Framework External Authentication Reference Manual

LDAP Configuration Options

5/7/2025

Contents

LDAP Configuration Options

This section describes the configuration options used to configure LDAP external authentication on Configuration Server and Configuration Server Proxy.

> **Warning**
> Configuration section names, configuration option names, and predefined option values are case-sensitive. Type them in the configuration file or in Genesys Administrator exactly as they are documented in this chapter.

Setting Configuration Options

Unless otherwise specified, you set LDAP configuration options at any of the following locations:

- In the options of the Configuration Server or Configuration Server Proxy Application object
- In a distributed environment, in the annex of a Tenant object
- In the annex of individual Person objects

This will turn on external authentication for all users enabled with External IDs, or for all users if the **enforce-external-auth** option is set to `true`.

You can also fine-tune your LDAP configuration throughout your system by configuring some or all options in the annex of Tenant objects. Refer to Using LDAP in a Configuration with More Than One Tenant for more information.

Mandatory Options

The following table lists the options that are mandatory for LDAP external authentication on Configuration Server and Configuration Server Proxy. Both options are set automatically during the installation of Configuration Server and Configuration Server Proxy.

Mandatory LDAP Configuration Options

Section	Option Name	Option Value
authentication	library	gauth_ldap
gauth_ldap	ldap-url	Valid URL of LDAP authentication module

authentication Section

This section is mandatory on the Server level to enable external authentication. It can, however, appear in other locations as mentioned in Setting Configuration Options.

This section must be called *authentication*.

enforce-external-auth

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

Optional. Enforces external authentication for every user. If you omit this parameter, LDAP AM performs authentication only if an External ID is specified in the Person object.

This option applies at the server level, and starting in release 8.5.1, also at the Tenant level.

If this option is configured at the server level as `true` in the database, but Configuration Server reads its configuration file and finds the option set to `false`, the value from the configuration file will override the value in the database, allowing all users of the Environment tenant to log in internally.

> **Warning**
> Do not set this option to `true` until you have configured all of the accounts in the configuration.

enforce-internal-auth

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

Optional. Specifies if all users are to be authenticated internally.

This option is set in the options of the Application object. If set to `true`, all users are authenticated internally by Configuration Server or Configuration Server Proxy, regardless of having a value in the External ID field. If set to `false` (the default), only those users with a value in the External ID field are authenticated by the LDAP AM.

library

Default Value: No default value
Valid Values: Depends on type configuration option, as follows:

`gauth_radius`	All
`gauth_ldap`	All

`gauth_radius, gauth_ldap`	Configuration Server, Configuration Server Proxy
`gauth_ldap, gauth_radius`	Configuration Server, Configuration Server Proxy
`internal`	Tenant, Person

Changes Take Effect: Upon restart of Configuration Server or Configuration Server Proxy; immediately for Tenants and Persons.

Specifies the section that specifies the external authentication parameters. This option is mandatory, and its value is set automatically during installation. If this Configuration Server or Configuration Server Proxy was previously configured for another type of authentication, such as RADIUS, you must manually add `, gauth_ldap` to the value of this option.

When set to `internal`, all users associated with the object in which the object is set to this value are validated internally.

gauth_ldap and gauth_ldap_<n> Sections

The **gauth_ldap** and **gauth_ldap_<n>** sections were added in release 8.1 to provide a more secure and easier method of configuring LDAP servers. They were designed to replace the legacy configuration structure and options (described in the table in Overriding the Defaults by Tenant). Instead of having all LDAP servers defined by sets of uniquely-named options in the **authentication** section, this new structure requires that each LDAP server be defined in its own section, making it easier to set up and maintain the configuration.

> ### Tip
> If you have existing Tenant, Server, or Person objects that use the legacy options in the **authentication** section, Genesys recommends that you migrate to the **gauth_ldap[_<n>]** (where **n** is 1 to 9) section format described in this section as soon as possible. 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.

Each gauth_ldap and gauth_ldap_<n> section contains information about one LDAP Authentication Module. The **gauth_ldap** section is mandatory.

If you are using more than one LDAP Server, you must identify the rest in individual **gauth_ldap_<n>** sections. Configuration Server supports up to ten LDAP authorization servers, so you can have up to nine of these sections, one section for each additional LDAP server. The name of each section must be unique, and Genesys recommends that they be in the same order as they are indexed. Each section must be named **gauth_ldap_<n>**, where n is a numeric index in the range of 1 to 9 for each LDAP server, as follows:

```
[gauth_ldap_<n>]
ldap-url=<value>
app-user=<value>
```

```
password=<value>
cacert-path=<value>
cert-path=<value>
key-path=<value>
idle-timeout=<value>
retry_attempts=<value>
retry-interval=<value>
connect-timeout=<value>
chase-referrals=<value>
keepalive-enable=<value>
keepalive-time=<value>
keepalive-probes=<value>
keepalive-interval=<value>
```

When you add a new section, it takes effect immediately. But if you remove a section, you must restart Configuration Server or Configuration Server Proxy to take the LDAP Server out of use.

LDAP Server Parameters

To define an LDAP server, set the parameters described in this section in the options of the object, in the **gauth_ldap** or **gauth_ldap_<n>** section, as appropriate.

ldap-url

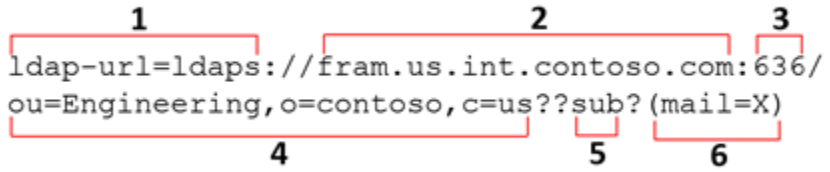
Default Value: Empty string
Valid Value: URL in RFC 2255 format, as described below
Changes Take Effect: Immediately

This URL contains the information needed to access the LDAP server and directory from which it retrieves the user's distinguished name. Enter the URL of one LDAP server in this field.

The LDAP URL contains default settings that are common to all Users in the Genesys Configuration Database. However, these settings may be overridden if the User's record in the Configuration Database also contains an LDAP URL with access parameters. The priorities used to obey configuration parameters, from highest to lowest, are:

1. LDAP URL in the user's record of the configuration database.
2. LDAP URL specified in the authentication section of the Tenant’s Annex.
3. LDAP URL in the configuration file (at first start only), or the Configuration Server or Configuration Server Proxy Application object.
4. AM default parameters, which cannot be changed by the user.

The following is an example of an LDAP URL parsed into its parameters, followed by a table describing them. Note that the URL contains no spaces and is a single expression that must be entered on a single line.



ldap-url Parameters

Parameter	Definition
1 Protocol type	Required. Valid values: `ldaps` (SSL/TLS secure) or `ldap` (unsecure)
2 LDAP server host name	Optional. Default is the local host; for example, `fram.us.int.vcorp.com`
3 LDAP server port	Optional. The default (636 for a secure connection and 389 for unsecured) is used if you omit this parameter. Unsecure means a simpler configuration, but also presents a risk. Genesys strongly advises that you use a secure connection.
4 Base DN	Required. Defines the node in the LDAP tree to use as base for the LDAP search; for example, `ou=Engineering,o=vcorp,c=us`
5 Search scope	Optional. Default: `sub`. Defines the scope of the search operation (according to the RFC 2251 format). Valid ValuesA: `base`, `one`, `sub`
6 Search filter	Optional. Limits the search by searching for a match with a specified field. Default: empty string. In the example URL above, X is a parameter that will be substituted with the value of the user's External ID. The filter expression must conform to the standard RFC 2251 format specification. Example: `(displayName=X)` Note: The user's External ID is defined in the properties of the Person object.

> ### Warning
> When used with TLS, host names specified in **ldap-url** are case-sensitive and must match the corresponding entries in the DNS. And if used in a Windows domain, they must also match Active Directory records.

For examples of LDAP URLs, see Examples.

app-user

Default Value: Empty string
Valid Value: Valid path
Changes Take Effect: Immediately

Distinguished name (which includes location in the directory tree and in any containers) of the application account used by the LDAP AM to search for the User's information that is needed to authenticate the user. For an example of the **app-user** parameter for RACF, see gauth_ldap Section Using IBM RACF.

password

Default Value: Empty string
Valid Value: A valid password
Changes Take Effect: Immediately

Password of the application account; required if **app-user** is set. This password is masked by default in all logs.

cacert-path

Default Value: Empty string
Valid Value: Valid path
Changes Take Effect: Immediately

Full path to the file containing a certificate from a trusted Certificate Authority, which is used to negotiate a secure LDAP connection to the server. Required for a secure connection. Refer to Configuring Server Authentication for more information about using this option when configuring secure connections.

> **Warning**
>
> When using LDAP servers in a secure environment, all LDAP servers must use SSL server certificates issued by the same certificate authority or subordinate authorities of the same public root authority. Configuration Server must be provisioned (using **cacert-path**) with a certificate of authority (or chain of certificates) that can validate all server SSL certificates.
>
> If mutual authentication is required on connections to LDAP servers, Configuration Server must be provisioned (using **cacert-path** and **key-path**) with the same local certificate that is accepted by all LDAP servers.
>
> Genesys does not support specifying different client certificates (and/or certificate authority certificates), for different connections.

cert-path

Default Value: Empty string
Valid Value: Valid path
Changes Take Effect: Immediately

Full path to the file containing a certificate for Configuration Server to connect to a remote LDAP Server that requires mutual authentication. Refer to Configuring Server Authentication for more information about using this option when configuring secure connections.

> **Important**
>
> The certificate must be in Base64 (PEM) format. This parameter must be set if the protocol portion of the LDAP URL defines a secure connection to the LDAP server and if the LDAP server enforces client Secure Socket Layer (SSL) authentication.

> ### Warning
> When using LDAP servers in a secure environment, all LDAP servers must use SSL server certificates issued by the same certificate authority or subordinate authorities of the same public root authority. Configuration Server must be provisioned (using **cacert-path**) with a certificate of authority (or chain of certificates) that can validate all server SSL certificates.
>
> If mutual authentication is required on connections to LDAP servers, Configuration Server must be provisioned (using **cacert-path** and **key-path**) with the same local certificate that is accepted by all LDAP servers.
>
> Genesys does not support specifying different client certificates (and/or certificate authority certificates), for different connections.

key-path

Default Value: Empty string
Valid Values: Valid path
Changes Take Effect: Immediately

Full path to the file containing the key for the Configuration Server certificate specified by **cert-path**. Refer to Configuring Server Authentication for more information about using this option when configuring secure connections.

> ### Important
> The certificate must be in Base64 (PEM) format. This parameter must be set if the protocol portion of the LDAP URL defines a secure connection to the LDAP server and if the LDAP server enforces client Secure Socket Layer (SSL) authentication.

> ### Warning
> When using LDAP servers in a secure environment, all LDAP servers must use SSL server certificates issued by the same certificate authority or subordinate authorities of the same public root authority. Configuration Server must be provisioned (using **cacert-path**) with a certificate of authority (or chain of certificates) that can validate all server SSL certificates.
>
> If mutual authentication is required on connections to LDAP servers, Configuration Server must be provisioned (using **cacert-path**) with the same local certificate that is accepted by all LDAP servers.
>
> Genesys does not support specifying different client certificates (and/or certificate authority certificates), for different connections.

idle-timeout

Default Value: 0
Valid Values: 0 to MAX_INTEGER
Changes Take Effect: Immediately

Defines how long (in seconds) the LDAP connection to the server defined in this section will be kept open if there are no more requests to send. When set to zero (0), this connection will be kept open indefinitely. Genesys recommends that it be set to a value that does not exceed the idle timeout of the LDAP server.

retry-attempts

Default Value: 3
Valid Values: 0 to MAX_INTEGER
Changes Take Effect: Immediately

The number of authorization retries that Configuration Server will generate if the current LDAP server does not respond. Specify a value for this parameter if you are using multiple LDAP servers. If Configuration Server does not receive a reply within this number of retries, it sends the request to the next LDAP authentication server specified in the object's options.

If you are using only one LDAP server, requests will always be sent to that server regardless of the value of **retry-attempts**.

If Configuration Server has tried all the LDAP servers without getting a response, an error is generated. See Error Handling.

retry-interval

Default Value: 10
Valid Value: 0 to MAX_INTEGER
Changes Take Effect: Immediately

The amount of time, in seconds, that Configuration Server waits for an authorization reply. If Configuration Server does not receive a reply from the current LDAP server during that time, it sends the request again, either to the same LDAP server or, if you are using multiple LDAP servers, to the next LDAP server, after the number of tries specified in **retry-attempts**.

connect-timeout

Default Value: 10
Valid Values: 0 to MAX_INTEGER
Changes Take Effect: Immediately

Defines the initial connection timeout (in seconds), after which Configuration Server deems the specified LDAP server to be unavailable. When set to zero (0), the default value (10) is used.

chase-referrals

Default Value: 0
Valid Values:

0	Configuration Server chases (follows) referrals and uses anonymous bind to connect to the referred servers. The user is bound to the original server to which the authentication request was sent (as specified by the LDAP configuration in Configuration Server).
1	Configuration Server chases referrals and uses the same login credentials specified in the configuration of the original LDAP server (in the **gauth_ldap** section). The user is bound to the server at which authentication occurs.
2	Configuration Server does not chase referrals, and returns an error if a referral is returned.

Changes Take Effect: At the next authentication request

Specifies how Configuration Server handles a referral returned by a configured LDAP server.

keepalive-enable

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

Specifies the Keep-Alive setting for Configuration Server. If set to `true`, Configuration Server will disconnect from the LDAP Server if the server has not responded within the limits set by the other Keep-Alive parameters—time, probes, and interval.

> **Important**
>
> - The Keep-Alive functionality can be enabled only on UNIX.
> - If this option is not set, or set to `false` the related options **keepalive-time**, **keepalive-probes**, and **keepalive-interval** are ignored.

keepalive-time

Default Value: `10`
Valid Values: `1` to `MAXINTEGER`
Changes Take Effect: Immediately

The number of seconds a connection must remain idle before TCP starts to send Keep-Alive probes.

> **Important**

- The Keep-Alive functionality can be enabled only on UNIX.
- This option is ignored if **keepalive-enable** is set to `false`.

keepalive-probes

Default Value: 3
Valid Values: 1 to `MAXINTEGER`
Changes Take Effect: Immediately

The maximum number of Keep-Alive probes that will be sent before Configuration Server disconnects from the LDAP Server.

Important

- The Keep-Alive functionality can be enabled only on UNIX.
- This option is ignored if **keepalive-enable** is set to `false`.

keepalive-interval

Default Value: `10`
Valid Values: 1 to `MAXINTEGER`
Changes Take Effect: Immediately

The time interval, in seconds, between individual Keep-Alive probes.

Important

- The Keep-Alive functionality can be enabled only on UNIX.
- This option is ignored if **keepalive-enable** is set to `false`.