Framework External Authentication Reference Manual

LDAP Deployment

5/6/2025

Contents

LDAP Deployment

This section describes how to deploy LDAP in your environment.

Deploying LDAP During Installation of Configuration Server

To deploy LDAP, do the following:

1. Install Configuration Server and deploy LDAP during the installation. This Configuration Server can be the primary or backup Configuration Server in a redundant configuration, or the master Configuration Server in a geographically distributed configuration. **[+] Show steps**

a. Begin installing Configuration Server as directed in the *Framework Deployment Guide*.

b. On the **Configuration Server Run Mode** page, select one of the following, as appropriate:

- Configuration Server Master Primary—If you are installing a Master or Primary Configuration Server.
- Configuration Server Proxy—If you are installing a Configuration Server Proxy.

c. Continue installing Configuration Server or Configuration Server Proxy, as appropriate.

d. On the **Configuration Server External Authentication** page, select **Lightweight Directory Access Protocol (LDAP)**.

e. On the **LDAP Server Access URL** page, enter the URL that the Configuration Server or Configuration Server Proxy will use to connect to the LDAP server.

If you are going to use multiple LDAP authentication servers, specify the first LDAP server on this page. After Configuration Server or Configuration Server Proxy starts up for the first time, you can configure additional LDAP servers in the options of the Configuration Server Application object.

> Important
>
> If you are going to use external authentication at the Tenant level, or are going to have a geographically distributed deployment of Configuration Servers, you can ignore this step, and configure the servers at the Tenant level after Configuration Server has been started.

f. Finish installing Configuration Server or Configuration Server Proxy.

> Warning
>
> There might be instances in which Configuration Server, or Configuration Server Proxy, and the external authentication system interpret a blank password differently. To eliminate this possibility, make sure that Configuration Server does not accept a blank password as valid. Refer to the *Framework Configuration Options Reference Manual* for instructions on configuring the **allow-empty-password** option to disallow a blank password.

If you installed the LDAP pluggable modules during installation of a new master Configuration Server, the following configuration option sections and options are added to the configuration file, and are copied into the database when Configuration Server starts (see Configuring the Master Configuration Server), as follows:

```
[authentication]
library=gauth_ldap
[gauth_ldap]
ldap-url=<URL as entered during installation>
```

When you install the LDAP pluggable module on Configuration Server Proxy, you must manually add the same two sections and options to the Application object:

- The **library** option specifies **gauth_ldap** as the section that specifies the external authentication parameters.
- The **ldap-url** option specifies the URL of the LDAP server and directory that you entered during installation. Both values are set automatically.

At this point, these two sections indicate that LDAP external authentication is to be used, and they are all that is required to use LDAP with one LDAP server that accepts anonymous LDAP binding. If your LDAP server requires authentication to perform searches using a query, specified in the option **ldap-url**, you must set the **app-user** and **password** options before you can use external authentication.

To maintain backwards compatibility, if an **ldapclient.conf** file exists, the master Configuration Server will also read the contents of that file and translate those settings into Configuration Server options at first startup, also storing them in the database. Any changes to that file will also be ignored at subsequent startups.

> Warning
>
> If a legacy **ldapclient.conf** or **confserv.conf** file from a previous version exists, you must do the following before the first startup of the master Configuration Server:
>
> - If either of the files contains passwords, make sure that both of the following conditions are true. If either of these conditions are omitted, Configuration Server may import the legacy passwords incorrectly.
>   - The passwords are encrypted.
>   - The **confserv** section of the **confserv.conf** file contains **encryption** set to `true`.
> - If the legacy **ldapclient.conf** file contains multiple servers, organize the servers list in the order in which the servers are indexed, that is **gauth_ldap**, **gauth_ldap_1**, **gauth_ldap_2**, and so on. Otherwise, Configuration Server will index the servers in the order in which they are read.

2. (Optional) Configure additional LDAP servers. Configuration Server supports up to ten LDAP authorization modules, or servers.

> Important
>
> Redundant RACF servers are not supported.

When you install Configuration Server, you can configure one LDAP server during the installation process. If you are using multiple LDAP Servers, you configure those additional LDAP servers in the options of the Configuration Server object.

> Important
>
> If you are going to use per-Tenant external authentication targeting distributed deployment, Genesys recommends that you configure the LDAP servers at the Tenant level, as described in Deploying LDAP on Configuration Server Proxy.

In the options, there is one section for each LDAP server. The name of each section must be unique, and should appear in the order in which they are indexed. The first section is named **gauth_ldap**, as described previously. Genesys recommends naming each additional section **gauth_ldap_<n>**, where *n* is a numeric index in the range of 1 to 9 for each LDAP server. Refer to gauth_ldap and gauth_ldap_<n> Sections for more information about configuring multiple LDAP servers.

When you are finished configuring all LDAP servers, the options will contain one or more sections that look like this (in addition to the mandatory **gauth_ldap** section for the first server):

```
[gauth_ldap_1]
ldaps://fram.us.int.vcorp.com:636/ou=Eng,o=vcorp,c=us??sub?(mail=X)
app-user=cn=Manager,o=vcorp,c=us
password=12345ABC9
cacert-path=keys/server.arm
cert-path=keys/client.arm
key-path=keys/private.pem
idle-timeout= 5
retry-attempts=3
retry-interval=10
connect-timeout=10
```

Each section will have a different numeric identifier.

3. (Optional) Install as many Configuration Servers as required, deploying LDAP during the installation, using the procedure in Step 1.

Deploying LDAP on Configuration Server Proxy

In geographically distributed systems prior to release 8.1, LDAP external authentication was configured only on the master Configuration Server, and each Configuration Server Proxy passed authentication requests to it.

Starting in release 8.1, LDAP External Authentication can be configured on the master Configuration Server and on each Configuration Server Proxy. This allows each Configuration Server Proxy to process authentication requests itself, without passing them on to the master Configuration Server. Use the same procedure as in step 1 of “Deploying LDAP”.

If you want to force specific users to use specific proxy servers for authentication, you can override the basic authentication configuration by setting the authentication parameters at the Tenant-, or even Person-, level. For example, if you have Configuration Server Proxies located in a geographic pattern such as one in each country where you do business, you can specify that each user be authenticated through the proxy server in the country in which they are located. See Customizing the External Authentication Configuration for more infomation about overwriting the authentication defaults.|2}}

Network Connectivity Options for LDAP

Starting in release 8.5.1, a Keep-Alive mechanism enables Configuration Server to disconnect from the LDAP Server if the server does not respond to a given number of probes sent at a given frequency. You define the parameters of this mechanism using these options:

- **keepalive-enable**

- **keepalive-time**
- **keepalive-probes**
- **keepalive-interval**

> ### Important
> The Keep-Alive mechanism can be enabled only on UNIX operating systems.

Using LDAP in a Configuration with More than One Tenant

> ### Important
> Genesys strongly recommends that, if there are multiple distributed Configuration Servers, all LDAP servers should be configured at the Tenant level to simplify the configuration of external authentication.

You can set LDAP configuration options at the Tenant level, in the annex of the Tenant object. This activates external authentication only for users belonging to that Tenant. You can override the Application-level settings at the Tenant level, by configuring the following in the annex of the Tenant, as follows:

```
[authentication]
library=’internal’
```

This disables external authentication for all users who belong to that Tenant, and they are authenticated internally. You can also configure multiple servers at the Tenant level, one each in a **gauth_ldap_<n>** section, as described in gauth_ldap and gauth_ldap_<n> Sections.

Using LDAP Referrals

Starting in release 8.1.2, Configuration supports the use of LDAP referrals. This enables authentication to occur at an LDAP server other than the server to which Configuration Server sent the authentication request.

> ### Important
> Full referrals are supported for servers existing in a Microsoft Active Directory. Full referral is not yet supported for multiple directories contained in the referral. If the referral contains more than one server, only the first referral is processed; the rest of

> the referrals are ignored.

When Configuration Server sends a request to the LDAP Server, it may receive in response not an authentication result, but a referral to another server. If activated, Configuration Server searches for the referred server, binds to it, and reissues the authentication request.

To configure how Configuration Server handles referrals, or to deactivate the use of referrals, use the **chase-referrals** option in the **gauth_ldap** or **gauth_ldap_<n>** section at the Tenant, Application, or User level.

> ### Tip
> If the LDAP configuration at the customer site consists of multiple LDAP servers, Genesys recommends that you configure each Tenant and/or individual User to be authenticated using the LDAP server that holds the authentication information for those Users, instead of relying on referrals from a single LDAP server. Configuring Configuration Server to chase referrals might lead to delays during login, and increase the risk of login failures because of the timeout expiring. Use of referrals should be considered only if a small number of user accounts depend on it.

If connection to the referred server fails, Configuration Server applies its configured **retry-interval** and **retry-attempts** to the LDAP server to which it originally sent the request.

Examples

LDAP URL

Example 1

```
ldap-url=ldaps://fram.us.int.vcorp.com:636/ou=Engineering,o=vcorp,c=us??sub?(mail=X)
```

Corresponding LDAP search syntax:

```
ldapsearch -p 636 -h fram.us.int.vcorp.com –b ou=Engineering,o=vcorp,c=us –s sub
mail=’X’ dn
```

In this example, the LDAP AM connects securely on host/port:
   `fram.us.int.vcorp.com:636`
and searches using the following variable values:
   base: `ou=Engineering,o=vcorp,c=us`
   scope: `sub`
   filter: `(mail=X)`
where X is the actual value of `external user ID`.

Example 2

```
ldap-url=ldap:///ou=Engineering%20Department,o=vcorp,c=us???(lastName=X)
```

Corresponding LDAP search syntax:

```
ldapsearch -p 389 -h localhost -b ìou=Engineering Department,o=vcorp,c=usî -s sub
lastName=’X’ dn
```

In this example, the LDAP AM connects insecurely on host/port:
  `localhost:389`
and searches using the following variable values:
  base: `ou=Engineering Department,o=vcorp,c=us`
  scope: `sub`
  filter: `(lastName=X)`
where X is the actual value of `external user ID`.

Example 3

```
ldap-url=ldaps://fram.us.int.vcorp.com/ou=Engineering,o=vcorp,c=us???(mail=X)
```

Corresponding LDAP search syntax:

```
ldapsearch –p 636 -h fram.us.int.vcorp.com -b ìou=Engineering,o=vcorp,c=usî -s sub
mail=’X’ dn
```

In this example, the LDAP AM connects securely on host/port:
  `fram.us.int.vcorp.com:636`
and searches using the following variable values:
  base: `ou=Engineering,o=vcorp,c=us`
  scope: `sub`
  filter: `(mail=X)`
where X is the actual value of `external user ID`.

Choosing this scope only verifies the existence of the DN specified in the search base parameter.

gauth_ldap Section Using IBM RACF

Using IBM RACF, the **gauth_ldap** section contains the same options. The **app-user** and **ldap-url** options contain the RACF-specific information.

```
[gauth_ldap]
app-user=racfid=TIMLDAP,profiletype=USER,sysplex=SYSPLEX2
password=+++
ldap-url=ldap://10.1.87.53:389/profiletype=USER,sysplex=SYSPLEX2??sub?(racfid=X)
connect-timeout=3
retry-interval=4
retry-attempts=5
```

where `TIMLDAP` is the user created to access RACF.