Genesys Rules System Deployment Guide

Role Permissions

5/12/2025

Role Permissions

Genesys Rules System 8.5 defines a set of role permissions for governing the tasks that can be performed in the Genesys Rules Authoring Tool.

The set of permissions is the following:

- Business Calendar - Create
- Business Calendar - Delete
- Business Calendar - Modify
- Business Calendar - View
- Business Rule - Create
- Business Rule - Delete
- Business Rule - Modify (see Business Rule - Edit Only)
- Business Rule - View
- Business Rule - Edit Only (new in 8.5.001.21)—Allows a user to edit and save only the parameter values of a rule. (No other permissions are granted with this role privilege—such as adding new conditions or actions, moving rules or changing their order, adding, deleting or copying rows, making changes to the rule summary.) If `Business Rule - Modify` is `false` and `Business Rule - Edit Only` is `true`, this behavior is enabled. If `Business Rule - Modify` is `true`, then `Business Rule - Edit Only` is ignored.
- Business Rule - View
- Rule Template - Create
- Rule Template - Delete
- Rule Template - Modify
- Rule Package - Create
- Rule Package - Delete
- Rule Package - Modify
- Rule Package - Deploy
- Test Scenario - Create
- Test Scenario - Modify
- Test Scenario - Delete
- Test Scenario - View
- Test Scenario - Execute
- Snapshot - Create
- Snapshot - Delete
- Snapshot - View: User can view and export snapshots. If this is not enabled, users will only see LATEST

in the list of snapshots, which represents 8.1.2 functionality where users can only deploy the latest version.

> **Important**
>
> Snapshot permissions are active on the `Deployment` tab of GRAT, so all snapshot permissions also require `Rule Package - Deploy` permission.

The combination of the access permissions and the role permissions will determine whether a task can be performed. For example:

- To view a rule a user must have Read permission for the node with which the rule is associated as well as the Business Rule - View role permission.
- To delete a rule, the user must have Read permissions for the node and the Business Rule - Delete role permission. In this example, Read access permission is also needed for the delete task, because the user will not have visibility to any object that is associated with the node without Read access permissions.

Role permissions for importing and exporting templates and rule packages must be set to the following values:

- To import a template, a user must have Create permission for the Rule Template.
- To export a template, a user must have read access to the Template Script Object representing the template. See Template Script Objects for more information.
- To import or export rule packages, a user must have full permissions granted. For example, if a user does not have the ability to view business calendars or test scenarios, they won't be exported in the rule package XML. Conversely, if a user doesn't have permission to create calendars or test scenarios on import, they will not be able to create these resources from the imported rule package.