Framework External Authentication Reference Manual

Customizing External Authentication Configuration

12/21/2025

Customizing External Authentication Configuration

Contents

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, it is possible to 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 multi-tenant or otherwise 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 Modifying the RADIUS Configuration Files or Configuration Server 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 `gauth_kerberos` enables Kerberos authentication. This applies only to the server on which it is configured; it cannot be customized at the tenant or user level.
- 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 by Tenant

Use the following procedure to override the defaults for all Person objects belonging to a specific Tenant.

1. Create an `authentication` section in that Tenant's Annex Property. 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 it one of the values in Tenant-specific External Authentication Providers.

Tenant-specific External Authentication Providers

Value of library	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 server, each defined in a `gauth-ldap` or `gauth_ldap_n` (see Configuring LDAP Servers) 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. **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 on the Tenant's Annex tab, and assign appropriate values to the options in each section. Refer to Configuring LDAP Servers for detailed information about configuring multiple LDAP servers, and to Configuration Options for detailed descriptions of the options.

   If you have existing Tenant, server, or Person objects that use legacy options (listed in Legacy Tenant-specific External Authentication Servers—LDAP) 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) configuration, the legacy options will be ignored.

Legacy Tenant-specific External Authentication Servers—LDAP

	Option Name	Option Value	Description
First LDAP server	`ldap-url`	`<value>`	URL of first LDAP server

	Option Name	Option Value	Description
	app-user	<value>	Distinguished name of application user for first LDAP server.
	password	<value>	Application user password for first LDAP server
	cacert-path	<value>	Path to CA certificate for first LDAP server
	cert-path	<value>	Path to certificate of client's key for first LDAP server
	key-path	<value>	Path to client's private key for first LDAP server
	idle-timeout	<value>	Time interval that the LDAP connection to the first LDAP server will be kept open if there are no more requests
	retry-attempts	<value>	Number of authorization retries that will be generated by Configuration Server if the first LDAP server does not respond
	retry-interval	<value>	Time that Configuration Server waits for an authorization reply from the first LDAP server.
	connect-timeout	<value>	Time that Configuration Server waits after initial connection before deeming first LDAP server to be unavailable.
Second LDAP server	ldap-url1	<value>	URL of second LDAP server
	app-user1	<value>	Distinguished name of application user for second

	Option Name	Option Value	Description
			LDAP server.
	password1	<value>	Application user password for second LDAP server
	cacert-path1	<value>	Path to CA certificate for second LDAP server
	cert-path1	<value>	Path to certificate of client's key for second LDAP server
	key-path1	<value>	Path to client's private key for second LDAP server
	idle-timeout2	<value>	Time interval that the LDAP connection to the second LDAP will be kept open if there are no more requests.
	retry-attempts2	<value>	Number of authorization retries that will be generated by Configuration Server if the second LDAP server does not respond.
	retry-interval2	<value>	Time that Configuration Server waits for an authorization reply from the second LDAP server.
	connect-timeout2	<value>	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.		

Overriding the Defaults 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 (see See 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 on the Tenant's Annex tab, and assign appropriate values to the options in each section. Refer to "Configuring LDAP Servers" on page 36 for detailed information about configuring multiple LDAP servers, and to "Configuration Options" on page 46 for detailed descriptions of the options.).

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.