



Qualys Web App Scanning Connector for Azure DevOps

User Guide

Version 1.1.1

October 6, 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 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](#) | [Upgrade 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**.

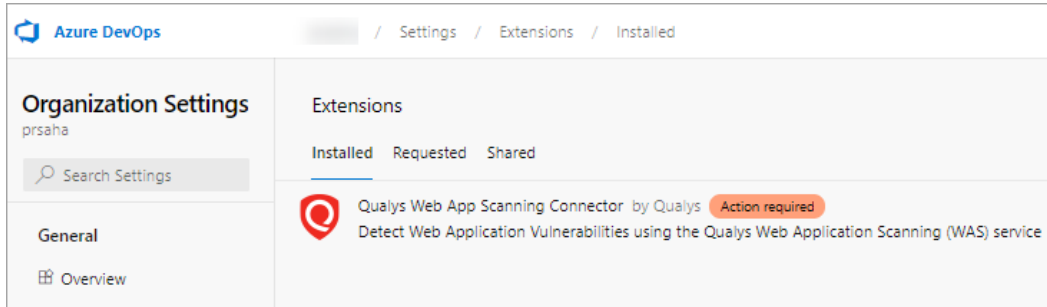
The Qualys Web App Scanning Connector gets installed/updated in your Azure DevOps instance. In case of an update, your existing configuration will continue to work. In case of a fresh install, you perform the configuration steps provided further in this document.

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

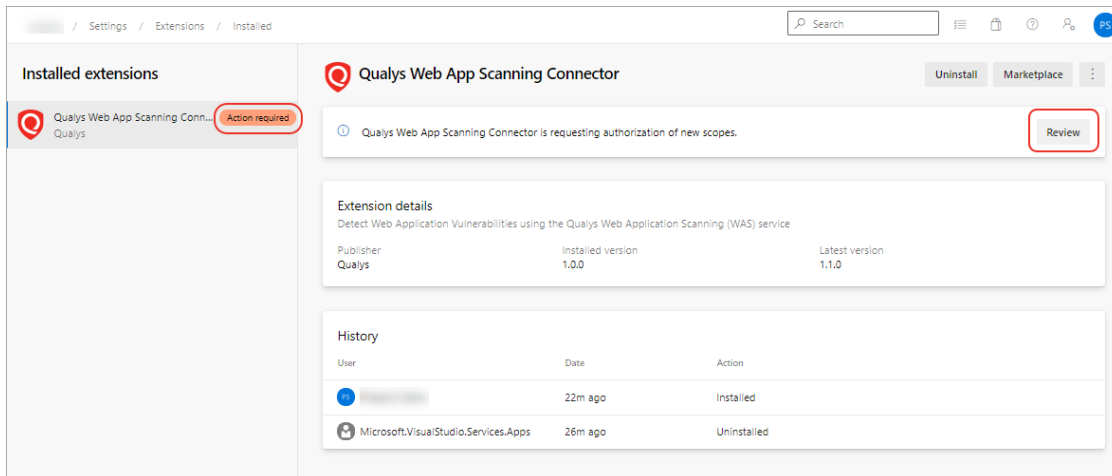
Upgrade the Plugin

If you have already installed the plugin, then follow these steps to upgrade the plugin:

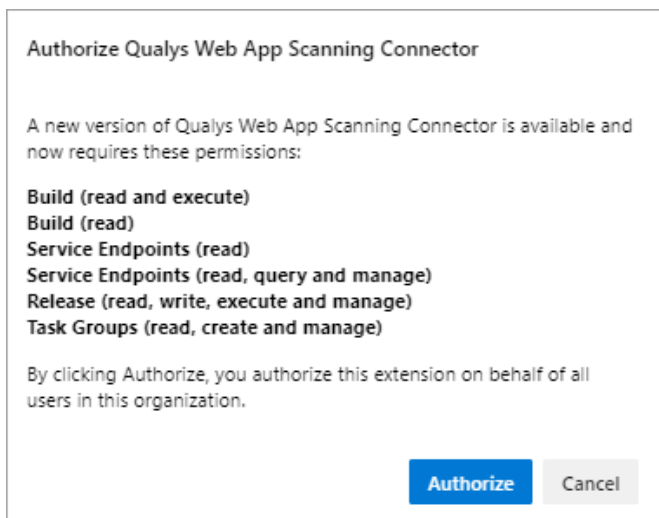
1. Go to **Organizational Settings > Extensions > Installed**.



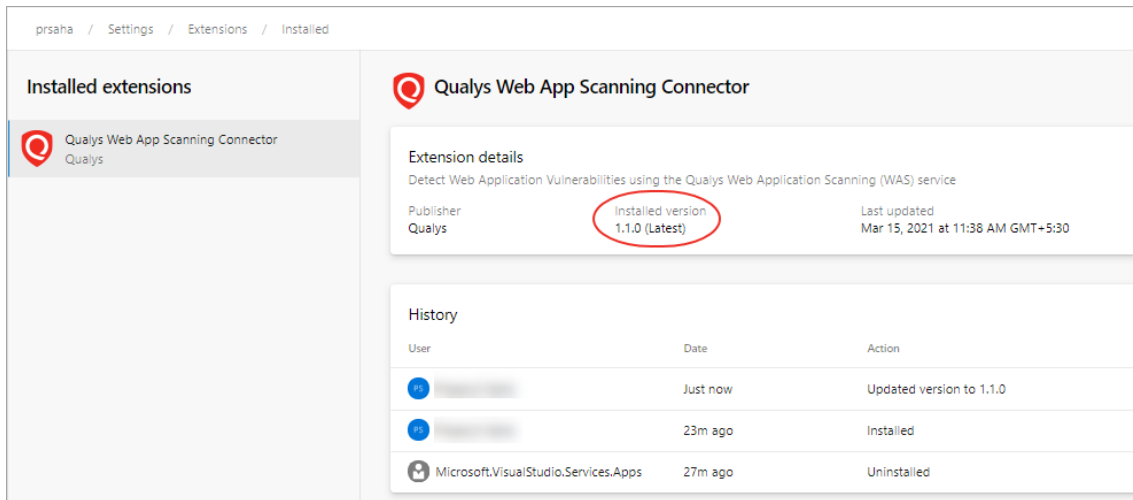
2. Click **Action Required** and then from the right pane, click **Review** to view and authorize the scope/permissions of the new plugin version.



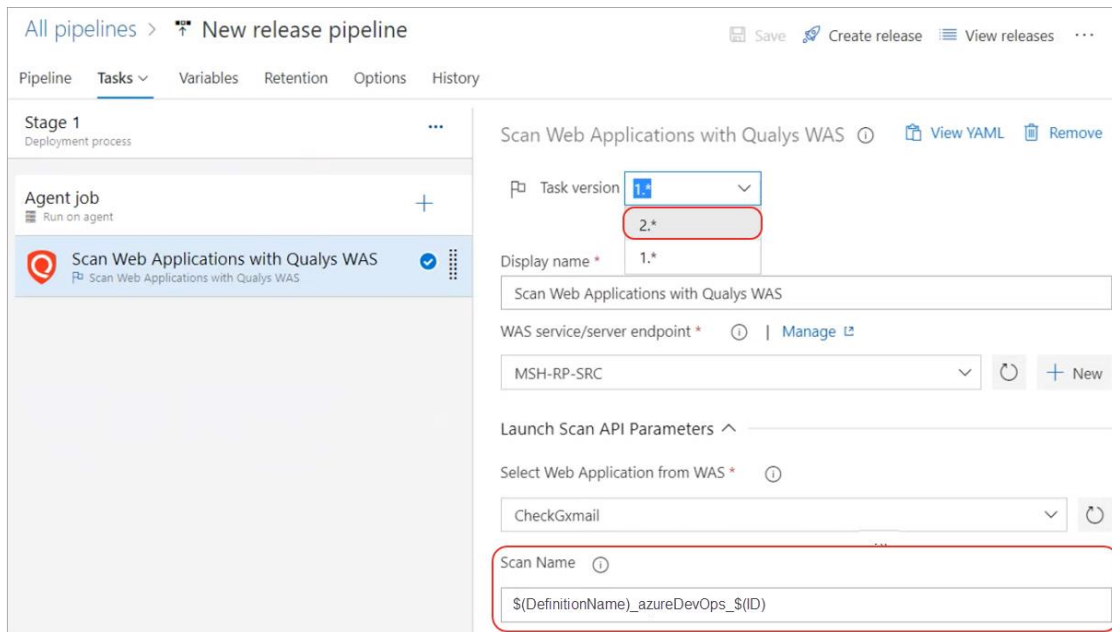
3. Click **Authorize** after reviewing the scope of new version of the plugin.



You will see the plugin version updated to the latest version.



Note: To use the upgraded plugin in your existing release pipeline project in which you have added the plugin as a task, go to the plugin task and then select the latest task version from the Task Version drop-down field.



In the Scan Name field, enter the scan name with this format or a custom name:

`$(DefinitionName)_azureDevOps_$(ID)`

Optionally, you can click the help  icon provided for the Scan Name field and copy this format from the help text.

To use the upgraded plugin in your existing build pipeline, go to the plugin task and just select the latest task version. Then you can run the job. For existing build pipeline projects, changing the scan name is optional.

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 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 preconfigure the web application, option profile, and authentication record in your Qualys WAS account for the plugin to populate them in the respective fields on the configuration form.
4. Ensure that the Azure DevOps user account for configuring WAS plugin is part of the Project Collection Administrators group. To view the Project Collection Administrators group, go to Organization Settings > Permissions > Project Collection Administrators.

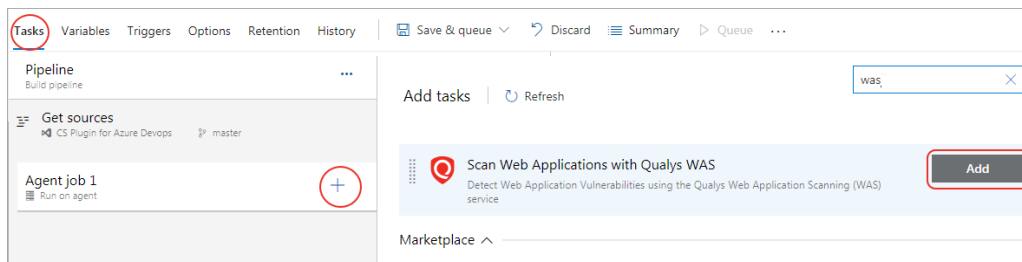
Configure the Plugin

The Qualys Web App Scanning Connector can be added as a task in your Build and Release Pipelines. The steps to configure the plugin in both the Build pipeline and the Release pipeline are the same.

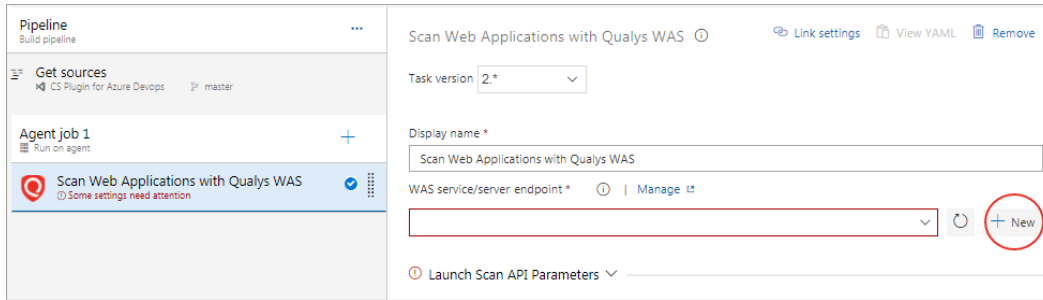
Note: Qualys Web Application Scanning Connector for Azure DevOps supports only one Qualys WAS task in the Build pipeline and the Release pipeline with one or more stages.

Configure the Plugin for Build Pipelines Projects

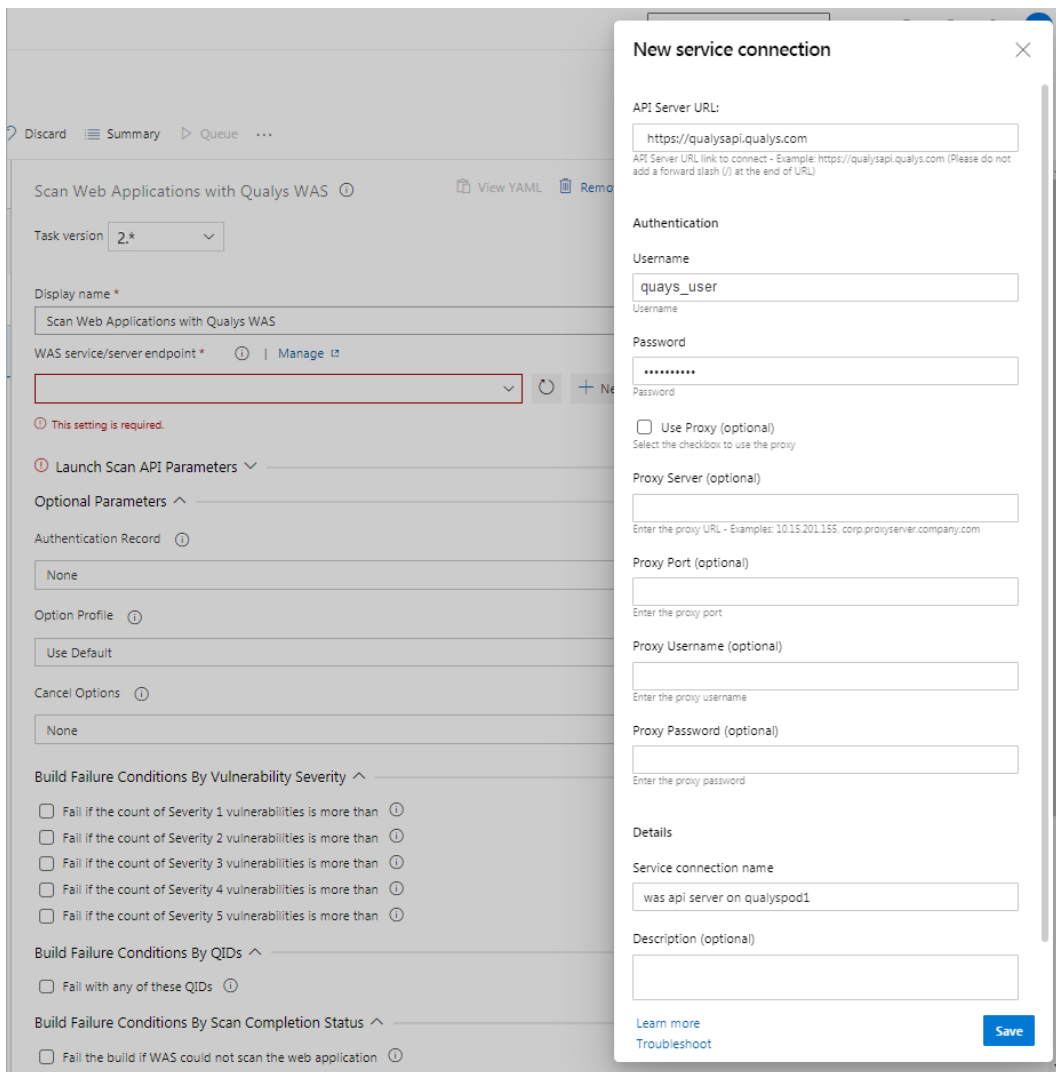
You can use this Qualys Web App Scanning Connector extension as a pre-deployment task in your project pipeline. After installing the Qualys Web App Scanning Connector, you see this plugin as a task in your pipeline. In the **Tasks** tab, click **Add** (plus icon) under your agent job, and search for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



You will see the task under the agent job. Click the task to configure the plugin.



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 required) 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**.



In the New service connection screen, 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.

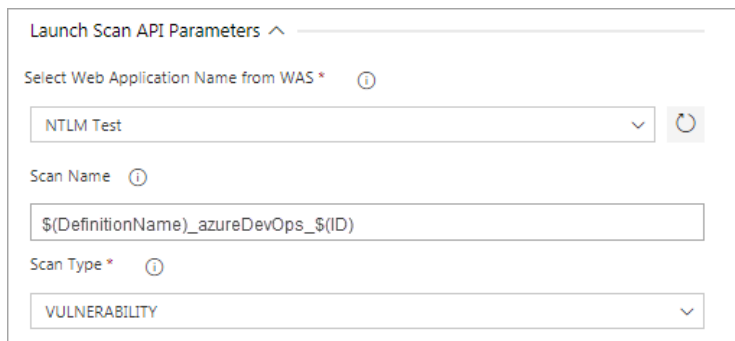
Note: What you select here depends on the Qualys platform your organization is using. [Learn more](#). We expect the user to provide “qualysapi” specific URL for their respective platform as input for “API Server URL”.

If your Azure DevOps instance does not have direct Internet access and requires a proxy, click the “Use Proxy Settings” check box, and enter the proxy server information.

Note: 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 valid credentials, 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:

```
$(DefinitionName)_azureDevOps_$(ID) + timestamp
```

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

If you are using plugin version 1.0.0, then the default WAS scan name will be:

```
[Build.DefinitionName]_azureDevOps_build_[ Build.BuildID] + timestamp
```

You can continue using this format for your existing build pipeline projects after upgrading your plugin version or choose the new format.

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

Optional Parameters

Next, configure optional scan parameters.



The screenshot shows a configuration panel titled "Optional Parameters" with a collapse arrow. It contains three sections, each with a dropdown menu and an information icon (i):

- Authentication Record**: The dropdown menu is set to "Use Default".
- Option Profile**: The dropdown menu is set to "Use Default".
- Cancel Options**: The dropdown menu is set to "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 we will use the default authentication record for the web app in WAS (if any). 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.

Note: You may not get any results if you cancel a running scan.

Next, configure the pass/fail criteria for a build, scan status polling frequency, and timeout duration for the scan.

Build Failure Conditions

Configure the scan pass/fail criteria to fail a build job.

Build Failure Conditions By Vulnerability Severity ^

- Fail if the count of Severity 1 vulnerabilities is more than ⓘ
- Fail if the count of Severity 2 vulnerabilities is more than ⓘ
- Fail if the count of Severity 3 vulnerabilities is more than ⓘ
- Fail if the count of Severity 4 vulnerabilities is more than ⓘ
- Fail if the count of Severity 5 vulnerabilities is more than ⓘ

Build Failure Conditions By QIDs ^

- Fail with any of these QIDs ⓘ

Build Failure Conditions By Scan Completion Status ^

- Fail the build if WAS could not scan the web application ⓘ

Timeout Settings ^

How often to check for data (in minutes) * ⓘ

How long to wait for scan results (in minutes) * ⓘ

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 the number of detections exceeds the number specified for one or more severity types in scan results. 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: 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 if 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 the 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.

Configure the Plugin for Release Pipeline Projects

You can add the plugin as a task in the release pipeline projects (Pipelines > Releases) and launch WAS scans. If you are using the plugin first time in your project, then first, install the Qualys Web App Scanning Connector Plugin from the Azure DevOps marketplace. See [Install the Plugin](#). Next, create a new release pipeline project and then configure the plugin as a task. The

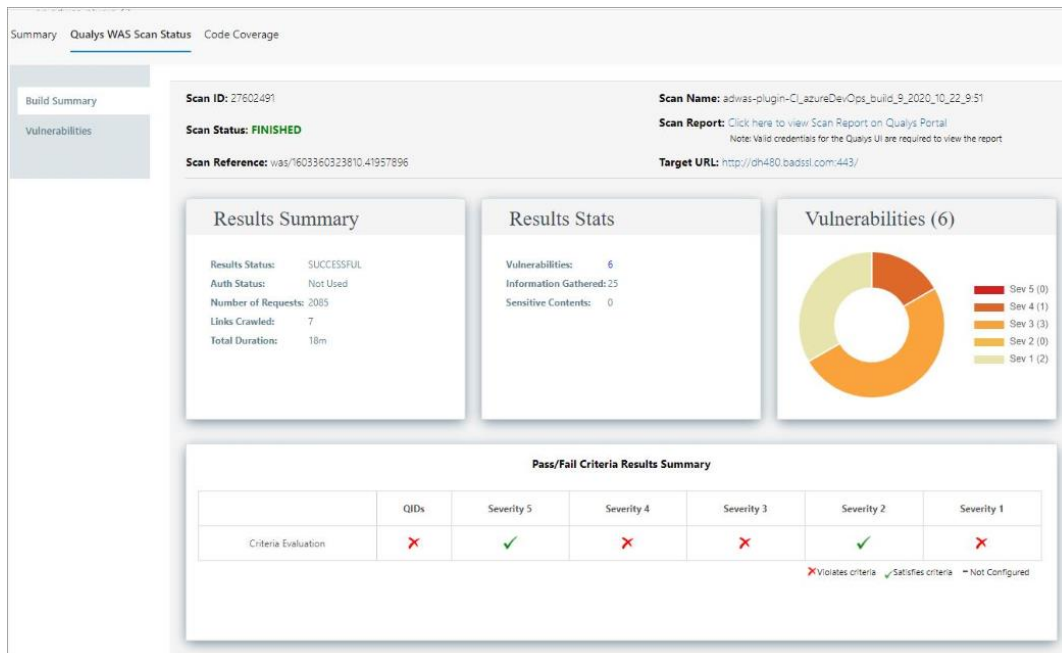
steps to configure plugin in the Build and Release pipeline are the same. To configure the plugin, see [Configure the Plugin for Build Pipelines Projects](#).

Note: You need to upgrade your plugin version to launch a WAS scan with an existing Release pipeline project that you created using plugin version 1.0.0. See [Upgrade the Plugin](#).

Qualys WAS Scan Status

After the scan is complete, the Build Summary tab will show two sections: Summary of 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 the **✓** icon is shown for the satisfied criteria.

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 you 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.

Summary **Qualys WAS Scan Status** Code Coverage

QUALYS VULNERABILITIES RESULTS

Show entries

QID	Title	URL	Available Unauthenticated?
150004	Path-Based Vulnerability	http://www.gxmail.com/webmail/	Yes
150263	Insecure Transport	http://www.gxmail.com/	Yes

Showing 1 to 2 of 2 entries Previous Next

View Qualys WAS Scan Status for Release Pipeline

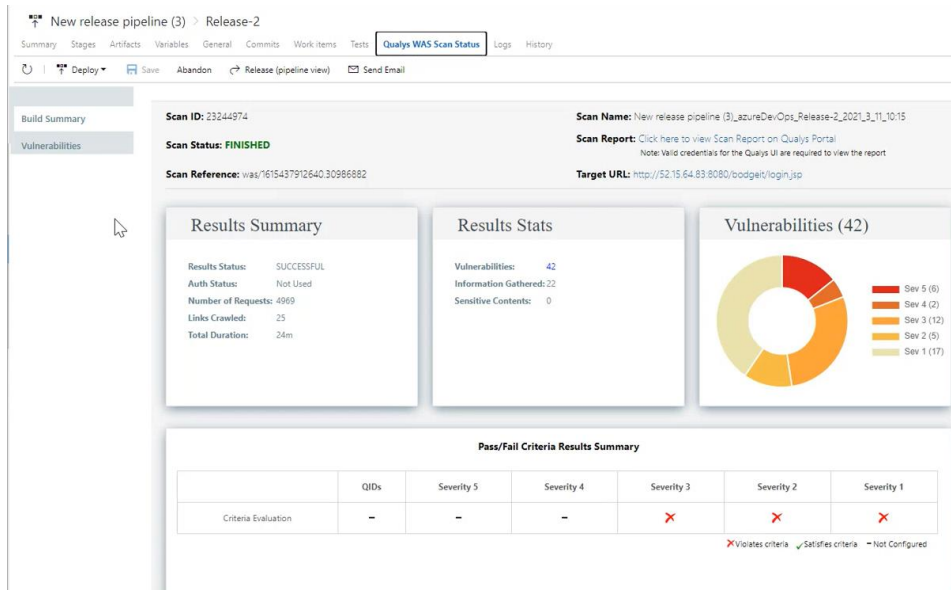
To view the WAS scan report, go to your release pipeline after the scan is completed. Click the ellipsis (...) and select the Release (old view) option. A new page opens in a new browser.

Azure DevOps interface showing a failed release pipeline. The 'Agent job' section is expanded, and a 'Release (old view)' button is highlighted with a red circle.

Select Qualys WAS Scan Status on the right pane to view the report.

Azure DevOps interface showing the 'Qualys WAS Scan Status' report for a failed release pipeline. The 'Summary' tab is selected, and the 'Qualys WAS Scan Status' link is highlighted with a red circle.

A sample WAS Scan Status report generated for release pipeline.



Troubleshooting

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

Check that the Azure DevOps User account used for configuring WAS plugin is part of the Project Collection Administrators group. To view the Project Collection Administrators group, go to Organization Settings > Permissions > Project Collection Administrators.

Also, verify that Qualys account provided have a proper role or scope to access the web application you wish to scan, the auth record, or the option profile you want to use. Ensure that the account has been set up with the required roles and scope.

What's New

Improvements in 1.1.1

We have fixed an issue for rendering scan report when multiple stages are present in the Release pipeline.