Framework 8.0

Configuration Options

Reference Manual

About Genesys

Genesys Telecommunications Laboratories, Inc., a subsidiary of Alcatel-Lucent, is 100% focused on software for contact centers. Genesys recognizes that better interactions drive better business and build company reputations. Customer service solutions from Genesys deliver on this promise for Global 2000 enterprises, government organizations, and telecommunications service providers across 80 countries, directing more than 100 million customer interactions every day. Sophisticated routing and reporting across voice, e-mail, and Web channels ensure that customers are quickly connected to the best available resource—the first time. Genesys offers solutions for customer service, help desks, order desks, collections, outbound telesales and service, and workforce management. Visit www.genesyslab.com for more information.

Each product has its own documentation for online viewing at the Genesys Technical Support website or on the Documentation Library DVD, which is available from Genesys upon request. For more information, contact your sales representative.

Notice

Although reasonable effort is made to ensure that the information in this document is complete and accurate at the time of release, Genesys Telecommunications Laboratories, Inc., cannot assume responsibility for any existing errors. Changes and/or corrections to the information contained in this document may be incorporated in future versions.

Your Responsibility for Your System’s Security

You are responsible for the security of your system. Product administration to prevent unauthorized use is your responsibility. Your system administrator should read all documents provided with this product to fully understand the features available that reduce your risk of incurring charges for unlicensed use of Genesys products.

Trademarks

Genesys, the Genesys logo, and T-Server are registered trademarks of Genesys Telecommunications Laboratories, Inc. All other trademarks and trade names referred to in this document are the property of other companies. The Crystal monospace font is used by permission of Software Renovation Corporation, www.SoftwareRenovation.com.

Technical Support from VARs

If you have purchased support from a value-added reseller (VAR), please contact the VAR for technical support.

Technical Support from Genesys

If you have purchased support directly from Genesys, please contact Genesys Technical Support at the regional numbers provided on page 9. For complete contact information and procedures, refer to the ***Genesys Technical Support Guide***.

Ordering and Licensing Information

Complete information on ordering and licensing Genesys products can be found in the ***Genesys Licensing Guide.***

Released by

Genesys Telecommunications Laboratories, Inc. www.genesyslab.com

Document Version: 80fr_ref-co_06-2010_v8.0.301.00

Table of Contents

Preface

Welcome to the *Framework 8.0 Configuration Options Reference Manual.* This document describes the configuration options for the Genesys Framework 8.0 components, which you must configure in the Configuration Layer. This document is designed to be used along with the *Framework 8.0 Deployment Guide.*

This document is valid only for the 8.0 release(s) of the Genesys Framework.

Note: For versions of this document created for other releases of this product, visit the Genesys Technical Support website, or request the Documentation Library DVD, which you can order by e-mail from Genesys Order Management at `orderman@genesyslab.com`.

This preface contains the following sections:

For information about related resources and about the conventions that are used in this document, see the supplementary material starting on page 107.

About Configuration Options

Configuration options, enabled when a component starts up, define that component's configuration. You set configuration option values in Configuration Wizards or in Configuration Manager or Genesys Administrator. You should set configuration options in configuration files, for those applications that are configured via such files (Configuration Server, DB Server for the Configuration Database, and Local Control Agent). The configuration procedure for Framework components is described in the *Framework 8.0 Deployment Guide.*

The options in the current document are divided by sections, as they are in a component configuration. Section names are set by default; changing them is not recommended. For applications that are configured via configuration files, the section name is put in square brackets—for example, `[dbserver]`.

If an option is not present in the component configuration, the default value applies. You must specify a value for every mandatory option that does not have a default value. You will find a list of mandatory options for a component at the beginning of the relevant chapter.

Intended Audience

This document is primarily intended for system administrators. It has been written with the assumption that you have a basic understanding of:

- Computer-telephony integration (CTI) concepts, processes, terminology, and applications
- Network design and operation
- Your own network configurations

You should also be familiar with:

- Genesys Framework architecture and functions.
- Configuration Manager or Genesys Administrator interface and object-managing operations.

Making Comments on This Document

If you especially like or dislike anything about this document, feel free to e-mail your comments to `Techpubs.webadmin@genesyslab.com`.

You can comment on what you regard as specific errors or omissions, and on the accuracy, organization, subject matter, or completeness of this document. Please limit your comments to the scope of this document only and to the way in which the information is presented. Contact your Genesys Account Representative or Genesys Technical Support if you have suggestions about the product itself.

When you send us comments, you grant Genesys a nonexclusive right to use or distribute your comments in any way it believes appropriate, without incurring any obligation to you.

Contacting Genesys Technical Support

If you have purchased support directly from Genesys, contact Genesys Technical Support at the following regional numbers:

Region	Telephone	E-Mail
North America and Latin America	+888-369-5555 (toll-free) +506-674-6767	support@genesyslab.com
Europe, Middle East, and Africa	+44-(0)-1276-45-7002	support@genesyslab.co.uk
Asia Pacific	+61-7-3368-6868	support@genesyslab.com.au
Malaysia	1-800-814-472 (toll-free) +61-7-3368-6868	support@genesyslab.com.au
India	000-800-100-7136 (toll-free) +91-(022)-3918-0537	support@genesyslab.com.au
Japan	+81-3-6361-8950	support@genesyslab.co.jp
Before contacting technical support, refer to the *Genesys Technical Support Guide* for complete contact information and procedures.		

Changes to This Document

This document has been updated for new and changed functionality in this release of Management Framework, as described in the Release Notes for Management Framework components. Changes to this document include:

- In Chapter 4, "Configuration Server Configuration Options," on page 47, detailed descriptions of the configuration options `allow-empty-password`, `allow-external-empty-password`, and `encryption` have been moved to the *Genesys 8.0 Security Deployment Guide*.
- Chapter 13, "Host Configuration Options," on page 101 has been added.
- Chapter 14, "Tenant Configuration Options," on page 105 has been added.

Chapter

1 Common Configuration Options

Unless otherwise noted, the common configuration options that this chapter describes are common to all Genesys server applications and applicable to any Framework server component. This chapter includes the following sections:

Note: Some server applications also support log options that are unique to them. For descriptions of a particular application's unique log options, refer to the chapter/document about that application.

Setting Configuration Options

Unless specified otherwise, set common configuration options in the `Options` of the `Application` object, using one of the following navigation paths:

- In Genesys Administrator—`Application` object > `Options` tab > `Advanced View (Options)`
- In Configuration Manager—`Application` object > `Properties` dialog box > `Options` tab

Warning! Configuration section names, configuration option names, and predefined option values are case-sensitive. Type them in Genesys Administrator or Configuration Manager exactly as they are documented in this chapter.

Mandatory Options

You do not have to configure any common options to start Server applications.

log Section

This section must be called `log`.

Warning! For applications configured via a configuration file, changes to log options take effect after the application is restarted.

verbose

Default Value: `all`
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. See also “Log Output Options” on page 18.

Note: For definitions of the Standard, Interaction, Trace, and Debug log levels, refer to the *Framework 8.0 Management Layer User's Guide*, *Framework 8.0 Genesys Administrator Help,* or to *Framework 8.0 Solution Control Interface Help.*

buffering

Default Value: `true`
Valid Values:

`true`	Enables buffering.
`false`	Disables buffering.

Changes Take Effect: Immediately

Turns on/off operating system file buffering. The option is applicable only to the `stderr` and `stdout` output (see page 18). Setting this option to `true` increases the output performance.

Note: When buffering is enabled, there might be a delay before log messages appear at the console.

segment

Default Value: `false`
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. This option is ignored if log output is not configured to be sent to a log file.

expire

Default Value: `false`
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 an option’s value is set incorrectly—out of the range of valid values— it will be automatically reset to `10`.

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`).

Note: This option applies only to T-Servers.

messagefile

Default Value: As specified by a particular application
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.

Warning! An application that does not find its `*.lms` file at startup cannot generate application-specific log events and send them to Message Server.

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
```

Note: Whether the full or short format is used, time is printed in the format specified by the `time_format` option.

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: `time`
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
```

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 8.0 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.

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.

memory

Default Value: No 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 (see "Log Output Options" on page 18). 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.

Note: If the file specified as the `memory` file is located on a network drive, an application does not create a snapshot file (with the extension `*.memory.log`).

memory-storage-size

Default Value: `2 MB`
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. See also "Log Output Options" on page 18.

spool

Default Value: The application's working directory
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.

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. For example, you configure the following options in the `log` section for a 6.x application and for a 7.x application:

```
[log]
verbose = all
debug = file1
standard = file2
```

The log file content of a 6.x application is as follows:

- `file1` contains Debug messages only.
- `file2` contains Standard messages only.

The log file content of a 7.x application is as follows:

- `file1` contains Debug, Trace, Interaction, and Standard messages.
- `file2` contains Standard messages only.

If you set `compatible-output-priority` to `true` in the 7.x application, its log file content will be the same as for the 6.x application.

Warning! Genesys does not recommend changing the default value of this option unless you have specific reasons to use the 6.x log output logic—that is, to mimic the output priority as implemented in releases 6.x. Setting this option to `true` affects log consistency.

Log Output Options

To configure log outputs, set log level options (`all`, `alarm`, `standard`, `interaction`, `trace`, and/or `debug`) to the desired types of log output (`stdout`, `stderr`, `network`, `memory`, and/or `[filename]`, for log file output).

You can use:

- One log level option to specify different log outputs.
- One log output type for different log levels.
- Several log output types simultaneously, to log events of the same or different log levels.

You must separate the log output types by a comma when you are configuring more than one output for the same log level. See “Examples” on page 22.

Warnings!

- If you direct log output to a file on the network drive, an application does not create a snapshot log file (with the extension `*.snapshot.log`) in case it terminates abnormally.
- Directing log output to the console (by using the `stdout` or `stderr` settings) can affect application performance. Avoid using these log output settings in a production environment.

Note: The log output options are activated according to the setting of the `verbose` configuration option.

all

Default Value: No default value
Valid Values (log output types):

`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. For example:

```
all = stdout, logfile
```

Note: To ease the troubleshooting process, consider using unique names for log files that different applications generate.

alarm

Default Value: No default value
Valid Values (log output types):

`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 resides anywhere on the network, and Message Server stores the log events 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 Alarm level. The log output types must be separated by a comma when more than one output is configured. For example:

```
standard = stderr, network
```

standard

Default Value: No default value
Valid Values (log output types):

`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.

`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. For example:

```
standard = stderr, network
```

interaction

Default Value: No default value
Valid Values (log output types):

`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.

`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. For example:

```
interaction = stderr, network
```

trace

Default Value: No default value
Valid Values (log output types):

`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.

`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. For example:

```
trace = stderr, network
```

debug

Default Value: No default value
Valid Values (log output types):

`stdout` Log events are sent to the Standard output (`stdout`).

`stderr` Log events are sent to the Standard error output (`stderr`).

`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—for example:

```
debug = stderr, /usr/local/genesys/logfile
```

Note: `Debug`-level log events are never sent to Message Server or stored in the Log Database.

Log File Extensions

You can use the following file extensions to identify log files that an application creates for various types of output:

- `*.log`—Assigned to log files when you configure output to a log file. For example, if you set `standard = confservlog` for Configuration Server, it prints log messages into a text file called `confservlog.<time_stamp>.log`.
- `*.qsp`—Assigned to temporary (spool) files when you configure output to the network but the network is temporarily unavailable. For example, if you set `standard = network` for Configuration Server, it prints log messages into a file called `confserv.<time_stamp>.qsp` during the time the network is not available.
- `*.snapshot.log`—Assigned to files that contain the output snapshot when you configure output to a log file. The file contains the last log messages that an application generates before it terminates abnormally. For example, if you set `standard = confservlog` for Configuration Server, it prints the last log message into a file called `confserv.<time_stamp>.snapshot.log` in case of failure.

Note: Provide `*.snapshot.log` files to Genesys Technical Support when reporting a problem.

- `*.memory.log`—Assigned to log files that contain the memory output snapshot when you configure output to memory and redirect the most recent memory output to a file. For example, if you set `standard = memory` and `memory = confserv` for Configuration Server, it prints the latest memory output to a file called `confserv.<time_stamp>.memory.log`.

Examples

This section presents examples of a `log` section that you might configure for an application when that application is operating in production mode and in two lab modes, debugging and troubleshooting.

Production Mode Log Section

```
[log]
verbose = standard
standard = network, logfile
```

With this configuration, an application only generates the log events of the `Standard` level and sends them to Message Server, and to a file named `logfile`, which the application creates in its working directory. Genesys recommends that you use this or a similar configuration in a production environment.

Warning! Directing log output to the console (by using the `stdout` or `stderr` settings) can affect application performance. Avoid using these log output settings in a production environment.

Lab Mode Log Section

```
[log]
verbose = all
all = stdout, /usr/local/genesys/logfile
trace = network
```

With this configuration, an application generates log events of the `Standard`, `Interaction`, `Trace`, and `Debug` levels, and sends them to the standard output and to a file named `logfile`, which the application creates in the `/usr/local/genesys/` directory. In addition, the application sends log events of the `Standard`, `Interaction`, and `Trace` levels to Message Server. Use this configuration to test new interaction scenarios in a lab environment.

Failure-Troubleshooting Log Section

```
[log]
verbose = all
standard = network
all = memory
memory = logfile
memory-storage-size = 32 MB
```

With this configuration, an application generates log events of the `Standard` level and sends them to Message Server. It also generates log events of the `Standard`, `Interaction`, `Trace`, and `Debug` levels, and sends them to the memory output. The most current log is stored to a file named `logfile,` which the application creates in its working directory. Increased memory storage allows an application to save more of the log information generated before a failure...

Note: If you are running an application on UNIX, and you do not specify any files in which to store the memory output snapshot, a core file that the application produces before terminating contains the most current application log. Provide the application's core file to Genesys Technical Support when reporting a problem.

Debug Log Options

The options in this section enable you to generate `Debug` logs containing information about specific operations of an application.

x-conn-debug-open

Default Value: `0`
Valid Values:

`0`	Log records are not generated.
`1`	Log records are generated.

Changes Take Effect: After restart

Generates `Debug` log records about "open connection" operations of the application.

Warning! Use this option only when requested by Genesys Technical Support.

x-conn-debug-select

Default Value: `0`
Valid Values:

`0`	Log records are not generated.
`1`	Log records are generated.

Changes Take Effect: After restart

Generates `Debug` log records about "socket select" operations of the application.

Warning! Use this option only when requested by Genesys Technical Support.

x-conn-debug-timers

Default Value: `0`
Valid Values:

`0`	Log records are not generated.
`1`	Log records are generated.

Changes Take Effect: After restart

Generates `Debug` log records about the timer creation and deletion operations of the application.

Warning! Use this option only when requested by Genesys Technical Support.

x-conn-debug-write

Default Value: `0`
Valid Values:

`0`	Log records are not generated.
`1`	Log records are generated.

Changes Take Effect: After restart

Generates `Debug` log records about "write" operations of the application.

Warning! Use this option only when requested by Genesys Technical Support.

x-conn-debug-security

Default Value: `0`
Valid Values:

`0`	Log records are not generated.
`1`	Log records are generated.

Changes Take Effect: After restart

Generates `Debug` log records about security-related operations, such as Transport Layer Security and security certificates.

Warning! Use this option only when requested by Genesys Technical Support.

x-conn-debug-api

Default Value: `0`
Valid Values:

`0`	Log records are not generated.
`1`	Log records are generated.

Changes Take Effect: After restart

Generates `Debug` log records about connection library function calls.

Warning! Use this option only when requested by Genesys Technical Support.

x-conn-debug-dns

Default Value: `0`
Valid Values:

`0`	Log records are not generated.
`1`	Log records are generated.

Changes Take Effect: After restart

Generates `Debug` log records about DNS operations.

Warning! Use this option only when requested by Genesys Technical Support.

x-conn-debug-all

Default Value: `0`
Valid Values:

`0`	Log records are not generated.
`1`	Log records are generated.

Changes Take Effect: After restart

Generates `Debug` log records about open connection, socket select, timer creation and deletion, write, security-related, and DNS operations, and connection library function calls. This option is the same as enabling or disabling all of the previous `x-conn-debug-<op type>` options.

Warning! Use this option only when requested by Genesys Technical Support.

log-extended Section

This section must be called `log-extended`.

level-reassign-<eventID>

Default Value: Default value of log event `<eventID>`
Valid Values:

`alarm`	The log level of log event `<eventID>` is set to `Alarm`.
`standard`	The log level of log event `<eventID>` is set to `Standard`.
`interaction`	The log level of log event `<eventID>` is set to `Interaction`.
`trace`	The log level of log event `<eventID>` is set to `Trace`.
`debug`	The log level of log event `<eventID>` is set to `Debug`.
`none`	Log event `<eventID>` is not recorded in a log.

Changes Take Effect: Immediately

Specifies a log level for log event `<eventID>` that is different than its default level, or disables log event `<eventID>` completely. If no value is specified, the log event retains its default level. This option is useful when you want to customize the log level for selected log events.

These options can be deactivated with the option `level-reassign-disable`.

Warning! Use caution when making these changes in a production environment.

Depending on the log configuration, changing the log level to a higher priority may cause the log event to be logged more often or to a greater number of outputs. This could affect system performance.

Likewise, changing the log level to a lower priority may cause the log event to be not logged at all, or to be not logged to specific outputs, thereby losing important information. The same applies to any alarms associated with that log event.

In addition to the preceding warning, take note of the following:

- Logs can be customized only by release 7.6 or later applications.
- When the log level of a log event is changed to any level except `none`, it is subject to the other settings in the `[log]` section at its new level. If set to `none`, it is not logged and is therefore not subject to any log configuration.
- Using this feature to change the log level of a log changes only its priority; it does not change how that log is treated by the system. For example, increasing the priority of a log to `Alarm` level does not mean that an alarm will be associated with it.
- Each application in a High Availability (HA) pair can define its own unique set of log customizations, but the two sets are not synchronized with each other. This can result in different log behavior depending on which application is currently in primary mode.
- This feature is not the same as a similar feature in Universal Routing Server (URS) release 7.2 or later. In this Framework feature, the priority of log events are customized. In the URS feature, the priority of debug messages only are customized. Refer to the *Universal Routing Reference Manual* for more information about the URS feature.
- You cannot customize any log event that is not in the unified log record format. Log events of the `Alarm`, `Standard`, `Interaction`, and `Trace` levels feature the same unified log record format.

Example

This is an example of using customized log level settings, subject to the following log configuration:

```
[log]
verbose=interaction
all=stderr
interaction=log_file
standard=network
```

Before the log levels of the log are changed:

- Log event 1020, with default level `standard`, is output to `stderr` and `log_file`, and sent to Message Server.
- Log event 2020, with default level `standard`, is output to `stderr` and `log_file`, and sent to Message Server.
- Log event 3020, with default level `trace`, is output to `stderr`.
- Log event 4020, with default level `debug`, is output to `stderr`.

Extended log configuration section:

```
[log-extended]
level-reassign-1020=none
level-reassign-2020=interaction
level-reassign-3020=interaction
level-reassign-4020=standard
```

After the log levels are changed:

- Log event 1020 is disabled and not logged.
- Log event 2020 is output to `stderr` and `log_file`.
- Log event 3020 is output to `stderr` and `log_file`.
- Log event 4020 is output to `stderr` and `log_file`, and sent to Message Server.

level-reassign-disable

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: Immediately

When this option is set to `true`, the original (default) log level of all log events in the `[log-extended]` section are restored. This option is useful when you want to use the default levels, but not delete the customization statements.

log-filter Section

The `log-filter` section contains configuration options used to define the default treatment of filtering data in log output. This section contains one configuration option, `default-filter-type`. Refer to the chapter “Hide Selected Data in Logs” in the *Genesys 8.0 Security Deployment Guide* for complete information about this option.

log-filter-data section

The `log-filter-data` section contains configuration options used to define the treatment of filtering data in log output on a key-by-key basis. This section contains one configuration option in the form of `<key name>`. Refer to the chapter “Hide Selected Data in Logs” in the *Genesys 8.0 Security Deployment Guide* for complete information about this option.

security Section

The security section contains configuration options used to specify security elements for your system. In addition to other options that may be required by your application, this section contains the configuration option disable-rbac, which is used to enable or disable Role-Based Access Control for an application. Refer to the chapter “Role-Based Access Control” in the *Genesys 8.0 Security Deployment Guide* for complete information about this option.

sml Section

This section must be called sml.

Options in this section are defined in the Annex of the Application object, as follows:

- in Genesys Administrator—Application object > Options tab > Advanced View (Annex)
- in Configuration Manager—Application object > Properties dialog box > Annex tab

Warning! Use the first three options in this section (heartbeat-period, heartbeat-period-thread-class-<n>, and hangup-restart) with great care, and only with those applications of which support for this functionality has been announced. Failure to use these options properly could result in unexpected behavior, from ignoring the options to an unexpected restart of the application.

heartbeat-period

Default Value: None
Valid Values:

0	This method of detecting an unresponsive application is not used by this application.
3-604800	Length of timeout, in seconds; equivalent to 3 seconds–7 days.

Changes Take Effect: Immediately

Specifies the maximum amount of time, in seconds, in which heartbeat messages are expected from an application. If Local Control Agent (LCA) does not receive a heartbeat message from the application within this period, it assumes the application is not responding and carries out corrective action.

This option can also be used to specify the maximum heartbeat interval for threads registered with class zero (0). This thread class is reserved for use by the Management Layer only.

If this option is not configured or is set to zero (0), heartbeat detection is not used by this application.

heartbeat-period-thread-class-<n>

Default Value: None
Valid Values:

0	Value specified by heartbeat-period in application is used.
3-604800	Length of timeout, in seconds; equivalent to 3 seconds–7 days.

Changes Take Effect: Immediately

Specifies the maximum amount of time, in seconds, in which heartbeat messages are expected from a thread of class <n> registered by an application. If a heartbeat message from the thread is not received within this period, the thread is assumed to be not responding, and therefore, the application is unable to provide service.

If this option is not configured or is set to zero (0), but the application has registered one or more threads of class <n>, the value specified by the value of heartbeat-period for the application will also be applied to these threads.

Refer to application-specific documentation to determine what thread classes, if any, are used.

hangup-restart

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

If set to true (the default), specifies that LCA is to restart the unresponsive application immediately, without any further interaction from Solution Control Server.

If set to false, specifies that LCA is only to generate a notification that the application has stopped responding.

suspending-wait-timeout

Default Value: 10
Valid Values: 5-600
Changes Take Effect: Immediately

Specifies a timeout (in seconds) after the Stop Graceful command is issued to an application during which the status of the application should change to Suspending if the application supports graceful shutdown. If the status of the application does not change to Suspending before the timeout expires, it is assumed that the application does not support graceful shutdown, and it is stopped ungracefully.

Use this option if you are unsure whether the Application supports graceful shutdown.

Note: Genesys recommends that you do not set this option for any Management Layer component (Configuration Server, Message Server, Solution Control Server, or SNMP Master Agent) or any DB Server. These components by definition do not support graceful shutdown, so this option is not required.

common Section

This section must be called `common`.

enable-async-dns

Default Value: `off`
Valid Values:

`off`	Disables asynchronous processing of DNS requests.
`on`	Enables asynchronous processing of DNS requests.

Changes Take Effect: Immediately

Enables the asynchronous processing of DNS requests such as, for example, host-name resolution.

Warnings!
- Use this option only when requested by Genesys Technical Support.
- Use this option only with T-Servers.

rebind-delay

Default Value: `10`
Valid Values: `0`–`600`
Changes Take Effect: After restart

Specifies the delay, in seconds, between socket-bind operations that are being executed by the server. Use this option if the server has not been able to successfully occupy a configured port.

Warning! Use this option only when requested by Genesys Technical Support.

Changes from 7.6 to 8.0

Table 1 on page 32 provides all the changes to common configuration options between release 7.6 and the latest 8.0 release.

Table 1: Common Configuration Option Changes from 7.6 to 8.0

Option Name	Option Values	Type of Change	Details
log Section			
expire	Increased range of value	Modified	See description on page 13.
log-filter Section			
default-filter-type	Additional option values	Modified	See description on page 28.
log-filter-data Section			
<key name>	Additional option values	Modified	See description on page 28.
security Section (New Section)			
disable-rbac	true, false	New	See description on page 29.
sml Section			
heartbeat-period	3–604800 seconds	New	See description on page 29.
heartbeat-period-thread-class-<n>	3–604800 seconds	New	See description on page 30.
hangup-restart	true, false	New	See description on page 30.
suspending-wait-timeout	5-600	New	See description on page 30.

Chapter

2

DB Server Configuration Options

This chapter describes configuration options and a configuration file for DB Server.

This chapter contains the following sections:

DB Server also supports the options described in Chapter 1 on page 11.

Setting Configuration Options

Unless specified otherwise, set DB Server configuration options in the Options of the DB Server Application object, using one of the following navigation paths:

- In Genesys Administrator—DB Server Application object > Options tab > Advanced View (Options)
- In Configuration Manager—DB Server Application object > Properties dialog box > Options tab

Warning! Configuration section names, configuration option names, and predefined option values are case-sensitive. Type them in Genesys Administrator or Configuration Manager exactly as they are documented in this chapter.

Mandatory Options

Table 2 lists the DB Server options for which you must provide values; otherwise, DB Server will not start. The options are listed by section.

Table 2: Mandatory Options

Option Name	Default Value	Details
DB Server Section		
host	No default value	Not used when configuring a DB Server Application object in the Configuration Database. A value for this option must be specified when configuring DB Server via a configuration file. See the description on page 35.
port	No default value	Not used when configuring a DB Server Application object in the Configuration Database. A value for this option must be specified when configuring DB Server via a configuration file. See the description on page 35.
dbprocess_name	No default value	See the description on page 36.
[a DB client process name option]	No default value	The option name depends on the DBMS type: `db2_name`, `informix_name`, `msql_name`, `oracle_name`, `postgre_name`, or `sybase_name`. See the descriptions beginning on page 37.

dbserver Section

This section must be called `dbserver`.

Starting with release 7.5, DB Server can communicate with its clients via multiple ports. One port must always be specified in the main DB Server section `dbserver`. To configure additional ports, use sections `dbserver-n` as described in “Multiple Ports Configuration” on page 40.

Note: In addition to the configuration options listed here, this section contains the option `transport`. Refer to the section “TLS Configuration” in the *Genesys 8.0 Security Deployment Guide* for complete information about this option.

host

Default Value: No default value
Valid Values: Any valid name or IP address
Changes Take Effect: After restart

The name or IP address of the host computer on which DB Server is installed.

Note: This configuration option is not used when configuring a DB Server `Application` object in the Configuration Layer. A value for this option must be specified when configuring DB Server via a configuration file.

port

Default Value: No default value
Valid Values: Any valid TCP/IP port from `2000`–`9999`
Changes Take Effect: After restart

Specifies the port number DB Server uses to establish client connections.

Note: This configuration option is not used when configuring a DB Server `Application` object in the Configuration Layer. A value for this option must be specified when configuring DB Server via a configuration file.

management-port

Default Value: `4051`
Valid Values: Any valid TCP/IP port
Changes Take Effect: After restart

Specifies the TCP/IP port DB Server reserves for connections established by its SNMP (Simple Network Management Protocol) Option Management Client.

connect_break_time

Default Value: `1200`
Valid Values: Any positive integer
Changes Take Effect: After restart

Specifies a timeout, in seconds, after which DB Server closes a connection to a DB client if DB Server could not send a request to the client. Do not set this option too small; if a value of 1 to 10 seconds is set, for example, network delay might prevent a request delivery. Genesys recommends that you set this option to a value equal to or greater than 60.

dbprocess_name

Default Value: No default value
Valid Values: Use one of the following, based on your DBMS.

dbclient_db2	For DB2
dbclient_informix	For Informix
dbclient_msql	For Microsoft SQL
dbclient_oracle	For Oracle
dbclient_postgre	For PostgreSQL
dbclient_sybase	For Sybase

Changes Take Effect: After restart

Specifies the type of DB client process, based on the DBMS being used. This option works with dbprocesses_per_client and the corresponding <DBMS>_name option (that is, db2_name, informix_name, msql_name, oracle_name, postgre_name, or sybase_name).

Note: Only enable this option for compatibility with previous releases of client applications (5.1, 6.0, or 6.1).

dbprocesses_per_client

Default Value: 1
Valid Values: Any positive integer from 1–255
Changes Take Effect: After restart

Note: Genesys recommends using the default value (1) for this option unless instructed otherwise by Technical Support or by the User's Guide of the applicable Genesys solution. Changing the default value (1) of this option may cause data loss.

Specifies the number of database client processes that DB Server's main process creates for each client if a user client does not make an explicit request. This option prioritizes client access to the database. For example, if multiple processes per client are set, DB Server spawns another child process if needed. This effectively gives the client application more of the database's processing time. See documentation for a particular client application to verify whether that application supports the Multiple Processes mode. If unsure of the appropriate number, set this option to 1. Increasing the value up to 4 increases performance; more than 4 does not increase performance.

db2_name

Default Value: `./dbclient_db2`
Valid Values:

`./dbclient_db2`	Strongly recommended.
`./dbclient_db2_32`	Use this value only if it is clearly indicated that you use the 32-bit DB Server client.
`./dbclient_db2_64`	Use this value only if it is clearly indicated that you use the 64-bit DB Server client.

Changes Take Effect: After restart

Specifies the name of the DB Server client process for the DB2 server. **This option is required for DB2 databases.** Also see `dbprocess_name`.

informix_name

Default Value: `./dbclient_informix`
Valid Values: `./dbclient_informix`
Changes Take Effect: After restart

Specifies the name of the DB Server client process for the Informix server if present. **This option is required for Informix databases.** Also see `dbprocess_name`.

msql_name

Default Value: `./dbclient_msql`
Valid Values: `./dbclient_msql`
Changes Take Effect: After restart

Specifies the name of the DB Server client process for the Microsoft SQL server. **This option is required for MSSQL databases.** Also see `dbprocess_name`.

oracle_name

Default Value: `./dbclient_oracle`
Valid Values:

`./dbclient_oracle`	Strongly recommended.
`./dbclient_oracle_32`	Use this value only if it is clearly indicated that you use the 32-bit DB Server client.
`./dbclient_oracle_64`	Use this value only if it is clearly indicated that you use the 64-bit DB Server client.

Changes Take Effect: After restart

Specifies the name of the DB Server client process for the Oracle server if present. **This option is required for Oracle databases.** Also see `dbprocess_name`.

postgre_name

Default Value: `./dbclient_postgre`
Valid Values: `./dbclient_postgre`
Changes Take Effect: After restart

Specifies the name of the DB Server client process for the PostgreSQL server. **This option is required for PostgreSQL databases.** Also see `dbprocess_name`.

sybase_name

Default Value: `./dbclient_sybase`
Valid Values: `./dbclient_sybase`
Changes Take Effect: After restart

Specifies the name of the DB Server client process for the Sybase server if present. **This option is required for Sybase databases.** Also see `dbprocess_name`.

client_stop_timeout

Default Value: `30`
Valid Values: `0` or any positive integer
Changes Take Effect: After restart

Specifies the interval, in seconds, that DB Server waits for a client to stop before DB Server terminates the DB client process.

db-request-timeout

Default Value: `0`
Valid Values: `0–604800` (in seconds, equivalent to 0 seconds–7 days)
Changes Take Effect: After DB Server reconnects to the database; no restart is required.

Specifies the period of time, in seconds, that it should take one DBMS request to be completed. If a request to the DBMS takes longer than this period of time, the database client process stops executing, and DB Server interprets this as a DBMS failure.

DB Server uses this option for all started database client processes, unless overwritten by the value of the option `db-request-timeout` in the `Annex` of a Database Access Point (DAP) object.

If this option is set to the default value of `0` (zero), no timeout is used.

Note: This option applies only to DB Servers that provide access to databases other than the Configuration Database. In other words, do not use this option for the Configuration DB Server.

verbose

Default Value: 3
Valid Values:

0	DB Server writes no debug messages.
1	DB Server writes errors and SQL statements.
2	DB Server writes information about all messages it has received and sent.
3	DB Server writes debug messages at the most detailed level.

Changes Take Effect: After restart

Sets the level of detail with which DB Server writes the debug messages. The option is configured in the dbserver section and is enabled only when the verbose option in the log section is set to either all or debug. DB Server writes the debug messages to a log output specified for the all and/or debug log output options.

Note: Although named the same, the verbose options in the log and dbserver sections are responsible for different types of log settings.

dbprocess_number

Default Value: 255
Valid Values:

0	Does not impose restrictions to the number of running DB Client processes
1 and above	Sets maximum number of simultaneously running DB Client processes

Changes Take Effect: After restart

Sets the maximum limit for the number of simultaneously running DB Client processes.

stored_proc_result_table

Default Value: No default value
Valid Values: Any valid table name
Changes Take Effect: After restart

Used by earlier versions of DB Server that did not directly retrieve output data from stored procedures. This option specifies the name of a table that you design, to which a stored procedure that you have created writes output data (the maximum allowed size of an output parameter from a stored procedure is 2000 B). DB Server then retrieves the data stored in the specified table and sends it to the user application. Using a result table can slow down DB Server, because each stored procedure call causes an additional select statement.

tran_batch_mode

Default Value: off
Valid Values: on, off
Changes Take Effect: After restart

Valid only for Microsoft SQL and Sybase databases. If set to on, DB Server executes all transactions as SQL batches, which increases performance for insert and update statements.

Note: Genesys recommends using the default value (off) for this option unless instructed otherwise by Technical Support or by the User's Guide of the applicable Genesys solution.

Ica Section

This section must be called lca.

lcaport

Default Value: 0
Valid Values: Any valid port from 2000–9999
Changes Take Effect: After restart

Specifies the port of the Local Control Agent (LCA) application. When the option value is set to 0, DB Server does not establish a connection to LCA. Otherwise, DB Server establishes a connection to LCA and can be controlled by the Management Layer. Only use this option when configuring DB Server as an independent server (that is, for the DB Server that provides access to the Configuration Database).

Multiple Ports Configuration

Starting with release 7.5, any DB Server configured via a configuration file (namely, one that is not a client of the Configuration Database such as the Configuration DB Server) can communicate with its clients via multiple ports. One listening port must always be specified in the main DB Server section dbserver. To configure additional listening ports, a new section called dbserver-*n* has been introduced, where *n* is a nonzero consecutive number.

Each dbserver-*n* section contains the configuration options for a single additional port. The number of dbserver-*n* sections corresponds to the number of additional ports. The order in which these sections appear in the configuration file is non-essential. To configure a secure connection, specify the certificate settings in the transport option in the section for that port. See “Sample Configuration File” on page 41. Refer to the “TLS Configuration” section in the *Genesys 8.0 Security Deployment Guide* for detailed information about the transport option.

port

Default Value: No default value
Valid Values: Any valid TCP/IP port from 2000–9999
Changes Take Effect: After restart

Specifies the port number DB Server uses to establish client connections.

DB Server Configuration File

Only the DB Server that provides access to the Configuration Database must be configured in a configuration file. This DB Server reads its configuration settings from the configuration file as opposed to reading them from the Configuration Database. DB Servers that provide access to other databases must be configured as Application configuration objects in the Configuration Layer.

Warning! When DB Server is configured via a configuration file, changes to its options take effect after DB Server is restarted.

The configuration file can contain the DB Server, Log, and LCA sections.

The default name of the DB Server section is dbserver. This section contains configuration information about DB Server: DB Server settings and the type of the DBMS with which DB Server operates. The dbserver section allows you to configure one listening port. Starting from release 7.5, you can configure multiple listening ports for DB Server, where each additional port is configured in a separate dbserver-*n* section. See “Multiple Ports Configuration” on page 40 for details.

The default name of the Log section is log. This section contains configuration information about the log.

The default name of the LCA section is lca. This section contains one option that enables the Management Layer to control the DB Server that provides access to the Configuration Database—that is, the DB Server that runs as an independent server.

Sample Configuration File

The following is a sample configuration file for DB Server.

```
[dbserver]
host = localhost
port = 4040
management-port = 4581
```

```
dbprocesses_per_client = 1
dbprocess_name = ./dbclient_sybase
oracle_name = ./dbclient_oracle
informix_name = ./dbclient_informix
sybase_name = ./dbclient_sybase
db2_name = ./dbclient_db2
postgre_name = ./dbclient_postgre
connect_break_time = 1200
tran_batch_mode = off

[dbserver-1]
port = 4333
transport= tls=1; certificate=f894 a455 3a5e d41e 1dc3 6449 d7f5

[log]
verbose = standard
all = stderr

[lca]
lcaport = 4999
```

Changes from 7.6 to 8.0

Table 3 provides all the changes to DB Server options between release 7.6 and the latest 8.0 release.

Table 3: DB Server Configuration Option Changes from 7.6 to 8.0

Option Name	Option Values	Type of Change	Details
dbserver Section			
dbprocess_name	dbclient_postgre	New value	See description on page 38.
	dbclient_db2, dbclient_informix, dbclient_msql, dbclient_oracle, dbclient_sybase	Modified values	Removed ./ from values. Documented incorrectly in previous version of this document. See description on page 36.
db2_name	./dbclient_db2_32, ./dbclient_db2_64	New values	See description on page 37.
	./dbclient_db2	Modified values	Documented incorrectly in previous version of this document.

Table 3: DB Server Configuration Option Changes from 7.6 to 8.0 (Continued)

Option Name	Option Values	Type of Change	Details
informix_name	./dbclient_informix	Modified values	Documented incorrectly in previous version of this document. See description on page 37.
msql_name	./dbclient_msql	Modified values	Documented incorrectly in previous version of this document. See description on page 37.
oracle_name	./dbclient_oracle_32, ./dbclient_oracle_64	New values	See description on page 37.
	./dbclient_oracle	Modified values	Documented incorrectly in previous version of this document.
postgre_name	./dbclient_postgre	New	See description on page 38.
sybase_name	./dbclient_sybase	Modified values	Documented incorrectly in previous version of this document. See description on page 38.
db-request-timeout	0–604800 seconds	New	See description on page 38.

Chapter

3 Database Access Point Configuration Options

This chapter describes configuration options for a Database Access Point.

This chapter contains the following sections:

Setting Configuration Options

Unless specified otherwise, set Database Access Point configuration options using one of the following navigation paths:

- In Genesys Administrator—Database Access Point Application object > Configuration tab > DB Info section > Query Timeout. This field sets the option value in the Annex.
- In Configuration Manager—Database Access Point Application object > Properties dialog box > DB info tab > Query Timeout. This field sets the option value in the Annex.

Note: In Genesys Administrator, you can also set options directly in the Annex of the Database Access Point Application object.

Warning! Configuration section names, configuration option names, and predefined option values are case-sensitive. Type them in Genesys Administrator or Configuration Manager exactly as they are documented in this chapter.

Mandatory Options

You do not have to configure any options for a Database Access Point.

default Section

This section must be called `default`.

db-request-timeout

Default Value: `0`
Valid Values: `0`–`604800` (in seconds, equivalent to 0 seconds–7 days)
Changes Take Effect: After DB Server reconnects to the database; no restart is required.

Specifies the period of time, in seconds, that it should take one DBMS request to be completed. If a request to the DBMS takes longer than this period of time, the database client process stops executing, and DB Server interprets this as a DBMS failure.

This option redefines the value of the option `db-request-timeout` specified by DB Server, for only to the database client process used for access to the database for which this Database Access Point is configured to provide the access.

If this option is set to the default value of `0` (zero), the value of the option `db-request-timeout` configured in DB Server is used.

Set this option in the `Query Timeout` field in the properties of the Database Access Point `Application` object.

Changes from 7.6 to 8.0

Table 4 provides all the changes to Database Access Point options between release 7.6 and the latest 8.0 release.

Table 4: Database Access Point Configuration Option Changes from 7.6 to 8.0

Option Name	Option Values	Type of Change	Details
	default Section (new section)		
db-request-timeout	0–604800 seconds	New	See description on page 46.

Chapter

4 Configuration Server Configuration Options

This chapter describes configuration options and a configuration file for Configuration Server, and includes the following sections:

Setting Configuration Options

You set Configuration Server configuration options in one of three ways:

- Using a configuration file for startup options
- Using Genesys Administrator
- Using Configuration Manager

Warning! Configuration section names, configuration option names, and predefined option values are case-sensitive. Type them in the configuration file, Genesys Administrator, or Configuration Manager exactly as they are documented in this chapter.

Using the Configuration File for Startup Options

Using a text editor, enter Configuration Server startup options directly in the configuration file. See “Startup Options in Configuration File” on page 48 for descriptions of the startup options.

Using Genesys Administrator for Runtime Options

In Genesys Administrator, set Configuration Server configuration options in the `Advanced View (Options)` view of the `Options` tab of the Configuration Server `Application` object.

See "Runtime Options in Configuration Database" on page 56 for descriptions of the runtime options. Refer to *Framework 8.0 Genesys Administrator Help* for additional information about the `Options` tab, and how to manage configuration options on it.

Using Configuration Manager for Runtime Options

In Configuration Manager, set Configuration Server configuration options in the `Options` tab of the `Application` object, unless specified otherwise. See "Runtime Options in Configuration Database" on page 56 for descriptions of the runtime options.

Startup Options in Configuration File

You must manually enter these options in the Configuration Server configuration file `confserv.cfg` (on Windows) or `confserv.conf` (on UNIX).

Mandatory Startup Options

Table 5 lists the Configuration Server options for which you must provide values; otherwise, Configuration Server will not start. The options in the table are listed by section.

Table 5: Mandatory Options

Option Name	Default Value	Details
Configuration Server Section		
port	No default value	Used only during the first start of Configuration Server with an initialized database. Upon subsequent restarts, Configuration Server reads the port information from its Application object in the Configuration Database and ignores the setting of the `port` option in the configuration file. See the description on page 49.
server	No default value	See the description on page 50.
Configuration Database Section		
host	No default value	See the description on page 52.

Table 5: Mandatory Options (Continued)

Option Name	Default Value	Details
port	No default value	See the description on page 52.
dbengine	No default value	See the description on page 52.
dbname	No default value	You must specify a value for this option unless `dbengine=oracle`. See the description on page 52.
dbserver	No default value	See the description on page 52.
username	No default value	See the description on page 53.
password	No default value	See the description on page 53.

confserv Section

This section contains the configuration options of Configuration Server.

This section must be called `confserv`.

Note: In addition to the options described here, this section also contains the following options:

- `allow-empty-password` and `allow-external-empty-password` determine if Configuration Server accepts or rejects empty (blank) passwords.
- `encryption` enables the Configuration Database password to be encrypted.
- `last-login` and `last-login-synchronization` control the use of the Last Logged-In User feature on the Configuration Server and its clients.

For complete information about these options, refer to the *Genesys 8.0 Security Deployment Guide.*

port

Default Value: No default value
Valid Values: Any valid TCP/IP port
Changes Take Effect: After restart

Specifies the TCP/IP port that Configuration Server clients use to connect to this server.

Note: The `port` option is used only during the first start of Configuration Server with an initialized database. Upon subsequent restarts, Configuration Server reads the port information from its `Application` object in the Configuration Database and ignores the setting of the `port` option in the configuration file.

management-port

Default Value: No default value
Valid Values: Any valid TCP/IP port
Changes Take Effect: After restart

Specifies the TCP/IP port that management software uses to monitor and control the operation of Configuration Server. If not specified, management agents cannot monitor and control the operation of Configuration Server. You cannot set this option to the value specified for the option `port`.

client-response-timeout

Default Value: `600`
Valid Values: Any positive integer
Changes Take Effect: After restart

Sets the interval, in seconds, that Configuration Server waits for any activity on a socket before closing a client's connection.

server

Default Value: No default value
Valid Values: Any character string
Changes Take Effect: After restart

Specifies the name of the Configuration Database section in the configuration file; see "Configuration Database Section" on page 51. You must specify a value for this option.

objects-cache

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

Specifies if Configuration Server uses internal caching. When set to `true`, Configuration Server caches objects requested by client applications. This is the default behavior of Configuration Server in previous releases. When this option is set to `false`, the objects are not cached, reducing the amount of memory used by Configuration Server.

Note: Disabling the cache may increase the load on Configuration Server during client application registration. Use this option with care.

force-reconnect-reload

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

When this option is set to `true,` Configuration Server checks the table `cfg_refresh` when switching from backup to primary mode, or when reconnecting to the database. If the field `notify_id` is different, Configuration Server disconnects all clients, closes all ports, reloads the configuration data, and then opens the ports again. This verification is done to ensure consistency of configuration information between the database and its image in Configuration Server.

disable-vag-calculation

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

Specifies whether Configuration Server calculates Virtual Agent Groups for existing and newly-created objects for the Application in which it is configured.

To manage the calculation of Virtual Agent Groups by primary and backup Configuration Servers before and after switchovers, you must set this option to `true` for both the primary and backup Configuration Servers. Set it in their corresponding configuration files. Then stop and restart both Configuration Servers. You must do this each time you change this option to ensure the accuracy of the contents of the Virtual Agent Group.

When set to `false`, the contents of the Virtual Agent Groups are not visible in Genesys graphical user interface applications.

Configuration Database Section

The Configuration Database section name is specified by the option `server` on page 50. This section contains information about the Configuration Database and DB Server that Configuration Server uses to access this database.

This option must be set in the configuration file `confserv.cfg` (on Windows) or `confserv.conf` (on UNIX).

Note: In addition to the configuration options listed here, this section contains the option `transport`. Refer to the section “TLS Configuration” in the *Genesys 8.0 Security Deployment Guide* for complete information about this option.

host

Default Value: No default value
Valid Values: Any valid host name
Changes Take Effect: After restart

Specifies the host where DB Server is running. You must specify a value for this option.

port

Default Value: No default value
Valid Values: Any valid TCP/IP port
Changes Take Effect: After restart

Specifies the TCP/IP port of the DB Server through which the Configuration Database is accessed. You must specify a value for this option.

dbengine

Default Value: No default value
Valid Values: `oracle, sybase, informix, mssql, db2, postgre`
Changes Take Effect: After restart

Specifies the type of DBMS that handles the Configuration Database. You must specify a value for this option.

dbname

Default Value: No default value
Valid Values: Any database name
Changes Take Effect: After restart

Specifies the name of the Configuration Database to be accessed as specified in the DBMS that handles this database. You must specify a value for this option unless `dbengine=oracle`. For Sybase, Informix, DB2, Microsoft SQL, and PostgreSQL, this value is the name of the database where the client will connect.

dbserver

Default Value: No default value
Valid Values: Any valid entry name
Changes Take Effect: After restart

Specifies the name or alias identifying the DBMS that handles the Configuration Database. The value of this option is communicated to DB Server so that it connects to the correct DBMS:

- For Sybase, this value is the server name stored in the Sybase interface file.
- For Oracle, the value is the name of the Listener service.
- For Informix, this value is the name of SQL server, specified in the `sqlhosts` file.

- For Microsoft SQL, set this value to the SQL server name (usually the same as the host name of the computer where Microsoft SQL runs).
- For DB2, set this value to the name or alias-name of the database specified in the db2 client configuration.
- For PostgreSQL, set this value to the SQL server name (usually the same as the host name of the computer where PostgreSQL runs).

username

Default Value: No default value
Valid Values: Any character string
Changes Take Effect: After restart

Specifies the user name established in the SQL server to access the Configuration Database. You must specify a value for this option.

password

Default Value: No default value
Valid Values: Any character string
Changes Take Effect: After restart

Specifies the password established in the SQL server to access the Configuration Database. You must specify a value for this option.

Note: The `password` option can only be specified in the configuration file. It is not visible in Genesys Administrator or Configuration Manager.

server

Default Value: No default value
Valid Values: Any character string
Changes Take Effect: After restart

Specifies the section name in the configuration file that describes the DB Server to be contacted if attempts to connect to the DB Server specified in this section fail. If not specified, Configuration Server attempts to reconnect to the DB Server described in this section.

reconnect-timeout

Default Value: `10`
Valid Values: Any positive integer
Changes Take Effect: After restart

Specifies the time interval, in seconds, between attempts to connect to DB Server(s).

response-timeout

Default Value: `600`
Valid Values: Any positive integer

Changes Take Effect: After restart

Specifies the time interval, in seconds, Configuration Server waits for a response from DB Server. If this timeout expires, Configuration Server generates log event 21-24402. Refer to *Framework 8.0 Combined Log Events Help* for a full description of this log event.

addp

Default Value: `off`
Valid Values:

`off`	Turns this feature off
`on`	Activates the Advanced Disconnect Detection Protocol

Changes Take Effect: After restart

Determines whether the Advanced Disconnect Detection Protocol (ADDP) feature is activated. If you specify the value `off,` or if this option is not present, this feature is not active. If you specify the value `on`, you must also specify values for the `addp-timeout` and `addp-trace` options.

addp-timeout

Default Value: `10`
Valid Values: Any integer from `1`–`3600`
Changes Take Effect: After restart

Specifies the time interval, in seconds, that this Configuration Server waits for a response from DB Server after sending a polling request. Applicable only if the value of the `addp` option is `on`.

addp-trace

Default Value: `off`
Valid Values:

`off`	Neither DB Server or Configuration Server are sending ADDP `ping` messages (ADDP is suspended).
`on`	DB Server and Configuration Server are sending ADDP `ping` messages to each other.

Changes Take Effect: After restart

Determine whether ADDP messages are actually sent between DB Server and Configuration Server. Applicable only if the value of the `addp` option is `on`.

log Section

Configuration Server also supports the common log options described in “log Section” on page 12. The value of any of these options values set in the configuration file apply during startup, and will override any values configured in the Configuration Database. You can change the value of any log option in runtime using Genesys Administrator or Configuration Manager.

soap Section

This section contains information about the Simple Object Access Protocol (SOAP) port that clients use to access Configuration Server.

Warning! SOAP functionality is restricted to certain environments.

This section must be called `soap`.

port

Default Value: No default value
Valid Values: Any valid TCP/IP port
Changes Take Effect: After restart

Specifies the SOAP port that clients use to connect to Configuration Server.

debug

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

Specifies whether Configuration Server prints SOAP port communication messages into its log.

client_lifespan

Default Value: `600`
Valid Values: Any positive integer
Changes Take Effect: After restart

Specifies the time, in seconds, that Configuration Server keeps information about a closed SOAP connection (particularly, the session ID—that is, a value of a Hypertext Transfer Protocol (HTTP) cookie). A client that connects within this time interval and uses the existing session ID is exempt from the authentication check. Configuration Server treats this client connection as a continued HTTP session.

hca Section

This section controls the change tracking, or History of Changes Adapter (HCA), functionality of Configuration Server.

This section must be called `hca`.

schema

Default Value: `none`
Valid Values:

`none`	HCA functionality is disabled.
`snapshot`	Configuration Server stores the most current state of certain objects and object associations, for the objects that still exist, or the last state of certain objects and object associations, for the objects that have been deleted from the database.
`journal`	Configuration Server stores the most current state of certain objects and object associations, and all intermediate states the objects have gone through.

Changes Take Effect: After restart

Specifies whether HCA functionality in Configuration Server is enabled, and if so, in which mode HCA currently operates. When enabled, Configuration Server stores intermediate states of certain objects in the Configuration Database and allows those of its clients that support this functionality to requests those states. The set of objects whose information is stored is pre-defined. Refer to the *Framework 8.0 Deployment Guide* for more information.

This option can only be set in the configuration file `confserv.cfg` (on Windows) or `confserv.conf` (on UNIX).

Warning! Using HCA functionality is highly resource-demanding. If you do not have applications using HCA functionality, do not change the default value. If you have applications using HCA functionality, consider disabling this option temporarily when you perform large changes to the Configuration Database.

Runtime Options in Configuration Database

The options in this section are set in the Configuration Server `Application` object using Genesys Administrator (on the `Options` tab) or Configuration Manager (on the `Options` or `Annex` tab).

confserv Section

This section contains the configuration options of Configuration Server.

This section must be called `confserv`.

encoding

Default Value: `UTF-8`
Valid Values: `UTF-8, UTF-16, ASCII, ISO-8859-1, ISO-8859-2, ISO-8859-3, ISO-8859-4, ISO-8859-5, ISO-8859-6, ISO-8859-7, ISO-8859-8, ISO-8859-9, ebcdic-cp-us, ibm1140, gb2312, Big5, koi8-r, Shift_JIS, euc-kr`
Changes Take Effect: Immediately

Sets the UCS (Universal Character Set) transformation format (such as, UTF-8, UTF-16, Shift_JIS, and so forth) that Configuration Server uses when exporting configuration data into an XML (Extensible Markup Language) file. The Configuration Import Wizard (CIW) must initiate the export operation. If the operating system settings do not support the specified value, Configuration Server uses the default value.

Specify the UTF-8 encoding format unless you are using wide-character codesets (such as Chinese, Japanese, Korean).

locale

Default Value: No default value
Valid Values: Any valid locale name or abbreviation
Changes Take Effect: Immediately

On Windows operating systems, specifies the locale setting that Configuration Server uses when transforming configuration object information from internal representation for export to an XML file. If you do not specify the option, Configuration Server uses the default operating system setting.

Select values for this option from the official Microsoft locale list. For example, for English, specify `english` or `eng`; for Japanese, specify `japan` or `jpn`; and so forth.

Note: The specified `locale` value must be supported by your operating system.

security Section

The `security` section contains configuration options used to configure default access privileges for new users. This section contains one configuration option, `no-default-access`. Refer to the chapter “No Default Access for New Users” in the *Genesys 8.0 Security Deployment Guide* for complete information about this option.

history-log Section

This section controls the History Log functionality during runtime. Refer to the *Framework 8.0 Deployment Guide* for more information about the History Log.

This section must be called `history-log`. This section is not created automatically; you must create it manually.

all

Default Value: `histlog`
Valid Values:

<any string value>	Specifies a full path to the history log database file including the filename without the extension. Configuration Server appends the extension .hdb.
`:memory:`	Stores the History Log in memory. Use this value to help improve system performance.

Changes Take Effect: After restart

Specifies where the history log database file is stored.

Warning! Genesys recommends that you store the history log file locally rather than on the network. Configuration Server opens a history log file in locking mode which may not be permitted in certain network configurations. Therefore, if you specify a path to a history log file located on the network, Configuration Server may issue an error message and disable the history log functionality.

expiration

Default Value: `30`
Valid Values: `1`–`30`
Changes Take Effect: Immediately

Specifies the maximum number of days the records of configuration updates will be kept in the history log database before they are deleted.

client-expiration

Default Value: `1`
Valid Values: `1`–`30`
Changes Take Effect: Immediately

Specifies the maximum number of days the records of client sessions will be kept in the history database before they are deleted. Also determines the time interval at which Configuration Server will check for expiration of records of both configuration updates and client sessions.

max-records

Default Value: `1000`
Valid Values: `1`–`1000`
Changes Take Effect: Immediately

Specifies the maximum number of records Configuration Server will send to a client in response to a history log data request.

active

Default Value: `true`
Valid Values: `true, false`
Changes Take Effect: Immediately

Turns the history log on and off. The value of this option can only be changed at runtime via the Configuration Server `Application` object properties. When Configuration Server is started, it automatically turns the history log on regardless of the previous setting of this option, and sets this option to `true`.

Refer to the *Framework 8.0 Deployment Guide* for more information on History Log configuration details.

failsafe-store-processing

Default Value: `true`
Valid Values:

`true`	Ensures that the history log database is preserved if both Configuration Server and the operating system fail.
`false`	Ensures that the history log database is preserved if only Configuration Server fails. The history log database may not be wholly preserved if operating system fails.

Changes Take Effect: Immediately

Specifies the scope of internal history log database protection when compared to system performance.

When this option is set to `true`, history log operations ensure that the history log database is preserved if both Configuration Server and the operating system fail. However, this is CPU-intensive.

When this option is set to `false`, history log operations ensure that the history log database is preserved if only the Configuration Server fails. If the operating system fails, the history log database may not be wholly preserved. However, this operation has a lesser impact on system performance.

Use this option when the volume of updates is sufficient to impact system performance, and when the impact is greater than the risk of losing some information in the history log database.

Configuration Server Configuration File

The configuration options described in this chapter must be specified in the configuration file of Configuration Server. The configuration file contains the Configuration Server, Configuration Database, HCA, and Log sections, and may contain an additional section called SOAP.

The name of the Configuration Server section is `confserv`. This section contains the configuration options of Configuration Server. In addition, the server configuration option in this section specifies the name of the Configuration Database section.

By default, the Configuration Database section does not have a name. The section name must be the same as the value of the server configuration option, specified in the confserv section. The Configuration Database section contains information about the Configuration Database and about the DB Server used to access this database.

Note: If you plan to use one or more DB Servers as a backup, you must configure the same number of Configuration Database sections in the configuration file. The server configuration option within a given Configuration Database section must specify the name for the subsequent Configuration Database section.

The name of the Log section is log. This section contains configuration information about the log.

The name of the History of Changes Adapter (change tracking) section is hca. This section controls Configuration Server's change-tracking functionality.

The name of the SOAP section is soap. This section contains information about the Simple Object Access Protocol (SOAP) port that clients can use to access Configuration Server.

Note: Starting with release 7.0.1, Configuration Server supports the RADIUS server external authentication system. In release 7.1, Configuration Server adds support of external authentication using LDAP. For information about enabling external authentication in Configuration Server, refer to the *Framework 8.0 External Authentication Reference Manual.*

Sample Configuration File

The following is a sample configuration file for Configuration Server:

```
[confserv]
port = 2020
management-port = 2021
server = dbserver
objects-cache = true
encryption = false
encoding = utf-8

[log]
verbose = standard
all = stderr

[hca]
```

```
schema = none

[soap]
port = 5555

[dbserver]
host = db-host
port = 4040
dbengine = mssql
dbserver = db-config
dbname = config
username = user1
password = user1pass
reconnect-timeout = 10
response-timeout = 600
transport = tls=1;certificate = 9a ab db c4 02 29 3a 73 35 90 b0 65 2f
3d 32 b5 1e aa f1 7c
```

Application Parameter Options

Set options in this section in the Application Parameters of the port's properties, using one of the following navigation paths:

- In Genesys Administrator—Configuration Server Application object > Configuration tab > Server Info section > Listening Ports > Port Info
- In Configuration Manager—Configuration Server Application object > Properties dialog box > Server Info tab > Port Properties dialog box > Advanced tab

Application Parameter options are not associated with a configuration option section, and do not appear in the options or annex of a Configuration Server Application object.

backlog

Default Value: 5
Valid Values: Any positive integer greater than 4
Changes Take Effect: Immediately

Specifies the maximum number of outstanding connection requests from clients. When the maximum is reached, Configuration Server does not accept a new request until an outstanding request is processed.

Warning! This option is for advanced use only, and is logged only in Debug level logs. Use this option only when requested by Genesys Technical Support.

Changes from 7.6 to 8.0

Table 6 provides all the changes to Configuration Server options between release 7.6 and the latest 8.0 release.

Table 6: Configuration Server Configuration Option Changes from 7.6 to 8.0

Option Name	Option Values	Type of Change	Details
confserv Section			
last-login	true, false	New	Refer to "Last Logged-In User" in the *Genesys 8.0 Security Deployment Guide*.
last-login-synchronize	true, false	New	
allow-external-empty-password	true, false	New	Refer to "User Passwords" in the *Genesys 8.0 Security Deployment Guide*.
objects-cache	true, false	New	See description on page 50.
disable-vag-calculation	true, false	New option added in 7.6	See description on page 51. New option added in 7.6; not documented.
Configuration Database Section			
dbengine	postgre	New value	See description on page 52.
history-log Section			
all	filename, :memory:	New option value added in 7.6	See description on page 58. New option value added in 7.6; not documented.
Application Parameters			
backlog	Positive integer greater than 4.	Clarified description	See description on page 61. Clarified description.

Note: For information about configuration options related to external authentication in Configuration Server, refer to the *Framework 8.0 External Authentication Reference Manual.*

Chapter

5 Configuration Server Proxy Configuration Options

This chapter describes configuration options for Configuration Server operating in Proxy mode (referred to as *Configuration Server Proxy*) and includes the following sections:

Configuration Server Proxy also supports the common options described in Chapter 1 on page 11.

Setting Configuration Options

Unless specified otherwise, set Configuration Server Proxy configuration options in the `Options` of the Configuration Server Proxy `Application` object, using one of the following navigation paths:

- In Genesys Administrator—Configuration Server Proxy `Application` object > `Options` tab > `Advanced View (Options)`
- In Configuration Manager—Configuration Server Proxy `Application` object > `Properties` dialog box > `Options tab`

Warning! Configuration section names, configuration option names, and predefined option values are case-sensitive. Type them in Genesys Administrator or Configuration Manager exactly as they are documented in this chapter.

Mandatory Options

Table 7 lists the Configuration Server Proxy options for which you must provide values; otherwise, Configuration Server Proxy will not start. The options are listed by section.

Table 7: Mandatory Options

Option Name	Default Value	Details
License Section		
license-file	No default value	This is the unified Genesys licensing option. See the description in *Genesys Licensing Guide*.

Note: For information about starting and configuring Configuration Server Proxy, refer to the *Framework 8.0 Deployment Guide*.

license Section

You must configure the `license` section for Configuration Server when running it in Proxy mode to support geographically distributed configuration environments.

This section must be called `license`.

The only configuration option in the License section is called `license-file`, and this is the Genesys unified licensing option. Refer to the *Genesys Licensing Guide* for the option description and values.

csproxy Section

This section must be called `csproxy`.

Note: In addition to the configuration options listed here, this section contains the options `last-login` and `last-login-synchronization`. Refer to the section "Last Logged-In User" in the *Genesys 8.0 Security Deployment Guide* for complete information about these options.

encoding

Default Value: `UTF-8`
Valid Values: `UTF-8, UTF-16, ASCII, ISO-8859-1, ISO-8859-2, ISO-8859-3, ISO-8859-4, ISO-8859-5, ISO-8859-6, ISO-8859-7, ISO-8859-8, ISO-8859-9, ebcdic-cp-us, ibm1140, gb2312, Big5, koi8-r, Shift_JIS, euc-kr`
Changes Take Effect: Immediately

Sets the UCS (Universal Character Set) transformation format (such as, UTF-8, UTF-16, Shift_JIS, and so forth) that Configuration Server Proxy uses when writing configuration data into an XML (Extensible Markup Language) export file that will be used by the Configuration Import Wizard (CIW). If the operating system settings do not support the specified value, Configuration Server Proxy uses the default value.

Specify the UTF-8 encoding format unless you are using wide-character codesets (such as Chinese, Japanese, Korean, and so forth).

locale

Default Value: No default value
Valid Values: Any valid locale name or abbreviation
Changes Take Effect: Immediately

On Windows operating systems, specifies the locale setting that Configuration Server Proxy uses when transforming configuration object information from internal representation for export to an XML file.

Select values for this option from the official Microsoft locale list. For example, for English, specify `english` or `eng`; for Japanese, specify `japan` or `jpn`; and so forth.

Note: The specified `locale` value must be supported by your operating system.

proxy-writable

Default Value: `false`
Valid Values:

`true`	Configuration Server Proxy accepts requests from Genesys Agent Desktop for updates to user-defined data, and forwards these requests to the Master Configuration Server.

`false` Configuration Server Proxy does not accept requests from Genesys Agent Desktop for updates to user-defined data. Genesys Agent Desktop must send the requests to the Master Configuration Server directly.

Changes Take Effect: Immediately

Specifies whether Configuration Server Proxy accepts requests from Genesys Agent Desktop applications for updates to user-defined data, such as hot keys, shortcuts, and recently dialed numbers. If accepted, Configuration Server Proxy then forwards the requests to the Master Configuration Server, where the updates are stored.

objects-cache

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

Specifies if Configuration Server Proxy uses internal caching. When set to `true`, Configuration Server Proxy caches objects requested by client applications. This is the default behavior of Configuration Server Proxy in previous releases. When this option is set to `false`, the objects are not cached, reducing the amount of memory used by Configuration Server Proxy.

Note: Disabling the cache may increase the load on Configuration Server Proxy during client application registration. Use this option with care.

history-log Section

The options in this section enable Configuration Server Proxy to save all information about client sessions and changes to configuration data in a history log database. Configuration Server Proxy updates the database as it receives notifications about the changes from Configuration Server and upon termination of client sessions.

This section must be called `history-log`.

all

Default Value: `histlog`
Valid Values:

<any string value> Specifies a full path to the history log database file including the filename without the extension. Configuration Server Proxy appends the extension .hdb.

`:memory:` Stores the file in memory as histlog.hdb. Use this value to help improve system performance.

Changes Take Effect: After restart

Specifies where the history log database file is stored.

Warning! Genesys recommends that you store the history log file locally rather than on the network. Configuration Server Proxy opens a history log file in locking mode which may not be permitted in certain network configurations. Therefore, if you specify a path to a history log file located on the network, Configuration Server Proxy may issue an error message and disable the history log functionality.

expiration

Default Value: `30`
Valid Values: `1`—`30`
Changes Take Effect: Immediately

Specifies the maximum number of days the records of configuration updates will be kept in the history log before they are deleted.

client-expiration

Default Value: `1`
Valid Values: `1`—`30`
Changes Take Effect: Immediately

Specifies the maximum number of days the records of client sessions will be kept in the history log before they are deleted. Also determines the time interval at which Configuration Server Proxy will check for expiration of records of both configuration updates and client sessions.

max-records

Default Value: `1000`
Valid Values: `1`—`1000`
Changes Take Effect: Immediately

Specifies the maximum number of records Configuration Server Proxy will send to a client in response to a history log data request.

active

Default Value: `true`
Valid Values: `true, false`
Changes Take Effect: Immediately

Turns the history log on and off. The value of this option can only be changed at runtime via the Configuration Server Proxy `Application` object properties. When Configuration Server Proxy is started, it automatically turns the history log on regardless of the previous setting of this option, and sets this option to `true`. Refer to the *Framework 8.0 Deployment Guide* for more information on History Log configuration details.

failsafe-store-processing

Default Value: `true`
Valid Values:

`true` Ensures that the history log database is preserved if both Configuration Server and the operating system fail.

`false` Ensures that the history log database is preserved if only Configuration Server fails. The history log database may not be wholly preserved if operating system fails.

Changes Take Effect: Immediately

Specifies the scope of internal history log database protection when compared to system performance.

When this option is set to `true,` history log operations ensure that the history log database is preserved if both Configuration Server and the operating system fail. However, this is CPU-intensive.

When this option is set to `false,` history log operations ensure that the history log database is preserved if only the Configuration Server fails. If the operating system fails, the history log database may not be wholly preserved. However, this operation has a lesser impact on system performance.

Use this option when the volume of updates is sufficient to impact system performance, and when the impact is greater than the risk of losing some information in the history log database.

soap Section

This section contains information about the Simple Object Access Protocol (SOAP) port that clients use to access Configuration Server Proxy.

Warning! SOAP functionality is restricted to certain environments.

This section must be called `soap`.

port

Default Value: No default value
Valid Values: Any valid TCP/IP port
Changes Take Effect: After restart

Specifies the SOAP port that clients use to connect to Configuration Server Proxy.

debug

Default Value: `no`
Valid Values: `yes, no`
Changes Take Effect: After restart

Specifies whether Configuration Server Proxy prints SOAP port communication messages into its log.

client_lifespan

Default Value: 600
Valid Values: Any positive integer
Changes Take Effect: After restart

Specifies the time, in seconds, that Configuration Server Proxy keeps information about a closed SOAP connection (particularly, the session ID—that is, a value of a Hypertext Transfer Protocol (HTTP) cookie). A client that connects within this time interval and uses the existing session ID is exempt from the authentication check. Configuration Server Proxy treats this client connection as a continued HTTP session.

Application Parameter Options

Set the options in this section in the Application Parameters of the port's properties, using one of the following navigation paths:

- In Genesys Administrator—Configuration Server Proxy Application object > Configuration tab > Server Info section > Listening Ports > Port Info
- In Configuration Manager—Configuration Server Proxy Application object > Properties dialog box > Server Info tab > Port Properties dialog box > Advanced tab

Application Parameter options are not associated with a configuration option section, and do not appear in the options or annex of a Configuration Server Proxy Application object.

backlog

Default Value: 5
Valid Values: Any positive integer greater than 4
Changes Take Effect: Immediately

Specifies the maximum number of outstanding connection requests from clients. When the maximum is reached, Configuration Server Proxy does not accept a new request until an outstanding request is processed.

This option is optional; if it is not configured, the default value is used.

Warning! This option is for advanced use only, and is logged only in Debug level logs. Use this option only when requested by Genesys Technical Support.

Changes from 7.6 to 8.0

Table 8 on page 70 provides all the changes to Configuration Server Proxy options between release 7.6 and the latest 8.0 release.

Table 8: Configuration Server Proxy Configuration Option Changes from 7.6 to 8.0

Option Name	Option Values	Type of Change	Details
csproxy Section			
last-login	true, false	New	Refer to "Last Logged-In User" in the *Genesys 8.0 Security Deployment Guide*.
last-login-synchronize	true, false	New	
proxy-writable	true, false	New in 7.6	See description on page 65. New in release 7.6; not documented in earlier releases.
objects-cache	true, false	New	See description on page 66.
history-log Section			
all	filename, :memory:	New option value added in 7.6	See description on page 66. New option value added in 7.6; not documented in earlier releases.
Application Parameters			
backlog	Positive integer greater than 4.	Clarified description	See description on page 69. Clarified description.

Chapter

6 Genesys Administrator Configuration Options

This chapter describes the configuration options for Genesys Administrator, and includes the following sections:

Setting Configuration Options

You can use Genesys Administrator or Configuration Manager to set Genesys Administrator configuration options.

Unless specified otherwise, set Genesys Administrator configuration options in the `Options` of the `Application` object to which Genesys Administrator was deployed (refer to the *Framework 8.0 Genesys Administrator Deployment Guide*). Use one of the following navigation paths:

- In Genesys Administrator—Genesys Administrator or Configuration Manager `Application` object > `Options` tab > `Advanced View (Options)`
- In Configuration Manager—Genesys Administrator or Configuration Manager `Application` object > `Properties` dialog box > `Options tab`

Warning! Configuration section names, configuration option names, and predefined option values are case-sensitive. Type them in Genesys Administrator or Configuration Manager exactly as they are documented in this chapter.

Mandatory Options

You do not have to configure any options to start Genesys Administrator.

default Section

This section must be called `default`, and is configured in the Genesys Administrator or Configuration Manager `Application` object with which Genesys Administrator was deployed.

metadata_store

Default Value: `<Genesys Administrator installation folder>\resources\metadata`
Valid Values: Any valid path and folder
Changes Take Effect: Immediately

Specifies the folder where all metadata files are stored.

security Section

This section must be called `security`, and is configured in the Genesys Administrator or Configuration Manager `Application` object with which Genesys Administrator was deployed.

enable_reconnection

Default Value: `true`
Valid Values: `true`, `false`
Changes Take Effect: After re-login to Genesys Administrator

If set to `true` (default), specifies that Genesys Administrator is to reconnect to a Configuration Server if the connection is lost. Genesys Administrator will continue trying to reconnect for the period of time specified by the option `reconnection_timeout`.

If set to `false`, Genesys Administrator will not attempt to reconnect to Configuration Server, and will redirect the user to the Login dialog.

reconnection_timeout

Default Value: `60`
Valid Values: `5`–`600` seconds
Changes Take Effect: After re-login to Genesys Administrator

Specifies the period of time that Genesys Administrator will try to reconnect to a Configuration Server if the connection is lost. This option applies only if the option `enable_reconnection` is set to `true`.

Chapter

7 Configuration Manager Configuration Options

This chapter describes the configuration options for Configuration Manager, and includes the following sections:

Setting Configuration Options

Unless specified otherwise, set Configuration Manager configuration options in the Options of the Configuration Manager Application object, using one of the following navigation paths:

- In Genesys Administrator—Configuration Manager Application object > Options tab > Advanced View (Options)
- In Configuration Manager—Configuration Manager Application object > Properties dialog box > Options tab

Warning! Configuration section names, configuration option names, and predefined option values are case-sensitive. Type them in Genesys Administrator or Configuration Manager exactly as they are documented in this chapter.

Mandatory Options

You do not have to configure any options to start Configuration Manager.

security Section

The `security` section contains configuration options related to security features. This section contains one configuration option, `inactivity-timeout`. Refer to the chapter "Inactivity Timeout" in the *Genesys 8.0 Security Deployment Guide* for complete information about this option.

Changes from 7.6 to 8.0

There are no changes to Configuration Manager configuration options between release 7.6 and the latest 8.0 release.

Chapter

8

Message Server Configuration Options

This chapter describes the configuration options for Message Server and includes the following sections:

Message Server also supports the common options described in Chapter 1 on page 11.

Setting Configuration Options

Unless specified otherwise, set Message Server configuration options in the `Options` of the Message Server `Application` object, using one of the following navigation paths:

- In Genesys Administrator—Message Server `Application` object > `Options` tab > `Advanced View (Options)`
- In Configuration Manager—Message Server `Application` object > `Properties` dialog box > `Options` tab

Warning! Configuration section names, configuration option names, and predefined option values are case-sensitive. Type them in Genesys Administrator or Configuration Manager exactly as they are documented in this chapter.

Mandatory Options

You do not have to configure any options to start Message Server.

MessageServer Section

This section must be called `MessageServer`.

signature

Default Value: `log`
Valid Values:

`log`	This Message Server is used for logging to the Centralized Log Database.
`general`	This Message Server is used for strategy monitoring from Interaction Routing Designer.
`scs_distributed`	This Message Server is used for communication between distributed Solution Control Servers.

Changes Take Effect: After restart

Specifies the role of this Message Server. Solution Control Server uses this option to determine what this Message Server does and what messages it handles.

If this option is not configured, this Message Server is used for logging.

messages Section

This section must be called `messages`.

thread_mode

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

Specifies the thread mode Message Server uses to process client connections. Currently, the single-threaded mode is always used.

thread_pool_size

Default Value: `10`
Valid Values: Any positive integer
Changes Take Effect: After restart

Specifies the number of threads started to process client connections. The recommended value is `10` even when only one processor is used. You can increase the number when more processors are used. Setting the option to a value greater than 50 is not recommended.

request_queue_size

Default Value: 1000
Valid Values: Any positive integer
Changes Take Effect: After restart

Specifies the maximum number of outstanding requests from clients. When the maximum is reached, Message Server does not accept a new request until an outstanding request is processed. The maximum value for this option is only limited by the amount of physical memory available on the computer where Message Server runs.

db_storage

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

Specifies whether log messages are stored in a database.

Note: For the value true to take effect, you must include an appropriate Database Access Point in the Connections of the Message Server Application object.

db_binding

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

Specifies whether Message Server uses DB Server’s binding functionality when storing messages in the database.

log-queue-exp-time

Default Value: 0
Valid Values: 0—604800 (7 days)
Changes Take Effect: Immediately

Specifies for how long (in seconds) the previously received log messages will be stored in the log queue during a connection failure between Message Server and DB Server. When the timeout expires, Message Server will delete all expired messages from the queue. The default value of 0 means no expiration time.

log-queue-size

Default Value: 0
Valid Values: 0—4294967295
Changes Take Effect: After restart

Specifies the maximum number of log messages to be stored in a log queue during a connection failure between Message Server and DB Server. When the maximum is reached, arrival of each new log message will cause removal of the oldest message from the queue until connection to DB Server is restored. The default value of `0` means an unlimited number of log messages can be stored in the log queue.

log-queue-response

Default Value: `0`
Valid Values: `0`—`65535`
Changes Take Effect: Immediately

Specifies the maximum number of log messages that Message Server may send to DB Server from its queue in a single request when the connection between them is restored after a failure. The next portion of log messages will be sent upon confirmation response from DB Server with respect to the previous request. The default value of `0` means an unlimited number of log messages can be sent to DB Server in a single request. Setting this option to a very small value may negatively affect system performance.

db-filter Section

The DB Filter section controls delivery of specified log events from specified applications and application types. See “Sample Configuration” on page 79. This section must be called `db-filter`.

block-messages

Default Value: No default value
Valid Values: Identifiers of any valid log events separated by commas
Changes Take Effect: Immediately

Specifies the log events reported by any application that will not be recorded in the Central Log Database.

block-messages-from-<DBID>

Default Value: No default value
Valid Values: Identifiers of any valid log events separated by commas
Changes Take Effect: Immediately

Specifies the log events reported by the specified application that will not be recorded in the Central Log Database, where <DBID> is the numeric value of the application.

Note: To acquire an application DBID, start Configuration Manager from a command-line prompt using the `-d` command-line parameter. For example, `D:\GCTI\sce.exe -d`. The application DBID is displayed with the application title in the Application `Properties` dialog box.

block-messages-by-<type>

Default Value: No default value
Valid Values: Identifiers of any valid log events separated by commas
Changes Take Effect: Immediately

Specifies the log events reported by applications of the specified type that will not be recorded in the Central Log Database, where <type> is the numeric value of the application type.

Note: For information about application types, refer to the "Database Format" section of the "Log Format" chapter in the *Framework 8.0 Management Layer User's Guide.*

Sample Configuration

The following is a sample configuration of the `db-filter` section for Message Server:

```
[db-filter]
block-messages = 4001,4002,4003
block-messages-from-201 = 1001,1002,1003
block-messages-by-9 = 5003,5004,5005
```

Changes from 7.6 to 8.0

Table 9 provides all the changes to Message Server options between release 7.6 and the latest 8.0 release.

Table 9: Message Server Configuration Option Changes from 7.6 to 8.0

Option Name	Option Values	Type of Change	Details
MessageServer Section			
signature	log, general, scs_distributed	New	See description on page 76. Not documented in previous releases.

Chapter

9 Solution Control Server Configuration Options

This chapter describes configuration options for Solution Control Server (SCS) and includes the following sections:

Solution Control Server also supports:

- The common options described in Chapter 1 on page 11.
- The `autostart` configuration option which you configure in other server applications and which Solution Control Server processes. Refer to the *Framework 8.0 Management Layer User's Guide* for more information.

Setting Configuration Options

Unless specified otherwise, set Solution Control Server configuration options in the `Options` of the Solution Control Server `Application` object, using one of the following navigation paths:

- In Genesys Administrator—Solution Control Server `Application` object > `Options` tab > `Advanced View (Options)`
- In Configuration Manager—Solution Control Server `Application` object > `Properties` dialog box > `Options tab`

Warning! Configuration section names, configuration option names, and predefined option values are case-sensitive. Type them in Genesys Administrator or Configuration Manager exactly as they are documented in this chapter.

Mandatory Options

You do not have to configure any options to start Solution Control Server.

License Section

You must configure the License section for Solution Control Server when you use the following functionality:

- Redundant configurations—either warm standby or hot standby—for any Genesys server that the Management Layer controls.
- SCS support for geographically distributed configuration environments.
- Simple Network Management Protocol (SNMP) interface.

This section must be called license.

The only configuration option in the License section is called license-file, and this is the Genesys unified licensing option. Refer to the *Genesys Licensing Guide* for the option description and values.

general Section

This section contains information about the SCS operational mode and relevant settings.

This section must be called general.

max_switchover_time

Default Value: 15
Valid Values: 0 or any positive integer
Changes Take Effect: After restart

Specifies the time interval, in seconds, that SCS waits for an application to perform the switchover command. If the application does not change its redundancy mode within the specified interval, SCS reports a failure of the switchover request.

disconnect-switchover-timeout

Default Value: `0`
Valid Values: `0` or any positive integer
Changes Take Effect: Immediately

Specifies the time interval, in seconds, that SCS waits for an LCA connection to be restored before switching operations over to the backup server of an application installed on the host running LCA. When the timeout expires, SCS determines whether the switchover condition still exists:

- If the LCA remains disconnected (because, for example, the LCA host is down) and the status of the application installed on the LCA host remains `Unknown`, SCS switches the backup server configured for the application to `Primary` mode.
- If the LCA connection is restored (because, for example, a temporary network problem no longer exists) and the status of the application installed on the LCA host becomes `Started`, SCS does not perform a switchover to the application's backup server.

Use this option when the network linking SCS and a monitored host is slow (such as a WAN).

distributed_mode

Default Value: `OFF`
Valid Values: `ON`, `OFF`
Changes Take Effect: After restart

Specifies whether SCS operates in Distributed mode, to support a distributed management environment. When set to `ON`, SCS verifies the existence of the appropriate license at startup and, if the license is found and valid, starts operating in Distributed mode.

distributed_rights

Default Value: `DEFAULT`
Valid Values:

`DEFAULT`	SCS controls the objects associated with it in the Configuration Database.
`MAIN`	SCS controls all objects that are not associated with any SCS in the Configuration Database.

Changes Take Effect: After restart

When SCS operates in Distributed mode (`distributed_mode` is set to `ON`), specifies what objects SCS controls. Use this option when you run SCS in a distributed management environment and you want to grant this SCS instance control permissions over all configuration objects (such as, Hosts, Applications, and Solutions) that you have not configured other SCS instances to control.

alive_timeout

Default Value: 30
Valid Values: Any value from range 15–300
Changes Take Effect: After restart

When SCS operates in Distributed mode (distributed_mode is set to ON), specifies the time interval, in seconds, that this SCS waits for a response from other instances of SCS. When using a Message Server to allow the Solution Control Servers in the Distributed SCS network to communicate with each other, this option must be considered when setting the Advanced Disconnect Detection Protocol (ADDP) timeout values. Refer to the section "Distributed Solution Control Servers" in the *Framework 8.0 Deployment Guide* for details about this relationship.

service-unavailable-timeout

Default Value: 0
Valid Values: Any value from range 0–5
Changes Take Effect: Immediately

Specifies the amount of time, in seconds, that SCS waits before applying the criteria for switchover if the primary and backup T-Servers report Service Unavailable simultaneously.

mailer Section

This section contains information about SMTP-related settings for SCS.

This section must be called mailer.

smtp_host

Default Value: No default value
Valid Values: <string> Host name
Changes Take Effect: After restart

Specifies the host name of the SMTP server to which SCS sends alarm reactions of the E-Mail type. If you do not configure this option or don't set its value, SCS does not use the SMTP mailing system to send alarm reactions via e-mail. SCS uses the Windows MAPI (Messaging Application Programming Interface) system is used instead.

smtp_port

Default Value: 25
Valid Values: <string> Port number
Changes Take Effect: After restart

Specifies the port number of the SMTP server to which SCS sends alarm reactions of the E-Mail type.

smtp_from

Default Value: No default value
Valid Values: <string> E-mail address
Changes Take Effect: Immediately

Specifies the value of the From field in the e-mail message that SCS sends as an alarm reaction of the E-Mail type.

log Section

This section controls SCS logging. This section must be called `log`.

Note: Solution Control Server supports the log options described in this section in addition to those described in Chapter 1, "Common Configuration Options," on page 11. Note, however, that SCS always uses full log message format, regardless of the `message_format` option setting.

eventloghost

Default Value: No default value
Valid Values: <string> Host name
Changes Take Effect: Immediately

Specifies the host name of the computer whose operating-system log should store Genesys alarm messages. The option works in conjunction with the `alarm` output level and applies only to computers running Windows NT. If you do not configure this option or don't set its value, alarms are sent to the operating-system log of the computer on which SCS runs.

alarm

Default Value: No default value
Valid Values (log output types):

`stdout`	Alarms are sent to the Standard output (stdout).
`stderr`	Alarms are sent to the Standard error output (stderr).
`network`	Alarms are sent to Message Server, which resides anywhere on the network, and Message Server stores the log events 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]`	Alarms are stored to a file with the specified name.
`syslog`	Alarms are sent to the operating-system log.

Changes Take Effect: Immediately

Specifies to which outputs SCS sends those alarms it generates as a result of appropriate Standard log events. When you configure more than one output type, separate them by a comma. This option is the same as the option `alarm` in Chapter 1 on page 11, with the additional value `syslog` that is specific to SCS.

Note: For SCS to generate alarms, you must set the `verbose` option to a value other than `none`.

Example

To output alarms generated as a result of appropriate Standard log events into the log of the operating system and to a network Message Server, specify `alarm` as the SCS configuration option and `syslog, network` as the option value.

Configuring ADDP Between SCS and LCA

Advanced Disconnection Detection Protocol (ADDP) is enabled automatically between Solution Control Server and Local Control Agent. To customize its settings, configure the options `addp-timeout` and `addp-remote-timeout` in the `Host` object, as described in Chapter 13 on page 101.

Changes from 7.6 to 8.0

There are no changes to Solution Control Server configuration options between release 7.6 and the latest 8.0 release.

Chapter

10 Solution Control Interface Configuration Options

This chapter describes the configuration options for Solution Control Interface, and includes the following sections:

Setting Configuration Options

Unless specified otherwise, set Solution Control Interface (SCI) configuration options in the `Options` of the SCI `Application` object, using one of the following navigation paths:

- In Genesys Administrator—SCI `Application` object > `Options` tab > `Advanced View (Options)`
- In Configuration Manager—SCI `Application` object > `Properties` dialog box > `Options` tab

Warning! Configuration section names, configuration option names, and predefined option values are case-sensitive. Type them in Genesys Administrator or Configuration Manager exactly as they are documented in this chapter.

Mandatory Options

You do not have to configure any options to start SCI.

host-status-display Section

This section defines the colors in which names of Hosts appear in SCI, based on the alarm status of Applications running on those Hosts. These color settings do not affect the display of Host status in the Status column.

This section must be called host-status-display.

Note: Options in this section are set in the Object highlight colors section of the Alarming tab of the Options dialog box of SCI.

critical-color

Default Value: red
Valid Values: black, gray, green, blue, yellow, amber, orange, red, purple
Changes Take Effect: After restart

Specifies in what color the name of a Host object will appear in SCI when there are outstanding Critical alarms for Applications running on that Host. If this option is not configured, or is configured with an invalid value, the default value (red) will be used.

major-color

Default Value: amber
Valid Values: black, gray, green, blue, yellow, amber, orange, red, purple
Changes Take Effect: After restart

Specifies in what color the name of a Host object will appear in SCI when there are no outstanding Critical alarms for Applications running on that Host but there are outstanding Major alarms. If this option is not configured, or is configured with an invalid value, the default value (amber) will be used.

other-color

Default Value: green
Valid Values: black, gray, green, blue, yellow, amber, orange, red, purple
Changes Take Effect: After restart

Specifies in what color the name of a Host object will appear in SCI when there are no outstanding Critical or Major alarms for Applications running on that Host. If this option is not configured, or is configured with an invalid value, the default value (green) will be used.

security Section

The security section contains configuration options related to security features. This section contains one configuration option, inactivity-timeout. Refer to the chapter “Inactivity Timeout” in the *Genesys 8.0 Security Deployment Guide* for complete information about this option.

Changes from 7.6 to 8.0

Table 10 provides all the changes to SCI options between release 7.6 and the latest 8.0 release.

Table 10: Solution Control Interface Configuration Option Changes from 7.6 to 8.0

Option Name	Option Values	Type of Change	Details
	host-status-display Section (new section)		
critical-color	black, gray, green, blue, yellow, amber, orange, red, purple	New	See description on page 88.
major-color	black, gray, green, blue, yellow, amber, orange, red, purple	New	See description on page 88.
other-color	black, gray, green, blue, yellow, amber, orange, red, purple	New	See description on page 88.

Chapter

11 SNMP Master Agent Configuration Options

This chapter describes the configuration options for Genesys Simple Network Management Protocol (SNMP) Master Agent and includes the following sections:

Genesys SNMP Master Agent also supports the options described in Chapter 1 on page 11.

Setting Configuration Options

Unless specified otherwise, set Genesys SNMP Master Agent options in the `Options` of the Genesys SNMP Master Agent `Application` object, using one of the following navigation paths:

- In Genesys Administrator—Genesys SNMP Master Agent `Application` object > `Options` tab >`Advanced View (Options)`
- In Configuration Manager—Genesys SNMP Master Agent `Application` object > `Properties` dialog box > `Options tab`

Warning! Configuration section names, configuration option names, and predefined option values are case-sensitive. Type them in Genesys Administrator or Configuration Manager exactly as they are documented in this chapter.

Mandatory Options

You do not have to configure any options to start Genesys SNMP Master Agent.

agentx Section

This section must be called `agentx`. Options in this section define the connection between Genesys SNMP Master Agent and Solution Control Server (SCS).

Note: If you use a third-party SNMP master agent to communicate between your Genesys installation and a third-party Network Management System (NMS), you have to configure the `agentx` section and appropriate options when you create an Application object of the SNMP Agent type. Although your third-party SNMP master agent does not retrieve or use this configuration, SCS checks these settings for its connection to the SNMP master agent. Also make sure that the option values match the actual configuration settings in your third-party SNMP master agent application.

mode

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

Specifies the connectivity mode for the AgentX-protocol connection between Genesys SNMP Master Agent and SCS. If you do not configure the option, don't set its value, or set it to `TCP`, Genesys SNMP Master Agent uses a TCP/IP socket for the connection. The `tcp_port` configuration option defines the actual port number in this case.

Note: For Genesys SNMP Master Agent (or a third-party SNMP master agent) running on a Windows operating system, `TCP` is always taken as the actual value for the mode configuration option.

tcp_port

Default Value: `705`
Valid Values:

`705`	Port number
`<string>`	Any valid port number

Changes Take Effect: After restart

Specifies the port number Genesys SNMP Master Agent opens for connection in the TCP mode. When you do not configure the option, don't set its value, or set it an invalid (noninteger or zero) value, Genesys SNMP Master Agent opens the default port (705) for the TCP/IP connection.

snmp Section

This section must be called `snmp`. Options in this section define SNMP-related parameters, as for SNMPv1/v2 and for SNMPv3. Because of the differences in security implementation for different versions of SNMP, some options control access to Genesys MIB (management information base) objects via SNMPv1/v2 requests and others control access to Genesys MIB objects via SNMPv3 requests.

Use the following options to configure SNMPv1/v2 access:

- `read_community`
- `write_community`

These configuration options do not control access to MIB objects via SNMPv3 requests.

Use the following options to configure SNMPv3 access:

- `v3_username`
- `v3auth_password`
- `v3priv_password`
- `v3auth_protocol`
- `v3priv_protocol`

These configuration options do not control access to MIB objects via SNMPv1/v2 requests.

Note: If you do not configure the `snmp` section or any of its options, Genesys SNMP Master Agent provides access in SNMPv3 mode, with the default settings as described in this section. Access in SNMPv1/SNMPv2 mode is denied.

read_community

Default Value: `none`
Valid Values:

`none`	
`<string>`	Any valid community name

Changes Take Effect: After restart

Specifies the SNMP community name that Genesys SNMP Master Agent uses to authenticate SNMPv1/v2c GET and GET NEXT requests. That is, Read permissions for all Genesys MIB objects are granted to the specified community. If you do not configure the option or don't set its value, the `write_community` option controls SNMPv1/v2 Read access.

write_community

Default Value: `none`
Valid Values:

`none`	
`<string>`	Any valid community name

Changes Take Effect: After restart

Specifies the SNMP community name that Genesys SNMP Master Agent uses to authenticate SNMPv1/v2c SET, GET, and GET NEXT requests. That is, the specified community receives:

- Read permissions for all Genesys MIB objects.
- Write permissions for all Genesys MIB objects except for the objects in the VACM and USM MIB files. Genesys SNMP Master Agent excludes VACM and USM MIB objects from the group of writable objects to prevent remote NMS users from changing security attributes.

If you don't configure the option or don't set its value, no SNMPv1/v2 Write access is allowed.

trap_target

Default Value: No default value
Valid Values: A list of any number of SNMP trap targets, separated by commas, in the following format:
`<host name>/<port number>:<community name>`
Changes Take Effect: After restart

Specifies where Genesys SNMP Master Agent sends trap notifications. You can specify a host IP address instead of a host name. If you do not specify a community name, Genesys SNMP Master Agent sends trap notifications to the `public` community.

For example:

```
host1/162:public_t1, 127.0.0.1/163:public_t2
```

v3_username

Default Value: `default`
Valid Values:

`default`	
`<string>`	User name

Changes Take Effect: After restart

Specifies the user name used for issuing SNMPv3 requests. Genesys SNMP Master Agent does not accept SNMPv3 requests other users may send. A user with the specified user name receives:

- Read permissions for all Genesys MIB objects.

- Write permissions for all Genesys MIB objects except for the objects in the VACM and USM MIB files. Genesys SNMP Master Agent excludes VACM and USM MIB objects from the group of writable objects to prevent remote NMS users from changing security attributes.

The user should send SNMPv3 requests for the default (empty) context.

v3auth_password

Default Value: No default value
Valid Values: `<string>` Any valid password
Changes Take Effect: After restart

Specifies the SNMPv3 user's password used for authentication.

v3priv_password

Default Value: No default value
Valid Values: `<string>` Any valid password
Changes Take Effect: After restart

Specifies the SNMPv3 user's password used for privacy of data.

v3auth_protocol

Default Value: `none`
Valid Values:

`MD5`	HMAC-MD5-96 authentication protocol
`SHA`	HMAC-SHA5-96 authentication protocol
`none`	No authentication

Changes Take Effect: After restart

Specifies the authentication protocol, if any, to authenticate messages sent or received on behalf of this user. If you don't configure the option, don't set its value, or set it to an invalid value, Genesys SNMP Master Agent uses no authentication.

v3priv_protocol

Default Value: `none`
Valid Values:

`DES`	CBC-DES privacy protocol
`none`	No encryption

Changes Take Effect: After restart

Specifies whether encryption is used for SNMPv3 messages sent or received on behalf of this user and, if so, using which privacy protocol. This option applies only if the `v3auth_protocol` option is set to a valid value other than `none`. If you do not configure the `v3priv_protocol` option, do not set its value, or set it to an invalid value, Genesys SNMP Master Agent uses no encryption.

Changes from 7.6 to 8.0

Table 11 provides all the changes to SNMP Master Agent configuration options between release 7.6 and the latest 8.0 release.

Table 11: SNMP Master Agent Configuration Option Changes from 7.6 to 8.0

Option Name	Option Values	Type of Change	Details
agentx Section			
mode	Removed value `UNIX`	Modified	See description on page 92. Value `UNIX` obsolete in release 7.1.1.
unix_port		Obsolete	Obsolete in release 7.1.1.
snmp Section			
v3priv_protocol	Removed value `IDEA`	Modified	See description on page 95. Not supported; included incorrectly in previous version of this document.

Chapter

12 Local Control Agent Configuration Options

This chapter describes the configuration options for Local Control Agent (LCA) and includes the following sections:

Setting Configuration Options

You change default LCA configuration options in the configuration file `lca.cfg`. See "LCA Configuration File" on page 98 for more information.

Warning! Configuration section names, configuration option names, and predefined option values are case-sensitive. Type them in the configuration file exactly as they are documented in this chapter.

Mandatory Options

You do not have to configure any options to start LCA.

log Section

This section must be called `log`.

The options you can configure in this section are the unified common log options described in Chapter 1 on page 11.

LCA Configuration File

Starting with release 7.0, LCA supports common log options which allows you to precisely configure log output for LCA. Because you do not configure an `Application` object for LCA, if you need to change the default log option settings, create a configuration file called `lca.cfg` and specify new values for appropriate options. The configuration file contains only the `log` section. The file must be located in the same directory as the LCA executable file.

Note: You can also specify a custom name for the configuration file using the `-c` command-line parameter. For example, `lca.exe -c lca_custom.cfg`, where `lca_custom.cfg` is the user defined configuration file.

The LCA configuration file must have the following format:

```
[log]
<log option name>=<log option value>
<log option name>=<log option value>
```

For more information on the LCA configuration file and for related instructions, see the *Framework 8.0 Deployment Guide.*

Sample Configuration File

Here is a sample configuration file for LCA:

```
[log]
verbose = standard
standard = stdout, logfile
```

Configuring ADDP Between LCA and SCS

Advanced Disconnection Detection Protocol (ADDP) is enabled automatically between LCA and Solution Control Server. To customize its settings, configure the options `addp-timeout` and `addp-remote-timeout` in the `Host` object, as described in Chapter 13 on page 101.

Changes from 7.6 to 8.0

There are no changes to LCA configuration options between release 7.6 and the latest 8.0 release.

Chapter

13 Host Configuration Options

This chapter describes configuration options for a Host object, and contains the following sections:

Setting Configuration Options

Unless specified otherwise, set Host configuration options in the Annex of the Host object, using one of the following navigation paths:

- In Genesys Administrator—Host object > Options tab > Advanced View (Annex)
- In Configuration Manager—Host object > Properties dialog box > Annex tab

Warning! Configuration section names, configuration option names, and predefined option values are case-sensitive. Type them in Genesys Administrator or Configuration Manager exactly as they are documented in this chapter.

Mandatory Options

You do not have to configure any options for a Host.

addp Section

This section contains the parameters necessary to configure Advanced Disconnect Detection Protocol (ADDP) between Local Control Agent (LCA) and Solution Control Server.

This section must be called `addp`.

addp-timeout

Default: `9`
Valid Values: `0` or any positive integer
Changes Take Effect: When connection is reestablished

Specifies the ADDP timeout in seconds used by Solution Control Server. If Solution Control Server does not receive messages from LCA within this interval, Solution Control Server sends a polling message. Solution Control Server interprets the lack of response from LCA within the same time period as a loss of connection.

If this value is set to `0` (default), ADDP is not used by Solution Control Server.

Note: If there is particular risk of network delays, Genesys recommends setting ADDP timeouts to values equal to or greater than 10 seconds, instead of relying on default values to avoid false detection of disconnection.

addp-remote-timeout

Default: `0`
Valid Values: `0` or any positive integer
Changes Take Effect: When connection is reestablished.

Specifies the ADDP timeout in seconds used by LCA. After the connection between Solution Control Server and LCA is established, this value is passed to LCA. If LCA does not receive messages from Solution Control Server within this interval, LCA sends a polling message. LCA interprets the lack of response from Solution Control Server within the same time period as a loss of connection.

If this value is set to `0` (default), ADDP is not used by LCA.

Changes from 7.6 to 8.0

Table 12 on page 103 provides all the changes to Host options between release 7.6 and the latest 8.0 release.

Table 12: Host Configuration Option Changes from 7.6 to 8.0

Option Name	Option Values	Type of Change	Details
addp Section			
addp-timeout	0 or any positive integer	Documentation only	See description on page 102. This option existed in previous releases, but was not documented.
addp-remote-timeout	0 or any positive integer	Documentation only	See description on page 102. This option existed in previous releases, but was not documented.

Chapter

14 Tenant Configuration Options

This chapter describes configuration options for a `Tenant` object, and contains the following sections:

Setting Configuration Options

Unless specified otherwise, set Tenant configuration options in the `Annex` of the `Tenant` object, using one of the following navigation paths:

- In Genesys Administrator—`Tenant` object > `Options` tab > `Advanced View (Annex)`
- In Configuration Manager—`Tenant` object > `Properties` dialog box > `Annex` tab

The options in this section applies to all objects owned by the Tenant in which the options are set.

Warning! Configuration section names, configuration option names, and predefined option values are case-sensitive. Type them in Genesys Administrator or Configuration Manager exactly as they are documented in this chapter.

Mandatory Options

You do not have to configure any options for a Tenant.

security-authentication-rules Section

This section must be called `security-authentication-rules`.

The `security-authentication-rules` section contains configuration options used to specify rules for user passwords to enhance user authentication for your system. This section contains the option `password-min-length`, which is used to set a minimum length for all user passwords in the Tenant. Refer to the chapter "User Passwords" in the *Genesys 8.0 Security Deployment Guide* for complete information about this option.

Changes from 7.6 to 8.0

Table 13 provides all the changes to Tenant options between release 7.6 and the latest 8.0 release.

Table 13: Tenant Configuration Option Changes from 7.6 to 8.0

Option Name	Option Values	Type of Change	Details
security-authentication-rules Section (new section)			
password-min-length	0–64	New	See description on page 106.

Supplements

Related Documentation Resources

The following resources provide additional information that is relevant to this software. Consult these additional resources as necessary.

Genesys Framework

- The *Framework 8.0 Deployment Guide,* which will help you configure, install, start, and stop Framework components.
- *Framework 8.0 Genesys Administrator Help,* which will help you use Genesys Administrator.
- *Framework 8.0 Configuration Manager Help,* which will help you use Configuration Manager.

Genesys

- The *Genesys 8.0 Security Deployment Guide*, which describes configuration options specific to Genesys security features, and how to use them.
- *Genesys Technical Publications Glossary,* which ships on the Genesys Documentation Library DVD and which provides a comprehensive list of the Genesys and computer-telephony integration (CTI) terminology and acronyms used in this document.
- *Genesys Migration Guide*, which ships on the Genesys Documentation Library DVD, and which provides documented migration strategies for Genesys product releases. Contact Genesys Technical Support for more information.
- Release Notes and Product Advisories for this product, which are available on the Genesys Technical Support website at http://genesyslab.com/support.

Information about supported hardware and third-party software is available on the Genesys Technical Support website in the following documents:

- *Genesys Supported Operating Environment Reference Manual*
- *Genesys Supported Media Interfaces Reference Manual*

For additional system-wide planning tools and information, see the release-specific listings of System Level Documents on the Genesys Technical Support website, accessible from the `system level documents by release` tab in the Knowledge Base `Browse Documents` Section.

Genesys product documentation is available on the:

- Genesys Technical Support website at `http://genesyslab.com/support`.
- Genesys Documentation Library DVD, which you can order by e-mail from Genesys Order Management at `orderman@genesyslab.com`.

Document Conventions

This document uses certain stylistic and typographical conventions—introduced here—that serve as shorthands for particular kinds of information.

Document Version Number

A version number appears at the bottom of the inside front cover of this document. Version numbers change as new information is added to this document. Here is a sample version number:

80fr_ref-co_10-2009_v8.0.100.01

You will need this number when you are talking with Genesys Technical Support about this product.

Screen Captures Used in This Document

Screen captures from the product graphical user interface (GUI), as used in this document, may sometimes contain minor spelling, capitalization, or grammatical errors. The text accompanying and explaining the screen captures corrects such errors *except* when such a correction would prevent you from installing, configuring, or successfully using the product. For example, if the name of an option contains a usage error, the name would be presented exactly as it appears in the product GUI; the error would not be corrected in any accompanying text.

Type Styles

Table 14 describes and illustrates the type conventions that are used in this document.

Table 14: Type Styles

Type Style	Used For	Examples
Italic	• Document titles • Emphasis • Definitions of (or first references to) unfamiliar terms • Mathematical variables Also used to indicate placeholder text within code samples or commands, in the special case where angle brackets are a required part of the syntax (see the note about angle brackets on page 110).	Please consult the *Genesys Migration Guide* for more information. Do *not* use this value for this option. A *customary and usual* practice is one that is widely accepted and used within a particular industry or profession. The formula, $x +1 = 7$ where x stands for . . .

Table 14: Type Styles (Continued)

Type Style	Used For	Examples
Monospace font (Looks like `teletype` or `typewriter text`)	All programming identifiers and GUI elements. This convention includes: • The *names* of directories, files, folders, configuration objects, paths, scripts, dialog boxes, options, fields, text and list boxes, operational modes, all buttons (including radio buttons), check boxes, commands, tabs, CTI events, and error messages. • The values of options. • Logical arguments and command syntax. • Code samples. Also used for any text that users must manually enter during a configuration or installation procedure, or on a command line.	Select the `Show variables on screen` check box. In the `Operand` text box, enter your formula. Click `OK` to exit the `Properties` dialog box. T-Server distributes the error messages in `EventError` events. If you select `true` for the `inbound-bsns-calls` option, all established inbound calls on a local agent are considered business calls. Enter `exit` on the command line.
Square brackets ([ ])	A particular parameter or value that is optional within a logical argument, a command, or some programming syntax. That is, the presence of the parameter or value is not required to resolve the argument, command, or block of code. The user decides whether to include this optional information.	`smcp_server -host [/flags]`
Angle brackets (< >)	A placeholder for a value that the user must specify. This might be a DN or a port number specific to your enterprise. **Note:** In some cases, angle brackets are required characters in code syntax (for example, in XML schemas). In these cases, italic text is used for placeholder values.	`smcp_server -host <confighost>`

Index