Framework External Authentication Reference Manual

LDAP External Authentication

4/4/2026

LDAP External Authentication

Contents

Management Framework supports external authentication using Lightweight Directory Access Protocol (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 section provides an overview of LDAP. For detailed instructions about deploying and using LDAP, refer to the following sections:

- Deploying LDAP
- LDAP Configuration Options
- Error Handling in LDAP
- Security Considerations

Overview

The Genesys 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.

> **Important**
> Redundant RACF servers are not supported.

Starting in release 8.0, LDAP messages concerning the failure (see Error Codes) 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

The following lists the pluggable modules that Genesys provides for LDAP.

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.
- **randgen.rnd**—used with Transport Layer Security.

LDAP Technical Notes

SSL Parameters

Genesys LDAP Authentication supports TLSv11 and TLSv12. 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+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**, where the client's private key is stored.

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 by the search clause in the **ldap-url** option for this connection.

Attributes for LDAP Entries

Configuration Server requests the LDAP Server to return only the DN (Distinguished Name) attribute for each entry it searches in LDAP. The list of attributes provided in the **ldap-url** option is ignored by Configuration Server.