This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Framework External Authentication Reference Manual

External Authentication

5/1/2025

External Authentication

Contents

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.

Supported Types of External Authentication

Genesys supports the following types of external authentication:

- RADIUS external authentication
- LDAP external authentication
- Kerberos external authentication

User Verification

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

1. Check the user's permission in the Configuration Database.
2. Pass the user's login information to a third-party server. If the external system returns positive authentication results, then perform the permission verification in the Configuration Database.

> ### 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.

Starting in release 8.1, only users with a valid **External ID** are 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.