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.

Genesys Security Deployment Guide

User Authentication and User Authorization

4/13/2025

User Authentication and User Authorization

Contents

Secure access to the resources of an interaction-management system plays an important role in ensuring trouble-free operation of all system parts and functions. Changes made by unqualified users can adversely affect system availability and the quality of service.

Secure access to a system requires that each user pass the following tests:

- User authentication—This test checks to see that the user is actually who he or she claims to be, and is usually carried out using a system of passwords or other unique and confidential (or unalterable) identifiers.
- User authorization—After the user is authenticated, this test determines that the user is entitled to access the system, either all or parts thereof, and defines what the user can do to or with the data that they can access. This is usually carried out using a system of permissions or similar access rules.

The data a Genesys solution requires for operating in a particular environment, as well as the applications and the solutions, are described in the form of Configuration Database objects. To be authenticated, any person who needs access to this data or these applications must have an account in this database.

User authorization is provided by the security mechanism implemented in Configuration Server, which allows the system administrator to define separately a level of access for any account with respect to any object.

> **Important**
>
> In the context of user authentication and authorization as described in this Guide, the term *object* refers to an instance of an object type, not the object type itself.

User Authentication

User authentication determines that a user is actually who he or she claims to be. In a physical environment, this is often implemented by photo identification cards. In a computer system, this is often accomplished by a password system—the user must enter the correct username and password combination before being authenticated.

Genesys software uses a password system. Each user is assigned a unique username and a confidential password. When logging in to any Genesys interface, the user must enter both of these identifiers before they can be authenticated. User authentication is carried out by one of the following:

- Configuration Server, as described in User Passwords.
- An external authentication module, to which Configuration Server sends the login credentials. The external authentication module performs the actual authentication. For more information about external authentication, refer to the *Framework External Authentication Reference Manual*.

Kerberos Authentication

Some Genesys components (Management Framework, Platform SDK, and Workspace Desktop Edition) also support the use of Kerberos external authentication to authenticate users. This enables authentication to be done on the client side before a connection to Configuration Server is made. For more information, refer to the "Kerberos External Authentication" chapter in the *Framework External Authentication Reference Manual*.

User Authorization

After the user is authenticated, user authorization determines that the user is entitled to access the system, either all or parts thereof, and defines what that user can do to or with the data that they can access. In a physical environment, this could be implemented by a series of locked doors - only certain people are authorized to access what lies behind each door, and only authorized people carry the keys to the doors to which they are authorized to enter. Similarly, in a computer system, this is often accomplished with a permissions system, in which only authorized users can see (in some cases) only specific data and can perform only certain tasks on that data.

Genesys software uses two levels of permissions to implement user authorization:

- Object-Based Access Control—What the user can see and do to an object is controlled by a set of permissions.
- Role-Based Access Control—Provides an additional layer of protection of your data from unauthorized users by defining what is displayed in the interface and therefore limiting the data to which a user has access.

Supporting Components

Most Genesys components support authentication and authorization as described in this document. The following components support authentication and authorization, but do not use Genesys Configuration Server:

- Genesys Interactive Insight (GI2)
- Genesys Enterprise Telephony Software (GETS)
- Genesys Quality Management (GQM) OEM products from Zoom
- Workforce Management-related OEM products from:
  - SilverLining
    - Genesys Training Manager
    - Genesys Skills Assessor
  - Aria
    - *Gplus* Adaptor for Aspect WFM
    - *Gplus* Adapter for IEX WFM

- *Gplus* Adapter for Teleopti WFM
- *Gplus* Adapter for Verint WFM