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

Authentication

4/23/2025

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 Backend 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 Backend 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

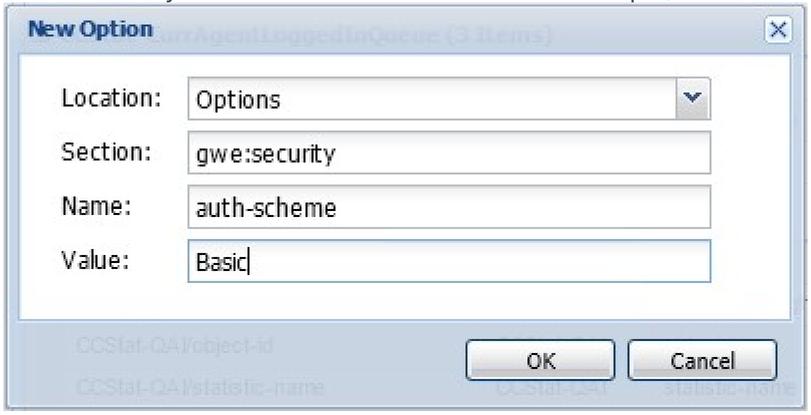
- You completed "Configuring Authentication in the Backend Server".

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`.



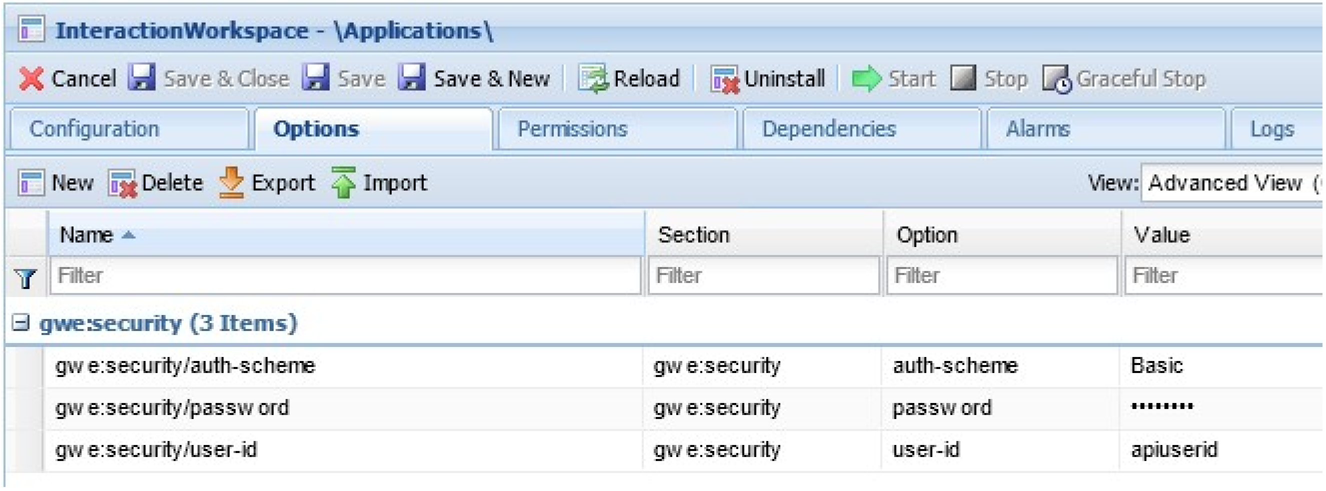
Location: Options
Section: gwe:security
Name: auth-scheme
Value: Basic

   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:



gwe:security (3 Items)

Name	Section	Option	Value
gwe:security/auth-scheme	gwe:security	auth-scheme	Basic
gwe:security/password	gwe:security	password	••••••••
gwe:security/user-id	gwe:security	user-id	apiuserid

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 Backend Server".
- Your SCXML strategy uses the REST API. See Customizing the Engagement Strategy for details.

Start

1. Go to **\apps\*application_name*\_composer-project\WebEngagement_EngagementLogic\src-gen** and open the **default.scxml** file in Composer, a text editor, or an XML editor.
2. Find the variables for **user** and **password** and set your authentication credentials. For example:

   ```
   var user = 'user1';
    var password = 'password1';
   ```

3. Save your changes.

End

Next Steps

- Return to the Genesys Web Engagement Security page.