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 Deployment Guide

Configuration Considerations

12/19/2025

Configuration Considerations

This section contains some considerations that you should keep in mind when you are configuring your Genesys Rules System environment.

Contents

Genesys Rules Authoring Tool (Server)

In a multi-tenant environment, the authorized tenant(s) must be added to the `Tenants` tab.

- This application must have a connection to at least one GRE application, Genesys Web Engagement Engine application, or application cluster.
- A default listening port must be specified in the configuration.
- On the `Security` tab, under `Log On As`, you must provide the username of a user who has Read, Change, and Create permissions to the `Scripts` folder.

The `Security` tab is available only in Genesys Administrator 8.1.0 or later. Otherwise, you must perform this part of the configuration through Configuration Manager.

Genesys Rules Authoring Tool (Client)

- Users or access groups must have, at a minimum, Read and Execute permissions to this application, in order to log in to the Genesys Rules Authoring Tool.
- Users or access groups must have, at a minimum, Read and Execute permissions to this application, in order to access the Repository through the Rules Development Tool. That is, on the Repository Server preferences screen in the Genesys Rules Development Tool, the user whose name and password is provided must have Read and Execute permission—or must belong to an access group that has those permissions—to the GRAT client application object.

Genesys Rules Engine

- Tenants that may use this Rules Engine must be specified.
    - When deploying a rule package from the Rules Authoring Tool, if there are no "target" Rules Engines to select from, check that the correct tenants have been specified for both the Rule Authoring Tool and Rules Engines. Only those Rules Engines whose tenants match will be displayed.
- A default listening port must be specified in the configuration.
- A second port must be specified in the configuration:
    - ID: genesys-rules-engine (the name of the Rules Engine web application; can be changed by the installer)
    - Port: (port being used by Tomcat or WebSphere)
    - Protocol: http
    - Secured: Optionally, select to activate deployment over a secured connection.

Access Groups

No access groups are created out of the box for Genesys Rules System. Suggested access groups to create, at a minimum, are the following:

- Rule Authors
- Rule Developers

Roles

- Requires Configuration Server and Genesys Administrator 8.0.2 or later.
- No roles are created out of the box for Genesys Rules System.
- Suggested roles to create, at a minimum, are the following:
  - Rules Administrator (all privileges)
  - Rules Author (relevant privileges in the Rule Authoring and Business Calendar groups)
  - Rules Developer (all privileges in the Rule Templates group)
- Users may be assigned individually to these roles, and/or access groups to which the users belong may be assigned to these roles.
- Role changes take effect immediately. See Role-Based Access Control for more information about roles and role-based access control.

Users/Persons

- No users are created out of the box for Genesys Rules System.
- Genesys Rules System users can be agents or non-agents.
- Users who log in to the GRAT must have access to one or more tenants, in a multi-tenant environment, with at least Read permission to the tenant(s).
- The user who is specified in the GRDT preferences must have access to one or more tenants, in a multi-tenant environment, with at least Read permission to the tenant(s).
- In addition to the users for the GRAT and the user(s) for the Rules Development Tool, you must create one non-agent user (for example, GRAT_Application_Proxy) who has Read and Change permissions to the Scripts folder.

Business Structure

- No business structure is created out of the box for Genesys Rules System.
- If you are using the Genesys Rules System with intelligent Workload Distribution, the business structure

is created in the iWD GAX Plug-in and is then synchronized with Configuration Server, after which it becomes available for use by the Genesys Rules System.

- A top-level folder must be created, of type Business Unit (called Configuration Unit in Configuration Manager) or Site, with the exact name of Business Structure.
- Within the Business Structure folder, at least one more Business Unit or Site must be created (it does not matter which one).

These first level nodes under Business Structure represent the Solution(s). Within each solution, additional levels of hierarchy may be created, as needed, using either Business Units or Sites. Those levels of hierarchy beneath the Solution level will represent the business context.

- Multiple solutions may be created by creating additional Business Units or Sites directly beneath the Business Structure folder.
- Business Structure is created under Resources for single tenant Configuration Server or under a Tenant for a multi-tenant Configuration Server.
- Read permission to the Business Structure folder must be provided to the users and/or access groups that you want to use the Rules Authoring Tool. Normally, if the user or access group has permission to the Tenant object, this will be propagated automatically. If you do not want a user or access group to have permission to see all nodes of the business structure, you can control this by not giving that user or access group(s) Read permission to those folders. See About Business Structure for more information.

Scripts

- A user (such as `GRAT_Application_Proxy`) on whose behalf the GRAT server will update the `Scripts` folder must have Read, Create, and Change permissions to this folder.
- Individual Rules Development Tool users, or one or more access group(s) to which they belong, must have Read permissions to the individual Script objects that represent the rule templates to which they should have access. Alternatively, you might decide to grant permission to the entire Template Access Control scripts folder to individual users or an access group such as Rule Developers, and allow that permission to propagate to all scripts that might be created in the future.
- Individual GRAT users, or one or more access group(s) to which they belong, must have read permissions to individual Script objects that represent the rule templates that rule authors should be able to add to a rule package when creating it.
- Users need Read access to parameter scripts. These scripts are maintained via Genesys Administrator Extension.