Genesys Rules System

Genesys Configuration Options Current

6/8/2023

Table of Contents

Genesys Rules System Options Reference

Welcome to the Options Reference for Genesys Rules System. This document describes the configuration options for the following components of Genesys Rules System:

- Genesys Rules Engine
- Genesys Rules Authoring Tool

Genesys Rules Engine

Options for this component are contained in the following configuration sections:

- log
- log-extended
- settings

> **Tip**
>
> In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.
>
> **Power users: Download a CSV file** containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
log	all	stdout	Immediately
log	buffering	false	Immediately
log	expire	false	Immediately
log	log-input-facts-on-no-rules-executed	false	Immediately
log	segment	10000	immediately
log	verbose	standard	Immediately
log-extended	level-reassign-disable	false	Immediately
log-extended	level-reassign-<eventID>	Default value of log event <eventID>. Refer to the *Common Log Events Help* or statserver.lms (located in the directory where Stat Server is installed) for a listing of each of Stat Server's the default levels.	Immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
settings	cache-business-calendars		Immediately
settings	cache-operational-parameters	true	Immediately
settings	check-expired-status-on-start	False	After restart
settings	clear-cache-on-disconnect	false	Immediately
settings	deployed-rules-directory	logs/GRE_DEPLOYDIR	After restart
settings	deployed-rules-directory-is-relative-to-shared-root	false	After restart
settings	enable-memory-monitor	false	After restart
settings	enable-memory-monitor-over-threshold-memory-cleanup	true	Immediately
settings	enable-memory-monitor-update-status	true	Immediately
settings	enable-package-serialization	False	Immediately
settings	esp-worker-threads	5	After restart
settings	ignore-config-connection-status	false	After restart
settings	include-rule-evaluation-detail-in-response	false	Immediately
settings	iwd-set-department-from-process	false	Immediately
settings	json-hierarchical-driver	false	After restart
settings	load-packages-on-start	true	After restart
settings	max-number-rule-executions	10000	Next rules execution
settings	memory-monitor-adaptive-threshold-safety-margin	10	Immediately
settings	memory-monitor-interval	60	After restart
settings	memory-monitor-threshold	70	Immediately
settings	memory-monitor-threshold-strategy	adaptive	Immediately
settings	parameter-cache-timeout	168	Immediately
settings	sequential-mode	false	On rules deployment
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
settings	shared-root-directory		After restart
settings	unload-inactive-package-timeout	-1	After restart
settings	verify-deploy-address	true	immediately
Section	**Option**	**Default**	**Changes Take Effect**

settings Section

cache-business-calendars

Default Value:
Valid Values: true, false
Changes Take Effect: Immediately
Introduced: 8.5.304.07, 9.0.000.13

When enabled, improves performance for rule packages using Business Calendars by enabling an in-memory cache.

If you are using the deprecated feature that allowed dynamic configuration of holidays, and so on, only for the duration of a rule execution, then enabling this caching feature will cause those dynamic configurations to apply across rules. Please confirm that this is acceptable behavior before enabling caching.

cache-operational-parameters

Default Value: true
Valid Values: true, false
Changes Take Effect: Immediately
Introduced: 8.5.0

This option controls whether or not operational parameter values that are used within rules are cached. If true, the first time an operational parameter is used, GRS will get the current value from Configuration Server, and then monitor for updates to the value. The rules will use the cached value instead of making a request to Configuration Server for each rule execution. If set to false, caching will be disabled, and GRS will get the current value from Configuration Server on each rule evaluation request. The default value is true.

Operational parameters are rule parameters whose value is obtained at rule execution time. They are configured in GAX as Parameter Groups, and stored in the Configuration Server database. Prior to 8.5, whenever an operational parameter was referenced during the execution of a rule, GRE would fetch the current value from Configuration Server. In high-volume environments, this could put unnecessary stress on Configuration Server.

In GRS 8.5, the value of the operational parameters can be cached inside GRE, to make fetching faster. Instead of fetching the value with each reference, GRE will set up a listener to Configuration server and maintain the value in a local cache. When the administrator changes the value of the parameter using GAX, GRE will receive an event and update its local cache.

If `cache-operational-parameters` is set to `true` (default), this new caching mechanism will be enabled.

If `cache-operational-parameters` is set to `false`, no caching will be used and each reference will fetch the current value from Configuration Server (as was done prior to 8.5).

check-expired-status-on-start

Default Value: False
Valid Values: true, false
Changes Take Effect: After restart
Introduced: 8.5.303.09

The configuration option **load-packages-on-start** determines whether to load all the rule packages on GRE startup. The **check-expired-status-on-start** option indicates whether to check if the rule package has previously expired from the cache or not. With value `true`, GRE loads only non-expired packages into memory. With value `false`, GRE loads all packages. Rule packages are marked as *expired=true* when the package has been unloaded from the cache because it has not been accessed for the period of time specified in option **unload-inactive-package-timeout**. When such packages are reloaded into memory, they are marked as *expired=false*. For the sake of backwards compatibility, if a rule package does not have the expired flag set, the package defaults to being *expired=false*.

clear-cache-on-disconnect

Default Value: false
Valid Values: true, false
Changes Take Effect: Immediately
Introduced: 8.5.0

GRE is not dependent on an active Configuration Server connection except for evaluating operational

parameters. This option defines whether the cache should return the cached value in the event that Configuration Server goes down or should be cleared in the event that the connection to Configuration Server is no longer active. The default value is false.

When `cache-operational-parameter` is set to `true`, the `clear-cache-on-disconnect` parameter defines what the behavior should be if GRE loses connection with the Configuration Server. If `clear-cache-on-disconnect` is set to `false`, GRE will continue to use the cached value for any rule evaluations, until such time as the Configuration Server is restored. With this option, there is a risk that GRE could use “stale” values for rule evaluation during the time the connection to Configuration Server is down. If `clear-cache-on-disconnect` is set to `true`, the cache will be cleared and a null (“”) value will be used in the rules. With this option, there is potential that rules will fail evaluation during the period that the Configuration Server connection is down.

deployed-rules-directory

Default Value: logs/GRE_DEPLOYDIR
Valid Values:
Changes Take Effect: After restart

Specifies the directory in which to keep the working copy of deployed rule packages. When a package is deployed, a copy of the deployed package is placed here. When the Rules Engine is restarted, packages defined in this directory are loaded when first referenced and made available for execution. When using shared deployment, this is considered as relative to the Shared root directory.

Specifying a deployed rules directory is recommended. If a value is not assigned to the `deployed-rules-directory` option, the rule packages are placed in the `WEB-INF\config` sub-directory within the `genesys-rules-engine` web application directory. At this location the deployed rule packages may be deleted when an updated `.war` file is deployed.

If you choose to change the default value, ensure that the path exists and that the application server can write to the specified directory.

In release 8.5.2, for a clustered GRE created using the GRE-type application cluster template, where the cluster application object has the `auto-synch-rules` option (new in 8.5.2) set to `false`, the deployed rules files will continue to be stored in the `deployed-rules-directory`. In such cases a manual re-deployment will be required if deployment status is partial or if a new node joins the cluster.

Where such a cluster application object has the `auto-synch-rules` option set to `true`, deployed rules data will be stored in a shared cluster folder defined in option `shared-root-directory` (new in 8.5.2). Each clustered GRE node will have its own deployment folder in the cluster shared folder. The shared folder will help synchronize the clustered GREs after either connection disruptions or when a new GRE is added to the cluster.

If multiple GREs share the same host, the value of `deployed-rules-directory` must be unique for each GRE.

deployed-rules-directory-is-relative-to-shared-root

Default Value: false
Valid Values: true, false
Changes Take Effect: After restart
Introduced: 8.5.2

Indicates whether to use the shared root directory as the root directory for `deployed-rules-directory` or not.

It must be set to `true` if GRE belongs to a cluster that has `auto-synch-rules` or just `auto-synch-rules-at-startup` enabled, so that GRE can participate in the auto-synch process.

This option can be used even when GRE does not belong to a cluster. If this option is set to `false`, auto-synch will not work.

enable-memory-monitor

Default Value: false
Valid Values: true, false
Changes Take Effect: After restart
Introduced: 8.5.200.12

Enables (true) or disables (false) the memory monitor that keeps a watch on memory usage by GRE and sets the appropriate status if memory usage reaches the threshold value set in `memory-monitor-threshold`. Invalid or missing values are treated as value `false`.

enable-memory-monitor-over-threshold-memory-cleanup

Default Value: true
Valid Values: true, false
Changes Take Effect: Immediately
Introduced: 8.5.303.06

With value `true`, Java garbage collection is triggered when memory use rises above the maximum threshold limit.

enable-memory-monitor-update-status

Default Value: true
Valid Values: true, false
Changes Take Effect: Immediately
Introduced: 8.5.303.06

When this option is `false`, memory monitor is decoupled from the status.jsp and LCA status update code.

esp-worker-threads

Default Value: 5
Valid Values: A positive integer greater than 4.
Changes Take Effect: After restart

The maximum number of worker threads available when using the ESP interface to execute rules.

include-rule-evaluation-detail-in-response

Default Value: false
Valid Values: true, false
Changes Take Effect: Immediately
Introduced: 8.5.001

Setting this option to true will make GRE include the rule evaluation detail in response. This includes details of rules that did not fire, conditions that evaluated `false` and the rule evaluation time back to the REST client invoking the rule evaluation request. Prior to 8.5.001, only the results of rules that fired were returned.

Note: Currently, the `rulesDisqualified` and `executionTime` is not returned via ESP to iWD.

iwd-set-department-from-process

Default Value: false
Valid Values: true, false
Changes Take Effect: Immediately
Introduced: 8.5.100.21

Enables (value = `true`), GRE to determine the Department from the properties of its Process, for ESP server requests. The setting of the Department from the Process properties will only occur if the Department is not specified and the business context level 1 is not specified.

json-hierarchical-driver

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

With value `true`, the `JsonHierarchicalStreamDriver` class is used to serialize JSON responses. With value `false`, the `JettisonMappedXmlDriver` class is used. The Jettison driver is unaware of the original data type and will try to detect numerical values and omit the quotes, whereas the `JsonHierarchicalStreamDriver` will maintain the data type.

load-packages-on-start

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

Indicates whether to load deployed rule packages at application start up. If packages are not loaded at startup, then a package is loaded on its first execution request.

max-number-rule-executions

Default Value: 10000
Valid Values: Any positive integer or -1
Changes Take Effect: Next rules execution

The maximum number of rules to be executed during a request. This is used to detect unwanted recursion when sequential-mode is `false`. If this maximum is reached an error is reported. May be set to -1 to denote no maximum.

memory-monitor-adaptive-threshold-safety-margin

Default Value: 10
Valid Values: Integer, min. 10, max. 30
Changes Take Effect: Immediately
Introduced: 8.5.200.12

The safety margin percentage used by the "adaptive" strategy, when set. The new threshold, set when application memory is exhausted, is obtained by reducing this percentage amount from the percentage memory usage at the time of memory exhaustion.

memory-monitor-interval

Default Value: 60
Valid Values: Integer, min. 1
Changes Take Effect: After restart
Introduced: 8.5.200.12

The interval in seconds between periodic memory usage checks.

memory-monitor-threshold

Default Value: 70
Valid Values: Integer, min 1, max 99
Changes Take Effect: Immediately
Introduced: 8.5.200.12

Modified: 8.5.303.06

Threshold in percentage. If memory usage exceeds this threshold, GRE will return unavailable status. Note: Range values changed from min 40, max 80 in 8.5.303.06.

The memory usage threshold expressed as a percentage. If memory usage goes above the threshold, GRE's status.jsp returns HTTP 503 status with a message `SYSTEM_STATUS_MEMORY_USAGE_ABOVE_THRESHOLD` (and in 8.5.303.06,Java garbage collection is requested). Genesys Management layer is also notified about GRE's unavailability via a status set in the LCA Connection. When memory usage is back below the threshold, GRE's status.jsp returns HTTP 200 status and Genesys Management Layer is notified that GRE is available. See new 8.5.303.06 options **enable-memory-monitor-update-status** and **enable-memory-monitor-over-threshold-memory-cleanup** to alter this behavior.

memory-monitor-threshold-strategy

Default Value: adaptive
Valid Values: adaptive/forced
Changes Take Effect: Immediately
Introduced: 8.5.200.12

Sets the strategy used by memory monitor to determine the threshold.

Allows you to change the out-of-memory error handling behavior of memory monitor.

- `adaptive`—At out-of-memory error, a new threshold is calculated and it is obtained by reducing the configured `memory-monitor-adaptive-threshold-safety-margin` amount from the percentage memory usage at the time Memory Monitor receives the out-of-memory notification. The threshold is reset only if the new calculated value is less than the configured threshold (or less than current override)—for example, if the configured threshold is 80 %, the safety margin is 10 % and if an out-of-memory error notification is retrieved when memory usage is 70 %, the new override threshold will be 70 - 10 = 60 %. In this scenario, Memory Monitor learned that out-of-memory error can happen at 70 % memory usage, so it adjusts the threshold to be 60 %.

  The override threshold that the "adaptive" strategy sets can be removed by temporarily setting the strategy to "forced". It must be kept as "forced" for at least the `memory-monitor-interval` time. The override can also be removed by reducing the configured threshold value so that the new configured value is equal to, or lower than, the override threshold.

  The override is removed if GRE is restarted, so it is recommended to change the configured threshold to match the override threshold before restarting the GRE.

- `forced`—At out-of-memory error, it does nothing except logging the current memory usage. It forces Memory Monitor to raise an alarm only when memory usage is above the threshold. If using this approach, the threshold must be set low enough so that no out-of-memory errors occur. Temporarily

setting this strategy allows the removal of the override threshold set by the "adaptive" strategy.

parameter-cache-timeout

Default Value: 168
Valid Values: A positive integer greater than 0 representing hours
Changes Take Effect: Immediately
Introduced: 8.5.0

Operational parameters can be cached in memory (see cache-operational-parameters option) and updated automatically from configuration server events. This parameter can be used to control how many hours we should cache all operational parameters in any parameter group (transaction). After the timeout expires, the transaction will be removed from the cache until the next time the value is requested. This is used to clean up old subscription to transaction which are no longer being used.

sequential-mode

Default Value: false
Valid Values: true, false
Changes Take Effect: On rules deployment

Indicates whether to run the rules engine in sequential mode. In sequential mode, after the initial data set, no more data can be inserted or modified. This allows for the rules engine to operate in a simplified way.

shared-root-directory

Default Value:
Valid Values: Any string
Changes Take Effect: After restart
Introduced: 8.5.200

Specifies the shared root directory. When this option is used, and if option 'Deployed rules directory is relative to shared root' is set to true, the effective deployed rules directory used by GRE is made by prepending this to the path specified in 'Deployed rules directory'. It can be used to specify the mapped path to the shared location used for Auto Synch Rules feature. Having this option empty (or not set), effectively allows setting an absolute path in option 'Deployed rules directory' even when 'Deployed rules directory is relative to shared root' is set to true.

It may be a value in Universal Naming Convention (UNC) format or mapped/mounted folder path backed by a service like Amazon S3 or simply an OS shared folder. Examples:

- If `shared-root-directory = C:\shared` and `deployed-rules-directory = \GRE1`, then the effective deployed rules directory path used by GRE is `C:\shared\GRE1` .
- If `shared-root-directory = \\10.10.0.11\shared` and `deployed-rules-directory = \GRE1`, then the effective deployed rules directory path used by GRE is `\\10.10.0.11\shared\GRE1` .

- If the shared folder is mapped on drive Z, the `shared-root-directory` will be `Z:`, `deployed-rules-directory` may be `\GRE1`, then the effective deployed rules directory path used by GRE will be `Z:\GRE1`.

Universal Naming Convention (UNC) format is not supported where GRE runs on the AIX operating system.

unload-inactive-package-timeout

Default Value: -1
Valid Values: Any positive integer or -1
Changes Take Effect: After restart
Introduced: 8.5.1

Time (in minutes) for an inactive package to remain loaded in memory before it is automatically unloaded.

If the option is not specified, or if the value is set to -1 (default), then packages will stay loaded indefinitely with no timeout. If an invalid value (for example, -500) is entered, the value is ignored and the default value of -1 is used.

If a request for a rule package is received after the package has been unloaded, it is automatically loaded into memory again and the timer is restarted.

verify-deploy-address

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

Indicates whether to verify the TCP address of the application deploying rules to be that of a valid associated Genesys Rules Authoring Tool (one in the valid list of application connections). With its default value of `true`, this option protects against illegal attempts to deploy packages from any other application.

ignore-config-connection-status

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

When this option is set to true and the Configuration Server connection goes down, the status servlet will ignore the Configuration Server connection status and report that the server is available in the response code. However, the status servlet will show Configuration Server connection is down in the readable text of the response.

enable-package-serialization

Default Value: False
Valid Values: True, False
Changes Take Effect: Immediately
Introduced: 9.0.000.11

Enables package serialization globally for GRAT rules packages. Package serialization can be used to bring less frequently accessed rule packages back into service much faster, improve performance when unloading expired packages, improve performance when loading rule packages into memory and use less GRE memory.

log Section

all

Default Value: stdout
Valid Values: stdout, stderr, network, memory, [filename]
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

- `stdout`—Log events are sent to the Standard output (stdout).
- `stderr`—Log events are sent to the Standard error output (stderr).
- `network`—Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- `memory`—Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- `[filename]`—Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

buffering

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

Turns on (`true`) or off (`false`) operating system file buffering. The option is applicable only to the

`stderr` and `stdout` output. Setting this option to `true` increases the output performance.

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 1-100.
- <*number*> day - Sets the maximum number of days before log files are deleted. Specify a number from 1-100. If an option&s value is set incorrectly-out of the range of valid values- it will be automatically reset to 10.
{noformat}
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.

log-input-facts-on-no-rules-executed

Default Value: false
Valid Values: false, true
Changes Take Effect: Immediately
Introduced: 9.0.000.28

Specifies if input data details is recorded in logs for cases where no rules are executed for the input request. This helps understand if there is any problem with the input data when no rules are applied.

segment

Default Value: 10000

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.

verbose

Default Value: standard
Valid Values: all
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.

- `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.

log-extended Section

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 and keep the customizations.

level-reassign-<eventID>

Default Value: Default value of log event <eventID>. Refer to the *Common Log Events Help* or statserver.lms (located in the directory where Stat Server is installed) for a listing of each of Stat Server's the default levels.

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 one of five log levels for log event <eventID>, which may differ from its default level, or disables logging of the named event altogether. This option is useful if you want to change the

behavior of what Stat Server logs for the specified log event ID. If no value is specified, then the named log event retains its default level.

You can deactivate these options with the l**evel-reassign-disable** configuration 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 might 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 not logged to specific outputs, thereby losing important information. The same applies to any alarms associated with that log event.

In addition to the precautionary message above, 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 therefore not subject to any log configuration.
- Changing the log level of a log using this feature 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, version 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 Server Reference Manual*, available on the Universal Routing page, 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 20009—with default level trace—is output to stderr.
- Log event 20018—with default level standard—is output to stderr and the log file, and sent to Message Server.
- Log event 20022—with default level debug—is output to stderr.

Extended log configuration section:

```
[log-extended]
level-reassign-20009=none
level-reassign-20018=interaction
level-reassign-20022=standard
```

After the log levels are changed:

- Log event 20009 is disabled and is not logged.
- Log event 20018 is output to stderr and to the log file.
- Log event 20022 is output to stderr and to the log file, and sent to Message Server.

Genesys Rules Engine Application Cluster

Options for this component are contained in the following configuration sections:

- settings

> **Tip**
>
> In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.
>
> **Power users: Download a CSV file** containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
settings	auto-synch-rules	false	After restart
settings	auto-synch-rules-at-startup	false	After restart
settings	auto-synch-rules-interval	5	After restart
Section	**Option**	**Default**	**Changes Take Effect**

settings Section

auto-synch-rules

Default Value: false
Valid Values: true, false
Changes Take Effect: After restart
Introduced: 8.5.200

Setting this option to true will make the clustered GRE to periodically synch rule packages with other GREs of the same cluster.

Set this to `true` to enable a GRE in cluster to start the periodic auto-synch and auto-deployment process.
Clustered GRE's option `deployed-rules-directory-is-relative-to-shared-root` must be set to `true` to have them participate in the rules auto-synch process.

Option `shared-root-directory` can be used to specify the directory which is shared among all the clustered GREs. See option `shared-root-directory` for more information.

If this is `true`, whether `auto-synch-rules-at-startup` is set to `true` or `false`, the GRE always auto-synchronizes rules at startup.

auto-synch-rules-at-startup

Default Value: false
Valid Values: true, false
Changes Take Effect: After restart
Introduced: 8.5.200

Set this option to `true` to have the GREs synchronize and deploy rules at startup. This value is ignored if `auto-synch-rules` is set to `true` (that is, when `auto-synch-rules` is `true` then auto-synch is always performed at startup.
This is useful if rules synchronization is required only at startup when `auto-synch-rules` is set to `false`.

auto-synch-rules-interval

Default Value: 5
Valid Values: Integer, min. 1
Changes Take Effect: After restart
Introduced: 8.5.200

Time interval (in minutes) between the end of last periodic auto-synch operation and the start of new auto-synch operation.

Genesys Rules Authoring Server

Options for this component are contained in the following configuration sections:

- log
- settings

> **Tip**
>
> In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.
>
> **Power users: Download a CSV file** containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
log	all	stdout	After restart
log	buffering	False	Immediately
log	expire	false	Immediately
log	segment	10000	immediately
log	verbose	standard	After restart
settings	**The ReplaceSet call limit ($1) has been reached.#The ReplaceSet call limit ($1) has been reached.** single-sign-on	false	Immediately
settings	allow-legacy-template-import	false	immediately
settings	allow-partial-cluster-deployment	false	Immediately
settings	allow-partial-cluster-undeployment	False	Immediately
settings	auto-fix-corruptions	true	Immediately
settings	clear-repository-cache	true	Immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
settings	context-services-rest-api-base-path	/	Immediately
settings	context-services-rest-api-host		Immediately
settings	context-services-rest-api-port	9080	Immediately
settings	context-services-rest-api-protocol	http	Immediately
settings	decision-table-enable-wildcards	true	Immediately
settings	deploy-method	auto	Immediately
settings	deploy-port	Uses the listening port of the application server	Immediately
settings	display-n-template-versions	3	Immediately
settings	enable-cep-calendars	false	Immediately
settings	enable-dynamic-loading	True	Immediately
settings	enable-nested-solutions	true	Immediately
settings	enable-pending-rule-count	true	Immediately
settings	enable-repository-connection-monitor	True	Immediately
settings	evaluate-decision-table-rows-top-down	false	Immediately
settings	force-snapshot-on-deployment	false	Immediately
settings	group-by-level	true	Immediately
settings	help-file-url	http://docs.genesys.com/Special:HelpLink/GRATHelp?context=8.5.3.index	immediately
settings	link-to-hub		Immediately
settings	list-object-use-name	false	Immediately
settings	max-connections	99	Immediately
settings	max-undo-revisions	10	Immediately
settings	repository-connection-monitor-interval	5	Immediately
settings	require-checkin-comment	false	Immediately
settings	rest-api	disabled	Immediately
settings	session-timeout	30	Immediately
settings	session-timeout-alert-interval	1	Immediately
Section	**Option**	**Default**	**Changes Take Effect**

Section	Option	Default	Changes Take Effect
settings	strict-mode	true	Immediately
settings	verify-deploy-address	true	Immediately
Section	**Option**	**Default**	**Changes Take Effect**

settings Section

allow-legacy-template-import

Default Value: false
Valid Values:
Changes Take Effect: immediately

This option must be set to true if importing templates from GRAT 8.1.1 or earlier. For security reasons, it should be immediately set to false after the migration is complete.

allow-partial-cluster-deployment

Default Value: false
Valid Values: true, false
Changes Take Effect: Immediately
Introduced: 8.5.200

This option must be set to `true` to allow partial deployment to a cluster. If it is set to `false`, the

cluster deployment will fail even if only one of the cluster nodes fails to deploy successfully.

allow-partial-cluster-undeployment

Default Value: False
Valid Values: true, false
Changes Take Effect: Immediately
Introduced: 8.5.303

With value `true`, GRAT can perform a partial undeployment to a GRE-type application cluster. Not applicable to GWE rules engines or to rule packages based on the CEP template.

auto-fix-corruptions

Default Value: true
Valid Values: true, false
Changes Take Effect: Immediately
Introduced: 8.5.304.14, 9.0.000.25
Modified: 9.0.000.31 — default value changed from false to true

Allows enabling (`true`) or disabling (`false`) of the automatic cleanup of repository inconsistencies that might occur where a rule package has been deleted but doesn't get fully cleaned up. When there is a repository inconsistency, an attempt to add another package with the same name would generate an exception and a message indicating that a package with this name already existed. It is recommended to keep this option enabled.

clear-repository-cache

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

If `true`, the server will clear the repository cache during startup. If `false`, the current repository cache will remain.

The GRAT server builds and maintains a cache of the rules repository database (for example, index files, and so on), and stores this on the file system under **WEB-INF/classes/repository**. The cache improves performance when accessing frequently used rules, calendars, and so on. However, this cache must stay synchronized with the rules repository database.

Normally, if GRAT is restarted, it re-uses the existing cache, which is synchronized with the rules repository database. In this case, the **clear-repository-option** should be set to `false` (default).

However, if you are configuring a second GRAT for cold standby (see High Availability Support), this option should be set to true for both the primary and the standby instances of GRAT. Since either GRAT could be brought online in the event of a failure, this option forces GRAT always to rebuild the

cache and re-synchronize it with the rules repository database. Setting this option to true can delay the startup of GRAT, since the cache must be rebuilt, but it ensures that it is properly synchronized with the rules repository database.

When a GRAT is part of a cluster, you should in general set the value of its clear-repository-cache option to true. For GRATs in a cluster, setting this value to true can help avoid the repository corruption errors that can occur if you forget to clear the cache when a node is re-added to the cluster or moved from a different cluster. However if there is a specific reason to avoid the possible slower startup of GRAT server that might ensue, then set the option to false.

If the GRAT startup delay is irrelevant or if GRAT startup is quick enough with the **clear-repository-cache option** set to `true`, then set it to `true`.

context-services-rest-api-base-path

Default Value: /
Valid Values: Any string
Changes Take Effect: Immediately
Introduced: 8.5.001

The base path of the Context Services REST API.

context-services-rest-api-host

Default Value:
Valid Values: Any string
Changes Take Effect: Immediately
Introduced: 8.5.001

The hostname of the Context Services that GRAT connects to.

context-services-rest-api-port

Default Value: 9080
Valid Values: Any positive integer
Changes Take Effect: Immediately
Introduced: 8.5.001

The port number of the Context Services REST API.

context-services-rest-api-protocol

Default Value: http
Valid Values: http, https
Changes Take Effect: Immediately
Introduced: 8.5.001

The protocol used to connect to Context Services REST API.

decision-table-enable-wildcards

Default Value: true
Valid Values: true, false
Changes Take Effect: Immediately
Introduced: 8.5.001

Controls whether the wild card feature is enabled in decision tables.

deploy-method

Default Value: auto
Valid Values: auto, http, https
Changes Take Effect: Immediately
Introduced: 8.5.100.21

Enables users to override the automatic detection of the protocol to construct the "callback" URL used by GRE to fetch the DRL. GRE will use the selected method to connect with the GRAT server during deployment.

deploy-port

Default Value: Uses the listening port of the application server
Valid Values: Any positive numbers
Changes Take Effect: Immediately

Used to override the automatic detection of deployment port.

display-n-template-versions

Default Value: 3
Valid Values: Any positive integer
Changes Take Effect: Immediately

Specifies the number of versions of each published rule template to display to the Rules Author when they are creating or changing a rule package.

f the current rule package is using an older version that is not included in the last "n" versions, it will also be shown, in order to allow the user to upgrade to a more recent template. For example, if "n" is 3, and there are 10 versions of a template, GRAT will show only version 10, 9, and 8. If the rule package is currently associated with an older version, for example, version "5", then that will also be shown, and the checkbox will be selected.
The minimum valid value is 1.

enable-cep-calendars

Default Value: false
Valid Values: true, false
Changes Take Effect: Immediately
Introduced: 8.5.200

Controls whether users can create business calendars for rule packages which support Complex Event Processing (CEP).

enable-dynamic-loading

Default Value: True
Valid Values: True, False
Changes Take Effect: Immediately
Introduced: 8.5.303.12

With value `true`, GRAT loads the business hierarchy and related rule packages on demand when the user opens folders. With value `false`, the entire hierarchy is loaded at user login.

When this feature is enabled, nodes and rule packages are loaded dynamically when the user expands the folders (on the left-hand side), rather than the entire hierarchy being loaded up-front when the user first logs in. In addition, this feature improves performance of creating, updating, and deleting rule packages.

enable-nested-solutions

Default Value: true
Valid Values: true, false
Changes Take Effect: Immediately
Introduced: 8.5.100.21

Controls whether users can create new rule packages under any node of the hierarchy. For iWD users, this option should be set to `false`—iWD does not support nested solutions.

enable-pending-rule-count

Default Value: true
Valid Values: true, false
Changes Take Effect: Immediately
Introduced: 9.0.000.22

Allows the user to disable the calculation of the number of rules that have a pending snapshot. This number is displayed for each rule package in parentheses in the Deploy Rules node (for example, `Deploy Rules (2)`). This is an expensive and frequently accessed function, and can slow down the

overall responsiveness of the GRAT UI.

With value `false`, GRAT will no longer show a count in the parenthesis, but just show an asterisk, indicating that rules have changed since the last snapshot. Users can still view which rules were updated in the rule summary page (**Pending Snapshot** column), or can search the entire rule package for pending rules using the **Search** function.

With value `true` (default), GRAT works as before, showing the number of rules.

For better performance, Genesys recommends setting this to value `false` if this count does not provide business value.

enable-repository-connection-monitor

Default Value: True
Valid Values: true, false
Changes Take Effect: Immediately
Introduced: 8.5.303.06

Specifies whether the repository connection monitor is enabled (`true`) or not (`false`).

evaluate-decision-table-rows-top-down

Default Value: false
Valid Values: true, false
Changes Take Effect: Immediately
Introduced: 8.5.0

This option effectively determines the order of execution for rows within a decision table whose conditions match. The pre-8.5.0 default has been that they are evaluated from the bottom-up. To preserve compatibility with previous releases of GRS, the default setting is `false`, which maintains this same behavior. You can override the default by setting this option to `true`. If you change this default value, you will see a change in behavior immediately when using GRAT's Test Scenario feature, but will need to re-deploy the rule package in order for the change to be observed in GRE, since this option affects how the DRL is encoded.

force-snapshot-on-deployment

Default Value: false
Valid Values: true, false
Changes Take Effect: Immediately
Modified: 8.5.303.06

If true, users can only deploy a package snapshot. If false, users can deploy the LATEST package or a snapshot.

From release 8.5.303 and later, this option also determines whether a user has the choice to

automatically create a snapshot on deployment of the LATEST package. If `true`, then a snapshot will always be created when the user selects the LATEST package. If `false`, then the user can select by using a checkbox whether or not to automatically create a snapshot prior to deploying the LATEST package.

group-by-level

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

if true, rules are grouped by business level. All global rules belong to agenda group "level0". Department rules belong to agenda group "level1". Process rules belong to agenda group "level2". When a rule package is executed, "level0" rules are executed first, facts are marked as updated, and "level1" rules are executed. This is repeated for each level. Note: The GRE option "sequential-mode" must be false when "group-by-level" is true.

There are three levels of rules: global, department, and process.

With value true, rules are grouped by business level:

- All global rules belong to agenda group level0.
- Department rules belong to agenda group level1.
- Process rules belong to agenda group level2.

When a rule package is executed, level0 rules are executed first. Updates from this first pass then influence the department (level1) rules which are executed in the second pass. Updates from this second pass then influence any process rules (level2), which are executed in a third pass.

Note: The GRE option '**sequential-mode**' must be `false` when **group-by-level** is set to `true`.

When **group-by-level** is set to `false`, all rules are executed in a single pass. Changes made by a rule do not influence which other rules are executed (unless a Drools “update” or “insert” command is used).

CEP functionality

Genesys Web Engagement's CEP functionality strips out the rule attribute that indicates which level a rule is associated with. So, the setting of the **group-by-level** has no influence on rule execution.

help-file-url

Default Value: http://docs.genesys.com/Special:HelpLink/GRATHelp?context=8.5.3.index
Valid Values: Any valid URL
Changes Take Effect: immediately
Introduced: 8.5.001
Discontinued: 8.5.1

This option specifies the URL for the online GRAT help, which is normally hosted on

docs.genesys.com. If you wish to host the help locally, you can change the default base URL using this configuration option.

link-to-hub

Default Value:
Valid Values: Any valid URL
Changes Take Effect: Immediately
Introduced: 8.5.0

The URL to which the browser will be redirected on exit from the rules authoring tool. Used only when single-sign-on = true.

Note: This configuration option should only be used when deploying in a Genesys Engage cloud single-sign on environment, and does not apply for Genesys on-premise customers deploying GRS.

This option specifies the URL to which GRAT should redirect once the GRAT SSO session completes. This URL is used in two situations:

- First, when the user clicks the log out button in GRAT, the browser will be redirected to this URL.
- Second, if an SSO login is successful but the subsequent login to Configuration Server fails, then an error box is displayed to the user. Once the error box is dismissed, the browser will be redirected to the specified URL.

Note: The user must have logged in via SSO for this to occur.

list-object-use-name

Default Value: false
Valid Values: true, false
Changes Take Effect: Immediately
Introduced: 8.5.001.21

When parameters are used that reference Configuration Server list objects, this option controls whether the name or display name is encoded in the rule file. Specify `true` to use the name field or `false` (default) to use the display name.

max-connections

Default Value: 99
Valid Values: Any positive integer
Changes Take Effect: Immediately

Specifies the maximum number of different users that may be connected to the server. Multiple connections from the same user ID are only counted once.

max-undo-revisions

Default Value: 10
Valid Values: Any positive integer
Changes Take Effect: Immediately
Modified: 9.0.000.13

The maximum number of undo/re-do revisions that can be made.

repository-connection-monitor-interval

Default Value: 5
Valid Values: Integer, minimum 1
Changes Take Effect: Immediately
Introduced: 8.5.303.06

Specifies the sleep time of the repository connection monitor task in seconds.

require-checkin-comment

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

If `true`, users must specify a check-in comment when committing changes to rules. These comments show up when viewing package history. If `false`, users can save changes to rules without specifying a comment.

rest-api

Default Value: disabled
Valid Values: disabled, enabled, requireSSL
Changes Take Effect: Immediately
Introduced: 8.5.200

Controls whether GRAT's REST API is enabled for rule authoring and deployment.

- disabled—The REST API is disabled and will not accept any requests
- enabled—The REST API is enabled and will accept both secure (https) and non-secure (http) requests
- requireSSL—The REST API is enabled and will only accept secure (https) requests.

In addition, this configuration option enable users to determine whether or not to force only SSL communications. Genesys recommends running over SSL in order to protect the authentication

tokens that flow on each request from compromise. SSL can be disable where appropriate (for example, testing labs, positioning server behind firewalls, and so on).

session-timeout

Default Value: 30
Valid Values: Any positive integer
Changes Take Effect: Immediately

Specifies the amount of time (in minutes) a client session can have no communication with the Rules Authoring Server before timing out. If no value is specified, the timeout (if any) defined by the application server applies. If the value is less than or equal to 0, the session will not timeout

session-timeout-alert-interval

Default Value: 1
Valid Values: Any positive integer
Changes Take Effect: Immediately

Virtual Agent (VAGs) Groups are used to group website visitors by the service they need from agents.

The VirtualAgentGroup name value must match the LivePerson RSI skill names.
The amount of time (in minutes), prior to an expected timeout, for a user to be warned of a pending timeout. If no value is specified, or if the value is less than or equal to `0`, the default warning period of 1 minute will be used. For example, if you set the value of this option to 3, the user will be warned 3 minutes prior to an expected timeout. This warning dialog box will prompt the user to extend the session. If the session is not extended, the user will be logged out and the login dialog box will be displayed. Any unsaved changes that the user made during their session will be lost.

strict-mode

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

This option controls whether or not the rules authoring tool enables *strict* mode in the DROOLS rule compiler. Strict mode will cause the compiler to catch common mistakes when the rule author attempts to validate or save a rule. Genesys recommends leaving this option set to its default value `true`.

verify-deploy-address

Default Value: true

Valid Values: true, false
Changes Take Effect: Immediately

Indicates whether to verify the TCP address of the application deploying rules to be that of a valid associated Genesys Rules Engine (one in the valid list of application connections). With its default value of `true`, this option protects against illegal attempts to deploy packages from any other application.

log Section

all

Default Value: stdout
Valid Values:
Changes Take Effect: After restart

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

- `stdout`—Log events are sent to the Standard output (stdout).
- `stderr`—Log events are sent to the Standard error output (stderr).
- `network`—Log events are sent to Message Server, which can reside anywhere on the network. Message Server stores the log events in the Log Database. Setting the all log level option to the network output enables an application to send log events of the Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
- `memory`—Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
- `[filename]`—Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

buffering

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

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

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 1-100.
- <*number*> day - Sets the maximum number of days before log files are deleted. Specify a number from 1-100. If an option&s value is set incorrectly-out of the range of valid values- it will be automatically reset to 10.
{noformat}
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.

segment

Default Value: 10000

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.

verbose

Default Value: standard
Valid Values:
Changes Take Effect: After restart

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.

- `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.

Genesys Rules Authoring Application Cluster

Options for this component are contained in the following configuration sections:

- settings

> **Tip**
>
> In the summary table(s) below, type in the Search box to quickly find options, configuration sections, or other values, and/or click a column name to sort the table. Click an option name to link to a full description of the option. Be aware that the default and valid values are the values in effect with the latest release of the software and may have changed since the release you have; refer to the full description of the option to see information for earlier releases.
>
> **Power users: Download a CSV file** containing default and valid values and descriptions.

The following options are configured at the application level (in other words, on the application object).

Section	Option	Default	Changes Take Effect
settings	janitor-enabled	true	After restart
settings	janitor-first-run-hour-of-day	3	After restart
settings	janitor-sleep	86400	After restart
settings	local-revisions-janitor-enabled	true	After restart
settings	local-revisions-janitor-first-run-hour-of-day	2	After restart
settings	local-revisions-janitor-sleep	15	After restart
settings	synch-delay	2000	After restart
Section	**Option**	**Default**	**Changes Take Effect**

settings Section

janitor-enabled

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

Specifies whether the clean-up task for the journal table is enabled. If journal table is not cleaned at regular intervals, based on GRAT usage, the database size can grow at very high rate. At regular intervals, the clean-up task cleans the journal table by removing the data which is no longer required by any of the cluster nodes.

janitor-first-run-hour-of-day

Default Value: 3
Valid Values:
Changes Take Effect: After restart

Specifies the hour at which the clean-up task initiates its first run (default = 3, which means 3:00 at night).

janitor-sleep

Default Value: 86400
Valid Values:
Changes Take Effect: After restart

Specifies the sleep time of the clean-up task in seconds (only useful when the clean-up task is enabled, default is 24 hours).

local-revisions-janitor-enabled

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

specifies whether the clean-up task for the local revisions table is enabled. At regular intervals, the clean-up task cleans the local revisions table by removing the entries for cluster nodes which are no longer part of the cluster. If this is not done then journal table Janitor will not be effective.

local-revisions-janitor-first-run-hour-of-day

Default Value: 2
Valid Values:
Changes Take Effect: After restart

Specifies the hour at which the clean-up task initiates its first run (default = 2, which means 2:00 at night).

local-revisions-janitor-sleep

Default Value: 15
Valid Values:
Changes Take Effect: After restart

Specifies the sleep time of the clean-up task in days (only useful when the clean-up task is enabled, default is 15 days).

synch-delay

Default Value: 2000
Valid Values:
Changes Take Effect: After restart

Specifies the delay in milliseconds after which GRAT node will check for new changes.

Change History

Content under development