Qualys Web App Scanning Connector for Azure DevOps

User Guide

Version 1.0.0

October 23, 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 Web App Scanning Connector to see your Qualys WAS scan data in Azure DevOps.

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/

About Web Application Scanning Documentation

This document provides information about using the Qualys Web App Scanning Connector for Azure DevOps.

For information on using the Web Application Scanning UI to monitor vulnerabilities in web applications, refer to the Qualys Web Application Scanning User Guide.

For information on using the Web Application Scanning API, refer to the Web Application Scanning API User Guide.

Introduction to Qualys Web App Scanning Connector for Azure DevOps

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. The plugin can be configured to fail or pass the builds based on the vulnerabilities detected.

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

Install the Plugin from Azure DevOps marketplace

You can install the Qualys Web App Scanning Connector for Azure DevOps from Azure DevOps marketplace.

Install the Plugin

1) To install the plugin from the Azure DevOps marketplace, log in to your Azure DevOps instance.

2) Click the  icon on the top pane at the right side of the page and choose **Browse marketplace**. A new browser will open to show you the plugins/extensions for Azure DevOps.

3) In the search bar, enter Qualys to search for all the Qualys plugins.

4) Click the Qualys Web App Scanning Connector plugin in the plugin list.

5) Click **Get it free**. You will be navigated to the Visual Studio Marketplace screen.

6) Select the organization and click **Install** to install the plugin in your Azure DevOps instance. You can see the installed plugin in the **Installed** tab when you navigate to **Organization Settings** > **Extension**.

The Qualys Web App Scanning Connector gets installed/updated in your Azure DevOps instance. In case of an update, your existing configuration will continue to work. In case of a fresh install, you perform the configuration steps provided further in this document.

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

Prerequisites for configuring the plugin

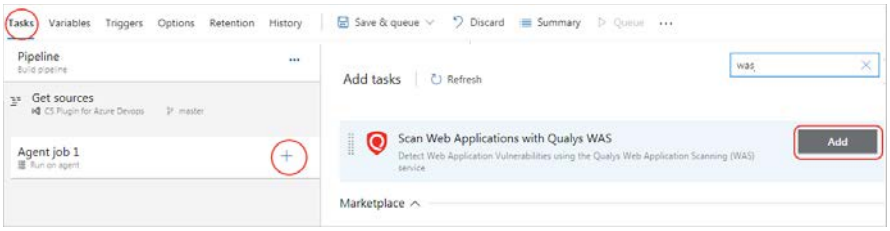
1. The current version of the Web App Scanning Connector supports only Azure DevOps Services. You can use self-hosted agents or Microsoft agents.

2. You must have a 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.

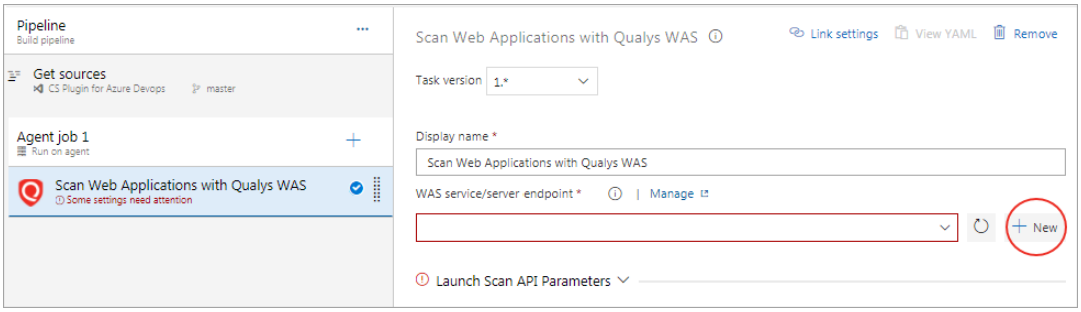
3. You need the web application, option profile and authentication record preconfigured in your Qualys WAS account for the plugin to populate them in the respective fields on the configuration form.

Configure the Plugin for Pipeline projects

You can use this Qualys Web App Scanning Connector extension as a pre-deployment task in your project pipeline. After installing the Qualys Web App Scanning Connector, you see this plugin as a task in your pipeline. In the **Tasks** tab, click **Add** Task under your agent job, and search for the plugin the "**Scan Web Application with Qualys WAS**" task. Select the task and click **Add** to add it as a task. You will see the task under the agent.



The first step after entering the display name is to configure the WAS service end point. To connect to the WAS APIs, you need to configure the service endpoint with Qualys account and proxy (if needed) on your Azure DevOps instance for Organization in which Qualys Web App Scanning Connector is installed. Go to the **WAS service/server endpoint** field and click **New**.

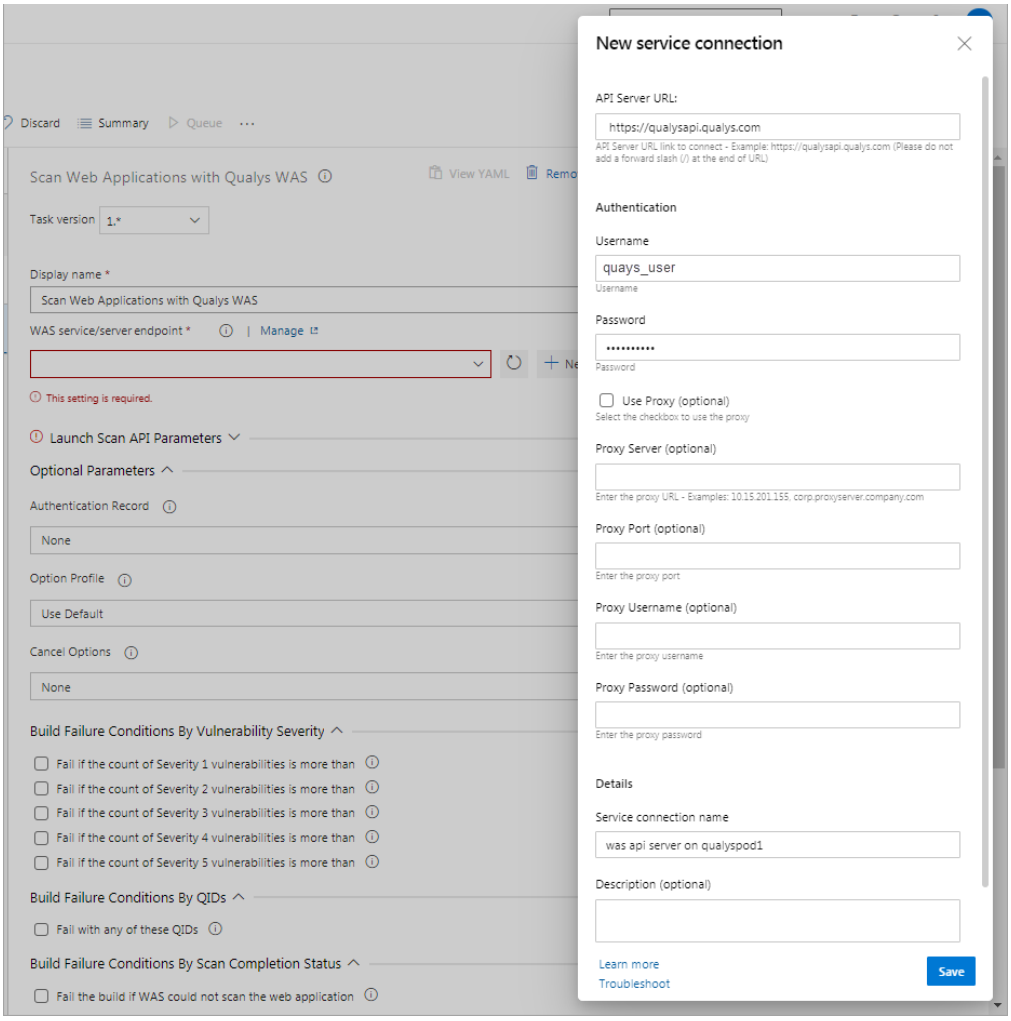


Enter the Qualys API server URL where your Qualys WAS account resides and your account credentials for authenticating to the WAS API server. Provide a name to the new service connection and click **Save**. Once added, the WAS service endpoint is listed in the "WAS service/server endpoint" drop-down field.

Note that what you select here depends on the Qualys platform your organization is using. Learn more. We expect the user to provide "qualysapi" specific URL for their respective platform as an input for "API Server URL".

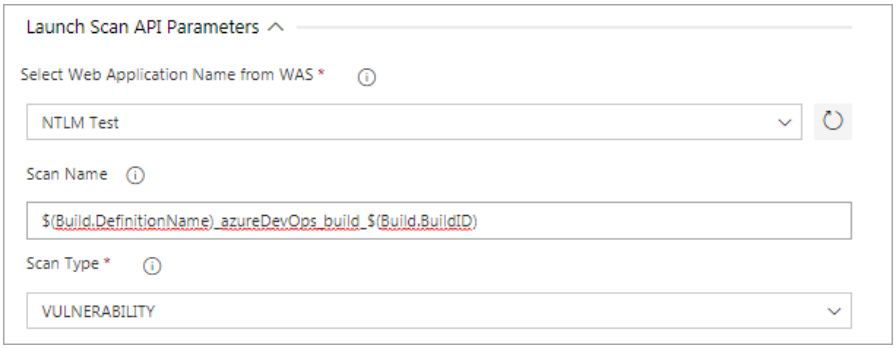
If your Azure DevOps instance does not have direct Internet access and a proxy is required, click the "Use Proxy Settings" check box, and enter the required information.

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



Launch Scan API Parameters

Next, assuming you have selected the correct platform for your subscription and the credentials are valid, we will fetch all the web applications from your Qualys account. Select the web application that you want to scan.



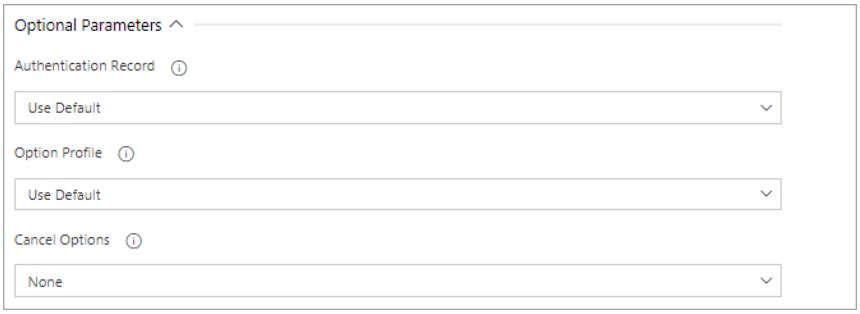
By default, the WAS scan name will be:
`[Build.DefinitionName]_azureDevOps_build_[Build.BuildID] + timestamp`

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 the Vulnerability scan.

Optional Parameters

Next, configure optional scan parameters.



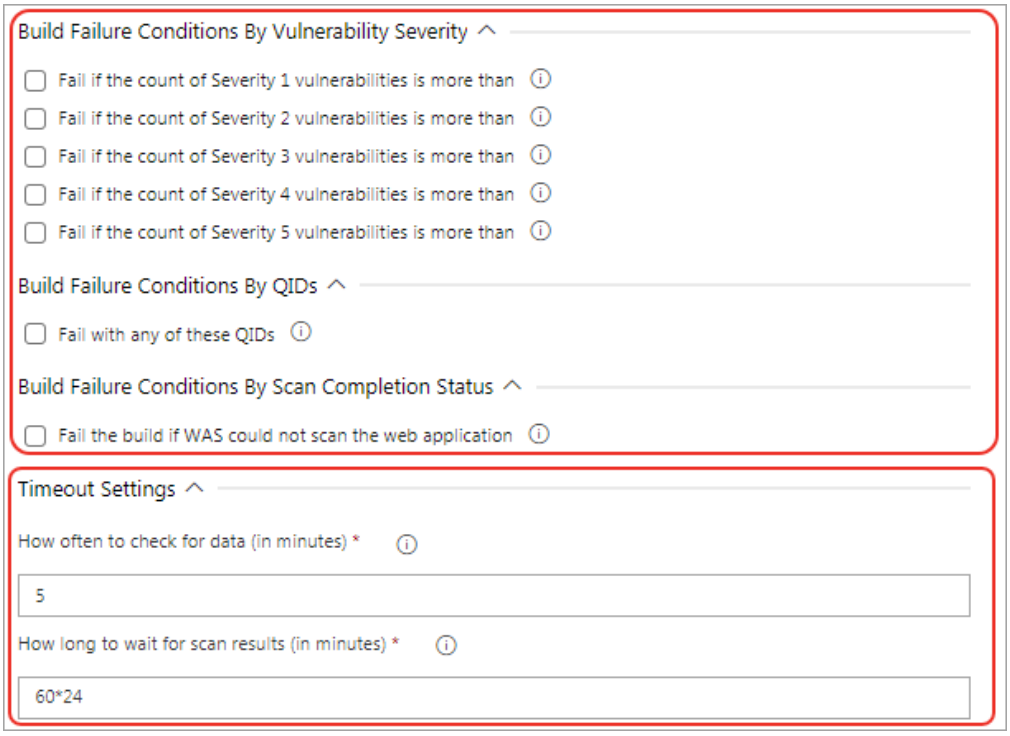
Authentication Record – You can choose to run the scan without authentication (the default) but keep in mind the scanner will not be able to log into the web application and test the authenticated surface area of the application in that case. You may instead want to select "Use Default", in which case 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 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.

Build Failure Conditions

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



You can set conditions to fail a build by:

1. Vulnerability Severity - 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 the 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.

2. Qualys WAS Vulnerability Identifiers (QIDs) – To fail a build by QIDs, select the "Fail with any of these QIDs" check box and specify a comma-separated list of QIDs or range of QIDs.

3. You may also choose to fail the build in case the plugin initiates the scan but the WAS module could not complete this scan due to some issues such as scanners not found and so on. If any of these three conditions are satisfied, then build is failed.

Timeout Settings

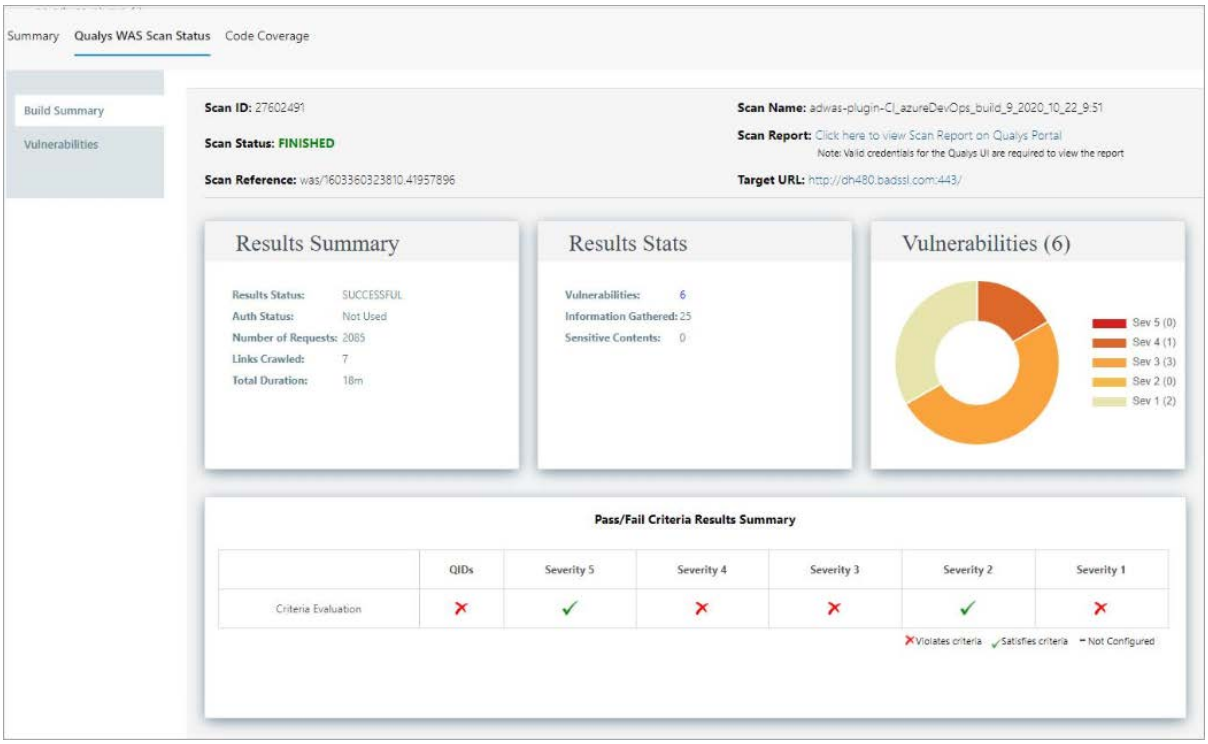
In the Timeout settings, specify the polling frequency in minutes for collecting the WAS scan status data and the timeout duration for a running scan.

Next, save the configuration and click **Queue** to run the pipeline.

Qualys WAS Scan Status

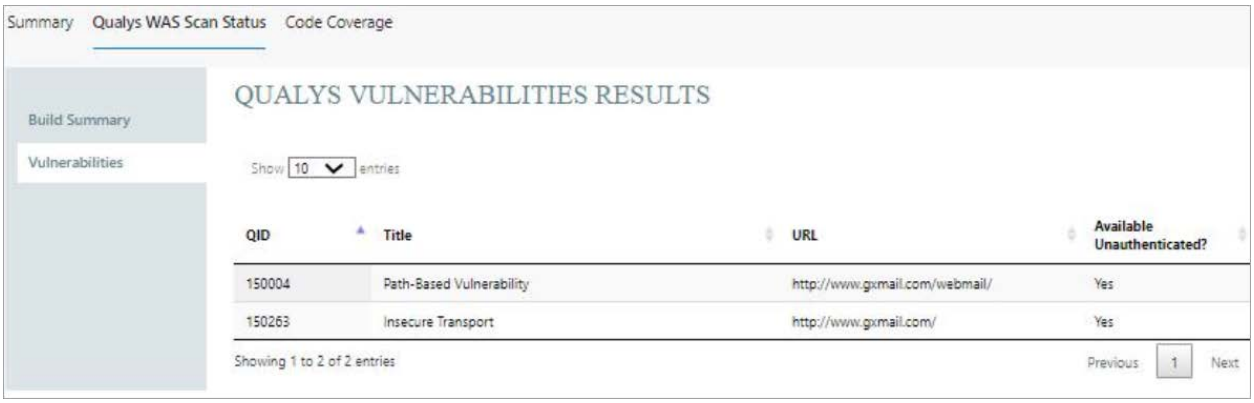
After the scan completes, the Summary tab will show two sections: Vulnerabilities and Pass/Fail Criteria Results Summary. The Summary section shows graphical data of the number of vulnerabilities by severity types for the Web application. Pass/Fail Criteria Results Summary shows the pass/fail criteria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



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 Vulnerabilities tab is available to provide you the details of vulnerabilities, such as QIDs, vulnerability titles, URLs where the vulnerabilities occur, and authentication status.



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 a 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 a 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.