



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 Rules System Overview

Role-Based Access Control

5/7/2025

Role-Based Access Control

Genesys Rules System role-based access control utilizes Configuration Server-defined access groups and roles to control visibility and access to rule packages, rule templates, rules, and business calendars. Because these objects are not stored in the Configuration Server database they will not have security permissions associated with them, as Configuration Server objects do. The GRAT server will utilize the access permissions for the container object, and the Genesys Rules System objects will inherit these access permissions.

Role-based access control requires Configuration Server 8.0.2 or higher and Genesys Administrator 8.0.2 or higher.

Rule packages and business calendars inherit their access permissions from the Tenant object with which they are associated and the Business Structure folder access permissions. Business rules are associated with a specific node in the business structure. Their access permissions are inherited from the Configuration Server-defined node with which they are associated (the business structure nodes are created by using Configuration Manager or Genesys Administrator). Rule templates have Script objects created in Configuration Server that are used to hold the individual access permissions of the rule template. Additionally, rule templates inherit the access permissions from the business structure node with which they are associated.

For more detail about Role-Based Access Control and GRS, go to the **Deployment Guide** (new document).

For a full discussion of Genesys Role-Based Access Control, please refer to the **Genesys Security Deployment Guide** (new document).