Deployment Guide

Authentication

2/26/2025

Authentication

Contents

You can enable secure communications with the History REST API by completing the procedures below to implement authentication. If you do enable authentication, then all the clients of the API must use the authentication scheme and credentials. Two common clients of the API are the Genesys Web Engagement Plug-in for Interaction Workspace and the Engagement Strategy. See "Configuring Authentication in Interaction Workspace" and "Configuring Authentication in the Engagement Strategy" for details.

Configuring Authentication in the Web Engagement Server

Complete the steps below to enable authentication for the History REST API.

Start

1. In Genesys Administrator, navigate to **Provisioning > Environment > Applications**, select the Genesys Web Engagement Server application, and click **Edit...**.
2. Click the **Options** tab and scroll down to the **[security]** section.
3. Set the following options:
   - auth-scheme
   - user-id
   - password
4. Click **Save & Close**.

End

Configuring Authentication in Interaction Workspace

If you enable authentication for the History REST API and use the Genesys Web Engagement Plug-in for Interaction Workspace, then you must complete the steps below to enable authentication for the plug-in.

Prerequisites

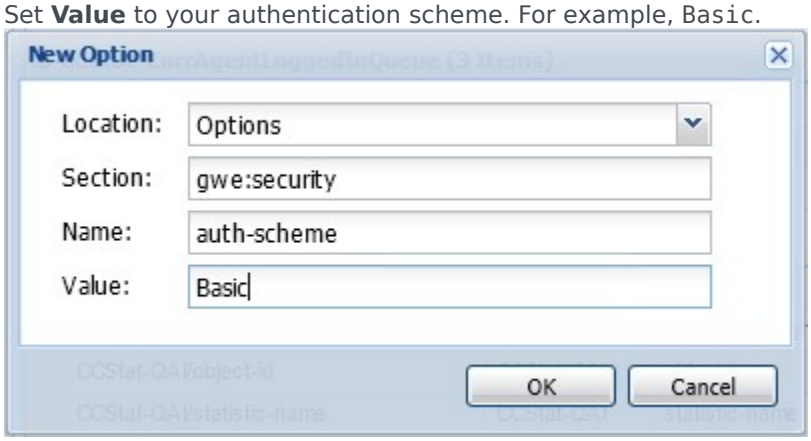
- You completed "Configuring Authentication in the Web Engagement Server".

Start

1. In Genesys Administrator, navigate to **Provisioning > Environment > Applications**, select the Interaction Workspace application, and click **Edit...**.
   Note: Before configuring the authentication options, be sure to read about each option to help determine the correct values for your deployment:
   - auth-scheme
   - user-id

- password

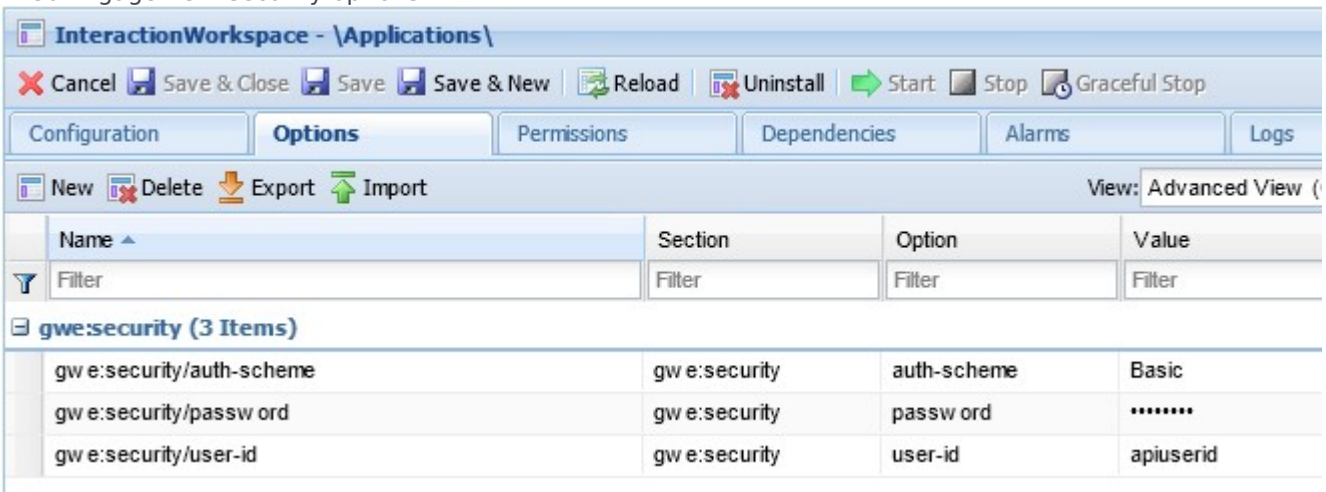
2. Click the options tab and then click **New**.
3. In the **New Option** window, configure the following:
   a. Set **Section** to `gwe:security`
   b. Set **Name** to `auth-scheme`
   c. Set **Value** to your authentication scheme. For example, `Basic`.



   d. Click **OK**
4. Complete steps a-d to configure the remaining security options:

Section	Name	Value
gwe:security	user-id	Your user ID.
gwe:security	password	Your user password.

Your configuration options for Interaction Workspace should now have a new section for the Genesys Web Engagement security options:



New security options for Genesys Web Engagement.

5. Click **Save & Close**.

End

Configuring Authentication in the Default Engagement Strategy

Complete the steps below to add security credentials to the default SCXML strategy to support authentication for the REST API.

Prerequisites

- You completed "Configuring Authentication in the Web Engagement Server".
- Your SCXML strategy uses the REST API. See Customizing the Engagement Strategy for details.

Start

1. Open the Engagement Logic strategy in Composer.
2. Open **default.workflow**.
3. Find and set your user and password credentials in the list of properties at the Entry point (Start).
4. Regenerate the SCXML and follow the Web Engagement application deployment procedure.

End

Next Steps

- Return to the Genesys Web Engagement Security page.