Voice Platform Media Control Platform

8.5.176.05

5/14/2025

8.5.176.05

Voice Platform Media Control Platform Release Notes

Release Date	Release Type	Restrictions	AIX	Linux	Solaris	Windows
01/30/17	General			X		X

Contents

What's New

This release contains the following new features and enhancements:

- Two new configuration options are now available to allow the Media Control Platform (MCP) to perform health check on the media threads.

  health.maxprocessingtime

  Section: mpc

  Valid values: Any positive integer

  Default value: `600000`

  Takes effect: At start/restart

  Specifies the maximum processing time (in milliseconds) that a media thread can take to process a media object, exceeding which, the MCP will be terminated. If the option is set to `0`, MCP does not perform any processing time check on media threads.

  health.waittime

  Section: mpc

  Valid values: Any positive integer

  Default value: `0`

  Takes effect: At start/restart

  Specifies the wait time (in milliseconds) after which the health thread performs the health check on the media threads. If the option is set to `0` (the default), MCP does not perform any health check.

  Genesys recommends to configure the **health.waittime** option only when necessary. Also, note that the value of the **health.waittime** option must be smaller than the value of the **health.maxprocessingtime** option.

- MCP now uses OpenSSL libraries version 1.0.2j. MCP supports these versions of Transport Layer Security (TLS): TLSv1.2, TLSv1.1, and TLSv1; and these versions of Secure Sockets Layer (SSL): SSLv2, SSLv3,

Helpful Links

Releases Info

- List of 8.5.x Releases
- 8.5.x Known Issues

Product Documentation

GVP

Genesys Products

List of Release Notes

and SSLv23.

The following configuration options support the versions of TLS and SSL listed above:

- **sip.transport.<n>** type = (default is TLSv1_2)
- **mrcpv2client.sip.transport.<n>** type = (default is TLSv1)
- **vrmrecorder.sip.transport.<n>** type = (default is TLSv1_2)
- **fm.ssl_version** = (default is 0)

Note: Please refer to the 8.5 Product Alerts before upgrading MCP to this version.

- You can now mask a customer’s sensitive information in MCP log files with asterisks (*) by using a new configuration option **mask_sensitive_data** in the **[log]** section. Masking sensitive data using this new option applies only when the MCP logging level is set to `trace, debug`, or `all`. This masking capability is not available for the `standard` or `interaction` levels of MCP logging, use the **gvp:private** option in such cases.

mask_sensitive_data

Section: log

Default Value: `false`

Valid Values: `true, false`

Changes Take Effect: Immediately

Determines whether a customer’s sensitive information needs to be masked in the MCP log file. This parameter is effective when the logging level is set to `trace, debug,` or `all`.

When the **mask_sensitive_data** parameter is set to `true`, the following values in the MCP log file are masked and replaced with four asterisks (****) regardless of the length of input information:

- DTMF and ASR input
- DTMF and TTS output
- All HTTP/HTTPS GET/POST data
- All URL query strings processed in VXML and the fetching modules
- Expressions or values evaluated during VXML runtime

When the **mask_sensitive_data** parameter is set to `false`, a customer’s sensitive information are not replaced with asterisks (*).

> **Important**
>
> A customer’s sensitive data logged at the transport level for protocol requests such as SIP, RTSP, and so on are not masked.

- MCP now supports uploading the call recordings to S3 servers that need Amazon Web Services (AWS) V4 signature.

Configure the two new parameters **record.amazonsignatureversion** and **record.amazonsignedpayload** in the **[msml]** section that allows MCP to support the AWS V4 signature.

record.amazonsignatureversion

Section: msml

Valid values: `V2, V4`

Default value: V4

Takes effect: Immediate or session

Specifies the Amazon’s method to generate the authentication signature for GET and PUT requests while uploading the call recordings to S3 servers.

The V4 signature algorithm (the default) requires the bucket location or region information as an authentication criterion. MCP retrieves the bucket or region information using the following methods:

- **Automatic:** MCP retrieves the bucket or region information using an Amazon service automatically.
- **Manual:** MCP retrieves the bucket or region information from the IVR profile parameters **recordingclient.AWSRegion** and **recordingclient.AWSRegion2** that are manually configured by the user.

record.amazonsignedpayload

Section: msml

Valid values: `true, false`

Default value: `false`

Takes effect: Immediate or session

Determines if the payload needs to be signed with the Amazon V4 signature.

Applies only when the signature authentication is configured as V4 in the option **recordingclient.AWSRegion**.

- When set to `false` (the default), MCP doesn’t calculate the payload hash.
- When set to `true`, MCP calculates the Hash SHA256 of the Amazon POST payloads.

Resolved Issues

This release contains the following resolved issues:

MCP no longer enters into an unresponsive state when the Configuration Server switches from primary to backup or vice-versa. (GVP-23620)

MCP now generates the SNMP traps for non-recoverable errors.

The non-recoverable error occurs in specific scenarios during the post-processing operations of the recording files. (GVP-23592)

When using SIP Secure, the MCP no longer terminates abnormally. Also, the issue of calls getting dropped is now resolved. (GVP-23540)

MCP no longer terminates abnormally when its recorder UserAgent receives the non-REGISTER SIP requests with wrong transports in the VIA header. (GVP-23528)

MCP now correctly uploads the recorded files to the newly created Amazon S3 buckets by enabling a new configuration option **enableuploadcontentrewind**.

enableuploadcontentrewind
Section: fm
Valid values: `0, 1`
Default value: 1

Specifies whether the libcurl resends the uploaded content during PUT requests when the content is redirected.

- When set to 1 (the default), the libcurl resends the uploaded content to the redirected location.
- When set to `0`, the libcurl doesn't resend the uploaded content to the redirected location. (GVP-23455)

Upgrade Notes

No special procedure is required to upgrade to release 8.5.176.05.