



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.

Deployment Guide

Configuring Genesys Rules System

12/14/2025

Configuring Genesys Rules System

Complete the procedures in the tabs below to tune Genesys Rules System to work with Web Engagement.

Genesys Rules Authoring Tool

Configuring Genesys Rules Authoring Tool

Prerequisites

- Your environment includes Genesys Rules Authoring Tool (GRAT). See [Genesys environment prerequisites](#) for compliant versions. For more information about installing GRAT, refer to the [Genesys Rules System Deployment Guide](#).

Start

1. In Genesys Administrator, navigate to **Provisioning > Environment > Applications**, select the GRAT Server application (the application with type Business Rules Application Server), and click **Edit**.
2. In the Connections section, click **Add....**
3. Select the Genesys Web Engagement Cluster and click **OK**.

Important: If your version of GRAT does not recognize connections with your Application Cluster object, you can connect to any of your Web Engagement Server node applications instead.

You can determine whether your Application Cluster is recognized by seeing whether it shows up as a valid location in the [rules package deployment scenario](#).

4. Select the Cluster in the list of connections and click **Edit**.
5. In the **Connection Info** window, select the correct port for the ID field, that is, /server/data/rules/deploy. Click **OK**.

The screenshot shows the 'Connection Info' dialog box with the 'General' tab selected. The 'Server' field contains 'GWE 85 Cluster'. The 'ID' field contains 'server/data/rules/deploy'. Below these are fields for 'Connection Protocol', 'Local Timeout' (0), 'Remote Timeout' (0), 'Trace Mode' ([Unknown Trace Mode]), and 'Connection Type'. At the bottom are 'OK' and 'Cancel' buttons.

ID is set to the correct port.

6. Select the **Options** tab.
7. In the **[settings]** section, set **verify-deploy-address** to false. You must set this option because in Genesys Web Engagement, rule packages are deployed to the Cluster, not to Genesys Rules Engine. When set to false, this option prevents GRS from trying to verify that the server deploying the rules is Genesys Rules Engine.

Configuration

Options

Permissions

Dependencies

Alarms

Logs

New

Delete

Export

Import

View:

Advanced View (Options)

Name	Section	Option	Value
Filter	Filter	Filter	Filter

settings (6 Items)

settings/group-by-level	settings	group-by-level	false
settings/max-connections	settings	max-connections	99
settings/session-timeout	settings	session-timeout	30
settings/session-timeout-alert-interval	settings	session-timeout-aler...	1
settings/strict-mode	settings	strict-mode	true
settings/verify-deploy-address	settings	verify-deploy-address	false

verify-deploy-address is set to false.

8. In the **Permissions** tab, set a user who has Read, Create, Change rights for the Scripts folder in **Log On As**. This user should also have: Read access to all tenants which are supposed to be used; Role with sufficient permissions (as detailed in [Genesys Rules System Deployment Guide](#)); Read access to Business Structure folder and associated nodes that are supposed to be used; Read access to Scripts folder and Scripts objects (which are representations of the rule templates).
9. Click **Save & Close**.

End

(Optional) Configuring Roles Settings for Rules Management

You should complete this procedure if you need to import permissions to enable a user to create rules for Genesys Web Engagement. Once roles are imported, you can assign them to the user who publishes the rule templates and creates rules for GWE.

You should not complete this procedure if you have already created a user who has permissions to create rules packages in Genesys Rules Authoring (as described in the "Role-based Access Control" chapter of the [Genesys Rules System Deployment Guide](#)).

Start

1. In Genesys Administrator, navigate to **Provisioning > Accounts > Roles** and click **New...**
2. Enter a name for the new role. For example, GWE_Rules_Administrator.
3. In the Members section, you can specify who should have this role. Click **Add** to add as many access groups or users as you need.

The screenshot shows the 'GWE_Rules_Administrator - \Roles\' window. The 'Configuration' tab is selected. Under the 'General' section, the 'Name' field is 'GWE_Rules_Administrator', 'Description' is 'in GRDT - import or create, modify and publish templates, in GRAT - create, modify, delete and dep', 'Tenant' is 'Environment', and 'State' is 'Enabled'. The 'Members' section has two sub-sections: 'Users' and 'Access Groups', both showing 'No objects to display'.

New Role

4. Select the **Role Privileges** tab and select Genesys Rules Authoring Tool. The privileges for GRAT are added to the GWE_Rules_Administrator role.

GWE_Rules_Administrator - \Roles

Cancel Save & Close Save Save & New Reload Validate Permissions

Configuration **Role Privileges** Permissions

Allow All Export Import

Add/Remove Products

☐ Interaction Workspace

☒ Genesys Rule Authoring Tool

☐ Genesys Administrator

Name	Value
Filter	Filter
Rule Authoring (4 Items)	
Create Rule	
Delete Rule	
Modify Rule	
View Rule	
Rule Packages (4 Items)	
Create Package	
Delete Package	
Deploy Package	
Modify Package	
Rule Templates (3 Items)	
Create Template	
Delete Template	
Modify Template	
Business Calendars (4 Items)	
Create Calendar	
Delete Calendar	
Modify Calendar	
View Calendar	

Imported Role Privileges

5. Click **Save & Close**.

End

Members of the GWE_Rules_Administrator role can now do the following:

- Create, modify, and delete rules
- Create, modify, delete, and deploy rule packages

- Create, modify, and publish CEP rule templates

Genesys Rules Development Tool

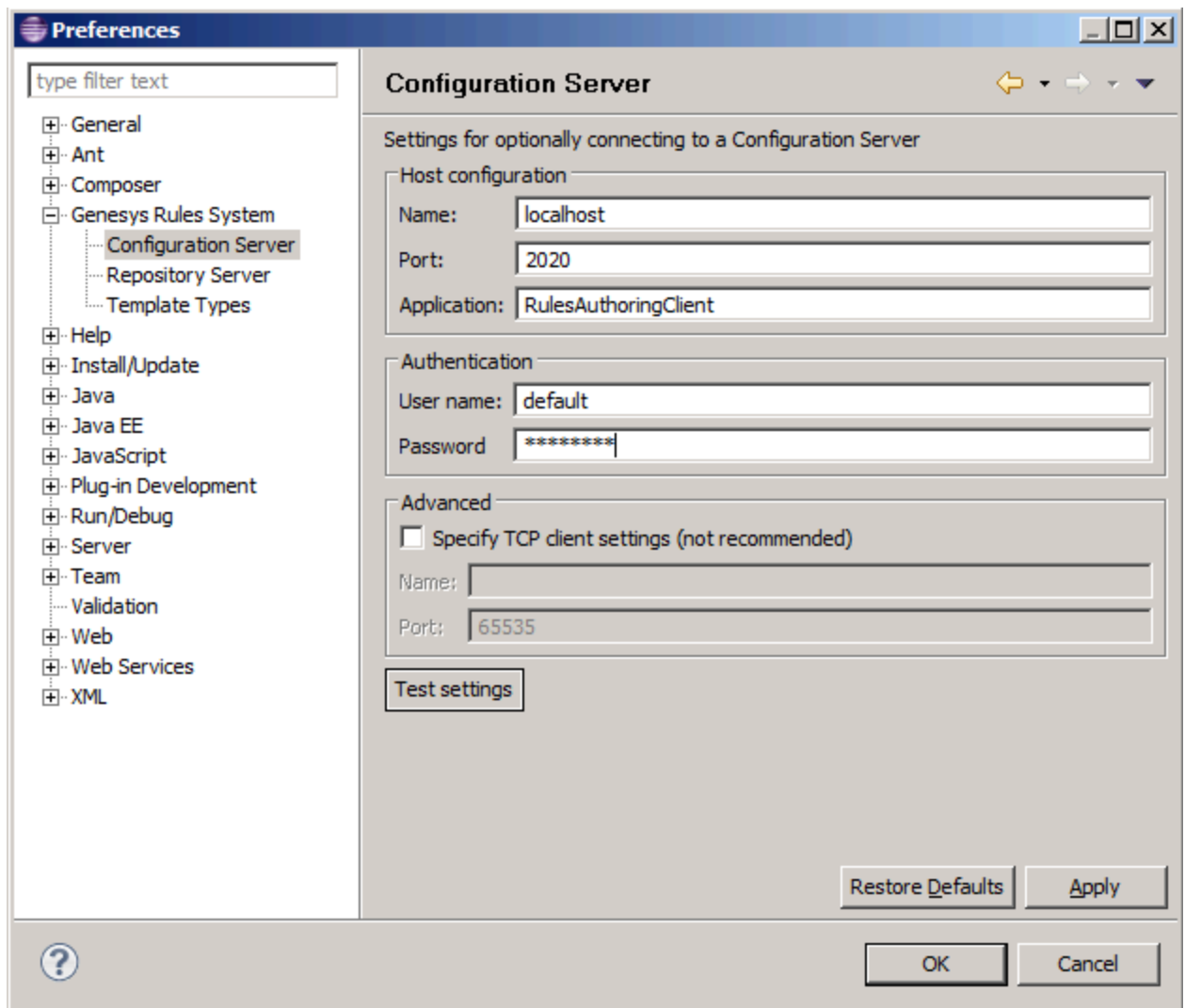
Configuring Genesys Rules Development Tool

Prerequisites

- Your environment includes Genesys Rules Development Tool (GRDT), deployed as a Composer plug-in. See [Genesys environment prerequisites](#) for compliant versions. For more information about installing GRDT, refer to [Installing the GRDT Component](#) in the the Genesys Rules System Deployment Guide.
- You enabled the Galileo update site in GRDT, as described in [Installing the GRDT Component](#).

Start

1. Open Genesys Rules Development Tool by starting Composer.
2. Navigate to **Window > Preferences**. The **Preferences** window opens.
3. Navigate to **Genesys Rules System > Configuration Server**. Edit the settings.
 - Enter the Configuration Server host name. For instance, localhost.
 - Enter the Configuration Server port. For instance, 2020.
 - Enter the application name for the Rules Authoring Client application. For instance, RulesAuthoringClient.
 - In the Authentication section, enter the name and password for a user who can connect to Configuration Server and click **Apply**.

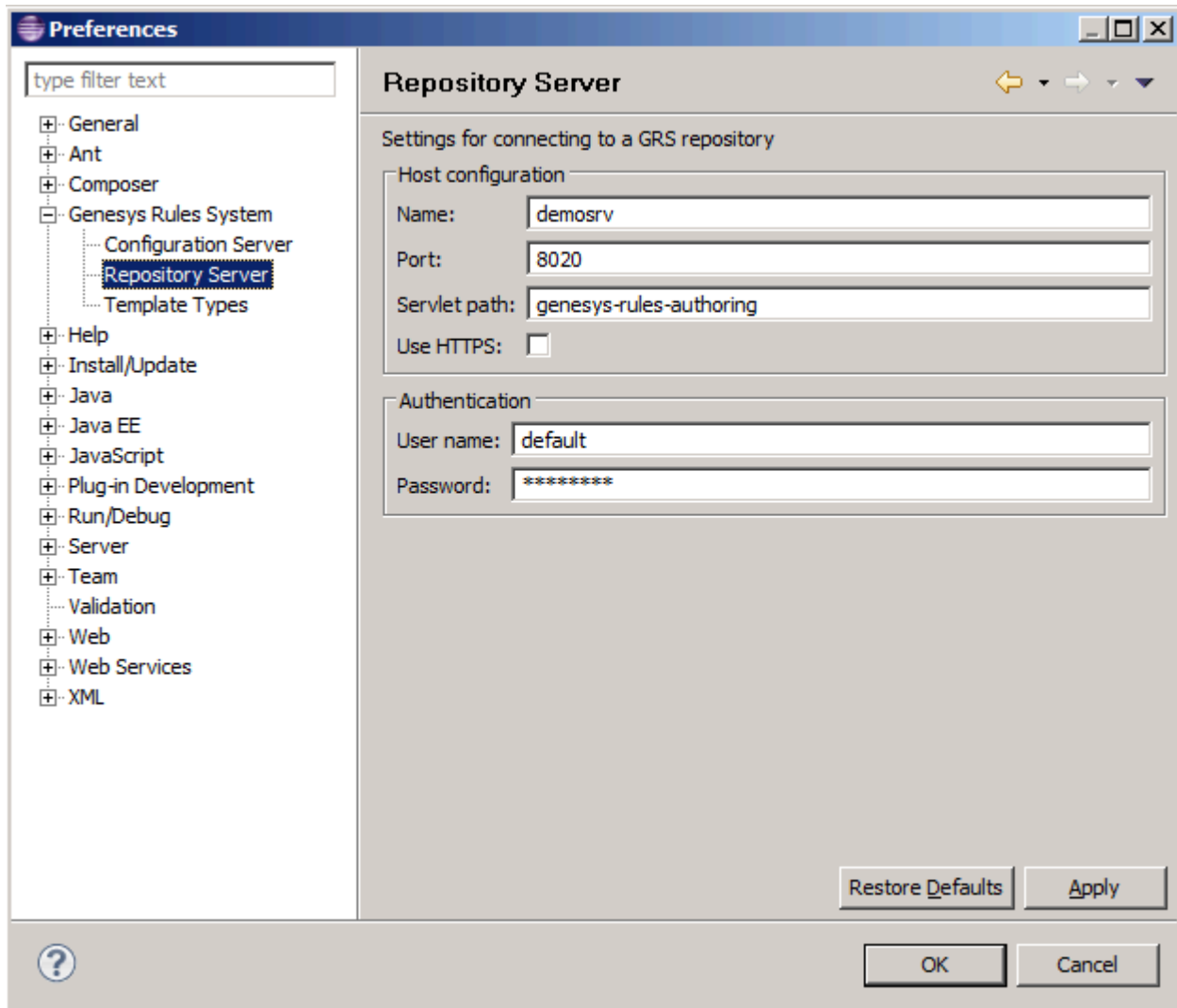


GRDT settings for Configuration Server.

4. Navigate to **Genesys Rules System > Repository Server**. Edit the settings.

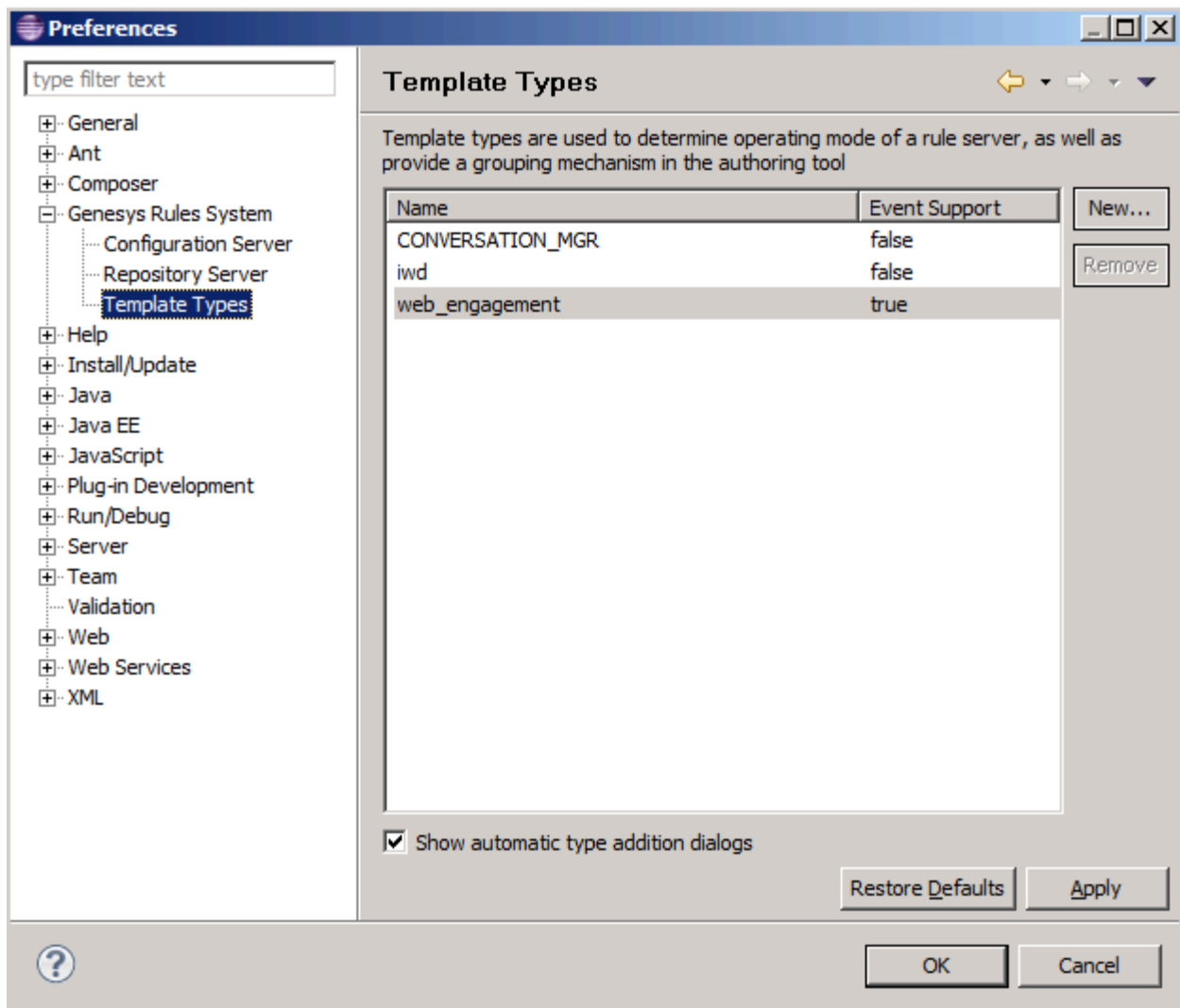
- Enter the Repository Server host name. This is the name of the host specified for the GRS application (application with type Business Rules Execution Server) in the Genesys Configuration Layer. For instance, localhost.
- Enter the Repository Server port. This is the port with the ID genesys - rules - engine that is specified for the GRS application (with type Business Rules Execution Server) in the Genesys Configuration Layer. For instance, 8020.
- Enter the Servlet path as genesys - rules - authoring.
- In the Authentication section, enter a name and password for a user who:
 - Has Read and Execute permissions for the Genesys Rules Authoring client application (set up in Configuration Server); this user must have explicit Read and Execute permissions or must belong to an access group with those permissions.
 - Belongs to a Role with the following privileges: Template - Create, Template - Modify, Template - Delete.

5. Click **Apply**.



GRDT settings for the Repository Server.

6. Navigate to **Genesys Rules System > Template Types**. If it is not present, add the **web_engagement** template type and set **Event Support** to true. Click **Apply**.



Template types in Composer

7. Click **OK**.

End

Next Steps

- Configure the [Generic Cassandra Settings](#) for your Web Engagement Server.