



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

Creating the GRAT Application Object in Configuration Manager

12/22/2025

Creating the GRAT Application Object in Configuration Manager

Purpose

To create the Application objects in Configuration Manager that will link the GRAT with Configuration Server. The GRAT requires two applications in Configuration Server: a server application and a client application.

Procedure

1. Import the GRAT application template for the server.

To import the application template that is to be used for the server application:

1. In Configuration Manager, navigate to the `Application Templates` folder.
2. Right-click the `Application Templates` folder, and select `Import Application Template`.
3. Browse to the templates folder of the installation CD, and select the appropriate template for your version of Management Framework.
 - For Management Framework 8.1.1, select `Genesys_Rules_Authoring_Server_852.apd`.
 - For Management Framework 8.1 and earlier, select `Genesys_Rules_Authoring_Generic_Server_852.apd`.
- Click `OK` to save the template.

2. Import the GRAT application template for the client.

To import the template that is to be used for the client application:

1. Right-click the `Application Templates` folder.
2. Select `Import Application Template`.
3. Browse to the templates folder of the installation CD.
4. Select `Genesys_Rules_Authoring_Generic_Client_852.apd`.

5. Click OK to save the template.

3. Configure the server application.

Configuring the server application

To configure the server application:

1. Right-click the Applications folder and select New > Application.
2. Select the Genesys_Rules_Authoring_Generic_Server template.
3. On the General tab, enter a name for the application, such as Rules_Authoring_Server.
4. On the Tenants tab, add the Tenants that will be visible in the GRAT interface.
5. On the Server Info tab, select the Host on which the application will be installed, and configure a default listening port.
6. On the Start Info tab, enter x for each field. This is required in order to save the configuration.
7. On the Connections tab, add a connection to the Rules Engine application (multiple Rules Engine applications can be added).

Tip

The Port ID selected for a Rules Engine connection should be the name of the Rules Engine Web application. Optionally, a connection to an application cluster of Rule Engines may be added.

8. On the Connections tab, add a connection to the Database Access Point (DAP).
9. On the Connections tab, add a connection to the Message Server.
10. Click **Apply**.
11. On the Options tab, configure log options.
12. In the settings section, the following options can be configured:

Important

Where the table below indicates that a GRAT (re-)start is required,

this means the GRAT Web Application must be restarted. This can be accomplished in different ways depending upon the application server. In Tomcat, JBOSS or Websphere, GRAT can be stopped and started from the administration console. This does not require restarting the entire app server (there could be other applications deployed to the same container, not only GRAT). If GRAT is the only application deployed, you can simply restart the application server (for example, restart Tomcat server).

Settings in GRAT

Description	Valid values	Default value	Takes effect
group-by-level (group rules by business level)			
There are three levels of rules: global, department, and process. With value <code>true</code>, rules are grouped by business level: • All global rules belong to agenda group <code>level0</code>. • Department rules belong to agenda group <code>level1</code>. • Process rules belong to agenda group <code>level2</code>. When a rule package is executed, <code>level0</code> rules are	<code>true/false</code>	<code>true</code>	Immediately

Description	Valid values	Default value	Takes effect
executed first. Updates from this first pass then influence the department (level1) rules which are executed in the second pass. Updates from this second pass then influence any process rules (level2), which are executed in a third pass. Note: The GRE option sequential-mode must be false when group-by-level is set to true. When group-by-level is set to false, all rules are executed in a single pass. Changes made by a rule do not influence which other rules are executed (unless a Drools “update” or “insert” command is used).			

Description	Valid values	Default value	Takes effect
<i>CEP functionality</i> Genesys Web Engagement's CEP functionality strips out the rule attribute that indicates which level a rule is associated with. So, the setting of the group-by-level has no influence on rule execution.			
max-connections			
Specifies the maximum number of different users that may be connected to the server. Multiple connections from the same user ID are only counted once.	Any positive integer	99	After GRAT (re-)start
session-timeout			
Specifies the amount of time (in minutes) a client session can have no communication with the Rules Authoring Server before timing out. If no value is specified, the	Any positive integer	30	Immediately

Description	Valid values	Default value	Takes effect
timeout (if any) defined by the application server applies. If the value is less than or equal to 0, the session will not time out.			
session-timeout-alert-interval			
The amount of time (in minutes), prior to an expected timeout, for a user to be warned of a pending timeout. If no value is specified, or if the value is less than or equal to 0, the default warning period of 1 minute will be used. For example, if you set the value of this option to 3, the user will be warned 3 minutes prior to an expected timeout. This warning dialog box will prompt the user to extend the	Any positive integer	1	Immediately

Description	Valid values	Default value	Takes effect
session. If the session is not extended, the user will be logged out and the login dialog box will be displayed. Any unsaved changes that the user made during their session will be lost.			
strict-mode			
This option controls whether or not the rules authoring tool enables <i>strict</i> mode in the DROOLS rule compiler. Strict mode will cause the compiler to catch common mistakes when the rule author attempts to validate or save a rule. Genesys recommends leaving this option set to its default value <code>true</code> .	true/false	true	Immediately
verify-deployer-address			
Indicates whether to verify the TCP address of the application deploying rules to be that of a valid associated Genesys Rules Engine (one in the valid list of application	true/false	true	Immediately

Description	Valid values	Default value	Takes effect
connections). With its default value of true, this option protects against illegal attempts to deploy packages from any other application.			
display-n-template-versions			
Specifies the maximum number of versions to display for any published template. Note: if the current rule package is using an older version that is not included in the last "n" versions, it will also be shown, in order to allow the user to upgrade to a more recent template. For example, if "n" is 3, and there are 10 versions of a template, GRAT will show only version 10, 9, and 8. If the rule	Minimum value 1	3	Immediately

Description	Valid values	Default value	Takes effect
package is currently associated with an older version, for example, version "5", then that will also be shown, and the checkbox will be selected.			
deploy-response-timeout (not in application template by default)			
Specifies the timeout (in seconds) applied to the deployment of a rule package before an error condition is indicated. If the timeout is reached, the deployment fails (is this true?) and an error is returned.	Any positive integer	300	Immediately
require-checkin-comment			
Specifies whether users must add a check-in comment when committing changes to rules. These comments show up when	true/false	false	Immediately

Description	Valid values	Default value	Takes effect
viewing package history. If the value is set to false (default), users can save changes to rules without specifying a comment.			
force-snapshot-on-deployment			
Specifies whether users can deploy only a package snapshot. If the value is true, users can only deploy a package snapshot. If false (default), users can deploy either the LATEST package or a snapshot.	true/false	false	Immediately
encoding (not in application template by default)			
Activates Unicode support for the conversion of data between the local character set that is used by Configuration Manager and the UTF-8 encoding that is used by the Rules Authoring Server. By default, code page conversion is disabled. To activate this functionality, set this option to the name of a converter that can translate the local character set to UTF format. The converter that is suitable for a particular deployment can be found by using the ICU Converter Explorer. There is no default value for this option. For valid values, see the ICU			After GRAT restart

Description	Valid values	Default value	Takes effect
Home > Converter Explorer pages (http://demo.icu-project.org/icu-bin/convexp).			
clear-repository-cache			
The GRAT server builds and maintains a cache of the rules repository database (for example, index files, and so on), and stores this on the file system under WEB-INF/classes/repository. The cache improves performance when accessing frequently used rules, calendars, and so on. However, this cache must stay synchronized with the rules repository database. Normally, if GRAT is restarted, it re-uses the existing cache, which is synchronized with the rules repository database. In this	true/false	false	After GRAT (re-)start

Description	Valid values	Default value	Takes effect
case, the clear-repository-option should be set to false (default). However, if you are configuring a second GRAT for warm standby (see High Availability Support), this option should be set to true for both the primary and the standby instances of GRAT. Since either GRAT could be brought online in the event of a failure, this option forces GRAT always to rebuild the cache and re-synchronize it with the rules repository database. Setting this option to true can delay the startup of GRAT, since the cache must be rebuilt, but it ensures that it is properly			

Description	Valid values	Default value	Takes effect
synchronized with the rules repository database.			
evaluate-decision-table-rows-top-down (new in 8.5.0)			
Determines the order that the Decision Table rows are written out to the DRL. The default value is false, meaning that the rows are executed from the bottom up. If you change this default option, the behavior of GRAT's Test Scenario feature changes immediately, but you will need to re-deploy the rule package in order for the change to be observed in GRE.	true/false	false	Immediately
single-sign-on (new in 8.5.0)			
Note: This configuration option should only be used when deploying in a Genesys	true/false	false	After GRAT (re-)start

Description	Valid values	Default value	Takes effect
Engage cloud single-sign on environment, and does not apply for Genesys on-premise customers deploying GRS.			
Indicates the login method: either single sign-on, or legacy login. With value false, the /index.jsp page will redirect to /login.jsp for legacy user login. With value true, then /index.jsp will redirect to /singlesignon.			
link-to-hub (new in 8.5.0)			
Note: This configuration option should only be used when deploying in a Genesys Engage cloud single-sign on environment, and does not	string	No default value	After GRAT (re-)start

Description	Valid values	Default value	Takes effect
apply for Genesys on-premise customers deploying GRS. This option specifies the URL to which GRAT should redirect once the GRAT SSO session completes. This URL is used in two situations: • First, when the user clicks the log out button in GRAT, the browser will be redirected to this URL. • Second, if an SSO login is successful but the subsequent login to Configuration Server fails, then an error box is displayed to the user. Once the error box is dismissed, the browser will be redirected to the specified URL. Note: The user must have logged in via SSO for this to occur.			
decision-table-enable-wildcards (new in 8.5.001)			

Description	Valid values	Default value	Takes effect
Controls whether the wild card feature is enabled in decision tables.	true/false	true	After GRAT (re-)start
help-file-url (new in 8.5.001)			
Specifies the base URL location of online help for GRAT. You can specify a local protected URL to install the wiki Help files if your organization prefers. If you change the default value, you must specify the location of your locally hosted Help files.	String	<a href="http://docs.genesys.com/Special:HelpLink/GRATHelp?context=<GRAT version>.index">http://docs.genesys.com/Special:HelpLink/GRATHelp?context=<GRAT version>.index	Immediately
use-legacy-language-pack-webhelp (introduced in 8.5.001 and removed in release 8.5.1)			
With value true, when the GRAT user clicks the Help button in non-English environments, GRAT will use the legacy WebHelp files shipped with the various language packs. These legacy files may not reflect the full set of current functionality. With value false (default), GRAT will retrieve online Help from the docs.genesys.com website in the desired language (if available). In release 8.5.1,	true/false	false	After GRAT (re-)start

Description	Valid values	Default value	Takes effect
translated online Help is available, so this option is not required.			
context-services-rest-api-protocol (new in 8.5.001)			
The protocol that GRAT uses for the Context Services metadata REST API. Valid values are: • http • https	http, https	http	After GRAT (re-)start
context-services-rest-api-host (new in 8.5.001)			
The hostname of the Context Services that GRAT connects to.	String		After GRAT (re-)start
context-services-rest-api-port (new in 8.5.001)			
The port of the Context Services metadata API	String		After GRAT (re-)start
context-services-rest-api-base-path (new in 8.5.001)			
The base path of the Context Services API.		/	After GRAT (re-)start
list-object-use-name (new in 8.5.001.21)			
Enables users to control whether		true/false	After GRAT (re-)start

Description	Valid values	Default value	Takes effect
either the name or the display name of a Configuration Server list object is encoded in the DROOLS rule file.			
enable-nested-solutions (new in 8.5.100.21)			
Controls whether users can create new rule packages under any node of the hierarchy. For iWD, it is recommended to set this option to false.	false	true/false	After GRAT (re-)start
deploy-method (new in 8.5.100.21))			
Enables users to override the automatic detection of the protocol to construct the "callback" URL used by GRE to fetch the DRL. GRE will use the selected method to connect with the GRAT server during deployment.	auto	auto / http / https	After GRAT (re-)start
enable-cep-calendars (new in 8.5.200.0x)			

Description	Valid values	Default value	Takes effect
Enables users to enable/disable business calendars for rules that are based on the Complex Event Processing (CEP) template.	false	true/false	After GRAT (re-)start
allow-partial-cluster-deployment (new in 8.5.200.0x)			
With value true, allows GRAT to perform a partial deployment to a GRE-type application cluster, as distinct from pre-8.5.2 behavior in which cluster deployment fails if even a single node fails.	false	true/false	Immediately
rest-api (new in 8.5.200.0x)			
Defines whether the REST API is enabled. In addition, this configuration option will enable them to determine whether or not to force only SSL	disabled	- disabled—The REST API is disabled and will not accept any requests - enabled—The REST API is enabled and will accept both secure (https) and non-secure (http) requests - requireSSL—The REST API is enabled and will only accept	After GRAT (re-)start

Description	Valid values	Default value	Takes effect
communications. Genesys recommends running over SSL in order to protect the authentication tokens that flow on each request from compromise. SSL can be disable where appropriate (for example, testing labs, positioning server behind firewalls, and so on).		secure (https) requests.	

13. Give the application Read, Create, and Change permissions on the Scripts folder for each Tenant that you add. (One approach is to create a user called GRAT_Application_Proxy and add that user to the SYSTEM access group. Then, on the Security tab of the application, in the Log On As section, select This account and add the GRAT_Application_Proxy user.)
14. Click Save.

4. Configure the client application.

To configure the client application:

1. Right-click the Applications folder.
2. Select New > Application.
3. Select the Genesys_Rules_Authoring_Generic_Client template.
4. On the General tab, enter a name for the application, such as Rules_Authoring_Client.
5. Click Save.

Next Steps

- **Installing the GRAT Component**