GENESYS Server and REST API Architecture

Zuken Vitech Inc.
2270 Kraft Drive, Suite 1600
Blacksburg, Virginia 24060
540.951.3322 | FAX: 540.951.8222
Customer Support: support@vitechcorp.com
www.vitechcorp.com

GENESYS™ is a trademark of Zuken Vitech Inc. and refers to all products in the GENESYS software product family.

Other product names mentioned herein are used for identification purposes only, and may be trademarks of their respective companies.

Publication Date: June 2023

TABLE OF CONTENTS

CUSTOMER RESOURCE OPTIONS

Supporting users throughout their entire journey of learning model-based systems engineering (MBSE) is central to Vitech's mission. For users looking for additional resources outside of this document, please refer to the links below. Alternatively, all links may be found at www.vitechcorp.com/online-resources/.

Webinars

Immense, on-demand library of webinar recordings, including systems engineering industry and tool-specific content.

Screencasts

Short videos to guide users through installation and usage of GENESYS.

A Primer for Model-Based Systems Engineering

Our free eBook and our most popular resource for new and experienced practitioners alike.

Help Files

Searchable online access to GENESYS help files.

Technical Papers

Library of technical and white papers for download, authored by Vitech systems engineers.

Technical Support

Frequently Asked Questions (FAQ), support-ticket web form, and information regarding email, phone, and chat support options.

GENESYS SERVER AND REST API ARCHITECTURE

GENESYS Server 2021 R2 and higher ship with a REST API. The REST API enables integrations with any client capable of handling HTTP/HTTPS communications, such as a web browser or other REST APIs. Running the REST service does not depend on external web services. The GENESYS Service contains a built-in web server that exposes the REST API, as shown in the diagram below.
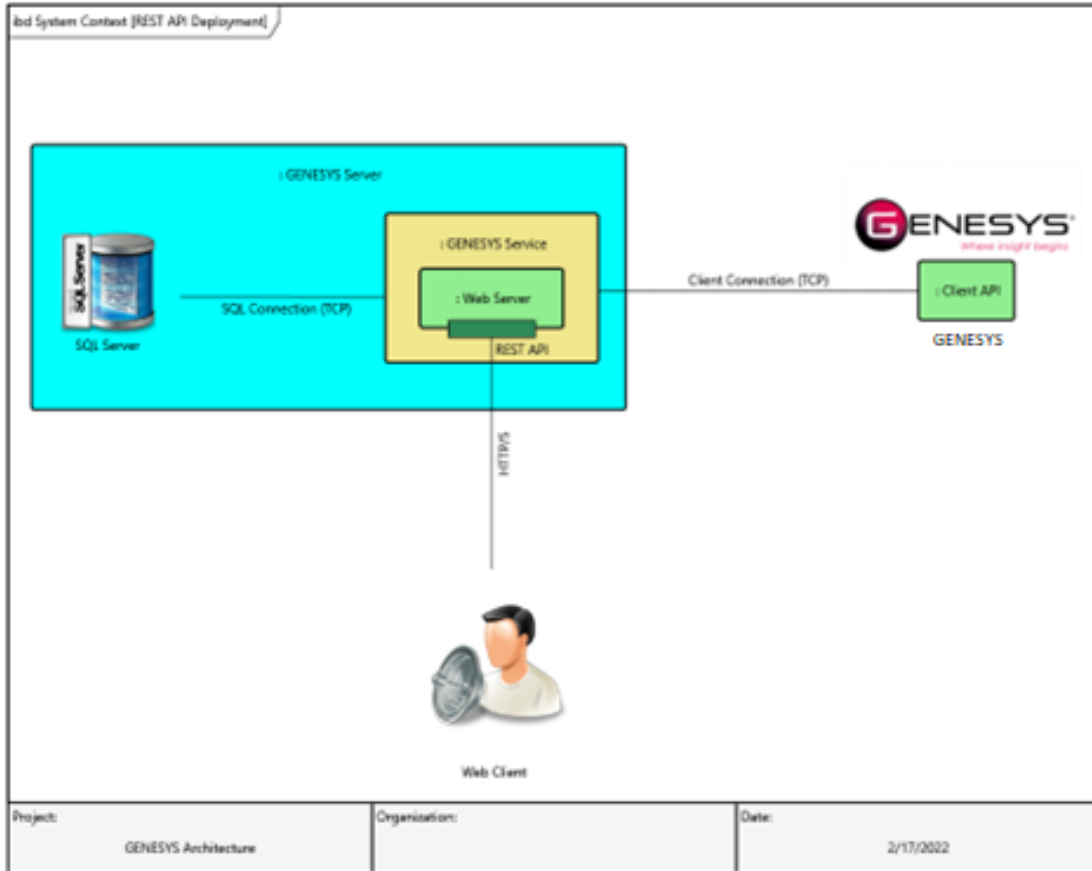
CONFIGURING THE REST API

After installing GENESYS 2021 R2 or higher, launch GENESYS and log in using credentials with administrative privileges.

Click on **Administrative Tools** on the *Home* screen. The following screen with Administrative Tools will display.
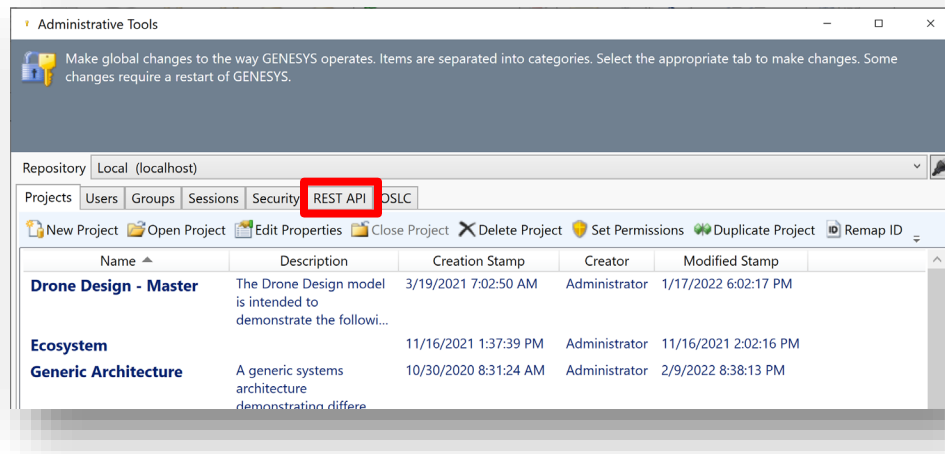
Locate the **REST API** tab and click on it to access the configuration settings. If you do not have a **REST API** tab, your license for GENESYS does not include use of REST services. REST services are supported by GENESYS Server 2021 R2 and higher. The following configuration screen will appear after the **REST API** tab is selected.
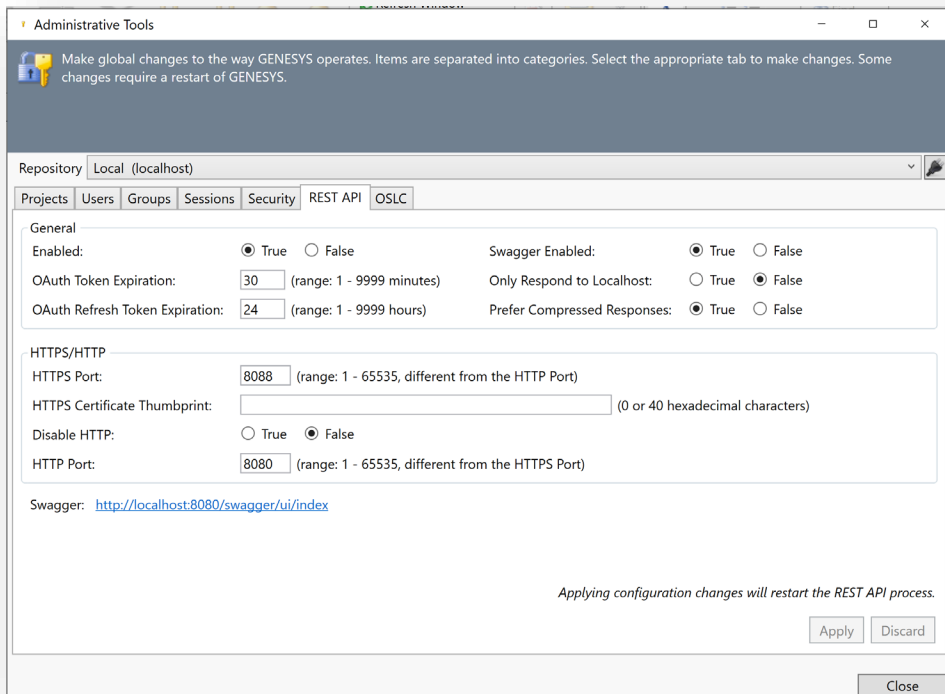
By default, the REST API is disabled. This is by design.

The table below describes all the different configuration options available for the REST API.

Setting	Options (Default shown in bold)	Function
General		
Enabled	True/**False**	Enables the embedded web server and REST service when True
OAuth Token Expiration	**30** (1-9999 minutes)	Sets the lifespan of the OAuth token in minutes
OAuth Refresh Token Expiration	**24** (1-9999 hours)	Sets the lifespan of the OAuth refresh token in hours
Swagger Enabled	**True**/False	If true, REST services will load with Swagger documentation, allowing developers to view and test the different calls in the API
Only Respond to Localhost	True/**False**	When set to True, the web server for the REST API only binds to localhost
Prefer Compressed Responses	**True**/False	Enabling this will result in compressed responses when a request's Accept-Encoding header(s) indicates it accepts **deflate** or **gzip**.
HTTPS/HTTP		
HTTPS Port	**8081** (1-65535)	Sets the port on which the embedded web server binds the HTTPS services
HTTPS Certificate Thumbprint	**Blank**	Enter the hexadecimal characters, without spaces, for the certificate to enable secure communications with the web server
Disable HTTP	True/**False**	Enables/disables REST hosting on HTTP. When false, the embedded web server will respond to both HTTP and HTTPS requests. If true, it will only respond to HTTPS, which is a more secure configuration.
HTTP Port	**8080** (1-65535)	Sets the port on which the embedded web server binds the HTTP services
Swagger		
http://localhost:8080/swagger/ui/index		The generated URL indicates where the built-in Swagger API documentation can be accessed. Clicking on the link will open your browser and load the page.

Turning on the REST Service

To enable the REST service:

1. Open the *REST API* tab in the *Administrative Tools* and set the ENABLED option to True.
2. Click Apply.

The changes will occur as soon as you apply the changes, without the need to restart the GENESYS Service. The act of clicking the Apply button automatically restarts the REST process.
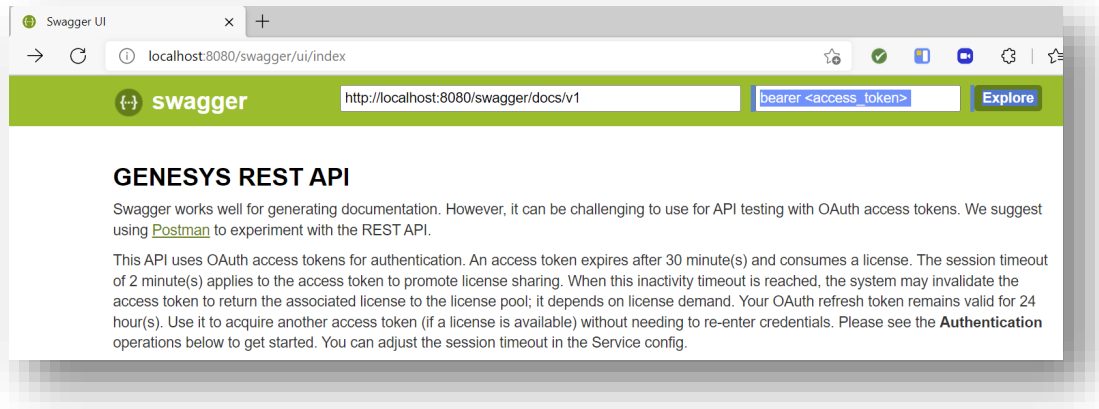
Confirming REST Services are Running

To confirm the service is running:

1. Open the *REST API* tab in the *Administrative Tools*.
2. Click on the Swagger link.

Your browser should launch and open the URL, displaying the following:

If the Swagger screen does not launch, make sure you have done the following:

1. Open the ***REST API*** tab in the ***Administrative Tools*** and set the SWAGGER ENABLED option to True.
2. Click Apply.

Try accessing the Swagger screen again. If it does not load, check the port bindings for HTTP and HTTPS. It is possible the service itself is not binding because the ports are in use by other services.

FIREWALL CONSIDERATIONS

Be sure to engage with your security team to ensure any firewalls along the path between the client and the server hosting REST API are properly configured to allow unfettered access. This includes both network and host-based firewalls. This guide will only address the portions related to the REST API.

To configure your firewalls, follow these basic steps:

1. Determine whether your REST API is configured to run HTTPS only or if it also runs HTTP.
2. Decide which port(s) you wish to expose for external access. HTTPS is more secure, but it also requires deployment of certificates to client machines that will be connecting to the REST API.
3. Add a rule to your firewall(s) that allows inbound traffic on the TCP port you wish to use for external API calls. The source for these IP's can be ANY or could be limited to a range or subnet of allowed IP's. The destination should be the IP of the machine on which the REST API is running.

The table shown here illustrates a sample firewall configuration rule for a GENESYS Server with IP 192.168.1.1. It is up to your team to determine the optimal settings for your organization's intended security posture and to conform to your security policy.

Source	Destination	Protocol	Port	Action
Any	192.168.1.1	TCP	8080	Allow

CONFIGURING AN HTTPS CERTIFICATE

This document will not cover the process of creating a certificate. However, you can reference the link below for instructions on how to generate a self-signed certificate. Note that a self-signed certificate is not recommended for production.

[Create a self-signed public certificate to authenticate your application - Microsoft identity platform | Microsoft Docs](#)

Getting the HTTPS Certificate Thumbprint

Using HTTP leaves the communication between the REST API and its clients unencrypted, allowing potential attackers to intercept your GENESYS data. HTTPS solves this by encrypting communications between the REST API and its clients. Providing GENESYS with a certificate thumbprint tells it which certificate to use with the embedded web server to enable HTTPS. Follow these steps to get the thumbprint:

1. Open the management console for "Computer Certificates" (certlm.msc).
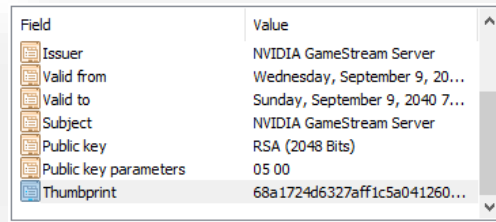2. Expand the **Personal** folder.
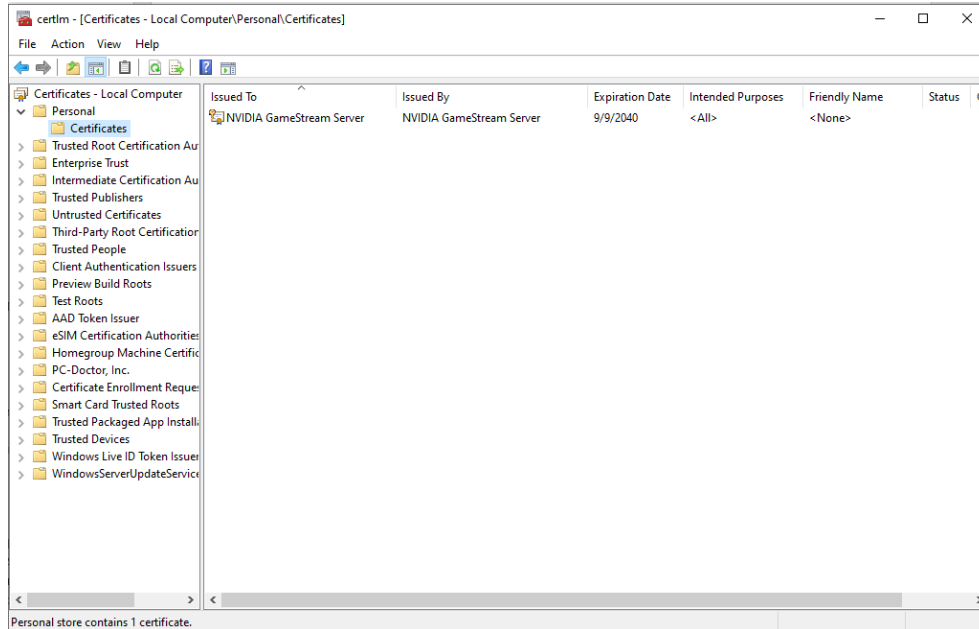
3. Click on Certificates. You will see the list of installed certificates on the right pane.
4. Double-click on the desired certificate to drill-down into the details of the certificate. You will see a window like this:
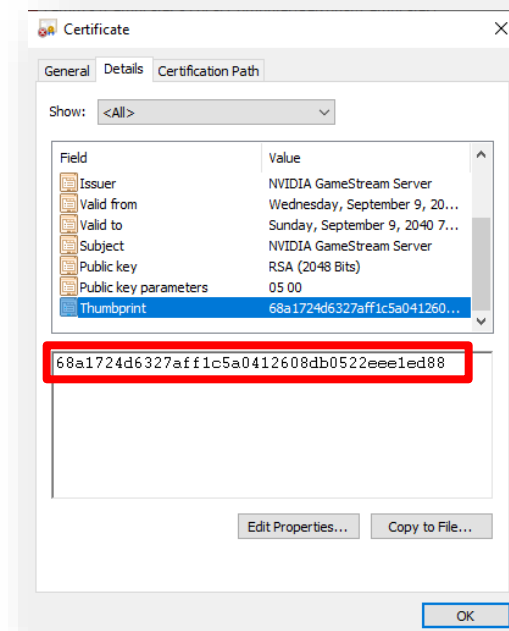
Vitech
A Zuken Company
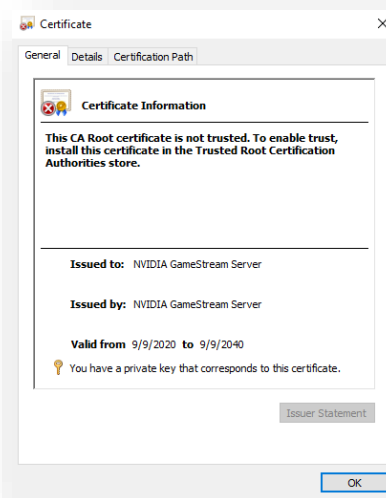
5. Click on the ***Details*** tab and scroll through the list of detailed fields until you see the field called Thumbprint.

6. Click on the Thumbprint field and copy the contents of the Thumbprint details from the content detail box by highlighting the content shown inside the red box and clicking CTRL-C.


7. Go back to the GENESYS interface and open the ***Administrative Tools***. This can be done by clicking on the Administrative Tools link in the initial screen after logging in, as shown in the Configuring the REST API section, or you can also click on ***Utilities*** on the GENESYS ribbon bar and then select Admin Tools, as shown below.

8. Open the ***REST API*** tab in the ***Administrative Tools*** and locate the HTTPS Certificate Thumbprint field.
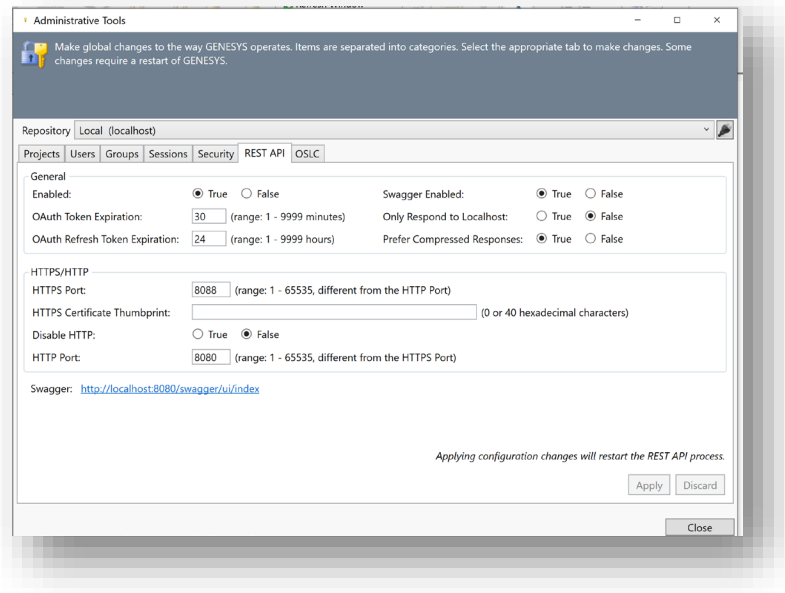
9. Paste the Thumbprint obtained in step 6 in the HTTPS Certificate Thumbprint field and click Apply.

SWAGGER DOCUMENTATION

The built-in Swagger documentation allows your development access to a web-based interface that defines and describes the calls and functions exposed by the REST API. For information on how to use Swagger UI, please visit the Swagger web site at https://www.swagger.io.

REST API CAPABILITIES

The REST API supports CRUD operations for the following data as defined below.

Data	Read	Create	Update	Delete
GENESYS Info Includes version info, current user ID, etc.	Y	N/A	N/A	N/A
Schema Includes reading available baselines for project creation	Y			
Projects	Y	Y	Y	
Project Proxies	Y	N/A	N/A	N/A
Folders Includes reading entities in a folder	Y	Y	Y	Y
Entities Excludes lock/unlock operations	Y	Y	Y	Y
Entity Proxies	Y	N/A	N/A	N/A
Entity Properties w/ inheritance	Y	Y	Y	Y
Entity Audit Logs (Properties sheet in GENESYS)	Y			
Entity Attributes w/ inheritance	Y	Y	Y	Y
Entity Parameters w/ bindings + inheritance Includes resolved values when reading, setting + removal of bindings (w/ cross-project)	Y	Y	Y	Y
Relationships Includes cross-project	Y	Y	Y	Y
Relationship Attributes	Y	Y	Y	Y
Structure	Y	N/A		N/A
Diagram Images • Stored Views (basic info – not all) • Hierarchy Definitions (basic info – not all) • Rule Sets (basic info – not all)				
Filters, Sort Blocks Primarily to sort/filter entity list results via the REST API	Y			
Node Templates				
Versions (Attribute/Parameter)				
Set Permissions				
Commands (E.g., Duplicate Transform, Undo/Redo, etc.)				
Preferences				
Reports				
Scripts				
Users Operations such as reactivate, disable, update password, reset password, and add/remove group are part of update	Y			
Groups Operations such as add/remove user are part of update	Y			

THIS PAGE INTENTIONALLY BLANK

2270 Kraft Drive, Suite 1600
Blacksburg, Virginia 24060
540.951.3322 | FAX: 540.951.8222
Customer Support: support@vitechcorp.com
www.vitechcorp.com