This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Configurations Options Reference Manual

[system] Section

12/14/2025

Contents

[system] Section

This section must be called **system**.

consistent-port-selection

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: At the next reconnect. For master Configuration Server, this option must be configured from the configuration files and it must be restarted for the changes to take effect. For proxies, this option can be configured at runtime and it must be specified in the application configuration objects.

When set to `true`, this option implements the following behavior in selecting ports for connections of Configuration Server Proxies to the master Configuration Server, including the connections of backup instances of both master and proxy to their primary peers:

- When a Configuration Server Proxy loses connection to the primary master Configuration Server, to reconnect to the primary backup instance, the proxy will consistently use the port with the same port ID that was used for its initial connection to the primary (specified in the command line). If the port with the same ID is not configured, the default port will be used. If a port with the ID default is not configured, any available port will be used.
- The backup instances of Configuration Servers, both master and proxy, will consistently use the ports marked as **HA Sync** to connect to their primary peers. If **HA Sync** port is not available, the default port will be used. If a port with the ID default is not configured, any available port will be used.

This option applies to the configurations where Configuration Server instances have multiple listening ports. If set to `false` (the default), this feature is disabled.

deferred-requests-expiration

Default Value: `3600` seconds
Valid Values: `0, 1–2147483647`
Changes Take Effect: Immediately

For transaction serialization mode (see **serialize-write-transactions** option), enables expiration of regular clients' deferred requests and specifies the time interval (in seconds) for which deferred requests are kept for further processing. A value of `0` means that that request never expires. If a deferred request cannot be processed within this time interval, processing of the request is cancelled and error response is sent to the client.

This value does not apply to the requests from Configuration Server proxies deferred upon data reload and internally generated requests.

Important

> - Genesys recommends that you not change the default value unless instructed to do so by your Genesys representative.
> - The **serialize-write-transactions** option must be set to `true` for this option to apply.

force-reconnect-reload

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: After next reconnection to database

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

prevent-mediatype-attr-removal

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

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

proxy-load-max

Default Value: `0` (zero)
Valid Values: `0, 1–2147483647`
Changes Take Effect: Immediately

Enables limiting the number of proxy servers concurrently loading and reloading data and specifies the maximum number of Configuration Server Proxies allowed to (re)load data in parallel. A value of `0` (zero, the default) indicates there is no limit on the number of Configuration Server Proxies. If more than the specified number of proxy servers attempt to reload their data concurrently, only requests from the maximum number of servers are processed; requests from the rest of the servers are deferred until other servers have finished loading their data. This enables the excess Configuration Server Proxies (those with deferred requests) to continue serving their clients with unchanged (original) data, and to prevent too many proxy servers from simultaneously disabling their services to reload data and overloading master Configuration Server.

> Important

> The **serialize-write-transactions** option must be set to true for this option to apply.

proxy-load-timeout

Default Value: `600` seconds
Valid Values: `0, 1–2147483647`
Changes Take Effect: Immediately

For transaction serialization mode (see **serialize-write-transactions** option), specifies the time limit during which transactional requests are deferred to avoid interference with a data load by a single Configuration Server Proxy. If set to 0 (zero), there is no limit. If a proxy server fails to complete its data load within the specified time interval since it was authorized, it is allowed to continue loading. However, transaction deferral mode is exited and deferred transactions are processed. If the **proxy-load-max** option is specified, expiration of this interval allows the next proxy server waiting in the queue to start loading its data.

> Important
>
> - The **serialize-write-transactions** option must be set to true for this option to apply.
> - Ensure that this interval is sufficient for the proxies to complete data load, based on the size of the database and the bandwidth of the communication channel between the master Configuration Server and Configuration Server Proxies. Premature termination of the transaction deferral mode allows data change transactions to be processed while the proxy is still loading data. This can cause data inconsistencies in the proxy's data once it completes loading.

serialize-write-transactions

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

Enables (`true`) or disables (`false`; the default) the following functionality:

- Transaction serialization
- Transactions deferral at proxy/backup startup/data (re)load
- Limiting of the number of proxies concurrently loading/reloading data (requires additional option **proxy-load-max**)
- Throttling of data updates (requires additional option **throttle-updates-interval**)

Transaction serialization is the mode of Configuration Server operation that prevents data change transactions from overlapping and potentially causing a loss of data integrity. It involves the deferral of data change requests so that each request can be processed completely, without impacting, or being impacted by other requests.

Transaction serialization mode also defers processing of data change requests for the time when Configuration Server Proxies or backup instance of master Configuration Server are in progress of loading/reloading data from the master primary Configuration Server. At that time, Configuration Server Proxies cannot always correctly process notifications on the data change. These notifications cannot always be correctly applied to partially loaded and not yet fully reconciled dataset. They could be missed or incorrectly applied, resulting in outdated or corrupt data in the proxy's memory. Deferring data changes for the time of data reload prevents this from happening.

> Important
>
> The **serialize-write-transactions** option must be set to true for this option to apply.

For detailed description of this functionality, refer to Transaction Serialization section in *Framework Deployment Guide*.

See also: **deferred-requests-expiration**, **proxy-load-timeout**

skip-annex-validation

Default Value: `0` (zero)
Valid Values: `0` (zero), `1, 16`
Changes Take Effect: Immediately

Specifies if Configuration Server validates the Annex of an object, checking for an empty or duplicate object section. By default, Configuration Server performs a full validation and rejects modifications that can potentially affect data integrity or cannot be displayed properly by Genesys Administrator.

Valid values are:

- `0` (zero, the default)—Full validation is performed, and changes are rejected if an empty section and/or a duplicate section are found.
- 1—Partial validation is performed, and changes are rejected if a duplicate section is found.
- 16—Disables validation completely

> Important
>
> Set this option to 16 only when requested by -Customer Care.

skip-environment-enum-transfer

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

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

throttle-updates-interval

Default Value: `0` (zero)
Valid Values: `0, 1–2147483647`
Changes Take Effect: Immediately

Enables transaction throttling and specifies, in milliseconds, the time interval used to throttle data update (transactional) requests. If a data update request is received before this time interval expires, the request is deferred until the interval expires. Any non-transactional requests received from the same client are also deferred and processed in FIFO (first-in, first-out) order after the deferred request is processed. A value of `0` (zero) disables this option.

> Important
>
> - The **serialize-write-transactions** option must be set to true for this option to apply.
> - When configuring this option, keep in mind that if actual load consistently exceeds the rate specified by this option for a significant time, deferred unprocessed requests will accumulate in the input queue and will be eventually cancelled as defined by the value of the **deferred-requests-expiration** option. To avoid this happening, consider adjusting the **throttle-updates-interval** option accordingly, to account for the expected actual load.

token-authentication-mode

Default Value: `disable`
Valid Values:

`enable`	Token level authentication supported on all ports.
`disable`	Token level authentication disabled on all ports (the default).
`gui-port-only`	Token level authentication supported on GUI-only port, where `user=1`.

Changes Take Effect: At next connection request

Enables or disables token-based authentication of connections to Configuration Server on particular listening ports by setting this option. In essence, this option restricts this functionality at port level.

For more information about token-based authentication of connections to Configuration Server, refer to Secure Communication with Configuration Server in the *Genesys Administrator Extension Deployment Guide*.

token-preambula

Default Value: {PXZ}
Valid Values: Any string of three random characters, enclosed in { } (parentheses), for a total of five characters. For example: {###} If the value is more than 5 characters long, including the parentheses, the default value is used.
Changes Take Effect: At next connection request

Specifies the preamble tag that is attached to the start of a password token by a client wanting to establish a connection to Configuration Server.

For more information about token-based authentication of connections to Configuration Server, refer to Secure Communication with Configuration Server in the *Genesys Administrator Extension Deployment Guide*.

token-tolerance

Default Value: 60
Valid Values: 1–2147483647
Changes Take Effect: Immediately

If GAX and Configuration Server clocks are not synchronized, this option specifies a tolerance time interval (in seconds) before the token start time and after the token end-time. If this option is not set or set to 0 (zero), the default value is used.

Example:

In the following scenario:

- GAX generates a token valid from 12:00:00 to 12:20:00
- The token-tolerance option is set to 60 (the default).

Configuration Server considers the token to be valid from 11:59:00 to 12:21:00.

For more information about token-based authentication of connections to Configuration Server, refer to Secure Communication with Configuration Server in the *Genesys Administrator Extension Deployment Guide*.

token-ttl

Default Value: 1440
Valid Values: 1–2147483647
Changes Take Effect: Immediately

Specifies how long (in minutes) the token is considered valid by Configuration Server.

If this option is set to a positive non-zero integer, the token is valid for the time interval specified by this option, starting from the start time specified by GAX. Note that this option applies only to the duration time of the token; the expiration time of the token cannot be changed.

Example:

- GAX generates a token valid from 12:00 to 1:00.
- If **token-ttl** is set to 60 minutes. Configuration Server considers the token valid from 12:00 to 1:00.
- If **token-ttl** is set to 65 minutes, Configuration Server considers the token valid from 11:55 to 1:00.
- If **token-tolerance** is set to 300 seconds and **token-ttl** is set to 65 minutes, Configuration Server considers the token valid from 11:50 to 1:05.
- If **token-ttl** is not set, or set to 0 (zero), Configuration Server uses the value of the **token_life_in_minAutes** option set in the **[general]** section of the GAX application. If **token_life_in_minutes** is not set or set to 0 (zero) in the GAX application. the default value of this option (**token-ttl**)) is used.

> ### Important
> Genesys recommends that you always use the default value for this option. If necessary, you can set a required value using the token_life_in_minutes option in the GAX application. The value of this option must always be greater than **token_life_in_minutes**.

For more information about token-based authentication of connections to Configuration Server, refer to Secure Communication with Configuration Server in the *Genesys Administrator Extension Deployment Guide*.

token-uuid

Default Value: Empty string
Valid Values: A string of 32 hexadecimal characters arranged in 5 groups separated by hyphens
Changes Take Effect: At next connection request

Specifies the UUID used to generate the symmetrical key using the secret algorithm. If this option is not configured or is an empty string, Configuration Server uses a value generated internally by the primary master Configuration Server for the particular Configuration Database.

The value must consist of 32 hexadecimal characters in groups separated by hyphens; like is:
`<8 hex digits>-<4 hex digits>-<4 hex digits>-<4 hex digits>-<8 hex digits>`

For example: `C7123227-9709-4E64-88F3-74BA83ACE826`

For more information about token-based authentication of connections to Configuration Server, refer to the Secure Communication with Configuration Server in the *Genesys Administrator Extension Deployment Guide*.

x-path-read-improvements

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

If set to `true`, Configuration Server uses the performance improvements for read requests that reads agent login details from Configuration Server. Enabling this option significantly improves the login experience in large environments where a number of agents log in concurrently.