Qualys API Security Connector for Jenkins

User Guide

Version 2.2.0

November 12, 2020

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Preface

Welcome to Qualys Cloud Platform! In this guide, we'll show you how to install and use the Qualys API Security Connector to see your Qualys API Security Connector for Jenkins.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance, and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/

Introduction to Qualys API Security Connector

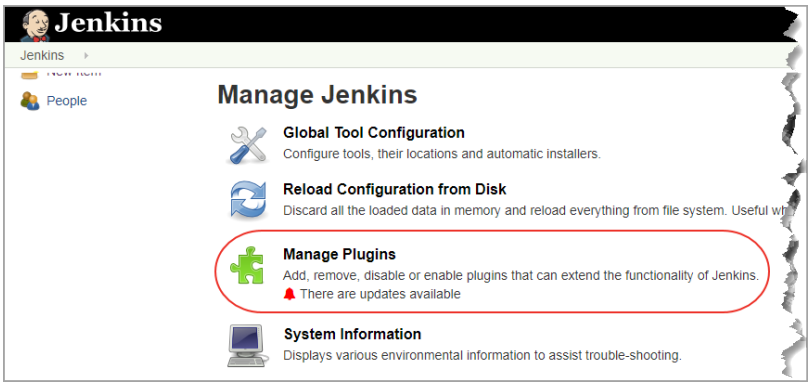
Qualys API Security Connector empowers you to assess API in their existing CI/CD processes with help of the Qualys API Security module. Integrating this assessment step will help you catch and eliminate API related flaws.

We'll help you: Install the Plugin | Configure the Plugin

Install the Plugin

To install Qualys API Security Connector into your Jenkins instance, log into your instance of Jenkins and click Manage Jenkins.

Next, click Manage Plugins.



If you are installing Qualys API Security Connector for the first time, click the Available tab and search for Qualys API Security Connector using the Search bar. Select the plugin and click either Install without restart or Download now and Install after restart.

After Qualys API Security Connector is installed, it will be listed in the Installed tab.

That's it! The installation is now complete. Read on to learn about configuring the plugin.

Good to Know

We support both OpenAPI Specification v2 and v3.

Plugin performs best when API definitions meet these conditions :

- Maximum key length: 256 characters
- Maximum string length: 8192 characters
- Maximum depth for nested objects: 36 levels
- Maximum number of properties in an object or items in an array: 300
- Maximum number limit: float64

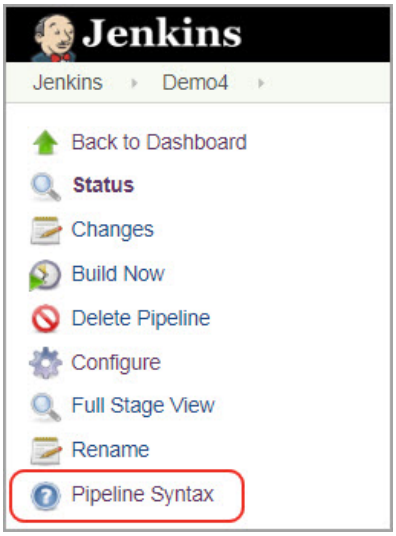
Prerequisite for Configuring the Plugin

You need to generate token from the link provided on the plugin configuration UI. This token will be valid only for 6 months.

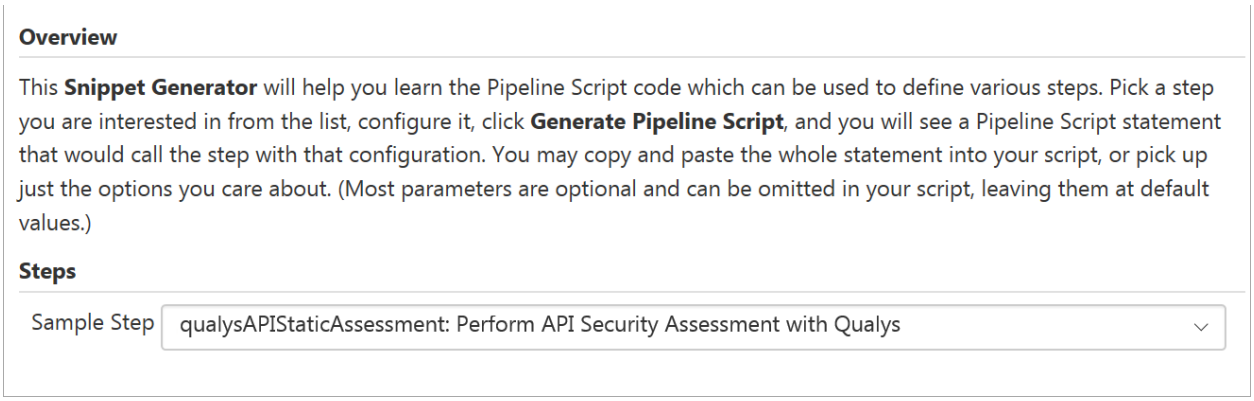
The swagger file that you want to assess should be relative to the Jenkins workspace directory of your application/project. Currently, we support swagger files in the JSON format.

Configure the Plugin for Pipeline projects

Open your application's pipeline project and click "Pipeline Syntax" to enter the Snippet Generator.



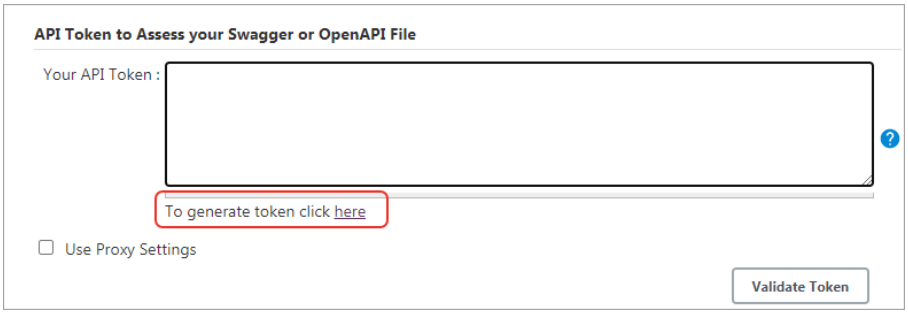
Select "qualysAPIStaticAssessment: Perform API Security Assessment with Qualys" from the drop-down menu.



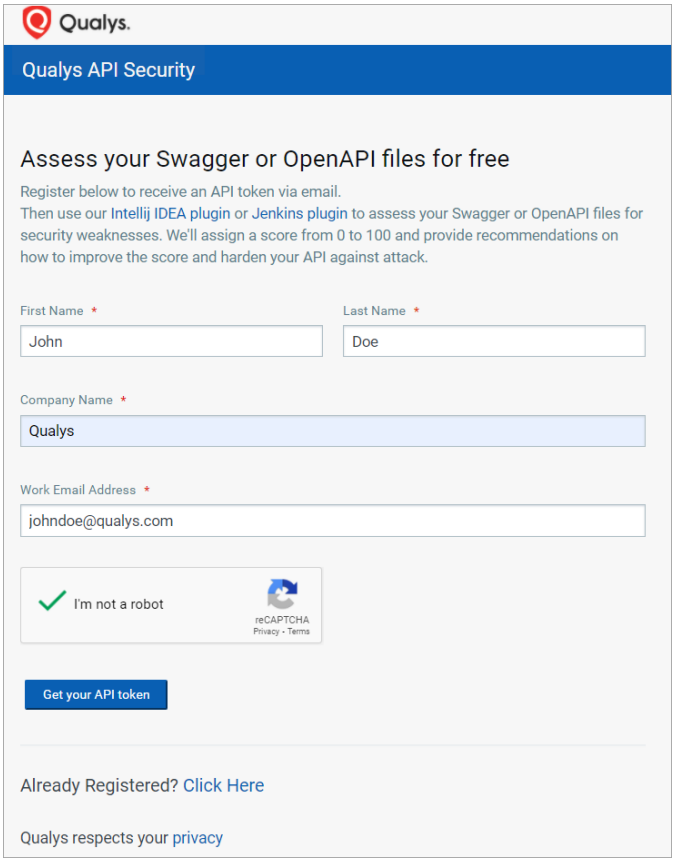
Now you are ready to configure the plugin.

Get API Token

To assess your Swagger or OpenAPI file free, you need to register to receive your token by email. Click the link to generate a token.



When you click the link, we will take you to the registration page. On the registration page, provide your name, company, email address, select CAPTCHA, then click **Get your API token**. You will receive the token in the email. This step is required for configuring both Pipeline and Freestyle projects.



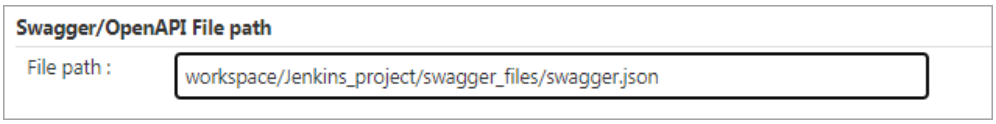
Note that the token will be valid for 6 months and after this duration, you need to request the token again using the link “Click Here” next to Already Registered? text at the bottom.

Next, copy the token from the email, and paste it in the **Your API token** text field. If your Jenkins instance does not have direct Internet access and a proxy is required, click the "Use Proxy Settings" check box, and enter the required information.

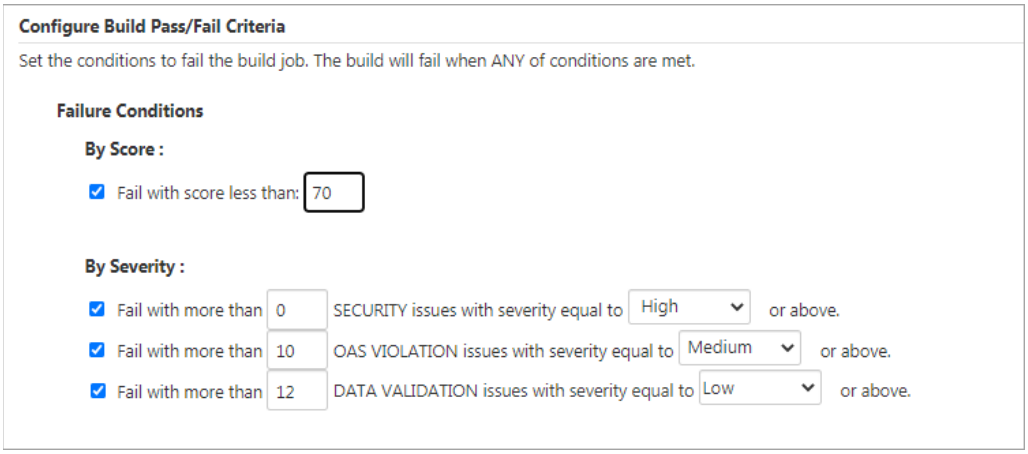
Click **Validate Token**.

Assuming you have provided a valid API token, the "Token Validation Successful" message is displayed.

Provide the swagger file path relative to Jenkins workspace directory of your application/project.



Next, configure the pass/fail criteria based on your API assessment score and severity of the issues in the API. If any of the failure conditions is met, the build will fail.



In the fail by score section, specify a score to fail the build if the API assessment score is less than that specified here.

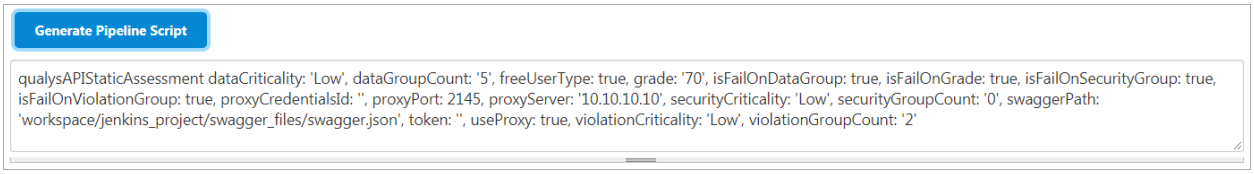
In the fail by severity section, specify the count and severity type as Low, High, or Medium for Security/OAS/Data Validation issues. Note that severities are evaluated from low to high and count is the total of all the issues found for all the evaluated severities.

For example, if you specify 2 in the count and select Low severity then we will evaluate all the issues with severity Low, Medium, and High and if the total of all the issues for these three severities is greater than 2 then we will fail the build.

Similarly, if you select Medium, then we will evaluate all the issues with severity from medium to high. In this case, low severity issues will not be evaluated. If you select High, then only high

severity issues will be evaluated and the total number of high severity issues will be compared with the count.

Next, click "Generate Pipeline Script". This is your pipeline snippet for launching a Static Assessment scan.

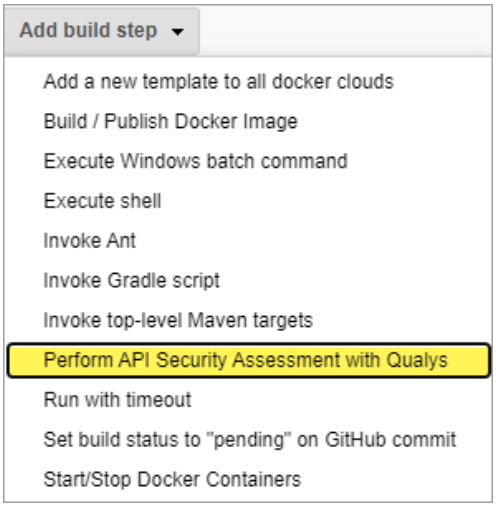


The pipeline snippet is now ready to be plugged into your pipeline script.

Configure the Plugin for Freestyle Projects

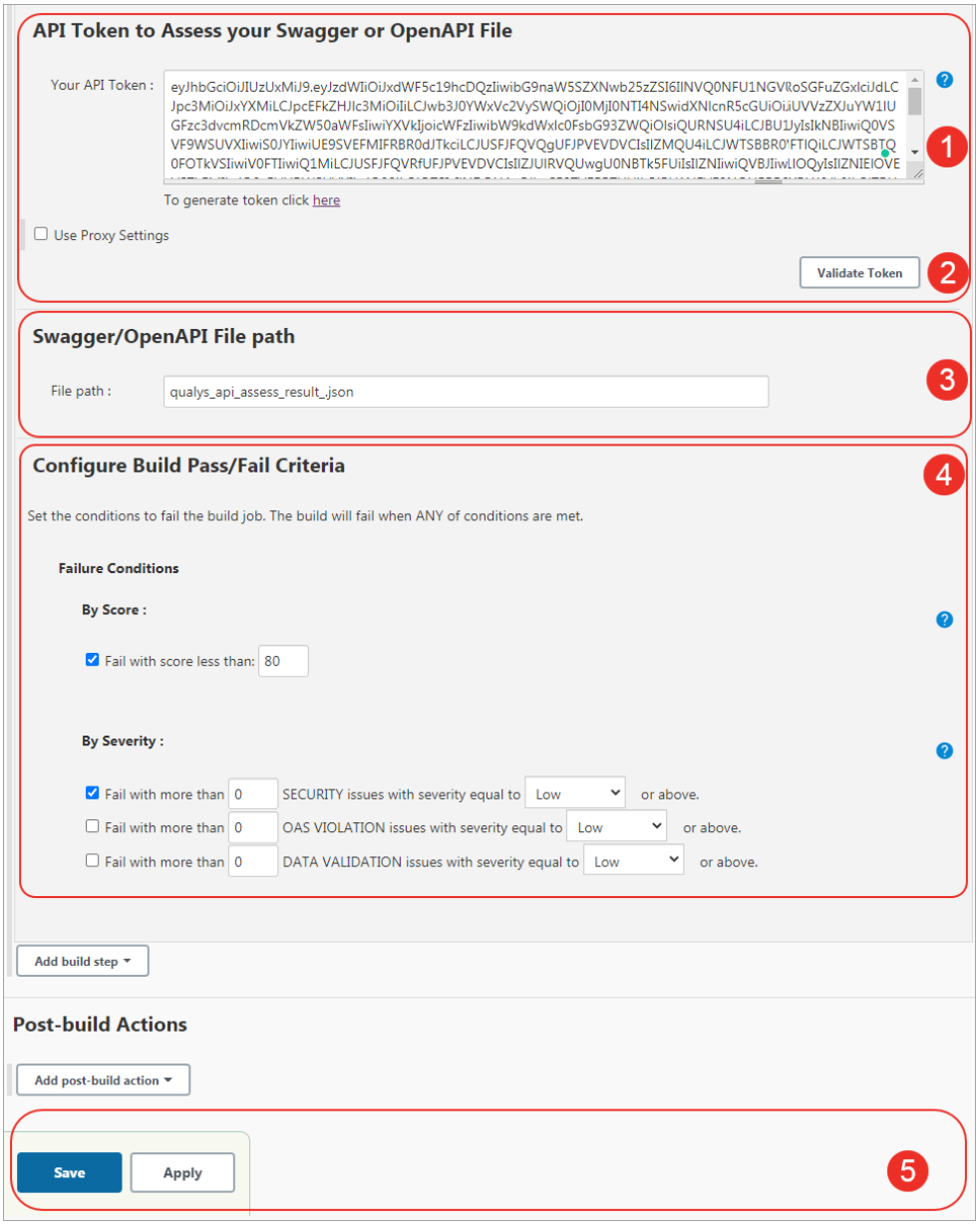
As the configuration settings are the same as Pipeline Project, see “Configure the Plugin Pipeline Project” for detailed configuration.

Navigate to the Build tab and select " Perform API Security Assessment with Qualys " from the Add build step drop-down menu.



Now, configure the steps required to generate the build.

Provide the following configuration details:



1) Click the generate token link to register for a free trial. You will receive a token by email. You need to copy and paste the token in Your API token field.

2) Click Validate Token. The token is validated by Qualys.

3) After the token validation is successful, provide the Swagger file path that should be assessed. The path must be relative to the Jenkins workspace directory path.

4) Configure the pass/fail criteria for a build by score and severity.

6) Finally, click Save.

Qualys API Security Assessment Report

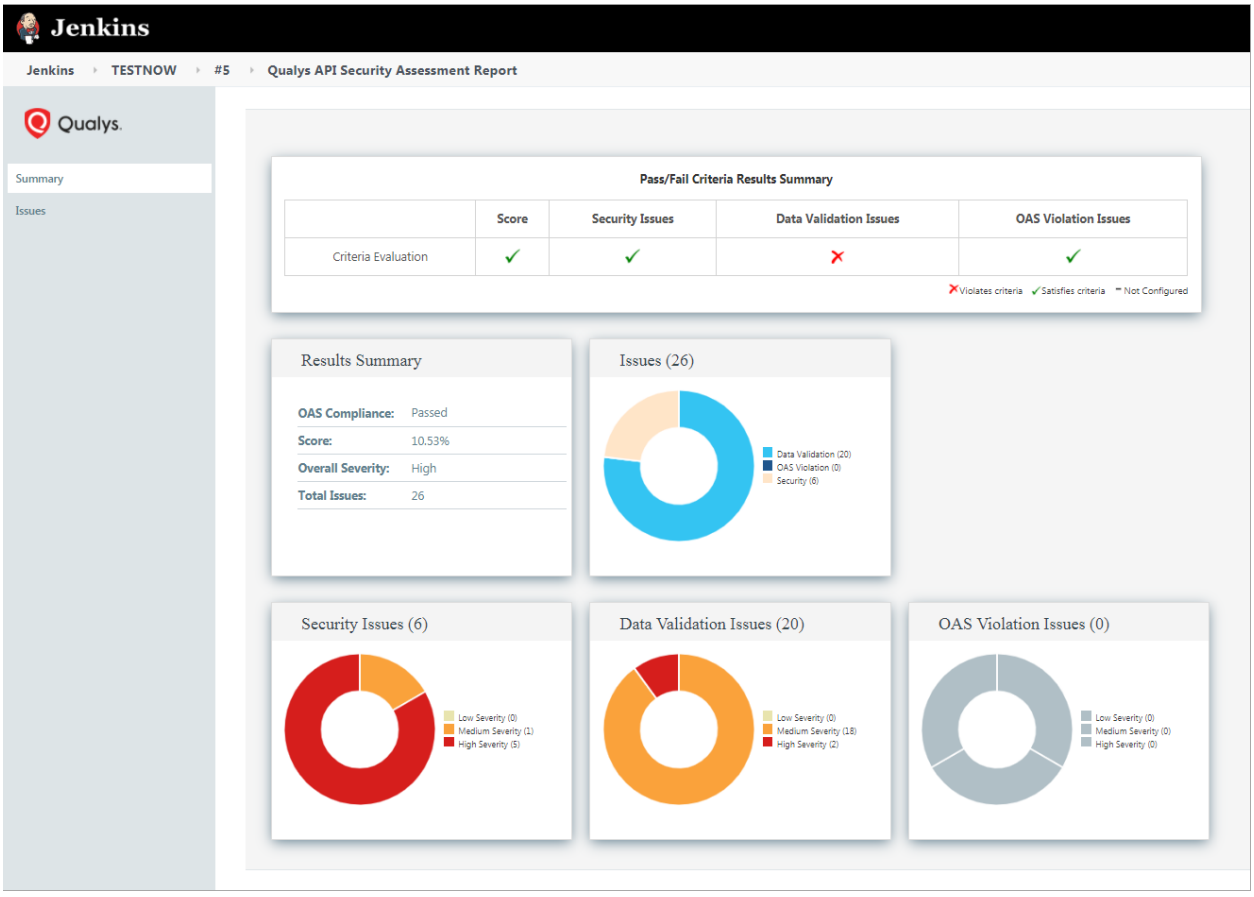
Once the scan is complete, Qualys Static API Security Assessment Report displays various statistics about the assessment.

Summary

The Summary section provides the Pass/Fail Criteria Results Summary telling us if the specified criteria were satisfied or not. The ✗ icon indicates criteria being violated, whereas the ✓ icon indicates criteria being satisfied. Move the mouse over the ✗ and ✓ icons to view the value that you have configured for the criteria, and the actual value obtained after the scan.

The Results Summary shows whether API has passed or failed the OAS compliance test, API assessment score with the total number of issues found, and overall severity of the issues.

The various graphs display information that includes 1) the total number of issues found for each issue type and 2) the break-down of issues by severity for each type of issue: Data Validation, OAS Violation, and Security.



The Issues tab provides the details of the issues including its QID, finding key of the issue and the total number of issues found for the QID. Click the green icon before the QID to view the API path where the issue has occurred, severity of the issue, the impact in percentage on score on fixing the issue, description of the issue and recommendations to fix the issue.