



Qualys Web App Scanning Connector for Jenkins

User Guide

Version 2.0.8

June 14, 2021

Copyright 2018-2021 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

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 Web App Scanning Connector to see your Qualys WAS scan data in 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 Web App Scanning Connector for Jenkins

The Qualys Web App Scanning Connector empowers DevOps teams to build application vulnerability scans into their existing CI/CD processes. By integrating scans in this manner, application security testing is accomplished earlier in the SDLC to catch and eliminate security flaws.

Note - Qualys Web App Scanning Connector supports Jenkins version 2.204.1 or greater.

We'll help you: [Install the Plugin](#) | [Configure the Plugin](#)

Install the Plugin

You can install the Qualys Web App Scanning Connector in two ways. Install the plugin from within Jenkins or download the plugin from Qualys and then install the plugin into your Jenkins instance.

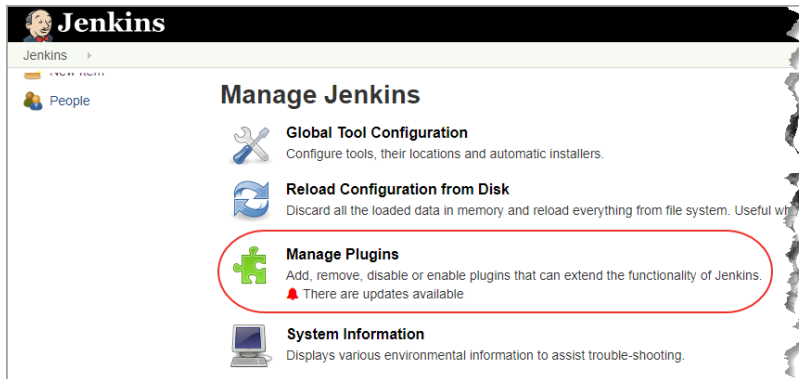
We do not support plugin upgrade from version 2.0.2 to 2.0.3 and above. To install plugin with a version higher than 2.0.2, you need to uninstall the older plugin version and then re-configure their existing jobs post installing WAS plugin.

Install the Plugin from Jenkins

To install the Qualys Web App Scanning Connector from Jenkins, log into your instance of Jenkins and click Manage Jenkins.

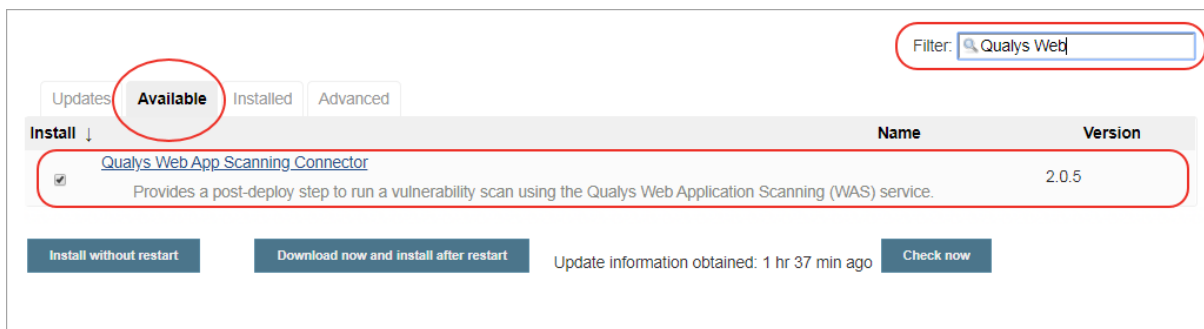


Next, click Manage Plugins.



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

After the Qualys Web App Scanning Connector is installed, it will be listed in the Installed tab.



If the plugin is already installed in Jenkins and you want to update the plugin, go to the Updates tab, search for the Qualys Web App Scanning Connector and click “Download now and Install after restart”.

Note that the plugin is also listed in the plugin store at <https://plugins.jenkins.io/>.

Download and Install the plugin

Optionally, you can download the plugin from Qualys. The plugin comes in the form of a .hpi file. You can find it here at <https://community.qualys.com/docs/DOC-6384>.

Once you have the .hpi file, log into your instance of Jenkins and click Manage Jenkins > Manage Plugins. Go to the "Advanced" tab.

Browse to select the .hpi file you downloaded and click the Upload button. Upload will auto-upgrade your current version of plugin to the installed version.

Upload Plugin

You can upload a .hpi file to install a plugin from outside the central plugin repository.


File: No file chosen

Confirm that the Success message appears. You must restart Jenkins to complete the plugin installation.

Installing Plugins/Upgrades

Preparation

qualys-was  qualys-was plugin is already installed. Jenkins needs to be restarted for the update to take effect

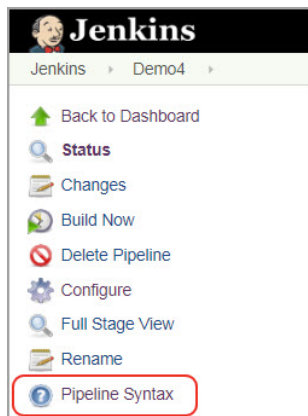
 [Go back to the top page](#)
(you can start using the installed plugins right away)

 Restart Jenkins when installation is complete and no jobs are running

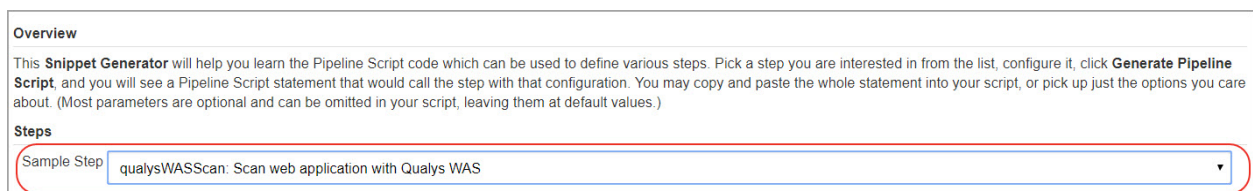
That's it! The installation is now complete. Read on to learn about configuring the plugin.

Configure the Plugin for Pipeline projects

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



Select "qualysWASScan: Scan web applications with Qualys WAS" from the drop-down menu.



Now you are ready to configure the plugin. The first step is to confirm that Jenkins can communicate to the Qualys Cloud Platform via the WAS API. You'll need valid account

credentials for an active Qualys WAS subscription. The account must have API access enabled as well as a role assigned with all necessary permissions. Qualys recommends using a service account restricted to API access only (no UI access) and having the least privileges possible.

Select the Qualys platform/portal where your Qualys account resides and your account credentials for authenticating to the WAS API server. Use the Add button to add account credentials in the Jenkins store for the new user. Once added, the credential is listed in the "Credentials" drop-down.

Note that what you select here depends on the Qualys platform your organization is using. [Learn more](#).

If your Jenkins instance does not have direct Internet access and a proxy is required, click the "Use Proxy Settings" checkbox and enter the required information.

The screenshot shows the 'API Login' form with the following fields: 'Your Qualys Portal' set to 'US Platform 1', 'Credentials' set to 'tamde qw/*****', and 'Use Proxy Settings' unchecked. A 'Test Connection' button is at the bottom right.

Click the "Test Connection" button. Assuming you have selected the correct platform for your subscription and the credentials are valid, you will see the message "Connection test successful!".

Note that if your Qualys account resides on a private cloud platform, select "Private Cloud Platform" as your Qualys cloud platform, specify the API server URL and your account credentials to access the API.

The screenshot shows the 'API Login' form with the following fields: 'Your Qualys Portal' set to 'Private Cloud Platform', 'API Server URL' set to 'https://qualysapi.mycloud.com', and 'Credentials' set to 'quavs ct51/***** (CS test ac on POD01)'. The 'Use Proxy Settings' checkbox is unchecked, and a 'Test Connection' button is at the bottom right.

Next, select the web application in Qualys WAS that you wish to scan.

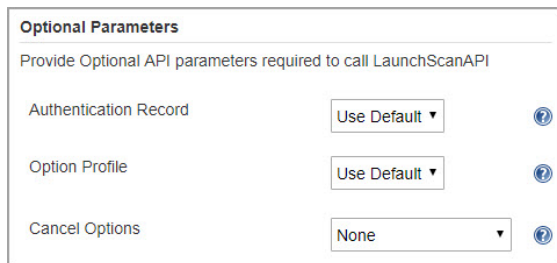
The screenshot shows the 'Launch Scan API Parameters' form with the following fields: 'Select Web Application from WAS' set to 'Qualys - QA Lab - Demo 6', 'Scan Name' set to '[job_name]_jenkins_build_[build_number]', and 'Scan Type' set to 'VULNERABILITY'.

By default, the WAS scan name will be:
[job_name]_jenkins_build_[build_number] + timestamp

You can edit the scan name, but a timestamp will automatically be appended regardless.

You can choose to run a Discovery scan or Vulnerability scan. The default is Vulnerability scan.

Next, configure optional scan parameters.



Optional Parameters		
Provide Optional API parameters required to call LaunchScanAPI		
Authentication Record	Use Default ▾	?
Option Profile	Use Default ▾	?
Cancel Options	None ▾	?

Authentication Record – You can choose to run the scan without authentication (the default) but keep in mind the scanner will not be able to log into the web application and test the authenticated surface area of the application in that case. You may instead want to select "Use Default", in which case the default authentication record for the web app in WAS (if any) will be used. Optionally, you can also select the Other option and choose a specific authentication record ID if desired.

Option Profile – The option profile contains the various scan settings such as the vulnerability types that should be tested (detection scope), scan intensity, error thresholds, etc. Selecting "Use Default" will use the default option profile for the web app in WAS. This is the recommended setting; however, you can also select the Other option and choose a specific option profile ID if desired.

Cancel Options – The default is not to cancel the scan, in which case the scan will run to completion. However, you can choose to the cancel the scan after a set number of hours. Keep in mind you may not get any results if the scan is canceled before finishing. Next, configure the pass/fail criteria for a build, scan status polling frequency and timeout duration for the scan.

Next configure the scan pass/fail criteria to fail a build job.

Configure Scan Pass/Fail Criteria

Set the conditions to fail the build job. The build will fail when ANY of conditions are met.

Failure Conditions

By Vulnerability Severity

- Fail with more than severity 1
- Fail with more than severity 2
- Fail with more than severity 3
- Fail with more than severity 4
- Fail with more than severity 5

By Qualys WAS Vulnerability Identifiers (QIDs)

- Fail with any of these QIDs:
- Fail the build if WAS could not scan the web application

Timeout Settings

Qualys WAS Scan results will be collected per these settings. For each enter a value in minutes or an expression like 2*60 for 2 hours.

Frequency

How often to check for data minutes.

Timeout

How long to wait for scan results minutes.

You can set conditions to fail a build by 1) Vulnerability Severity, 2) Qualys WAS Vulnerability Identifiers (QIDs). You may also choose to fail the build in case the Plugin initiates the scan but WAS module could not complete this scan due to some issues such as scanners not found and so on. If any of these conditions are satisfied, then build is failed.

To fail the build by vulnerability severity, specify the count of vulnerabilities for one or more severity types. A build will fail if in scan results the number of detections exceeds the number specified for one or more severity types. For example, to fail a build if severity 5 vulnerabilities count is more than 2, select the “Fail with more than severity 5” option and specify 2.

Note that a Qualys severity “5” rating is the most dangerous vulnerability while severity “1” is the least.

Similarly, to fail a build by QIDs, select “Fail with any of these QIDs” check box and specify one or more QIDs in Fail with any of these QIDs.

In the Timeout settings, specify the polling frequency in minutes for collecting the WAS scan status data and the timeout duration for a running scan.

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

Generate Pipeline Script

```
qualysWASScan authRecord: 'useDefault', cancelOptions: 'none', credsId: '4a84332f-d6f8-472b-96b9-61b0d81e039f', optionProfile: 'useDefault', platform: 'US_PLATFORM_1', pollingInterval: '5', proxyPassword: '2d2822980dc64922b3e19a79a12ec46f', proxyPort: 3128, proxyServer: '10.115.27.54', proxyUsername: 'admin', scanName: '[job_name]_jenkins_build_[build_number]', scanType: 'VULNERABILITY', useProxy: true, vulnsTimeout: '60*24', webAppId: '21325'
```

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

Configure the Plugin for Freestyle Projects

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

Provide the following configuration details:

- 1) Provide your login account credentials to access the Qualys WAS API server on the Qualys cloud platform. Select **Use Proxy Settings** to provide proxy information if your Jenkins server is behind a firewall.
- 2) Click **Test Connection** to verify that the plugin can connect to the Qualys WAS API server.
- 3) Provide parameters: web application name, scan name and scan type required to call the launch scan API.
- 4) Optional parameters that you can pass to launch scan API.
- 5) Build fail conditions by vulnerabilities detected for severity types and by QIDs. Provide data collection frequency and timeout duration for the running scan. Finally, click **Save**.

API Login

Provide details for accessing the Qualys WAS API

Your Qualys Portal: CANADA Platform

Credentials: qualysgg1/***** (CanadaPod)

Use Proxy Settings

Test Connection

Launch Scan API Parameters

Provide information required to launch the scan

Select Web Application from WAS: web app 1

Scan Name: [job_name]_jenkins_build_[build_number]

Scan Type: VULNERABILITY

Optional Parameters

Provide Optional API parameters required to call LaunchScanAPI

Authentication Record: Use Default

Option Profile: Other

Profile Name: Initial WAS Options

Cancel Options: None

Configure Scan Pass/Fail Criteria

Set the conditions to fail the build job. The build will fail when ANY of conditions are met.

Failure Conditions

By Vulnerability Severity

Fail with more than 4 severity 1 (NOTE: Severity 1 rating is least severe and severity 5 is most severe)

Fail with more than 0 severity 2

Fail with more than 0 severity 3

Fail with more than 0 severity 4

Fail with more than 0 severity 5

By Qualys WAS Vulnerability Identifiers (QIDs)

Fail with any of these QIDs: 150004

Fail the build if WAS could not scan the web application

Timeout Settings

Qualys WAS Scan results will be collected per these settings. For each enter a value in minutes or an expression like 2*60 for 2 hours.

Frequency

How often to check for data: 5 minutes

Timeout

How long to wait for scan results: 60 minutes

Add post-build action

Save Apply

Qualys WAS Scan Status

After the scan completes, the Summary tab will show two sections: Vulnerabilities and Pass/Fail Criteria Results Summary. Summary section shows graphical data for the number of vulnerabilities by severity types for the Web application. Pass/Fail Criteria Results Summary shows the pass/fail criteria and whether they are violated or satisfied. When the criteria are violated, the **✗** icon is shown while for satisfied criteria, the **✓** icon is shown.

Click the link shown in the Scan Report field to view the detailed WAS scan report on the Qualys portal.

The screenshot shows the Jenkins interface for a Qualys WAS scan. The page is titled "WAS_Freestyle #1 Qualys WAS Scan Status". It displays the following information:

- Scan ID:** 23701005
- Scan Name:** WAS_Freestyle_jenkins_build_1_2021-05-19-17-49
- Scan Status:** FINISHED
- Scan Reference:** was/1621408450813.31858480
- Target URL:** http://www.gmail.com/

The "Results Summary" section shows:

- Results Status: SUCCESSFUL
- Auth Status: Not Used
- Number of Requests: 444
- Links Crawled: 1
- Total Duration: 16 min 9 s

The "Results Stats" section shows:

- Vulnerabilities: 5
- Information Gathered: 15
- Sensitive Contents: 0

The "Vulnerabilities (5)" section features a donut chart showing the distribution of vulnerabilities by severity level (Sev 1-5).

The "Pass/Fail Criteria Results Summary" table is as follows:

	QIDs	Severity 5	Severity 4	Severity 3	Severity 2	Severity 1
Criteria Evaluation	✗	✓	✓	✗	✗	✗

Legend: ✗ Violates criteria, ✓ Satisfies criteria, * Not Configured

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.

This screenshot is identical to the previous one, but with a tooltip visible over the "QIDs" cell in the "Pass/Fail Criteria Results Summary" table. The tooltip displays:

- configured:** 150001,150124,150179, 150181
- Found:** 150124

The Vulnerabilities tab is available to provide you the details of vulnerabilities, such as QIDs, vulnerability titles, severity (All, (1-5)) URLs where the vulnerabilities occur and authentication status.

At the top, on the right side, the **Severity** filter lets you find vulnerabilities by their severity. Select **Breaking Vulnerabilities** check box to list the vulnerabilities because of which the build has failed. Breaking Vulnerabilities are those vulnerabilities that match the failure conditions that you have configured and because of which the build got failed.

The screenshot shows the Jenkins interface for a Qualys WAS Scan. The page title is "QUALYS VULNERABILITIES RESULTS". It includes a search bar, a breadcrumb trail, and a sidebar with "Summary" and "Vulnerabilities" tabs. The main content area shows a table of vulnerabilities with columns for QID, Title, Severity, URL, and Available Unauthenticated?.

QID	Title	Severity	URL	Available Unauthenticated?
150004	Path-Based Vulnerability	2	http://zero.webappsecurity.com/README.txt	Yes
150004	Path-Based Vulnerability	2	http://zero.webappsecurity.com/docs/	Yes
150004	Path-Based Vulnerability	2	http://zero.webappsecurity.com/errors/	Yes
150004	Path-Based Vulnerability	2	http://zero.webappsecurity.com/index.html.old	Yes
150004	Path-Based Vulnerability	2	http://zero.webappsecurity.com/admin/	Yes
150023	Directory Listing	2	http://zero.webappsecurity.com/errors/	Yes
150053	Login Form Is Not Submitted Via HTTPS	4	http://zero.webappsecurity.com/signin.html	Yes
150081	X-Frame-Options header is not set	1	http://zero.webappsecurity.com/forgot-password.html	Yes
150081	X-Frame-Options header is not set	1	http://zero.webappsecurity.com/index.html	Yes
150081	X-Frame-Options header is not set	1	http://zero.webappsecurity.com/	Yes

Showing 1 to 10 of 24 entries

Previous 1 2 3 Next

✘ Denotes the "Breaking Vulnerabilities" as per the configured fail criteria

Troubleshooting

You entered valid Qualys credentials, but the drop-down menu to select a Web application is empty or does not show the desired Web application.

This issue occurs when the Qualys account provided does not have proper role or scope to access the web application you wish to scan. Ensure that the account has been set up with the required roles and scope to access the desired Web application.

You entered valid Qualys credentials, but the drop-down menu for Authentication Record Name or Profile Name is empty or does not show the desired item.

This issue occurs when the Qualys account provided does not have proper role or scope to access the auth record or option profile you wish to use. Ensure that the account has been set up with the required roles and scope to access the desired authentication record or option profile.

URL to the Qualys API Server

The Qualys API URL you should use for API requests depends on the Qualys platform where your account is located.

Click [here](#) to identify your Qualys platform and get the API URL.

What's New

Improvements in 2.0.7

With this release, we will use the upgraded third-party library for rendering graphical charts that are used for displaying WAS scan results in the Jenkins scan report section.

Improvements in 2.0.8

- With this release, we have added 2 new filters: Severity and Breaking Vulnerabilities in the Vulnerabilities tab on the "Qualys Vulnerabilities Results" screen. The Severity filter lets you find vulnerabilities by their severity. Select Breaking Vulnerabilities check box to list the vulnerabilities because of which the build has failed.
- We have added a new column Severity in the table in the in the Vulnerabilities tab on the "Qualys Vulnerabilities Results" screen to show the severity information of the vulnerability.