Framework 8.0

External Authentication

Reference Manual

About Genesys

Genesys Telecommunications Laboratories, Inc., a subsidiary of Alcatel-Lucent, is 100% focused on software for contact centers. Genesys recognizes that better interactions drive better business and build company reputations. Customer service solutions from Genesys deliver on this promise for Global 2000 enterprises, government organizations, and telecommunications service providers across 80 countries, directing more than 100 million customer interactions every day. Sophisticated routing and reporting across voice, e-mail, and Web channels ensure that customers are quickly connected to the best available resource—the first time. Genesys offers solutions for customer service, help desks, order desks, collections, outbound telesales and service, and workforce management. Visit www.genesyslab.com for more information.

Each product has its own documentation for online viewing at the Genesys Technical Support website or on the Documentation Library DVD, which is available from Genesys upon request. For more information, contact your sales representative.

Notice

Although reasonable effort is made to ensure that the information in this document is complete and accurate at the time of release, Genesys Telecommunications Laboratories, Inc., cannot assume responsibility for any existing errors. Changes and/or corrections to the information contained in this document may be incorporated in future versions.

Your Responsibility for Your System's Security

You are responsible for the security of your system. Product administration to prevent unauthorized use is your responsibility. Your system administrator should read all documents provided with this product to fully understand the features available that reduce your risk of incurring charges for unlicensed use of Genesys products.

Trademarks

Genesys, the Genesys logo, and T-Server are registered trademarks of Genesys Telecommunications Laboratories, Inc. All other trademarks and trade names referred to in this document are the property of other companies. The Crystal monospace font is used by permission of Software Renovation Corporation, www.SoftwareRenovation.com.

Technical Support from VARs

If you have purchased support from a value-added reseller (VAR), please contact the VAR for technical support.

Technical Support from Genesys

If you have purchased support directly from Genesys, please contact Genesys Technical Support at the regional numbers provided on page 8. For complete contact information and procedures, refer to the ***Genesys Technical Support Guide***.

Ordering and Licensing Information

Complete information on ordering and licensing Genesys products can be found in the ***Genesys Licensing Guide.***

Released by

Genesys Telecommunications Laboratories, Inc. www.genesyslab.com

Document Version: 80fr_ref-exta_09-2009_v8.0.101.00

Table of Contents

Appendix

Supplements

Index

List of Procedures

Preface

Welcome to the *Framework 8.0 External Authentication Reference Manual.* This document introduces you to the concepts, terminology, and procedures related to integrating Genesys software with third-party authentication systems.

This document is valid only for the 8.0 release(s) of this product.

Note: For versions of this document created for other releases of this product, visit the Genesys Technical Support website, or request the Documentation Library DVD, which you can order by e-mail from Genesys Order Management at `orderman@genesyslab.com`.

This preface contains the following sections:

For information about related resources and about the conventions that are used in this document, see the supplementary material starting on page 53.

About External Authentication

A third-party External Authentication system can be used to control user access to Genesys applications. This manual contains the following information:

- How to implement in the Configuration Layer an integration with third-party authentication systems.
- How to enable external authentication in Configuration Server.
- How to configure the Genesys authentication client for Remote Authentication Dial In User Service (RADIUS).
- How to deploy, configure, and use the Lightweight Directory Access Protocol (LDAP) authentication system.

Intended Audience

This document is intended primarily for system administrators. It has been written with the assumption that you have a basic understanding of:

- Computer-telephony integration (CTI) concepts, processes, terminology, and applications
- Network design and operation
- Your own network configurations

You should also be familiar with your authentication system, Genesys Framework architecture and functions, and Genesys configuration data structure.

Making Comments on This Document

If you especially like or dislike anything about this document, feel free to e-mail your comments to Techpubs.webadmin@genesyslab.com.

You can comment on what you regard as specific errors or omissions, and on the accuracy, organization, subject matter, or completeness of this document. Please limit your comments to the scope of this document only and to the way in which the information is presented. Contact your Genesys Account Representative or Genesys Technical Support if you have suggestions about the product itself.

When you send us comments, you grant Genesys a nonexclusive right to use or distribute your comments in any way it believes appropriate, without incurring any obligation to you.

Contacting Genesys Technical Support

If you have purchased support directly from Genesys, contact Genesys Technical Support at the following regional numbers:

Region	Telephone	E-Mail
North and Latin America	+888-369-5555 (toll-free) +506-674-6767	support@genesyslab.com
Europe, Middle East, and Africa	+44-(0)-1276-45-7002	support@genesyslab.co.uk
Asia Pacific	+61-7-3368-6868	support@genesyslab.com.au

Region	Telephone	E-Mail
India	1-800-407-436379 (toll-free) +91-(022)-3918-0537	support@genesyslab.com.au
Japan	+81-3-6361-8950	support@genesyslab.co.jp
Before contacting technical support, refer to the *Genesys Technical Support Guide* for complete contact information and procedures.		

Chapter

1 External Authentication Process

This chapter introduces the concept of external authentication and describes how Configuration Server communicates with a third-party authentication server in this schema. It also highlights the procedure for activating external authentication.

This chapter contains the following sections:

Introduction

Genesys software allows you to integrate it with a third-party authentication system. That is, you can deploy a third-party authentication system to control user access to Genesys applications. This way, you can benefit from your established security system, which can be fairly sophisticated and can provide functions that Genesys does not provide. Using an existing authentication system saves you from creating an additional security schema in your Genesys configuration environment.

Configuration Server release 7.0.1 was the first generally available release that supported integration with external authentication systems. In release 7.0.1, Configuration Server supported the only external authentication system that was available at that time—the Remote Authentication Dial In User Service (RADIUS) server. Release 7.1.0 added support for external authentication using Lightweight Directory Access Protocol (LDAP).

To enable and configure RADIUS external authentication, see Chapter 2 on page 21. To enable and configure LDAP Authentication, see Chapter 3 on page 29.

User Verification

To verify the identity of a user who logs in to a Genesys application, Configuration Server can:

- Check the user's permission in the Configuration Database.
- Pass the user's login information to a third-party server and perform the permission verification in the Configuration Database only in case of positive authentication results from the external system.

Warning! There might be instances in which Configuration Server 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 8.0 Configuration Options Reference Manual* for instructions on configuring the `allow-empty-password` option to disallow a blank password.

This document explains the authentication process that involves a third-party authentication server.

When an external system handles the authentication process, Configuration Server communicates with the external authentication server by means of a *pluggable module* that Genesys has developed for a particular third-party server.

Architecture

Figure 1 on page 13 shows connections and information flows when a Genesys CTI installation is integrated with an external authentication system. When logging in to a Genesys application, a user types the user name and password in the standard Genesys Login dialog box. Using the pluggable module, Configuration Server passes the user name and password to the third-party authentication server. The third-party server checks this user's identity with whatever security system is set up and sends the results to Configuration Server.

If the user is authenticated, Configuration Server continues processing the user login:

- If the user has permission for this application in the Configuration Database, he or she can work with the application and access data in the Configuration Database in a way appropriate to this application type.

- If the user does not have permission for this application in the Configuration Database, Configuration Server generates a login error.

If the third-party authentication server does not authenticate the user, Configuration Server generates a login error. The error message appears on the graphical user interface (GUI) from which the user is trying to log in. The exact wording of the message depends on the specific external authentication system in use.

To provide all diagnostics from the external system to the user, Configuration Server passes error and warning messages from external authentication systems to the client.

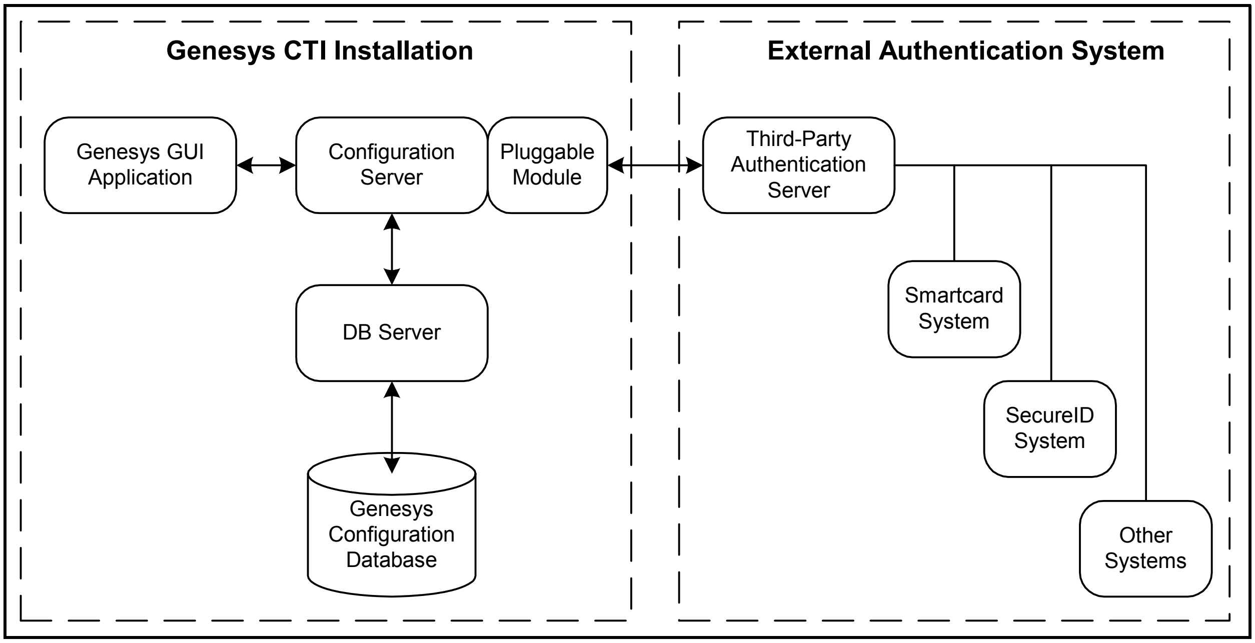


Figure 1: Authentication Architecture Involving an External System

Enabling External Authentication

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 8.0 Deployment Guide.*

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

The following table summarizes how to enable external authentication.

Task Summary: Enabling External Authentication

Objective	Related Procedures and Information
1. Set up the external authentication system.	Refer to the system documentation for your RADIUS or LDAP system.

Task Summary: Enabling External Authentication (Continued)

Objective	Related Procedures and Information
2. Deploy the external authentication module during the installation of Configuration Server release 7.1 or later	Do one of the following, as appropriate: • To deploy RADIUS, follow the instructions in “Deploying RADIUS Authentication” on page 22. • To deploy LDAP, follow the instructions in “Deploying LDAP Authentication” on page 30.
3. Configure Configuration Server to run the selected external authentication systems:	Do one of the following, as appropriate: • For RADIUS, follow the instructions in “Modifying the RADIUS Configuration Files” on page 24. • For LDAP, follow the instructions in “Modifying the Configuration Files” on page 32
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.

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.

To simplify the synchronization of user accounts, use the Genesys Configuration Import Wizard. For information about the wizard, refer to the *Framework 8.0 Imported Configuration Data Formats Reference Manual.*

Customizing External Authentication Configuration

With release 7.2 and later, you can customize the configuration of external authentication for specific Person and Tenant objects. Values specified in the Configuration Server configuration file enable External Authentication and are the default; but Person-specific or Tenant-specific configuration values can override them.

Establishing the Defaults

The authentication section in the Configuration Server configuration file 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” on page 24 or “Modifying the Configuration Files” on page 32.

The authentication section library option of the Configuration Server configuration file 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 enables both LDAP and RADIUS.

Overriding the Defaults by Tenant

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

Procedure: Overriding defaults for Person objects by Tenant

Start of procedure

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 configuration file.
2. In the authentication section, create the option library, and assign it one of the values in Table 1.

Table 1: Tenant-specific External Authentication Providers

Value of Option library	Description
internal	Authentication is performed internally, using the passwords stored in the Genesys database. Do not specify any additional options. Go to Step 4 on page 17.

Table 1: Tenant-specific External Authentication Providers (Continued)

Value of Option library	Description
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. Go to Step 4 on page 17.
gauth_ldap	All users of this Tenant are authenticated through the LDAP server 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. **Note:** You cannot override the global options `verbose`, `retry-attempts`, `retry-interval`, or the content of `ldaperrors.txt`.

3. If the Tenant is using LDAP external authentication (`library=gauth_ldap`), in the `authentication` section, create a set of LDAP server options for each LDAP server, and assign corresponding values. See Table 2. Refer to "LDAP Server Parameters" on page 34 for detailed descriptions of the options.

Table 2: Tenant-specific External Authentication Providers—LDAP

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

Table 2: Tenant-specific External Authentication Providers—LDAP (Continued)

	Option Name	Option Value	Description
Second LDAP server	ldap-url1	<value>	URL of second LDAP server
	app-user1	<value>	Distinguished name of application user for second 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
Third LDAP server	...	...	...
	...	...	...
	Continue configuring groups of options for each LDAP server, as required, up to a maximum of 10 servers.		

4. Restart Configuration Server.

End of procedure

Overriding the Defaults by Person Object

Note: 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 (in Genesys Administrator), or on the General tab (in Configuration Manager), 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 Table 2 on page 16).

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.

High-Availability External Authentication Configurations

You can configure multiple external authentication servers to add to the reliability and efficiency of your system. Instructions for doing so for RADIUS and LDAP are provided in the respective chapters that follow.

Beginning in release 8.0, specific log events are provided to help you determine the state of the connection between Configuration Server and those external authentication servers in your configuration. This is in addition to the troubleshooting functionality described elsewhere in this document.

The following log events provide information about connections between Configuration Server and external authentication servers:

- 24100—Indicates that the connection between Configuration Server and the specified external authentication server has failed, and to which alternate external authentication server Configuration Server is trying to connect.
- 24101—Identifies that no external authentication servers are available. In other words, the connections between Configuration Server and all external authentication servers have failed.
- 24102— Indicates that connection to the specified external authentication server has been restored, and that that server is available for processing authentication requests.

For more information about these log events, refer to *Framework 8.0 Combined Log Events Help*.

Chapter

2 RADIUS External Authentication

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

This chapter contains the following sections:

Overview

Genesys Configuration Server supports all versions of RADIUS, an industry standard for authentication. The architectural schema is identical to the one shown in Figure 1 on page 13, where a RADIUS server acts as a third-party authentication server.

To set up RADIUS:

1. Deploy the RADIUS module during installation of Configuration Server.
2. Modify the RADIUS configuration files.

Note: To disable external authentication, remove the `authentication` section from the configuration file of Configuration Server, and then restart Configuration Server.

Starting in release 7.5, 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.

Deploying RADIUS Authentication

Use the following procedure to deploy RADIUS authentication during Configuration Server installation.

Procedure: Deploying RADIUS external authentication during Configuration Server installation

Purpose: To install the RADIUS pluggable module for your environment where Configuration Server is installed and/or running.

Start of procedure

1. Begin the installation of Configuration Server.
2. On the `Configuration Server Run Mode` page, select `Configuration Server Master Primary`.
3. Continue installing Configuration Server.
4. On the `Configuration Server External Authentication` page, select `Remote Authentication Dial In User Service (RADIUS)`.
5. Finish installing Configuration Server.

End of procedure

Next Steps

- Modify the RADIUS configuration files as described in “Modifying the RADIUS Configuration Files” on page 24.

RADIUS External Authentication Files

Table 3 on page 23 lists the pluggable modules used for communication with the third-party authentication server.

Table 3: 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
Tru64	Not Applicable	libgauth_radius.so
AIX	libgauth_radius_32.so	libgauth_radius_64.so
HP-UX	libgauth_radius_32.sl	libgauth_radius_64.sl
Red Hat Linux	libgauth_radius_32.so	Not Applicable

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.

Configuration Server Configuration File

The Configuration Server configuration file has different names for different operating systems:

- Windows: `confserv.cfg`
- UNIX: `confserv.conf`

During the installation of Configuration Server, a section named `authentication` is added to the configuration file. The `authentication` section indicates that RADIUS external authentication is to be used.

[authentication] Section

This section must be called `authentication`.

library

Specifies `gauth_radius` as the section that specifies the output level for debugging information produced by the Authentication Module. This option is mandatory, and its value is set automatically during installation.

Example

The following is an example of the authentication section in a Configuration Server configuration file:

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

See "Troubleshooting the Connection" on page 27 for information about how to use the gauth-radius section specified here.

Modifying the RADIUS Configuration Files

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

Note: Use the pound sign (#) to comment out a line in a configuration file.

Modifying 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
```

Modifying 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:

1. 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.

2. 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.

3. 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
   ```

4. default_realm—the extension to add to a user name if the RADIUS server required 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, if you specify

   ```
   default_realm        genesys.us
   ```

   and 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
   ```

Deploying RADIUS External Authentication in Geographically Distributed Systems

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.

Procedure: Deploying RADIUS external authentication in Geographically Distributed Systems

Start of procedure

1. Install the Master Configuration Server with RADIUS External authentication, as previously described in this chapter. Before continuing, ensure that the `servers` file contains all of the servers listed in `radiusclient.conf`.
2. Do one of the following:
   - 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`
     - `libgauth_radius_32.so` or `libgauth_radius_64.so`, as appropriate
     - `radius.seq`
     - `radiusclient.conf`
     - `servers`
   - If Configuration Server Proxy is not installed, install it now as described in the *Framework 8.0 Deployment Guide*, being sure to select the RADIUS external authentication option when prompted.
3. In the Configuration Server Proxy `Application` object, configure the following options in the indicated sections, and set them to the specified values:
   - To configure external authentication on Configuration Server Proxy, in the `authentication` section, set the option `library` 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 options of the Configuration Server Proxy `Application` object, as described in the following section, "Troubleshooting the Connection".

4. Restart Configuration Server Proxy.

End of procedure

Troubleshooting the Connection

To obtain debugging information about the connection between any Configuration Server, including Configuration Server Proxy, and the RADIUS server, use the configuration option `verbose` described in this section.

[gauth_radius] Section

This section must be called `gauth_radius`.

verbose

Default Value: `0`
Valid Values:

0	Disables this feature.
1	Produces debug information for the Authentication Module.
2	Produces debug information for the Authentication Module and associated libraries. This is the maximum level, and is recommended.

Changes Take Effect: After Configuration Server is started

Specifies the output level for debugging information that the Authentication Module produces. This information is used to troubleshoot the connection between Configuration Server and the RADIUS server, from the Configuration Server side.

For any Configuration Server except Configuration Server Proxy, add this section and option to the configuration file. For Configuration Server Proxy, add them on the `Options` tab of the Configuration Server Proxy `Application` object, using either Genesys Administrator or Configuration Manager.

Example The following is an example of the `gauth-radius` section in a Configuration Server configuration file, with the value set to the recommended maximum:

```
[gauth_radius]
verbose=2
```

In a High-Availability external authentication configuration, you may also want to use the connection-specific logs that were introduced in release 8.0 to identify and monitor connection problems. See “High-Availability External Authentication Configurations” on page 19.

Chapter

3 LDAP External Authentication

This chapter describes how to set up Lightweight Directory Access Protocol (LDAP) external authentication.

This chapter contains the following sections:

Overview

Management Framework 8.0 supports external authentication using LDAP as a way to verify a user's permissions to log on to Genesys applications. The LDAP Authentication Module (AM) delivers an authentication request to one of the supported LDAP Directory Servers and passes back the results of that authentication to the client.

This LDAP implementation supports all versions of the following LDAP servers:

- Novell E-Directory
- IBM Tivoli Directory Server (or Blue Pages)
- Microsoft Active Directory
- Oracle LDAP Proxy/Internet Directory

Starting in release 7.6, Configuration Server external authentication supports multiple LDAP servers. The active, or responding, authentication server is used for authorization of all subsequent clients. If this server does not respond, the next server in the list is tried, and if it responds, it becomes the active authentication server. This process continues sequentially through the list of authentication servers. The list of servers consists of servers defined in the `ldapclient.conf` file, in the Configuration Server configuration file, and, if customized authentication is used, in the `Annex` of the Tenant or Person `Application` objects.

Starting in release 8.0, LDAP messages concerning the failure (see "Error Codes" on page 40) of each LDAP authentication attempt are relayed from the LDAP AM back through Configuration Server for display to the end user.

Deploying LDAP Authentication

Use the following procedure to deploy LDAP external authentication during Configuration Server installation.

Procedure: Deploying LDAP external authentication during Configuration Server installation

Purpose: To install the LDAP pluggable module for your environment where Configuration Server is installed and/or running.

Note: If you are adding LDAP to an already deployed Configuration Server, you need only to modify the Configuration Server configuration file as described in the "Configuration Server Configuration File" on page 32. You do not need to reinstall Configuration Server

Start of procedure

1. Begin installing Configuration Server (multi-tenant or single-tenant).
2. On the `Configuration Server Run Mode` page, select `Configuration Server Master Primary.`
3. Continue installing Configuration Server.
4. On the `Configuration Server External Authentication` page, select `Lightweight Directory Access Protocol (LDAP).`
5. On the `LDAP Server Access URL` page, do one of the following:
   - If you are going to use only one LDAP server, enter the URL that the Configuration Server will use to connect to the LDAP server.

- If you are going to use multiple LDAP authentication servers, do one of the following:
  - — Specify the first LDAP server on this page. Enter additional LDAP servers in the ldapclient.conf file, as described in "Modifying the Configuration Files" on page 32. Genesys recommends this method if you are upgrading Configuration Server.
  - — Leave the field on this page blank, and specify all the LDAP servers in the ldapclient.conf file. Genesys recommends this method for new installations with multiple LDAP servers.

6. Finish installing Configuration Server.

End of procedure

Next Steps

- Modify the configuration files as described in "Modifying the Configuration Files" on page 32.

External Authentication Files

Table 4 lists the pluggable modules that Genesys provides for LDAP.

Table 4: Pluggable Module Names for LDAP

Operating System	Module for 32-bit Version	Module for 64-bit Version
Windows	gauth_ldap.dll	
Solaris	libgauth_ldap_32.so	libgauth_ldap_64.so
Tru64	Not Applicable	libgauth_ldap.so
AIX	libgauth_ldap_32.so	libgauth_ldap_64.so
HP-UX	libgauth_ldap_32.sl	libgauth_ldap_64.sl
Red Hat Linux	libgauth_ldap_32.so	Not Applicable

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

- ldapclient.sample.conf—an example of an LDAP configuration file. This file can be used as the template for configuring multiple LDAP servers (see "Modifying the ldapclient.conf File" on page 33).
- ldaperrors.txt—contains default LDAP errors. For its content, see "Error Codes" on page 40.
- randgen.rnd—used with Transport Layer Security.

Configuration Server Configuration File

The Configuration Server configuration file has different names for different operating systems:

- Windows: `confserv.cfg`
- UNIX: `confserv.conf`

During the installation of Configuration Server, two sections are added to the Configuration Server configuration file: `[authentication]` and `[gauth_ldap]`. 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.

[authentication] Section

library

Specifies `gauth_ldap` as the section that specifies the external authentication parameters, as described in "[gauth_ldap] Section" below and on page 38. This option is mandatory, and its value is set automatically during installation.

[gauth_ldap] Section

ldap-url

This URL is expressed in the RFC 2255 format, and contains the information needed to access the LDAP server and directory, to retrieve the user's distinguished name.

Enter a URL in this field if you are using only one LDAP server, or if you are upgrading from previous releases of Configuration Server. However, if you are using multiple LDAP servers, and if you are not upgrading Configuration Server, Genesys recommends that you leave this field blank and define all your LDAP servers in the `ldapclient.conf` file.

For a more detailed description of this option, see page 35.

Modifying the Configuration Files

Initially, the Configuration Server configuration file contains only basic information for LDAP. This is sufficient for LDAP external authorization using one LDAP server.

If you want to use more than one LDAP server, you must configure the additional LDAP servers in the `ldapclient.conf` file. Refer to the section "Modifying the ldapclient.conf File" on page 33.

Warning! The ldapclient.conf file cannot be used with Configuration Server 7.5 or earlier.

Before configuring LDAP servers, note the following:

- To maintain backward-compatibility with Configuration Server 7.5 and earlier, Genesys recommends that you define one LDAP server in the gauth_ldap section of the Configuration Server configuration file, and then define any additional LDAP servers in the ldapclient.conf file.
- If this is a first-time installation of a Genesys system, Genesys recommends that you define all LDAP servers in the ldapclient.conf file.

Warning! There might be instances in which Configuration Server 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 8.0 Configuration Options Reference Manual* for instructions on configuring the allow-empty-password option to disallow a blank password.

This section describes the modifications that must be made to the two files. For examples, refer to “Modified Configuration Files” on page 45.

Modifying the ldapclient.conf File

Warning! The ldapclient.conf file cannot be used with Configuration Server 7.5 or earlier.

Theldapclient.conf file specifies all the LDAP servers used for LDAP external authentication. Starting with release 7.6, Configuration Server supports up to ten LDAP authorization servers. The ldapclient.conf file is not created automatically; you must create this file by modifying the ldapclient.sample.conf file that was copied to the destination directory during the installation of Configuration Server.

File Format

The ldapclient.conf file consists of a one or more sections, one section for each LDAP server. The name of each section must be unique, but the sections themselves need not be in any particular order. Genesys recommends naming each section [gauth_ldap_*n*] (where *n* is a numeric identifier in the range of 0 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>
```

The options, or server parameters, are listed in Table 5 on page 35, and described in detail after the table.

Modifying the File

To modify the `ldapclient.conf` file:

1. Do one of the following:
   - If the file already exists, open the file.
   - If the file does not exist, open the `ldapclient.sample.conf` file.
2. For each LDAP authentication server, specify:

   > **Note:** Configuration Server supports a maximum of ten LDAP application servers.
   >
   > Use the pound sign (#) to comment out a line in a configuration file.

   a. A unique section name. Genesys recommends the format `[gauth_ldap_` followed by a unique single-digit identifier and a closing bracket (`]`)—for example, `[gauth_ldap_0]`.

   b. The six parameters listed in Table 6 on page 36, and described immediately following the table.
3. Save the file as `ldapclient.conf`.

Example:

When you are finished, `ldapclient.conf` will contain one or more sections that look like this:

```
[gauth_ldap_0]
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
```

Each section will have a different numeric identifier, however.

LDAP Server Parameters

Table 5 on page 35 lists the parameters for an LDAP authentication server. Each is described in detail after the table.

Table 5: LDAP Server Parameters

Parameter	Definition of value
ldap-url	LDAP URL used to access LDAP server
app-user	Distinguished name of the application user
password	Application user password
cacert-path	Path to CA certificate for LDAP server
cert-path	Path to certificate of client’s key
key-path	Path to client’s private key

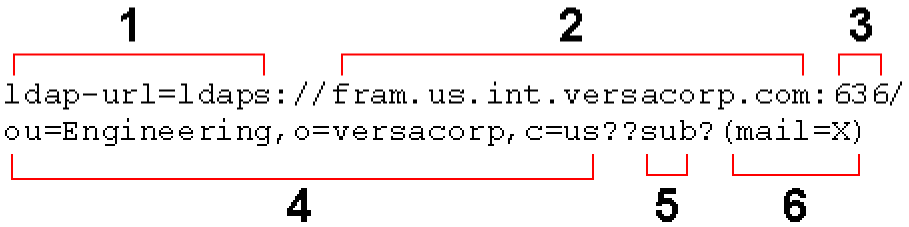
ldap-url

This URL is expressed in the RFC 2255 format, and contains the information needed to access the LDAP server and directory from which it retrieves the user's distinguished name.

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:

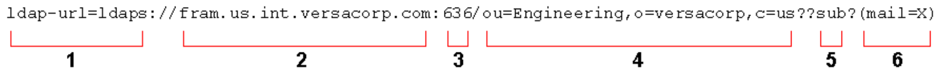
1. LDAP URL in the user's record of the configuration database.
2. LDAP URL specified in the `authentication` section of the Tenant’s `Annex`.
3. LDAP URL in the configuration file.
4. AM default parameters, which cannot be changed by the user.

The following is a sample of an LDAP URL parsed into its parameters (as listed in Table 6 on page 36):



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

This URL contains no spaces and is a single expression that must be entered on a single line. Below is the proper (but in a book, nearly unreadable) form.



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

Table 6: ldap-url parameters

Parameter	Definition of *value*
1 Protocol type	Required. Range: `ldaps` (SSL/TLS secure) or `ldap` (unsecure).
2 LDAP server host name	Optional. Default is the local host. 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 represents a risk. Genesys strongly advises using a secure connection.
4 Base DN	Required. Defines the node in the LDAP tree to use as base for the LDAP search. 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). Range: `base, one, sub.`
6 Search filter	Optional. Limits the search by searching for a match with a specified field. Default: `mail`. In the example, 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, as follows: • In Genesys Administrator—`Person` object > `Configuration` tab > `General` section > `External ID` • In Configuration Manager—`Person` object > `General` tab > `External Authentication` area > `External User ID`

app-user

Distinguished name (which includes location in the directory tree and in any containers) of the application account used by AM to search for the user's information that is needed to perform an authentication.

password

Password of the application account. Required if the `app-user` parameter is set. This parameter must be encrypted inside the configuration file. To do so, you must start Configuration Server in its special encryption mode with these parameters:

`confserv -p gauth_ldap` *`password`*, where *password* is the actual value.

cacert-path

Full path to the file containing a certificate of a trusted Certificate Authority, which is used to negotiate a secure LDAP connection to the server. Required for a secured connection.

cert-path

Full path to the file containing a certificate of the LDAP client's private key.

Note: The certificate must be in Base64 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.

key-path

Full path to the file containing an LDAP client's private key.

Note: 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 SSL authentication.

Modifying the Configuration Server Configuration File

The `[authentication]` and `[gauth_ldap]` sections of the Configuration Server configuration file, specify that Configuration Server will use LDAP external authentication. Add the following parameters as required.

[authentication] Section

enforce-external-auth

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

Warning! Do not set `enforce-external-auth` to `true` until you have configured all of the accounts in the configuration.

[gauth_ldap] Section

verbose

Output level for debugging information produced by the Authentication Module (AM). Optional. Range:

`0` (false) - turns off all debugging.

`1` - activates output of the AM itself.

`2` - activates output of LDAP/SSL libraries.

retry-attempts

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 `ldapclient.conf file.`

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".

Default value is `3`.

retry-interval

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`.

Default value is `10`.

Note: If, for purposes of backward compatibility, you want to specify an LDAP server in this file, add the necessary options (described in "LDAP Server Parameters" on page 34) to this section. However, this LDAP server must be included in the total number of LDAP servers supported by Configuration Server (the maximum is ten).

Security Considerations

To ensure a secure LDAP environment, Genesys strongly recommends that you do the following:

- Set the Genesys URL used to access LDAP to use LDAPS (secure LDAP) protocol.
- Configure your LDAP server to prevent anonymous or unauthenticated access. For example, do not configure LDAP users with blank or empty passwords. This is in addition to not configuring users with empty passwords in the Configuration Database, as described on page 33.
- Configure your LDAP server to prevent the directory base being set to `null`.
- Restrict knowledge of the structure of your LDAP data. For example, some of this information is contained in the ExternalID field of Users objects in the Configuration Database. Therefore, a user who has access to these objects could figure out the LDAP structure.

For more information and recommendations for securing your LDAP environment, refer to the LDAP benchmarks published by the Center for Internet Security and available on the Center's web site.

Error Handling

When there is an error, the LDAP AM delivers two error-related properties to Configuration Server: `error code` and `error description string.` The property `Error code` is reported in the log files, but only the property `error description string` is shown on the client's GUI.

The LDAP AM uses one of three methods to extract this property (listed from highest priority to lowest):

1. Explicit error description returned by the LDAP server.
2. Error description produced from an error code based on the mapping table inside the Authentication Module. This table is populated from a supplied and configured LDAP error description file (`ldaperrors.txt`). See "Error Codes" on page 40.
3. Error description produced from a standard LDAP error code. See "Error Codes" on page 40.

Management Layer Configuration

You can configure the Management Layer to generate various alarms in response to error codes sent from the LDAP AM. See the *Framework 8.0 Management Layer User's Guide.*

Special Treatment

If the LDAP AM receives an error code that is marked for retry in the error description file (see "Error Codes"), it initiates retry attempts according to the policy described in the `retry-attempts` and `retry-interval` parameters in the configuration file. A negative response is returned back to the client only after all retry attempts on all available servers were completed without success.

Error Codes

The LDAP Directory Administrator (Novel E-Directory, IBM Tivoli Directory Server, or Microsoft Active Directory) defines the error codes. Please refer to their documentation.

The following is the content of the default error file (`ldaperrors.txt`) that corresponds to the error descriptions in the OpenLDAP client package:

```
; server codes
1             Operations error
2             Protocol error
3             Time limit exceeded
4             Size limit exceeded
5             Compare False
6             Compare True
7             Authentication method not supported
8             Strong(er) authentication required
9             Partial results and referral received
10            Referral
11            Administrative limit exceeded
12            Critical extension is unavailable
13            Confidentiality required
14            SASL bind in progress
16            No such attribute
17            Undefined attribute type
18            Inappropriate matching
19            Constraint violation
20            Type or value exists
21            Invalid syntax
32            No such object
33            Alias problem
34            Invalid DN syntax
35            Entry is a leaf
36            Alias dereferencing problem
47            Proxy Authorization Failure
48            Inappropriate authentication
49            Invalid credentials
50            Insufficient access
51            Server is busy
52            Server is unavailable
53            Server is unwilling to perform
54            Loop detected
```

```
64            Naming violation
65            Object class violation
66            Operation not allowed on non-leaf
67            Operation not allowed on RDN
68            Already exists
69            Cannot modify object class
70            Results too large
71            Operation affects multiple DSAs
80            Internal (implementation specific) error
; API codes
81            Can't contact LDAP server
82            Local error
83            Encoding error
84            Decoding error
85            Timed out
86            Unknown authentication method
87            Bad search filter
88            User cancelled operation
89            Bad parameter to an ldap routine
90            Out of memory
91            Connect error
92            Not Supported
93            Control not found
94            No results returned
95            More results to return
96            Client Loop
97            Referral Limit Exceeded
; Old API codes
-1            Can't contact LDAP server
-2            Local error
-3            Encoding error
-4            Decoding error
-5            Timed out
-6            Unknown authentication method
-7            Bad search filter
-8            User cancelled operation
-9            Bad parameter to an ldap routine
-10           Out of memory
-11           Connect error
-12           Not Supported
-13           Control not found
-14           No results returned
-15           More results to return
-16           Client Loop
-17           Referral Limit Exceeded
16640         Content Sync Refresh Required
16654         No Operation
16655         Assertion Failed
16656         Cancelled
16657         No Operation to Cancel
16658         Too Late to Cancel
```

```
16659         Cannot Cancel
; retry-errors: 81 85 91 -1 -11
```

Error Messages

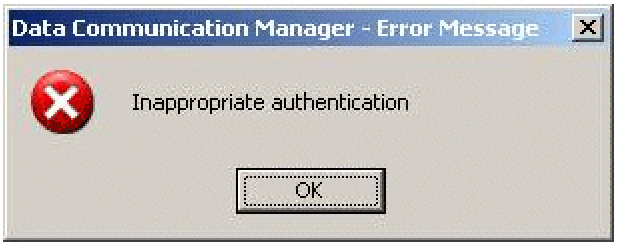
This section describes error messages returned by the LDAP server.

Note: The messages in this section correspond to standard LDAP messages. However, your particular LDAP server may be configured to produce different messages in the same situations.

Inappropriate Authentication

A message similar to that shown in Figure 2 may appear when *both* of the following conditions are true:

- Option `allow-empty-password` is set to `true` (the default).
- A blank password has been passed to the LDAP AM.



Data Communication Manager - Error Message

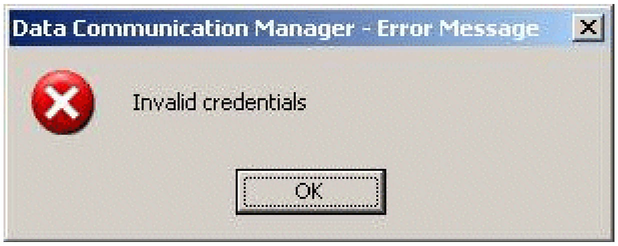
Inappropriate authentication

Figure 2: Error Message—Blank Password

To correct this error, log on to your GUI application with a valid non-empty password. See page 32 for more information.

Invalid Credentials

A message similar to that shown in Figure 3 may appear when an incorrect password has been passed to the LDAP AM.



Data Communication Manager - Error Message

Invalid credentials

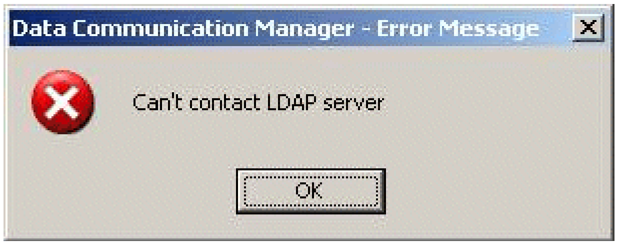
Figure 3: Error Message—Incorrect Password

To correct this error, log on to your GUI application with a valid non-empty password. See page 32 for more information.

Can't Contact LDAP Server

A message similar to that shown in Figure 4 may appear when the Configuration Server cannot contact any LDAP server for one or more of the following reasons:

- The LDAP server is down.
- The LDAP server cannot be accessed due to network problems.
- If you configured Genesys Security Using the TLS Protocol, one or more security parameters specified in the configuration file are not valid.



Data Communication Manager - Error Message

Can't contact LDAP server

Figure 4: Error Message—LDAP Server is Not Accessible

To correct this error, do the following:

- Check that at least one LDAP server is running.
- Check that at least one LDAP server is accessible over the network.
- If you configured Genesys Security Using the TLS Protocol, check that the security parameters specified in the configuration file are valid.

Technical Notes

SSL Parameters

Genesys LDAP Authentication supports SSLv3 and TLSv1. It supports server authentication and server+client authentication.

If the LDAP server is configured to perform server-only authentication, then the only SSL parameter to configure is `cacert-path`, which specifies a file where the Certificate Authority certificate file that is related to the LDAP server is stored.

If the LDAP server is configured to perform server and client authentication, there must be two additional parameters configured besides `cacert-path`: `cert-path` which specifies a file where the client certificate is stored and `key-path` is stored where the client's private key is stored.

Note: Genesys LDAP Authentication supports only the PEM (Base64) format of the certificates. You must convert certificates of all other formats to the PEM (Base64) format.

Application Account

An optional (but worthy) idea is to configure a special dedicated account in the LDAP repository that can be called the “application account.” If it exists, the LDAP AM uses this account to perform its search for the distinguished name of the user being authenticated and to maintain the LDAP inbound connection between authentications. You should configure the application account parameters (`DN (app-user)` and `password (password)`) in the Configuration Server configuration file. The password parameter should be encrypted by using the special startup mode of Configuration Server.

Troubleshooting the Connection

In a High-Availability external authentication configuration, you can use the connection-specific logs that were introduced in release 8.0 to identify and monitor connection problems. See “High-Availability External Authentication Configurations” on page 19.

Examples

Note: All examples belong on single lines. They appear here in a large font, which causes the examples to wrap across multiple lines, for readability.

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 ³ou=Engineering
Department,o=vcorp,c=us¿ -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
```

Corresponding LDAP search syntax:

```
ldapsearch ·p 636 -h fram.us.int.vcorp.com -b
³ou=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`

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

Modified Configuration Files

This section contains examples of modified configuration files for two scenarios.

LDAP Server Defined in ldapclient.conf File

```
# content of Configuration Server configuration file
...
[authentication]
library=gauth_ldap
...
[gauth_ldap]
verbose=false
retry-attempts=3
retry-interval=10
...

# content of ldapclient.conf file
[gauth_ldap_0]
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

[gauth_ldap_1]
ldaps://fram.us.int.vcorp.com:677/ou=Eng,o=vcorp,c=us??sub?(mail=X)
app-user=cn=Manager,o=vcorp,c=us
password=1357XYZ9
cacert-path=keys/server.arm
cert-path=keys/client.arm
key-path=keys/private.pem
```

One LDAP Server Defined in Configuration Server Configuration File, and the Rest Defined in the ldapclient.conf File

```
# content of Configuration Server configuration file
...
[authentication]
library=gauth_ldap
...
[gauth_ldap]
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
verbose=false
retry-attempts=3
retry-interval=10
```

```
...


# content of ldapclient.conf file

[gauth_ldap_0]
ldaps://fram.us.int.vcorp.com:123/ou=Eng,o=vcorp,c=us??sub?(mail=X)
app-user=cn=Manager,o=vcorp,c=us
password=4321DHFG9
cacert-path=keys/server.arm
cert-path=keys/client.arm
key-path=keys/private.pem

[gauth_ldap_1]
ldaps://fram.us.int.vcorp.com:567/ou=Eng,o=vcorp,c=us??sub?(mail=X)
app-user=cn=Manager,o=vcorp,c=us
password=1357XYZ9
cacert-path=keys/server.arm
cert-path=keys/client.arm
key-path=keys/private.pem
```

Appendix

Importing User Data from External Sources

This chapter describes how to create user records in the Genesys configuration that are required when using a RADIUS or LDAP external authentication system.

This chapter contains the following sections:

Introduction

To authenticate a user in a Genesys program using one of the external authentication systems (RADIUS or LDAP), create in the Genesys configuration a user record that matches a record in the external authentication system.

When you create the user record, you must specify these three properties: `User name`, `Employee ID`, and `External User ID`. Table 7 describes these properties.

Table 7: Mandatory User Record Properties

Property	Description
`User name`	Corresponds to `name` in the XML schema. This property is the user's Genesys logon ID, and it uniquely identifies the user in the Genesys configuration. It must be unique across the entire configuration. For a RADIUS server, this property corresponds to the `user name` in the RADIUS system.

Table 7: Mandatory User Record Properties (Continued)

Property	Description
Employee ID	Corresponds to employeeID in the XML schema. This numeric user ID is assigned by the user's company. This ID does not participate in authentication, but is still required by Configuration Server.
External User ID	Corresponds to externalID in the XML schema. Required by LDAP configuration only. Configuration Server uses this ID to match a record in the Genesys configuration with a record in the LDAP directory server. Specifically, Configuration Server substitutes an X symbol in the LDAP URL filter with the value of this property. The filter is part 6 of the LDAP URL; see "Configuration Server Configuration File" on page 32. Therefore, if the filter in the LDAP URL is (mail=X), then the External User ID property in Genesys configuration represents the mail attribute of the user record in LDAP server.

Note: You can also populate other fields—for example, E-Mail, First name, and Last name—but neither the authentication process nor Configuration Server requires them.

Creating a User Record in the Genesys Configuration

This section describes three suggested methods to create a user record in your Genesys configuration:

Manual Entry using Genesys Administrator or Configuration Manager

Use Genesys Administrator or Configuration Manager to create user records manually, one by one. To do this, create a Person object under one of the folders designated to store Persons information. There is no bulk process available. Be certain to populate all three mandatory fields.

Import an XML data file using Configuration Import Wizard

Create an XML file containing the user records and then import it using the Configuration Import Wizard (CIW). With this method, you can add several user records to Configuration Server in a single stroke. Use the CIW `Import Agent Data` and then `Raw XML Data` modes to import. You may create either the `CfgAgent` object (ordinary Call Center operator), or the `CfgPerson` object (Administrator).

The XML file can also contain records which update or remove user information from Configuration Server. See "Sample XML Data File".

Import XML Data using the Genesys Configuration SDK

Use the Genesys Configuration SDK to create custom programs which write user information to Configuration Server in XML format.

These custom programs can be written in Java, Visual Basic script or JavaScript. They can monitor changes to the user information on the LDAP directory server, then transform those changes to the format described in the latest version of the *Configuration SDK Web Services API Reference,* and write them directly to Configuration Server.

Sample XML Data File

This sample XML data file contains the three properties that are required by external authentication:

```
<CfgData mode="mt" xmlns="http://www.genesyslab.com/cs">

<CfgReference>
  <CfgProviderTenantRef id="Environment" name="Environment"/>
  <CfgAgentRef id="AgentToUpdate" name="smith"/>
</CfgReference>

<CfgCreate>
  <CfgAgent
    id="Betty"
    firstName="Betty"
    lastName="Smith"
    employeeID="00001"
    name="bettys"
    ownerDBID="Environment"
    emailAddress="bettys@company.com"
    externalID="bettys@company.com"/>
</CfgCreate>

<CfgUpdate>
```

```
   <CfgAgentUpdate id="UpdateAgent" DBIDref="AgentToUpdate"
externalID=newmail@Company.com/>
</CfgUpdate>

<CfgRemove>
   <CfgAgentRef id="AgentToRemove" name="Johnson"/>
</CfgRemove>

</CfgData>
```

You could use this data to import user information into the Genesys Database with either the Configuration Import Wizard or the Genesys Configuration SDK.

Related Documentation Resources

The following resources provide additional information that is relevant to this software. Consult these additional resources as necessary.

Genesys Framework

- *Framework 8.0 Architecture Help,* which will help you understand the Genesys Framework architecture.
- *Framework 8.0 Deployment Guide,* which will help you install and configure the Genesys Framework components.
- *Framework 8.0 Genesys Administrator Help,* which will help you configure and create any necessary configuration objects in Genesys Administrator.
- *Framework 8.0 Configuration Manager Help,* which will help you configure and create any necessary configuration objects in Configuration Manager.
- *Framework 8.0 Configuration Options Reference Manual,* which will provide you with the configuration option descriptions for Configuration Server and other Framework components.
- *Genesys 8.0 Security Deployment Guide*, which will help you understand Genesys security and permissions schema.

Genesys

- *Genesys Technical Publications Glossary,* which ships on the Genesys Documentation Library DVD and which provides a comprehensive list of the Genesys and computer-telephony integration (CTI) terminology and acronyms used in this document.

- *Genesys Migration Guide*, which ships on the Genesys Documentation Library DVD, and which provides documented migration strategies for Genesys product releases. Contact Genesys Technical Support for more information.
- Release Notes and Product Advisories for this product, which are available on the Genesys Technical Support website at `http://genesyslab.com/support`.

Information about supported hardware and third-party software is available on the Genesys Technical Support website in the following documents:

- *Genesys Supported Operating Environment Reference Manual*
- *Genesys Supported Media Interfaces Reference Manual*

For additional system-wide planning tools and information, see the release-specific listings of System Level Documents on the Genesys Technical Support website, accessible from the `system level documents by release` tab in the Knowledge Base `Browse Documents` Section.

Genesys product documentation is available on the:

- Genesys Technical Support website at `http://genesyslab.com/support`.
- Genesys Documentation Library DVD, which you can order by e-mail from Genesys Order Management at `orderman@genesyslab.com`.

Document Conventions

This document uses certain stylistic and typographical conventions—introduced here—that serve as shorthands for particular kinds of information.

Document Version Number

A version number appears at the bottom of the inside front cover of this document. Version numbers change as new information is added to this document. Here is a sample version number:

80fr_ref-exta_06-2008_v8.0.001.00

You will need this number when you are talking with Genesys Technical Support about this product.

Screen Captures Used in This Document

Screen captures from the product graphical user interface (GUI), as used in this document, may sometimes contain minor spelling, capitalization, or grammatical errors. The text accompanying and explaining the screen captures corrects such errors *except* when such a correction would prevent you from installing, configuring, or successfully using the product. For example, if the name of an option contains a usage error, the name would be presented exactly as it appears in the product GUI; the error would not be corrected in any accompanying text.

Type Styles

Table 8 describes and illustrates the type conventions that are used in this document.

Table 8: Type Styles

Type Style	Used For	Examples
Italic	• Document titles • Emphasis • Definitions of (or first references to) unfamiliar terms • Mathematical variables Also used to indicate placeholder text within code samples or commands, in the special case where angle brackets are a required part of the syntax (see the note about angle brackets on page 56).	Please consult the *Genesys 8 Migration Guide* for more information. Do *not* use this value for this option. A *customary and usual* practice is one that is widely accepted and used within a particular industry or profession. The formula, $x + 1 = 7$ where x stands for . . .

Table 8: Type Styles (Continued)

Type Style	Used For	Examples
Monospace font (Looks like `teletype` or `typewriter text`)	All programming identifiers and GUI elements. This convention includes: • The *names* of directories, files, folders, configuration objects, paths, scripts, dialog boxes, options, fields, text and list boxes, operational modes, all buttons (including radio buttons), check boxes, commands, tabs, CTI events, and error messages. • The values of options. • Logical arguments and command syntax. • Code samples. Also used for any text that users must manually enter during a configuration or installation procedure, or on a command line.	Select the `Show variables on screen` check box. In the `Operand` text box, enter your formula. Click `OK` to exit the `Properties` dialog box. T-Server distributes the error messages in `EventError` events. If you select `true` for the `inbound-bsns-calls` option, all established inbound calls on a local agent are considered business calls. Enter `exit` on the command line.
Square brackets ([ ])	A particular parameter or value that is optional within a logical argument, a command, or some programming syntax. That is, the presence of the parameter or value is not required to resolve the argument, command, or block of code. The user decides whether to include this optional information.	`smcp_server -host [/flags]`
Angle brackets (< >)	A placeholder for a value that the user must specify. This might be a DN or a port number specific to your enterprise. **Note:** In some cases, angle brackets are required characters in code syntax (for example, in XML schemas). In these cases, italic text is used for placeholder values.	`smcp_server -host <confighost>`

Index