



Framework 8.5

Configuration Options

Reference Manual

The information contained herein is proprietary and confidential and cannot be disclosed or duplicated without the prior written consent of Genesys Telecommunications Laboratories, Inc.

Copyright © 2000–2015 Genesys Telecommunications Laboratories, Inc. All rights reserved.

About Genesys

Genesys is the world's leading provider of customer service and contact center software - with more than 4,000 customers in 80 countries. Drawing on its more than 20 years of customer service innovation and experience, Genesys is uniquely positioned to help companies bring their people, insights and customer channels together to effectively drive today's customer conversation. Genesys software directs more than 100 million interactions every day, maximizing the value of customer engagement and differentiating the experience by driving personalization and multi-channel customer service - and extending customer service across the enterprise to optimize processes and the performance of customer-facing employees. Go to www.genesys.com for more information.

Each product has its own documentation for online viewing at the Genesys Documentation 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. © 2014 Genesys Telecommunications Laboratories, Inc. All rights reserved. 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 Customer Care](#). Before contacting Customer Care, please refer to the [Genesys Care Support Guide for On-Premises](#) for complete contact information and procedures.

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.genesys.com

Document Version: 85fr_ref-co_12-2015_v8.5.104.00



Table of Contents

Preface	7
About Configuration Options	7
Intended Audience.....	8
Making Comments on This Document	8
Contacting Genesys Customer Care.....	8
Changes in This Document	9
Version 8.5.104.00	9
Version 8.5.103.00	9
Version 8.5.102.00	10
Version 8.5.101.00	10
Version 8.5.001.00	11
 Chapter 1	 Common Configuration Options..... 13
Setting Configuration Options.....	13
Mandatory Options	14
Common Log Options.....	14
log Section	14
Log Output Options.....	21
Examples	25
Debug Log Options	26
Common Security Options.....	30
Filtering and/or Tagging Data in Logs	31
TLS Options.....	34
Secure User Authentication	38
sml Section	38
common Section.....	40
Transport Parameter Options	41
Configuring Client-side Port Definition	42
Configuring Secure Connections Using Security Certificates	43
Configuring Mixed IPv4 and IPv6 Environments	47
Changes from 8.1 to 8.5	48
 Chapter 2	 Database Access Point Configuration Options..... 51
Setting Configuration Options.....	51

	Mandatory Options	51
	default Section	51
	dbclient Section	52
	Changes from 8.1 to 8.5	52
Chapter 3	Configuration Server Configuration Options.....	53
	Setting Configuration Options.....	53
	Using the Configuration File for Startup Options	53
	Using Genesys Administrator for Runtime Options	54
	Startup Options in Configuration File.....	54
	Mandatory Startup Options	55
	Configuration Server Section	55
	Configuration Database Section	68
	Runtime Options in Configuration Database	70
	Configuration Server section	71
	system Section	71
	log Section	72
	security Section	73
	history-log Section	74
	Application Parameter Options.....	75
	Transport Parameter Options	76
	Sample Configuration Server Configuration File	77
	Changes from 8.1 to 8.5	78
Chapter 4	Configuration Server Proxy Configuration Options.....	83
	Setting Configuration Options.....	83
	Mandatory Options	84
	license Section	84
	csproxy Section	84
	history-log Section	88
	Application Parameter Options	89
	Changes from 8.1 to 8.5	90
Chapter 5	Local Control Agent Configuration Options	93
	Setting Configuration Options.....	93
	Mandatory Options	93
	general Section.....	94
	log Section.....	94
	security Section	94
	LCA Configuration File	95
	Sample Configuration File	96

	Configuring ADDP Between LCA and Solution Control Server	96
	Changes from 8.1 to 8.5	96
Chapter 6	Genesys Deployment Agent Configuration Options.....	97
	Setting Configuration Options.....	97
	Mandatory Options	97
	log Section.....	98
	web Section	98
	security Section	98
	Genesys Deployment Agent Configuration File.....	99
	Sample Configuration File	99
	Changes from 8.1 to 8.5	100
Chapter 7	Message Server Configuration Options	101
	Setting Configuration Options.....	101
	Mandatory Options	101
	MessageServer Section	102
	messages Section	102
	db-filter Section.....	104
	log Section.....	105
	Changes from 8.1 to 8.5	105
Chapter 8	Solution Control Server Configuration Options	107
	Setting Configuration Options.....	107
	Mandatory Options	108
	License Section	108
	general Section.....	108
	mailer Section.....	111
	log Section.....	112
	Transport Parameter Options	113
	Configuring ADDP Between SCS and LCA.....	114
	Changes from 8.1 to 8.5	114
Chapter 9	SNMP Master Agent Configuration Options	115
	Setting Configuration Options.....	115
	Mandatory Options	116
	agentx Section.....	116
	snmp Section.....	117
	snmp-v3-auth Section.....	120

	snmp-v3-priv Section	120
	Changes from 8.1 to 8.5	121
Chapter 10	Host Configuration Options	123
	Setting Configuration Options	123
	Mandatory Options	123
	addp Section	124
	ntp-service-control Section	124
	rdm Section	125
	security Section	125
	Changes from 8.1 to 8.5	129
Chapter 11	Tenant and User Configuration Options	131
	Setting Configuration Options	131
	Mandatory Options	132
	Passwords in Configurations with Multiple Tenants	132
	security-authentication-rules Section	133
	Tenant-level Options	133
	User-level Options	140
	Changes from 8.1 to 8.5	142
Supplements	Related Documentation Resources	143
	Document Conventions	145
Index	147



Preface

Welcome to the *Framework 8.5 Configuration Options Reference Manual*. This document describes the configuration options for the Genesys Framework 8.5 components, which you must configure in the Configuration Layer. This document is designed to be used along with the *Framework 8.5 Deployment Guide*.

This document is valid only for the 8.5 release(s) of the Genesys Framework.

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

This preface contains the following sections:

- [About Configuration Options, page 7](#)
- [Intended Audience, page 8](#)
- [Making Comments on This Document, page 8](#)
- [Contacting Genesys Customer Care, page 8](#)
- [Changes in This Document, page 9](#)

For information about related resources and about the conventions that are used in this document, see the supplementary material starting on [page 143](#).

About Configuration Options

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

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.
- 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@genesys.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 Customer Care 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 Customer Care

If you have purchased support directly from Genesys, please contact [Genesys Customer Care](#).

Before contacting Customer Care, please refer to the [Genesys Care Support Guide for On-Premises](#) for complete contact information and procedures.

Changes in This Document

Version 8.5.104.00

This document has been updated to support Management Framework release 8.5.1. Changes for each component are summarized in the “Changes from 8.1 to 8.5” sections at the end of each chapter.

The following table summarizes the changes specific to this release of the document:

Table 1: Changes in Configuration Options Reference Manual version 8.5.104.00

Component	Section	Options
Common	log	snapshot
	security	sec-protocol
	Transport Parameters	sec-protocol
Configuration Server	Configuration Server	allow-empty-password
Configuration Server		allow-external-empty-password
	Application Parameter	user
Configuration Server Proxy	Application Parameter	user
Host	security	sec-protocol
User object	security-authentication-rules	account-override-lockout

Version 8.5.103.00

This document has been updated to support Management Framework release 8.5.1. Changes for each component are summarized in the “Changes from 8.1 to 8.5” sections at the end of each chapter.

The following table summarizes the changes specific to this release of the document:

Table 2: Changes in Configuration Options Reference Manual version 8.5.103.00

Component	Section	Options
Configuration Server	Configuration Server	packet-size

Table 2: Changes in Configuration Options Reference Manual version 8.5.103.00

Component	Section	Options
Configuration Server Proxy	csproxy	packet-size
		proxy-cluster-name
LCA	general	wmiquery-timeout

Version 8.5.102.00

This document has been updated to support Management Framework release 8.5.1. Changes for each component are summarized in the “Changes from 8.1 to 8.5” sections at the end of each chapter.

The following table summarizes the changes specific to this release of the document:

Table 3: Changes in Configuration Options Reference Manual version 8.5.102.00

Component	Section	Options
Configuration Server	Configuration Server	allow-mixed-encoding
	system	postgre-standard-conforming-strings

Version 8.5.101.00

This document has been updated to support Management Framework release 8.5.1. Changes for each component are summarized in the “Changes from 8.1 to 8.5” sections at the end of each chapter.

The following table summarizes the changes specific to this release of the document:

Table 4: Changes in Configuration Options Reference Manual version 8.5.101.00

Component	Section	Options
Common	security	cipher-list, sec-protocol, tls-mutual
	Transport Parameters	cipher-list, sec-protocol
Configuration Server	Configuration Server	decryption-key, encryption
	system	postgre-standard-conforming-strings
Message Server	messages	thread-mode, thread-pool-size

Table 4: Changes in Configuration Options Reference Manual version 8.5.101.00

Component	Section	Options
Solution Control Server	general	<code>distributed_sync_timeout</code>
Host	security	<code>cipher-list</code> , <code>sec-protocol</code>

Version 8.5.001.00

This is the first release of the *Framework 8.5 Configuration Options Reference Manual*.



Chapter

1

Common Configuration Options

Unless otherwise noted, the common configuration options that this chapter describes are common to all Framework server components. They may also be used by other Genesys server applications; refer to product-specific documentation to determine if these options apply to your product.

This chapter includes the following sections:

- [Setting Configuration Options, page 13](#)
- [Mandatory Options, page 14](#)
- [Common Log Options, page 14](#)
- [Common Security Options, page 30](#)
- [sml Section, page 38](#)
- [common Section, page 40](#)
- [Transport Parameter Options, page 41](#)
- [Changes from 8.1 to 8.5, page 48](#)

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 for that application.

Setting Configuration Options

Unless specified otherwise, use Genesys Administrator to set common configuration options in the options of the Application object, using the following navigation path:

Application object > Options tab > Advanced View (Options)

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

Mandatory Options

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

Common Log Options

This section contains all options relating to creating, viewing, and otherwise using the Centralized Log facility in Genesys software.

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.

buffering

Default Value: `true`

Valid Values:

<code>true</code>	Enables buffering.
<code>false</code>	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 21](#)). 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.

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.

enable-threadDefault Value: `false`Valid Values: `true`, `false`

Changes Take Effect: Immediately

Specifies whether to enable or disable the logging thread. If set to `true` (the logging thread is enabled), the logs are stored in an internal queue to be written to the specified output by a dedicated logging thread. This setting also enables the log throttling feature, which allows the `verbose` level to be dynamically reduced when a logging performance issue is detected. Refer to the *Framework 8.5 Management Framework User's Guide* for more information about the log throttling feature.

If this option is set to `false` (the logging thread is disabled), each log is written directly to the outputs by the thread that initiated the log request. This setting also disables the log throttling feature.

expireDefault Value: `10`

Valid Values:

<code>false</code>	No expiration; all generated segments are stored.
<code><number> file</code> or <code><number></code>	Sets the maximum number of log files to store. Specify a number from 1–1000.
<code><number> day</code>	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-fileDefault Value: `false`

Valid Values:

<code>false</code>	No startup segment of the log is kept.
<code>true</code>	A startup segment of the log is kept. The size of the segment equals the value of the <code>segment</code> option.
<code><number> KB</code>	Sets the maximum size, in kilobytes, for a startup segment of the log.
<code><number> MB</code>	Sets the maximum size, in megabytes, for a startup segment of the log.

Changes Take Effect: After restart

Specifies whether a startup segment of the log, containing the initial configuration options, 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 is set to `false`).

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 21](#)). 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, the application does not create a snapshot file (with the extension `*.memory.log`). Logging output to a file at a network location is not recommended and could cause performance degradation.

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 21](#).

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.

messagefile

Default Value: As specified by a particular application

Valid Values: Any valid message file (`<filename>.lms`)

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.

no-memory-mapping

Default Value: `false`

Valid Values: `true`, `false`

Changes Take Effect: At restart

Specifies if memory-mapped files, including memory log output (with file extension `.memory.log`) and snapshot files (with file extension `.snapshot.log`) are disabled for file outputs.

print-attributesDefault 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 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.

segmentDefault Value: `100 MB`

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.

snapshot

Default Value: No value

Valid Values:

- No value or not specified (default) Snapshot is created in log output folder.
- `<path>/<folder>` Full or relative path and folder in which snapshot is created.

Changes Take Effect: Immediately

A snapshot file is created for each log output file to temporarily store logs that have not been flushed to the log file. This option specifies the folder, either a full path or a path relative to the application's working directory, in which the

application creates the memory-mapped snapshot file associated with the log file. If this option is not configured, or a value is not specified (the default), the file is created in the log output folder.

Note: Do not write the snapshot file to a network drive, because disconnection of the network drive might cause application failure. If the application detects that the output folder is a network drive, the snapshot file will be disabled. However, this detection may not be possible for Storage Area Network (SAN) devices because of operating system limitations.

spool

Default Value: The application's working directory

Valid Values: Any valid 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.

throttle-period

Default Value: 30

Valid Values: 0–3600

Changes Take Effect: Immediately

Specifies, in seconds, how long to keep the throttled [verbose](#) level. When this period of time has expired, the original log verbose level will be restored when the log queue size has decreased to less than 50% of the threshold.

Note: This option applies only if [enable-thread](#) is set to true.

throttle-threshold

Default Value: 5000

Valid Values: 0–10000

Changes Take Effect: Immediately

Specifies the size of the internal log queue at which the [verbose](#) level is to be reduced so as to lessen the load generated by logging. If this option is set to 0 (zero), throttling does not occur. For more information about log throttling, refer to the *Framework 8.5 Management Layer User's Guide*.

Note: This option applies only if [enable-thread](#) is set to true.

time_convertDefault 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 00:00:00 UTC, January 1, 1970.

time_formatDefault 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
```

verboseDefault 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 Trace level and higher (that is, log events of Standard, Interaction, and Trace levels) are generated, but log events of the Debug level are not generated.
- `interaction` Log events of Interaction level and higher (that is, log events of Standard and Interaction levels) are generated, but log events of Trace and Debug levels are not generated.
- `standard` Log events of Standard level are generated, but log events of Interaction, Trace, and Debug levels are not generated.
- `none` No log output is produced.

Changes Take Effect: Immediately

Specifies if log output is created, and if so, the minimum level of log events generated. Log event levels, starting with the highest priority level, are Standard, Interaction, Trace, and Debug. See also “Log Output Options” on [page 21](#).

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

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 25](#).

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.

<code>memory</code>	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
<code>[filename]</code>	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):

<code>stdout</code>	Log events are sent to the Standard output (<code>stdout</code>).
<code>stderr</code>	Log events are sent to the Standard error output (<code>stderr</code>).
<code>network</code>	Log events are sent to Message Server, which resides anywhere on the network, and Message Server stores the log events in the Log Database.
<code>memory</code>	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
<code>[filename]</code>	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:

```
alarm = stderr, network
```

standard

Default Value: No default value

Valid Values (log output types):

<code>stdout</code>	Log events are sent to the Standard output (<code>stdout</code>).
<code>stderr</code>	Log events are sent to the Standard error output (<code>stderr</code>).
<code>network</code>	Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database.
<code>memory</code>	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):

<code>stdout</code>	Log events are sent to the Standard output (<code>stdout</code>).
<code>stderr</code>	Log events are sent to the Standard error output (<code>stderr</code>).
<code>memory</code>	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
<code>[filename]</code>	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 Customer Care 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 Customer Care 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-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 Customer Care.

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 Customer Care.

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 Customer Care.

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 Customer Care.

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 Customer Care.

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 Customer Care.

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 Customer Care.

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 Customer Care.

log-extended Section

This section must be called log-extended.

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.

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 option [level-reassign-disable](#) option.

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.

Common Security Options

Common security options are used to implement some security features in Genesys software. These options are configured on supporting `Application` objects.

In addition to the options described in this section, also see “Transport Parameter Options” on [page 41](#).

For information about the security features that use these options, refer to the *Genesys Security Deployment Guide*.

Filtering and/or Tagging Data in Logs

log-filter Section

The `log-filter` section contains configuration options used to define the default treatment of filtering data in log output. Specifically, it defines the treatment of all KV pairs in the User Data, Extensions, and Reasons attributes of the log.

This section must be called `log-filter`.

default-filter-type

Default Value: `copy`

Valid Values: One of the following:

<code>copy</code>	The keys and values of the KVList pairs in the User Data, Extensions, or Reasons attribute are copied to the log.
<code>hide</code>	The keys of the KVList pairs in the User Data, Extensions, or Reasons attribute are copied to the log; the values are replaced with asterisks.
<code>hide-first, <n></code>	The keys of the KVList pairs in the User Data, Extensions, or Reasons attribute are copied to the log; the first <n> characters of the value are replaced with asterisks. If <n> exceeds the number of characters in the value, the number of asterisks will be equal to the number of characters in the value.
<code>hide-last, <n></code>	The keys of the KVList pairs in the User Data, Extensions, or Reasons attribute are copied to the log; the last <n> characters of the value are replaced with asterisks. If <n> exceeds the number of characters in the value, the number of asterisks will be equal to the number of characters in the value.
<code>skip</code>	The KVList pairs in the User Data, Extensions, or Reasons attribute are not copied to the log.

`tag[(<tag-prefix>, <tag-postfix>)]` The KVList pairs in the User Data, Extensions, or Reasons attribute are tagged with the prefix specified by `<tag-prefix>` and the postfix specified by `<tag-postfix>`. If the two parameters are not specified, the default tags `<#` and `#>` are used as prefix and postfix, respectively.

To use the default tags, you can use any of the following values:

- `tag`
- `tag()`
- `tag(,)`

To define your own tags, replace the two parameters in the value with your tags. Your own tag can be any string up to 16 characters in length; any string longer than that will be truncated. If the string includes a blank space or any of the characters `,` (comma), `(`, or `)` as start and stop characters, they will not be counted as part of the length of the string.

`unhide-first, <n>` The keys of the KVList pairs in the User Data, Extensions, or Reasons attribute are copied to the log; all but the first `<n>` characters of the value are replaced with asterisks. If `<n>` exceeds the number of characters in the value, the value of the key appears, with no asterisks.

`unhide-last, <n>` The keys of the KVList pairs in the User Data, Extensions, or Reasons attribute are copied to the log; all but the last `<n>` characters of the value are replaced with asterisks. If `<n>` exceeds the number of characters in the key, the value of the key appears, with no asterisks.

Changes Take Effect: Immediately

Specifies the default way of presenting KVList information (including User Data, Extensions, and Reasons) in the log. This setting will be applied to all KVList pairs in the User Data, Extensions, or Reasons attribute except those that are explicitly defined in the `log-filter-data` section.

Refer to the “Hide Selected Data in Logs” chapter in the *Genesys Security Deployment Guide* for information about how to use this option.

filtering

Default Value: `true`

Valid Values: `true`, `false`

Changes Take Effect: Immediately, if application is subscribed to notifications that this option has been changed.

Enables (`true`) or disables (`false`) log filtering at the Application level.

log-filter-data Section

The `log-filter-data` section defines the treatment of specific KV pairs in the User Data, Extensions, and Reasons attributes of the log. It overrides the general settings in the `log-filter` section.

This section must be called `log-filter-data`.

<key-name>

Default Value: No default value

Valid Values: One of the following:

<code>copy</code>	The key and value of the given KVList pair in the User Data, Extensions, or Reasons attribute is copied to the log.
<code>hide</code>	The key of the given KVList pair in the User Data, Extensions, or Reasons attribute is copied to the log; the value is replaced with a string of asterisks.
<code>hide-first, <n></code>	The key of the given KVList pair in the User Data, Extensions, or Reasons attribute is copied to the log; the first <n> characters of the value are replaced with asterisks. If <n> exceeds the number of characters in the value, the number of asterisks will be equal to the number of characters in the value.
<code>hide-last, <n></code>	The key of the given KVList pair in the User Data, Extensions, or Reasons attribute is copied to the log; the last <n> characters of the value are replaced with asterisks. If <n> exceeds the number of characters in the value, the number of asterisks will be equal to the number of characters in the value.
<code>skip</code>	The KVList pair in the User Data, Extensions, or Reasons attribute is not copied to the log.
<code>tag[(<tag-prefix>, <tag-postfix>)]</code>	The KVList pair in the User Data, Extensions, or Reasons attribute is tagged with the prefix specified by <tag-prefix> and the postfix specified by <tag-postfix>. If the two parameters are not specified, the default tags <# and #> are used as prefix and postfix, respectively.

To use the default tags, you can use any of the following values:

- `tag`
- `tag()`
- `tag(,)`

To define your own tags, replace the two parameters in the value with your tags. Your own tag can be any string up to 16 characters in length, and cannot include a blank space or any of the characters `,` (comma), `(`, or `)`. If the string is longer than 16 characters, it will be truncated.

- `unhide-first, <n>` The key of the given KVList pair in the User Data, Extensions, or Reasons attribute is copied to the log; all but the first <n> characters of the value are replaced with asterisks. If <n> exceeds the number of characters in the value, the value of the key appears, with no asterisks.
- `unhide-last, <n>` The key of the given KVList pair in the User Data, Extensions, or Reasons attribute is copied to the log; all but the last <n> characters of the value are replaced with asterisks. If <n> exceeds the number of characters in the value, the value of the key appears, with no asterisks.

Changes Take Effect: Immediately

Specifies the way of presenting the KVList pair defined by the key name in the log. This setting supersedes the default way of KVList presentation as defined in the `log-filter` section for the given KVList pair.

If no value is specified for this option, no additional processing of this data element is performed.

Note: For T-Server Application objects, if the T-Server common configuration option `log-trace-flags` is set to `-udata`, it will disable writing of user data to the log regardless of the settings of any options in the `log-filter-data` section. Refer to the documentation for your particular T-Server for information about the `log-trace-flags` option.

Refer to the chapter “Hide Selected Data in Logs” in the *Genesys Security Deployment Guide* for complete information about how to use this option.

TLS Options

security Section

The `security` section contains configuration options used to specify security elements for your system. This section must be called `security`.

cipher-list

Default Value: No default value

Valid Values: The list of ciphers

Changes Take Effect: After component restart

Related Option: [crl](#)

Specifies the defined list of ciphers. The cipher list must be in a valid format. See the chapter “Genesys TLS Configuration” in the *Genesys Security Deployment Guide* for information about cipher formatting rules and examples of valid cipher strings.

This option can be configured at the host, application, or connection (port) level. This section assumes you are configuring it at the application level. To configure it at another level, refer to:

- To configure it at the port level, see [page 43](#).
- To configure it at the host level, see [page 126](#).

Note: If this option is configured at multiple levels (connection, application, host), the value set at the lowest level takes precedence. That is:

- The value set at the connection level takes precedence over the value set at the application and host levels.
 - The value set at the application level takes precedence over the value set at the host level.
-

client-auth

Default Value: 1

Valid Values: 0, 1

Changes Take Effect: After application restart

Specifies whether authentication of the security certificate in the client TLS socket is to be disabled. When set to 1 (default), authentication is enabled. When set to 0, the client socket does not authenticate the server when connected over TLS.

This option must be set at the same level where the certificate itself is configured. Use this option if the security certificate is configured at the application level. If it is configured at another level, do one of the following:

- If the security certificate is configured at the connection level, see [page 44](#).
- If the security certificate is configured at the host level, see [page 126](#).

Note: If this option is configured at multiple levels (connection, application, host), the value set at the lowest level takes precedence. That is:

- The value set at the connection level takes precedence over the value set at the application and host levels.
 - The value set at the application level takes precedence over the value set at the host level.
-

sec-protocol

Default Value: SSLv23

Valid Values: SSLv23, SSLv3, TLSv1, TLSv11, TLSv12

Changes Take Effect: Immediately

Specifies the protocol used by the component to set up secure connections. Exactly how this option behaves depends on the platform on which the application, for which the option is configured, is running.

When configured on the Windows platform, this option complements Windows operating system settings that enable and disable a particular secure

protocol. If there is a conflict between Windows settings and this option, the operating system settings are used.

Note: On the Windows platform, this option applies to only a limited number of 8.5.x components. Check the documentation for your particular component to see if this option does apply, and if so, if there are additional limitations.

On UNIX and Linux platforms, this option controls how the Security Pack on UNIX selects the protocol to use, as shown in [Table 5](#).

Table 5: Values for sec-protocol option

Option Value	SSL Protocol Version			TLS Protocol Version		
	2 ^a	2.3	3	1	1.1	1.2
SSLv23 ^b	X	X	X	X	X	X
SSLv3			X			
TLSv1				X		
TLSv11					X	
TLSv12						X

- SSL 2 is supported only if SSL 2 ciphers are explicitly defined. In this case, SSL 2 clients can connect only to servers running in SSLv23 mode.
- SSL 2.3 is compatible with all other supported versions, and connects to a client running in the highest mode used by the client.

For more information about using this option on UNIX and Linux platforms, refer to “Genesys Implementation of Secure Protocol Connections” in the [Framework 8.5 Deployment Guide](#).

Where this option is configured depends on the component on which it is configured. Specific components might have different places where this option can be set. Applicability may also differ, based on whenever they made connections as clients or open listening ports as servers. Check with the documentation for the particular component to see if there are any additional limitations.

In Framework, this option is configured on one of three levels:

- Host-level (the application host): In the `security` section of the annex of the Host object.
- Application-level: In the `security` section of the options of the Application object.

- **Port-level (connection-level):** As a transport parameter of the application's connection.

If the component reads its configuration information solely from its configuration file, such as LCA or Genesys Deployment Agent, set this option in the `security` section of the appropriate configuration file (such as `lca.cfg` for LCA or `gda.cfg` for Genesys Deployment Agent).

On a single component, this option must be set at the same level where the security certificate is configured. Use this option if the security certificate is configured at the application level. If it is configured at another level, do one of the following:

- If the security certificate is configured at the connection level, see [page 45](#).
- If the security certificate is configured at the host level, see [page 126](#).

Note: If this option is configured at multiple levels (connection, application, host) across the network, the value set at the lowest level takes precedence. That is:

- The value set at the connection level takes precedence over the value set at the application and host levels.
 - The value set at the application level takes precedence over the value set at the host level.
-

tls-mutual

Default Value: 0

Valid Values: 0, 1

Changes Take Effect: Immediately

Specifies if mutual TLS is used for secure data transfer. If set to 1, TLS certificates must be configured on both the server and client applications. If set to 0 (the default), client certificates are not required, and either simple TLS or data encryption (if `client-auth=0`) is used.

tls-target-name-check

Default Value: no

Valid Values: no, host

Changes Take Effect: After component restart

Specifies whether the subject field in the server's certificate will be compared to the target host name (option value `host`). If they are not identical, the connection fails. If the option is set to `no`, a comparison is not made, and the connection is allowed.

Secure User Authentication

security-authentication-rules Section

The `security-authentication-rules` section contains configuration options that relate to user accounts and user passwords. Refer to the chapter “User Passwords” in the *Genesys Security Deployment Guide* for full information about how to use these options.

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

no-change-password-at-first-login

Default Value: `false`

Valid Values: `false`, `true`

Changes Take Effect: At the next attempt to log in to this application

Specifies whether this application supports password change when a user first logs in. If set to `true`, this application can override of the policy of changing passwords at first login. If set to `false` (the default), this application supports password change at first login.

This option does not apply if the `force-password-reset` option is set to `true` at the Tenant level, enforcing the current policy of changing passwords at first login.

Note: This option is set in the options of the `Application` object.

sml Section

This section must be called `sml`.

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

- `Application object > Options tab > Advanced View (Annex)`

Warning! Use the `hangup-restart`, `heartbeat-period`, and `heartbeat-period-thread-class-<n>` options with great care, and only with those applications for 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.

autostart

Default Value: `false`

Valid Values: `true`, `false`

Changes Take Effect: After restart of the application

Specifies if SCS can start this application automatically every time that SCS establishes a connection with LCA, and if LCA does not report this application as Started.

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 user intervention.

If set to false, specifies that LCA is only to generate a notification that the application has stopped responding; the application is not automatically restarted.

Note: This option is set to true automatically in Solution Control Server; any other value is ignored.

heartbeat-period

Default Value: None

Valid Values:

- 0 This method of detecting an unresponsive application is not used by this application.
- <min value>-604800 Length of timeout, in seconds, where min value is:
 - 40 seconds for Configuration Server and Solution Control Server.
 - 10 seconds for applications that support hangup detection if you are using Solution Control Server 8.1.1 (or later).

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.

Note: Genesys does not recommend that you set the heartbeat period option for Configuration Server and Solution Control Server if you are using Solution Control Server 8.1.0.(or earlier).

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.

Note: Do not set this option to a value less than the `heartbeat-period` option.

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.

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). 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: 0

Valid Values:

- 0 Disables asynchronous processing of DNS requests.
- 1 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 Customer Care.
 - Use this option only with T-Servers.
-

enable-ipv6

Default Value: 0

Valid Values:

- 0 Off (default), IPv6 support is disabled.
- 1 On, IPv6 support is enabled.

Changes Take Effect: Immediately

When set to 1, specifies that this application supports IPv6. It is set to 0 by default to ensure backward compatibility. Refer to component-specific documentation and the *Framework Deployment Guide* for more information about IPv6 and any specific considerations for deploying IPv6 in your situation.

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 Customer Care.
-

Transport Parameter Options

Set options in this section in the `Transport Parameters` of the connection's properties. Transport Parameter options are not associated with a configuration option section, and do not appear in the options or annex of an `Application` object.

transport In a configuration file, these options appear in the following format:
Option `transport = <option name>=<value>; <option name>=<value>; ...`
 Collectively, the options make up the parameters of the transport option.
 When entering the options in Genesys Administrator, only the options are required; `transport =` is prefixed automatically to the list of option/value pairs.

Note: Valid values for these options must have no spaces before or after the delimiter characters “;” (semi-colon) and “=”.

Configuring Client-side Port Definition

This Transport Parameter options in this section are used to configure client-side port definition, Refer to the chapter “Client-Side Port Definition” in the *Genesys Security Deployment Guide* for information about how to use these options.

Set these options in the following navigation path in Genesys Administrator:

- Application object > Configuration tab > General section > Connections > <Connection> > Connection Info > Advanced tab > Transport Parameters

port

Default Value: No default value

Valid Values: A valid port number

Changes Take Effect: After client application restart

The port that the client application uses for its TCP/IP connection to the server.

address

Default Value: No default value

Valid Values: A valid IP address

Optional. Specifies the IP address or host name that a client uses for its TCP/IP connection to the server.

backup-port

Default Value: No default value

Valid Values: A valid port number

Changes Take Effect: After client application restart

In an HA pair, the port on the backup server that the client application will use for its TCP/IP connection to the server.

Note: If the client application servers are in an HA pair, the port and backup-port values will be propagated from the primary server to the backup. As a result, after switchover, these ports will be in use by another server, so the new primary client application will be unable to open and use them.

To prevent this, Genesys recommends that you do one of the following:

- Locate the backup pair on different hosts.
 - Manually change the port and backup-port settings for the backup server.
-

Configuring Secure Connections Using Security Certificates

The options in this section are used to define the use of security certificates and configuring secure connections between components. Refer to the chapter “Genesys TLS Configuration” in the *Genesys Security Deployment Guide* for more information about security certificates, configuring secure connections, and TLS security.

Some options used to configure secure connections using security certificates may not be configured as Transport Parameter options, either directly or depending on the situation. Refer also to “TLS Options” on [page 34](#) to see those options configured in security section.

Set options in this section in one of the following locations:

- In the Transport Parameters of the port’s properties, using the following navigation path in Genesys Administrator:
Application object > Configuration tab > General section > Connections > Connection Info > Network Security tab > Transport Parameters
- If the component reads its configuration information solely from its configuration file, such as LCA or Genesys Deployment Agent, in the security section of the appropriate configuration file.

cipher-list

Default Value: No default value

Valid Values: The list of ciphers

Changes Take Effect: After component restart

Related Option: [crl](#)

Specifies the defined list of ciphers. The cipher list must be in a valid format. See the chapter “Genesys TLS Configuration” in the *Genesys Security Deployment Guide* for information about cipher formatting rules and examples of valid cipher strings.

This option can be configured at the host, application, or connection (port) level. This section assumes you are configuring it at the port level. To configure it at another level, refer to:

- To configure it at the application level, see [page 34](#).
- To configure it at the host level, see [page 126](#).

Note: If this option is configured at multiple levels (connection, application, host), the value set at the lowest level takes precedence. That is:

- The value set at the connection level takes precedence over the value set at the application and host levels.
 - The value set at the application level takes precedence over the value set at the host level.
-

client-auth

Default Value: 1

Valid Values: 0, 1

Changes Take Effect: After application restart

Specifies whether authentication of the security certificate in the client TLS socket is to be disabled. When set to 1 (default), authentication is enabled. When set to 0, the client socket does not authenticate the server when connected over TLS.

This option must be set at the same level where the certificate itself is configured. Use this option if the security certificate is configured at the port level. If it is configured at another level, do one of the following:

- If the security certificate is configured at the application level, see [page 35](#).
- If the security certificate is configured at the host level, see [page 126](#).

Note: If this option is configured at multiple levels (connection, application, host), the value set at the lowest level takes precedence. That is:

- The value set at the connection level takes precedence over the value set at the application and host levels.
 - The value set at the application level takes precedence over the value set at the host level.
-

crl

Default Value: No default value

Valid Values: Valid file name

Changes Take Effect: After a server restart

Related Option: [cipher-list](#)

Specifies the name of the file that contains one or more certificates in PEM format, defining the Certificate Revocation List. As part of the authentication process, the system checks whether a presented certificate is included in this list of revoked certificates before completing authentication.

Note: Configuration of a CRL in SIP Server differs slightly from other Genesys components. Refer to the *Framework SIP Server Deployment Guide* for more information.

sec-protocol

Default Value: SSLv23

Valid Values: SSLv23, SSLv3, TLSv1, TLSv11, TLSv12

Changes Take Effect: Immediately

Specifies the protocol used by the component to set up secure connections. Exactly how this option behaves depends on the platform on which the application, for which the option is configured, is running.

When configured on the Windows platform, this option complements Windows operating system settings that enable and disable a particular secure protocol. If there is a conflict between Windows settings and this option, the operating system settings are used.

Note: On the Windows platform, this option applies to only a limited number of 8.5.x components. Check the documentation for your particular component to see if this option does apply, and if so, if there are additional limitations.

On UNIX and Linux platforms, this option controls how the Security Pack on UNIX selects the protocol to use, as shown in [Table 6](#).

Table 6: Values for sec-protocol option

Option Value	SSL Protocol Version			TLS Protocol Version		
	2 ^a	2.3	3	1	1.1	1.2
SSLv23 ^b	X	X	X	X	X	X
SSLv3			X			
TLSv1				X		
TLSv11					X	
TLSv12						X

- SSL 2 is supported only if SSL 2 ciphers are explicitly defined. In this case, SSL 2 clients can connect only to servers running in SSLv23 mode.
- SSL 2.3 is compatible with all other supported versions, and connects to a client running in the highest mode used by the client.

For more information about using this option on UNIX and Linux platforms, refer to “Genesys Implementation of Secure Protocol Connections” in the [Framework 8.5 Deployment Guide](#).

This option is configured on one of three levels:

- **Host-level (the application host):** In the `security` section of the annex of the Host object.
- **Application-level:** In the `security` section of the options of the Application object.
- **Port-level (connection-level):** As a transport parameter of the application's connection.

If the component reads its configuration information solely from its configuration file, such as LCA or Genesys Deployment Agent, set this option in the `security` section of the appropriate configuration file (such as `lca.cfg` for LCA or `gda.cfg` for Genesys Deployment Agent).

On a single component, this option must be set at the same level where the security certificate is configured. Use this option if the security certificate is configured at the port (connection) level. If it is configured at another level, do one of the following:

- If the security certificate is configured at the application level, see [page 35](#).
- If the security certificate is configured at the host level, see [page 126](#).

Note: If this option is configured at multiple levels (connection, application, host) across the network, the value set at the lowest level takes precedence. That is:

- The value set at the connection level takes precedence over the value set at the application and host levels.
 - The value set at the application level takes precedence over the value set at the host level.
-

tls

Default Value: `tls=0`

Valid Values:

`tls=0`

Regular (unsecured) connections will be used.

For Windows:

Secure connections will be used, where

`tls=1; certificate=<value>`

`certificate` = certificate value.

For UNIX:

```
tls=1; certificate=<path>;
[certificate-key=<path>];
trusted-ca=<path>
```

Secure connections will be used, where:

- `certificate`—full path to the `<serial_#>_<host_name>_cert.pem` file
- `certificate-key`—full path to the `<serial_#>_<host_name>_priv_key.pem` file (unless the private key is stored together with a certificate)
- `trusted-ca`—full path to the `ca_cert.pem` file

This option is used to enable the set up of secure connections between Genesys components. Refer to the section “Configuring Secure Configuration Server and DB Server Connections” in the *Genesys Security Deployment Guide* for information about how to use this option.

You also specify the `transport` option in any section of the DB Server configuration file that contains port configuration.

Configuring Mixed IPv4 and IPv6 Environments

For connections with servers that support both IPv4 and IPv6, use the `ip-version` transport parameter option to specify which version to use.

ip-version

Default Value: 4, 6

Valid Values: 4, 6 and 6, 4

Changes Take Effect: At restart

Specifies the order in which IPv4 (4) and IPv6 (6) are used for the connection with a server that has a mixed IPv4/IPv6 configuration. This parameter has no effect if the environment variable `GCTI_CONN_IPV6_ON` or the option `enable-ipv6` is set to 0.

[Table 7](#) summarizes how this parameter affects the connection for which it is configured.

Table 7: IP Version Selected by ip-version Parameter/Option

Connecting Server	ip-version=4,6	ip-version=6,4
Supports only IPv4	IPv4 is used	IPv4 is used
Supports only IPv4 and IPv6	IPv4 is used	IPv6 is used
Supports only IPv6	IPv6 is used	IPv6 is used

For more information about IPv6, refer to the “Solution Availability” and “IPv6” sections of the *Framework Deployment Guide*.

Changes from 8.1 to 8.5

Table 8 on [page 48](#) lists all changes to common configuration options between release 8.1 and the latest 8.5 release.

Table 8: Common Configuration Option Changes from 8.1 to 8.5

Option Name	Option Values	Type of Change	Details
log Section			
compatible-output-priority	true, false	Removed	
enable-thread	true, false	New	See description on page 15 .
expire	false, <number> [file day]	Changed Default Value	See description on page 15 . Previous Default Value: false
message-format	short, full	Renamed	See description on page 16 . Previously named message_format
no-memory-mapping	true, false	New	See description on page 17 . Added in earlier release; not previously documented.
segment	false, <number> [KB MB hr]	Changed Default Value	See description on page 18 . Previous Default Value: false
snapshot	empty string; valid path/folder name; 0	New	See description on page 18 .
throttle-period	0–3600	New	See description on page 19 .
throttle-threshold	0–10000	New	See description on page 19 .
security Section			
cipher-list	List of ciphers	Modified	See description on page 34 . To configure cipher list at Application level. Documented incorrectly in previous release.
sec-protocol	SSLv23, SSLv3, TLSv1, TLSv11	New	See description on page 35 . If security certificate configured at Application level.

Table 8: Common Configuration Option Changes from 8.1 to 8.5 (Continued)

Option Name	Option Values	Type of Change	Details
tls-mutual	0, 1	New	See description on page 37 .
sml Section			
autostart	true, false	New	See description on page 38 . Added in earlier release; not previously documented.
dbserver Section (removed)			
dml-retry	0-32766	Moved	Moved to Configuration Server chapter. See page 69 . Documented incorrectly in previous release.
Transport Parameter Options			
cipher-list	List of ciphers	Modified	See description on page 43 . To configure cipher list at port level. Documented incorrectly in previous release.
ip-version	4, 6 and 6, 4	New	See description on page 47 . Added in release 8.1; not previously documented.
sec-protocol	SSLv23, SSLv3, TLSv1, TLSv11	New	See description on page 45 . If security certificate configured at port level.



Chapter

2

Database Access Point Configuration Options

This chapter describes configuration options for a Database Access Point.

This chapter contains the following sections:

- [Setting Configuration Options, page 51](#)
- [Mandatory Options, page 51](#)
- [default Section, page 51](#)
- [dbclient Section, page 52](#)
- [Changes from 8.1 to 8.5, page 52](#)

Setting Configuration Options

Refer to the description of the particular option for information about where to set its value. Configuration section names, configuration option names, and predefined option values are case-sensitive. Type them in Genesys Administrator 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 the application 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 the application interprets this as a DBMS failure.

**Setting this
Option**

Set this option in Genesys Administrator at the following location:

Database Access Point Application object > Configuration tab > DB Info section > Query Timeout field

dbclient Section

This section must be called `dbclient`.

utf8-ucs2

Default Value: false

Valid Values: true, false

Changes Take Effect: At startup

This option applies only if you are working with an MS SQL Log Database that has been initialized as a multi-language database. MS SQL uses UCS-2 encoding instead of UTF-8. Setting this option to `true` forces the transcoding of UTF-8 to UCS-2 encoding before writing to the MS SQL database, and the transcoding of UCS-2 to UTF-8 encoding after reading from the database. Therefore, the MS SQL database is able to work with other components encoded using UTF-8.

**Setting this
Option**

Set this option in Genesys Administrator, at the following location:

Database Access Point Application object > Configuration tab > UTF-8 for MSSQL field.

Changes from 8.1 to 8.5

There are no changes to Database Access Point options between release 8.1 and the latest 8.5 release.

3

Configuration Server Configuration Options

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

- [Setting Configuration Options, page 53](#)
- [Startup Options in Configuration File, page 54](#)
- [Runtime Options in Configuration Database, page 70](#)
- [Application Parameter Options, page 75](#)
- [Transport Parameter Options, page 76](#)
- [Sample Configuration Server Configuration File, page 77](#)
- [Changes from 8.1 to 8.5, page 78](#)

Setting Configuration Options

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

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

Warning! Configuration section names, configuration option names, and predefined option values are case-sensitive. Type them in the configuration file or Genesys Administrator 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 54](#) 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 70](#) for descriptions of the runtime options. Refer to *Framework Genesys Administrator Help* for additional information about the Options tab, and how to manage configuration options on it.

Startup Options in Configuration File

These options are located in the Configuration Server configuration file. At first startup of the master Configuration Server, the configuration file is named `confserv.cfg` (on Windows) or `confserv.conf` (on UNIX) by default. This file can be renamed as required, but must be specified by the `-c` command-line option at startup. If there is a Configuration Server section in the configuration file other than `confserv`, you must use the `-c <section>` parameter in the command line to make sure that Configuration Server is using configuration settings from that section. The section name must also match the name of the Configuration Server object.

-
- Note:**
- If you have a configuration file and/or a Configuration Server section with a name other than the default, you must specify the parameters `-c <config file name>` and/or `-s <Configuration Server section name>` in the command line when starting this instance of Configuration Server. This is in addition to any other command-line options that you want to use, whenever you start Configuration Server or any command-line utility modes provided by Configuration Server.
 - Options in the Configuration Server and `dbserver` sections are always read from the configuration file and re-saved to the Configuration Database at each startup. Values from the database are ignored. Genesys Administrator restricts the editing of such options in runtime. Some options in these sections are exempt from this rule, such as the `port` option. See the option descriptions for details.
 - Options in the `log` section of the configuration file apply up to the point that Configuration Server is fully initialized. After initialization is complete, log options stored in the Configuration Database are applied. You can still use the `log` section in the configuration file to change options that are in effect during startup, but be aware that they will be overridden with those in the database.
-

Mandatory Startup Options

[Table 9](#) lists the Configuration Server options for which you must provide values; otherwise, Configuration Server will not start. These options are provided during the installation of Configuration Server and then written to the configuration file.

Table 9: Mandatory Options

Option Name	Default Value	Details
Configuration Server Section		
langid	1033	See the description on page 62
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 66 .
server	No default value	See the description on page 66 .
Configuration Database Section		
host	No default value	Used only if <code>dbthread=false</code> , in which case they are mandatory. Refer to Framework 8.1 documentation for descriptions of these options.
port	No default value	
dbengine	No default value	See the description on page 69 .
dbname	No default value	You must specify a value for this option unless <code>dbengine=oracle</code> . See the description on page 69 .
dbserver	No default value	See the description on page 69 .
username	No default value	See the description on page 70 .
password	No default value	Set manually only if you are not using an encrypted password to access the Configuration Database. For more details, see the description on page 70 .

Configuration Server Section

This section contains the configuration options of Configuration Server. The name of the section depends on the name of the Configuration Server Application object. On the first Configuration Server (named `confserv`), this section is named `confserv`. On other Configuration Servers being installed, this section has the same name as the Configuration Server object.

allow-empty-password

Default Value: `true`

Valid Values: `true`, `false`

Changes Take Effect: Immediately

Specifies whether Configuration Server allows an empty (blank) password in a client connection request. If the option is set to `false` and the password in a request is not specified, Configuration Server rejects the request and generates a corresponding error message.

Note: The Tenant option `password-min-length` (see [page 136](#)) overrides the value of `allow-empty-password` for all users in the Tenant in which the latter option is configured.

Genesys strongly recommends that you use `password-min-length` instead of `allow-empty-password`. The latter has been provided only for purposes of backward compatibility.

Refer to the “User Passwords” chapter of the *Genesys Security Deployment Guide* for more information about this option and how to use it.

allow-external-empty-password

Default Value: `true`

Valid Values: `true`, `false`

Changes Take Effect: Immediately

This option is used only if external authentication is being used.

Specifies whether Configuration Server allows an empty (blank) password in a client connection request when these requests are authenticated externally. When set to `true` (default), Configuration Server will permit an unspecified password in an externally authenticated request.

Note: There might be instances where an LDAP server, instead of rejecting a blank password, might (depending on the LDAP Server configuration) interpret this to mean that it should make an unauthenticated connection, giving the false impression that authentication has succeeded. To allow empty passwords in Configuration Server and still avoid this, set the `allow-empty-external-password` option to `false` so that configuration will enforce at least one character in a password sent to an external system.

If the option is set to `false` and the password in a request is not specified, Configuration Server rejects the request and generates a corresponding error message, regardless of the value of the two other options.

Refer to the “User Passwords” chapter of the *Genesys Security Deployment Guide* for more information about this option and how to use it.

allow-mixed-encoding

Default Value: `false`

Valid Values: `true`, `false`

Changes Take Effect: After restart

Specifies if Configuration Server checks if the encoding of user interface client applications at client registration matches the current encoding of Configuration Server. If set to `false` (the default), only those interface clients with the same encoding mode can connect to Configuration Server. If set to `true`, Configuration Server will not check, and the interface client can connect to Configuration Server regardless of its encoding mode.

Warning! Be very careful if you are setting this option to `true`. If a client sends any string data that is encoded differently than the encoding used by Configuration Server, the behavior of Configuration Server will be undefined.

client-connect-timeout

Default Value: `40`

Valid Values: Any positive integer from 1 to 65536

Changes Take Effect: After restart

Specifies the client connection timeout. The client should be authenticated before this timeout expires.

client-response-timeout

Default Value: `600`

Valid Values: Positive integer up to 86400 (24 hours)

Changes Take Effect: Immediately

Limits the time, in seconds, during which Configuration Server retains prepared unsent data in its memory. If this timeout expires and the data is still unsent, Configuration Server disconnects the client and discards all the data related to it.

dbthread

Default Value: `true`

Valid Values: `true`, `false`

`true` Uses internal database thread. This is the preferred method.

`false` Uses separate DB Server, as in releases prior to 8.5.

Changes Take Effect: After restart

Specifies how Configuration Server accesses the Configuration Database.

If set to `true`, Configuration Server attempts to launch a database client process locally using the options specified in the Configuration Database section, but not the host and port options. This is the preferred method of accessing a database.

If set to `false`, Configuration Server attempts to use a remote DB Server, as specified in the Configuration Database section, including the `host` and `port` options. This was the only way to access a database in releases prior to 8.5. Genesys recommends that you use this method only with older Genesys applications.

decryption-key

Default Value: No default value

Valid Values: Valid path to decryption file

Changes Take Effect: After restart

Specifies the path to an external `.pem` file containing the RSA key used for decrypting the password to the Configuration Database. The presence of this option, plus `encryption` set to `true`, indicates that the password was encoded using an asymmetric algorithm, with an encryption key from an external file.

Configuration Server creates or updates the value of this option if the `-keys` parameter is specified in the command-line at startup.

Warning! This option is set automatically by Configuration Server. Do not change the value of this option manually, except in the following circumstance.

If you want to switch back to using an unencrypted Configuration password, set the value of this option to empty (no value) and set the `encryption` option to `false`, then manually enter the unencrypted password into the Configuration Server configuration file. **Note:** You must have Write access to the Configuration Server configuration file to do this.

If you then want to revert back to using symmetric encryption, set the value of this option to empty (no value), and restart Configuration Server from the command line using the `-p <name of Configuration Database section> <password>` parameter.

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, add this option to both the primary and backup Configuration Servers, in the sections with the same name as the corresponding `Application` objects. If this option is set to `true`, Configuration Server does not calculate Virtual Agent Groups for existing and newly-created objects.

Note: You must set this option to the same value for both the primary and backup Configuration Servers. Then stop and restart both Configuration Servers. You must do this each time you change this option to retain the contents of the Virtual Agent Group.

enable-pre-812-security

Default Value: `false`

Valid Values: `false`, `true`

Changes Take Effect: Immediately

If set to `true`, this option restores pre-8.1.2 security behavior as follows:

- Enables a user, who does not have Change permission on a folder, to move objects from that folder to another location.
- Enables a user, who does not have Change Permissions permission on an object, to change the object's permissions implicitly by moving the object with inherited permissions between folders with different permission.

If set to `false` (the default), both actions are disabled.

Note: To take effect, this option must be set to `true` in both the `confserv` section of the primary master Configuration Server, and in the corresponding main section of the backup master Configuration Server.

Warning! Use this option only in exceptional cases, and only as a temporary measure.

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: After restart

Sets the UCS (Universal Character Set) transformation format (such as `UTF-8`, `UTF-16`, `Shift_JIS`, and so on) 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).

Note: In single-language format on UNIX platforms, the value of this option must match the value defined by the `LANG` environment variable (or derived from the values of the `LC_ALL` and `LC_CTYPE` environment variables as specified in the vendor documentation). On the Solaris platform, you might be required to set the environment variable `GCTI_TRANSLLOCALCP` to the value that represents the current local system encoding name (returned by the `iconv -l` command). You must set this Genesys-specific variable only if, in your environment, the value returned by the command does not match the codepage name specified in system locale settings (`LANG`, `LC_ALL`, or `LC_CTYPE`) on Solaris.

encryption

Default Value: `false`

Valid Values: `true`, `false`

Changes Take Effect: After restart

When set to `true`, the values of the `password` options in all Configuration Database sections are interpreted as being encrypted. Configuration Server decrypts the value when reading its configuration file at startup, accesses the Configuration Database using the decrypted value, and prints an encrypted string of characters as the password value into the log.

This option is set to `true` automatically by Configuration Server when the `-p` parameter is specified in the startup command line.

Warning! This option is set automatically by Configuration Server. Do not change the value of this option manually, except in the following circumstance.

If you want to switch back to using an unencrypted Configuration password, set the value of this option to `false` and set the `decryption-key` option to empty (no value), then manually enter the unencrypted password into the Configuration Server configuration file. **Note:** You must have Write access to the Configuration Server configuration file to do this.

fix_cs_version_7x

Default Value: `true`

Valid Values: `true`, `false`

Changes Take Effect: After restart

Use this option when using a master Configuration Server running release 8.0.3 (or later) with a Configuration Server Proxy running release 8.1.1 (or earlier). Setting this option to `true` enables the master Configuration Server to treat Configuration Server Proxy as running an equivalent schema. This prevents Configuration Server Proxy from using an incorrect schema and reading configuration data incorrectly.

Warning! If you are trying to run a Configuration Server Proxy release 8.1.1 (or earlier) with a Master Configuration Server 8.x, make sure that this option is set to `true` before setting up the connection between the two servers. Otherwise, the configuration schema of Configuration Server Proxy will be incorrect, and you will have to reinstall Configuration Server Proxy.

However, note that Genesys strongly recommends that Configuration Server and Configuration Server proxy be running the same version of software. The only exception is during migration, in which case the servers can run different version but only until migration is complete.

force-md5

Default Value: `false`

Valid Values: `false`, `true`

Changes Take Effect: After next login

Specifies whether Configuration Server uses the MD5 hashing algorithm to hash user passwords. MD5 was the default algorithm prior to Management Framework 8.1.2, when it was replaced by the SHA256 algorithm. If set to `false` (the default), all new and changed passwords will be hashed using SHA256. If set to `true`, all new and existing passwords will be hashed using MD5.

Use this option if you are running Configuration Server Proxy 8.1.0 (or earlier) that supports MD5, and a master Configuration Server 8.1.1 (or later) that supports SHA256. In this case, the two servers can be running together long enough to encounter password requests. Because they use two different hashing algorithms, the master Configuration Server will be unable to process the requests. You must force Configuration Server to use MD5 by setting the `force-md5` option to `true` in the `confserv` section of the master Configuration Server.

Note: Genesys does not recommend that you run a newer version of Configuration Server with an earlier version of Configuration Server Proxy. However, this situation is allowed for a short time during migration.

For more information about the security of user passwords using this hashing algorithm, refer to the “User Passwords” chapter in the *Genesys Security Deployment Guide*.

langid

Default Value: 1033 (English); refer to the corresponding Language Pack documentation to see if you need to change the default value.

Valid Values: Valid integer from list of LCID to language mappings

Changes Take Effect: After restart

Specifies the language used by Configuration Server operating in single-language mode. If Configuration Server Proxies are configured, the value of this option determines the language used by each Configuration Server Proxy.

This option is not used by Configuration Server in multi-language mode, in which the default language is English.

last-login

Default Value: `false`

Valid Values: `true`, `false`

Changes Take Effect: Immediately

Specifies whether the Last Logged In Display feature is to be used. If set to `true`, the feature is used for this Configuration Server. Last Logged In information is sent to its clients, and is stored and displayed by Genesys graphical user interfaces that support this feature.

If set to `false` (the default), this feature is not used for this Configuration Server.

For more information about the Last Logged In Display feature and this option, see the “Last Logged In Display” chapter in the *Genesys Security Deployment Guide*.

last-login-synchronization

Default Value: `false`

Valid Values: `true`, `false`

Changes Take Effect: Immediately

Specifies whether Last Logged In information is synchronized between this Configuration Server or Configuration Server Proxy and others in the environment. If set to `true`, this Configuration Server or Configuration Server Proxy sends notifications about changes in Last Logged In information to others in the configuration.

If set to `false` (the default), Last Logged In information is not synchronized between this Configuration Server or Configuration Server Proxy and others in the configuration.

This option is ignored if the `last-login` option is set to `false`.

For more information about the Last Logged In Display feature and this option, see the “Last Logged In Display” chapter in the *Genesys Security Deployment Guide*.

locale

Default Value: No default value

Valid Values: Any valid locale name or abbreviation

Changes Take Effect: After restart

Specifies the locale setting that Configuration Server uses for date/time/currency format (where applicable). It also affects encoding that is selected by Configuration Server in single-language mode 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.

Genesys recommends that you rely on operating system settings for locale selection, instead of this Genesys option. If you do have to set it up here, 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 on. For UNIX, consult the vendor documentation for your operating system.

The specified locale value must be supported by your operating system, and must match the value that is defined by the `LANG` environment variable (or derived from the values of the `LC_ALL` and `LC_CTYPE` environment variables, as specified in the vendor documentation). When this option is set, its value must also be aligned with the [encoding](#) option; that is, the locale in use must activate the same encoding as specified by that option.

Note: On the Solaris platform, you might be required to set the environment variable `GCTI_TRANSLLOCALCP` to the value that represents the current local system encoding name (returned by the `iconv -li` command). You must set this Genesys-specific variable only if, in your environment, the value returned by the command does not match the codepage name specified in system locale settings (`LANG`, `LC_ALL`, or `LC_CTYPE`) on Solaris.

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 `port` option.

max-client-output-queue-size

Default Value: 1024

Valid Values:

0 No limit

Any positive integer Threshold value (in KB)

Changes Take Effect: Immediately

Specifies the threshold on the amount of memory (in KB), used by prepared unsent data for a single client, at which Configuration Server defers processing requests from that client.

When the amount of unsent data drops below that threshold, Configuration Server restarts processing incoming requests from the client in the order that they were originally received.

max-output-queue-size

Default Value: 0

Valid Values:

0 No limit

Any positive integer Threshold value (in MB)

Changes Take Effect: Immediately

Specifies the threshold on the total amount of memory (in MB), used by prepared unsent data, at which Configuration Server defers processing of all incoming requests. While processing of the incoming requests is deferred, Configuration Server continues to receive and store incoming requests for further processing.

When the amount of unsent data drops below that threshold, Configuration Server restarts processing incoming requests.

Note: Use this option with extreme care. Reaching the threshold specified by this option effectively halts Configuration Server until the size of outgoing buffers drops below the specified value. This option is intended to be a last resort defense against unexpected termination due to memory starvation.

multi-languages

Default Value: false

Valid Values: false, true

Changes Take Effect: At first start of Configuration Server; subsequent changes not permitted

Specifies if Configuration Server supports UTF-8 encoding internally.

Warning! You can only set this option to true if you are using a multi-language version of the Configuration Database initialization scripts.

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.

packet-size

Default Value: 1024000

Valid Values: 1–2147483648

Changes Take Effect: After restart

Specifies, in bytes, the target maximum size of the packet in a single message.

Warning! Do not change this option unless instructed by Customer Care.

password-change

Default Value: `true`

Valid Values: `true`, `false`

Changes Take Effect: After restart

Specifies whether Configuration Server allows users to change his or her own password, if the user does not have Change permission for his or her own object. If set to `false`, the user can change his or her own password only if he or she has Change permissions on his or her own object. If this option is set to `true` (default), Configuration Server allows the user to change the password regardless of the Change permission.

Note: This option does not apply if the System Administrator has configured the Force Password at Next Login feature.

For more information about this option and how to use it in your password system, refer to the “User Passwords” chapter in the *Genesys Security Deployment Guide*.

peer-switchover-tmout

Default Value: 30

Valid Values: 10—600

Changes Take Effect: After restart

Specifies the time interval (in seconds) that a Configuration Server, when switching to primary, waits for the other Configuration Server in the HA pair to close its side of the connection between the two servers. The servers cannot switch over if one server has the connection open. If the specified time expires before the connection is closed, the switchover request is ignored and the server mode does not change.

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.

primary-startup-tmout

Default Value: 30

Valid Values: 1—MAXINT

Changes Take Effect: After restart

Specifies the time interval (in seconds) that the backup Configuration Server, waits for the backup Configuration Server to finish starting up and run as primary before continuing its own startup.

When two Configuration Servers in an HA pair start at the same time and detect each other's presence before either has completed its initialization, this option effectively determines which server starts as primary and which starts as backup. In this case, the server configured as primary continues its startup and initialization to completion to run as the primary Configuration Server. The server configured as backup, delays its initialization and waits for the primary server to start up and open its ports. After the time specified by this option, the backup Configuration Server attempts to connect to the now-running primary Configuration Server, and if successful, continues its start-up as backup.

Notes:

- Genesys strongly recommends that, to avoid concurrency during startup, you start one Configuration Server at a time.
- Do not use this option unless instructed to do so by Genesys Customer Care.

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 68](#). You must specify a value for this option.

upgrade-mode

Default Value: 0

Valid Values: 0, 1

Changes Take Effect: After restart

Used during migration to specify if peer Configuration Servers are able to start up side-by-side without contacting each other. If set to 1, this independent side-by-side startup is permitted. If set to 0 (zero, the default), the startup of one Configuration Server is communicated to the other. For more information about the requirement for migration with minimum downtime, refer to the *Genesys Migration Guide*.

Configuring ADDP Between Primary and Backup Configuration Servers

Use the options in this section to configure Advanced Disconnect Detection Protocol (ADDP) between primary and backup Configuration Servers.

Configure the options in the following sections:

- In the primary Configuration Server, set them in the `confserv` section.
- In the backup Configuration Server, set them in the section that has the same name as the backup Configuration Server Application name.

Note: If one or both Configuration Servers have not been started up for the first time, set the options in the configuration file of the appropriate servers.

protocol

Default Value: No default value

Valid Values: `addp`

Changes Take Effect: After restart

Specifies if ADDP is to be used between the primary and backup Configuration Servers. If set to `addp`, the ADDP protocol is implemented as defined by the configuration options `addp-timeout`, `addp-remote-timeout`, and `addp-trace` in the same configuration server section (`confserv`, or its equivalent in the backup Configuration Server) of the configuration file. If this option is set to any other value, or if it is not specified at all, ADDP is not used and the ADDP-related configuration options in this section are ignored.

addp-remote-timeout

Default Value: 0

Valid Values: 0–3600

Changes Take Effect: After restart

Specifies the time interval, in seconds, that Configuration Server in backup mode instructs the other Configuration Server in the redundant pair to use when polling to check the connection between the two servers. If set to zero

(0), Configuration Server in backup mode does not send any such instruction. This option applies only if the value of the `protocol` option is `addp`.

Note: Because any Configuration Server can be in primary or backup mode, regardless of how it is configured, you must set this option to the same value in both the primary and backup Configuration Servers.

addp-timeout

Default Value: 0

Valid Values: 0–3600

Changes Take Effect: After restart

Specifies the time interval, in seconds, that Configuration Server in backup mode waits before polling the other Configuration Server in the redundant pair. If set to zero (0), Configuration Server in backup mode does not poll the other Configuration Server in the redundant pair. This option applies only if the value of the `protocol` option is `addp`.

Note: Because any Configuration Server can be in primary or backup mode, regardless of how it is configured, you must set this option to the same value in both the primary and backup Configuration Servers.

addp-trace

Default Value: off

Valid Values:

`false`, `no`, `off` Turns ADDP off.

`true`, `yes`, `on`, `local` ADDP trace occurs on the side of the Configuration Server in backup mode.

`remote` ADDP trace occurs on the side of the Configuration Server in primary mode.

`both`, `full` ADDP trace occurs at both the primary and backup Configuration Servers.

Changes Take Effect: After restart

Determines whether ADDP messages are written to the primary and backup Configuration Servers log files. This option applies only if the value of the `protocol` option is `addp`.

Configuration Database Section

The Configuration Database section name is specified by the value of the `server` option on [page 66](#). This section contains information about the Configuration Database. The options in this section can only be edited in the Configuration Server configuration file, not via an `Application` object's options.

dbengine

Default Value: No default value

Valid Values: `oracle`, `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 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, as follows:

- For Oracle, the value is the name of the Listener service.
- 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).

dml-retry

Default Value: 1

Valid Values: Integer values in the range of 0 to 32766

Changes Take Effect: After restart of Configuration Server

Specifies the number of retries for issuing a DML statement or transaction to DB Server after receiving TAF range error from Oracle DBMS. When the number of retries has been attempted with no success, Configuration Server considers the database operation to have failed and reports the error to the database client. A value of zero (0) specifies that no retry is to be attempted, in which the error is reported to the client immediately, without any retries.

Note: The node failover procedure can be time- and resource-consuming, so take care to set this option to a reasonable value to avoid overloadingdbserver.

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 if you are not encrypting the password. If you are encrypting the password, Configuration Server sets this option to the encrypted password in its configuration file.

Note: The password option is visible only in the configuration file. It is not visible in Genesys Administrator.

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 the DBMS. If this timeout expires, Configuration Server generates log event 21-24402. Refer to *Framework Combined Log Events Help* for a full description of this log event.

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.

Runtime Options in Configuration Database

The options in this section are set in the Options of the Configuration Server Application object using Genesys Administrator.

Configuration Server section

Note: In addition to the configuration options listed here, this section contains the `license` option. You cannot read or modify this option. It is intended for use by only License Resource Manager (LRM). Configuration Server sets this option itself.

force-offline

Default Value: `false`

Valid Values: `true`, `false`

Changes Take Effect: Immediately

When set to `true`, immediately stops database connections if the DBMS is not responding or database clients have stopped responding. When set back to `false` (the default), the connections are restored.

Use this option to restart database connections if the DBMS is not responding or database clients have stopped responding. This option takes effect only if `dbthread=true`. You can change this option only when editing the properties of the Configuration Server instance that is currently running in Primary mode.

system Section

This section must be called `system`.

force-reconnect-reload

Default Value: `false`

Valid Values: `true`, `false`

Changes Take Effect: After next reconnection to database

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.

postgre-standard-conforming-strings

Default Value: `false`

Valid Values: `false`, `off`, `no`

Changes Take Effect: Immediately

This option applies only when Configuration Server is connected to a PostgreSQL database. The value of this option must match the value of the PostgreSQL `standard_conforming_strings` option.

PostgreSQL must be configured with the `standard_conforming_strings` option set to `false`, meaning that the Configuration Server option `postgres-standard-conforming-strings` must also be set to `false`.

Notes:

- Starting in PostgreSQL 9.1, the `standard_conforming_strings` option defaults to `true`. To use the Configuration Database, you must set this option to `false`.
- Previously documented valid values `true`, `on`, and `yes` are currently not supported, and are known to cause problems with persistent binary data.

prevent-mediatype-attr-removal

Default Value: `false`

Valid Values: `true`, `false`

Changes Take Effect: Immediately

Specifies whether to remove MediaType business attributes and some values that may directly impact legacy solutions that depend on fixed DBIDs for these predefined objects in the Environment tenant.

skip-environment-enum-transfer

Default Value: `false`

Valid Values: `true`, `false`

Changes Take Effect: Immediately

Specifies whether business attributes are created automatically when creating a new tenant. By default, all business attributes that are available in the Environment tenant are duplicated (except their options) in the new tenant.

log Section

Configuration Server supports the common log options described in “log Section” on [page 14](#).

Note: Any options set in this section of the configuration file are read only at initial startup. After that, Configuration Server reads values from its `Application` object. Likewise, you can change the value of any log option in runtime using Genesys Administrator.

Debug Log Options

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

x-dblib-debug

Default Value: `0`

Valid Values:

- | | |
|-----|---|
| 0 | Log records are not generated. |
| 1–5 | Log records are generated. The higher the value, the more log records are generated |

Changes Take Effect: Immediately

Generates Debug log records about DB Client operations of the application.

-
- Notes:**
- This option takes effect only if the following two conditions are met:
 - The verbose option is set to debug or all.
 - The dbthread option is set to true.
 - Use this option only when requested by Genesys Customer Care.
-

x-dblib-sql

Default Value: 0

Valid Values:

- | | |
|-----|--------------------------------|
| 0 | Log records are not generated. |
| 1–5 | Log records are generated. |

Changes Take Effect: After restart

Generates Debug log records with additional output from the thread used for access to the Configuration Database.

-
- Notes:**
- This option takes effect only if the following two conditions are met:
 - The verbose option is set to debug or all.
 - The dbthread option is set to true.
 - Use this option only when requested by Genesys Customer Care.
-

security Section

This section contains configuration options that relate to security features. This section must be called `security`, and is configured in the options of the Configuration Server Application object.

no-default-access

Default Value: 0

Valid Values: One of the following:

- | | |
|---|------------------------------|
| 0 | No default access privileges |
| 1 | Default access privileges |

Changes Take Effect: Immediately

Specifies whether new users created under this application have default privileges assigned to them. If this option is not present, the default value is assumed.

With redundant Configuration Servers, this option must be configured identically on both the primary and backup servers.

Refer to the chapter “No Default Access for New Users” in the *Genesys 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 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.

Note: If the Configuration Server configuration file contains legacy options `history-log-xxx` specified in its `confserv` section, they will be converted and copied into the this `history-log` section when Configuration Server first starts up. After that, they will be ignored in favor of the new options in this section.

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 on the history log regardless of the previous setting of this option, and sets this option to `true`.

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 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.

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.

write-former-value

Default Value: `true`

Valid Values: `true`, `false`

Changes Take Effect: Immediately

Specifies if old history values are stored for purposes of the configuration audit trail. If set to `false`, audit trail feature will be disabled.

-
- Notes:**
- Genesys recommends that you temporarily switch off this option if you are doing batch updates, such as tenant removal or switch removal, and are concerned about performance.
 - Make sure you always back up your database before doing large updates.
-

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.

Application Parameter Options

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

Configuration Server Application object > Configuration tab > Server Info section > Listening Ports > Port Info

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 Customer Care.

user

Default Value: No default value

Valid Values: 1 or not set

Changes Take Effect: Immediately

When set to 1, the port refuses all connection requests from applications that do not require user-level authentication. When not set, or set to any other value, the option is ignored.

Transport Parameter Options

Set options in this section in the Transport Parameters of the port's properties, using the following navigation path:

Configuration Server Application object > Configuration tab > General section > Connections > Connection Info > Advanced tab > Transport Parameters

Transport 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.

transport Option In a configuration file (see the example on [page 77](#)), these options appear in the following format:

```
transport = <option name>=<value>; <option name>=<value>; ...
```

Collectively, the options make up the parameters of the transport option. When entering the options in Genesys Administrator, only the options are required; transport = is prefixed automatically to the list of option/value pairs.

Note: Valid values for these options must have no spaces before or after the delimiter characters “;” (semi-colon) and “=”.

tls

Default Value: tls=0

Valid Values:

tls=0

Regular (unsecured) connections will be used.

For Windows:

Secure connections will be used, where
certificate = certificate value.

tls=1; certificate=<value>

For UNIX:

```
tls=1; certificate=<path>;
[certificate-key=<path>];
trusted-ca=<path>
```

Secure connections will be used, where:

- `certificate`—full path to the `<serial_#>_<host_name>_cert.pem` file
- `certificate-key`—full path to the `<serial_#>_<host_name>_priv_key.pem` file (unless the private key is stored together with a certificate)
- `trusted-ca`—full path to the `ca_cert.pem` file

This option is used to enable the set up of secure connections between Genesys components. Refer to the chapter “Configuring Secure Configuration Server and DB Server Connections” in the *Genesys Security Deployment Guide* for information about how to use this option.

Sample Configuration Server 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

[dbserver]
dbengine = mssql
dbserver = db-config
dbname = config
username = user1
password = user1pass
transport = tls=1;certificate=9a ab db c4 02 29 3a 73 35 90 b0 65 2f
```

Changes from 8.1 to 8.5

[Table 10](#) lists all changes to Configuration Server options between release 8.1 and the latest 8.5 release.

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

Table 10: Configuration Server Configuration Option Changes from 8.1 to 8.5

Option Name	Option Values	Type of Change	Details
Configuration Server Section			
allow-empty-password	true, false	Modified	See description on page 56 . Corrected Changes Take Effect.
allow-external-empty-password	true, false	Modified	See description on page 56 . Corrected Changes Take Effect.
allow-mixed-encoding	true, false	Modified Changes Take Effect	See description on page 57 .
client-connect-timeout	true, false	New	See description on page 57 . Not previously documented.
client-response-timeout	Positive integer up to 86400	Modified Valid Values and Changes Take Effect	See description on page 57 . Previous Valid Values: Any positive integer Previous Changes Take Effect: After restart
dbthread	true, false	New	See description on page 57 .
decryption-key	Valid path name	New	See description on page 58 .
encryption	true, false	Modified	See description on page 60 . Now set automatically by Configuration Server.
force-offline	true, false	New	See description on page 71 .

Table 10: Configuration Server Configuration Option Changes from 8.1 to 8.5 (Continued)

Option Name	Option Values	Type of Change	Details
force-reconnect-reload	true, false	Moved	See description on page 71 . Moved to system section; documented incorrectly in previous release.
langid	Valid integer from list of LCID to language mappings	New	See description on page 62 .
license	Binary value	New	Inserted/removed automatically and is read-only.
max-client-output-queue-size	1024	New	See description on page 63 .
max-output-queue-size	0	New	See description on page 64 .
packet-size	1–2147483648	Modified	See description on page 65 . Default value documented incorrectly in previous release. Added warning to description.
peer-switchover-tmout	10–600	New	See description on page 65 .
primary-startup-tmout	1–MAXINT	New	See description on page 66 .
upgrade-mode	0, 1	New	See description on page 67 .
Configuration Database Section			
addp	on, off	Removed	
addp-timeout	1–3600	Removed	
addp-trace	on, off	Removed	
dbengine	oracle, mssql, db2, postgre	Modified valid values	Removed sybase and informix. See description on page 69 .
dml-retry	0–32766	Moved	See description on page 69 Moved from Common Configuration Options chapter; documented incorrectly in previous release.

Table 10: Configuration Server Configuration Option Changes from 8.1 to 8.5 (Continued)

Option Name	Option Values	Type of Change	Details
history-log-guid	Binary value	Removed	
history-log-minid	Binary value	Removed	
history-log-version	Binary value	Removed	
host	Any valid host name	Removed	Used only if dbthread=false, in which case they are working with an older environment; refer to Framework 8.1 documentation for descriptions.
port	Any valid TCP/IP port.	Removed	
reconnect-timeout	0 or any positive integer	Removed	
server	No default value	Removed	
hca Section (removed)			
schema	none, snapshot, journal	Removed	
log Section			
x-dblib-debug	0–5	New	See description on page 72 . Use this option only when requested by Genesys Customer Care.
x-dblib-sql	0–5	New	See description on page 73 . Use this option only when requested by Genesys Customer Care.
soap Section (removed)			
client-lifespan	1–65535	Removed	
debug	true, false	Removed	
port	0 or any valid TCP/IP port	Removed	Used only if dbthread=false. Refer to Framework 8.1 documentation for information about using this option.

Table 10: Configuration Server Configuration Option Changes from 8.1 to 8.5 (Continued)

Option Name	Option Values	Type of Change	Details
system Section (new)			
force-reconnect-reload	true, false	Moved	See description on page 71 . Moved from Configuration Server section; documented incorrectly in previous release.
postgre-standard-conforming-strings	false, off, no	New	See description on page 71 .
prevent-mediatype-attr-removal	true, false	New	See description on page 72 .
skip-environment-enum-transfer	true, false	New	See description on page 72 .
history-log Section			
write-former-value	true, false	New	See description on page 75 .
Application Parameters			
user	1 or not set	New	See description on page 76 .

4

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:

- [Setting Configuration Options, page 83](#)
- [Mandatory Options, page 84](#)
- [license Section, page 84](#)
- [csproxy Section, page 84](#)
- [history-log Section, page 88](#)
- [Application Parameter Options, page 89](#)
- [Changes from 8.1 to 8.5, page 90](#)

Configuration Server Proxy also supports the common options described in Chapter 1 on [page 13](#).

Setting Configuration Options

Unless specified otherwise, set Configuration Server Proxy configuration options in the options of the Configuration Server Proxy Application object, using the following navigation path:

- Configuration Server Proxy Application object > Options tab > Advanced View (Options)

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

Mandatory Options

Table 11 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 11: 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 <i>the Genesys Licensing Guide</i> .

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

allow-mixed-encoding

Default Value: `false`

Valid Values: `true`, `false`

Changes Take Effect: When the next client connects

Specifies if Configuration Server Proxy checks if the encoding of user interface client applications at client registration matches the current encoding of Configuration Server Proxy. If set to `false` (the default), only those interface clients with the same encoding mode can connect to Configuration Server Proxy. If set to `true`, Configuration Server Proxy will not check, and the

interface client can connect to Configuration Server Proxy regardless of its encoding mode.

Warning! Be very careful if you are setting this option to `true`. If a client sends any string data that is encoded differently than the encoding used by Configuration Server Proxy, Configuration Server Proxy will terminate immediately.

client-response-timeout

Default Value: `600`

Valid Values: Positive integer up to `86400` (24 hours)

Changes Take Effect: Immediately

Limits the time, in seconds, during which Configuration Server Proxy retains prepared unsent data in its memory. If this timeout expires and the data is still unsent, Configuration Server Proxy disconnects the client and discards all the data related to it.

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: After restart

Sets the UCS (Universal Character Set) transformation format (such as `UTF-8`, `UTF-16`, `Shift_JIS`, and so on) that Configuration Server Proxy 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 Proxy uses the default value.

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

last-login

Default Value: `false`

Valid Values: `true`, `false`

Changes Take Effect: Immediately

Specifies whether the Last Logged In Display feature is to be used. If set to `true`, the feature is used for this Configuration Server Proxy. Last Logged In information is sent to clients of the Application, and is stored and displayed by Genesys graphical user interfaces that support this feature.

If set to `false` (the default), this feature is not used for this Configuration Server Proxy.

For more information about the Last Logged In Display feature and this option, see the “Last Logged In Display” topic in the *Genesys Security Deployment Guide*.

last-login-synchronization

Default Value: `false`

Valid Values: `true`, `false`

Changes Take Effect: Immediately

Specifies whether Last Logged In information is synchronized between this Configuration Server Proxy and others in the environment. If set to `true`, this Configuration Server Proxy sends notifications about changes in Last Logged In information to others in the configuration.

If set to `false` (the default), Last Logged In information is not synchronized between this Configuration Server Proxy and others in the configuration.

This option is ignored if the `last-login` option is set to `false`.

For more information about the Last Logged In Display feature and this option, see the “Last Logged In Display” chapter in the *Genesys Security Deployment Guide*.

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 on.

The specified locale value must be supported by your operating system, and must match the value that is defined by the `LANG` environment variable (or derived from the values of the `LC_ALL` and `LC_CTYPE` environment variables, as specified in the vendor documentation).

max-client-output-queue-size

Default Value: 1024

Valid Values:

0 No limit

Any positive integer Threshold value (in KB)

Changes Take Effect: Immediately

Specifies the threshold on the amount of memory (in KB), used by prepared unsent data for a single client, at which Configuration Server Proxy defers processing requests from that client.

When the amount of unsent data drops below that threshold, Configuration Server Proxy restarts processing incoming requests from the client in the order that they were originally received.

max-output-queue-size

Default Value: 0

Valid Values:

0 No limit

Any positive integer Threshold value (in MB)

Changes Take Effect: Immediately

Specifies the threshold on the total amount of memory (in MB), used by prepared unsent data, at which Configuration Server Proxy defers processing of all incoming requests. While processing of the incoming requests is deferred, Configuration Server Proxy continues to receive and store incoming requests for further processing.

When the amount of unsent data drops below that threshold, Configuration Server Proxy restarts processing incoming requests.

Note: Use this option with extreme care. Reaching the threshold specified by this option effectively halts Configuration Server Proxy until the size of outgoing buffers drops below the specified value. This option is intended to be a last resort defense against unexpected termination due to memory starvation.

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.

packet-size

Default Value: 1024000

Valid Values: 1–2147483648

Changes Take Effect: Immediately

Specifies, in bytes, the target maximum size of the packet in a single message.

Warning! Do not change this option unless instructed by Customer Care.

proxy-cluster-name

Default Value: No default value

Valid Values: Name of Configuration Server objects

Changes Take Effect: When next client connects

Specifies the name of a Configuration Server object that represents a load balancer network interface to Configuration Server Proxy clients.

The object represented by this name must exist in the Configuration Database, be of type Configuration Server, have a port configured to match the listening port of the load balancer, and be associated with a host with the address of the load balancer network interface to which clients must connect.

The object must not be associated with any real Genesys Configuration Server process in the system. All clients that are configured to use load-balanced Configuration Server Proxies must be configured to use this application object instead of actual Configuration Server Proxies when configuring their ADDP and other connections parameters.

This option takes effect only in a load-based Configuration Server Proxies configuration.

proxy-writable

Default Value: `false`

Valid Values:

<code>true</code>	Configuration Server Proxy accepts requests from clients for updates to user-defined data, and forwards these requests to the Master Configuration Server.
<code>false</code>	Configuration Server Proxy does not accept requests from clients for updates to user-defined data. Clients must send the requests to the Master Configuration Server directly.

Changes Take Effect: Immediately

Specifies whether Configuration Server Proxy accepts requests from client 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.

Note: This mode is intended to be used with Genesys agent-facing applications only. You should still connect your administrative GUIs, and any other applications that write extensively to the configuration, to the Master Configuration Server directly.

history-log Section

This section must be called `history-log`.

client-expiration

Default Value: 1

Valid Values: 1—30

Changes Take Effect: Immediately

Specifies the time interval, in days, at which Configuration Server Proxy will check for expiration of records of both configuration updates and client sessions.

Application Parameter Options

Set the options in this section in the Application Parameters of the port's properties, using the following navigation path in Genesys Administrator:

- Configuration Server Proxy Application object > Configuration tab > Server Info section > Listening Ports > Port Info

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 Customer Care.

user

Default Value: No default value

Valid Values: 1 or not set

Changes Take Effect: Immediately

When set to 1, the port refuses all connection requests from applications that do not require user-level authentication. When not set, or set to any other value, the option is ignored.

Changes from 8.1 to 8.5

Table 12 on [page 90](#) lists all changes to Configuration Server Proxy options between release 8.1 and the latest 8.5 release.

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

Table 12: Configuration Server Proxy Configuration Option Changes from 8.1 to 8.5

Option Name	Option Values	Type of Change	Details
csproxy Section			
client-response-timeout	Positive integer up to 86400	Modified Valid Values and Changes Take Effect	See description on page 85 . Previous Valid Values: Any positive integer Previous Changes Take Effect: After restart
max-client-output-queue-size	1024	New	See description on page 86 .
max-output-queue-size	0	New	See description on page 87 .
packet-size	1–2147483648	Modified	See description on page 87 . Default value documented incorrectly in previous release. Added warning to description.
proxy-cluster-name		New	See description on page 88 .
history-log Section			
active	true, false	Removed	
all	:memory:, valid path and name	Removed	
expiration	1–30	Removed	
failsafe-store-processing	true, false	Removed	
max-records	1–1000	Removed	
soap Section (removed)			
client_lifespan	Any positive integer	Removed	

Table 12: Configuration Server Proxy Configuration Option Changes from 8.1 to 8.5

Option Name	Option Values	Type of Change	Details
debug	yes, no	Removed	
port	Any valid TCP/IP port	Removed	
Application Parameters			
user	1 or not set	New	See description on page 89 .

5

Local Control Agent Configuration Options

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

- [Setting Configuration Options, page 93](#)
- [Mandatory Options, page 93](#)
- [general Section, page 94](#)
- [log Section, page 94](#)
- [security Section, page 94](#)
- [LCA Configuration File, page 95](#)
- [Configuring ADDP Between LCA and Solution Control Server, page 96](#)
- [Changes from 8.1 to 8.5, page 96](#)

Setting Configuration Options

You change default LCA configuration options in the configuration file `lca.cfg`. See “LCA Configuration File” on [page 95](#) 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.

general Section

This section must be called `general`.

lookup_clienthost

Default Value: `false`

Valid Values: `false`, `true`, `on`, `off`, `yes`, `no`

Changes Take Effect: After restart

Specifies whether to look up the host name of the connected client. If set to `false`, the default, LCA does not look up the host name and uses the IP address of the connected client in audit logs. If set to `true`, LCA looks up the host name and uses it in audit logs.

wmiquery-timeout

Default Value: No default value (infinite time interval)

Valid Values: `-1`, `0`, or any positive integer

Changes Take Effect: After restart

Specifies, in milliseconds, the length of time for which LCA will wait for a response to its WMI query for performance results. If not set, or set to `-1` or `0`, there is no timeout; LCA will wait for an infinity. Otherwise, it will wait for the specified time, and then return to processing requests from Solution Control Server.

This option applies only on the Windows platform.

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 13](#).

security Section

This section must be called `security`.

This section contains information required for LCA to support TLS on connections with its clients. Refer to the “TLS Configuration” section in the *Genesys Security Deployment Guide* for complete information about configuring TLS. Refer also to the related option `lca-upgrade` on [page 127](#).

upgrade

Default Value: `0` (false)

Valid Values: 0 (false), 1 (true); corresponding to the numerical equivalent of the `lca-upgrade` option

Note: Valid values for this option must have no spaces before or after the = delimiter character.

Changes Take Effect: After restart of LCA

Specifies whether TLS will be used to secure the connection between LCA and SCS. If set to 0 (false, the default), regular (unsecured) connections will be used. If set to 1 (true), this option must be followed by these parameters:

For Windows:

`certificate=<thumbprint>` Thumbprint of the security certificate.

For UNIX:

`certificate=<path>` Full path to the
`<serial_#>_<host_name>.cert.pem` file

`[certificate-key=<path>]` Full path to the
`<serial_#>_<host_name>.priv_key.pem` file
 (unless the private key is stored together with a
 certificate)

`trusted-ca=<path>` Full path to the `ca_cert.pem` file

This option is set in the LCA configuration file, `lca.cfg`.

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, modify the configuration file called `lca.cfg` and specify new values for appropriate options. The file is located in the same directory as the LCA executable file.

Note: You can give a custom name to the configuration file and specify it at startup using the `-c` command-line parameter. For example, `lca.exe -c lca_custom.cfg`, where `lca_custom.cfg` is the name of the 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 Deployment Guide*.

Sample Configuration File

Here is a sample configuration file for LCA:

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

Configuring ADDP Between LCA and Solution Control Server

Advanced Disconnection Detection Protocol (ADDP) is enabled automatically between LCA and Solution Control Server. To customize its settings, configure the `addp-timeout` and `addp-remote-timeout` options in the Host object, as described in Chapter 10 on [page 123](#).

Changes from 8.1 to 8.5

[Table 13](#) lists all changes to LCA options between release 8.1 and the latest 8.5 release.

Table 13: LCA Configuration Option Changes from 8.1 to 8.5

Option Name	Option Values	Type of Change	Details
general Section			
<code>wmiquery-timeout</code>	-1, 0, positive integer	Added	See description on page 94 .
security Section			
<code>upgrade</code>	0, valid certificate information	Added	See description on page 94 . Moved from Host options; documented incorrectly in previous version.

6

Genesys Deployment Agent Configuration Options

This chapter describes the configuration options for the Genesys Deployment Agent and includes the following sections:

- [Setting Configuration Options, page 97](#)
- [Mandatory Options, page 97](#)
- [log Section, page 98](#)
- [web Section, page 98](#)
- [security Section, page 98](#)
- [Genesys Deployment Agent Configuration File, page 99](#)
- [Changes from 8.1 to 8.5, page 100](#)

Setting Configuration Options

You can change default Genesys Deployment Agent configuration options in the configuration file `gda.cfg`. See “Genesys Deployment Agent Configuration File” on [page 99](#) 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 Genesys Deployment Agent.

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 13](#).

web Section

This section must be called `web`.

rootdir

Default: Path to LCA and Genesys Deployment Agent installation folder

Valid Values: Path to any valid folder

Change Takes Effect: After restart of Genesys Deployment Agent

Specifies the path to the folder that is used to store files uploaded during the Installation Package (IP) deployment.

security Section

This section contains the configuration options that are required to configure secure data exchange using TLS. For information about how to use these options, refer to the “Genesys TLS Configuration” chapter in the *Genesys Security Deployment Guide*.

This section must be called `security`.

transport

Default Value: 0 (false)

Valid Values: 0 (false), 1 (true); correspond to the numerical equivalent of the `gda-tls` option

Note: Valid values for this option must have no spaces before or after the delimiter character `=`.

Changes Take Effect: After restart of Genesys Deployment Agent

Specifies whether TLS will be used to secure the connection between Genesys Deployment Agent and its clients. If set to 0 (false, the default), regular (unsecured) connections will be used. If set to 1 (true), this option must be followed by these parameters:

For Windows:

`certificate=<thumbprint>` Thumbprint of the security certificate

For UNIX:

certificate=<path> Full path to the
 <serial_#>_<host_name>.cert.pem file

[certificate-key=<path>] Full path to the
 <serial_#>_<host_name>.priv_key.pem file
 (unless the private key is stored together with a
 certificate)

trusted-ca=<path> Full path to the ca_cert.pem file

This option is set in the Genesys Deployment Agent configuration file,
 gda.cfg.

Refer to the “TLS Configuration” section in the *Genesys Security Deployment Guide* for detailed instructions on how to configure TLS.

Genesys Deployment Agent Configuration File

Genesys Deployment Agent supports common log options which allows you to precisely configure log output for it. Because you do not configure an Application object for Genesys Deployment Agent, if you need to change the default log option settings, create a configuration file called gda.cfg (or rename and modify the gda.cfg.sample file that is located in the installation folder) and specify new values for appropriate options. The file must be located in the same directory as the Genesys Deployment Agent executable file.

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

The Genesys Deployment Agent configuration file must have the following format:

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

[web]
rootdir=<path>
```

Sample Configuration File

The following is a sample configuration file for Genesys Deployment Agent:

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

```
[web]  
rootdir=./gdaroot
```

Changes from 8.1 to 8.5

There are no changes to Genesys Deployment Agent options between release 8.1 and the latest 8.5 release.

7

Message Server Configuration Options

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

- [Setting Configuration Options, page 101](#)
- [Mandatory Options, page 101](#)
- [MessageServer Section, page 102](#)
- [messages Section, page 102](#)
- [db-filter Section, page 104](#)
- [log Section, page 105](#)
- [Changes from 8.1 to 8.5, page 105](#)

Setting Configuration Options

Unless specified otherwise, set Message Server configuration options in the options of the Message Server Application object, using the following navigation path:

- Message Server Application object > Options tab > Advanced View (Options)

Warning! Configuration section names, configuration option names, and predefined option values are case-sensitive. Type them in Genesys Administrator 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:

<code>log</code>	This Message Server is used for logging to the Centralized Log Database.
<code>general</code>	This Message Server is used for strategy monitoring from Interaction Routing Designer.
<code>scs_distributed</code>	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`.

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.

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.

dbthread

Default Value: true

Valid Values: true, false

true Uses internal database thread. This is the preferred method.

false Uses separate DB Server, as in releases prior to 8.5.

Changes Take Effect: After restart

Specifies how Message Server accesses the Log Database. If set to true, Message Server server attempts to launch a database client process locally that will access the Log Database using the Log DAP. This is the preferred method of accessing a database starting in 8.5.

If set to false, Message Server attempts to use a remote DB Server, as in previous releases. Genesys recommends that you use this method only with older Genesys applications.

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-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.

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.

db-filter Section

The DB Filter section controls delivery of specified log events from specified applications and application types. See “Sample Configuration” on [page 105](#).

This section must be called `db-filter`.

block-messages

Default Value: No default value

Valid Values: Comma-separated list of identifiers of any valid log events

Changes Take Effect: Immediately

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

block-messages-by-<type>

Default Value: No default value

Valid Values: Identifiers of any applications, 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 Management Layer User’s Guide*.

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.

Tip: The application DBID can be retrieved by using the `-getallappstatus` parameter of the `mlcmd` command-line utility. Refer to the *Framework 8.5 Management Layer User’s Guide* for the correct syntax of this command, and how to use it.

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
```

log Section

In addition to the option in this section, Message Server supports the common options described in Chapter 1 on [page 13](#).

The following option enables you to generate Debug logs containing information about specific operations of an application.

x-dblib-debug

Default Value: 0

Valid Values:

- | | |
|-----|---|
| 0 | Log records are not generated. |
| 1–5 | Log records are generated. The higher the value, the more log records are generated |

Changes Take Effect: Immediately

Generates Debug log records about DB Client operations of the application.

-
- Notes:**
- This option takes effect only if the following two conditions are met:
 - The `verbose` option is set to `debug` or `all`.
 - The `dbthread` option is set to `true`.
 - Use this option only when requested by Genesys Customer Care.
-

Changes from 8.1 to 8.5

Table 14 on [page 106](#) lists all changes to Message Server options between release 8.1 and the latest 8.5 release.

Table 14: Configuration Server Configuration Option Changes from 8.1 to 8.5

Option Name	Option Values	Type of Change	Details
messages Section			
dbthread	true, false	New	See description on page 103 .
thread-mode	ST	Removed	Incorrectly added in 8.0; option never functional.
thread-pool-size	Any positive integer	Removed	Incorrectly added in 8.0; option never functional.
log Section			
x-dblib-debug	0-5	New	See description on page 105 .

8

Solution Control Server Configuration Options

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

- [Setting Configuration Options, page 107](#)
- [Mandatory Options, page 108](#)
- [License Section, page 108](#)
- [general Section, page 108](#)
- [mailer Section, page 111](#)
- [log Section, page 112](#)
- [Transport Parameter Options, page 113](#)
- [Configuring ADDP Between SCS and LCA, page 114](#)
- [Changes from 8.1 to 8.5, page 114](#)

Solution Control Server also supports:

- The common options described in Chapter 1 on [page 13](#).
- The autostart configuration option that you configure in other server applications and that Solution Control Server processes. Refer to the *Framework 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 the following navigation path:

- Solution Control Server Application object > Options tab > Advanced View (Options)

Warning! Configuration section names, configuration option names, and predefined option values are case-sensitive. Type them in Genesys Administrator 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`.

alive_timeout

Default Value: 30

Valid Values: Any value from 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 “Distributed Solution Control Servers” section in the *Framework Deployment Guide* for details about Distributed Solution Control Servers.

disable-switchoverDefault Value: `false`Valid Values: `true`, `false`

Changes Take Effect: Immediately

Specifies if all switchover activity is to be disabled. Set this option to `true` to avoid false switchovers during dynamic migration. When dynamic migration is complete, set this option to `false` (the default) to restore normal behavior, enabling all switchover activity.

disconnect-switchover-timeoutDefault 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_modeDefault 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_rightsDefault Value: `default`

Valid Values:

<code>default</code>	SCS controls the objects associated with it in the Configuration Database.
<code>main</code>	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.

distributed_sync_timeout

Default Value: 0

Valid Values: 0 or any positive integer

Changes Take Effect: Immediately

Specifies a time interval, in seconds, after which a distributed Solution Control Server sends to other Solution Control Servers a request for the status of objects controlled by them, while also sending the statuses of objects that it controls. This enables all Solution Control Servers in the configuration to synchronize object statuses and report them accordingly. If this option is set to zero (0, the default) or is not defined, synchronization attempts are not sent in a timely manner.

Set this option in each Solution Control Server.

-
- Notes:**
- Genesys recommends that, if you want to enable this synchronization, you set this option to a value of no less than 60 seconds to reduce network traffic.
 - With this option enabled, Solution Control Server processes a higher number of messages, and may disconnect from Local Control Agent if the Advanced Disconnect Detection Protocol (ADDP) timeout is too small. Before using this option, ensure that the ADDP timeout between Solution Control Server and Local Control Agent is large enough.
-

ha_service_unavail_primary

Default Value: true

Valid Values: false, true, on off, yes, no

Changes Take Effect: Immediately

Specifies if an application in the HA pair is promoted to primary mode when it is in a Service Unavailable state. If set to true (the default), the application is promoted to primary. If set to false, the application is not promoted. This setting prevents a race condition of HA scripts, which occurs when both SIP Servers are started almost at the same time and go into primary mode for a brief period of time.

lookup_clienthost

Default Value: false

Valid Values: true, false, on, off, yes, no

Changes Take Effect: After restart

Specifies whether to look up the host name of the connected client. If set to `false` (default), SCS does not look up the host name and uses the IP address of the connected client in audit logs. If set to `true`, SCS looks up the host name and uses that in audit logs.

max-req-per-loop

Default Value: 20

Valid Values: 0—32767

Changes Take Effect: After restart

Specifies the maximum number of requests that SCS will process without pausing to scan its connection with LCA and respond appropriately, therefore preventing the connection from closing because of ADDP timing out. When it is set to 0 (zero, disabled), the SCS processes all LCA requests in the queue without pausing. Set this to a non-zero value if SCS manages a large set of hosts and applications, and ADDP is used between SCS and LCA.

Warning! Use this option only when requested by Genesys Customer Care.

service-unavailable-timeout

Default Value: 0

Valid Values: Any value from 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_from

Default Value: No default value

Valid Values: 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.

smtp_host

Default Value: No default value

Valid Values: 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 do not 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 instead.

smtp_port

Default Value: 25

Valid Values: 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.

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 13](#). Note, however, that SCS always uses full log message format, regardless of the `message_format` option setting.

alarm

Default Value: No default value

Valid Values (log output types):

<code>stdout</code>	Alarms are sent to the Standard output (stdout).
<code>stderr</code>	Alarms are sent to the Standard error output (stderr).
<code>network</code>	Alarms are sent to Message Server, which resides anywhere on the network, and Message Server stores the log events in the Log Database.
<code>memory</code>	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
<code>[filename]</code>	Alarms are stored to a file with the specified name.
<code>syslog</code>	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 `alarm` option in Chapter 1 on [page 13](#), 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.

eventloghost

Default Value: No default value

Valid Values: 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 with the `alarm` output level and applies only to computers running Windows NT. If you do not configure this option or do not set its value, alarms are sent to the operating-system log of the computer on which SCS runs.

Transport Parameter Options

Set options in this section in the Transport Parameters of the properties of the port used for the connection to Message Server, using the following navigation path in Genesys Administrator:

- Solution Control Server Application object > Configuration tab > General section > Connections > Connection to Log Message Server > Connections Info > Advanced tab > Transport Parameters

transport Option Collectively, the options make up the parameters of the transport option. When entering the options in Genesys Administrator, only the options are required; `transport =` is prefixed automatically to the list of option/value pairs.

Note: Valid values for these options must have no spaces before or after the delimiter characters “;” (semi-colon) and “=”.

alarms-port

Default Value: 0 (zero)

Valid Values: A valid port number

Changes Take Effect: After restart of Solution Control Server.

Specifies the port number of a client-side port that will be used for the subscription connection from Solution Control Server to the primary Log Message Server.

backup-alarms-port

Default Value: 0 (zero)

Valid Values: A valid port number

Changes Take Effect: After restart of Solution Control Server.

Specifies the port number of a client-side port that will be used for the subscription connection from Solution Control Server to the backup Log Message Server.

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 `addp-timeout` and `addp-remote-timeout` options in the Host object, as described in Chapter 10 on [page 123](#).

Changes from 8.1 to 8.5

[Table 15](#) lists all changes to Solution Control Server options between release 8.1 and the latest 8.5 release.

Table 15: Solution Control Server Configuration Option Changes from 8.1 to 8.5

Option Name	Option Values	Type of Change	Details
general Section			
<code>disable-switchover</code>	<code>true</code> , <code>false</code>	New	See description on page 109 .
<code>distributed_sync_timeout</code>	0 or any positive integer	New	See description on page 110 .
<code>max_switchover_time</code>	0 to any positive integer	Removed	

9

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:

- [Setting Configuration Options, page 115](#)
- [Mandatory Options, page 116](#)
- [agentx Section, page 116](#)
- [snmp Section, page 117](#)
- [snmp-v3-auth Section, page 120](#)
- [snmp-v3-priv Section, page 120](#)
- [Changes from 8.1 to 8.5, page 121](#)

Genesys SNMP Master Agent also supports the options described in Chapter 1 on [page 13](#).

Setting Configuration Options

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

- Genesys SNMP Master Agent `Application` object > `Options` tab > `Advanced View (Options)`

Warning! Configuration section names, configuration option names, and predefined option values are case-sensitive. Type them in Genesys Administrator 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

Options in this section define the connection between Genesys SNMP Master Agent and Solution Control Server (SCS).

This section must be called `agentx`.

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: 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 (non-integer or zero) value, Genesys SNMP Master Agent opens the default port (705) for the TCP/IP connection.

snmp Section

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.

This section must be called `snmp`.

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`
- `password` (in section `snmp-v3-auth`)
- `password` (in section `snmp-v3-priv`)

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: No default value

Valid Values: 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, this `write_community` option controls SNMPv1/v2 Read access.

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: Any valid password

Changes Take Effect: After restart

Specifies the SNMPv3 user password used for authentication.

Warning! The password specified by this option is visible in Genesys Administrator, and is not encrypted in the Configuration Database.

To hide the password in the interface and encrypt it in the database, use the [password](#) option in the `snmp-v3-auth` section instead of this option.

Do *not* use both of these options in the same SNMP Master Agent.

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 do not configure the option, do not set its value, or set it to an invalid value, Genesys SNMP Master Agent uses no authentication.

v3priv_password

Default Value: No default value

Valid Values: Any valid password

Changes Take Effect: After restart

Specifies the SNMPv3 user password used for privacy of data.

Warning! The password specified by this option is visible in Genesys Administrator, and is not encrypted in the Configuration Database.

To hide the password in the interface and encrypt it in the database, use the [password](#) option in the `snmp-v3-priv` section instead of this option.

Do *not* use both of these options in the same SNMP Master Agent.

v3priv_protocol

Default Value: none

Valid Values:

none	No encryption
DES	CBC-DES privacy protocol

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.

write_community

Default Value: No default value

Valid Values: 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 do not configure the option or set its value, no SNMPv1/v2 Write access is allowed.

snmp-v3-auth Section

This section contains options used to mask and encrypt the SNMPv3 user password used for authentication. Refer to the *Genesys Security Deployment Guide* for information about this feature.

This section must be called `snmp-v3-auth`.

password

Default Value: No default value

Valid Value: A valid password

Changes Take Effect: After restart

The user password for authentication in the SNMPv3 system. This option causes the SNMPv3 password to be masked in Genesys Administrator to prevent others from seeing what is being typed. This option also causes Configuration Server to encrypt the password when storing it in the Configuration Database.

Warning! Do not use this option and the `v3auth_password` option in the same SNMP Master Agent.

snmp-v3-priv Section

This section contains options used to mask and encrypt the SNMPv3 user password used for privacy of data. Refer to the *Genesys Security Deployment Guide* for complete information about this feature.

This section must be called `snmp-v3-priv`.

password

Default Value: No default value

Valid Value: A valid password

Changes Take Effect: After restart

The user password for data privacy in the SNMPv3 system. This option causes the SNMPv3 password to be masked in Genesys Administrator to prevent others from seeing what is being typed. This option also causes Configuration Server to encrypt the password when storing it in the Configuration Database.

Warning! Do not use this option and the `v3priv_password` option in the same SNMP Master Agent.

Changes from 8.1 to 8.5

There are no changes to SNMP Master Agent options between release 8.1 and the latest 8.5 release.

10

Host Configuration Options

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

- [Setting Configuration Options, page 123](#)
- [Mandatory Options, page 123](#)
- [addp Section, page 124](#)
- [ntp-service-control Section, page 124](#)
- [rdm Section, page 125](#)
- [security Section, page 125](#)
- [Changes from 8.1 to 8.5, page 129](#)

Setting Configuration Options

Unless specified otherwise, set Host configuration options in the annex of the Host object, using the following navigation path:

- Host object > Options tab > Advanced View (Annex)

Warning! Configuration section names, configuration option names, and predefined option values are case-sensitive. Type them in Genesys Administrator 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.

ntp-service-control Section

This section contains configuration options to control NTP services.

This section must be called `ntp-service-control`.

signature

Default Value:

Windows	W32Time
Red Hat Linux	/usr/sbin/ntpd
AIX	/usr/sbin/xntpd
Solaris	/usr/lib/inet/xntpd

Valid Values:

Windows Valid service name
Other platforms: Command line for executing NTP daemon process.

Changes Take Effect: Immediately

Enables the configuration of an NTP service or daemon signature.

rdm Section

This section contains the option necessary to configure remote deployment using Genesys Administrator.

This section must be called `rdm`.

port

Default: 5000

Valid Values: A valid port number

Changes Take Effect: Immediately

Specifies the port used by the Genesys Deployment Agent to remotely deploy applications on this host.

Note: The value of this option must be the same as the port number entered on the command line when starting Genesys Deployment Agent. Refer to the *Framework Deployment Guide* for information about starting Genesys Deployment Agent. Refer to the *Genesys Administrator Extension Help* file for information about remote deployment using Genesys Administrator.

security Section

This section contains the configuration options required to configure secure data exchange using TLS. For information about how to use these options, refer to the chapter “Genesys TLS Configuration” in the Genesys Security Deployment Guide.

This section must be called `security`.

cipher-list

Default Value: No default value

Valid Values: The list of ciphers

Changes Take Effect: After component restart

Specifies the defined list of ciphers. The cipher list must be in a valid format. See the chapter “Genesys TLS Configuration” in the *Genesys Security Deployment Guide* for information about cipher formatting rules and examples of valid cipher strings.

This option can be configured at the host, application, or connection (port) level. This section assumes you are configuring it at the host level. To configure it at another level, refer to:

- To configure it at the port level, see [page 43](#).
- To configure it at the application level, see [page 34](#).

Note: If this option is configured at multiple levels (connection, application, host), the value set at the lowest level takes precedence. That is:

- The value set at the connection level takes precedence over the value set at the application and host levels.
 - The value set at the application level takes precedence over the value set at the host level.
-

client-auth

Default Value: 1

Valid Values: 0, 1

Changes Take Effect: After application restart

Specifies whether authentication of the security certificate in the client TLS socket is to be disabled. When set to 1 (default), authentication is enabled. When set to 0, the client socket does not authenticate the server when connected over TLS.

This option must be set at the same level where the certificate itself is configured. Use this option if the security certificate is configured at the host level. If it is configured at another level, do one of the following:

- If the security certificate is configured at the port level, see [page 44](#).
- If the security certificate is configured at the application level, see [page 35](#).

Note: If this option is configured at multiple levels (connection, application, host), the value set at the lowest level takes precedence. That is:

- The value set at the connection level takes precedence over the value set at the application and host levels.
 - The value set at the application level takes precedence over the value set at the host level.
-

gda-tls

Default Value: `false`

Valid Values: `false`, `true`

Changes Take Effect: After restart of Genesys Deployment Agent

Specifies whether all communication between Genesys Deployment Agent and its clients must be through a secured connection. Genesys Deployment Agent does not use this option. If set to `true`, it indicates to clients that Genesys Deployment Agent is listening on a secure channel.

This option is set in the annex of the host on which Genesys Deployment Agent is running.

lca-upgrade

Default Value: `0` (`false`)

Valid Values: `0` (`false`), `1` (`true`)

Changes Take Effect: After restart of LCA

Specifies whether all communication between SCS and LCA must be done through a secured connection.

This option is set in the annex of the host on which LCA is running.

ip-version

Default Value: `4, 6`

Valid Values: `4, 6` and `6, 4`

Changes Take Effect: At restart

Specifies the order in which IPv4 (`4`) and IPv6 (`6`) are used on the connection between SCS and LCA. This option is set in the Annex of the Host object.

Refer to Table 7 on [page 47](#) to see how this option affects the connection for which it is configured.

For more information about IPv6, refer to the “Solution Availability” and “IPv6” sections of the *Framework Deployment Guide*.

sec-protocol

Default Value: `SSLv23`

Valid Values: `SSLv23`, `SSLv3`, `TLSv1`, `TLSv11`, `TLSv12`

Changes Take Effect: Immediately

Specifies the protocol used by the component to set up secure connections. Exactly how this option behaves depends on the platform on which the application, for which the option is configured, is running.

When configured on the Windows platform, this option complements Windows operating system settings that enable and disable a particular secure protocol. If there is a conflict between Windows settings and this option, the operating system settings are used.

Note: On the Windows platform, this option applies to only a limited number of 8.5.x components. Check the documentation for your particular component to see if this option does apply, and if so, if there are additional limitations.

On UNIX and Linux platforms, this option controls how the Security Pack on UNIX selects the protocol to use, as shown in [Table 16](#).

Table 16: Values for sec-protocol option

Option Value	SSL Protocol Version			TLS Protocol Version		
	2 ^a	2.3	3	1	1.1	1.2
SSLv23 ^b	X	X	X	X	X	X
SSLv3			X			
TLSv1				X		
TLSv11					X	
TLSv12						X

- SSL 2 is supported only if SSL 2 ciphers are explicitly defined. In this case, SSL 2 clients can connect only to servers running in SSLv23 mode.
- SSL 2.3 is compatible with all other supported versions, and connects to a client running in the highest mode used by the client.

For more information about using this option on UNIX and Linux platforms, refer to “Genesys Implementation of Secure Protocol Connections” in the [Framework 8.5 Deployment Guide](#).

This option is configured on one of three levels:

- Host-level (the application host): In the `security` section of the annex of the Host object.
- Application-level: In the `security` section of the options of the Application object.
- Port-level (connection-level): As a transport parameter of the application's connection.

If the component reads its configuration information solely from its configuration file, such as LCA or Genesys Deployment Agent, set this option in the `security` section of the appropriate configuration file (such as `lca.cfg` for LCA or `gda.cfg` for Genesys Deployment Agent).

On a single component, this option must be set at the same level where the security certificate is configured. Use this option if the security certificate is

configured at the host level. If it is configured at another level, do one of the following:

- If the security certificate is configured at the port level, see [page 45](#).
- If the security certificate is configured at the application level, see [page 35](#).

Note: If this option is configured at multiple levels (connection, application, host) across the network, the value set at the lowest level takes precedence. That is:

- The value set at the connection level takes precedence over the value set at the application and host levels.
- The value set at the application level takes precedence over the value set at the host level.

Changes from 8.1 to 8.5

[Table 17](#) lists all changes to Host options between release 8.1 and the latest 8.5 release.

Table 17: Host Configuration Option Changes from 8.1 to 8.5

Option Name	Option Values	Type of Change	Details
security Section			
cipher-list	List of ciphers	Modified	See description on page 126 . To configure cipher list at Host level. Documented incorrectly in previous release.
ip-version	4, 6 and 6, 4	New	See description on page 127 . Added in release 8.1; not previously documented.
lca-upgrade	0, 1	Documentation correction	See description on page 127 . Valid values documented incorrectly (<i>false</i> , <i>true</i>) in previous version.
sec-protocol	SSLv23, SSLv3, TLSv1, TLSv11	New	See description on page 127 . If security certificate configured at Host level.

Table 17: Host Configuration Option Changes from 8.1 to 8.5

Option Name	Option Values	Type of Change	Details
upgrade	0, valid certificate information	Removed	Moved to LCA chapter; documented incorrectly in previous version.

11

Tenant and User Configuration Options

This chapter describes configuration options for a Tenant object and related options for a User object. The options set at the User level either override Tenant-level options, or contain information about actions taken as a result of Tenant-level options or their overrides.

This chapter contains the following sections:

- [Setting Configuration Options, page 131](#)
- [Mandatory Options, page 132](#)
- [Passwords in Configurations with Multiple Tenants, page 132](#)
- [security-authentication-rules Section, page 133](#)
- [Changes from 8.1 to 8.5, page 142](#)

Note: The User configuration options described in this chapter are not a complete set of options available, nor are they considered mandatory for a User. Refer to the documentation for the Genesys applications you are installing for additional User-level options that may be required.

Setting Configuration Options

Unless specified otherwise, set Tenant configuration options in the annex of the Tenant object, using the following navigation path:

- Tenant object > Options tab > Advanced View (Annex)

The options in this section applies to all objects owned by the Tenant in which the options are set, unless the options are overridden in a child Tenant or at the User level.

Unless specified otherwise, set User configuration options in the annex of the User object, using the following navigation path:

- User object > Options tab > Advanced View (Annex)

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

Mandatory Options

You do not have to configure any options described in this chapter for a Tenant or User.

Passwords in Configurations with Multiple Tenants

In configurations with multiple Tenants, the inheritance rule applies for many of the password-related features listed in this chapter. If a feature is not configured for a particular tenant, rules for ancestor tenants are used, up to the ENVIRONMENT tenant (assuming there is no termination of inheritance otherwise). If no rule is set in the ancestor tree, no limits exist.

If a particular tenant requires different settings from its ancestors, you can configure it in two ways:

- Configure only those settings to be changed. Use this method only if you want to change a few specific settings; otherwise use inherited value for the other settings. This will override the inherited values for those settings and leave the values of other settings unchanged, including those inherited from ancestor tenants. Where applicable, child tenants of this tenant will inherit the new values of the changed settings.
- Reset all options to their default values, and then customize the values as required for this tenant. Use this method only if you want to reset or change multiple settings for this tenant and its descendents. To set all options in the `security-authentication-rules` section to their default settings, set the `tenant-override-section` option (see [page 139](#)) to true. This option breaks the inheritance chain, effectively making this tenant a new inheritance node for all child tenants, and is easier than changing each option manually. Then, for this tenant and its child tenants, you can set appropriate values for any individual option for which you do not want the default value to apply.

security-authentication-rules Section

This section contains configuration options for defining custom properties of user passwords, and setting up and using passwords. The options in this section are configured at either the tenant level ([page 133](#)) or the user level ([page 140](#)). Refer to the “User Passwords” chapter in the *Genesys Security Deployment Guide* for complete information about these options.

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

Tenant-level Options

The options in this section are configured in the `security-authentication-rules` section in the annex of the Tenant object, as follows:

- Tenant object > Options tab > Advanced View (Annex)

account-expiration

Default Value: 0

Valid Values: 0 to 365

Takes Effect: Rule validation occurs the next time an account belonging to this Tenant tries to log in or authenticate, or when a User object belonging to this Tenant is retrieved or changed

Specifies the maximum number of days for which an account can remain idle. After this time interval, the account will be considered expired and the user will not be able to log in until the account has been reactivated by the system administrator. Configuration Server checks for expired accounts when an account belonging to this Tenant tries to log in or authenticate, or when a User object belonging to this Tenant is retrieved or changed.

Note: Account expiration functionality does not work correctly if the Last Login feature is not configured. That is, the master Configuration Server and all Configuration Server Proxies must have the `last-login` ([pages 62 and 85](#)) and `last-login-synchronization` ([pages 62 and 86](#)) options both set to true. Calculations for the expiration of a particular account starts after the first login is recorded as a part of the Last Login feature; if the last login is not available, account expiration does not apply.

If set to 0 (the default), there is no expiration of idle accounts for any user.

In configurations with multiple Tenants, this value applies to all child Tenants unless it is overridden in a child Tenant. See “Passwords in Configurations with Multiple Tenants” on [page 132](#) for more information.

-
- Notes:**
- This option does not apply to the `Default` account, which does not expire.
 - This option does not apply to accounts that are externally authenticated, if an external authentication Domain was configured.
 - This option can be overridden for individual users using the `override-account-expiration` option (see [page 141](#)).
-

account-lockout-attempts-period

Default Value: 0

Valid Values: 0 · 20

Takes Effect: At the next occurrence of an unsuccessful login attempt

Specifies the length of time (in minutes) since the last unsuccessful login attempt in which another unsuccessful attempt will be counted toward the lockout threshold specified by `account-lockout-threshold`. If another unsuccessful attempt is recorded before this time interval expires, the time of this latest attempt becomes the basis from which this time period is calculated. In effect, this period is a sliding window.

If no additional unsuccessful attempts occur within this time period, the number of unsuccessful attempts is cleared, and previous attempts are not counted towards the lockout threshold.

This time period applies to all user accounts belonging to this Tenant, unless overridden at the User level by the `account-override-lockout` option.

In configurations with multiple Tenants, this value applies to all child Tenants unless it is overridden in a child Tenant. See “Passwords in Configurations with Multiple Tenants” on [page 132](#) for more information.

account-lockout-duration

Default Value: 30

Valid Values: 0 · 1440

Takes Effect: Next time an account is locked out

Specifies the length of time (in minutes) that the lockout lasts after the lockout condition has been met.

Accounts already locked when this option is changed are released after the time specified by this option elapses, regardless of how long they were locked out originally.

This lockout duration applies to all user accounts belonging to this Tenant unless overridden at the User level by the `account-override-lockout` option.

In configurations with multiple Tenants, this value applies to all child Tenants unless it is overridden in a child Tenant. See “Passwords in Configurations with Multiple Tenants” on [page 132](#) for more information.

account-lockout-threshold

Default Value: 0

Valid Values: 0 to 8

Takes Effect: At next attempt to log in

Specifies the number of consecutive unsuccessful login attempts that a user account can make before being locked out. When set to the 0 (the default), no lockout will occur. This threshold applies to all user accounts belonging to this Tenant unless overridden at the User level by the [account-override-lockout](#) option.

force-password-reset

Default Value: false

Valid Values: false, true

Takes Effect: Immediately

Specifies whether all applications must prompt all of their users to change their passwords at first login. If set to true, all users for whom password reset is enabled (Reset password is checked on the user Configuration tab) will be unable to login unless they reset their password the next time that they log in. Any exceptions to the policy of changing passwords at first login (down-level applications or applications for which the no-change-password-at-first-login option is set to true) will not be permitted. The user will not be able to log in until he or she uses the correct application or the administrator clears the Reset password checkbox on the corresponding User object's Configuration tab.

For example, you might want to use this option to ensure that there are no exceptions to the policy of changing passwords at first login.

max-account-sessions

Default Value: 0

Valid Values: 0 to 128

Takes Effect: At next attempt to connect to Configuration Server.

Specifies the number of simultaneous connections that each account can have with a single instance of Configuration Server. If an account tries to exceed the number of connections, login is denied.

In configurations with multiple Tenants, if this option is missing from the Tenant in which the account is logging in, the value set in the Parent up to the inheritance node for this Tenant applies. See “Passwords in Configurations with Multiple Tenants” on [page 132](#) for more information.

If this option is set to 0 (the default), there are no limits.

This option can be overridden for individual users by setting this option, with the same valid values, in the annex of the particular User object.

Note: Sessions restored and authenticated through existing sessions are not included in the count of sessions for this option.

password-expiration

Default Value: 0

Valid Values: 0 to 365

Takes Effect: Immediately

Specifies the number of days from when the user password was created and after which the password is considered expired and cannot be used. If set to 0 (the default), the password will not expire.

This option does not apply to empty passwords, nor to the password for the default account that never expires.

In configurations with multiple Tenants, this value applies to all child Tenants unless it is overridden in a child Tenant. See “Passwords in Configurations with Multiple Tenants” on [page 132](#) for more information.

password-expiration-notify

Default Value: 0

Valid Values: 0 to 364

Takes Effect: Immediately

Specifies the number of days before a user password expires that a notice will be displayed to the user warning that his or her password will expire. To take effect, the specified value must be less than the number of days left before the password expires. If set to 0 (the default), no notification is sent.

This option applies only if the password-expiration option (see [page 136](#)) is configured at the Tenant level.

In configurations with multiple Tenants, this value applies to all child Tenants unless it is overridden in a child Tenant. See “Passwords in Configurations with Multiple Tenants” on [page 132](#) for more information.

password-min-length

Default Value: No default value

Valid Values: 0 to 64

Takes Effect: Immediately

Optional. Specifies the minimum length (in characters) of a password used by all users in the Tenant in which the option is defined. If this option is present, it overrides the allow-empty-password (see [page 56](#)) option.

If this option is set to 0, an empty password is permitted (regardless of the value of allow-empty-password). If this option is set to a value greater than the maximum allowed value (64), the maximum value is used.

-
- Notes:**
- This option applies only to passwords used with internal authentication. It does not apply if you are using external authentication. However, if you are using external authentication, do not set this option to a value greater than the length set by the external authentication.
 - This option applies only to passwords set after this option has been configured. Existing valid passwords that do not meet the minimum length requirement are not rejected during login; however, when the user tries to change one of these passwords, the new password will be subject to this option.
 - Genesys recommends you use this option instead of the `allow-empty-password` option, which is provided only for purposes of backward compatibility.
-

password-no-repeats

Default: 0

Valid Values: 0 to 10

Changes Take Effect: At the next password creation or change

Specifies the number of password changes that must occur (that is, the number of old passwords) before a prior password can be reused. If set to 0 (the default), no history of used passwords is kept, and a password can be re-used as desired.

In configurations with multiple Tenants, this value applies to all child Tenants unless it is overridden in a child Tenant. See “Passwords in Configurations with Multiple Tenants” on [page 132](#) for more information.

password-req-alpha

Default: false

Valid Values: false, true

Changes Take Effect: At the next password creation or change

Specifies whether a password must contain at least one US-ASCII alphabetic character (a-z, A-Z). If set to true, and a password being created or changed does not contain one or more alphabetic characters, Configuration Server will not save the changes.

In configurations with multiple Tenants, this value applies to all child Tenants unless it is overridden in a child Tenant. See “Passwords in Configurations with Multiple Tenants” on [page 132](#) for more information.

-
- Notes:**
- This option applies only to passwords used with internal authentication. It does not apply if you are using external authentication.
 - This option applies only to passwords set after this option has been configured. Existing valid passwords that do not meet the alphabetic requirement are not rejected during login; however, when the user tries to change one of these passwords, the new password will be subject to this option.
-

password-req-mixed-case

Default: `false`

Valid Values: `false`, `true`

Changes Take Effect: At the next password creation or change

Specifies whether a password must contain at least one uppercase character (A-Z) and one lowercase character (a-z) from the US-ASCII character set. If set to `true`, and a password being created or changed does not contain one or more uppercase characters and one or more lowercase characters, Configuration Server will not save the changes.

In configurations with multiple Tenants, this value applies to all child Tenants unless it is overridden in a child Tenant. See “Passwords in Configurations with Multiple Tenants” on [page 132](#) for more information.

-
- Notes:**
- This option applies only if `password-req-alpha=true`; see [page 137](#).
 - This option applies only to passwords used with internal authentication. It does not apply if you are using external authentication.
 - This option applies only to passwords set after this option has been configured. Existing valid passwords that do not meet the mixed-case requirement are not rejected during login; however, when the user tries to change one of these passwords, the new password will be subject to this option.
-

password-req-number

Default: `false`

Valid Values: `false`, `true`

Changes Take Effect: At the next password creation or change

Specifies whether a password must contain at least one numeric character (0-9). If set to `true`, and a password being created or changed does not contain one or more numeric characters, Configuration Server will not save the changes.

In configurations with multiple Tenants, this value applies to all child Tenants unless it is overridden in a child Tenant. See “Passwords in Configurations with Multiple Tenants” on [page 132](#) for more information.

-
- Notes:**
- This option applies only to passwords used with internal authentication. It does not apply if you are using external authentication.
 - This option applies only to passwords set after this option has been configured. Existing valid passwords that do not meet the numeric requirement are not rejected during login; however, when the user tries to change one of these passwords, the new password will be subject to this option.
-

password-req-punctuation

Default: `false`

Valid Values: `false`, `true`

Changes Take Effect: At the next password creation or change

Specifies whether a password must contain at least one punctuation character from the US-ASCII character set. If set to `true`, and a password being created or changed does not contain one or more punctuation characters, Configuration Server will not save the changes.

The following punctuation characters are permitted:

- `! " # $ % & ' () * + , - . /`
- `: ; < = > ?`
- `[\] ^ _ ``
- `{ | } ~`

In configurations with multiple Tenants, this value applies to all child Tenants unless it is overridden in a child Tenant. See “Passwords in Configurations with Multiple Tenants” on [page 132](#) for more information.

-
- Notes:**
- This option applies only to passwords used with internal authentication. It does not apply if you are using external authentication.
 - This option applies only to passwords that are set after this option has been configured. Existing valid passwords that do not meet the punctuation requirement are not rejected during login; however, when the user tries to change one of these passwords, the new password will be subject to this option.
-

tenant-override-section

Default: `false`

Valid Values: `false`, `true`

Changes Take Effect: Immediately

Applies only in a configuration with multiple Tenants; specifies how Configuration Server interprets or applies values for options in the configuration option section `security-authentication-rules`, as follows:

- If this Tenant has values configured for one or more of these options, those values are applied. Values for the other options are assigned as described in the following two bullets, depending on the value of this option (`tenant-override-section`).
- If this Tenant has no values configured for any of these options, and this option (`tenant-override-section`) is either absent or set to `false`, values defined at the nearest ancestor Tenant are applied.
- If this Tenant has no values configured for any of these options, and this option (`tenant-override-section`) is set to `true`, default values are applied to all options. Values assigned in ancestor Tenants are ignored for this Tenant.

In effect, this option allows customization of these options for this Tenant and its child Tenants, if required, and applies to all options in the `security-authentication-rules` section in the same object.

User-level Options

These options are configured at the User-level. They either override settings made at the Tenant level, or contain information about actions taken as a result of settings at the Tenant level or their overrides at the User level. Options in this section are configured in the `security-authentication-rules` section in the annex of the User object, as follows:

- User object > Options tab > Advanced View (Annex)

Note: The User configuration options described in this section are not a complete set of options available for a User. Refer to the documentation for Genesys applications that you are installing for additional User-level options that might be required.

account-override-lockout

Default Value: `false`

Valid Values: `false`, `true`

Takes Effect: At the next attempt to log in to any instance of Configuration Server

Specifies whether this user account can be locked out. If set to `true`, this user can override the lockout rules set at its Tenant level. A `true` value can also be used to unlock, or clear, a locked account if set before the `account-lockout-duration` option (see [page 134](#)) is set at the Tenant level. If set to `false` (the default), the lockout will expire as configured at the Tenant level.

last-expired-at

Specifies when the user account expired, for example:

Sat Oct 13 12:42:52 2012

This option is set automatically by Configuration Server or Configuration Server Proxy and appears in the annex of the User object. The value is read-only, and is for reference purposes only.

last-locked-at

Specifies when the user account was locked, and the name of the instance of Configuration Server in which the lockout occurred. For example:

09/12/09 10:445 PM @confserv

This option is set automatically by Configuration Server or Configuration Server Proxy and appears in the annex of the User object. The value is read-only, and is for reference purposes only.

override-account-expiration

Default Value: 0

Valid Values:

- | | |
|---|--|
| 0 | Default. No override; the expiration value set at the Tenant level applies. Each time that this account tries to log in or authenticate, or an attempt is made to read or change the User object, the idle time calculation restarts. |
| 1 | No check for account expiration is made when the user tries to log in or authenticate, or when the User object is retrieved; the value of the Tenant-level option <code>account-expiration</code> is ignored. If this account is marked as expired (<code>last-expired-at</code> is set to a valid date/time stamp), it is reactivated. |
| 2 | Check for idle time does not occur at next login attempt. After user has logged in successfully, idle time calculation restarts and the value of this option is reset to 0 (the default). |

Takes Effect: At the next time the user tries to log in or authenticate, or an attempt is made to read or change the User object.

Specifies if account expiration, as defined by the Tenant-level option `account-expiration` (see [page 133](#)), applies to a particular user account.

-
- Notes:**
- This option does not apply to the Default account, which does not expire.
 - This option does not apply to accounts that are externally authenticated.
-

override-password-expiration

Default Value: false

Valid Values: false, true

Takes Effect: At the next attempt to log in or authenticate the user

Specifies whether a password of the user for which this option is configured can override the expiration policy specified at the Tenant level by the `password-expiration` option. If set to `true`, the user password for this user will not expire. If set to `false` (default), the user password will expire as configured at the Tenant level.

This option applies only if `password-expiration` is configured at the Tenant level.

Changes from 8.1 to 8.5

[Table 18](#) lists all changes to Tenant and User options between release 8.1 and the latest 8.5 release

Note: For information about Tenant configuration options that relate to external authentication, refer to the *Framework External Authentication Reference Manual*.

Table 18: Tenant and User Configuration Option Changes from 8.1 to 8.5

Option Name	Option Values	Type of Change	Details
security-authentication-rules Section			
account-override-logout	false, true	Modified	User-level option. See description on page 140 . Corrected description of when set to false.



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 8.5 Deployment Guide*](#), which will help you configure, install, start, and stop Framework components.
- [*Framework 8.1 Genesys Administrator Help*](#), which will help you use Genesys Administrator.
- Release Notes and Product Advisories for this product, which are available on the [*Genesys Documentation*](#) website.

Genesys

- [*Genesys 8.5 Security Deployment Guide*](#), which describes configuration options specific to Genesys security features, and how to use them.
- [*Genesys Technical Publications Glossary*](#), which provides a comprehensive list of the Genesys and computer-telephony integration (CTI) terminology and acronyms used in this document.
- [*Genesys Migration Guide*](#) and [*Management Framework Migration Guide*](#), which provide documented migration strategies for Genesys product releases. Contact Genesys Customer Care for more information.

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

- [*Genesys Supported Operating Environment Reference Guide*](#)
- [*Genesys Supported Media Interfaces Reference Manual*](#)

Consult the following additional resources as necessary:

- [*Genesys Interoperability Guide*](#), which provides information on the compatibility of Genesys products with various Configuration Layer Environments; Interoperability of Reporting Templates and Solutions; and Gplus Adapters Interoperability.
- [*Genesys Licensing Guide*](#), which introduces you to the concepts, terminology, and procedures that are relevant to the Genesys licensing system.

For additional system-wide planning tools and information, see the release-specific listings of System Level Documents on the [Genesys Documentation](#) website.

Genesys product documentation is available on the:

- Genesys Customer Care website at <http://genesys.com/customer-care>.
- Genesys Documentation wiki at <http://docs.genesys.com/>.
- Genesys Documentation Library DVD, which you can order by e-mail from Genesys Order Management at orderman@genesys.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:

81fr_ref-co_04-2012_v8.1.100.01

You will need this number when you are talking with Genesys Customer Care 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 19 on [page 146](#) describes and illustrates the type conventions that are used in this document.

Table 19: Type Styles

Type Style	Used For	Examples
Italic	<ul style="list-style-type: none"> Document titles Emphasis Definitions of (or first references to) unfamiliar terms Mathematical variables <p>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 146).</p>	<p>Please consult the <i>Genesys Migration Guide</i> for more information.</p> <p>Do <i>not</i> use this value for this option.</p> <p>A <i>customary and usual</i> practice is one that is widely accepted and used within a particular industry or profession.</p> <p>The formula, $x + 1 = 7$ where x stands for...</p>
Monospace font (Looks like teletype or typewriter text)	<p>All programming identifiers and GUI elements. This convention includes:</p> <ul style="list-style-type: none"> The <i>names</i> 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. <p>Also used for any text that users must manually enter during a configuration or installation procedure, or on a command line.</p>	<p>Select the Show variables on screen check box.</p> <p>In the Operand text box, enter your formula.</p> <p>Click OK to exit the Properties dialog box.</p> <p>T-Server distributes the error messages in EventError events.</p> <p>If you select true for the inbound-bsns-calls option, all established inbound calls on a local agent are considered business calls.</p> <p>Enter exit on the command line.</p>
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.	<code>smcp_server -host [/flags]</code>
Angle brackets (< >)	<p>A placeholder for a value that the user must specify. This might be a DN or a port number specific to your enterprise.</p> <p>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.</p>	<code>smcp_server -host <confighost></code>



Index

Symbols

<key-name>
configuration option 33

A

account-expiration
Tenant option 133
account-lockout-attempts-period
Tenant option 134
account-lockout-duration
configuration option 140
Tenant option 134
account-lockout-threshold
configuration option 134
Tenant option 135
account-override-lockout
configuration option 134, 135
User option 140, 142
active
Configuration Server option 74
Configuration Server Proxy option 90
addp
Configuration Server option 79
addp section
Host 124
ADDP, configuring between
redundant Configuration Servers 67
SCS and LCA 124
addp-remote-timeout
Configuration Server option 67
Host option 124
addp-timeout
Configuration Server option 68, 79
Host option 124
addp-trace
Configuration Server option 68, 79
address
common configuration option 42

agentx section
SNMP Master Agent 116–117
alarm
common log option 22
Solution Control Server option 112
alarms-port
Solution Control Server option 113
alive_timeout
Solution Control Server option 108
all
common log option 21
Configuration Server Proxy option 90
allow-empty-password
configuration option 56, 78, 136, 137
allow-external-empty-password
configuration option 56, 78
allow-mixed-encoding
Configuration Server option 57, 78
Configuration Server Proxy option 84
Application Parameter options
Configuration Server 75–76
Configuration Server Proxy 89
autostart
common configuration option 38, 49
configuration option 107

B

backlog
Configuration Server option 75
Configuration Server Proxy option 89
backup-alarms-port
Solution Control Server option 114
backup-port
common configuration option 42
block-messages
Message Server option 104
block-messages-by-<type>
Message Server option 104
block-messages-from-<DBID>
Message Server option 104

buffering
 common log option 14

C

changes from 8.1 to 8.5
 common configuration options 48
 Configuration Server options 78
 Configuration Server Proxy options 90
 Database Access Point options 52
 Genesys Deployment Agent options 100
 Host options 129
 LCA options 96
 Message Server options 105
 SNMP Master Agent options 121
 Solution Control Server options 114
 Tenant/User options 142
 check-point
 common log option 14
 cipher-list
 common configuration option 34, 43, 48,
 49, 126
 Host option 129
 client_lifespan
 Configuration Server Proxy option 90
 client-auth
 common configuration option 35, 44
 host configuration option 126
 client-connect-timeout
 Configuration Server option 57, 78
 client-expiration
 Configuration Server option 74
 Configuration Server Proxy option 89
 client-lifespan
 Configuration Server option 80
 client-response-timeout
 Configuration Server option 57, 78
 Configuration Server Proxy option 85, 90
 common configuration options 14-48
 address 42
 autostart 38, 49
 backup-port 42
 changes from 8.1 to 8.5 48
 cipher-list 34, 43, 48, 49, 126
 client-auth 35, 44
 common section 40-41
 crl 44
 dbserver section 40-70
 dml-retry 49, 79
 enable-async-dns 41
 enable-ipv6 41
 hangup-restart 39
 heartbeat-period 39
 heartbeat-period-thread-class-<n> 40
 ip-version 47, 49, 127
 log section 14-28

log-extended section 28-30
 log-filter section 31-32
 log-filter-data section 33-34
 mandatory 14
 port 42
 rebind-delay 41
 sec-protocol 35, 45, 48, 49
 security section 34-37
 security-authentication-rules section 38
 setting 13
 sml section 38-40
 suspending-wait-timeout 40
 throttle-period 48
 throttle-threshold 48
 tls 46
 tls-mutual 37, 49
 tls-target-name-check 37
 transport 42
 Transport Parameter options 41-47
 x-dblib-debug 72, 105
 common log options 14-32
 alarm 22
 all 21
 buffering 14
 check-point 14
 compatible-output-priority 48
 debug 24
 default-filter-type 31
 enable-thread 15, 48
 expire 15, 48
 filtering 32
 interaction 23
 keep-startup-file 15
 level-reassign-<eventID> 28
 level-reassign-disable 28
 log section 14-28
 log-extended section 28-30
 log-filter section 31-32
 log-filter-data section 33-34
 mandatory options 14
 memory 16
 memory-storage-size 16
 message_format 16, 48
 messagefile 17
 message-format 48
 no-memory-mapping 17, 48
 print-attributes 18
 segment 18, 48
 setting 13
 snapshot 18, 48
 spool 19
 standard 22
 throttle-period 19
 time_convert 20
 time_format 20
 trace 23

- verbose 20
- x-conn-debug-all 26
- x-conn-debug-api 26
- x-conn-debug-dns 27
- x-conn-debug-open 27
- x-conn-debug-security 27
- x-conn-debug-select 27
- x-conn-debug-timers 28
- x-conn-debug-write 28
- common options
 - common log options 14–32
 - common section 40–41
 - dbserver section 40–70
 - mandatory options 14
 - sml section 38–40
- common section
 - common options 40–41
- compatible-output-priority
 - common log option 48
- Configuration Database section
 - Configuration Server 68–70
- configuration files
 - Configuration Server 77
 - Genesys Deployment Agent 99
 - LCA 96
 - Message Server 105
- configuration options
 - <key-name> 33
 - account-lockout-duration 140
 - account-lockout-threshold 134
 - account-override-lockout 134, 135
 - allow-empty-external-password 78
 - allow-empty-password 56, 78, 136, 137
 - allow-external-empty-password 56
 - autostart 107
 - common log options 14–32
 - common options 14–48
 - Configuration Server 55–77
 - Configuration Server Proxy 84–89
 - Database Access Point 51–52
 - force-password-reset 38
 - Genesys Deployment Agent 98–99
 - Host 124–129
 - last-login 62, 85
 - LCA 94–96
 - mandatory
 - common 14
 - Configuration Server Proxy 84
 - Database Access Point 51
 - Genesys Deployment Agent 97
 - Host 123
 - LCA 93
 - log 14
 - Message Server 101
 - SNMP Master Agent 116, 108
 - Tenant/User 132
 - Message Server 102–105
 - no-change-password-at-first-login 38, 135
 - password 120
 - password-expiration 136, 142
 - password-min-length 56, 136
 - setting
 - common 13
 - Configuration Server 53, 83
 - Database Access Point 51
 - Genesys Deployment Agent 97
 - Host 123
 - LCA 93
 - Message Server 101
 - SNMP Master Agent 115, 107
 - Tenant 131
 - User 132
 - SNMP Master Agent 116–120
 - Solution Control Server 108–114
 - Tenant 133–140
 - Tenant/User 133–142
 - User 140–142
- Configuration Server
 - log section 72–73
 - runtime options 70–75
 - sample configuration file 77
 - security section 73–74
 - system section 71–72
- Configuration Server options 55–77
 - active 74
 - addp 79
 - addp-remote-timeout 67
 - addp-timeout 68, 79
 - addp-trace 68, 79
 - allow-mixed-encoding 57, 78
 - Application Parameters 75–76
 - backlog 75
 - changes from 8.1 to 8.5 78
 - client-connect-timeout 57, 78
 - client-expiration 74
 - client-lifespan 80
 - client-response-timeout 57, 78
 - Configuration Database section 68–70
 - Configuration Server section 55–68
 - confserv section 55–68
 - dbengine 69, 79
 - dbname 69
 - dbserver 69
 - dbthread 57, 78, 103
 - debug 80
 - decryption-key 58, 78
 - disable-vag-calculation 58
 - dml-retry 69
 - enable-pre-812-security 59
 - encoding 59, 85

- encryption 60, 78
 - expiration 74
 - fix_cs_version_7x 60
 - force-md5 61
 - force-offline 71, 78
 - force-reconnect-reload 71, 79, 81
 - hca section 80
 - history-log 74–75
 - history-log-guid 80
 - history-log-minid 80
 - history-log-version 80
 - host 80
 - langid 62, 79
 - last-login 62
 - last-login-synchronization 62, 86
 - license 71, 79
 - locale 63
 - log section 72–73
 - management-port 63
 - max-client-output-queue-size 63, 79
 - max-output-queue-size 64, 79
 - max-records 75
 - multi-languages 64
 - no-default-access 73
 - objects-cache 64
 - packet-size 65, 79
 - password 70
 - password-change 65
 - peer-switchover-tmout 65, 79
 - port 66, 80
 - postgre-standard-conforming- 81
 - postgre-standard-conforming-strings 71
 - prevent-mediatype-attr-removal 72, 81
 - primary-startup-tmout 66, 79
 - protocol 67
 - reconnect-timeout 80
 - response-timeout 70
 - runtime options 70–75
 - schema 80
 - security section 73–74
 - server 66, 67, 68, 80
 - setting 53
 - skip-environment-enum-transfer 72, 81
 - soap section 80
 - startup options 54–70
 - system section 71–72, 81
 - tls 76
 - transport 76
 - Transport Parameter options 76–77
 - upgrade-mode 79
 - user 76, 81
 - username 70
 - write-former-value 75, 81
 - x-dblib-sql 73, 80
 - Configuration Server Proxy options 84–89
 - active 90
 - all 90
 - allow-mixed-encoding 84
 - Application Parameters 89
 - backlog 89
 - changes from 8.1 to 8.5 90
 - client_lifespan 90
 - client-expiration 89
 - client-response-timeout 85, 90
 - csproxy section 84–88
 - debug 91
 - expiration 90
 - failsafe-store-processing 90
 - history-log section 88–89
 - last-login 85
 - license section 84
 - locale 86
 - mandatory options 84
 - max-client-output-queue-size 86, 90
 - max-output-queue-size 87, 90
 - max-records 90
 - objects-cache 87
 - packet-size 87, 90
 - port 91
 - proxy-cluster-name 88, 90
 - proxy-writable 88
 - setting 83
 - soap section 90
 - user 89, 91
 - Configuration Server section
 - Configuration Server 55–68
 - Configuration Server startup options 54–70
 - confserv section
 - Configuration Server 55–68
 - crl
 - common configuration option 44
 - csproxy section
 - Configuration Server Proxy 84–88
- ## D
- ### DAP
- See Database Access Point
 - Database Access Point options 51–52
 - changes from 8.1 to 8.5 52
 - dbclient section 52
 - db-request-timeout 51
 - default section 51–52
 - mandatory options 51
 - setting 51
 - utf8-ucs2 52
 - db_binding
 - Message Server option 102
 - db_storage
 - Message Server option 102
 - dbclient section
 - Database Access Point 52

dbengine
 Configuration Server option 69, 79
db-filter section
 Message Server 104–105
dbname
 Configuration Server option 69
db-request-timeout
 Database Access Point option 51
dbserver
 Configuration Server option 69
dbserver section
 common options 40–70
dbthread
 Configuration Server option 57, 78, 103
 Message Server option 106
debug
 common log option 24
 Configuration Server option 80
 Configuration Server Proxy option 91
decryption-key
 Configuration Server option 58, 78
default section
 Database Access Point 51–52
default-filter-type
 common log option 31
disable_switchover
 Solution Control Server option 109, 114
disable-vag-calculation
 Configuration Server option 58
disconnect-switchover-timeout
 Solution Control Server option 109
distributed_mode
 Solution Control Server option 109
distributed_rights
 Solution Control Server option 109
distributed_sync_timeout
 Solution Control Server option 110, 114
dml_retry
 common configuration option 49, 79
dml-retry
 Configuration Server option 69
document
 audience 8
 conventions 145
 errors, commenting on 8
 version numbering 145

E

enable-async-dns
 common configuration option 41
enable-ipv6
 common configuration option 41
enable-pre-812-security
 Configuration Server option 59

enable-thread
 common log option 15, 48
encoding
 Configuration Server option 59, 85
encryption
 Configuration Server option 60, 78
eventloghost
 Solution Control Server option 113
expiration
 Configuration Server option 74
 Configuration Server Proxy option 90
expire
 common log option 15

F

failsafe-store-processing
 Configuration Server Proxy option 90
filtering
 common log option 32
fix_cs_version_7x
 Configuration Server option 60
force-md5
 Configuration Server option 61
force-offline
 Configuration Server option 71, 78
force-password-reset
 configuration option 38
 Tenant option 135
force-reconnect-reload
 Configuration Server option 71, 79, 81

G

gda-tls
 Host option 127
general section
 LCA 94
 Solution Control Server 108–111
Genesys Deployment Agent
 sample configuration file 99
Genesys Deployment Agent options 98–99
 changes from 8.1 to 8.5 100
 log section 98
 mandatory options 97
 rootdir 98
 security section 98–99
 setting 97
 web section 98
Genesys SNMP Master Agent
 See SNMP Master Agent

H

ha_service_unavail_primary	
Solution Control Server option	110
hangup-restart	
common configuration option	39
hca section	
Configuration Server	80
heartbeat-period	
common configuration option	39
heartbeat-period-thread-class-<n>	
common configuration option	40
history-log section	
Configuration Server	74–75
Configuration Server Proxy	88–89
history-log-guid	
Configuration Server option	80
history-log-minid	
Configuration Server option	80
history-log-version	
Configuration Server option	80
host	
Configuration Server option	80
host configuration options	
sec-protocol	127, 129
Host options	124–129
addp section	124
addp-remote-timeout	124
addp-timeout	124
changes from 8.1 to 8.5	129
cipher-list	129
client-auth	126
gda-tls	127
ip-version	129
lca-upgrade	127, 129
mandatory options	123
ntp-service-control section	124–125
port	125
rdm section	125
security section	125–129
setting	123
signature	125
upgrade	130

I

interaction	
common log option	23
ip-version	
common configuration option	47, 49, 127
Host option	129

K

keep-startup-file	
common log option	15

L

langid	
Configuration Server option	62, 79
last-expired-at	
User option	141
last-locked-at	
User option	141
last-login	
configuration option	62, 85
Configuration Server option	62
Configuration Server Proxy option	85
last-login-synchronization	
Configuration Server option	62, 86
LCA	
configuring ADDP with SCS	96, 114, 124
sample configuration file	96
LCA options	94–96
changes from 8.1 to 8.5	96
general section	94
log section	94
lookup_clienthost	94
mandatory options	93
security section	94–95
setting	93
upgrade	94, 96
wmiquery-timeout	94, 96
lca-upgrade	
Host option	127, 129
level-reassign-<eventID>	
common log option	28
level-reassign-disable	
common log option	28
license	
Configuration Server option	71, 79
License section	
Solution Control Server	108
license section	
Configuration Server Proxy	84
Local Control Agent	
See LCA	
locale	
Configuration Server option	63
Configuration Server Proxy option	86
log configuration options	14–21
log section	
common log options	14–28
Configuration Server	72–73
Genesys Deployment Agent	98
LCA	94

- Message Server 105
- Solution Control Server 112–113
- log-extended section
 - common log options 28–30
- log-filter section
 - common log options 31–32
- log-filter-data section
 - common log options 33–34
- log-queue-exp-time
 - Message Server option 103
- log-queue-response
 - Message Server option 103
- log-queue-size
 - Message Server option 103
- lookup_clienthost
 - LCA option 94
 - Solution Control Server option 110

M

- mailer section
 - Solution Control Server 111–112
- management-port
 - Configuration Server option 63
- max_switchover_time
 - Solution Control Server option 114
- max-client-output-queue-size
 - Configuration Server option 63, 79
 - Configuration Server Proxy option 86, 90
- max-output-queue-size
 - Configuration Server option 64, 79
 - Configuration Server Proxy option 87, 90
- max-records
 - Configuration Server option 75
 - Configuration Server Proxy option 90
- max-req-per-loop
 - Solution Control Server option 111
- memory
 - common log option 16
- memory-storage-size
 - common log option 16
- Message Server
 - sample configuration file 105
- Message Server options 102–105
 - block-messages 104
 - block-messages-by-<type> 104
 - block-messages-from-<DBID> 104
 - changes from 8.1 to 8.5 105
 - db_binding 102
 - db_storage 102
 - db-filter section 104–105
 - dbthread 106
 - log section 105
 - log-queue-exp-time 103
 - log-queue-response 103
 - log-queue-size 103

- mandatory options 101
- messages section 102–104
- MessageServer section 102
 - setting 101
 - signature 102
 - thread-mode 106
 - thread-pool-size 106
 - x-dblib-debug 106
- message_format
 - common log option 16, 48
- messagefile
 - common log option 17
- message-format
 - common log option 48
- messages section
 - Message Server 102–104
- MessageServer section
 - Message Server 102
- mode
 - SNMP Master Agent option 116
- multi-languages
 - Configuration Server option 64

N

- no-change-password-at-first-login
 - configuration option 38, 135
- no-default-access
 - Configuration Server option 73
- no-memory-mapping 48
 - common log option 17
- ntp-service-control section
 - Host 124–125

O

- objects-cache
 - Configuration Server option 64
 - Configuration Server Proxy option 87
- override-account-expiration
 - User option 141
- override-password-expiration
 - User option 141

P

- packet-size
 - Configuration Server option 65, 79
 - Configuration Server Proxy option 87, 90
- password
 - Configuration Server option 70
 - SNMP Master Agent option 120
- password-change
 - Configuration Server option 65

password-expiration
 configuration option 136
 Tenant option 136, 142
password-expiration-notify
 Tenant option 136
password-min-length
 configuration option 56, 136
 Tenant option 136
password-no-repeats
 Tenant option 137
password-req-alpha
 Tenant option 137
password-req-mixed-case
 Tenant option 138
password-req-number
 Tenant option 138
password-req-punctuation
 Tenant option 139
peer-switchover-tmout
 Configuration Server option 65, 79
port
 common configuration option 42
 Configuration Server option 66, 80
 Configuration Server Proxy option 91
 Host option 125
postgre-standard-conforming-strings
 Configuration Server option 71, 81
prevent-mediatype-attr-removal
 Configuration Server option 72, 81
primary-startup-tmout
 Configuration Server option 66, 79
print-attributes
 common log option 18
protocol
 Configuration Server option 67
proxy-cluster-name
 Configuration Server Proxy option 88, 90
proxy-writable
 Configuration Server Proxy option 88

R

rdm section
 Host 125
read_community
 SNMP Master Agent option 117
rebind-delay
 common configuration option 41
reconnect-timeout
 Configuration Server option 80
redundant Configuration Servers
 configuring ADDP 67
response-timeout
 Configuration Server option 70
rootdir
 Genesys Deployment Agent option 98

runtime options
 Configuration Server 70–75

S

schema
 Configuration Server option 80
sec-protocol
 common configuration option 35, 45, 48, 49
 host configuration option 127, 129
security section
 common configuration options 34–37
 Configuration Server 73–74
 Genesys Deployment Agent 98–99
 Host 125–129
 LCA 94–95
security-authentication-rules section
 common configuration options 38
 Tenant/User 132, 133–142
segment
 common log option 18, 48
server
 Configuration Server option 66, 67, 68, 80
service-unavailable-timeout
 Solution Control Server option 111
setting configuration options
 common 13
 Configuration Server 53
 Configuration Server Proxy 83
 Database Access Point 51
 Genesys Deployment Agent 97
 Host 123
 LCA 93
 Message Server 101
 SNMP Master Agent 115
 Solution Control Server 107
 Tenant 131
 User 132
signature
 Host option 125
 Message Server option 102
skip-environment-enum-transfer
 Configuration Server option 72, 81
sml section
 common options 38–40
smtp_from
 Solution Control Server option 111
smtp_host
 Solution Control Server option 111
smtp_port
 Solution Control Server option 112
snapshot
 common log option 18, 48
SNMP Master Agent options 116–121
 agentx section 116–117
 changes from 8.1 to 8.5 121

- mandatory options 116
- mode 116
- password 120
- read_community 117
- setting 115
- snmp section 117–120
- snmp-v3-auth section 120
- snmp-v3-priv section 120–121
- tcp_port 116
- trap_target 118
- v3_username 118
- v3auth_password 118
- v3auth_protocol 119
- v3priv_password 119
- v3priv_protocol 119
- write_community 119
- snmp section
 - SNMP Master Agent 117–120
- SNMPv3 options
 - password 120
- snmp-v3-auth section
 - SNMP Master Agent 120
- snmp-v3-priv section
 - SNMP Master Agent 120–121
- soap
 - Configuration Server Proxy section 90
 - Configuration Server section 80
- Solution Control Server
 - configuring ADDP with LCA 96, 114
- Solution Control Server options 108–114
 - alarm 112
 - alarms-port 113
 - alive_timeout 108
 - backup-alarms-port 114
 - changes from 8.1 to 8.5 114
 - disable_switchover 109, 114
 - disconnect-switchover-timeout 109
 - distributed_mode 109
 - distributed_rights 109
 - distributed_sync_timeout 110, 114
 - eventloghost 113
 - general section 108–111
 - ha_service_unavail_primary 110
 - log section 112–113
 - lookup_clienthost 110
 - mailer section 111–112
 - mandatory options 108
 - max_switchover_time 114
 - max-req-per-loop 111
 - service-unavailable-timeout 111
 - setting 107
 - smtp_from 111
 - smtp_host 111
 - smtp_port 112
 - transport 113
 - Transport Parameter options 113–114

- spool
 - common log option 19
- standard
 - common log option 22
- suspending-wait-timeout
 - common configuration option 40
- system
 - Configuration Server section 81
- system section
 - Configuration Server 71–72

T

- tcp_port
 - SNMP Master Agent option 116
- Tenant options 133–140
 - account-expiration 133
 - account-lockout-attempts-period 134
 - account-lockout-duration 134
 - account-lockout-threshold 135
 - force-password-reset 135
 - password-expiration 136, 142
 - password-expiration-notify 136
 - password-min-length 136
 - password-no-repeats 137
 - password-req-alpha 137
 - password-req-mixed-case 138
 - password-req-number 138
 - password-req-punctuation 139
 - security-authentication-rules section 133–140
 - setting 131
 - tenant-override-section 132, 139
- Tenant/User options 133–142
 - changes from 8.1 to 8.5 142
 - mandatory options 132
 - security-authentication-rules section 132, 133–142
 - Tenant options 133–140
 - User options 140–142
- tenant-override-section
 - Tenant option 132, 139
- thread-mode
 - Message Server option 106
- thread-pool-size
 - Message Server option 106
- throttle-period
 - common configuration option 48
 - common log option 19
- throttle-threshold
 - common configuration option 48
- time_convert
 - common log option 20
- time_format
 - common log option 20
- tls
 - common configuration option 46

- Configuration Server option 76
- tls-mutual
 - common configuration option 37, 49
- tls-target-name-check
 - common configuration option 37
- trace
 - common log option 23
- transport
 - common configuration option 42
 - Configuration Server option 76
 - Solution Control Server option 113
- Transport Parameter options
 - address 42
 - alarms-port 113
 - backup-alarms-port 114
 - backup-port 42
 - cipher-list 34, 43, 126
 - client-auth 35
 - common configuration options 41–47
 - Configuration Server 76–77
 - crl 44
 - ip-version 47, 127
 - port 42
 - sec-protocol 35
 - Solution Control Server 113–114
 - tls 46, 76
 - transport 42, 76, 113
- trap_target
 - SNMP Master Agent option 118

U

- upgrade
 - Host option 130
 - LCA option 94, 96
- upgrade-mode
 - Configuration Server option 79
- user
 - Configuration Server option 76, 81
 - Configuration Server Proxy option 89, 91
- User options 140–142
 - account-override-lockout 140, 142
 - last-expired-at 141
 - last-locked-at 141
 - override-account-expiration 141
 - override-password-expiration 141
 - security-authentication-rules section 140–142
 - setting 132
- username
 - Configuration Server option 70
- utf8-ucs2
 - Database Access Point option 52

V

- v3_username
 - SNMP Master Agent option 118
- v3auth_password
 - SNMP Master Agent option 118
- v3auth_protocol
 - SNMP Master Agent option 119
- v3priv_password
 - SNMP Master Agent option 119
- v3priv_protocol
 - SNMP Master Agent option 119
- verbose
 - common log option 20

W

- web section
 - Genesys Deployment Agent 98
- wmquery-timeout
 - LCA option 94, 96
- write_community
 - SNMP Master Agent option 119
- write-former-value
 - Configuration Server option 75, 81

X

- x-conn-debug-all
 - common log option 26
- x-conn-debug-api
 - common log option 26
- x-conn-debug-dns
 - common log option 27
- x-conn-debug-open
 - common log option 27
- x-conn-debug-security
 - common log option 27
- x-conn-debug-select
 - common log option 27
- x-conn-debug-timers
 - common log option 28
- x-conn-debug-write
 - common log option 28
- x-dblib-debug
 - common configuration option 72, 105
 - Message Server option 106
- x-dblib-sql
 - Configuration Server option 73, 80