Genesys Voice Platform

fm Section

4/14/2025

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: 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.