant. The users configured under access group are allowed to send HTTP requests to SSG.

DialPrefix

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

The dial prefix, if present, will be prepended to all the target numbers. This applies to all outbound calls (across all IVR profiles) for the tenant. The dial prefix can be used, for example, to select a specific trunk in SIP Server or to select a specific ROUTE in PSTN Connector or to pass some predefined numbers to the switch (if the outbound call is going out via a switch) or any combination of these. Please see GVP User Guide for more details. This parameter is optional.

RPDN

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

The Routing Point DN is used by SSG to make outbound calls in case of Legacy GVP VXML Interpreter is used to play the IVR

TGDN

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

The Trunk Group DN parameter is used by SSG to fetch the resource information like available ports, total ports etc and also to make outbound calls in case of Next Generation VXML Interpreter is used to play the IVR. The tenant name is same as TGDN.

Third Party Call Recorder

Options for this component are contained in the following configuration sections:

- gvp.rm
- provision

Tip

In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.

Power users: **Download a CSV file** containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
gvp.rm	aor		At start/restart
gvp.rm	port-capacity	500	At start/restart
gvp.rm	redundancy-type	active	At start/restart
provision	recording-server	1	At start/restart
Section	**Option**	**Default**	**Changes Take Effect**

gvp.rm Section

- aor
- port-capacity
- redundancy-type

aor

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

This parameter specifies the SIP service address of the resource. The format is sip[s]:<host>:port

port-capacity

Default Value: 500
Valid Values:
Changes Take Effect: At start/restart

This parameter specifies maximum port capacity of the resource. The number of active SIP sessions to the resource will not be allowed to exceed this capacity.

redundancy-type

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

This parameter specifies the redundancy type of the resource. If all of the active redundancy type resources are up, then only the resources with the active redundancy-type will be used. If any one of them are down, then passive redundancy type resources will also be used.

provision Section

- recording-server

recording-server

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

This parameter indicates to the Resource Manager that this is a recording server resource. Unless this parameter is set to 1, this application will not be used by the RM as the recording server resource.