Genesys Mobile Services Deployment Guide

Configuration Options Reference

12/14/2025

Configuration Options Reference

> **Important**
>
> This page provides descriptions and explanations of Genesys Mobile Services-specific options. Refer to the Genesys Mobile Services Options Reference for a full list of options.

Default Configuration Sections

By default, the **Options** tab for your Genesys Mobile Services Application object contains several sections with configuration values.

Services Configuration Sections

Every service you want to provide using this instance of Genesys Mobile Services can have a custom entry created using this format. The default installation provides two examples:

- service.request-interaction
- service.query

The Services and Tools UI will create these options for you.

[chat] Section

This section configures additional chat parameters for the GMS application.

Required Chat Server Options (HA)

Section: endpoints:1	
Option Name	**Option Value**
default	Chat In
Section: settings	
Option Name	**Option Value**
session-restoration-mode	simple
transcript-auto-save	2

[config] Section

Added in 8.5.209.02

Options in the **config** section enable you to manage configuration objects' caching in GMS. By default, only `Route Point` objects are loaded at startup; other objects are not loaded unless you enable the corresponding option. See the [config] section in the *Genesys Mobile Engagement Configuration Options Reference* guide for a detailed list of options.

[log] Section

According to your application and your needs, you can activate the following additional logs for your GMS application. By default, all these log options are set to `false`.

For example:

```
[log]
ChatService=false
ClusterService=false
DataDepotService=false
DistributedJobExecutor=false
DistributedJobQueue=false
SharedService=false
[callback]
log-background-activity=false
```

[log-filter] and [log-filter-data] Section

These sections enable to hide selected attached data in Logs. See Hiding Selected Data in Logs for details and examples about filters.

- Changes take effect: Immediately.

Option	Default	Description
<KV-List-key> Optional	N/A	Describes the filter to hide parts or the totality of the associated string values in the logs. • `copy` • `hide` • `hide-first,<n>` • `hide-last,<n>`

Option	Default	Description
		• `unhide-first,<n>` • `unhide-last,<n>` • `skip` • `tag` (*) • `tag()` (*) • `tag(,)` (*) • `tag(<custom_prefix>, <custom_postfix>)`; for instance `tag(!!!,!!!)` (*) use default system prefix/postfix <# #> **Important** Passwords are automatically hidden in GMS logs.

[log-hidden-attributes] Section

Introduced: 8.5.200

Use this section to hide selected Genesys internal message attributes in Logs. See Hiding Selected Data in Logs for details.

Changes Take Effect: Immediately

Option	Description
<ProtocolName>.<MessageName>	Comma-separated list of message attributes.
<ProtocolName>.<Complex AttributeName>	Comma-separated list of complex attribute's attributes.

Here is a configuration sample, which hides the content of the chat text from the logs while GMS communicates with the Chat Server:

```
[log-hidden-attributes]
FlexChat.EventInfo=Text
FlexChat.MessageText=Text
FlexChat.NoticeText=Text
```

[notification] Section

unsubscribe-delay

Section: notification
Default Value: 0
Valid Values: Any positive integer
Changes Take Effect: Immediately
Introduced: 8.5.109.05

Time in seconds to wait for deleting notification subscriptions. In scenarios where the publish notification and the delete subscription requests are received concurrently, the subscription may be deleted before the notification gets published. If you set this option to a value greater than 0, you will force GMS to wait for the specified duration before deleting the subscription and this will allow the pending push notifications to be sent out.

[ors] Section

Modified in 8.5.107

_ors_lb_strategy

Section: ors
Default Value: circular
Valid Values: circular, linear
Changes Take Effect: After restart

Added in: 8.5.107
Strategy for ORS added to the **Connections** tab of the GMS application.

enable_ors_loadbalancer

Section: ors
Default Value: true since 8.5.107; false previously
Valid Values: true, false
Changes Take Effect: After restart

Enables GMS to send request to the `/hearbeat` URI of ORS to check availability.

max_ors_idle_connection_time

Section: ors
Default Value: 3600
Valid Values: Any integer
Changes Take Effect: After restart

Added in: 8.5.107
Maximum idle time (seconds) for an ORS connection before this connection will be deleted from the load-balancer cache.

ors_loadbalancer_refresh_rate

Section: ors
Default Value: 45000
Valid Values: Integer>=30000
Changes Take Effect: After restart
Discontinued: 8.5.219.03

Refresh rate of the ORS Load balancer in milliseconds. This option value must be greater than or equal to 30,000 (30 seconds). By default, all ORS URL values are checked every 45 seconds.

[port_restrictions] Section

You can control port access to GMS APIs by adding a `port_restrictions` section in the **Options** tab of GMS configuration, at the node level or cluster level. This section is optional and not defined in the default template. The content of this section is a list of key/values, where key is an URI pattern (`/genesys/1/storage/*, /genesys/1/service/*, /genesys/1/service/request-interaction,` and so on), and the `value` is a list of ports or a port range.

Example `[port_restrictions]` section:

Option Name	Option Value	Description
/genesys/1/storage*	80-90	Storage API will be accessible from port 80 to port 90.
/genesys/1/service/*	92-98,100	Services API will be accessible from port 92 to port 98, plus the port 100.

Important

- There are no default values or default option names. You can define various URL patterns; such as `/genesys/1/resource*`, `/genesys/1/resource*`, `/genesys/1/service/*`, `/genesys/1/service/request-interaction`, and so on.
- If the request is sent on another port, an HTTP error `403 Forbidden` occurs.
- The Admin UI and APIs not listed in the `port_restrictions` section will be available on all ports listed in the `port_restrictions` section.

See Restricting Ports for further information about these configuration options. Changes in this section require an update to the `jetty-http.xml` file on all GMS nodes, and then restarting GMS.

[push] Section

Changes take effect: After restart.

The push configuration includes three logical groups of options: general configuration, push provider configuration, and OS-specific message formatting. For more information about providers and OS-specific message formatting refer to Genesys Mobile Services Push Notification Service.

It is possible for some mandatory options to be absent in this section. In this case, the corresponding push type will be disabled (even if enabled using the *push.pushEnabled* option) and a log entry will be created.

Important

For security reasons, if you wish to hide some private keys that are specific to the notification mechanism, you can define sensitive options in a dedicated section.

Common Notification Options

customhttp.url

Section: push
Default Value:
Valid Values: Any valid URL
Changes Take Effect: After restart

Mandatory URL where the notifications will be pushed. The subscriber must provide a URL that will be invoked. GMS posts the payload to this URL (using HTTP POST). The Payload is a JSON object that contains two properties: the `deviceId`, which is the custom id provided at subscription time by the subscriber, and the `message`, which is the notification message.

This option describes the provider configuration used for accessing the target (APPLE APNS service, HTTP address).

You can use the HTTPS scheme without adding the server certificate if you configure the http.ssl_trust_all option to true in the [gms] section.

If you do not use the **http.ssl_trust_all** option, add the server certificate to the Java cacerts.

For example, in a Linux platform:

```
keytool -import -alias genesys -keystore /etc/pki/java/cacerts -file /security/
custom_https_server_certificate.crt -noprompt -storepass changeit
```

defaultSubscriptionExpiration

Section: push
Default Value:
Valid Values: Any integer (>=30)
Changes Take Effect: After restart

Default subscription expiration (in seconds). If the option is not set or if you assign an incorrect value, the default value (30) will be used.

filtering_chat_events

Section: push
Default Value: Notice.TypingStarted,Notice.TypingStopped
Valid Values:
Changes Take Effect: After restart

Comma-separated list of the following events:

- `Notice.TypingStarted`
- `Notice.TypingStopped`
- `Notice.Joined`
- `Notice.Left`

- `Notice.PushUrl`
- `Notice.Custom`
- `Message.Text`

A comma-delimited list that sets the default value for the `_filtering_chat_events` service parameter. By default, this list is set to "`Notice.TypingStarted,Notice.TypingStopped`".

pushEnabled

Section: push
Default Value: comet
Valid Values: android, gcm, ios, httpcb, orscb, customhttp, fcm,comet
Changes Take Effect: After restart.
Modified: 8.5.113.10, 8.5.112.05

A comma-delimited list of strings that describe the enabled push types. Currently, the following push types are supported:

- **android**
- **gcm**
- **ios**
- **httpcb**
- **orscb**
- **customhttp**
- **fcm** (starting in 8.5.112.05)
- **comet** (starting in 8.5.103.10)

Any other push type will be ignored. If an option value is not set, then it will be handled as empty string option value (that is, push will be disabled for all supported types and the push service will not work).

> **Note:** Starting in 8.5.103.10, this option requires the default value (**comet**) even if you do not enable push notifications. If you enable push notifications, use one of the above valid values.

httpcb.connection_max_connections_per_route

Section: push

Default Value: 20
Valid Values: Any integer >= 2
Changes Take Effect: After restart.

The maximum allowed number of simultaneously opened connections for one route. Default value (used if option not set or incorrect) 20.

httpcb.connection_timeout

Section: push
Default Value: 5
Valid Values: Any positive integer
Changes Take Effect: After restart.

The http connection timeout in seconds. Default value is 5

httpcb.max_connections_total

Section: push
Default Value: 200
Valid Values: Any integer >= 5
Changes Take Effect: After restart.

The maximum allowed total number of simultaneously opened connections. Default value (used if option not set or incorrect) 200

localizationFileLocation

Section: push
Default Value:
Valid Values:
Changes Take Effect: After restart.

Location of the file containing the list of localized messages.

Apple Notification Options

Note: Please see the relevant documentation at developer.apple.com for information about OS-Specific message formatting options. Note that if no alert-related options are specified, the *alert* dictionary entry will not be included in the JSON sent to the Apple device.

apple.alert

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

Enables an iOS standard alert and defines the text of this alert with two buttons: **Close** and **View**. If the user taps **View**, the application is launched. If this option is null, the **alert** property will not be added to the notification.

apple.alertMessage.action-loc-key

Section: push
Default Value:
Valid Values: Any string
Changes Take Effect: After restart

If set (not null), is used as an *action-loc-key* entry in the alert dictionary (iOS-specific).

apple.alertMessage.body

Section: push
Default Value:
Valid Values: any String, may be null(=absence of option)
Changes Take Effect: After restart.

If set, defines a body entry in the alert dictionary (iOS-specific).

apple.alertMessage.launch-image

Section: push

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

If set, is used as the *badge* entry in the *aps* dictionary (iOS-specific).

apple.alertMessage.loc-argnames

Section: push
Default Value:
Valid Values: Any string
Changes Take Effect: After restart

If set (not null), used as a *loc-args* entry in the alert dictionary (iOS-specific).

apple.alertMessage.loc-key

Section: push
Default Value:
Valid Values: Any string
Changes Take Effect: After restart

If set (not null), used as *loc-key* entry in the alert dictionary (iOS-specific).

apple.title

Section: push
Default Value: Empty string
Valid Values: String
Changes Take Effect: After restart.

Apple Notification title. If not specified, GMS sends a blank title.

apple.badge

Section: push
Default Value: 0
Valid Values: any, may be null (=not set)
Changes Take Effect: After restart.

If set, number used as *badge* entry in the *aps* dictionary (iOS-specific). If this property is absent, any badge number currently shown is removed. If not set, the *badge* entry will not be part of the push notification.

apple.content-available

Section: push
Default Value:
Valid Values: Any string
Changes Take Effect: After restart

Set this key with a value of 1 to indicate that new content is available and let the remote notification act as a silent notification. This is used to support Newsstand apps and background content downloads. Newsstand apps are guaranteed to be able to receive at least one push with this key per 24-hour window.

When a silent notification arrives, iOS wakes up your app in the background so that you can get new data from your server or do background information processing. Users aren’t told about the new or changed information that results from a silent notification, but they can find out about it the next time they open your app.

apple.keystore

Section: push
Default Value:
Valid Values: Valid file path
Changes Take Effect: After restart.

keystore location (path to file) for iOS push notifications

apple.keystorePassword

Section: push
Default Value:
Valid Values: Not null (but may be empty string)
Changes Take Effect: After restart.

Password to access keystore. If the password is incorrect, the attempts to push messages will fail with the corresponding log entries.

apple.sound

Section: push
Default Value:
Valid Values: any String, may be null(=absence of option)
Changes Take Effect: After restart.

If set, used as *sound* entry in the *aps* dictionary (iOS-specific). Use the name of a sound file in the application bundle. The sound in this file is played as an alert. If the sound file doesn't exist or you set this value to **default**, the default alert sound is played. If not set, the corresponding entity will not be added to the notification.

debug.apple.keystore

Section: push
Default Value: No default value
Valid Values: Valid file path
Changes Take Effect: After restart

Keystore location (filepath) for iOS push notifications. This option applies to notifications whose debug value is set to true.

debug.apple.keystorePassword

Section: push
Default Value: No default value
Valid Values: Not null or empty string
Changes Take Effect: After restart

Password to access keystore. If the password is incorrect, the attempts to push messages will fail with the corresponding log entries. This option applies to notifications whose debug value is set to true.

Android Notification Options

android.collapseKey

Section: push
Default Value:
Valid Values: not empty
Changes Take Effect: After restart.
Discontinued: 8.5.114.09

An arbitrary string that is used to collapse a group of like messages when the device is offline, so that only the last message gets sent to the client. This is intended to avoid sending too many messages to the phone when it comes back online. Note that since there is no guarantee of the order in which messages get sent, the "last" message may not actually be the last message sent by the application server

android.delayWhileIdle

Section: push
Default Value: false
Valid Values: true, false
Changes Take Effect: After restart.
Discontinued: 8.5.114.09

If included and true, indicates that the message should not be sent immediately if the device is idle. The server will wait for the device to become active (only 1 last message will be delivered to device when it becomes active). Default (if not specified) - false;

android.gcm.apiKey

Section: push
Default Value:
Valid Values: Valid Google api Key. See Google GCM description.
Changes Take Effect: After restart.
Discontinued: 8.5.114.09

Valid Google API Key. See Google CDM description. Please see https://developers.google.com/cloud-messaging/gcm

android.gcm.retryNumber

Section: push
Default Value: 2
Valid Values: Any integer
Changes Take Effect: After restart.
Discontinued: 8.5.114.09

Retry attempts (in case the GCM servers are unavailable).

android.senderAccountType

Section: push
Default Value:
Valid Values: not null, may be empty
Changes Take Effect: After restart.
Discontinued: 8.5.114.09

Specified when initializing c2dm push service

android.senderEmail

Section: push
Default Value: @gmail.com
Valid Values: valid mail (sender account registered in Google service)
Changes Take Effect: After restart.
Discontinued: 8.5.114.09

Valid name of mail account. The notifications will be sent from behalf of this account. After signing up for C2DM, the sender account will be assigned the default quota, which currently corresponds to approximately 200,000 messages per day.

android.senderPassword

Section: push

Default Value:
Valid Values: valid password of registered account
Changes Take Effect: After restart.
Discontinued: 8.5.114.09

Password of account

android.source

Section: push
Default Value:
Valid Values: not empty
Changes Take Effect: After restart.
Discontinued: 8.5.114.09

Specifying when sending push notification service

android.ssl_trust_all

Section: push
Default Value: false
Valid Values: true, false
Changes Take Effect: After restart.
Discontinued: 8.5.114.09

If included and true, indicates that any SSL certificate provided during establishing https connection to https://www.google.com/accounts/ClientLogin and https://android.apis.google.com/c2dm/send addresses are considered valid, regardless of their presence in keystore/truststore used by environment. Default value - false. Please note that setting this option to true is highly unadvised. The most correct way is to configure the security system to permit the actually received certificates.

android.unavailability_retry_timeout

Section: push
Default Value: 120
Valid Values: Any positive integer
Changes Take Effect: After restart.
Discontinued: 8.5.114.09

This parameter specifies the default timeout (in seconds) to wait before Google C2DM service can

be accessed again if the request returned the 503 code (Service unavailable). Please note, that this value is ignored if the 503 response from Google contains valid Retry-After header. Default value for this parameter is 120 (used if value not set or incorrect).

Firebase Cloud Messaging

Introduced in: 8.5.112

Due to recent changes in Google Cloud Messaging, GMS now supports Firebase Cloud Messaging (FCM). To configure Native Push Notification through Firebase Cloud Messaging, you can either specify an apiKey or create a dedicated section to secure passwords (recommended for production environments).

Development

```
[push]
fcm.apiKey=<serverKey>
pushEnabled=fcm
```

Production

```
[push]
fcm=fcmsection
pushEnabled=fcm

[fcmsection]
password=***** (<serverKey>)
```

fcm.apiKey

Section: push
Default Value: No default value
Valid Values: String
Changes Take Effect: After restart
Introduced: 8.5.112.05

Valid Firebase Cloud Messaging API key. Refer to the official documentation for further details.

debug.fcm.apiKey

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

Introduced: 8.5.114.09

Valid Firebase Cloud Messaging API key to use if debug=true.

You can also define title and body messaging for the event received at the provider event level detailed below below.

fcm.title

Section: push
Default Value: No default value
Valid Values: Any string
Changes Take Effect: After restart
Introduced: 8.5.114.09

Firebase Cloud Messaging title for an event defined at the provider level.

more...

fcm.body

Section: push
Default Value: No default value
Valid Values: Any string
Changes Take Effect: After restart
Introduced: 8.5.114.09

Firebase Cloud Messaging body message for an event defined at the provider level.

more...

Windows Notification options

wns.clientSecret

Section: push
Default Value:
Valid Values:
Changes Take Effect: After restart

The secret key associated to the application. See Microsoft Official documentation.

wns.notificationType

Section: push
Default Value:
Valid Values:
Changes Take Effect: After restart

Type of notification that GMS will send to the Windows application. This value must match the `X-WNS-Type` header. For example, you can specify a toast notification by setting this option to `wns/toast`.

wns.sid

Section: push
Default Value:
Valid Values:
Changes Take Effect:

Unique identifier for your Windows Store app. See Microsoft Official documentation.

wns.xmlTemplate

Section: push
Default Value:
Valid Values:
Changes Take Effect: After restart

XML string that defines the notification. For example, to set up a toast notification, you can set this option to:

```
<toast><visual><binding template="ToastText01"><text
id="1">bodyText</text></binding></visual></toast>
```

push.provider options

Each provider can contain 2 *channels* for message sending - **production** and **debug** for each target

type. The provider-affiliated options enlisted above describe the production channel. For each provider-related option **<option-name>** the sibling option can be provided with name **debug.<option-name>**. Such options will describe the provider-specific configuration of debug channel for corresponding target type. The debug channel will be enabled for enabled target type only if all mandatory options will be specified for debug channel. The OS-message formatting options do not have production-debug differentiation.

push.provider.*providername* Section

It is possible to create providers by adding **push.provider.*providername*** sections which contain the appropriate credential configuration options that are associated with a given provider. This allows you to control and isolate notifications and events between a given provider and the associated services/applications that are using it. This type of provider name section can only contain provider-related options (as listed in **push** section). All providers are isolated - if the option is not specified in provider's section, then it is not specified. If a mandatory option is missing then the corresponding target type will not be enabled, even if that type is present in the **pushEnabled** option.

Please note that we have the following restriction on **providername**: it may only contain alphanumeric characters, the underscore (_), and the minus sign (**-**).

push.provider.event Section

You can define the event definitions associated across providers by adding your **push.provider.event** section, and then setting the appropriate OS-specific attribute options within. This will allow you to add OS-specific attributes to a published event message that is going to any provider’s push notification system. This section can contain OS formatting-related options. All other options will be ignored. For more information about providers and OS-specific message formatting refer to Genesys Mobile Services Push Notification Service.

push.provider.event.*eventname* Section

You can define the events associated across providers by adding a custom push.provider.event.**eventname** section, and then setting the appropriate OS-specific attribute options within. This will allow you add OS-specific attributes to a published event message that is going to a specific channel for given group of events tags.

- This section can contain OS formatting-related options.
- All other options will be ignored.

> **Important**
>
> For more information about providers and OS-specific message formatting, see Push Notification Service.

For instance, you can create a push.provider.event.chat section to define options for chat events. The following configuration samples show how to configure iOS chat push alert text for chat events.

Configuring iOS Chat Push Alert Text Without Localization

1. Edit your GMS application (with Configuration Manager for example) and select the **Options** tab.
2. Create a `push.provider.event.chat.newagentmessage` section.
3. Click **New** to set the `apple.alert` parameter to an accurate value; for instance, `New message from Agent`.

Configuring iOS Chat Push Alert Text Using Localization

1. Edit your GMS application (with Configuration Manager for example) and select the **Options** tab.
2. Create a `push.provider.event.chat.newagentmessage` section.
3. Click **New** to set the `apple.alertMessage.loc-key` parameter to `CHAT_NEW_AGENT_MESSAGE`.
4. Click **New** to set the `apple.alertMessage.action-loc-key` parameter to `ACTION_KEY`.

> **Important**
>
> `CHAT_NEW_AGENT_MESSAGE` and `ACTION_KEY` are keys to lookup the string values for the current language in the `Localizable.strings` resource of the iOS application. See also the official Apple documentation about Localized Formatted Strings.

push.provider.*providername*.event.*eventname* Section

You can define the event definitions associated with given provider by adding your push.provider.*providername*.event.**eventname** section, and then setting the appropriate OS-specific attribute options within. This will allow you add OS-specific attributes to a published event message that is going to a specific provider and channel for given group of events tags. This section can contain OS formatting-related options. All other options will be ignored. For more information about providers and OS-specific message formatting refer to Genesys Mobile Services Push Notification Service.

[resources] Section

patterns_list_name

Section: resources
Default Value: GMS_Patterns
Valid Values: Valid CME name for List object
Changes Take Effect: Immediately upon notification.

Name of the configuration object (with type List), which holds the configuration of patterns and pattern groups. For further details, see Creating and configuring a pattern list.

resources_list_name

Section: resources
Default Value: GMS_Resources
Valid Values: Valid CME name for List object
Changes Take Effect: Immediately upon notification.

Name of the configuration object (with type List), which holds the configuration of resources and resource groups. For further details, see Creating and configuring a resource list.

user_control

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

This option enables GMS to control resource access based on the `gms_user` header passed in the GMS request. This option is dynamic.

List Object Options

Each section in the Annex is a group that should have distinct list options specified. Changes take effect: Immediately.

Option	Default	Description
_allocation_strategy RANDOM, LOCAL, CLUSTER Optional	RANDOM	Supported strategies: • RANDOM—Allocate a randomly selected resource from the group. No reservations or locks are made, so the same resource can be selected by different users at the same time. • LOCAL—A resource is allocated from the group and reserved/locked, so that only one user can hold it at the time. For the resource to return to the group it should be released either by the corresponding API call or by a timeout.

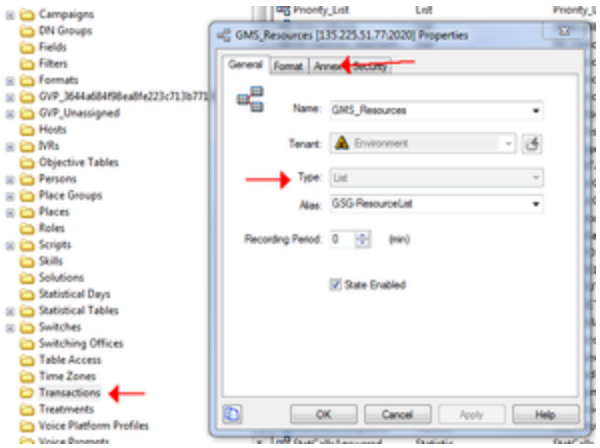
Option	Default	Description
		• CLUSTER—A resource is allocated from the group and reserved/locked through the GSG cluster, so that only one user can hold it at the time. For the resource to return to the group it should be released either by the corresponding API call or by a timeout.
_booking_expiration_timeout Integer (s) Optional	30	Determines the maximum amount of time, in seconds, that a resource may be allocated. If the resource is not released before this time limit elapses, it is automatically returned to the pool of available resources. This option is used with the LOCAL and CLUSTER allocation strategies.
_backup_resource String Optional	String	The resource returned if there are no regular resources available. This option is used with the LOCAL and CLUSTER allocation strategies.

List Entries

Changes take effect: Immediately.

Option	Default	Description
All keys not starting with # or _ String Optional	N/A	The value is put into the pool of resources. The option name may be anything (since that value is not currently used).

The following screenshot shows an example of an application object configured in Configuration Manager.



Example

```
[Dnis_Pool]
 _allocation_strategy = LOCAL
 _booking_expiration_timeout = 20
 dnis1 = 1-888-call-me1
 dnis2 = 1-888-call-me2
 dnis3 = 1-888-call-me3
```

Note: For testing purposes, Genesys recommends that you include at least three numbers in the pool. If only a single number is defined in the pool, when the API call is made, that number is allocated for 30 seconds (default). If another API call is made before the number is returned to the pool, an error will occur. Alternatively, if using a single number, use `_allocation_strategy = RANDOM`.

[server] Section

Modified in 8.5.107

_ors

Section: server
Default Value:
Valid Values:
Changes Take Effect: Immediately

Comma-separated list of ORS URLs.

```
http://host1:port1,http://host2:port2
```

This list will be used for all services sections and can be overridden in each service.

_ors_lb_strategy

Section: server
Default Value: circular
Valid Values: circular, linear
Changes Take Effect: Immediately

Strategy for the ORS load balancer in the server section and service sections; this value can be overridden in each service. Supported values are: `circular` or `linear`.

access_code_prefix

Section: server
Default Value:
Valid Values: Any integer
Changes Take Effect: Immediately

This value is a range of `access_code`; the value must be unique for each GMS node across the cluster. GMS will randomly choose within this range the `access_code_prefix` that it will associate as the prefix for `access_code`. If the option is not present, GMS will use the `nodeId` value instead. An example range is `455,456-458` where the prefix can be `455`, `456`, `457`, or `458`.

dateFormat

Section: server
Default Value:
Valid Values:
Changes Take Effect: Immediately

The string used to format dates. The string syntax should match the expectations of the java class `java.text.SimpleDateFormat`. See Simple Date Format for details.

external_url_base

Section: server
Default Value:
Valid Values: http://<hostname>:<port>/ or https://<hostname>:<port>/
Changes Take Effect: Immediately

Specifies the external URL used by the Storage Service to allow the retrieval of a binary attachment. Configure this option in the case of a Load Balancer deployment.

The valid value is http://<hostname>:<port>/, where:

- <hostname> is used by the cluster service to identify a node
- <port> is used by the cluster service to identify a node.

The <port> value must be the same as the GMS port described in the jetty configuration file, otherwise, an alarm will be displayed in Solution Control Interface (SCI) and GMS will stop.

gsgadmin_redirect

Section: server
Default Value: default
Valid Values:
Changes Take Effect: Immediately

Configures the host and port to use in the redirection message that is sent by GSG Admin upon logout process. In a load balancing deployment, you should set up this option to make sure that GMS redirects to the Load Balancer address instead of the local GMS.
The possible values for this option are the following:

- default—Redirects to the local GMS instance (default behavior).
- external_url_base—Uses the value of external_url_base for the redirection.
- <host>:<port>—Specifies another URL to use for the redirection.

Limitation: Internet Explorer may not correctly depict the port redirection set in external_url_base.

max-sessions

Section: server

Default Value: 9999
Valid Values: Any integer
Changes Take Effect: Immediately

Maximum number of concurrent sessions for the Service Management UI.

node_id

Section: server
Default Value: 1
Valid Values:
Changes Take Effect:

Specifies a two digit number that should be unique in the GMS deployment. It is used in the generation of DTMF access tokens.

Cluster Service options

app_name

Section: server
Default Value:
Valid Values: Any valid URL
Changes Take Effect: Immediately

Web application "context" path.

web_host

Section: server
Default Value: Result of `InetAddress.getLocalHost()`
Valid Values: Valid host name
Changes Take Effect: Immediately

The default `InetAddress.getLocalHost()` value will be used in the most cases. Change this configuration value if you have issues obtaining the local name when your environment has

multiple network interfaces. In this scenario, to ensure GMS internode communication, set this option's value to the IP Address used by the Jetty interface (which is not configurable).

This option is required for internode communication.

web_port

Section: server
Default Value: 80
Valid Values: Valid TCP port; for HTTPS internode communication, 8443 or check either your jetty configuration or restriction port
Changes Take Effect: Immediately

Sets a port different from the port that GMS uses. Note: GMS uses port 8080, which can be changed in the `jetty-http.xml` file. This option can be used in the case of proxy role of the customer to forward requests.

At startup, GMS checks that a GMS is available on the port specified by `web_port`. If a GMS is not available, the web_port option alarm (EventId 2002) is thrown.

Required to ensure the GMS internode communication.

web_scheme

Section: server
Default Value: http
Valid Values: http or https
Changes Take Effect: Immediately

Scheme of the internal URL to `https` if GMS jetty is configured to support only SSL/TLS for one node or for a cluster of nodes.

Optional, required for GMS internode communication.

max-file-upload

Section: server
Default Value: 5000000

Valid Values: Long (bytes)
Changes Take Effect: After restart

Allowed maximum size before uploads are refused.

Configuration Use Cases for web_host and Admin UI

In scenarios that involve internode communication, the value of the `web_host` option can determine the successful display of the GMS nodes status in the Admin UI. Check the examples below and edit this option accordingly.

Use case	Action	Comment
The Configuration Server hosts do not have IP addresses and no DHCP has been setup, or you cannot resolve the hostname for any other reason	Set the `web_host` option to the node's IP address for **each** GMS node	In the Admin UI, the node status will be `true` but the `node_hostipaddress` field in the IP address response will be: `<not provided>`
The Configuration Server hosts do not have IP addresses and the GMS host includes several network interfaces	Set the `web_host` option to the node's IP address for **each** GMS node	In the Admin UI, the node status will be `true` but the `node_hostipaddress` field in the IP address response will contain the IP address of another network interface of the host.
The Configuration Server hosts have IP addresses	N/A	In the Admin UI, the node status will be `true` and the `node_hostipaddress` field in the IP address response will contain the correct IP address.

[service.*servicename*] Section

You can create customized services by adding your service.*servicename* section, and then setting the appropriate options within. Additional options vary depending on the type of service being created. For more information, refer to documentation for the corresponding service in the Genesys Mobile Services API Reference.

For a list of the available options, refer to the Service option reference page.

[stat.*statname*] Section

This section defines Stat Server statistics that can be opened at startup by listing them in the [reporting] startup-statistics configuration option. You can also subscribe to these statistics using the Stat Service API. In either case, Genesys Mobile Services will initialize the statistics, start collecting the data from Stat Server, and place that data in the GMS cache.

Please note that:

- The cache is global and common to all GMS instances.
- The statistics that are not used are removed and closed by a scheduled function every 10 minutes.

filter

Section: stat.statname
Default Value: No default value
Valid Values: Any string
Changes Take Effect: After restart

The business attribute value to use to filter the results.

metric

Section: stat.statname
Default Value: No default value
Valid Values: Any string
Changes Take Effect: After restart

The name of the metric, for example, **TotalLoginTime**. This option defines a Stat Server statistic that can be opened at startup by listing it in the [reporting] startup-statistics configuration option.

notificationMode

Section: stat.statname
Default Value: No default value
Valid Values: NoNotification, Reset, or Immediate
Changes Take Effect: After restart

Notification mode. Mandatory.

objectId

Section: stat.statname
Default Value: No default value
Valid Values: Any string
Changes Take Effect: After restart

Statistic object ID.

objectType

Section: stat.statname
Default Value: No default value
Valid Values: Any string
Changes Take Effect: After restart

Statistic object type; for example, **Agent**.

tenant

Section: stat.statname
Default Value: No default value
Valid Values: Any string
Changes Take Effect: After restart

Tenant name; for example, **Environment**.

tenantPassword

Section: stat.statname
Default Value: No default value
Valid Values: Any string
Changes Take Effect: After restart

Tenant password.

Example

```
[reporting]
startup-statistics=stat1,stat2

[stat.stat1]
metric=TotalLoginTime
notificationMode=NoNotification
objectId=KSippola
objectType=Agent
tenant=Environment
filter=Bronze

[stat.stat2]
metric=ExpectedWaitTime
notificationMode=NoNotification
objectId=9002@SIP_Switch
objectType=Queue
tenant=Environment
```