Framework External Authentication Reference Manual

RADIUS External Authentication

4/13/2026

RADIUS External Authentication

Contents

This section describes how to set up Remote Authentication Dial In User Service (RADIUS) external authentication.

Overview

Genesys Configuration Server supports all versions of RADIUS, an industry standard for authentication. The architectural schema is identical to the one shown here, where a RADIUS server acts as a third-party authentication server.

Configuration Server external authentication supports multiple RADIUS servers. The active, or responding, authentication server is used for authorization of all subsequent clients. When this server does not respond, the next server in the list (of servers, as specified in the servers file) is tried, and if it responds, it becomes the active authentication server. This process continues sequentially through the list of authentication servers.

Starting in release 8.0, RADIUS messages concerning the success and failure of each RADIUS authentication attempt are relayed from the RADIUS server back through Configuration Server for display to the end user.

In geographically distributed systems prior to release 8.0, RADIUS external authentication was configured only on the Master Configuration Server, and each Configuration Server Proxy passed authentication requests to it. Starting in release 8.0, RADIUS External Authentication can be configured on the Master Configuration Server and on each Configuration Server Proxy. Therefore, each Configuration Server Proxy can process authentication requests itself, and not pass them on to the Master Configuration Server.

Deploying RADIUS External Authentication

To deploy RADIUS, do the following:

1. Install Configuration Server and deploy RADIUS during installation. **[+] Show steps**

a. Begin the installation of Configuration Server.

b. On the **Configuration Server Run Mode** page, select **Configuration Server Master Primary**.

c. Continue installing Configuration Server.

d. On the **Configuration Server External Authentication** page, select **Remote Authentication Dial In User Service (RADIUS)**.

e. Finish installing Configuration Server.

During the installation of Configuration Server, a configuration options section named **authentication** is added to the configuration file, and is copied into the database when Configuration Server starts (see Configuring the Master Configuration Server). This section indicates if external authentication is to be used, and if so, what type.

The following is an example of the authentication section in the configuration file of a Configuration Server that will use only RADIUS external authentication:

```
[authentication]
library=gauth_radius
```

2. Modify the RADIUS configuration files.

The following table lists the pluggable modules used for communication with the third-party authentication server.

Pluggable Module Names for RADIUS

Operating System	Module for 32-bit Version	Module for 64-bit Version
Windows	gauth_radius.dll	
Solaris	libgauth_radius_32.so	libgauth_radius_64.so
AIX	libgauth_radius_32.so	libgauth_radius_64.so
Red Hat Linux	libgauth_radius_32.so	libgauth_radius_64.so

In addition to the pluggable module file, three RADIUS configuration files are copied to the destination directory when you install Configuration Server:

- **servers**—specifies connection parameters of the RADIUS servers.
- **radiusclient.conf**—specifies the RADIUS client parameters.
- **dictionary**—contains communication protocol data.

> **Important**
>
> When creating user reply messages, note that the length of the `Reply Message` attribute or `State` attribute strings is 128 characters or less.

You must modify the **servers** and **radiusclient.conf** files. Do not modify the **dictionary** file.

[+] Show steps

Modify the servers File

The RADIUS Configuration Authentication Module uses the configuration file **servers** to determine to which RADIUS server it must connect. Each line of the file contains the connection parameters for one RADIUS server.

For each RADIUS server, specify:

1. The name or IP address of each RADIUS server.
2. A key; that is, a word that matches the shared secret word configured for each RADIUS server.

For example:

```
#Server Name or Client/Server pair Key
#---------------- ---------------
server1 key1
server2 key2
server3 Key3
```

Modify the radiusclient.conf File

The RADIUS Configuration Authentication Module uses the configuration file **radiusclient.conf** to read its own configuration. In the

file, specify values for the following parameters:

- **authserver**—The names or IP addresses of the RADIUS servers. These must be the same values as configured in the **servers** file. If necessary, also specify a port for the RADIUS server after a column. For example:

  ```
  authserver server1:1812 server2:1820 server3
  ```

  where:

  - `server1` is the first RADIUS authorization server that will be used.
  - `server2` is the backup RADIUS authorization server that will be used if `server1` does not respond.
  - `server3` is the backup RADIUS authorization server that will be used if `server2` does not respond.

  If you specify only one RADIUS server, that server will continue to be used whether it responds or not.
- **acctserver**—The RADIUS server to use for accounting requests. If this parameter is not set, the RADIUS libraries will not load.
  For example:

  ```
  acctserver <server1> <server2>
  ```

  where:

  - `server1` is the first RADIUS server that will be used.
  - `server2` is the backup RADIUS server that will be used if `server1` does not respond.
- **radius_retries**—The number of authorization retries that will be generated by Configuration Server if the current external authorization server does not respond. Specify a value for this parameter if you are using multiple RADIUS servers. If Configuration Server does not receive a reply within this number of retries, it sends the request to the next RADIUS authentication server specified in the list.
  For example:

  ```
  #resend request 6 times before trying the next server
  radius_retries 6
  ```

  If you are using only one RADIUS server, requests will always be sent to that server regardless of the value of **radius_retries**.
- **radius_timeout**—The time, in seconds, that Configuration Server waits for an authorization reply. If Configuration Server does not receive a reply from the current RADIUS server during that time, it sends the request again, either to the same RADIUS server or, if you are using multiple RADIUS servers, to the next RADIUS server after the number of tries specified in **radius_retries**.
  For example:

  ```
  #wait 20 seconds for a reply from the RADIUS server
  radius_timeout 20
  ```
- **default_realm**—The extension to add to a user name if the RADIUS server requires names in this format. If a value is specified, the RADIUS module adds it after the `@` sign to all user names received from Configuration Server.
  For example:

  ```
  default_realm genesys.us
  ```

  If you log in to a Genesys application with the user name `scott`, the resulting name that the RADIUS client passes to the RADIUS server is `scott@genesys.us`.

3. (Optional) Install as many Configuration Servers, including Configuration Server Proxies as required, deploying RADIUS during the installation. Repeat the previous steps to deploy RADIUS on regular Configuration Servers, and use the following steps to deploy it on Configuration Server Proxies: **[+] Show steps**

Start of Procedure

a. Do one of the following:
   - If Configuration Server Proxy is not installed, install it now as described in the *Framework Deployment Guide*, being sure to select the **RADIUS external authentication** option when prompted.
   - If Configuration Server Proxy has been installed but not configured to use external authentication, copy the following files from the Master Configuration Server installation directory to the Configuration Server Proxy installation directory:
     - **dictionary**
     - the appropriate pluggable file, as listed in the Pluggable Module Names table.
     - **radius.seq** This file is required by the Configuration Server Proxy, but not by Configuration Server. If the file is missing, Configuration Server automatically generates it.
     - **radiusclient.conf**
     - **servers**

b. In the Configuration Server Proxy Application object, configure the following options in the indicated sections, and set them to the specified values:
   - If not set during installation, configure external authentication on Configuration Server Proxy by setting the option **library** in the **authentication** section to `gauth_radius`.
   - To set the log level for monitoring the connection between Configuration Server Proxy and the RADIUS server, use the option **verbose** in the **gauth_radius** section of the options of the Configuration Server Proxy Application object, as described in Troubleshooting the External Authentication Connection.

c. Restart Configuration Server Proxy.

Configuration Options

This section describes the configuration options used when deploying and using RADIUS External Authentication.

authentication Section

This section must be called *authentication*.

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 the object for which this option is set

Specifies the section that specifies the external authentication parameters. This option is mandatory, and its value is set automatically during installation. You can deploy both RADIUS and LDAP on the same Configuration Server or Configuration Server Proxy. If this Configuration Server or Configuration Server Proxy was previously configured for another type of authentication, add, `gauth_radius` 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.