Framework 8.1

# Configuration Options

# Reference Manual

### 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.genesyslab.com for more information.

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

### Notice

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

### Your Responsibility for Your System's Security

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

### Trademarks



### Technical Support from VARs

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

### Technical Support from Genesys

If you have purchased support directly from Genesys, please contact Genesys Technical Support. Before contacting technical support, please refer to the ***Genesys Care Program Guide*** 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.genesyslab.com

**Document Version:** 81fr_ref-co_06-2013_v8.1.301.00

# Table of Contents

# Preface

Welcome to the *Framework 8.1 Configuration Options Reference Manual.* This document describes the configuration options for the Genesys Framework 8.1 components, which you must configure in the Configuration Layer. This document is designed to be used along with the *Framework 8.1 Deployment Guide.*

This document is valid only for the 8.1 release(s) of the Genesys Framework.

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

This preface contains the following sections:



For information about related resources and about the conventions that are used in this document, see the supplementary material starting on page 151.

## About Configuration Options

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

The options in the current document are divided by sections, as they are in a component configuration. Section names are set by default; changing them is

not recommended. For applications that are configured via configuration files, the section name is put in square brackets—for example, `[dbserver]`.

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

# Intended Audience

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

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

You should also be familiar with:

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

# Making Comments on This Document

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

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

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

# Contacting Genesys Technical Support

If you have purchased support directly from Genesys, please contact Genesys Technical Support.

Before contacting technical support, please refer to the *Genesys Care Program Guide* for complete contact information and procedures.

# Changes in This Document

## Version 8.1.301.00

This document has been updated for new changed functionality in the 8.1.3 release. Changes for each component are summarized in the "Changes from 8.0 to 8.1 section at the end of each chapter.

In addition:

- Transport Parameter options have been moved to a new section called Transport Parameter Options in the chapters in which they occur.

## Version 8.1.201.00

This document has been updated for new and changed functionality in the 8.1.2 release. Changes for each component are summarized in the "Changes from 8.0 to 8.1 section at the end of each chapter.

In addition:

- Full details of all security-related options are now contained in this guide. These options were previously described in full in the *Genesys Security Deployment Guide.*
- Chapter 14, "Tenant and User Configuration Options," on page 137 has been renamed from "Tenant Configuration Options" to reflect that it also contains configuration options that are set in `User` objects. These options either override or report the results of the actions that result from the application of the Tenant-level options, which are also described in this chapter.

## Version 8.1.101.00

This document has been updated for new and changed functionality in the 8.1.0 and 8.1.1 releases. Changes for each component are summarized in the "Changes from 8.0 to 8.1" sections at the end of each chapter.

In addition:

- The chapter "Genesys Administrator Configuration Options" has been moved to the *Framework Genesys Administrator Deployment Guide*.
- Chapter 12, "Genesys Deployment Agent Configuration Options," on page 127 has been added.

Genesys

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:



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

## Setting Configuration Options

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

- In Genesys Administrator—`Application` object > `Options` tab > `Advanced View (Options)`

- In Configuration Manager—`Application` object > `Properties` dialog box > `Options` tab

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

# Mandatory Options

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

# 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:

| | |
|---|---|
| `true` | Enables buffering. |
| `false` | Disables buffering. |

Changes Take Effect: Immediately

Turns on/off operating system file buffering. The option is applicable only to the `stderr` and `stdout` output (see page 20). 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.

### compatible-output-priority

Default Value: `false`
Valid Values:

| | |
|---|---|
| `true` | The log of the level specified by "Log Output Options" is sent to the specified output. |
| `false` | The log of the level specified by "Log Output Options" and higher levels is sent to the specified output. |

Changes Take Effect: Immediately

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

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

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

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

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

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

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

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

### expire

Default Value: `false`
Valid Values:

| | |
|---|---|
| `false` | No expiration; all generated segments are stored. |
| `<number> file` or `<number>` | Sets the maximum number of log files to store. Specify a number from `1`–`1000`. |
| `<number> day` | Sets the maximum number of days before log files are deleted. Specify a number from `1`–`100`. |

Changes Take Effect: Immediately

Determines whether log files expire. If they do, sets the measurement for determining when they expire, along with the maximum number of files (segments) or days before the files are removed. This option is ignored if log output is not configured to be sent to a log file.

**Note:** If an option's value is set incorrectly—out of the range of valid values— it will be automatically reset to `10`.

### keep-startup-file

Default Value: `false`
Valid Values:

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

Changes Take Effect: After restart

Specifies whether a startup segment of the log, containing the initial 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 20). The new snapshot overwrites the previously written data. If the application terminates abnormally, this file will contain the latest log messages. Memory output is not recommended for processors with a CPU frequency lower than 600 MHz.

**Note:** If the file specified as the `memory` file is located on a network drive, an application does not create a snapshot file (with the extension `*.memory.log`). Log 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 20.

### 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: `<string>.lms` (message file name)

Changes Take Effect: Immediately, if an application cannot find its `*.lms` file at startup

Specifies the file name for application-specific log events. The name must be valid for the operating system on which the application is running. The option value can also contain the absolute path to the application-specific `*.lms` file. Otherwise, an application looks for the file in its working directory.

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

### print-attributes

Default Value: `false`
Valid Values:

| | |
|---|---|
| `true` | Attaches extended attributes, if any exist, to a log event sent to log output. |
| `false` | Does not attach extended attributes to a log event sent to log output. |

Changes Take Effect: Immediately

Specifies whether the application attaches extended attributes, if any exist, to a log event that it sends to log output. Typically, log events of the Interaction log level and Audit-related log events contain extended attributes. Setting this option to `true` enables audit capabilities, but negatively affects performance. Genesys recommends enabling this option for Solution Control Server and Configuration Server when using audit tracking. For other applications, refer to *Genesys 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.

### segment

Default Value: `false`
Valid Values:

| | |
|---|---|
| `false` | No segmentation is allowed. |
| `<number> KB` or `<number>` | Sets the maximum segment size, in kilobytes. The minimum segment size is `100 KB`. |
| `<number> MB` | Sets the maximum segment size, in megabytes. |
| `<number> hr` | Sets the number of hours for the segment to stay open. The minimum number is `1` hour. |

Changes Take Effect: Immediately

Specifies whether there is a segmentation limit for a log file. If there is, sets the mode of measurement, along with the maximum size. If the current log segment exceeds the size set by this option, the file is closed and a new one is created. This option is ignored if log output is not configured to be sent to a log file.

### spool

Default Value: The application's working directory
Valid Values: `<path>` (the folder, with the full path to it)

Changes Take Effect: Immediately

Specifies the folder, including full path to it, in which an application creates temporary files related to network log output. If you change the option value while the application is running, the change does not affect the currently open network output.

### time_convert

Default Value: `Local`

Valid Values:

| | |
|---|---|
| `local` | The time of log record generation is expressed as a local time, based on the time zone and any seasonal adjustments. Time zone information of the application's host computer is used. |
| `utc` | The time of log record generation is expressed as Coordinated Universal Time (UTC). |

Changes Take Effect: Immediately

Specifies the system in which an application calculates the log record time when generating a log file. The time is converted from the time in seconds since the Epoch (00:00:00 UTC, January 1, 1970).

### time_format

Default Value: `time`

Valid Values:

| | |
|---|---|
| `time` | The time string is formatted according to the `HH:MM:SS.sss` (hours, minutes, seconds, and milliseconds) format. |
| `locale` | The time string is formatted according to the system's locale. |
| `ISO8601` | The date in the time string is formatted according to the ISO 8601 format. Fractional seconds are given in milliseconds. |

Changes Take Effect: Immediately

Specifies how to represent, in a log file, the time when an application generates log records.

A log record's time field in the ISO 8601 format looks like this:

```
2001-07-24T04:58:10.123
```

### verbose

Default Value: `all`

Valid Values:

| | |
|---|---|
| `all` | All log events (that is, log events of the Standard, Trace, Interaction, and Debug levels) are generated. |
| `debug` | The same as `all`. |
| `trace` | Log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels) are generated, but log events of the Debug level are not generated. |

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

Changes Take Effect: Immediately

Determines whether a log output is created. If it is, specifies the minimum level of log events generated. The log events levels, starting with the highest priority level, are Standard, Interaction, Trace, and Debug. See also "Log Output Options" on page 20.

**Note:** For definitions of the Standard, Interaction, Trace, and Debug log levels, refer to the *Framework Management Layer User's Guide*, *Framework Genesys Administrator Help,* or to *Framework Solution Control Interface 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 24.

**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.<br>Setting the `all` log level option to the `network` output enables an application to send log events of the `Standard`, `Interaction`, and `Trace` levels to Message Server. `Debug`-level log events are neither sent to Message Server nor stored in the Log Database. |
| `memory` | Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance. |
| `[filename]` | Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory. |

Changes Take Effect: Immediately

Specifies the outputs to which an application sends all log events. The log output types must be separated by a comma when more than one output is configured. For example:

```
all = stdout, logfile
```

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

### alarm

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

| | |
|---|---|
| `stdout` | Log events are sent to the Standard output (`stdout`). |
| `stderr` | Log events are sent to the Standard error output (`stderr`). |
| `network` | Log events are sent to Message Server, which resides anywhere on the network, and Message Server stores the log events in the Log Database. |
| `memory` | Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance. |
| `[filename]` | Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory. |

Changes Take Effect: Immediately

Specifies the outputs to which an application sends the log events of the Alarm level. The log output types must be separated by a comma when more than one output is configured. For example:

```
alarm = stderr, network
```

### standard

Default Value: No default value

Valid Values (log output types):

| | |
|---|---|
| `stdout` | Log events are sent to the Standard output (`stdout`). |
| `stderr` | Log events are sent to the Standard error output (`stderr`). |
| `network` | Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. |
| `memory` | Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance. |
| `[filename]` | Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory. |

Changes Take Effect: Immediately

Specifies the outputs to which an application sends the log events of the `Standard` level. The log output types must be separated by a comma when more than one output is configured. For example:

```
standard = stderr, network
```

### interaction

Default Value: No default value

Valid Values (log output types):

| | |
|---|---|
| `stdout` | Log events are sent to the Standard output (`stdout`). |
| `stderr` | Log events are sent to the Standard error output (`stderr`). |
| `network` | Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. |
| `memory` | Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance. |
| `[filename]` | Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory. |

Changes Take Effect: Immediately

Specifies the outputs to which an application sends the log events of the `Interaction` level and higher (that is, log events of the `Standard` and `Interaction` levels). The log outputs must be separated by a comma when more than one output is configured. For example:

```
interaction = stderr, network
```

### trace

Default Value: No default value

Valid Values (log output types):

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

| | |
|---|---|
| network | Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. |
| memory | Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance. |
| [filename] | Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory. |

Changes Take Effect: Immediately

Specifies the outputs to which an application sends the log events of the Trace level and higher (that is, log events of the Standard, Interaction, and Trace levels). The log outputs must be separated by a comma when more than one output is configured. For example:

```
trace = stderr, network
```

### debug

Default Value: No default value

Valid Values (log output types):

| | |
|---|---|
| stdout | Log events are sent to the Standard output (stdout). |
| stderr | Log events are sent to the Standard error output (stderr). |
| memory | Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance. |
| [filename] | Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory. |

Changes Take Effect: Immediately

Specifies the outputs to which an application sends the log events of the Debug level and higher (that is, log events of the Standard, Interaction, Trace, and Debug levels). The log output types must be separated by a comma when more than one output is configured—for example:

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

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

## Log File Extensions

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

- *.log—Assigned to log files when you configure output to a log file. For example, if you set standard = confservlog for Configuration Server, it prints log messages into a text file called confservlog.<time_stamp>.log.
- *.qsp—Assigned to temporary (spool) files when you configure output to the network but the network is temporarily unavailable. For example, if

you set `standard = network` for Configuration Server, it prints log messages into a file called `confserv.<time_stamp>.qsp` during the time the network is not available.

- `*.snapshot.log`—Assigned to files that contain the output snapshot when you configure output to a log file. The file contains the last log messages that an application generates before it terminates abnormally. For example, if you set `standard = confservlog` for Configuration Server, it prints the last log message into a file called `confserv.<time_stamp>.snapshot.log` in case of failure.

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

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

# Examples

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

## Production Mode Log Section

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

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

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

## Lab Mode Log Section

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

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

### Failure-Troubleshooting Log Section

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

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

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

## Debug Log Options

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

### x-conn-debug-all

Default Value: `0`

Valid Values:

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

Changes Take Effect: After restart

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

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

### x-conn-debug-api

Default Value: `0`
Valid Values:

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

Changes Take Effect: After restart

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

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

### x-conn-debug-dns

Default Value: `0`
Valid Values:

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

Changes Take Effect: After restart

Generates `Debug` log records about DNS operations.

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

### x-conn-debug-open

Default Value: `0`
Valid Values:

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

Changes Take Effect: After restart

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

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

### x-conn-debug-security

Default Value: `0`
Valid Values:

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

Changes Take Effect: After restart

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

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

### x-conn-debug-select

Default Value: `0`
Valid Values:

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

Changes Take Effect: After restart

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

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

### x-conn-debug-timers

Default Value: `0`
Valid Values:

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

Changes Take Effect: After restart

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

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

### x-conn-debug-write

Default Value: `0`
Valid Values:

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

Changes Take Effect: After restart

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

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

## 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.

## 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 `AttributeUserData` section of the log.

This section must be called `log-filter`.

#### default-filter-type

Default Value: `copy`
Valid Values: One of the following:

| | |
|---|---|
| `copy` | The keys and values of the KVList pairs in the `AttributeUserData` section are copied to the log. |
| `hide` | The keys of the KVList pairs in the `AttributeUserData` section are copied to the log; the values are replaced with asterisks. |
| `hide-first,<n>` | The keys of the KVList pairs in the `AttributeUserData` section 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. |
| `hide-last,<n>` | The keys of the KVList pairs in the `AttributeUserData` section 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. |
| `skip` | The KVList pairs in the `AttributeUserData` section are not copied to the log. |

`tag[(<tag-prefix>, <tag-postfix>)]` The KVList pairs in the `AttributeUserData` section 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 is 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 `AttributeUserData` section 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 `AttributeUserData` section 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 `UserData`, `Extensions`, and `Reasons`) in the log. This setting will be applied to the attributes of all KVList pairs in the `AttributeUserData` section 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 `AttributeUserData` section 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:

| | |
|---|---|
| `copy` | The key and value of the given KVList pair in the `AttributeUserData` section is copied to the log. |
| `hide` | The key of the given KVList pair in the `AttributeUserData` section is copied to the log; the value is replaced with a string of asterisks. |
| `hide-first,<n>` | The key of the given KVList pair in the `AttributeUserData` section 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. |
| `hide-last,<n>` | The key of the given KVList pair in the `AttributeUserData` section 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. |
| `skip` | The KVList pair in the `AttributeUserData` section is not copied to the log. |
| `tag[(<tag-prefix>,<tag-postfix>)]` | The KVList pair in the `AttributeUserData` section 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.<br><br>To use the default tags, you can use any of the following values:<br>· `tag`<br>· `tag()`<br>· `tag(,)`<br><br>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 AttributeUserData section 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 AttributeUserData section 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`.

### 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 41.
- If the security certificate is configured at the host level, see page 134.

**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.

#### 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`, such 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:

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

**Warning!** Use the first three options in this section (`hangup-restart`, `heartbeat-period`, and`heartbeat-period-thread-class-<n>`) 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.

### 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) or any DB Server. These components by definition do not support graceful shutdown, so this option is not required.

# dbserver Section

In addition to options specific to an application that may exist in this section, this section also contains an option to support Oracle 11g RAC in TAF mode. When this option is set, Configuration Server can resubmit DML statements (DML transactions or binding package execution) when the appropriate error messages are received from the DBMS. For more information, refer to the *Framework Deployment Guide*.

This section must be called `dbserver`.

### 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 overloading Configuration Server and the DBMS.

# 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 Technical Support.
- 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 Technical Support.

# 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` **Option**

In a configuration file, 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 or Configuration Manager, 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 one of the following navigation paths:

- In Genesys Administrator—`Application` object > `Configuration` tab > General section > Connections > `<Connection>` > `Connection Info` > `Advanced` tab > `Transport Parameters`
- In Configuration Manager—`Application` object > `Properties` dialog box > `Connections` tab > `Connection Properties` dialog box > `Advanced` tab > `Transport Protocol 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.

Unless otherwise stated, set options in this section in the `Transport Parameters` of the port's properties, using one of the following navigation paths:

- In Genesys Administrator—`Application` object > `Configuration` tab > `General` section > `Connections > Connection Info` > `Advanced` tab > `Transport Parameters`
- In Configuration Manager—`Application` object > `Properties` dialog box > `Connection` tab > `Connection Properties` dialog box > `Advanced` tab > `Transport Protocol Parameters`

### 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.

### 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 33.
- If the security certificate is configured at the host level, see page 134.

**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.

### tls

Default Value: tls=0
Valid Values:

| | |
|---|---|
| tls=0 | Regular (unsecured) connections will be used. |
| For Windows:<br>tls=1;certificate=<value> | Secure connections will be used, where 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.

# Changes from 8.0 to 8.1

Table 1 on page 42 lists all changes to common configuration options between release 8.0 and the latest 8.1 release.

**Table 1: Common Configuration Option Changes from 8.0 to 8.1**

| Option Name | Option Values | Type of Change | Details |
|---|---|---|---|
| **common Section** | | | |
| enable-async-dns | `0`, `1` | Changed values | Values `off` and `on` replaced with `0` and `1`, respectively. |
| enable-ipv6 | `0`, `1` | New | See description on page 38. |
| **dbserver Section** | | | |
| dml-retry | `0` to `32766` | New | See description on page 37. |

**Table 1: Common Configuration Option Changes from 8.0 to 8.1 (Continued)**

| Option Name | Option Values | Type of Change | Details |
|---|---|---|---|
| **log-filter Section** | | | |
| default-filter-type | `copy`; `hide`; `hide-first, <n>`; `hide-last, <n>`; `skip`; `unhide-first, <n>`; `unhide-last, <n>`; `tag(tag-prefix, tag-postfix)` | Added two valid values in 8.1 | See description on page 30. |
| | `copy`; `hide`; `hide-first, <n>`; `hide-last, <n>`; `skip`; `unhide-first, <n>`; `unhide-last, <n>` | New in 8.0 | See description on page 30<br>Not previously documented. |
| filtering | `true`, `false` | New | See description on page 31. |
| **security Section** | | | |
| client-auth | `1, 0` | New | See description on page 33. |
| tls-target-name-check | `no`, `host` | New | See description on page 34. |
| **security-authentication-rules Section (new)** | | | |
| no-change-password-at-first-login | `true`, `false` | New | See description on page 34. |
| **sml Section** | | | |
| heartbeat-period | `<min value>` to `604800` | Changed minimum value | See description on page 35. |
| **Transport Parameters** | | | |
| cipher-list | `List of ciphers` | New | See description on page 40. |
| client-auth | `1, 0` | New | See description on page 41. |
| crl | `Valid file name` | New | See description on page 41. |
| address | <valid IP address> | New in 7.6 | Not documented in 7.6.<br>See description on page 39. |
| backup-port | <any port number> | New in 7.6 | Not documented in 7.6.<br>See description on page 40. |

**Table 1: Common Configuration Option Changes from 8.0 to 8.1 (Continued)**

| Option Name | Option Values | Type of Change | Details |
|---|---|---|---|
| port | <any port number> | New in 7.6 | Not documented in 7.6.<br>See description on page 39. |

Genesys

Chapter

# 2 DB Server Configuration Options

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

This chapter contains the following sections:



DB Server also supports the options described in Chapter 1 on page 13.

## Setting Configuration Options

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

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

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

# Mandatory Options

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

**Table 2: Mandatory Options**

| Option Name | Default Value | Details |
|---|---|---|
| **DB Server Section** | | |
| host | No default value | Not used when configuring a DB Server Application object in the Configuration Database. A value for this option must be specified when configuring DB Server via a configuration file.<br>See the description on page 49. |
| port | No default value | Not used when configuring a DB Server Application object in the Configuration Database. A value for this option must be specified when configuring DB Server via a configuration file.<br>See the description on page 50. |
| dbprocess_name | No default value | See the description on page 48. |
| [a DB client process name option] | No default value | The option name depends on the DBMS type: `db2_name`, `informix_name`, `msql_name`, `oracle_name`, `postgre_name`, or `sybase_name`.<br>See the descriptions beginning on page 47. |

# dbserver Section

This section must be called `dbserver`.

Starting with release 7.5, DB Server can communicate with its clients via multiple ports. One port must always be specified in the main DB Server

section `dbserver`. To configure additional ports, use sections `dbserver-n` as described in "Multiple Ports Configuration" on page 52.

### client_stop_timeout

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

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

### connect_break_time

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

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

### db-request-timeout

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

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

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

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

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

### db2_name

Default Value: `./dbclient_db2`
Valid Values:

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

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

Changes Take Effect: After restart

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

### dbprocess_name

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

| | |
|---|---|
| `./dbclient_db2` | For DB2 |
| `./dbclient_informix` | For Informix |
| `./dbclient_msql` | For Microsoft SQL |
| `./dbclient_oracle` | For Oracle |
| `./dbclient_postgre` | For PostgreSQL |
| `./dbclient_sybase` | For Sybase |

Changes Take Effect: After restart

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

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

### dbprocess_number

Default Value: `255`
Valid Values:

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

Changes Take Effect: After restart

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

### dbprocesses_per_client

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

Specifies the number of database client processes that DB Server's main process creates for each client if a user client does not make an explicit request. This option prioritizes client access to the database. For example, if multiple

processes per client are set, DB Server spawns another child process if needed. This effectively gives the client application more of the database's processing time. See documentation for a particular client application to verify whether that application supports the Multiple Processes mode. If unsure of the appropriate number, set this option to `1`. Increasing the value up to `4` increases performance; more than `4` does not increase performance.

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

### host

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

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

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

### informix_name

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

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

### management-port

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

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

### msql_name

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

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

### oracle_name

Default Value: `./dbclient_oracle`
Valid Values:

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

Changes Take Effect: After restart

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

### port

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

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

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

### postgre_name

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

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

### stored_proc_result_table

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

Used by earlier versions of DB Server that did not directly retrieve output data from stored procedures. This option specifies the name of a table that you design, to which a stored procedure that you have created writes output data (the maximum allowed size of an output parameter from a stored procedure is 2000 B). DB Server then retrieves the data stored in the specified table and

sends it to the user application. Using a result table can slow down DB Server, because each stored procedure call causes an additional select statement.

### sybase_name

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

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

### tran_batch_mode

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

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

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

### verbose

Default Value: `3`
Valid Values:

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

Changes Take Effect: After restart

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

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

# lca Section

This section must be called `lca`.

### lcaport

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

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

# Multiple Ports Configuration

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

Each `dbserver-`*`n`* section contains the configuration options for a single additional port. The number of `dbserver-`*`n`* sections corresponds to the number of additional ports. The order in which these sections appear in the configuration file is non-essential. To configure a secure connection, specify the certificate settings in the `transport` option in the section for that port. See “Sample Configuration File” on page 54. Refer to the “TLS Configuration” section in the *Genesys Security Deployment Guide* for detailed information about the `transport` option.

### port

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

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

# Transport Parameter Options

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

- In Genesys Administrator—DB Server Application object > Configuration tab > General section > Connections > Connection Info > Advanced tab > Transport Parameters
- In Configuration Manager—DB Server Application object > Properties dialog box > Connections tab > Connection Properties dialog box > Advanced tab > Transport Protocol Parameters

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

**transport Option**

In a configuration file (see the example on page 54), 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 or Configuration Manager, 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-colin) and "=".

### tls

Default Value: tls=0
Valid Values:

| | |
|---|---|
| tls=0 | Regular (unsecured) connections will be used. |
| For Windows:<br>tls=1;certificate=<value> | Secure connections will be used, where certificate = certificate value. |
| For UNIX:<br>tls=1;certificate=<path>;[certificate-key=<path>];trusted-ca=<path> | Secure connections will be used, where:<br>• certificate—full path to the <serial_#>_<host_name>_cert.pem file<br>• certificate-key—full path to the <serial_#>_<host_name>_priv_key.pem file (unless the private key is stored together with a certificate)<br>• trusted-ca—full path to the ca_cert.pem file |

You specify the transport option in any section of the DB Server configuration file that contains port configuration, and in the Configuration Database section of the Configuration Server configuration file. 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.

# DB Server Configuration File

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

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

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

The default name of the DB Server section is `dbserver`. This section contains configuration information about DB Server: DB Server settings and the type of the DBMS with which DB Server operates. The `dbserver` section allows you to configure one listening port. Starting from release 7.5, you can configure multiple listening ports for DB Server, where each additional port is configured in a separate `dbserver-`*n* section. See "Multiple Ports Configuration" on page 52 for details.

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

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

## Sample Configuration File

The following is a sample configuration file for DB Server.

```
[dbserver]
host = localhost
port = 4040
management-port = 4581
dbprocesses_per_client = 1
dbprocess_name = ./dbclient_sybase
oracle_name = ./dbclient_oracle
informix_name = ./dbclient_informix
sybase_name = ./dbclient_sybase
db2_name = ./dbclient_db2
```

```
postgre_name = ./dbclient_postgre
connect_break_time = 1200
tran_batch_mode = off

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

[log]
verbose = standard
all = stderr

[lca]
lcaport = 4999
```

# Changes from 8.0 to 8.1

Table 3 lists all changes to DB Server options between release 8.0 and the latest 8.1 release.

**Table 3: DB Server Configuration Option Changes from 8.0 to 8.1**

| Option Name | Option Values | Type of Change | Details |
|---|---|---|---|
| **Transport Parameters** | | | |
| tls | `0`, 1 | New in 7.5 | See description on page 53.<br>Previously documented as `transport` option. |

Genesys

Chapter

# 3 Database Access Point Configuration Options

This chapter describes configuration options for a Database Access Point.

This chapter contains the following sections:



## Setting Configuration Options

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 or Configuration Manager exactly as they are documented in this chapter.

## Mandatory Options

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

## default Section

This section must be called `default`.

### db-request-timeout

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

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

This option overrides the value of the `db-request-timeout` option specified by DB Server, for this Database Access Point only.

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

**Setting this Option**

You can configure this option in any of the following locations:

- In Genesys Administrator
  - Database Access Point `Application` object > `Options` tab > `Advanced View (Annex)`
  - Database Access Point `Application` object > `Configuration` tab > `DB Info` section > `Query Timeout` field
- In Configuration Manager
  - Database Access Point `Application` object > `Properties` dialog box > `DB Info` tab > `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 only in Genesys Administrator, as the following location:

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

You cannot configure this option in Configuration Manager. Multi-language functionality is available only in Genesys Administrator.

# Changes from 8.0 to 8.1

Table 4 lists all changes to Database Access Point options between release 8.0 and the latest 8.1 release.

**Table 4: Database Access Point Option Changes from 8.0 to 8.1**

| Option Name | Option Values | Type of Change | Details |
|---|---|---|---|
| **dbclient Section (new section)** | | | |
| utf8-ucs2 | `true`, `false` | New | See description on page 58. |

Genesys

Chapter

# 4 Configuration Server Configuration Options

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



## Setting Configuration Options

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

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

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

## Using the Configuration File for Startup Options

Using a text editor, enter Configuration Server startup options directly in the configuration file. See "Startup Options in Configuration File" on page 62 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 77 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.

## Using Configuration Manager for Runtime Options

In Configuration Manager, set Configuration Server configuration options in the `Options` tab of the `Application` object, unless specified otherwise. See "Runtime Options in Configuration Database" on page 77 for descriptions of the runtime options.

# Startup Options in Configuration File

These options in the Configuration Server configuration file `confserv.cfg` (on Windows) or `confserv.conf` (on UNIX).

**Notes:**
- Options in the `confserv` 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 from any other section of the configuration file are read only at first startup. Configuration Server copies those options into the Configuration Database as part of their `Application` objects, and ignores any future changes in the configuration file. Users must change them in the `Options` tab of the object after Configuration Server is started, and for all subsequent starts.

# Mandatory Startup Options

Table 5 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 5: Mandatory Options**

| Option Name | Default Value | Details |
|---|---|---|
| **Configuration Server Section** | | |
| port | No default value | Used only during the first start of Configuration Server with an initialized database. Upon subsequent restarts, Configuration Server reads the port information from its Application object in the Configuration Database and ignores the setting of the `port` option in the configuration file.<br>See the description on page 71. |
| server | No default value | See the description on page 71. |
| **Configuration Database Section** | | |
| host | No default value | See the description on page 74. |
| port | No default value | See the description on page 75. |
| dbengine | No default value | See the description on page 73. |
| dbname | No default value | You must specify a value for this option unless `dbengine=oracle`.<br>See the description on page 74. |
| dbserver | No default value | See the description on page 74. |
| username | No default value | See the description on page 75. |
| password | No default value | See the description on page 74. |

# confserv Section

This section contains the configuration options of Configuration Server.

This section must be called `confserv`.

In an environment with redundant Configuration Servers, this section is usually called `confserv` on the primary Configuration Server. On the backup Configuration Server, this section has the same name as the backup Configuration Server `Application` object.

### allow-empty-password

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

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 142) 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: After restart

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), the validity of an empty password depends on whether empty passwords are permitted without external authentication, as defined by the value of `password-min-length` (see page 142) or, in its absence, `allow-empty-password` (see page 64). 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: When the next client connects

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, Configuration Server will terminate immediately.

### client-response-timeout

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

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

### 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 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). On the Solaris platform, you might be required to set the environment variable `GCTI_TRANSLOCALCP` to the value that represents the current local system encoding name (returned by the `lconv -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.

**Warning!** Set the encryption value to `true` only after you finish encrypting the password values for all Configuration Database sections within the configuration file.

Refer to the "Encrypted Configuration Database Password" chapter in the *Genesys Security Deployment Guide for more information*.

### 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 a pre-8.0 version. 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 7.x 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 Server8.1.1 (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*.

### force-reconnect-reload

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

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

### 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 or Configuration Server Proxy. 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 or Configuration Server Proxy.

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 parameter. 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 the `encoding` option.

**Note:** On the Solaris platform, you might be required to set the environment variable `GCTI_TRANSLOCALCP` to the value that represents the current local system encoding name (returned by the `lconv -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.

### 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.

### 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.

**Warnings!**
- You must set this option after you have run the database initialization and locale scripts but before you first start Configuration Server. You cannot set this option at any other time.
- This option can be set only once, and cannot be changed after it has been set.

### 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: `102400`
Valid Values: Any positive integer
Changes Take Effect: After restart

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

### password-change

Default Value: `true`

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

Specifies whether Configuration Server allows a user 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*.

### 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.

### 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 73. You must specify a value for this option.

## 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 ADDP-related 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` | No ADDP trace occurs. |
| `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 `server` option on page 71. This section contains information about the Configuration Database and DB Server that Configuration Server uses to access this database, and its options can only be edited in the configuration file, not via an `Application` object's options.

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

**Note:** In addition to the configuration options listed here, this section contains the following options:

- `history-log-guid`, `history-log-minid`, `history-log-version`— These options are not editable, and are inserted into an Application's objects by Configuration Server to display internal runtime information about the status of the History Log feature. They are intended for use by Technical Support.

### dbengine

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

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

### dbname

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

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

### dbserver

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

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

- For Sybase, this value is the server name stored in the Sybase interface file.
- For Oracle, the value is the name of the Listener service.
- For Informix, this value is the name of SQL server, specified in the `sqlhosts` file.
- For Microsoft SQL, set this value to the SQL server name (usually the same as the host name of the computer where Microsoft SQL runs).
- For DB2, set this value to the name or alias-name of the database specified in the db2 client configuration.
- For PostgreSQL, set this value to the SQL server name (usually the same as the host name of the computer where PostgreSQL runs).

### host

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

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

### password

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

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

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

### port

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

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

### reconnect-timeout

Default Value: `10`
Valid Values: 0 or any positive integer
Changes Take Effect: After restart

Specifies the time interval, in seconds, between attempts to connect to DB Server(s). If set to 0, reconnection will be disabled.

### response-timeout

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

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

### server

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

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

### 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.

## Configuring ADDP Between Configuration Server and DB Server

Use the options in this section to configure Advanced Disconnect Detection Protocol (ADDP) between Configuration Server and the Configuration DB Server.

### addp

Default Value: `off`
Valid Values:

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

Changes Take Effect: After restart

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

### addp-timeout

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

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

### addp-trace

Default Value: `off`
Valid Values:

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

Changes Take Effect: After restart

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

## hca Section

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

This section must be called `hca`.

### schema

Default Value: `none`

Valid Values:

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

Changes Take Effect: After restart

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

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

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

# Runtime Options in Configuration Database

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

# 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 or Configuration Manager.

# soap Section

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

**Warning!** SOAP functionality is restricted to certain environments.

**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 option in this section in runtime using Genesys Administrator or Configuration Manager.

This section must be called `soap`.

### client_lifespan

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

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

### debug

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

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

### port

Default Value: `0`
Valid Values: `0` or any valid TCP/IP port
Changes Take Effect: After restart

Specifies the SOAP port that clients use to connect to Configuration Server. The default value of `0` means that SOAP is not used.

**Note:** The SOAP `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.

## 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.

To maintain backward compatibility with previous releases, you must manually add this option to all release 7.5 (or earlier) Configuration Server `Application` objects imported into Configuration Server 7.6 (or later), and set its value to `1`. This will ensure that new users created for these objects are automatically assigned to the default Access Groups, as was the case in those pre-7.6 releases.

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 the history log on 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 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.

### 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 the port's properties, using one of the following navigation paths:

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

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

### backlog

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

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

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

# Transport Parameter Options

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

- In Genesys Administrator—Configuration Server Application object > Configuration tab > General section > Connections > Connection Info > Advanced tab > Transport Parameters
- In Configuration Manager—Configuration Server Application object > Properties dialog box > Connections tab > Connection Properties dialog box > Advanced tab > Transport Protocol 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 82), 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 or Configuration Manager, 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:<br>tls=1;certificate=<value> | Secure connections will be used, where `certificate` = certificate value. |
| For UNIX:<br>tls=1;certificate=<path>;<br>[certificate-key=<path>];<br>trusted-ca=<path> | Secure connections will be used, where:<br>• `certificate`—full path to the `<serial_#>_<host_name>_cert.pem` file<br>• `certificate-key`—full path to the `<serial_#>_<host_name>_priv_key.pem` file (unless the private key is stored together with a certificate)<br>• `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.

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

# 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

[hca]
schema = none

[soap]
port = 5555

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

# Changes from 8.0 to 8.1

Table 6 on page 83 lists all changes to Configuration Server options between release 8.0 and the latest 8.1 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 6: Configuration Server Configuration Option Changes from 8.0 to 8.1**

| Option Name | Option Values | Type of Change | Details |
|---|---|---|---|
| **confserv Section** | | | |
| allow-mixed-encoding | `true`, `false` | New | See description on page 64. |
| enable-pre-812-security | `true`, `false` | New | See description on page 65. |
| force-md5 | `true`, `false` | New | See description on page 67. |
| multi-languages | false, true | New | See description on page 70. |
| password-change | `true`, `false` | New | See description on page 70. |
| packet-size | Any positive integer | New | See description on page 70 |

**Table 6: Configuration Server Configuration Option Changes from 8.0 to 8.1 (Continued)**

| Option Name | Option Values | Type of Change | Details |
|---|---|---|---|
| fix_cs_version_7x | `true`, `false` | New option in 8.0 | See description on page 67.<br>Not documented in 8.0. |
| protocol | `true`, `false` | New option in 8.0 | See description on page 72.<br>Not documented in 8.0. |
| addp-timeout | `0-3600` | New option in 8.0 | See description on page 72.<br>Not documented in 8.0. |
| addp-remote-timeout | `0-3600` | New option in 8.0 | See description on page 72.<br>Not documented in 8.0. |
| addp-trace | `off`, `on`, `remote`, `full` | New option in 8.0 | See description on page 73.<br>Not documented in 8.0. |
| **Configuration Database Section** | | | |
| reconnect-timeout | `0`, any positive integer | Added value | Added valid value of zero (`0`).<br>See description on page 75. |
| **soap Section** | | | |
| port | `0`, valid TCP/IP port | Changed default value | Previous default value was “no default value”.<br>See description on page 79. |
| **history-log Section** | | | |
| all | `<any string>`, `:memory:` | Removed in 8.0 | Not documented in 8.0. |
| failsafe-store-processing | true, false | Removed in 8.0 | Not documented in 8.0. |
| **Transport Parameters** | | | |
| tls | `0`, 1 | New in 7.6 | See description on page 82.<br>Previously documented as transport option. |

Chapter

# 5 Configuration Server Proxy Configuration Options

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



Configuration Server Proxy also supports the common options described in Chapter 1 on page 13.

## Setting Configuration Options

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

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

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

# Mandatory Options

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

**Table 7: Mandatory Options**

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

**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: Any positive integer
Changes Take Effect: After restart

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

### encoding

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

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

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

### 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 or 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 or Configuration Server Proxy.

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 Proxies 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 Proxies 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 forth.

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).

### 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: `102400`
Valid Values: Any positive integer
Changes Take Effect: Immediately

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

### proxy-writable

Default Value: `false`
Valid Values:

| | |
|---|---|
| `true` | Configuration Server Proxy accepts requests from clients for updates to user-defined data, and forwards these requests to the Master Configuration Server. |
| `false` | 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.

# history-log Section

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

This section must be called `history-log`.

### active

Default Value: `true`

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

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

### all

Default Value: `:memory:`
Valid Values:

| | |
|---|---|
| `:memory:` | Stores the file in memory as histlog.hdb. Use this value to help improve system performance. |
| <valid path and filename> | Specifies a full path to the history log database file including the filename without the extension. Configuration Server Proxy appends the extension .hdb. |

Changes Take Effect: After restart

Specifies where the history log database file is stored.

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

### client-expiration

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

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

### expiration

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

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

### failsafe-store-processing

Default Value: `true`
Valid Values:

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

Changes Take Effect: Immediately

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

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

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

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

### max-records

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

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

# soap Section

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

**Warning!** SOAP functionality is restricted to certain environments.

This section must be called `soap`.

### client_lifespan

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

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

### debug

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

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

### port

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

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

# Application Parameter Options

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

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

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

### backlog

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

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

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

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

# Changes from 8.0 to 8.1

Table 8 lists all changes to Configuration Server Proxy options between release 8.0 and the latest 8.1 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 8: Configuration Server Proxy Configuration Option Changes from 8.0 to 8.1**

| Option Name | Option Values | Type of Change | Details |
|---|---|---|---|
| **csproxy Section** | | | |
| allow-mixed-encoding | `true`, `false` | New | See description on page 86. |
| client-response-timeout | Any positive integer | New | See description on page 87 |
| packet-size | Any positive integer | New | See description on page 89 |
| **history-log Section** | | | |
| all | `:memory:`, valid path and filename | Changed default value | New default value `:memory:`<br>See description on page 90 |

Chapter

# 6 Configuration Manager Configuration Options

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



## Setting Configuration Options

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

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

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

## Mandatory Options

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

# security Section

The `security` section contains configuration options that relate to security features. This section must be called `security`.

### inactivity-timeout

Default Value: `0`

Valid Values: Any nonnegative integer

Changes Take Effect: Immediately

Specifies the amount of time (in minutes) that a user who is logged in to the application can be inactive before application screens are minimized and the user forced to be re-authenticated. The default value `0` (zero) means that the feature is disabled.

Refer to the "Inactivity Timeout" chapter in the *Genesys Security Deployment Guide* for complete information about this option.

# Changes from 8.0 to 8.1

There were no changes to Configuration Manager configuration options between release 8.0 and the latest 8.1 release.

Chapter

# 7 Message Server Configuration Options

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



Message Server also supports the common options described in Chapter 1 on page 13.

## Setting Configuration Options

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

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

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

# Mandatory Options

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

# MessageServer Section

This section must be called `MessageServer`.

### signature

Default Value: `log`
Valid Values:

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

Changes Take Effect: After restart

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

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

# messages Section

This section must be called `messages`.

### 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.

### 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.

### thread_mode

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

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

### thread_pool_size

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

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

# db-filter Section

The DB Filter section controls delivery of specified log events from specified applications and application types. See “Sample Configuration” on page 101. This section must be called `db-filter`.

### block-messages

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

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

### block-messages-by-<type>

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

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

**Note:** For information about application types, refer to the “Database Format” section of the “Log Format” chapter in the *Framework 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.

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

### Sample Configuration

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

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

# Changes from 8.0 to 8.1

Table 9 lists all changes to Message Server configuration options between release 8.0 and the latest 8.1 release.

**Table 9: Message Server Configuration Option Changes from 8.0 to 8.1**

| Option Name | Option Values | Type of Change | Details |
|---|---|---|---|
| **messages Section** | | | |
| request-queue-size | Positive integer | Removed | Option removed in 8.0; not documented. |

Genesys

Chapter

# 8 Solution Control Server Configuration Options

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



Solution Control Server also supports:

- The common options described in Chapter 1 on page 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 one of the following navigation paths:

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

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

# Mandatory Options

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

# License Section

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

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

This section must be called `license`.

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

# general Section

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

This section must be called `general`.

### alive_timeout

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

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

Control Servers" section in the *Framework Deployment Guide* for details about this relationship.

### disconnect-switchover-timeout

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

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

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

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

### distributed_mode

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

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

### distributed_rights

Default Value: `DEFAULT`
Valid Values:

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

Changes Take Effect: After restart

When SCS operates in Distributed mode (`distributed_mode` is set to `ON`), specifies what objects SCS controls. Use this option when you run SCS in a distributed management environment and you want to grant this SCS instance control permissions over all configuration objects (such as, Hosts,

Applications, and Solutions) that you have not configured other SCS instances to control.

### 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: `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, 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 it in audit logs.

### max-req-per-loop

Default Value: `20`
Valid Values:`10`—`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.

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

### max_switchover_time

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

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

### service-unavailable-timeout

Default Value: `0`

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

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

# mailer Section

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

This section must be called `mailer`.

### smtp_from

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

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

### smtp_host

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

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

### smtp_port

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

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

# 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):

| | |
|---|---|
| `stdout` | Alarms are sent to the Standard output (stdout). |
| `stderr` | Alarms are sent to the Standard error output (stderr). |
| `network` | Alarms are sent to Message Server, which resides anywhere on the network, and Message Server stores the log events in the Log Database. |
| `memory` | Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance. |
| `[filename]` | Alarms are stored to a file with the specified name. |
| `syslog` | Alarms are sent to the operating-system log. |

Changes Take Effect: Immediately

Specifies to which outputs SCS sends those alarms it generates as a result of appropriate Standard log events. When you configure more than one output type, separate them by a comma. This option is the same as the `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: `<string>`
Changes Take Effect: Immediately

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

# 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 one of the following navigation paths:

- In Genesys Administrator—Solution Control Server `Application` object > `Configuration` tab > `General` section > `Connections` > Connection to Log Message Server > `Connections Info` > `Advanced` tab > `Transport Parameters`
- In Configuration Manager—Solution Control Server `Application` object > `Properties` dialog box > `Connections` tab > Connection to Log Message Server > `Connection Info` > `Advanced` tab > `Transport Protocol Parameters`

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` **Option**

In a configuration file, 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 or Configuration Manager, 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 13 on page 131.

# Changes from 8.0 to 8.1

Table 10 lists all changes to Solution Control Server options between release 8.0 and the latest 8.1 release.

**Table 10: Solution Control Server Configuration Option Changes from 8.0 to 8.1**

| Option Name | Option Values | Type of Change | Details |
|---|---|---|---|
| **general Section** | | | |
| ha_service_unavail_primary | `false, true, on, off, yes, no` | New | See description on page 106. |
| lookup_clienthost | `false, true, on, off, yes, no` | New | See description on page 106. |
| max-req-per-loop | `10—32767` | New | See description on page 106 |
| **Transport Parameters** | | | |
| alarms-port | `0·<max number of OS ports>` | New | See description on page 109. |
| backup-alarms-port | `0·<max number of OS ports>` | New | See description on page 109. |

Genesys

Chapter

# 9 Solution Control Interface Configuration Options

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



## Setting Configuration Options

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

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

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

# Mandatory Options

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

# host-status-display Section

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

This section must be called `host-status-display`.

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

### critical-color

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

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

### major-color

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

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

### other-color

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

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

# security Section

The `security` section contains configuration options related to security features. This section must be called `security`.

### inactivity-timeout

Default Value: `0`
Valid Values: Any nonnegative integer
Changes Take Effect: Immediately

Specifies the amount of time (in minutes) that a user who is logged in to the application can be inactive before application screens are minimized and the user forced to be re-authenticated. The default value `0` (zero) means that the feature is disabled.

Refer to the "Inactivity Timeout" chapter in the *Genesys Security Deployment Guide* for complete information about this option.

# config Section

The `config` section contains configuration options related to SCI configuration. This section must be called `config`.

### log_auto_refresh

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

Specifies if the list of log records displayed in the SCI Centralized Log view refreshes automatically. This option must be set in the `Annex` of the SCI `Application` object.

# Changes from 8.0 to 8.1

Solution Control Interface 8.0.x has not been updated to 8.1.x, and is released with Management Framework 8.1.x. Refer to the *Framework 8.0 Configuration Options Reference Manual* for information about changes to Solution Control Interface configuration options in releases 8.0.x.

Chapter

# 10 SNMP Master Agent Configuration Options

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



Genesys SNMP Master Agent also supports the options described in Chapter 1 on page 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 one of the following navigation paths:

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

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

# Mandatory Options

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

# agentx Section

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

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

### mode

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

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

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

### tcp_port

Default Value: `705`
Valid Values:

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

Changes Take Effect: After restart

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

# snmp Section

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

Use the following options to configure SNMPv1/v2 access:

- `read_community`
- `write_community`

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

Use the following options to configure SNMPv3 access:

- `v3_username`
- `v3auth_password`
- `v3priv_password`
- `v3auth_protocol`
- `v3priv_protocol`
- `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: `none`
Valid Values:

`none`

`<string>` Any valid community name

Changes Take Effect: After restart

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

### trap_target

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

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

For example:

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

### v3_username

Default Value: `default`
Valid Values:

`default`

`<string>` User name

Changes Take Effect: After restart

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

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

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

### v3auth_password

Default Value: No default value

Valid Values: `<string>` Any valid password
Changes Take Effect: After restart

Specifies the SNMPv3 user password used for authentication. The password specified by this option can be viewed in Genesys Administrator or Configuration Manager, and is not encrypted in the Configuration Database.

**Note:** To hide the password in the interface and encrypt it in the database, use the option in the `snmp-v3-auth` section (see page 120) 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 don't configure the option, don't set its value, or set it to an invalid value, Genesys SNMP Master Agent uses no authentication.

### v3priv_password

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

Specifies the SNMPv3 user password used for privacy of data. The password specified by this option can be viewed in Genesys Administrator or Configuration Manager, and is not encrypted in the Configuration Database.

**Note:** To hide the password in the interface and encrypt it in the database, use the option in the `snmp-v3-priv` section (see page 121) instead of this option.

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

### v3priv_protocol

Default Value: `none`
Valid Values:

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

Changes Take Effect: After restart

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

### write_community

Default Value: `none`
Valid Values:

`none`

`<string>` Any valid community name

Changes Take Effect: After restart

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

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

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

## snmp-v3-auth Section

This section contains options that are 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 that are 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 8.0 to 8.1

Table 11 on page 121 lists all changes to SNMP MA configuration options between release 8.0 and the latest 8.1 release.

**Table 11: SNMP Master Agent Configuration Option Changes from 8.0 to 8.1**

| Option Name | Option Values | Type of Change | Details |
|---|---|---|---|
| **snmp-v3-auth Section (new section)** | | | |
| password | `Any valid password` | New | See description on page 120. |
| **snmp-v3-priv Section (new section)** | | | |
| password | `Any valid password` | New | See description on page 121. |

Genesys

Chapter

# 11 Local Control Agent Configuration Options

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



## Setting Configuration Options

You change default LCA configuration options in the configuration file `lca.cfg`. See "LCA Configuration File" on page 124 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.

# 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 options `lca-upgrade` and `upgrade` on page 134.

# LCA Configuration File

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

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

The LCA configuration file must have the following format:

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

For more information on the LCA configuration file and for related instructions, see the *Framework 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 13 on page 131.

# Changes from 8.0 to 8.1

Table 12 lists all changes to Local Control Agent options between release 8.0 and the latest 8.1 release.

**Table 12: Solution Control Server Configuration Option Changes from 8.0 to 8.1**

| Option Name | Option Values | Type of Change | Details |
|---|---|---|---|
| **general Section (new section)** | | | |
| lookup_clienthost | `false`, `true`, `on`, `off`, `yes`, `no` | New | See description on page 124. |

Chapter

# 12 Genesys Deployment Agent Configuration Options

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



## 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 129 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 Genesys Deployment Agent. 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 8.0 to 8.1

Table 13 lists all changes to Genesys Deployment Agent options between release 8.0 and the latest 8.1 release.

**Table 13: Genesys Deployment Agent Configuration Option Changes from 8.0 to 8.1**

| Option Name | Option Values | Type of Change | Details |
|---|---|---|---|
| **web Section** | | | |
| rootdir | Valid path | New | New option added in 8.0; not documented. |
| **security Section (new section)** | | | |
| transport | See details | New | See description on page 128. |

Chapter

# 13 Host Configuration Options

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



## Setting Configuration Options

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

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

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

## Mandatory Options

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

# addp Section

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

This section must be called `addp`.

### addp-timeout

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

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

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

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

### addp-remote-timeout

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

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

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

# 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` |
| HP-UX | `/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 Deployment Guide* and associated help file for information about remote deployment using Genesys Adminsitrator.

# 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`

### 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 41.
- If the security certificate is configured at the application level, see page 33.

**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: `false`
Valid Values: `false`, `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.

### 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`.

# Changes from 8.0 to 8.1

Table 14 lists all changes to Host options between release 8.0 and the latest 8.1 release.

**Table 14: Host Configuration Option Changes from 8.0 to 8.1**

| Option Name | Option Values | Type of Change | Details |
|---|---|---|---|
| **ntp-service-control (new section)** | | | |
| `signature` | See details | | See description on page 133 |
| **rdm (new section)** | | | |
| `port` | Valid port number | New | See description on page 133.<br>New in 8.0, not previously documented. |
| **security Section (new section)** | | | |
| client-auth | `1, 0` | New | See description on page 134. |

### Table 14: Host Configuration Option Changes from 8.0 to 8.1

| Option Name | Option Values | Type of Change | Details |
|---|---|---|---|
| `upgrade` | See details | New | See description on page 134. |
| `lca-upgrade` | See details | New | See description on page 134. |

Chapter

# 14 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:



**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 Genesys applications that 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 one of the following navigation paths:

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

The options in this section applies to all objects owned by the Tenant in which the options are set, 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 one of the following navigation paths:

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

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

# Mandatory Options

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

# Passwords in Multi-Tenant Configuration

In multi-tenant configurations, 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 that are 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 145) 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 139) or the user level (page 146). 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:

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

### account-expiration

Default Value: `0`
Valid Values: `0` to `365`
Takes Effect: Rule validation occurs the next time that 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. of which this option is a part, 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 68 and 87) and `last-login-synchronization` (pages 68 and 88) 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.

**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 147).

In multi-tenant configurations, this value applies to all child Tenants unless it is overridden in a child Tenant. See "Passwords in Multi-Tenant Configuration" on page 138 for more information.

### 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 multi-tenant configurations, this value applies to all child Tenants unless it is overridden in a child Tenant. See "Passwords in Multi-Tenant Configuration" on page 138 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 that are 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 multi-tenant configurations, this value applies to all child Tenants unless it is overridden in a child Tenant. See “Passwords in Multi-Tenant Configuration” on page 138 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 multi-tenant configurations, 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 Multi-Tenant Configuration” on page 138 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 that are 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 multi-tenant configurations, this value applies to all child Tenants unless it is overridden in a child Tenant. See “Passwords in Multi-Tenant Configuration” on page 138 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 142) is configured at the Tenant level.

In multi-tenant configurations, this value applies to all child Tenants unless it is overridden in a child Tenant. See “Passwords in Multi-Tenant Configuration” on page 138 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 64) 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 that are 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 that 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 multi-tenant configurations, this value applies to all child Tenants unless it is overridden in a child Tenant. See “Passwords in Multi-Tenant Configuration” on page 138 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 multi-tenant configurations, this value applies to all child Tenants unless it is overridden in a child Tenant. See “Passwords in Multi-Tenant Configuration” on page 138 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 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 multi-tenant configurations, this value applies to all child Tenants unless it is overridden in a child Tenant. See “Passwords in Multi-Tenant Configuration” on page 138 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 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 multi-tenant configurations, this value applies to all child Tenants unless it is overridden in a child Tenant. See “Passwords in Multi-Tenant Configuration” on page 138 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 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 multi-tenant configurations, this value applies to all child Tenants unless it is overridden in a child Tenant. See “Passwords in Multi-Tenant Configuration” on page 138 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 multi-tenant configuration; 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:

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

**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 140) is set at the Tenant level. If set to `false` (the default), this account cannot be locked out.

### 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 `account-expiration` is ignored. If this account is marked as expired (`last-expired-at` is set to a valid date/time stamp, [see page 147]), 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 139), 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 8.0 to 8.1

Table 15 lists all changes to Tenant configuration options between release 8.0 and the latest 8.1 release.

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

**Table 15: Tenant Configuration Option Changes from 8.0 to 8.1**

| Option Name | Option Values | Type of Change | Details |
|---|---|---|---|
| **security-authentication-rules Section (new)** | | | |
| `account-override-lockout` | `true`, `false` | New | See description on page 146. |
| `force-password-reset` | `true`, `false` | New | See description on page 141. |
| `last-expired-at` | <date and time stamp> | New | See description on page 147<br>Read-only. |
| `last-locked-at` | <date and time stamp> | New | See description on page 147<br>Read-only. |
| `max-account-sessions` | `0` to `128` | New | See description on page 141. |
| `override-account-expiration` | `0`, `1`, `2` | New | See description on page 147. |
| `override-password-expiration` | `true`, `false` | New | See description on page 148. |
| `password-expiration` | `0` to `365` | New | See description on page 142. |

**Table 15: Tenant Configuration Option Changes from 8.0 to 8.1 (Continued)**

| Option Name | Option Values | Type of Change | Details |
|---|---|---|---|
| password-expiration-notify | 0 to 365 | New | See description on page 142. |
| password-no-repeats | 0 to 10 | New | See description on page 143. |
| password-req-punctuation | true, false | New | See description on page 145. |
| tenant-override-section | true, false | New | See description on page 145. |
| account-lockout-attempts-period | 0 to 20 | New | See description on page 140.<br>Added in 8.0; not documented. |
| account-lockout-duration | 0 to 1440 | New | See description on page 140.<br>Added in 8.0; not documented. |
| account-lockout-threshold | 0 to 8 | New | See description on page 141.<br>Added in 8.0; not documented. |
| password-req-alpha | true, false | New | See description on page 143.<br>Added in 8.0; not documented. |
| password-req-mixed-case | true, false | New | See description on page 144.<br>Added in 8.0; not documented. |
| password-req-number | true, false | New | See description on page 144.<br>Added in 8.0; not documented. |

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 8.1 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.
- *Framework 8.1 Configuration Manager Help,* which will help you use Configuration Manager.
- Release Notes and Product Advisories for this product, which are available on the Genesys Technical Support website at http://genesyslab.com/support.

## Genesys

- The *Genesys 8.1 Security Deployment Guide*, which describes configuration options specific to Genesys security features, and how to use them.
- *Genesys Technical Publications Glossary,* which ships on the Genesys Documentation Library DVD and which provides a comprehensive list of the Genesys and computer-telephony integration (CTI) terminology and acronyms used in this document.
- *Genesys Migration Guide*, which ships on the Genesys Documentation Library DVD, and which provides documented migration strategies for Genesys product releases. Contact Genesys Technical Support for more information.

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

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

Consult the following additional resources as necessary:

- *Genesys Hardware Sizing Guide,* which provides information about Genesys hardware sizing guidelines for the Genesys 8.x releases.
- *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.
- *Genesys Database Sizing Estimator 8.x Worksheets,* which provides a range of expected database sizes for various Genesys products.

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

Genesys product documentation is available on the:

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

# Document Conventions

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

## Document Version Number

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

81fr_ref-co_04-2012_v8.1.100.01

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

## Screen Captures Used in This Document

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

## Type Styles

Table 16 on page 154 describes and illustrates the type conventions that are used in this document.

### Table 16: Type Styles

| Type Style | Used For | Examples |
|---|---|---|
| Italic | • Document titles<br>• Emphasis<br>• Definitions of (or first references to) unfamiliar terms<br>• Mathematical variables<br>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 154). | Please consult the *Genesys Migration Guide* for more information.<br>Do *not* use this value for this option.<br>A *customary and usual* practice is one that is widely accepted and used within a particular industry or profession.<br>The formula, $x + 1 = 7$<br>where *x* stands for... |
| Monospace font<br>(Looks like `teletype` or `typewriter text`) | All programming identifiers and GUI elements. This convention includes:<br>• The *names* of directories, files, folders, configuration objects, paths, scripts, dialog boxes, options, fields, text and list boxes, operational modes, all buttons (including radio buttons), check boxes, commands, tabs, CTI events, and error messages.<br>• The values of options.<br>• Logical arguments and command syntax.<br>• Code samples.<br>Also used for any text that users must manually enter during a configuration or installation procedure, or on a command line. | Select the `Show variables on screen` check box.<br>In the `Operand` text box, enter your formula.<br>Click `OK` to exit the `Properties` dialog box.<br>T-Server distributes the error messages in `EventError` events.<br>If you select `true` for the `inbound-bsns-calls` option, all established inbound calls on a local agent are considered business calls.<br>Enter `exit` on the command line. |
| Square brackets ([ ]) | A particular parameter or value that is optional within a logical argument, a command, or some programming syntax. That is, the presence of the parameter or value is not required to resolve the argument, command, or block of code. The user decides whether to include this optional information. | `smcp_server -host [/flags]` |
| Angle brackets (< >) | A placeholder for a value that the user must specify. This might be a DN or a port number specific to your enterprise.<br>**Note:** In some cases, angle brackets are required characters in code syntax (for example, in XML schemas). In these cases, italic text is used for placeholder values. | `smcp_server -host <confighost>` |

# Index

## Symbols



## A



## B

## C

## D

## E



## F

## G



## H



## I



## K



## L

## M



## N

## O



## P



## R



## S

## T

## U



## V



## W



## X