



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

Authentication and Authorization

5/1/2025

Authentication and Authorization

Unauthorized data access and the abuse of user privileges are common concerns for multi-user environments. Ensuring data correctness and its instant availability over the course of its lifecycle is critical for the business. Data, software, or the configuration must not be corrupted or modified by an unauthorized party.

Genesys provides the following security features to address data confidentiality:

- [User Authentication and User Authorization](#)
- [User Passwords](#)
- [SNMPv3 Passwords](#)
- [Object-Based Access Control](#)
- [Role-Based Access Control](#)
- [No Default Access for New Users](#)
- [Inactivity Timeout](#)
- [Security Banner at Login](#)
- [Last Logged In Display](#)

Tip

Genesys strongly recommends careful consideration of network, file system, database, and operating system permissions to complete the protection afforded by these features.