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.

Genesys Mobile Services Deployment Guide

Enabling Basic Authentication

4/30/2025

Contents

Enabling Basic Authentication

Modified in 8.5.108

HTTP Basic Authentication is a method for an HTTP client to provide a user name and a user password for each HTTP request where a resource needs access control.

GMS supports Basic Authentication on the following services:

- Storage service
- Notification service
- Callback service
- and all services that have a section (with the prefix **`service.`**) in the GMS application.

> **Important**
>
> Best practice is to use Basic Authentication over HTTPS.

Configuration

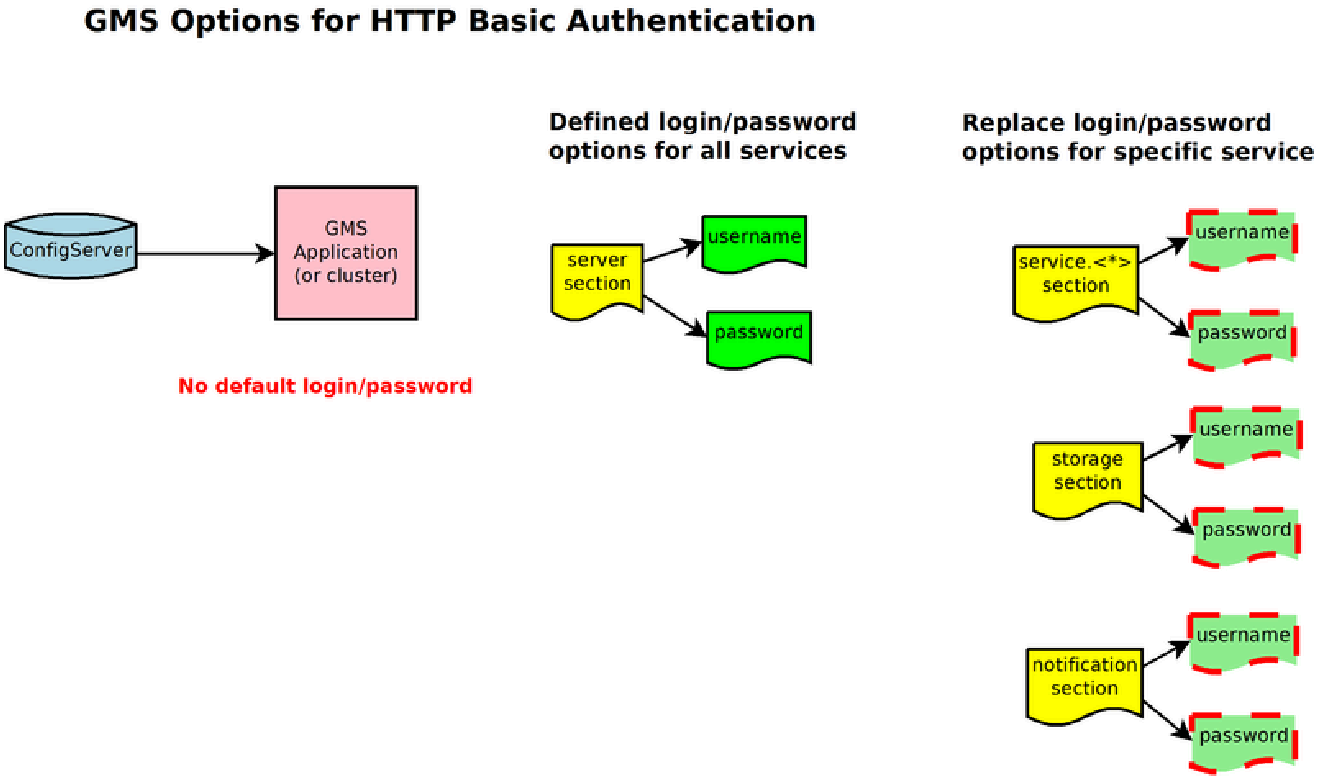
By default, the Basic Authentication feature is turned off. The following sections and options must be set in the GMS application in order to turn on this feature.

> **Important**
>
> Basic Authentication options are taken into account dynamically.

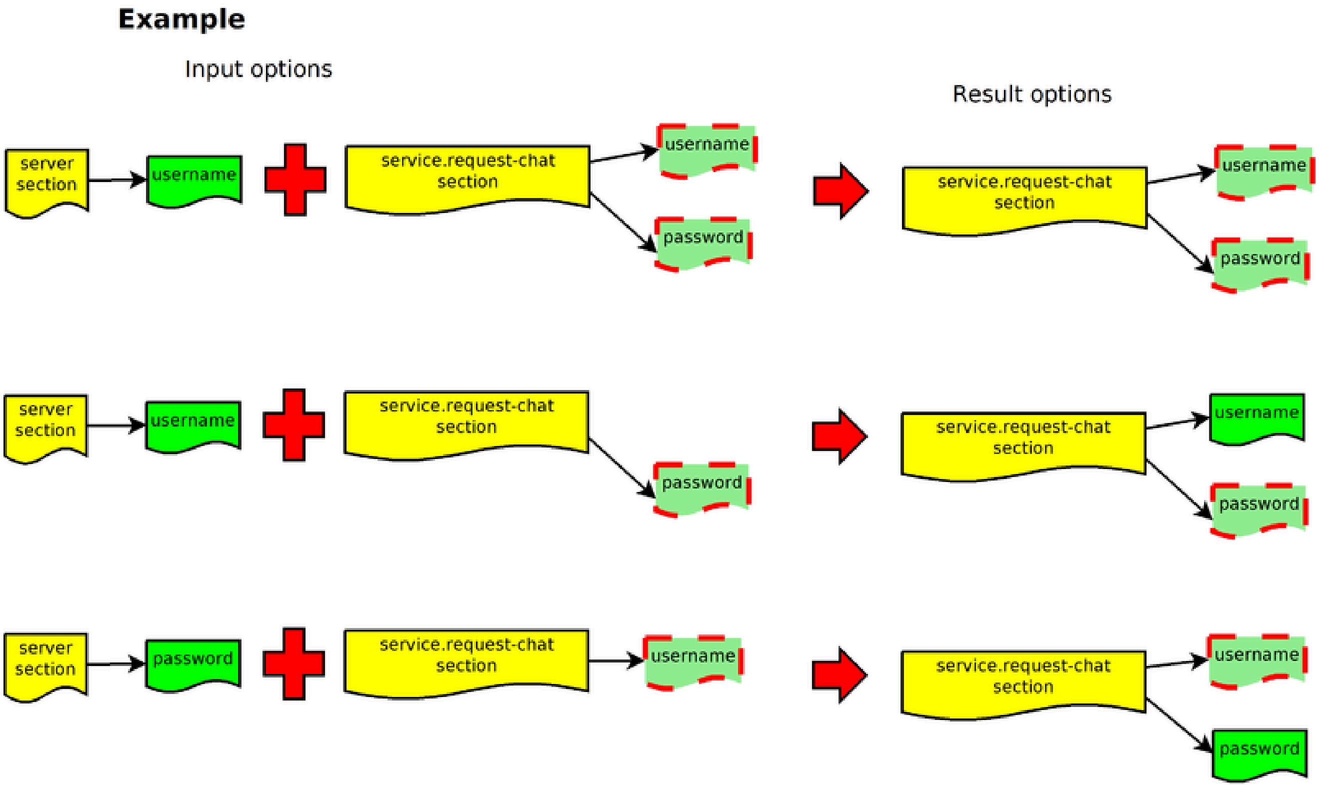
Section	Option	Supersedes	Description
server	realm		Defines the authentication scheme. The default value is `Genesys Application Configuration Needed.`
server	username		Defines a global username for all services. Note: Without the password option, no authentication is effective.

Section	Option	Supersedes	Description
server	password		Defines a global password for all services. With this option, Basic Authentication is turned on for all services.
service.*	username	server/username	Defines a specific username for one service. Note: Without the password option in the same service section, the server section password is used. If there is no server section password, no authentication is applied.
service.*	password	server/password	Defines a specific password for one service.
callback	username	server/username	Defines a specific username for the callback service. This option is not taken into account for other callback API URLs which still use **`service.*`** configuration (if defined). Note: Without the password option in the same service section, the server section password is used. If there is no server section password, no authentication is applied.
callback	password	server/password	Defines a specific password for the callback service.
storage	username	server/username	Defines a specific username for the storage service. Note: Without the password option in the same service section, the server section password is used. If there is no server section password, no authentication is applied.
storage	password	server/password	Defines a specific

Section	Option	Supersedes	Description
			password for the storage service.
notification	username	server/username	Defines a specific username for the notification service. Note: Without password option in the same service section, the server section password is used. If there is no server section password, no authentication is applied.
notification	password	server/password	Defines a specific password for notification service.

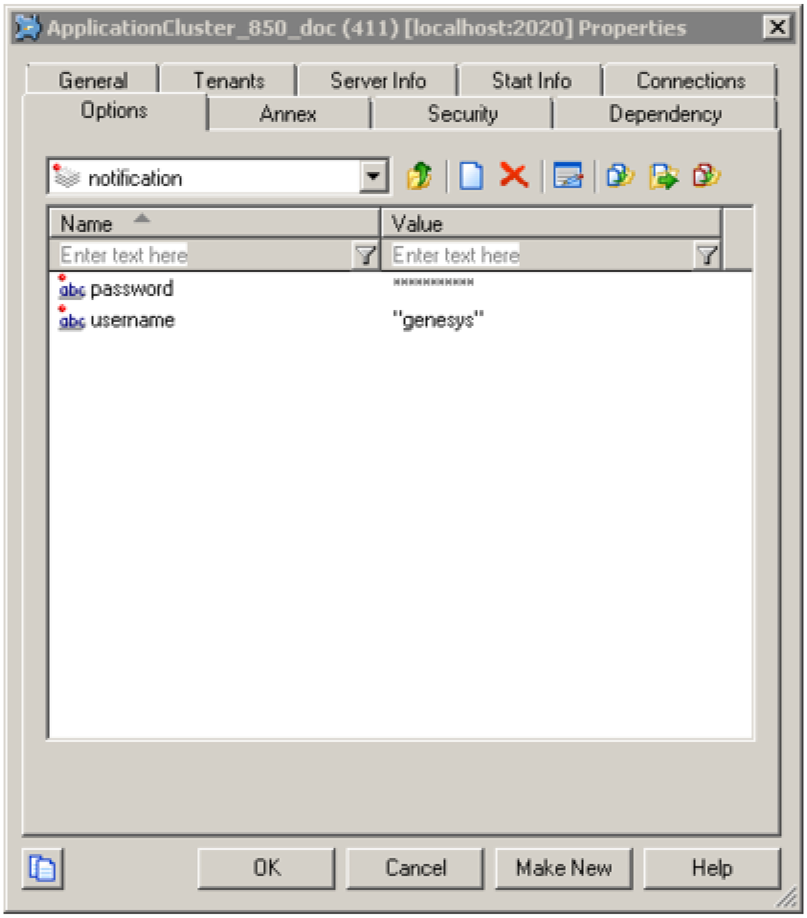

GMS Options for HTTP Basic Authentication
ConfigServer
GMS Application (or cluster)
No default login/password
Defined login/password options for all services
server section
username
password
Replace login/password options for specific service
service.<*> section
username
password
storage section
username
password
notification section
username
password

Precedence Example



Configuration Option Examples

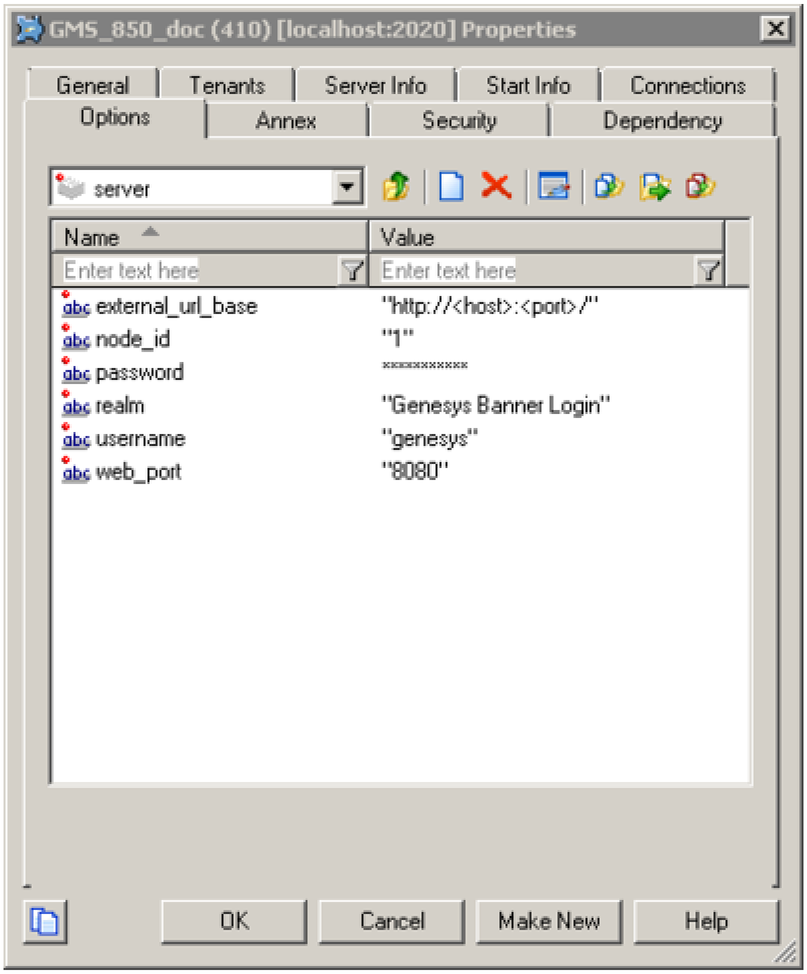
Basic Authentication Username and Password for Notification API:



notification

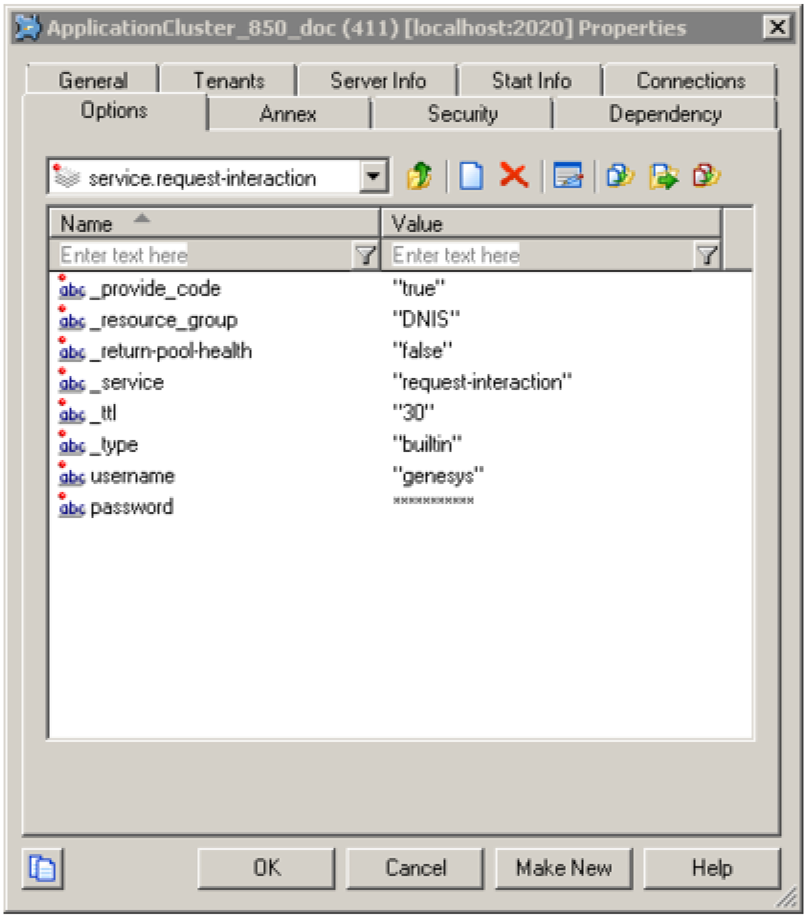
Name	Value
password	**********
username	"genesys"

Basic Authentication Username and Password for GMS Node API:



Name	Value
external_url_base	"http://<host>:<port>/"
node_id	"1"
password	**********
realm	"Genesys Banner Login"
username	"genesys"
web_port	"8080"

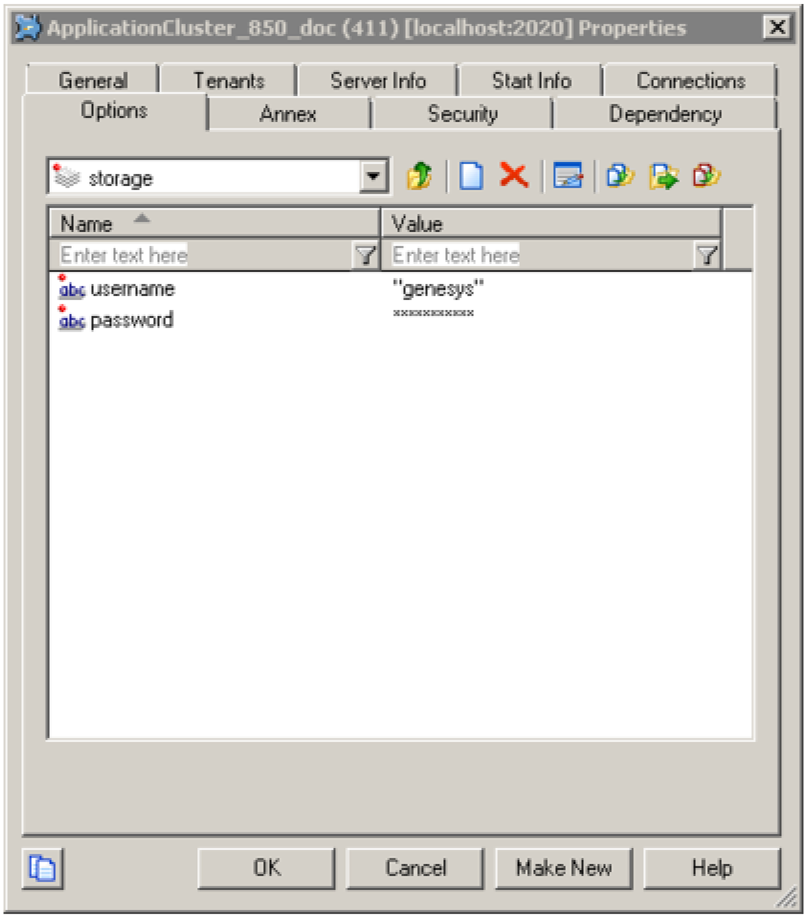
Basic Authentication Username and Password for Service API:



service.request-interaction

Name	Value
_provide_code	"true"
_resource_group	"DNIS"
_return-pool-health	"false"
_service	"request-interaction"
_ttl	"30"
_type	"builtin"
username	"genesys"
password	**********

Basic Authentication Username Password for Storage API:



storage

Name	Value
username	"genesys"
password	**********

Digital Channels API

Starting in 8.5.108, Basic Authentication is supported for the Digital Channels API. You can configure Basic Authentication for your GMS application using the options described above and these settings will apply to all of your services; or, you can turn Basic Authentication on and off on the Digital Channels channel or service level independently from GMS.

For compatibility reasons, Basic Authentication for Digital Channels API is turned off by default. To enable this feature, create the `disable_authentication` option in the appropriate media section (chat or email) and set this option to `false`.

```
disable_authentication=false
```

By default, `disable_authentication=true` and this disables Basic Authentication for Digital Channels API even if you configure Basic Authentication in your GMS configuration.

You can also define and override the `username` and `password` options either in `server`, media, or media service sections. Refer to Digital Channels API configuration for additional details. .

Client Side

When Basic Authentication is turned on from the GMS server-side, the client must manage the HTTP Authentication header to set the username and password in the Authorization header. Only HTTP Basic Authentication is supported. The header request for authentication should look like the following (credential is a string with a specific format [username:password], and base64 encoded):

```
Request
> GET /genesys/1/storage/id HTTP/1.1
> Host: localhost:8080
> Accept: */*
> Authorization: Basic ZGVmYXVsdDpwYXNzd29yZA==

Response
< HTTP/1.1 200 OK
< Date: Thu, 13 Feb 2014 14:44:14 GMT
```

If the authentication fails, the response looks like this:

```
Request
> GET /genesys/1/storage/id HTTP/1.1
> Host: localhost:8080
> Accept: */*
> Authorization: Basic ZGVmYBVsdDpwYXNzd29yZA==

Response
< HTTP/1.1 401 Unauthorized
< Date: Thu, 13 Feb 2014 14:47:55 GMT
< WWW-Authenticate: Basic realm="Genesys Application Configuration Needed"
< Content-Length: 0
```

Example:

Configuration Manager is configured for the `service.request-interaction` section using the following basic authentication parameters:

- username = genesys
- password = genesys

Request without credential:

```
POST /genesys/1/service/request-interaction HTTP/1.1
Host: localhost:8080
Accept: */*
Content-Length: 40
Content-Type: application/x-www-form-urlencoded
```

Response with the authentication error:

```
HTTP/1.1 401 Unauthorized
Date: Thu, 13 Mar 2014 07:55:38 GMT
WWW-Authenticate: Basic realm="Genesys Application Configuration Needed"
```

The same request with credential:

```
POST /genesys/1/service/request-interaction HTTP/1.1
```

```
Authorization: Basic Z2VuZXN5czpnZW5lc3lz
Host: localhost:8080
Accept: */*
Content-Length: 40
Content-Type: application/x-www-form-urlencoded
```

Response of the request:

```
HTTP/1.1 200 OK
Date: Thu, 13 Mar 2014 07:55:55 GMT
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: application/json;charset=UTF-8
{"_access_code":"152606","_expiration_time":"29","_id":"413-ac85eb82-3e5e-414e-9ed2-08392320f234",
 "_access_number":"6504664630"}
```

DFM Configuration

When using Basic Authentication, you must also update DFM in order to protect the username/password.

1. In Configuration Manager, locate and open the Application object for your Orchestration Server (ORS).
2. Select the *Options* tab.
3. Add a new section `dfm.<server_name>`.
4. Add the following options and values:
   - `username`, value = `genesys1`
   - `password`, value = `password1`
   - `maxage`, value = `60` (optional)
   - `maxstale`, value = `60` (optional)
5. Repeat Steps 3 and 4 for each server.
6. Save the ORS application object and restart ORS.

Important

If the username/password is changed in GMS sections (`server`, `storage`, `notification`, `service[s]`), the username/password must also be changed in ORS DFM accordingly. For example, if you set username/password in `server` section, you can use the same username/password for all GMS DFM in ORS (if you change the GMS username/password, you must also change it in ORS DFM for GMS). If you set a specific username/password for Service, Storage, or Notification API rather than using the main one (in `server` section), you must also change the settings in each GMS DFM in ORS in order to manage different username/passwords.

Stat Service API

Two access interfaces are available for the Stat Service API.

One interface is for external access with Basic Authentication.

Example:

```
curl --request POST \
  --url http://demosrv-gme.genesyslab.com/genesys/1/statistic \
  --header 'authorization: Basic ZGVmYXVsdDpwYXNzd29yZA==' \
  --header 'content-type: application/x-www-form-urlencoded' \
  --data objectId=KSippola \
  --data objectType=Agent \
  --data tenant=Environment \
  --data metric=TotalLoginTime
```

And the other interface is for internal usage (that is, internal access without authentication, for instance, between an ORS strategy and GMS).

```
curl --request POST \
  --url http://demosrv-gme.genesyslab.com/genesys/1/internal_statistic \
  --header 'content-type: application/x-www-form-urlencoded' \
  --data objectId=KSippola \
  --data objectType=Agent \
  --data tenant=Environment \
  --data metric=TotalLoginTime
```

In the external access interface for the Stat Service API, Basic Authentication is achieved using credentials from the Config Server. Configure a user in CME/GAX, in the **Member Of** tab add `Administrator`, and in the **Annex** tab specify the following key/value:

```
[gms]
roles=Administrator,Supervisor
```

For the other GMS services/APIs, authentication is set up in the GMS application options:

- For all API authentication setup, the option can be set in the `server` section using the following options: username and password
- For individual selection of authentication setup per service, the `username` and `password` options can be set in the following sections:
  - `callback` section for all callback services (Callback API)
  - `service.<callback name>` section for a callback service (Callback API)
  - `storage` section for the Storage API
  - `notification` section for the Subscribe/Publish API (Notification API)