Framework External Authentication Reference Manual

Using External Authentication

4/30/2025

Using External Authentication

Contents

External authentication works with Configuration Server. If you are installing Genesys software for the first time, you must first set up the Configuration Layer following the instructions in the *Framework Deployment Guide*.

By default, Configuration Server does not communicate with an external authentication server.

Enabling External Authentication

The following is a summary of how to enable external authentication.

1. Set up the external authentication system. Refer to the system documentation for your external authentication system.
2. Deploy the external authentication module during the installation of Configuration Server.
3. Configure Configuration Server to run the selected external authentication systems.
4. Start Configuration Server. Refer to the *Framework Deployment Guide* for information about starting Configuration Server.

At startup, when external authentication is activated, Configuration Server verifies the presence of both the configuration option that points to the pluggable module, and the pluggable module itself. If either one of these is not found, Configuration Server considers external authentication to be disabled.

Refer to the appropriate sections to install the corresponding type of external authentication:

- RADIUS
- LDAP
- Kerberos

Configuring the Master Configuration Server

A new installation of a Master Configuration Server at its first startup reads values from its configuration file and saves those values in the Configuration Database. On all subsequent starts, it reads all values from the database and ignores those in its configuration file. (The backup Master Configuration Server, if configured, saves the information when the first switchover is completed.) As a result, you must make any changes to server-level external authentication parameters in the Options tab of the Configuration Server and Configuration Server Proxies. Any changes you make in the configuration file are ignored.

The only exception to this is the option **enforce-internal-auth** in the **[authentication]** section. If **enforce-internal-auth** in the configuration file section **[authentication]** is set to `true`, the option is set to `true` in the database and overrides authentication to internal for all users (regardless of the value of **enforce-external-auth** at the application level). All users include those with an External User ID or under tenants in which **enforce-external-auth** is set to `true` (see step 4 of Overriding the Defaults by Tenant). Changing the option value to `false` or removing the **enforce-internal-auth** option from the database reverts server operation to the configured mode at the application, tenant, and user levels without server restart.

> **Important**
>
> For legacy Configuration Servers 8.5.100.07 or earlier, where **enforce-internal-auth** is not available, setting the option **enforce-external-auth** to `false` in the configuration file can be used to regain access. If **enforce-external-auth** is set to `true` in the database, but a newly installed Configuration Server reads its configuration file and finds the option set to `false`, Configuration Server sets it to `false` in the database. This ensures that all users are authenticated internally, including those with an External User ID.

Synchronizing User Accounts

For Configuration Server to verify user permissions in the Configuration Database, you must synchronize the user accounts in the Configuration Database with the accounts in the external authentication system. In other words, you must create a Person object in the Configuration Database for each user who will operate in the Genesys environment. The properties of that object must correspond to the user's parameters in the external authentication system. For information about creating the Person objects, see Importing User Data from External Sources.

Person Objects and External IDs

To be considered for external authentication, a Person must be configured with an **External ID**. In the simplest case, the **External ID** is equal to the person's account name.

Customizing the External Authentication Configuration

You can customize the configuration of external authentication for specific Person and Tenant objects. Values specified in the Configuration Server options enable External Authentication and are the default; but values defined at the Person or Tenant level can override them.

> **Important**
>
> In release 8.1 and later, you can use the same configuration sections and options at the server-level, Tenant-level, and Person-level. Genesys recommends this approach. Furthermore, Genesys recommends that in a distributed environment, external authentication be configured at the Tenant level to simplify the configuration process and ensure consistency system-wide.

Establishing the Defaults

The **authentication** section in Configuration Server options enables external authentication, and defines the default external authentication values for all Person objects within the configuration. For details, see Deploying RADIUS External Authentication, step 2 or LDAP Configuration Options.

The **library** option in the **authentication** section must specify a value for each external authentication provider that your implementation supports:

- The value **gauth_ldap** enables LDAP authentication.
- The value **gauth_radius** enables RADIUS authentication.
- The value **gauth_ldap, gauth_radius** or **gauth_radius, gauth_ldap** enables both LDAP and RADIUS.
- The value **internal**, available only for setting at the Tenant or Person level, means that all users associated with the object in which the option is set to this value must validate internally.

Overriding the Defaults

You can override the defaults for Person objects by Tenant, Application, or the Person objects themselves.

By Tenant

To override the defaults for all Person objects belonging to a specific Tenant:

1. Create a section called **authentication** section in that Tenant's annex. You must do this for all Tenants if you specify both provider types (LDAP and RADIUS) in the Configuration Server options.
2. In the **authentication** section, create the option **library**, and assign to it one of the values from the following table.

Tenant-specific External Authentication Providers

Option Value	Description
internal	Authentication is performed internally, using the passwords stored in the Genesys database. Do not specify any additional options.
gauth_radius	All users of this Tenant are authenticated using the RADIUS access parameters specified in the local **radiusclient.conf** configuration file. Do not specify any additional options. Note that you cannot assign different Tenants to different RADIUS servers.
gauth_ldap	All users of this Tenant are authenticated through one or more LDAP servers, each defined in a **gauth_ldap** or **gauth_ldap_<n>** section (see gauth_ldap and gauth_ldap_n Sections) and specified in the additional option **ldap-url**. You must specify at least one **ldap-url** option. You can specify other LDAP-related options, such as password, or more **ldap-url** options to specify a specific set of LDAP servers. You must define all valid LDAP-specific options in the annex of the Tenant object.

Option Value	Description
	Important You cannot override the global option verbose or the content of **ldaperrors.txt**. In addition, settings defined at the Tenant level can be overridden for individual users at the Person level.

3. If the Tenant is using LDAP external authentication (**library=**`gauth_ldap`), create a **gauth_ldap** section for the first LDAP server and a **gauth_ldap_<n>** section for each additional server in the Tenant's annex, and assign appropriate values to the options in each section. Refer to gauth_ldap and gauth_ldap_n Sections.

> **Tip**
>
> If you have existing Tenant, Server, or Person objects that use legacy options (listed in the following table) in the **authentication** section, Genesys recommends that you migrate to the **gauth_ldap[_<n>]** (where **n** is 1 to 9) section format as soon as possible, for security reasons. If you have both current options (in **gauth_ldap[_<n>]** sections) and legacy options (in the **authentication** section) in the same configuration, the legacy options will be ignored.

[+] Show table of legacy options

Legacy Tenant-specific External Authentication Servers—LDAP

	Option Name	Description
First LDAP server	ldap-url	URL of first LDAP server.
	app-user	Distinguished name of application user for first LDAP server.
	password	Application user password for first LDAP server.
	cacert-path	Path to CA certificate for first LDAP server.
	cert-path	Path to certificate of client's key for first LDAP server.
	key-path	Path to client's private key for first LDAP server.
	idle-timeout	Time interval that the LDAP connection to the first LDAP server will be kept open if there are no more requests.
	retry-attempts	Number of authorization retries that will be generated by Configuration Server if the first LDAP server does not respond.
	retry-interval	Time that Configuration Server waits for an authorization reply from the first LDAP server.
	connect-timeout	Time that Configuration Server

	Option Name	Description
		waits after initial connection before deeming first LDAP server to be unavailable.
Second LDAP server	ldap-url1	URL of second LDAP server.
	app-user1	Distinguished name of application user for second LDAP server.
	password1	Application user password for second LDAP server.
	cacert-path1	Path to CA certificate for second LDAP server.
	cert-path1	Path to certificate of client's key for second LDAP server.
	key-path1	Path to client's private key for second LDAP server.
	idle-timeout2	Time interval that the LDAP connection to the second LDAP will be kept open if there are no more requests.
	retry-attempts2	Number of authorization retries that will be generated by Configuration Server if the second LDAP server does not respond.
	retry-interval2	Time that Configuration Server waits for an authorization reply from the second LDAP server.
	connect-timeout2	Time that Configuration Server waits after initial connection before deeming second LDAP server to be unavailable.
Third LDAP server	...	...
	...	...
	Continue configuring groups of options for each LDAP server, as required, up to a maximum of 10 servers.	

4. If the **enforce-external-auth** option in the **[authentication]** section is set to `true`, all users will use external authentication, including those without an External User ID. The user ID will be used if External User ID is not set for a user.

By Application

To override the external authentication options in the master Configuration Server, you can set **enforce-internal-auth** in the options of the associated Configuration Server Proxy applications.

By Person Object

> **Important**
> You cannot override RADIUS defaults for individual Person objects.

To override the default or Tenant-specific LDAP access parameters for any individual Person object, specify one or more partial LDAP URLs in the **External User ID** field in the **General** section of the **Configuration** tab of the Person object.

You can also override the list of servers specified by default or by the Tenant by specifying LDAP servers in the annex, in the same way as you do for a Tenant.

These settings override both default and Tenant-specific settings, and *do not require that you restart Configuration Server*.

The scope of the override depends on whether there is an LDAP server address included in the LDAP URL given in the **External User ID** field. Generally:

- If the LDAP URL in the **External User ID** field includes a server address, the LDAP server given by this address is considered part of the set of servers specified in the Annex. In this case, the LDAP search parameters specified in the **External User ID** field URL apply only to this LDAP server.
- If the LDAP URL in the **External User ID** field does not contain a server address (only search and scope parameters), these search parameters are used to customize the search using the current set of LDAP servers, regardless of where, or at what level, they are defined.

Examples

Example 1: The External User ID field contains only a username.
For example: `user1`

The username is used for authorization. If LDAP servers have been configured in the Person object's annex, the username will be used for authorization with only those servers.

Example 2: The External User ID field contains an LDAP URL consisting of only the server address.
For example: `ldaps://luxor.us.int.vcorp.com:1636/`

The server address in the **External User ID** field is used as the authentication server for this Person. Additional properties of the server can be specified in the Person object's annex.

Additional LDAP servers can also be specified in the Annex. In this case, the options for the first LDAP server (**url_ldap**) are ignored, as they are overridden by the server specified in the **External User ID** field. Only the subsequent servers (such as **ldap-url1**, **ldap-url2**, and so on) are used.

Example 3: The External User ID field contains an LDAP URL consisting of the search parameters but no server address.
For example: `ldap:///???(mail=test@vcorp.com)`

The specified search parameters override the corresponding parameters for all servers used by the Person, whether they are default or defined at the Tenant or Person level.

Disabling External Authentication

To disable external authentication at the Tenant or Person level, set the **library** option in the **authentication** section to `internal` in the object. For Configuration Server or Configuration Server Proxy, set the option to an empty value, and then restart the server to unload the authentication module and stop the authentication. Refer to RADIUS or LDAP for more information about using the **library** option.

To disable external authentication at the Tenant or Person level without unloading the authentication modules, set **enforce-internal-auth** to `true` in the [authentication] section of an application object. That overrides authentication for that application object and sets it to internal for all users regardless of the value of `enforce-external-auth` at the application level, including users with an External User ID those users under tenants with **enforce-external-auth** option set to `true`.

High-Availability External Authentication Configurations

You can configure multiple external authentication servers to add to the reliability and efficiency of your system, as follows:

- For LDAP, redundant configurations are supported with each additional server configured in **gauth_ldap_n** sections. This can be done at all levels–server, tenant, and user.
- For RADIUS, redundant authentication servers are configured in the **radiusclient.conf** configuration file of Configuration Server. This can be done only at the server level.
- For Kerberos, redundant configurations are not supported; each configuration applies only to the server for which it is configured.