



Framework 8.5

External Authentication

Reference Manual

The information contained herein is proprietary and confidential and cannot be disclosed or duplicated without the prior written consent of Genesys Telecommunications Laboratories, Inc.

Copyright © 2002–2014 Genesys Telecommunications Laboratories, Inc. All rights reserved.

About Genesys

Genesys is the world's leading provider of customer service and contact center software - with more than 4,000 customers in 80 countries. Drawing on its more than 20 years of customer service innovation and experience, Genesys is uniquely positioned to help companies bring their people, insights and customer channels together to effectively drive today's customer conversation. Genesys software directs more than 100 million interactions every day, maximizing the value of customer engagement and differentiating the experience by driving personalization and multi-channel customer service - and extending customer service across the enterprise to optimize processes and the performance of customer-facing employees. Go to www.genesys.com for more information.

Each product has its own documentation for online viewing at the Genesys Documentation 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. © 2014 Genesys Telecommunications Laboratories, Inc. All rights reserved. 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 Customer Care](#). Before contacting Customer Care, please refer to the [Genesys Care Program Guide](#) for complete contact information and procedures.

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.genesys.com

Document Version: 85fr_ref-exta_04-2014_v8.5.001.00



Table of Contents

List of Procedures	7
Preface	9
About External Authentication	9
Intended Audience	10
Making Comments on This Document	10
Contacting Genesys Customer Care	10
Changes in this Document	10
Chapter 1	External Authentication Process 11
Introduction	11
Architecture	12
Enabling External Authentication	13
Configuring the Master Configuration Server	14
Synchronizing User Accounts	15
Person Objects and External IDs	15
Customizing External Authentication Configuration	15
High-Availability External Authentication Configurations	21
Disabling External Authentication	21
Troubleshooting the External Authentication Connection	21
Chapter 2	RADIUS External Authentication 23
Overview	23
Task Summary	24
Deploying RADIUS Authentication	24
Modifying the RADIUS Configuration Files	26
Modifying the Servers File	26
Modifying the radiusclient.conf File	27
Deploying RADIUS on Configuration Server Proxy	28

Chapter 3	LDAP External Authentication	31
	Overview.....	31
	External Authentication Files	32
	Task Summary.....	33
	Deploying LDAP	33
	Configuration Server Options	34
	Configuring LDAP Servers	36
	Deploying LDAP on Configuration Server Proxy	37
	Using LDAP in a Multi-Tenant Configuration	38
	Using LDAP Referrals	38
	Security Considerations.....	39
	Error Handling	40
	Error Codes	40
	Error Messages	42
	Technical Notes	44
	SSL Parameters	44
	Application Account	44
	Examples.....	45
	LDAP URL	45
	gauth_Idap Section Using IBM RACF.....	46
	Configuration Options.....	46
	Setting Configuration Options.....	47
	Mandatory Options	47
	authentication Section	47
	gauth_Idap and gauth_Idap_n Sections	48
 Chapter 4	 Kerberos External Authentication	 55
	Overview.....	55
	Kerberos vs RADIUS/LDAP	55
	Supported Environments	56
	Configuring Kerberos.....	56
	Kerberos Initialization File.....	61
	Redundant Configuration Servers	62
	Configuration Options.....	62
	Setting Configuration Options.....	63
	Mandatory Options	63
	authentication Section	63
	gauth_kerberos Section.....	63
 Appendix A	 Importing User Data from External Sources.....	 65
	Introduction.....	65

	Creating a User Record in the Genesys Configuration	66
	Manual Entry using Genesys Administrator.....	66
	Import an XML data file using Configuration Import Wizard	67
	Import XML Data using the Genesys Configuration SDK	67
	Sample XML Data File.....	67
Appendix B	Sample Certificate Authority Certificates File	69
	CA Certificates File.....	69
	Output Using OpenSSL Utility	70
	Configuring Server Authentication.....	72
Appendix C	Sample Kerberos Configuration	73
	MIT Key Distribution Center	73
	Microsoft Active Directory	74
Supplements	Related Documentation Resources	77
	Document Conventions	79
Index	81



List of Procedures

Overriding defaults for Person objects by Tenant	16
Deploying RADIUS external authentication during Configuration Server installation.	25
Deploying RADIUS external authentication on Configuration Server Proxy	28
Deploying LDAP during Configuration Server installation	33
Configuring Kerberos on Configuration Server or Configuration Server Proxy	56
Installing Kerberos on Configuration Server/Proxy host running Windows 32-bit	57
Installing Kerberos on Configuration Server/Proxy host running Windows 64-bit	58
Installing Kerberos on Configuration Server/Proxy host running RHEL	58
Installing Kerberos on Configuration Server/Proxy host running Solaris 10 64-bit.	59
Installing Kerberos on Configuration Server/Proxy host running AIX 64-bit.	60



Preface

Welcome to the *Framework 8.5 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 8.5 release(s) of this product.

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

This preface contains the following sections:

- [About External Authentication, page 9](#)
- [Intended Audience, page 10](#)
- [Making Comments on This Document, page 10](#)
- [Contacting Genesys Customer Care, page 10](#)
- [Changes in this Document, page 10](#)

For information about related resources and about the conventions that are used in this document, see the supplementary material starting on [page 77](#).

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.

- How to configure Kerberos external authentication.

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@genesys.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 Customer Care 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 Customer Care

If you have purchased support directly from Genesys, please contact [Genesys Customer Care](#).

Before contacting Customer Care, please refer to the [Genesys Care Program Guide](#) for complete contact information and procedures.

Changes in this Document

This is the first release of the *Framework 8.5 External Authentication Reference Manual*. In the future, this section will list topics that are new or have changed significantly since the first release of this document.



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, page 11](#)
- [Architecture, page 12](#)
- [Enabling External Authentication, page 13](#)
- [High-Availability External Authentication Configurations, page 21](#)
- [Disabling External Authentication, page 21](#)
- [Troubleshooting the External Authentication Connection, page 21](#)

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.

To enable and configure RADIUS external authentication, see Chapter 2 on [page 23](#). To enable and configure LDAP Authentication, see Chapter 3 on [page 31](#).

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 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.

Starting in release 8.1, only users with a valid External ID will be considered for external authentication, unless the option `enforce-external-auth` is set to `true`. Genesys recommends that the `default` user not be configured with an External ID, to allow for system access if all external authentication servers are down.

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.

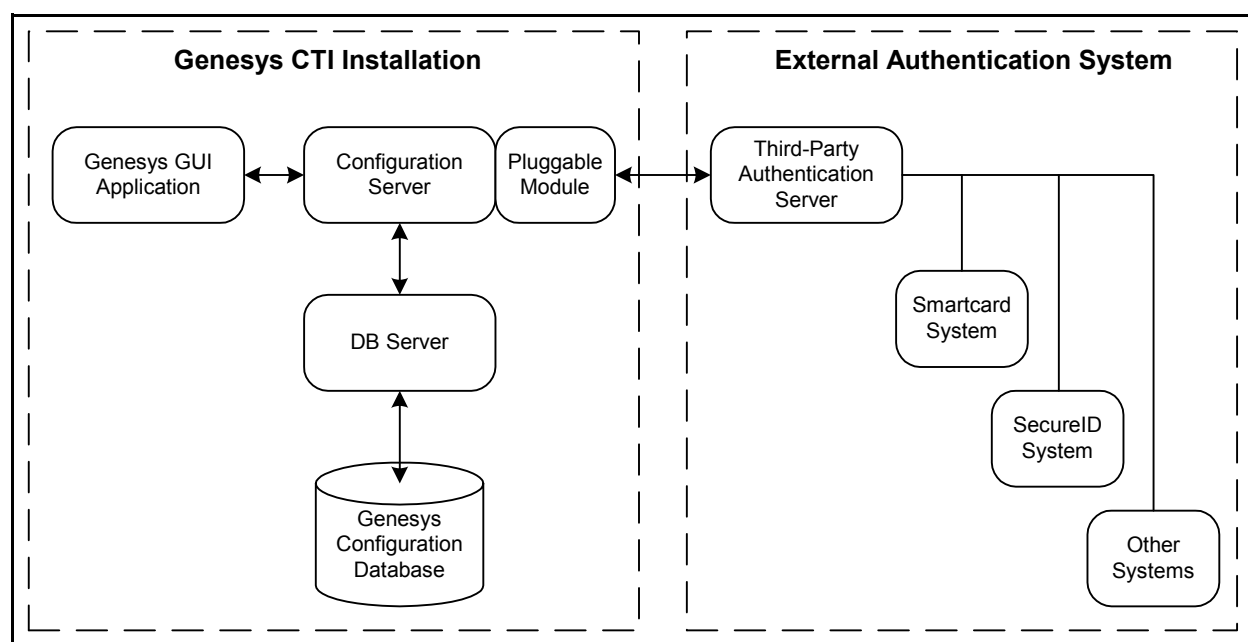


Figure 1: Authentication Architecture Involving an External System

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 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.
2. Deploy the external authentication module during the installation of Configuration Server.	Do one of the following, as appropriate: <ul style="list-style-type: none"> To deploy RADIUS, follow the instructions in “Deploying RADIUS Authentication” on page 24. To deploy LDAP, follow the instructions in “Deploying LDAP” on page 33.
3. Configure Configuration Server to run the selected external authentication systems:	Do one of the following, as appropriate: <ul style="list-style-type: none"> For RADIUS, follow the instructions in “Modifying the RADIUS Configuration Files” on page 26. For LDAP, follow the instructions in “Configuring LDAP Servers” on page 36.
4. Start Configuration Server.	Refer to the <i>Framework Deployment Guide</i> 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.

Configuring the Master Configuration Server

A new installation of the Master Configuration Server at its first startup reads values from its configuration file and saves those values in the Configuration Database. On all subsequent starts, it reads all values from the database and ignores those in its configuration file. (The backup Master Configuration Server, if configured, saves the information when the first switchover is completed.) As a result, you must make any changes to server-level external authentication parameters in the `Options` tab of the Configuration Server and Configuration Server Proxies. Any changes you make in the configuration file are ignored.

The only exception to this is the option `enforce-external-auth` (see [page 47](#)). If this option is set to `true` in the database, but a newly installed Configuration Server reads its configuration file and finds the option set to `false`, Configuration Server sets it to `false` in the database. This ensures that all users are authenticated internally, including those without an External ID.

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*.

Person Objects and External IDs

To be considered for external authentication, a Person must be configured with an External ID. In the simplest case, the External ID, it could be equal to the person's account name.

Customizing External Authentication Configuration

You can customize the configuration of external authentication for specific Person and Tenant objects. Values specified in the Configuration Server options enable External Authentication and are the default; but values defined at the Person or Tenant level can override them.

Note: In release 8.1 and later, it is possible to use the same configuration sections and options at the server-level, Tenant-level, and Person-level. Genesys recommends this approach. Furthermore, Genesys recommends that in a multi-tenant or otherwise distributed environment, external authentication be configured at the Tenant level to simplify the configuration process and ensure consistency system-wide.

Establishing the Defaults

The `authentication` section in Configuration Server options enables External Authentication, and defines the default External Authentication values for all Person objects within the configuration. For details, see “Modifying the RADIUS Configuration Files” on [page 26](#) or “Configuration Server Options” on [page 34](#).

The `library` option in the `authentication` section must specify a value for each External Authentication provider that your implementation supports:

- The value `gauth_ldap` enables LDAP authentication.
- The value `gauth_radius` enables RADIUS authentication.

- The value `gauth_ldap`, `gauth_radius` or `gauth_radius, gauth_ldap` enables both LDAP and RADIUS.
- The value `gauth_kerberos` enables Kerberos authentication. This applies only to the server on which it is configured; it cannot be customized at the tenant or user level.
- The value `internal`, available only for setting at the Tenant or Person level, means that all users associated with the object in which the option is set to this value must validate internally.

Overriding the Defaults by Tenant

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

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 options.
2. In the authentication section, create the option `library`, and assign it one of the values in Table 1 on [page 16](#).

Table 1: Tenant-specific External Authentication Providers

Value of <code>library</code>	Description
<code>internal</code>	Authentication is performed internally, using the passwords stored in the Genesys database. Do not specify any additional options.
<code>gauth_radius</code>	All users of this Tenant are authenticated using the RADIUS access parameters specified in the local <code>radiusclient.conf</code> configuration file. Do not specify any additional options. Note that you cannot assign different Tenants to different RADIUS servers.

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

Value of library	Description
gauth_ldap	<p>All users of this Tenant are authenticated through one or more LDAP server, each defined in a <code>gauth-ldap</code> or <code>gauth_ldap_n</code> (see “Configuring LDAP Servers” on page 36) and specified in the additional option <code>ldap-url</code>. You must specify at least one <code>ldap-url</code> option. You can specify other LDAP-related options, such as <code>password</code>, or more <code>ldap-url</code> options to specify a specific set of LDAP servers. You must define all valid LDAP-specific options in the Annex of the Tenant object.</p> <p>Note: You cannot override the global option <code>verbose</code> or the content of <code>ldaperrors.txt</code>. In addition, settings defined at the Tenant level can be overridden for individual users at the Person level.</p>

3. If the Tenant is using LDAP external authentication (`library=gauth_ldap`), create a `gauth_ldap` section for the first LDAP server and a `gauth_ldap_n` section for each additional server on the Tenant’s Annex tab, and assign appropriate values to the options in each section. Refer to “Configuring LDAP Servers” on [page 36](#) for detailed information about configuring multiple LDAP servers, and to “Configuration Options” on [page 46](#) for detailed descriptions of the options.

If you have existing Tenant, server, or Person objects that use legacy options (listed in [Table 2](#)) in the `authentication` section, Genesys recommends that you migrate to the `gauth_ldap[_n]` (where `n` is 1 to 9) section format as soon as possible, for security reasons. If you have both current options (in `gauth-ldap[_n]` sections) and legacy options (in the `authentication` section) configuration, the legacy options will be ignored.

End of procedure

Table 2: Legacy Tenant-specific External Authentication Servers—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
	idle-timeout	<value>	Time interval that the LDAP connection to the first LDAP server will be kept open if there are no more requests
	retry-attempts	<value>	Number of authorization retries that will be generated by Configuration Server if the first LDAP server does not respond
	retry-interval	<value>	Time that Configuration Server waits for an authorization reply from the first LDAP server.
	connect-timeout	<value>	Time that Configuration Server waits after initial connection before deeming first LDAP server to be unavailable.

Table 2: Legacy Tenant-specific External Authentication Servers—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
	idle-timeout2	<value>	Time interval that the LDAP connection to the second LDAP will be kept open if there are no more requests.
	retry-attempts2	<value>	Number of authorization retries that will be generated by Configuration Server if the second LDAP server does not respond.
	retry-interval2	<value>	Time that Configuration Server waits for an authorization reply from the second LDAP server.
	connect-timeout2	<value>	Time that Configuration Server waits after initial connection before deeming second LDAP server to be unavailable.
Third LDAP server

	Continue configuring groups of options for each LDAP server, as required, up to a maximum of 10 servers.		

Overriding the Defaults by Person Object

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 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 [Step 3 on page 17](#)).

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, as follows:

- For LDAP, redundant configurations are supported with each additional servers configured in [gauth_ldap_n] sections. This can be done at all levels—server, tenant, and user.
- For RADIUS, redundant authentication servers are configured in the redisuclient.conf configuration file of Configuration Server. This can be done only at the server level.
- For Kerberos, redundant configurations are not supported, each configuration applies only to the server for which it is configured.

Disabling External Authentication

To disable external authentication at the Tenant or Person level, set the `library` option in the `authentication` section to `internal` in the object. For Configuration Server or Configuration Server Proxy, set the option to an empty value, and then restart the server to unload the authentication module and stop the authentication.

Refer to [page 25](#) (for RADIUS) or [page 48](#) (for LDAP) for information about the `library` option.).

Troubleshooting the External Authentication Connection

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

[authentication] Section

This section must be called `authentication`.

verbose

Default Value: `0`

Valid Values:

`0` Disables this feature.

- 1 Produces debug information involving only unexpected situations, data, or internal states.
- 2 Produces debug information without OpenLDAP library output. (The newer OpenLDAP contains a much larger internal debug size, which reduces system performance. This is the recommended level.
- 3 Produces debug information, including all OpenLDAP library output.

Changes Take Effect: If switching of OpenLDAP output occurs, the changes take effect when the next connection is created (after disconnection, timeout expiry, or switch to a new LDAP server). Otherwise, the changes take effect immediately, when the next authentication request is processed.

Specifies the output level for debugging information for the external authentication server. This information is used to troubleshoot the connection between Configuration Server and the RADIUS or LDAP server, from the Configuration Server side.

For any Configuration Server, including Configuration Server Proxy, add this section and option to the options of the `Applicat ion` object.

Example The following is an example of the `authentication` section, with the value set to the recommended maximum:

```
[authentication]
verbose=2
```

Specific log events may also 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 the server is available for processing authentication requests.

For more information about these log events, refer to *Framework 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, page 23](#)
- [Task Summary, page 24](#)
- [Deploying RADIUS Authentication, page 24](#)
- [Modifying the RADIUS Configuration Files, page 26](#)
- [Deploying RADIUS on Configuration Server Proxy, page 28](#)

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.

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.

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.

Task Summary

The following Task Summary lists the tasks required to deploy RADIUS in your configuration.

Task Summary: Deploying RADIUS External Authentication

Task	Related Procedures and Information
1. Install Configuration Server and deploy RADIUS 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. Use the procedure “Deploying RADIUS external authentication during Configuration Server installation” on page 25 .
2. Modify the RADIUS configuration files.	Modify the RADIUS configuration files <code>servers</code> and <code>radiusclient.conf</code> . Refer to “Modifying the RADIUS Configuration Files” on page 26 .
3. (optional) Install as many Configuration Servers as required, deploying RADIUS during the installation.	If you are deploying RADIUS in a geographically distributed configuration, install RADIUS on each Configuration Server Proxy using the procedure “Deploying RADIUS external authentication on Configuration Server Proxy” on page 28 .

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

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” on [page 14](#)). The `authentication` section indicates that RADIUS external authentication is to be used.

[authentication] Section

This section must be called `authentication`.

library

Default Value: No default value

Valid Values: Depends on type configuration option, as follows:

<code>gauth_radius</code>	All
<code>gauth_ldap</code>	All
<code>gauth_radius, gauth_ldap</code>	Configuration Server, Configuration Server Proxy
<code>gauth_ldap, gauth_radius</code>	Configuration Server, Configuration Server Proxy
<code>internal</code>	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,

such as LDAP, you must manually 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.

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

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

Modifying the RADIUS Configuration Files

Table 3 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	<code>gauth_radius.dll</code>	
Solaris	<code>libgauth_radius_32.so</code>	<code>libgauth_radius_64.so</code>
AIX	<code>libgauth_radius_32.so</code>	<code>libgauth_radius_64.so</code>
Red Hat Linux	<code>libgauth_radius_32.so</code>	<code>libgauth_radius_64.so</code>

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.

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 colon.

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 on Configuration Server Proxy

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 on Configuration Server Proxy

Prerequisites

- RADIUS is installed on the Master Configuration Server.
- The `servers` configuration file contains all of the servers listed in `radiusclient.conf`.

Start of procedure

1. 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 Table 3 on [page 26](#)
 - `radius.seq`
 - `radiusclient.conf`
 - `servers`
2. 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” on [page 21](#).
3. Restart Configuration Server Proxy.

End of procedure

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, page 31](#)
- [Task Summary, page 33](#)
- [Deploying LDAP, page 33](#)
- [Configuring LDAP Servers, page 36](#)
- [Deploying LDAP on Configuration Server Proxy, page 37](#)
- [Using LDAP in a Multi-Tenant Configuration, page 38](#)
- [Using LDAP Referrals, page 38](#)
- [Security Considerations, page 39](#)
- [Error Handling, page 40](#)
- [Technical Notes, page 44](#)
- [Examples, page 45](#)
- [Configuration Options, page 46](#)

Overview

Management Framework 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 has been tested to work with the following LDAP servers:

- Novell E-Directory

- IBM Tivoli Directory Server (or Blue Pages)
- Microsoft Active Directory
- Oracle LDAP Proxy/Internet Directory
- IBM Resource Access Control Facility (RACF)

Configuration Server external authentication supports multiple LDAP 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 is tried, and if it responds, it becomes the active authentication server. This process continues sequentially through the list of authentication servers.

Note: Redundant RACF servers are not supported.

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.

Starting in release 8.1, LDAP can be configured on each Configuration Server Proxy in a geographically distributed environment. Therefore, each Configuration Server Proxy can process authentication requests itself, and not pass them on to the Master Configuration Server.

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
AIX	libgauth_ldap_32.so	libgauth_ldap_64.so
Red Hat Linux	libgauth_ldap_32.so	libgauth_ldap_64.so

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

- `ldaperrors.txt`—contains default LDAP errors. For its content, see “Error Codes” on [page 40](#).
- `randgen.rnd`—used with Transport Layer Security.

Task Summary

The following Task Summary lists the tasks required to deploy LDAP in your configuration.

Task Summary: Deploying LDAP External Authentication

Task	Related Procedures and Information
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. Use the procedure “Deploying LDAP during Configuration Server installation” on page 33 .
2. (Optional) Configure additional LDAP Servers.	If you are using multiple LDAP servers, configure them on the Options tab of the Tenant object (preferred) or of the Configuration Server object. Refer to “Configuring LDAP Servers” on page 36 .
3. (optional) Install as many Configuration Servers as required, deploying LDAP during the installation.	If you are deploying LDAP in a geographically distributed configuration, install each Configuration Server Proxy using the procedure “Deploying LDAP during Configuration Server installation” on page 33 .

Deploying LDAP

Use the following procedure to deploy LDAP while you are installing Configuration Server or Configuration Server Proxy.

Procedure:

Deploying LDAP during Configuration Server installation

Purpose: To deploy LDAP while installing Configuration Server or Configuration Server Proxy.

Start of procedure

1. Begin installing Configuration Server or Configuration Server Proxy (multi-tenant or single-tenant).

2. 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.
3. Continue installing Configuration Server or Configuration Server Proxy, as appropriate.
4. On the Configuration Server External Authentication page, select Lightweight Directory Access Protocol (LDAP).
5. 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 enter additional LDAP servers on the Options tab of the Configuration Server or Configuration Server Application object.

Note: 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.

6. Finish installing Configuration Server or Configuration Server Proxy.

End of procedure

Configuration Server Options

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” on [page 14](#)), 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` (see [page 49](#)), you must set the `app-user` and `password` options (see [page 51](#)) 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.

Warnings! 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:
 - The passwords are encrypted.
 - The `confserv` section of the `confserv.conf` file contains the option `encryption=true`.

If either of these conditions are omitted, Configuration Server may import the legacy passwords incorrectly.

- 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. If you don't do this, Configuration Server will index the servers in the order in which they are read.
-

Configuring LDAP Servers

Configuration Server supports up to ten LDAP authorization modules, or servers.

Note: 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 on the `Options` tab of the Configuration Server object.

Note: 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” on [page 37](#).

On the `Options` tab, 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.

A section for a single server has a format like this:

```
[gauth_ldap] or [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, in a section are listed in [Table 5](#), and described in detail starting on [page 46](#).

Table 5: LDAP Server Parameters

Parameter	Definition of value
ldap-url	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

Table 5: LDAP Server Parameters (Continued)

Parameter	Definition of value
idle-timeout	Time interval that the connection to the LDAP server will be kept open if there are no more requests
retry-attempts	Number of authorization retries that will be generated by Configuration Server if the LDAP server does not respond
retry-interval	Time that Configuration Server waits for an authorization reply from the LDAP server.
connect-timeout	Initial timeout after which Configuration Server deems the specified LDAP server is not available.

When you are finished configuring all LDAP servers, the `Options` tab 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.

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 procedure “Deploying LDAP during Configuration Server installation” on [page 33](#).

Using LDAP in a Multi-Tenant Configuration

Note: 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 Tenant object's Annex. 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 Tenant's Annex, 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 “Configuring LDAP Servers” on [page 36](#).

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.

Note: 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 (see [page 54](#)) 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` (see [page 54](#)) and `retry-attempts` (see [page 53](#)) to the LDAP server to which it originally sent the request.

Security Considerations

Warning! When using LDAP servers in a secure environment, all LDAP servers must use SSL server certificates issued by the same certificate authority or subordinate authorities of the same public root authority. Configuration Server must be provisioned (using the `cacert-path` option [[page 51](#)]) with a certificate of authority (or chain of certificates) that can validate all server SSL certificates.

If mutual authentication is required on connections to LDAP servers, Configuration Server must be provisioned (using the `cert-path` and `key-path` [[page 52](#)] options) with the same local certificate that is accepted by all LDAP servers.

Genesys does not support specifying different client certificates (and/or certificate authority certificates), for different connections.

In addition, 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 34](#).
- 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 External ID field of User 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 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 specified for this connection. 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 on [page 43](#) 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.

To correct this error, log on to your GUI application with a valid non-empty password.



Figure 2: Error Message—Blank Password

Invalid Credentials

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

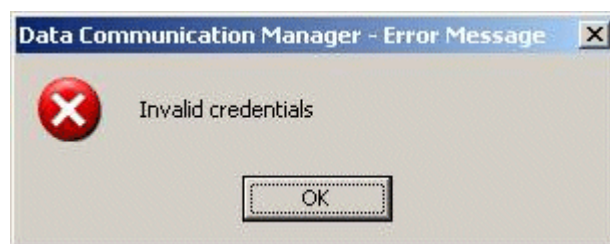


Figure 3: Error Message—Incorrect Password

To correct this error, log on to your GUI application with a valid non-empty password.

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.



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

Your LDAP server may not allow an anonymous BIND operation. Instead, configure a dedicated account (called “the application account”) that will be able to BIND and perform searches for the distinguishing name of the user being authenticated as defined the search clause in the `ldap-url` option (see [page 49](#)) for this connection.

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 'ou=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???
(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

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??s
ub?(racfid=X)
connect-timeout=3
retry-interval=4
retry-attempts=5
```

where TIMLDAP is the user created to access RACF.

Configuration Options

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

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

Setting Configuration Options

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

- In the `Options` tab of the Configuration Server or Configuration Server Proxy Application object
- In a multi-tenant and distributed environment, on the `Annex` tab of a Tenant object
- In the `Annex` of individual Person objects

This will turn on external authentication for all users enabled with External IDs, or for all users if the option `enforce-external-auth` (see [page 47](#)) is set to `true`.

You can also fine-tune your LDAP configuration throughout your system by configuring some or all options in the Tenant object's `Annex`. Refer to “Using LDAP in a Multi-Tenant Configuration” on [page 38](#) for more information.

Mandatory Options

Table 6 on [page 47](#) lists the options that are mandatory for LDAP external authentication on Configuration Server and Configuration Server Proxy. Both options are set automatically during the installation of Configuration Server and Configuration Server Proxy.

Table 6: Mandatory LDAP configuration options

Section	Option	Value
<code>authentication</code>	<code>Library</code>	<code>gauth_ldap</code>
<code>gauth_ldap</code>	<code>ldap_url</code>	Valid URL of LDAP authentication module

authentication Section

This section is mandatory on the Server level to enable external authentication. It can, however, appear in other locations as mentioned in “Setting Configuration Options” on [page 47](#).

This section must be called `authentication`.

enforce-external-auth

Default Value: `false`

Valid Values: `true`, `false`

Changes Take Effect: Immediately

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

If this option is set to `true` in the database, but a newly installed Configuration Server reads its configuration file and finds the option set to `false`, Configuration Server sets it to `false` in the database. This ensures that all users are authenticated internally, including those without an External ID.

This option applies only at the server level.

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

library

Default Value: No default value

Valid Values: Depends on type configuration option, as follows:

<code>gauth_ldap</code>	All
<code>gauth_radius</code>	All
<code>gauth_ldap, gauth_radius</code>	Configuration Server, Configuration Server Proxy
<code>gauth_radius, gauth_ldap</code>	Configuration Server, Configuration Server Proxy
<code>internal</code>	Tenant, Person

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

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

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

`gauth_ldap` and `gauth_ldap_n` Sections

Each of these sections contains information about one LDAP Authentication Module. If you are using RACF, or if there is only one LDAP server, the section is called `gauth_ldap`. This section is mandatory. If you are using more than one LDAP Server, you must identify one in the `gauth_ldap` section, and the rest in individual `gauth_ldap_n` sections.

Configuration Server supports up to ten LDAP authorization servers. You can have up to nine of these sections, one section for each LDAP server. The name of each section must be unique, and Genesys recommends that they be in the same order as they are indexed. Each section must be named `gauth_ldap_n`,

where *n* is a numeric index in the range of 1 to 9 for each LDAP server, as follows:

```
[gauth_ldap_n>
ldap-url= <value>
app-user= <value>
password= <value>
cacert-path= <value>
cert-path= <value>
key-path= <value>
idle-timeout=<value>
retry_attempts=<value>
retry-interval=<value>
commit-timeout=<value>
chase-referrals=<value>
```

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

An LDAP Server is defined using the following options, described in this section:

- ldap-url
- app-user
- password
- ca-cert-path
- cert-path
- key-path
- idle-timeout
- retry-attempts
- retry-interval
- connect-timeout
- chase-referrals

To define an LDAP server, set these options on the `Options` tab of the object, in the `gauth_ldap` section. If you are using multiple LDAP servers, define the options for the additional servers in the appropriate `gauth_ldap_n` section.

ldap-url

Default Value: Empty string

Valid Value: URL in RFC 2255 format, as described below.

Changes Take Effect: Immediately

This URL contains the information needed to access the LDAP server and directory from which it retrieves the user's distinguished name.

Enter the URL of one LDAP server in this field. If you are using multiple LDAP servers, define the rest of your LDAP servers (a maximum of nine) in

the `gauth_ldap_n` section in the Configuration Server or Configuration Server Proxy Application object's Options.

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

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

The following is a sample of an LDAP URL parsed into its parameters (as listed in Table 7 on [page 50](#)). Note that the URL contains no spaces and is a single expression that must be entered on a single line.

The diagram shows the LDAP URL `ldaps://fram.us.int.versacorp.com:636/ou=Engineering,o=versacorp,c=us??sub?(mail=X)` with the following annotations:

- 1**: Points to the protocol type `ldaps`.
- 2**: Points to the LDAP server host name `fram.us.int.versacorp.com`.
- 3**: Points to the LDAP server port `636`.
- 4**: Points to the Base DN `ou=Engineering,o=versacorp,c=us`.
- 5**: Points to the search scope `sub`.
- 6**: Points to the search filter `(mail=X)`.

Table 7: ldap-url parameters

Parameter	Definition of value
1 Protocol type	Required. Range: <code>ldaps</code> (SSL/TLS secure) or <code>ldap</code> (unsecure).
2 LDAP server host name	Optional. Default is the local host. Example: <code>fram.us.int.vcorp.com</code>
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: <code>ou=Engineering,o=vcorp,c=us</code>
5 Search scope	Optional. Default: <code>sub</code> . Defines the scope of the search operation (according to the RFC 2251 format). Range: <code>base</code> , <code>one</code> , <code>sub</code> .

Table 7: ldap-url parameters (Continued)

Parameter	Definition of value
6 Search filter	<p>Optional. Limits the search by searching for a match with a specified field. Default: empty string. 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)</p> <p>Note: The user's external ID is defined in the properties of the Person object, as follows:</p> <ul style="list-style-type: none"> Person object > Configuration tab > General section > External ID

For examples of LDAP URLs, see [page 45](#).

app-user

Default Value: Empty string

Valid Value: Valid path

Changes Take Effect: Immediately

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

For an example of the app-user parameter for RACF, see [page 46](#).

password

Default Value: Empty string

Valid Value: A valid password

Changes Take Effect: Immediately

Password of the application account. Required if app-user parameter is set.

cacert-path

Default Value: Empty string

Valid Value: Valid path.

Changes Take Effect: Immediately

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.

Warning! When using LDAP servers in a secure environment, all LDAP servers must use SSL server certificates issued by the same certificate authority or subordinate authorities of the same public root authority. Configuration Server must be provisioned (using the `cacert-path` option [page 51]) with a certificate of authority (or chain of certificates) that can validate all server SSL certificates.

If mutual authentication is required on connections to LDAP servers, Configuration Server must be provisioned (using the `cert-path` and `key-path` [page 52] options) with the same local certificate that is accepted by all LDAP servers.

Genesys does not support specifying different client certificates (and/or certificate authority certificates), for different connections.

cert-path

Default Value: Empty string

Valid Value: Valid path

Changes Take Effect: Immediately

Full path to the file containing a certificate 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.

Warning! When using LDAP servers in a secure environment, all LDAP servers must use SSL server certificates issued by the same certificate authority or subordinate authorities of the same public root authority. Configuration Server must be provisioned (using the `cacert-path` option [page 51]) with a certificate of authority (or chain of certificates) that can validate all server SSL certificates.

If mutual authentication is required on connections to LDAP servers, Configuration Server must be provisioned (using the `cert-path` and `key-path` [page 52] options) with the same local certificate that is accepted by all LDAP servers.

Genesys does not support specifying different client certificates (and/or certificate authority certificates), for different connections.

key-path

Default Value: Empty string

Valid Values: Valid path.

Changes Take Effect: Immediately

Full path to the file containing 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.

Warning! When using LDAP servers in a secure environment, all LDAP servers must use SSL server certificates issued by the same certificate authority or subordinate authorities of the same public root authority. Configuration Server must be provisioned (using the `cacert-path` option [\[page 51\]](#)) with a certificate of authority (or chain of certificates) that can validate all server SSL certificates.

If mutual authentication is required on connections to LDAP servers, Configuration Server must be provisioned (using the `cert-path` and `key-path` [\[page 52\]](#) options) with the same local certificate that is accepted by all LDAP servers.

Genesys does not support specifying different client certificates (and/or certificate authority certificates), for different connections.

idle-timeout

Default Value: 0

Valid Values: 0 – MAX_INTEGER

Changes Take Effect: Immediately

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

retry-attempts

Default Value: 3

Valid Values: 0 – MAX_INTEGER

Changes Take Effect: Immediately

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

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

If Configuration Server has tried all the LDAP servers without getting a response, an error is generated. See “Error Handling” on [page 40](#).

retry-interval

Default Value: 10

Valid Value: 0 – MAX_INTEGER

Changes Take Effect: Immediately

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

connect-timeout

Default Value: 10

Valid Values: 0 – to MAX_INTEGER

Changes Take Effect: Immediately

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

chase-referrals

Default Value: 0

Valid Values:

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

Changes Take Effect: At the next authentication request

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



Chapter

4

Kerberos External Authentication

This chapter describes how Configuration Server supports Kerberos external authentication for Genesys user interface applications.

This chapter contains the following sections:

- [Overview, page 55](#)
- [Configuring Kerberos, page 56](#)
- [Redundant Configuration Servers, page 62](#)
- [Configuration Options, page 62](#)

Overview

Configuration Server and Configuration Server Proxy support the use of the Kerberos authentication protocol for user authentication in Genesys user interface applications. Kerberos enables secure communication between nodes over a non-secure network, using tickets to enable the nodes to prove their identity to each other in a secure manner.

Configuration Server uses Windows Active Directory and MIT key distribution centers to implement Kerberos authentication.

Kerberos vs RADIUS/LDAP

Kerberos, RADIUS, and LDAP are all types of external authentication. However, Kerberos differs slightly from the existing external authentication protocols (RADIUS, LDAP, and others) in when the authentication is performed, as follows:

- Existing external authentication protocols operate in “in behind” mode. That is, the authentication is carried out when the interface application

sends the request to Configuration Server, which then forwards it to the authentication system.

- Kerberos operates in “in front” mode. The authentication is activated on the client side before a connection to Configuration Server is made. When the actual connection to Configuration Server is made, the interface gets an authentication ticket (a Kerberos token) that is already authenticated. This ticket is sent to Configuration Server with the login request to assert that authentication is already done.

Supported Environments

Configuration Server supports Kerberos authentication on the following platforms:

- Red Hat Enterprise Linux (RHEL) version 5 and later
- Windows 2008 and later
- Solaris version 10 and later
- AIX version 5.3 and later

The following versions of MIT Kerberos are used:

- krb5-1.11 for supported UNIX platforms
- kfw-4.0.1 for Windows

Configuring Kerberos

This section provides detailed procedures for configuring Kerberos. Sample configurations are provided in [Appendix C](#) on page 73

Procedure: Configuring Kerberos on Configuration Server or Configuration Server Proxy

Start of procedure

1. In the options of the Configuration Server or Configuration Server Proxy Application object, do the following:
 - a. (Optional) Do one of the following:
 - If the authentication section does not exist, create it and add the following option and value:
Option: library
Value: gauth_kerberos

- If the authentication section already exists, add the following to the end of the line of values for the `Library` option.

`, gauth_kerberos`

For example:

`gauth_ldap, gauth_kerberos`

- b. Create the `gauth_kerberos` section, and set the following options:
 - `SPN`
 - `realm`
 - `keytab`

Refer to the section “`gauth_kerberos` Section” on [page 63](#) for descriptions of these options.

2. Finish the configuration by completing one of the following procedures, depending on the operating system you are using:
 - Windows 32-bit—Use the procedure “” on [page 57](#).
 - Windows 64-bit—Use the procedure “” on [page 58](#).
 - RHEL—Use the procedure “” on [page 58](#).
 - Solaris 64-bit—Use the procedure “” on [page 59](#).
 - AIX 64-bit—Use the procedure “” on [page 60](#).

End of procedure

Procedure: Installing Kerberos on Configuration Server/Proxy host running Windows 32-bit

Prerequisites

- Configuration Server or Configuration Server Proxy is configured as described in the procedure “” on [page 56](#)

Start of procedure

1. Install MIT kerberos for Windows 4.0.1 32 on the host on which Configuration Server or Configuration Server Proxy is running. The executable file is available at:
<http://web.mit.edu/Kerberos/dist/kfw/4.0/kfw-4.0.1-i386.msi>
2. Make sure that the `krb5.ini` file contains correct information in the `libdefaults` and `realms` sections. This file is usually located in the Windows directory or in the Kerberos initialization directory (`C:\ProgramData\MIT\Kerberos5`), but may have been placed elsewhere. If

you cannot find it, use a file-search utility, such as Windows Search, to locate it. See “Kerberos Initialization File” on [page 61](#) for more information about this file.

End of procedure

Procedure: Installing Kerberos on Configuration Server/Proxy host running Windows 64-bit

Prerequisites

- Configuration Server or Configuration Server Proxy is configured as described in the procedure “” on [page 56](#)

Start of procedure

1. Install MIT kerberos for Windows 4.0.1 64 on the host on which Configuration Server or Configuration Server Proxy is running. The executable file is available at:
<http://web.mit.edu/Kerberos/dist/kfw/4.0/kfw-4.0.1-amd64.msi>
2. Make sure that the `krb5.ini` file contains correct information in the `libdefaults` and `realms` sections. This file is usually located in the Windows directory or in the Kerberos initialization directory (`C:\ProgramData\MIT\Kerberos5`), but may have been placed elsewhere. If you cannot find it, use a file-search utility, such as Windows Search, to locate it. See “Kerberos Initialization File” on [page 61](#) for more information about this file.

End of procedure

Procedure: Installing Kerberos on Configuration Server/Proxy host running RHEL

Prerequisites

- Configuration Server or Configuration Server Proxy is configured as described in the procedure “” on [page 56](#)

Start of procedure

1. Install MIT kerberos 5-1.11 on the host on which Configuration Server or Configuration Server Proxy is running. The executable installation file is available at:

<http://web.mit.edu/Kerberos/dist/krb5/1.11/krb5-1.11-signed.tar>

The installation process is described at:

http://web.mit.edu/Kerberos/krb5-latest/doc/build/doing_build.html

2. After executing `make install`, add the `/usr/local/lib` path to the `/etc/ld.so.conf` file.
3. Run `/sbin/ldconfig`.
4. Make sure that the `/etc/krb5.conf` file contains the correct information in the `libdefaults` and `realms` sections. This file is located in `/etc` by default, but its location can be overridden by setting the environment variable `KRB5_CONFIG`.

See “Kerberos Initialization File” on [page 61](#) for more information about this file.

End of procedure

Procedure: Installing Kerberos on Configuration Server/Proxy host running Solaris 10 64-bit

Prerequisites

- Configuration Server or Configuration Server Proxy is configured as described in the procedure “” on [page 56](#)

Start of procedure

1. Install MIT kerberos 5-1.11 on the host on which Configuration Server or Configuration Server Proxy is running. The executable installation file is available at:

<http://web.mit.edu/Kerberos/dist/krb5/1.11/krb5-1.11-signed.tar>

The installation process is described at:

http://web.mit.edu/Kerberos/krb5-latest/doc/build/doing_build.html

2. Extract the file as follows:

```
mkdir .krb5_install
cd .krb5_install
tar xvf ../krb5-1.11-signed.tar
tar xzvf krb5-1.11.tar.gz
```

3. During the installation, specify the following values for the following configuration options:


```
./configure CC='opt/SUNWspro/bin/cc' CXX='opt/SUNWspro/bin/cc'
CFLAGS='-g -v -xarch=v10' CXXFLAGS='-g -v -xarch=v10'
LDFLAGS='-xarch=v10' LIBS='-lsocket -lnsl -ldl -lresolv'
and
correspondent --prefix
```
4. After the corresponding stage, before the make stage, do the following:
 - a. Add a symbolic link, using the following command (on one line):


```
ln s <installation directory>/plugins/kdb/db2/libdb2/libdb.so
<installation directory>/lib/libdb.so
```
 - b. Patch the code at line 358:


```
<source_dir>src.lib.krb5/os/expand_path.c
```

 With:


```
-static const struct token {
+static const struct {
const char *tok;
PTYPE param;
const char *postfix;
```
5. Make sure that the `/etc/krb5.conf` file contains the correct information in the `libdefaults` and `realms` sections. This file is located in `/etc` by default, but its location can be overridden by setting the environment variable `KRB5_CONFIG`.
See “Kerberos Initialization File” on [page 61](#) for more information about this file.

End of procedure

Procedure: Installing Kerberos on Configuration Server/Proxy host running AIX 64-bit

Prerequisites

- Configuration Server or Configuration Server Proxy is configured as described in the procedure “” on [page 56](#)

Start of procedure

1. Install MIT kerberos 5-1.11 on the host on which Configuration Server or Configuration Server Proxy is running. The executable installation file is available at:
<http://web.mit.edu/Kerberos/dist/krb5/1.11/krb5-1.11-signed.tar>

The installation process is described at:

http://web.mit.edu/Kerberos/krb5-latest/doc/build/doing_build.html

2. Extract the file as follows:

```
mkdir .krb5_install
cd .krb5_install
tar xvf ../krb5-1.11-signed.tar
tar xzvf krb5-1.11.tar.gz
```

3. During the installation, specify the following values for the following configuration options, as prompted:

```
./configure CC='/usr/vacapp/bin/xlc' CXX='/usr/vacapp/bin/xlc'
CFLAGS='-g -v -q64 -qlanglvl=newexcp' CXXFLAGS='-g -v -q64
qlanglvl=newexcp' LDFLAGS='-b64 -brtl' LIBS='-ldl' AR='ar -X 32_64'
and
correspondent --prefix
```

4. After the corresponding stage, before the make stage, do the following:

- a. Add a symbolic link, using the following command (on one line):

```
ln s <installation directory>plugins/kdb/db2/libdb2/libdb.so
<installation directory>/lib/libdb.so
```

- b. Patch the code at line 358:

```
<source_dir>src/lib/krb5/os/expand_path.c
```

With:

```
-static const struct token {
+static const struct {
const char *tok;
PTYPE param;
const char *postfix;
```

5. Make sure that the /etc/krb5.conf file contains the correct information in the libdefaults and realms sections. This file is located in /etc by default, but its location can be overridden by setting the environment variable KRB5_CONFIG.

See “Kerberos Initialization File” on [page 61](#) for more information about this file.

End of procedure

Kerberos Initialization File

When Kerberos is installed on the host of the Configuration Server or Configuration Server Proxy, it creates an initialization file that contains information about the realms used by Kerberos. This file has different names depending on the platform on which Kerberos is installed, but contains two sections, as follows:

- **libdefaults**—This section is required by Kerberos, and must contain the name of the realm used for authentication.

- **realms**—This section must contain subsections keyed by Kerberos realm names. Each subsection describes realm-specific information, especially the kdc key with the key distribution center host.

The following is a sample of a Kerberos initialization file:

```
[libdefaults]
default_realm = ROOTDOMAIN.CONTOSO.COM

[realms]
  KRBTEST.GENESYSLAB.COM = {
    kdc = rh5qa64-1.genesyslab.com
    admin_server = rh5qa64-1.genesyslab.com
  }
  ROOTDOMAIN.CONTOSO.COM = {
    kdc = 135.225.51.144
    admin_server = 135.225.51.144
  }
```

For more information, see

<http://web.mit.edu/Kerberos/krb5-1.5/krb5-1.5/doc/krb5-admin/krb5.conf.html>

Redundant Configuration Servers

When primary and backup Configuration Servers are running on separate hosts, they can both use the same principal name (SPN). Each Configuration Server must be configured to use Kerberos, as described in this section; otherwise, no special configuration is required.

If the two servers are running on the same host and using the same principal name (SPN), the server applications must run under different system user accounts. That is, they must use a different user name in the Windows Services property—the **Log in as** field on the **Log on** tab.

Configuration Options

This section describes the configuration options used to configure Kerberos on Configuration Server and Configuration Server Proxy.

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

Setting Configuration Options

Unless otherwise specified, set Kerberos configuration options at the following location:

- In the `Options` tab of the Configuration Server or Configuration Server Proxy Application object

This will turn on Kerberos external authentication for all users.

Mandatory Options

All options in this section are mandatory. They must be set before using Kerberos.

authentication Section

This section is mandatory on the server level to enable external authentication. This section must be called `authentication`.

library

Default Value: No default value

Valid Values: Depends on type configuration option, as follows:

<code>gauth_kerberos</code>	All
<code>gauth_ldap</code>	All
<code>gauth_radius</code>	All
<code>gauth_ldap, gauth_radius</code>	Configuration Server, Configuration Server Proxy
<code>gauth_radius, gauth_ldap</code>	Configuration Server, Configuration Server Proxy
<code>internal</code>	Tenant, Person

Changes Take Effect: Upon restart of Configuration Server or Configuration Server Proxy

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

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

gauth_kerberos Section

This section is mandatory, and contains information about the Kerberos installation on this Configuration Server or Configuration Server Proxy.

This section must be called `gauth_kerberos`.

A Kerberos installation is defined using the following options, described in this section:

- SPN
- realm
- keytab

Set these options on the `Options` tab of the Configuration Server or Configuration Server Proxy Application object, in the `gauth_kerberos` section.

Note: These options must be set before using Kerberos.

SPN

Default Value: Empty string

Valid Value: Any valid name

Changes Take Effect: Immediately

The Service Principal Name, in the format `service/hostname`, the same as that used by a client in the `service` parameter. This name must be registered with the key distribution center to which this configuration is pointing (as defined by the platform-specific configuration).

realm

Default Value: Empty string

Valid Value: Any valid name

Changes Take Effect: Immediately

The name of the Kerberos infrastructure, as known by the MIT client library and/or the key distribution server being used. The value must be specified in all upper-case letters in the form of a domain address (`ENTITY.SUBDOMAIN.ROOTDOMAIN`).

keytab

Default Value: Empty string

Valid Value: Any valid name

Changes Take Effect: Immediately

The name of the keytab file that is generated by the key distribution center and propagated to the host on which this Configuration Server or Configuration Server Proxy is running. This file must exist in the installation directory of this Configuration Server (primary or backup) or Configuration Server Proxy.



Appendix

A

Importing User Data from External Sources

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

This appendix contains the following sections:

- [“Introduction” on page 65](#)
- [“Creating a User Record in the Genesys Configuration” on page 66](#)

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 8](#) describes these properties.

Table 8: 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 8: 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 “ldap-url” on page 49 . Therefore, if the filter in the LDAP URL is (ma i l=X), then the External User ID property in Genesys configuration represents the ma i l 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

Use Genesys Administrator 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.

B

Sample Certificate Authority Certificates File

This appendix contains an example of a Certificate Authority (CA) certificates file that can be used to validate the LDAP server authentication without mutual authentication, and the output produced by running the `openssl.exe` utility.

This appendix contains the following sections:

- [CA Certificates File, page 69](#)
- [Output Using OpenSSL Utility, page 70](#)
- [Configuring Server Authentication, page 72](#)

CA Certificates File

The following sample CA certificates file is a concatenation of several CAs. The CA to validate the remote LDAP server certificate is selected automatically by Configuration Server. The first example is valid for the target host; the second is not.

```
-----BEGIN CERTIFICATE-----
MIIErTCCA5WgAwIBAgIJA0GkFzNTb8K0MA0GCSqGSIb3DQEBBQUAMIGVMQswCQYD
VQGGewJSVTEVMBMGA1UECBMU3QuUGV0ZXJidXJnMRUwEwYDVQQHEwxd5QZXRl
cmJ1cmcxEDA0BgNVBAoTB0dlbmVzeXMxCzAJBgNVBAsTAlFBMRYYFAYDVQQDEw0x
OTIuMTY4Ljg1LjgyMSEwHwYJKoZIhvcNAQkBFhJyb290QDE5Mi4xNjguODUuMjIw
HhcNMTIwMTI3MTMyODM4WcNMTI1MTMyODM4WjCBTELMAKGA1UEBhMCULX
FTATBgNVBAgTDFN0LlBlldGVyYnVyZzEVMBMGA1UEBxMMU3QuUGV0ZXJidXJnMRAw
DgYDVQQKEwdHZW5lc3LzMQswCQYDVQQLEwJRQTEWMBQGA1UEAxMNMTkyLjE2OC44
NS44MjEhMB8GCSqGSIb3DQEJARYScm9vdEAXOTIuMTY4Ljg1LjIyMIIBIjANBgkq
hkIG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAskJTR7g4+XJOHVuWRbt4az0TdI/WN5u
EuSQSotxzGLqCmQQws77xM1/Xyy5W5ik7tJnbToZzYjVVkamucmWMu9bQkr6726Q
S4ZHTLjFqAQ1L/E2vaHcTktmdx0EDXfH4uv9ghv7J88/m5ptqorM0T2uZwasj0LI
w9ehpt5UICirx0/LD8LvsP0Sc5odhDQCVf/VCa0aY8PY+0mT2eSPh/tRly0DfvMp
```

```
jN4Xa6wL2qWWZoDzTk6g5WUXERPgkPyj6gKv0rUyKzMTRITb+5Ky82qoGRTL2aUC
6nLVJYc1ZLCY9rU9d0LDft5mdX5P+AQq+p0UARRDELtP/AMyo96qSwIDAQABo4H9
MIH6MB0GA1UdDgQWBBo7rdRmh9S/9AQKI+0HWVCvbo/UjCBYgYDVR0jBIHCMIG/
gBTo7rdRmh9S/9AQKI+0HWVCvbo/UqGBm6SBmDCB1TELMAKGA1UEBhMCULUxFTAT
BgNVBAgTDFN0LlBldGVyYnVyZzEVMBMGA1UEBxMMU3QuUGV0ZXJidXJnMRAwDgYD
VQQKEwdHZW5lc3ZlMQswCQYDVQQLZWJlRQTEWMBQGA1UEAxMNMTkyLjE2OC44NS44
MjEhMB8GCSqGSIb3DQEJARYScm9vdEAXOTIuMTY4Ljg1LjIyggKA4aQXM1Nvwo4w
DAYDVR0TBAAUwAwEB/zANBgkqhkiG9w0BAQUFAA0CAQEAGKdPXqZ9j13Ekz3G42vU
CIvvEonhUSF0/nGV8pEJivHZ00+oYXndRCeiORKF/6nzab17b+w15fbU0uEJyR+D
S3IkVKEukBxguLeu93kQ5Ds4vuj0JqcvZ9aM1cVWwXDJ0jH9tWK++17QU0D8Cj0Q
T+kBWqhYgYwqZE7rcKapzQtKo0ZR6APgY4B8fUkb0qHbRJGELxLNsXB19VGcYQh
+LN1ZqdRPic8qqYuBt+7y4e9VBVseoSNnIcPmaTkAS0obvJx6qQhBu8NSIU5pIR
RP93LtSqUm+Vj7n8kAMPVje60MKNSNLC56mH4/TY47wMJ6JHh9q0jB4jbybDTu4
5A==
```

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

```
MIIE2TCCA8GgAwIBAgIJAJ59ncLvV1gRMA0GCSqGSIb3DQEBBQUAMIGjMQswCQYD
VQQGEWJydTETMBEGA1UECBMKc29tZS1zdGF0ZTEZMBcGA1UEBxMMU2FpbnQtUGV0
ZXJzYnVyZzETMBEGA1UEChMKZ2VuZXN5c2xhYjELMAKGA1UECXMUUEXfjAUBGNV
BAMTDTE5Mi4xNjguNzMuMjIxKjAoBgkqhkiG9w0BCQEWG3JvbWFuLn1lc2hpbkBn
ZW5lc3ZlbGF1LmNvbTAeFw0wOTA0MDkwnjA1NDZaFw0xNDA0MDgwnjA1NDZaMIGj
MQswCQYDVQQGEWJydTETMBEGA1UECBMKc29tZS1zdGF0ZTEZMBcGA1UEBxMMU2Fp
bnQtUGV0ZXJzYnVyZzETMBEGA1UEChMKZ2VuZXN5c2xhYjELMAKGA1UECXMUUEXfj
AUBGNVBAMTDTE5Mi4xNjguNzMuMjIxKjAoBgkqhkiG9w0BCQEWG3JvbWFuLn1lc2h
pbkBnZW5lc3ZlbGF1LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggE
BA0ZGBia4Dw878dtr17CuV0+r3hYD/voMB0brsPAhHMA64P0FTtVPExt8E7p5
5ysd0VLjf7593wHzcAYSfD5j3NTr07Nui80toB77U/urTxMu1jq9o3LfrqN6rgg0
p0fbkuv1S7vmCiidS1G00bIob6GAav3swC38t8Rzv50NCMpiITxKS3Gww1edVfij
dlfG7ookxe2wJALGp8HYygoQKqN2h5C+QUhvg4T/NNv3up+LI/1T4U269EK3NaEL
Chf26q380H0BG/rYcX1iZJdPx1Z1L4BsspMfhgK3Zff3WJWVjEon5xG/Igbl82vo
NK73WCotSWIa22cxsPK/BvP7jUCAwEAAa0CAQwwggEIMB0GA1UdDgQWBRLdA7o
98BjAragLk0L5rj89HsveDCB2AYDVR0jBIHQMIHNgBRLdA7o98BjAragLk0L5rj8
9HsveKGBqasBpjCBozELMAKGA1UEBhMCnUxEzARBGNVBAGTCnNvbWUtc3RhdGUx
GTAXBGNVBACTEFNhW50LVBldGVyc2J1cmcxZzARBGNVBAoTCmdlbmVzeXNsYWIx
CzAJBgNVBAsTA1FBMRyWfAYDVQQDEw0xOTIuMTY4Ljg1LjIyMSowKAYJKoZIhvcNAQ
AQkBFhtyb21hb155dXNoaW5AZ2VuZXN5c2xhYj5jb22CCQCEfZ3Jb1dYETAMBGNV
HRMEBTADAQH/MA0GCSqGSIb3DQEBBQUAA4IBAQBZLUuooFJB4UFxlmrnVvyw0atr
sN7dCiEr418uK4VgCndRw+lga1PcMGe0IVRI0/uJuAKC+GJXPL5wheTT+NIhGW5B
NpLam4PPikb3mo8GwdDldqXbbsVUmpI/9hL9eGNAh/IJ1CJD6Jkp7IKmiU6yTzv5
qqw84EkXDDfvmhFvnYU6SG1zouxg2W8H20bWuFGIX9W4wNMmpdH+SaLWRnrVGX7
ABv+AGNkhqCe8qmgw5PkiO/HbPd77jqgrSUMYtnWB6cEXhzqkV3T0kb9sFKN9APY
x/L7AeSD0+Ldc1IL3yBjsy9KUicroeBF7J1HGqLFnw0v+SY40I+7m6QXiMMk
```

Output Using OpenSSL Utility

`openssl.exe` is the main utility in the OpenSSL toolkit. When it is run against the CA certificates file in the previous section, the following output is produced:

```

depth=1 /C=RU/ST=St.Peterburg/L=St.Peterburg/O=Genesys/OU=QA/CN=123.456.78.90/emailAddress=root@123.456.78.09
verify return:1
depth=0 /C=RU/ST=St.Peterburg/L=St.Peterburg/O=Genesys/OU=QA/CN=123.456.78.90/emailAddress=johndoe@abcd.com
verify return:1
---
Certificate chain
0 s:/C=RU/ST=St.Peterburg/L=St.Peterburg/O=Genesys/OU=QA/CN=123.456.78.90/emailAddress=johndoe@abcd.com
  i:/C=RU/ST=St.Peterburg/L=St.Peterburg/O=Genesys/OU=QA/CN=123.456.78.90/emailAddress=root@123.456.78.09
1 s:/C=RU/ST=St.Peterburg/L=St.Peterburg/O=Genesys/OU=QA/CN=123.456.78.90/emailAddress=root@123.456.78.09
  i:/C=RU/ST=St.Peterburg/L=St.Peterburg/O=Genesys/OU=QA/CN=123.456.78.90/emailAddress=root@123.456.78.09
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIDKTCaHECCQCHnoaG7KJ6jANBgkqhkiG9w0BAQUFADCBITELMAKGA1UEBhMC
ULUxFTATBgNVBAgTDFN0LBldGVyYnVyZzEVMBMGA1UEBxMMU3QuUGV0ZXJidXJn
MRAwDgYDVQQKEWdHZW5lc3lzMQswCQYDVQQLZWJQTEwJRQTEWMBQGA1UEAxMNMTkyLjE2
OC44NS44MjEhMB8GCSqGSIb3DQEJARYScm9vdEAXOTIuMTY4Ljg1LjIyMB4XDTEy
MDEzMDEwNDExNVowDTE1MDEyOTIuMTY4Ljg1LjIyMDEyOTIuMTY4Ljg1LjIyMDEyOTIu
MTY4Ljg1LjIyMDEyOTIuMTY4Ljg1LjIyMDEyOTIuMTY4Ljg1LjIyMDEyOTIuMTY4Ljg1LjIy
VQIQIEwTdC5QZXRlcjJlcmxFTATBgNVBAcTDFN0LBldGVyYnVyZzEVMDEyOTIuMTY4Ljg1LjIy
ChMHR2VuZXRlcjE1UECjE1UECjE1UECjE1UECjE1UECjE1UECjE1UECjE1UECjE1UECjE1UE
JjAKBgkqhkiG9w0BCQEF3Z2b2xvZGluQ6dldmVzeXNsYWluY29tMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCrLZ+/59mVFg3sTGZrnQf0Ln5VdypLz55HoHlq
Ffx0nax70BLGgZqhvioUL7vwmwmhzUXqcpeJxBLAGKGYzHh6SPkBHinaQLfdKG5o
9108Iu+S9RtdTBMGc8hQH1zuQQl araSLvKS5TPTvkyd+mHMLKvDCGAg0cL/q585V
+ir3pwIDAQABMA0GCSqGSIb3DQEBBQUAA4IBAQBmR82yIr/j0iYu9I1+sprv+gMV
9XTHSpqBK67Xuw+X4G3tGI+uS05gdHHZGz5or76nMIUUSYCsDC86aAapXDyGfxf
LLbY/NoQdn1FPrJQpeRFRk1o4i7zFR2+LyYZfNr3JDbhLGspe6NOHkzNBFghxWpG
ysJIXLTLBvdKcM5Tj/PGSMQTS CFWai0brm9P5L6yxx+uFdF+oLYa/hE0V99d0fYI
sYYocjKrYmNNGpKK2kPWuu8F1uG01MhLAskihjYD2LT3MkPoSowphtMkDw6Gnxz5
Z4YB2JJW2r//IEIhNvT/qhV+A0Tv0EYL6Lo4BAHleTMwvhRWltDAK73LooDB
-----END CERTIFICATE-----
subject=/C=RU/ST=St.Peterburg/L=St.Peterburg/O=Genesys/OU=QA/CN=123.456.78.90/emailAddress=johndoe@abcd.com
issuer=/C=RU/ST=St.Peterburg/L=St.Peterburg/O=Genesys/OU=QA/CN=123.456.78.90/emailAddress=root@123.456.78.09
---
No client certificate CA names sent
---
SSL handshake has read 2179 bytes and written 340 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 1024 bit
Compression: NONE
Expansion: NONE
SSL-Session:

```

```
Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: 7D705B895D61F2A200108095528864BB8C74EDE80168B69FA96AF3AD5FE0F4F8
Session-ID-ctx:
Master-Key: F1446F0B8F8B6E605AD923B0B24A08BADD91B82ABA24C13FCEB59D3B939822779A331F
583C66EC91187740F49F2F572C
Key-Arg : None
Krb5 Principal: None
Start Time: 1351273962
Timeout : 300 (sec)
Verify return code: 0 (ok)
---
```

Configuring Server Authentication

To configure LDAP server authentication, you must configure the `cacert-path` configuration option (see [page 51](#)) in the `gauth_ldap` section of the options of Configuration Server. Set this option to the path of the file that contains the CA certificate definition. This option is required whether the LDAP server requires mutual authentication or not.

If your LDAP server requires mutual authentication, you must also set the `cert-path` (see [page 52](#)) and `key-path` (see [page 52](#)) options.



Appendix

C

Sample Kerberos Configuration

This appendix contains examples of how to configure Kerberos for integration with an MIT Key Distribution Center implementation, and for a Microsoft Active Directory implementation.

This appendix contains the following sections:

- [MIT Key Distribution Center, page 73](#)
- [Microsoft Active Directory, page 74](#)

MIT Key Distribution Center

This section contains a sample configuration to integrate with an MIT Key Distribution Center (KDC) implementation.

Basic Information

KDC installed at: `rh5qa64-1.genesyslab.com`

Realm: `KRBTEST.GENESYSLAB.COM`

Sample service name: `genesys_sample`

Username (known by KDC): `testclient` with password `123456`

On cfglib Client Machine, MIT Client Configuration

File `C:\WINDOWS\krb5.ini`, section `[realms]`:

```
KRBTEST.GENESYSLAB.COM = {  
    kdc = rh5qa64-1.genesyslab.com:88  
    admin_server = rh5qa64-1.genesyslab.com:749  
}
```

On Configuration Server (Server Level):

```
[authentication]
Library=gauth_ldap
...
[gauth_kerberos]
SPN=genesys_sample/rh5qa64-1
realm=KRBTEST.GENESYSLAB.COM
kdc_host=rh5qa64-1.genesyslab.com
...
```

Person object with username and external ID testclient under the Environment tenant.

Microsoft Active Directory

This section contains a sample configuration to integrate with a Microsoft Active Directory implementation.

Basic Information

Windows domain controller is being used as KDC:

- Domain rootDomain.contoso.com
- Controller machine: W2k8r-ay-root.rootDomain.contoso.com (135.225.51.14)

Realm: ROOTDOMAIN.CONTOSO.COM

Sample Service name: confserver/somehost; there is a mapping made from this service name to the windows domain account rootUser2 with password genesys to produce a keytab file with a secret password that can be used on the Configuration Server side.

User name (known by KDC): rootUser1 with password genesys

On cfglib Client Machine, MIT Client Configuration:

File C:\WINDOWS\ krb5.ini, section [realms]:

```
ROOTDOMAIN.CONTOSO.COM = {
    kdc = 135.225.51.144
    admin_server = 135.225.51.144
}
```

On Configuration Server (Server Level):

```
[authentication]
Library=gauth_ldap
...
```

```
[gauth_kerberos]
SPN=confserver/somehost
realm=ROOTDOMAIN.CONTOSO.COM
kdc_host=135.225.51.144
```

...

Person object with username and external ID rootUser1 under Environment tenant.

Related Documentation Resources

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

Genesys Framework

- *Framework 8.5 Deployment Guide*, which helps you understand the Genesys Framework architecture, and install and configure the Genesys Framework components.
- [*Framework 8.1 Genesys Administrator Help*](#), which helps you configure and create any necessary configuration objects in Genesys Administrator.
- *Framework 8.5 Configuration Options Reference Manual*, which provides you with the configuration option descriptions for Configuration Server and other Framework components.
- [*Genesys 8.1 Security Deployment Guide*](#), which helps you understand Genesys security and permissions schema.
- Release Notes and Product Advisories for this product, available on the [Genesys Documentation](#) website.

Genesys

- [*Genesys Technical Publications Glossary*](#), which provides a comprehensive list of the Genesys and computer-telephony integration (CTI) terminology and acronyms used in this document.
- [*Genesys Migration Guide*](#), which provides documented migration strategies for Genesys product releases. Contact Genesys Customer Care for more information.
- [*Genesys Licensing Guide*](#), which introduces you to the concepts, terminology, and procedures that are relevant to the Genesys licensing system.

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

- [*Genesys Supported Operating Environment Reference Guide*](#)
- [*Genesys Supported Media Interfaces Reference Guide*](#)

For additional system-wide planning tools and information, see the release-specific listings of System Level Documents on the Genesys Documentation website.

Genesys product documentation is available on the:

- Genesys Customer Care website at <http://genesys.com/customer-care>.
- Genesys Documentation website at <http://docs.genesys.com/>.
- Genesys Documentation Library DVD, which you can order by e-mail from Genesys Order Management at orderman@genesys.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:

85fr_ref-exta_04-2014_v8.5.001.00

You will need this number when you are talking with Genesys Customer Care 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 9 on [page 80](#) describes and illustrates the type conventions that are used in this document.

Table 9: Type Styles

Type Style	Used For	Examples
Italic	<ul style="list-style-type: none"> Document titles Emphasis Definitions of (or first references to) unfamiliar terms Mathematical variables <p>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 80).</p>	<p>Please consult the <i>Genesys 8 Migration Guide</i> for more information.</p> <p>Do <i>not</i> use this value for this option.</p> <p>A <i>customary and usual</i> practice is one that is widely accepted and used within a particular industry or profession.</p> <p>The formula, $x + 1 = 7$ where x stands for...</p>
Monospace font (Looks like teletype or typewriter text)	<p>All programming identifiers and GUI elements. This convention includes:</p> <ul style="list-style-type: none"> The <i>names</i> 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. <p>Also used for any text that users must manually enter during a configuration or installation procedure, or on a command line.</p>	<p>Select the Show variables on screen check box.</p> <p>In the Operand text box, enter your formula.</p> <p>Click OK to exit the Properties dialog box.</p> <p>T-Server distributes the error messages in EventError events.</p> <p>If you select true for the inbound-bsns-calls option, all established inbound calls on a local agent are considered business calls.</p> <p>Enter exit on the command line.</p>
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.	<code>smcp_server -host [/flags]</code>
Angle brackets (< >)	<p>A placeholder for a value that the user must specify. This might be a DN or a port number specific to your enterprise.</p> <p>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.</p>	<code>smcp_server -host <confighost></code>



Index

A

- allow-empty-password
(configuration option) 34
- app-user (LDAP server parameter) 36, 51
- architecture
 - external authentication 12
- authentication (configuration section) 21
 - Kerberos 63
 - LDAP 47
 - RADIUS 25
- authserver (RADIUS parameter) 27

B

- base DN (ldap-url parameter) 50

C

- cacert-path (LDAP server parameter) . . . 36, 51
- Can't contact LDAP server
(error message) 43
- cert-path (LDAP server parameter) 36, 52
- chase-referrals
(LDAP configuration option) 38, 54
- configuration files
 - LDAP
 - ldapclient.sample.conf 32
 - RADIUS
 - dictionary 26
 - radiusclient.conf 26, 27
 - servers 26
- configuration options
 - authentication section 25, 29, 47
 - chase-referrals (LDAP) 38, 54
 - connect-timeout (LDAP) 54
 - gauth_radius section 21
 - idle-timeout (LDAP) 53
 - library (RADIUS) 25, 29
 - retry-attempts (LDAP) 40, 53

- retry-interval (LDAP) 40, 54
- setting 47, 63
- verbose (RADIUS) 21, 29
- Configuration Server options
 - setting 47, 63
- connect-timeout
(LDAP configuration option) 54
- connect-timeout (LDAP server parameter) . . 37
- customizing external authentication 15
 - establishing defaults 15
 - overriding defaults by Person objects . . . 19
 - overriding defaults by Tenant 16

D

- default_realm (RADIUS parameter) 28
- dictionary (RADIUS file) 26
- displaying messages
 - LDAP 32
 - RADIUS 24
- document
 - audience 10
 - commenting on 10
 - conventions 79
 - typographical styles 79
 - version number 79

E

- enforce-external-auth
(LDAP configuration option) 47
- error code (LDAP property) 40
- error description string (LDAP property) . . 40
- error handling in LDAP 40
 - default error codes 41
 - error code (property) 40
 - error description string (property) 40
 - error messages 42, 43
- error messages 42
 - Can't contact LDAP server 43

Inappropriate authentication	42
Invalid credentials	43
external authentication	11
architecture	12
customizing	15
enabling	14
external authentication files	
for LDAP	32

G

gauth_kerberos (configuration section)	63
gauth_ldap (configuration section)	36, 48
gauth_ldap_n (configuration section)	36, 48
geographically distributed systems	
deploying LDAP	37
deploying RADIUS	28

I

IBM Resource Access Control Facility	
Server (RACF)	32
IBM Tivoli Directory Server	32
idle-timeout	
(LDAP configuration option)	53
idle-timeout (LDAP server parameter)	37
Inappropriate authentication	
(error message)	42
Invalid credentials (error message)	43

K

Kerberos configuration options	
authentication section	63
gauth_kerberos section	63
keytab	64
library	63
realm	64
setting	63
SPN	64
key-path (LDAP server parameter)	36, 52
keytab (configuration option)	
Kerberos	64

L

LDAP	
application account	44
external authentication files	32
in geographically distributed systems	37
on Configuration Server Proxy	37
referrals	38
security considerations	39
SSL parameters	44

supported LDAP servers	31
supported versions	31
LDAP Authentication Module	31
LDAP configuration files	
ldapclient.sample.conf	32
LDAP configuration options	35, 36, 49
app-user	36, 51
cacert-path	36, 51
chase-referrals	38, 54
connect-timeout	37, 54
enforce-external-auth	47
idle-timeout	37, 53
key-path	36, 52
ldap-url	49
library	35, 48
password	36, 51
retry-attempts	37, 40, 53
retry-interval	37, 40, 54
LDAP default errors file	41
LDAP error messages	42
Can't contact LDAP server	43
Inappropriate authentication	42
Invalid credentials	43
LDAP pluggable modules	32
LDAP radio button	34
LDAP referrals	38
chase-referrals option	38
LDAP server host name	
(ldap-url parameter)	50
LDAP server parameters	
app-user	36, 51
cacert-path	36, 51
cert-path	36, 52
connect-timeout	37
idle-timeout	37
key-path	36, 52
ldap-url	35, 36, 49
password	36, 51
retry-attempts	37
retry-interval	37
ldapclient.sample.conf (LDAP file)	32
ldapperrors.txt (LDAP file)	32
ldap-url (LDAP server parameter)	35, 36, 49
ldap-url parameters	
base DN	50
LDAP server host name	50
LDAP server port	50
protocol type	50
search filter	51
search scope	50
library (configuration option)	
Kerberos	63
LDAP	35, 48
RADIUS	25, 29
Lightweight Directory Access Protocol	31

M

Microsoft Active Directory 32
 multiple servers
 LDAP 32
 RADIUS 23

N

Novell E-Directory 31

O

Oracle LDAP Proxy/Internet Directory 32
 overriding defaults by Person objects 19
 establishing defaults. 15
 overriding defaults by Tenant. 16
 establishing defaults. 15

P

password (LDAP server parameter) 36, 51
 PEM (Base64) format role in LDAP 44
 pluggable module 12
 LDAP 32
 RADIUS 26
 protocol type (ldap-url parameter) 50

R

RACF. 32
 RADIUS
 disable. 21
 in geographically distributed systems 28
 on Configuration Server Proxy 28
 supported versions 23
 RADIUS configuration files
 dictionary 26
 radiusclient.conf 26, 27
 servers. 26
 RADIUS configuration options
 library 25, 29
 verbose 21, 29
 RADIUS parameters
 authserver 27
 default_realm 28
 radius_retries 27, 28
 radius_timeout. 27
 RADIUS pluggable modules 26
 RADIUS radio button. 25
 radius_retries (RADIUS parameter) 27, 28
 radius_timeout (RADIUS parameter). 27
 radiusclient.conf (RADIUS file). 26, 27
 configuring. 27

randgen.rnd (LDAP file) 32
 realm (configuration option)
 Kerberos 64
 retry-attempts
 (LDAP configuration option) 40, 53
 retry-attempts (LDAP server parameter). 37
 retry-interval
 (LDAP configuration option) 40, 54
 retry-interval (LDAP server parameter) 37

S

search filter (ldap-url parameter). 51
 search scope (ldap-url parameter). 50
 server port (ldap-url parameter) 50
 servers (RADIUS file) 26
 configuring 26
 setting configuration options. 47, 63
 SPN (configuration option)
 Kerberos 64

T

Tivoli Directory Server, IBM 32

V

verbose (configuration option). 21, 29

