# Genesys Voice Platform

fm Section

12/18/2025

# fm Section



## 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.