Genesys Rules System Deployment Guide

Role Permissions for Rules and Rule Packages

12/16/2025

Role Permissions for Rules and Rule Packages

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.

Rules

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.

Rule Packages

- Release 8.5.302 provides package-level overrides to these global roles—a user's role privileges can be restricted to specific rule packages by applying Role-Based Access Control at the rule package level. See **Changes in 8.5.302**.

List of Permissions

- Business Calendar - Create
- Business Calendar - Delete
- Business Calendar - Modify
- Business Calendar - View
- Business Rule - Create
- Business Rule - Delete
- Business Rule - Modify
- Business Rule - View
- Business Rule - Edit Only - allows a user to edit and save only the parameter values of a rule. No other permissions are granted.

- Rule Template - Create
- Rule Template - Delete
- Rule Template - Modify
- Rule Package - Create
- Rule Package - Delete
- Rule Package - Modify
- Rule Package - Deploy
- From 8.5.303—Rule Package - Undeploy (also requires Rule Package - Deploy permission)
- From 8.5.303—Rule Package History - Admin View—Allows viewing of complete package history for a rule package without checking access to the business hierarchy subnodes used inside the rule package. Even with this role privilege enabled, the package history will only be shown for packages that the user can view.
- From 8.5.303—Rule Package History - View Changed By—Allows users to view Changed By information in Package History.
- Locks - Override
- 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.

Changes in 8.5.302

Support for Role-Based Access Control at the Rules Package Level

> **Important**
> GRS requires Genesys Administrator 8.1.305.04 (minimum) for configuring package level permissions.

You can expand the graphics by clicking on them.

Background

Previously, GRAT used Configuration Server Roles to provide only global access control to all packages in a given node of the business hierarchy. The privileges, like `Modify Rule Package`, `Delete Rule Package`, `Modify Rule`, `Delete Rule` and so on, are granted to users via roles. With this approach, if a user is granted the `Modify Rule Package` (for example) privilege, then they can modify all the rule packages defined in a node of the GRAT business hierarchy.

Release 8.5.302 now provides package-level overrides to these global roles—role privileges can be restricted to specific rule packages by applying Role-Based Access Control at the rule package level. The new Rule Package Level Roles (roles created specifically for use with rule packages only) can be mapped to rule packages to override the global-level roles. These Rule Package Level Roles will have no effect if not mapped to a rule package.

New Role Permission—View Rule Package

View access for specific rule packages can now be controlled by using the new role permission **View Rule Package**. The new permission is applicable to only the rule package level.

Existing Role Permissions

All of the existing role permissions except **Create Rule Package** and template-related permissions are applicable at the rule package level too.

Example

In 8.5.302 you can now assign role permissions at both global/node level and at rule-package level to achieve the following outcome:

- Department A
  - Rule package 1
  - Rule package 2
  - Sales
    - Rule package 3

- Department B
  - Rule package 4

- User A—Can see Department A but not Department B
- User B—Can see Department B but not Department A
- User C—Can see rule package 1, but rule package 2 is hidden

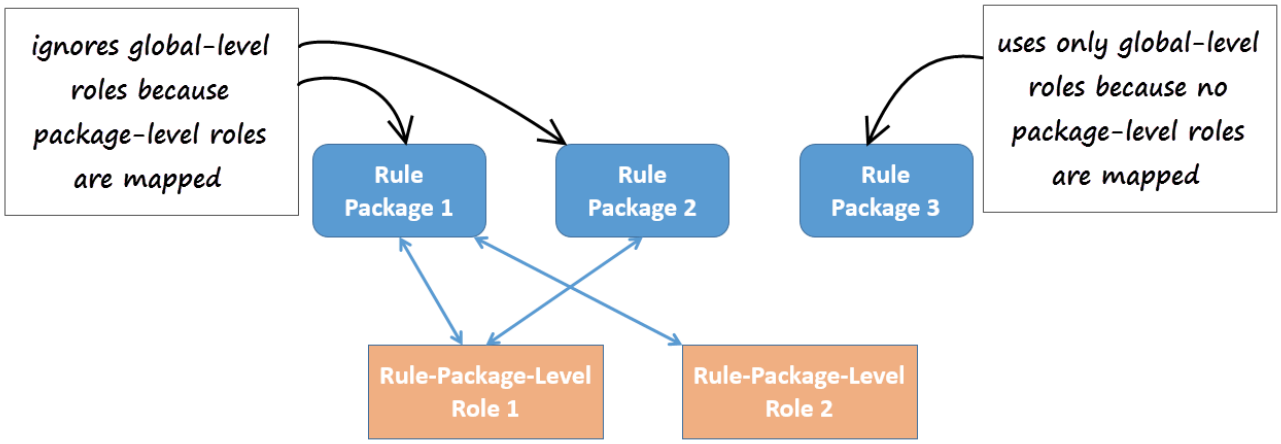
Location

To distinguish these new roles from global-level roles, they are placed in a new folder:

```
[Tenant] > Roles > GRS Rule Package Level Roles
```

Package-Level Overrides

Where package-level roles are mapped to a rule package, they override global-level roles.

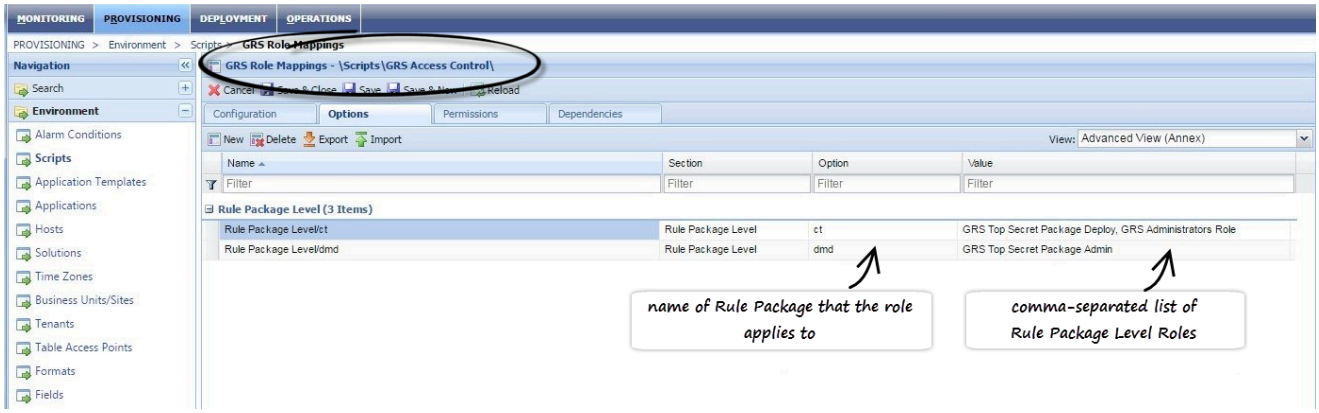


Managing the Mapping of Roles

The mapping of the rule packages to Rule Package Level Roles is managed in Genesys Administrator or Genesys Administrator Extensions, in the options under section **Rule Package Level** of the **\Scripts\GRS Access Control\GRS Role Mappings** script. The example below is from Genesys Administrator.

> **Important**
> Because the delimiter in the list of roles is a comma, you can't use commas in the

> names of any role.



Viewing GRAT User Permissions

To enable GRAT users to view their current list of permissions, a **Check My Permissions** button is now also available at the rule-package level and shows the permissions at selected package level.