# Qualys Web App Scanning Connector for Azure DevOps

User Guide

Version 1.2.2

April 28, 2023

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**.

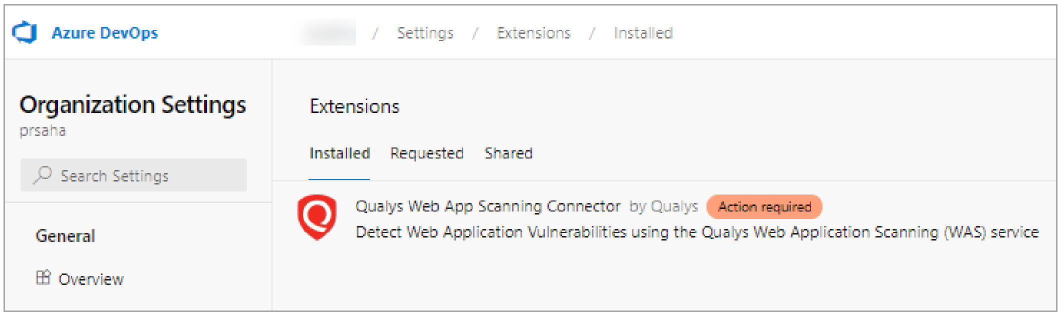
The Qualys Web App Scanning Connector gets installed/updated in your Azure DevOps instance. In case of an update, your existing configuration will continue to work. In case of a fresh install, you perform the configuration steps provided further in this document.

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**.



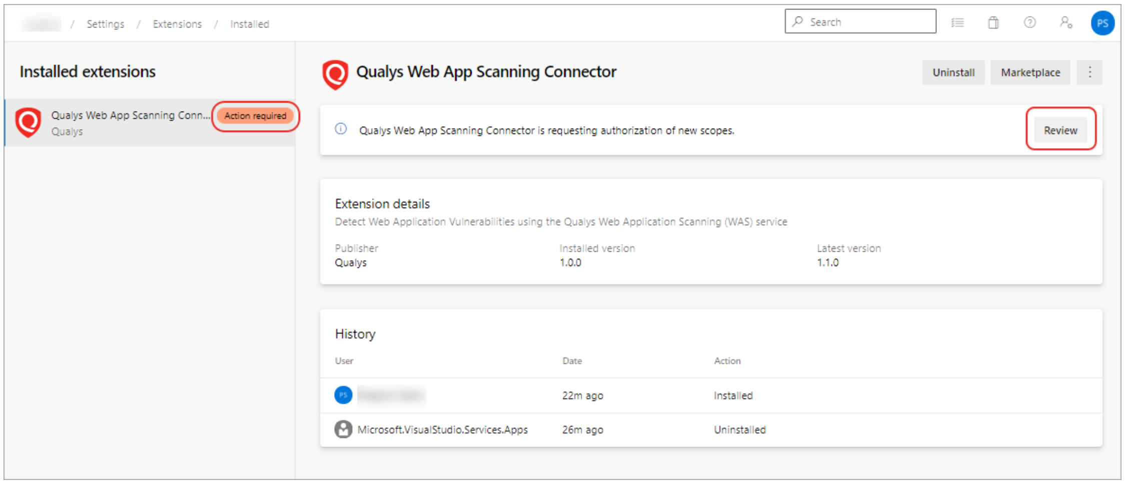
Azure DevOps [redacted] / Settings / Extensions / Installed

Organization Settings
prsaha

Extensions

Qualys Web App Scanning Connector by Qualys Action required
Detect Web Application Vulnerabilities using the Qualys Web Application Scanning (WAS) service

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



[redacted] / Settings / Extensions / Installed

Installed extensions

Qualys Web App Scanning Conn... Action required
Qualys

Qualys Web App Scanning Connector

Qualys Web App Scanning Connector is requesting authorization of new scopes.

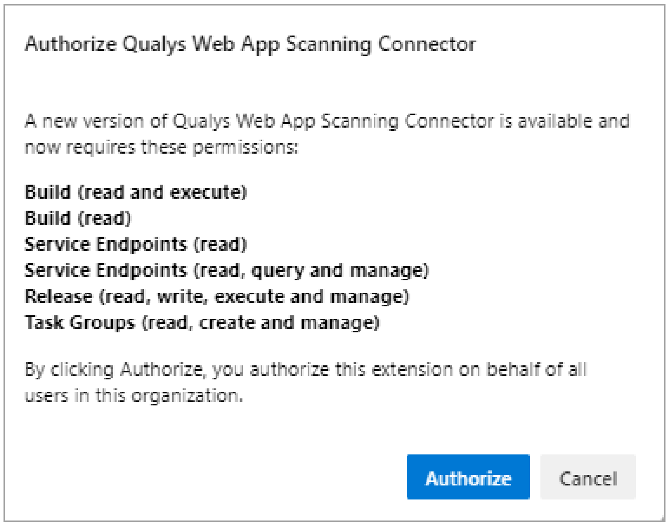
Extension details
Detect Web Application Vulnerabilities using the Qualys Web Application Scanning (WAS) service

| Publisher | Installed version | Latest version |
|---|---|---|
| Qualys | 1.0.0 | 1.1.0 |

History

| User | Date | Action |
|---|---|---|
| [redacted] | 22m ago | Installed |
| Microsoft.VisualStudio.Services.Apps | 26m ago | Uninstalled |

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



Authorize Qualys Web App Scanning Connector

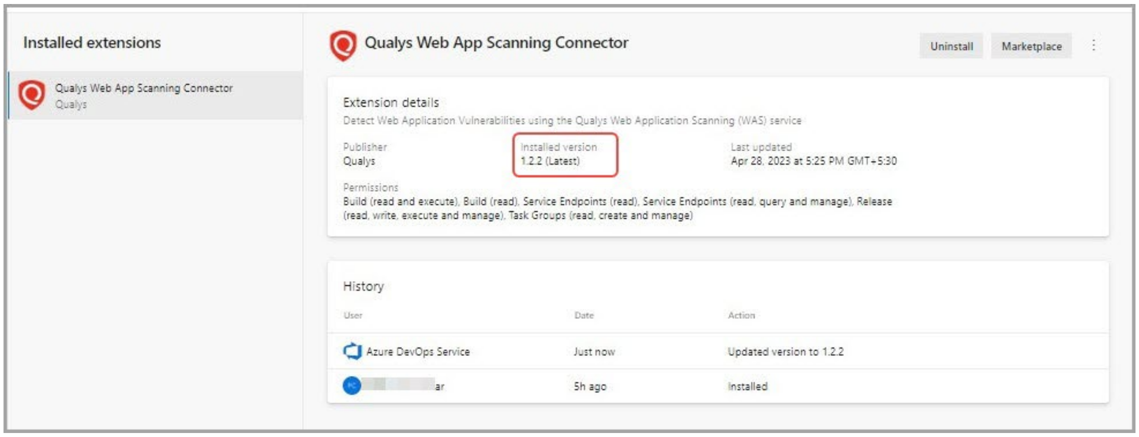
A new version of Qualys Web App Scanning Connector is available and now requires these permissions:

**Build (read and execute)**
**Build (read)**
**Service Endpoints (read)**
**Service Endpoints (read, query and manage)**
**Release (read, write, execute and manage)**
**Task Groups (read, create and manage)**

By clicking Authorize, you authorize this extension on behalf of all users in this organization.

**Note:** The upgrade steps mentioned above are applicable only if you are upgrading from v1.0.0; For versions 1.1.0 and higher, Qualys WAS scanning connector for Azure DevOps gets upgraded automatically when a new version is released in the marketplace, as per the Azure DevOps design. Users may want to select the updated task version in their pipeline for new changes to reflect in the respective task.

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



Qualys Web App Scanning Connector

Extension details

Detect Web Application Vulnerabilities using the Qualys Web Application Scanning (WAS) service

Publisher: Qualys

Installed version: 1.2.2 (Latest)

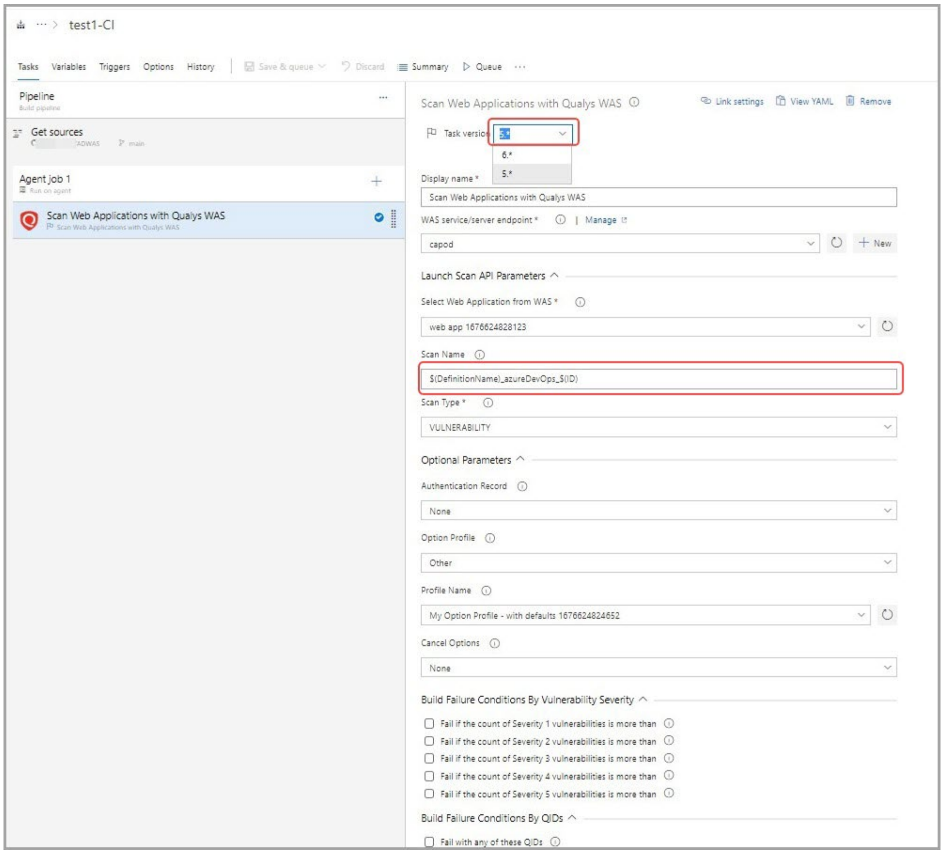
Last updated: Apr 28, 2023 at 5:25 PM GMT+5:30

Permissions: Build (read and execute), Build (read), Service Endpoints (read), Service Endpoints (read, query and manage), Release (read, write, execute and manage), Task Groups (read, create and manage)

History

| User | Date | Action |
|---|---|---|
| Azure DevOps Service | Just now | Updated version to 1.2.2 |
| [redacted]ar | 5h ago | Installed |

**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 select the latest task version from the Task Version drop-down field.



Scan Web Applications with Qualys WAS

Task version: 5.* (options: 6.*, 5.*)

Display name *: Scan Web Applications with Qualys WAS

WAS service/server endpoint *: capod

Launch Scan API Parameters

Select Web Application from WAS *: web app 1676624828123

Scan Name: $(DefinitionName)_azureDevOps_$(ID)

Scan Type *: VULNERABILITY

Optional Parameters

Authentication Record: None

Option Profile: Other

Profile Name: My Option Profile - with defaults 1676624824652

Cancel Options: None

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

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

$(DefinitionName)_azureDevOps_$(ID)

Optionally, 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 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

- The current version of the Web App Scanning Connector supports only Azure DevOps Services. You can use self-hosted agents or Microsoft agents.
- You must have valid account credentials for an active Qualys WAS subscription. The account must have API access enabled and a role assigned with all necessary permissions.
- 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.

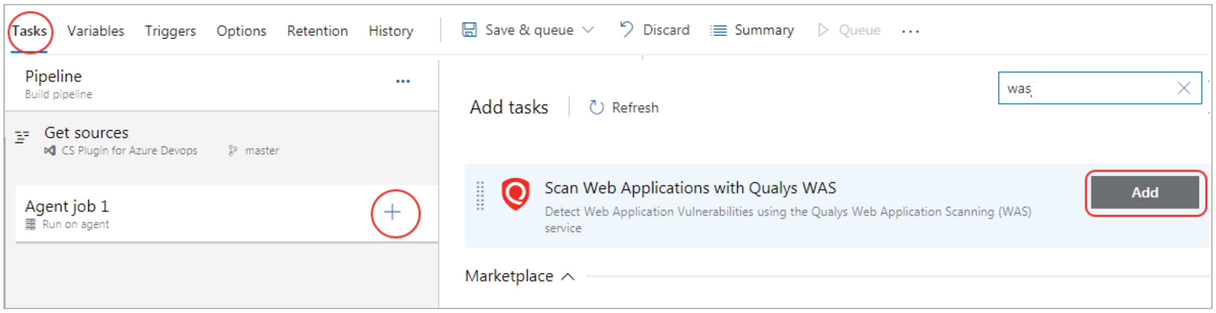
## Configure the Plugin

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 and Release pipelines 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.

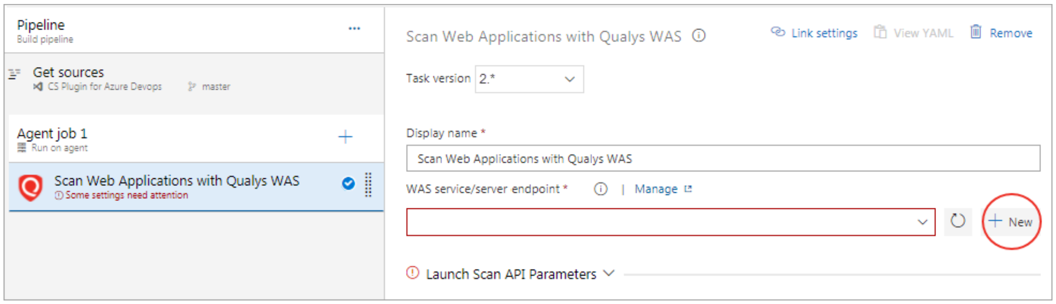
### Configure the Plugin for Build Pipelines Projects

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.



Detect Web Application Vulnerabilities using the Qualys Web Application Scanning (WAS) service

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

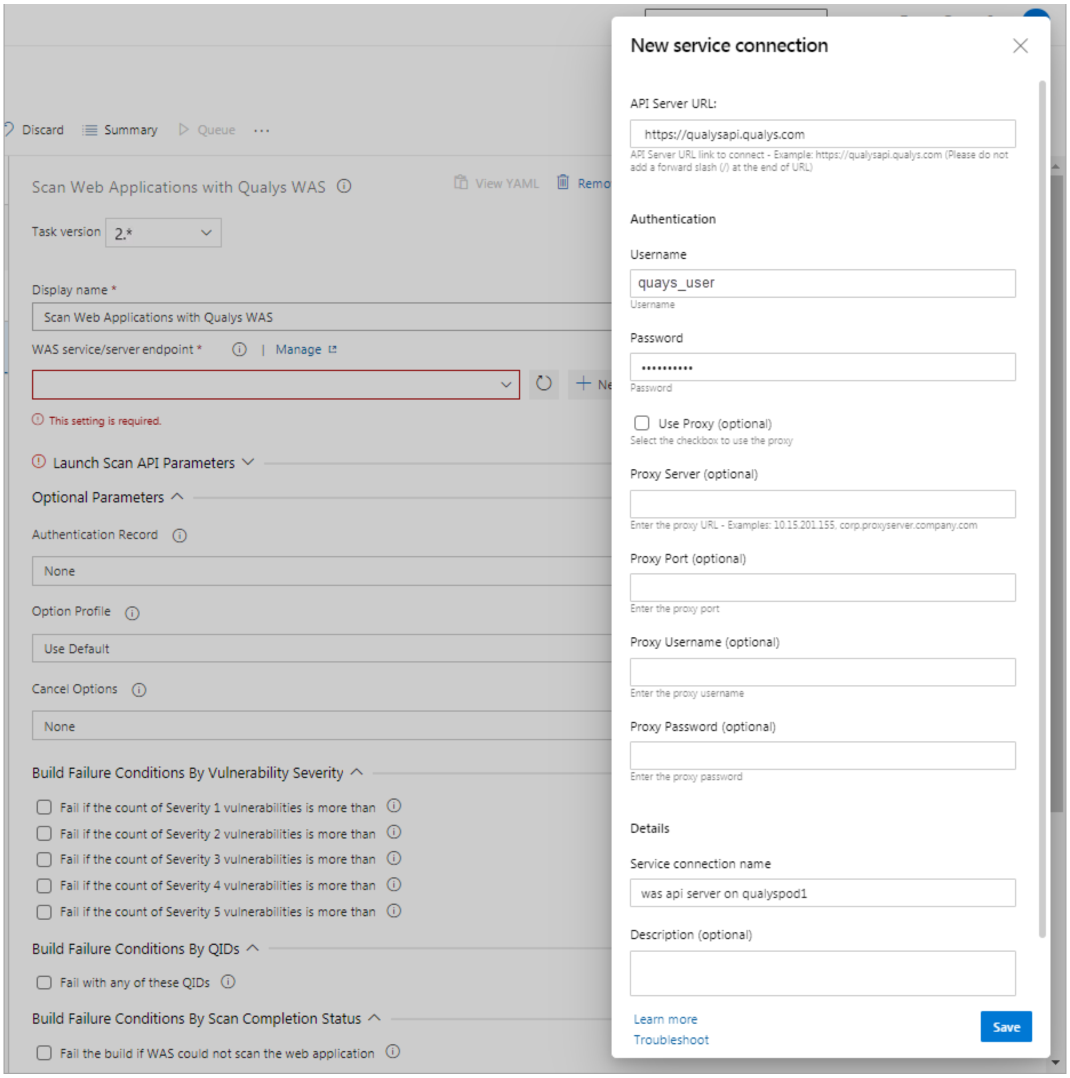

Pipeline
Build pipeline
...
Get sources
CS Plugin for Azure Devops
master
Agent job 1
Run on agent
+
Scan Web Applications with Qualys WAS
Some settings need attention
Scan Web Applications with Qualys WAS
Link settings
View YAML
Remove
Launch Scan API Parameters
New
Manage

Task version 2.*

Display name * Scan Web Applications with Qualys WAS

WAS service/server endpoint *

After entering the display name, the first step is configuring the WAS service endpoint. To connect to the WAS APIs, you need to configure the service endpoint with a 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**.


Discard
Summary
Queue
...
Scan Web Applications with Qualys WAS
View YAML
Remo
Manage
Ne
Launch Scan API Parameters
Optional Parameters
Build Failure Conditions By Vulnerability Severity
Build Failure Conditions By QIDs
Build Failure Conditions By Scan Completion Status
New service connection
Authentication
Details
Learn more
Troubleshoot
Save

Task version 2.*

Display name * Scan Web Applications with Qualys WAS

WAS service/server endpoint *

This setting is required.

Authentication Record: None

Option Profile: Use Default

Cancel Options: None

□ 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

□ Fail with any of these QIDs

□ Fail the build if WAS could not scan the web application

API Server URL: https://qualysapi.qualys.com

API Server URL link to connect - Example: https://qualysapi.qualys.com (Please do not add a forward slash (/) at the end of URL)

Username: quays_user

Password: ••••••••••

□ Use Proxy (optional)

Select the checkbox to use the proxy

Proxy Server (optional)

Enter the proxy URL - Examples: 10.15.201.155, corp.proxyserver.company.com

Proxy Port (optional)

Enter the proxy port

Proxy Username (optional)

Enter the proxy username

Proxy Password (optional)

Enter the proxy password

Service connection name: was api server on qualyspod1

Description (optional)

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.

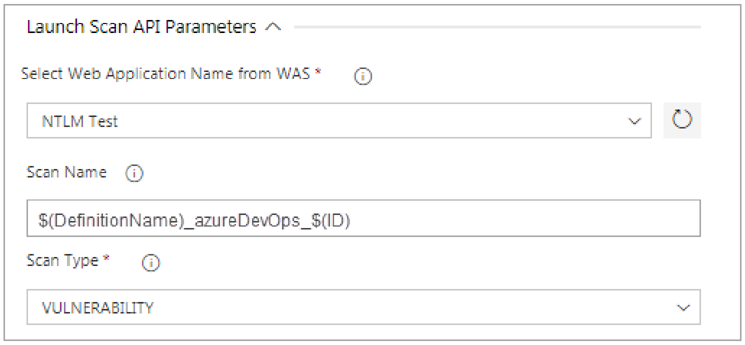
**Note**: What you select here depends on the Qualys platform your organization is using. Learn more. We expect the user to provide “qualysapi” specific URL for their respective platform as input for the "API Server URL."

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.



Launch Scan API Parameters

Select Web Application Name from WAS *: NTLM Test

Scan Name: $(DefinitionName)_azureDevOps_$(ID)

Scan Type *: VULNERABILITY

By default, the WAS scan name will be:

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

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

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

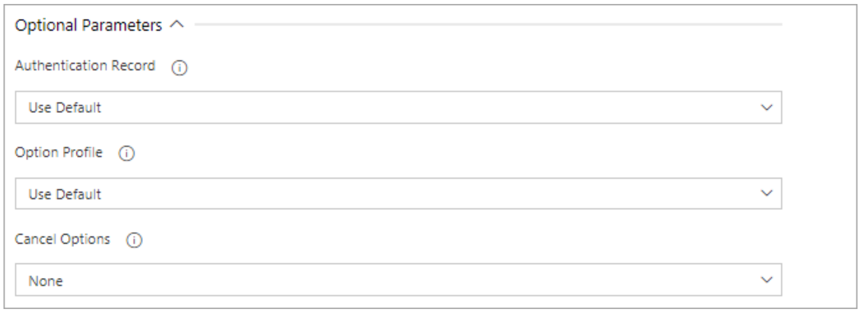
```
[Build.DefinitionName]_azureDevOps_build_[ Build.BuildID] + timestamp
```

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 a Vulnerability scan. The default is the Vulnerability scan.

### Optional Parameters

Next, configure optional scan parameters.



Optional Parameters

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 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.

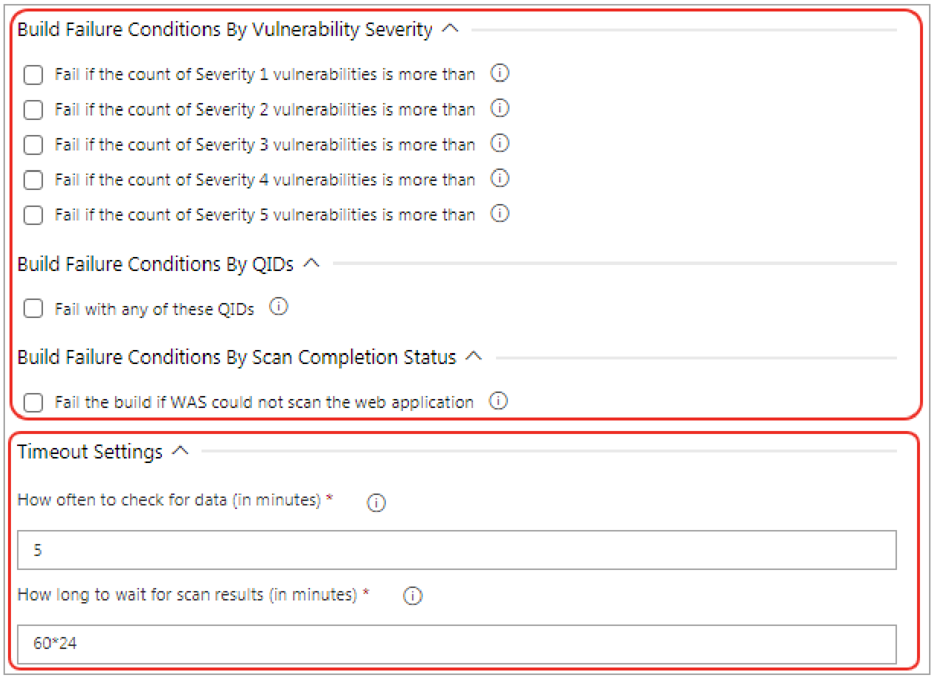
Cancel Options – The default is not to cancel the scan, in which case the scan will run to completion. However, you can cancel the scan after a set number of hours.

**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) * ⓘ

5

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

60*24

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, the build fails.

## 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

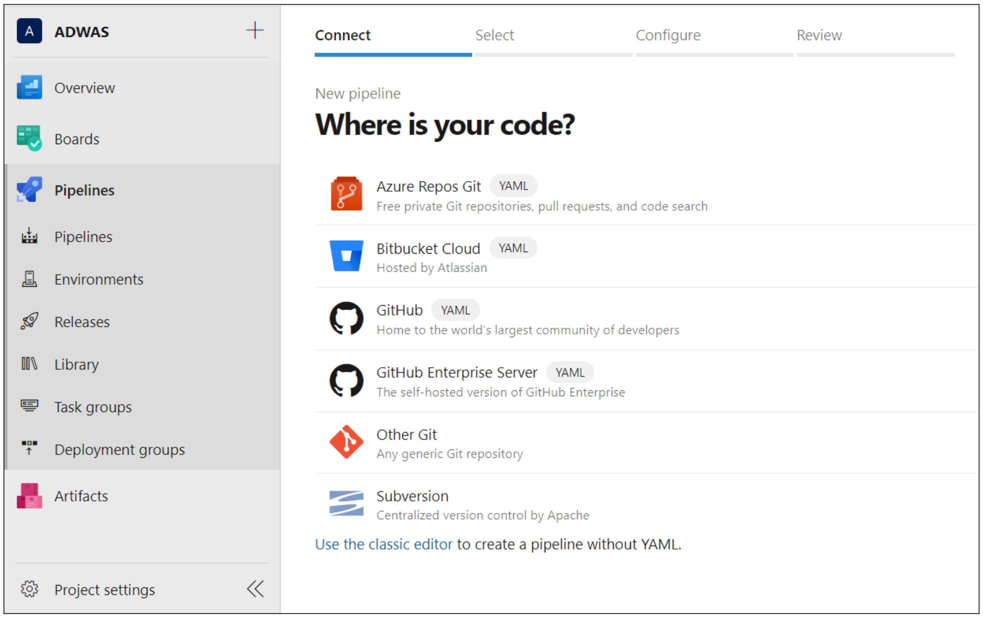
You can add the plugin as a task in the release pipeline projects (Pipelines > Releases) and launch WAS scans. If you are using the plugin for the first time in your project, install the Qualys Web App Scanning Connector Plugin from the Azure DevOps marketplace. See Install the Plugin. Next, create a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

## Configure the Plugin for YAML-based Pipeline Projects

You can add a plugin as a task in YAML pipeline projects and launch WAS scans. The steps for this scan differs slightly from build/release pipeline. Follow these instructions to configure YAML pipeline.

1. On the Microsoft Azure portal, navigate to the Organization and select the required project.
2. Click **Pipeline**.
3. Create a new Pipeline.
4. Select the Azure Repo to store the pipeline YAML file.



New pipeline

Where is your code?

Azure Repos Git YAML
Free private Git repositories, pull requests, and code search

Bitbucket Cloud YAML
Hosted by Atlassian

GitHub YAML
Home to the world's largest community of developers

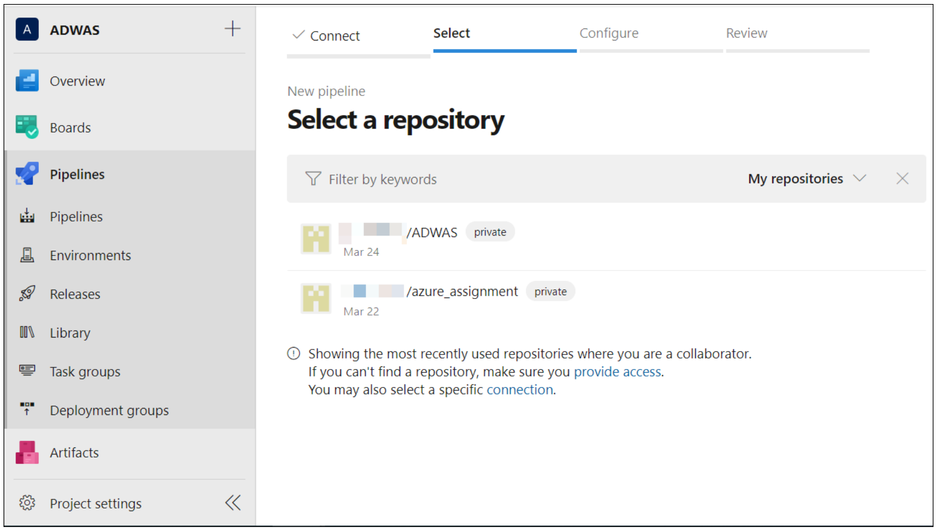
GitHub Enterprise Server YAML
The self-hosted version of GitHub Enterprise

Other Git
Any generic Git repository

Subversion
Centralized version control by Apache

Use the classic editor to create a pipeline without YAML.

5. Select a repository from an existing list.



New pipeline

Select a repository

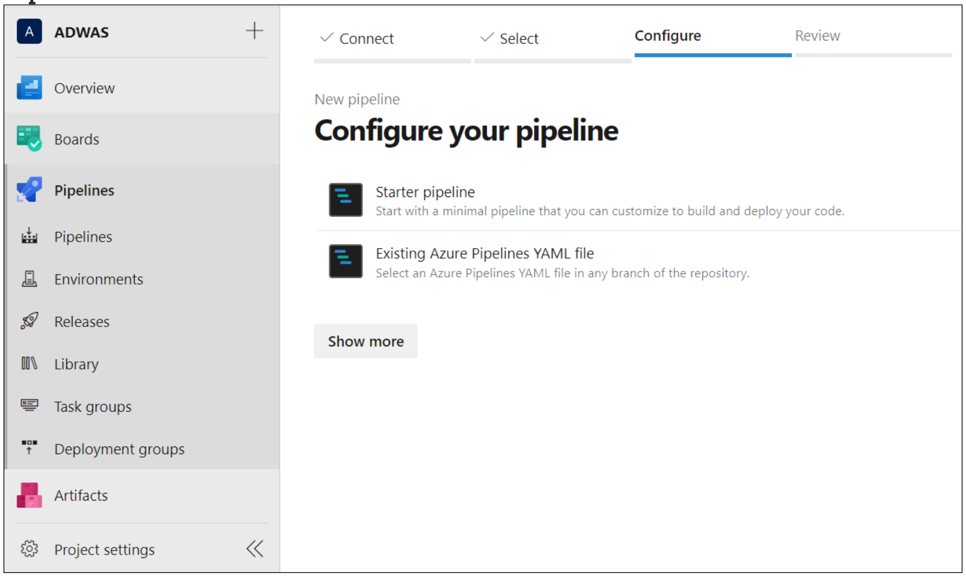
Filter by keywords My repositories

[redacted]/ADWAS private
Mar 24

[redacted]/azure_assignment private
Mar 22

Showing the most recently used repositories where you are a collaborator.
If you can't find a repository, make sure you provide access.
You may also select a specific connection.

6. If you have an existing YAML pipeline file, select the **Existing Azure Pipeline YAML file** option and paste the generated configuration steps into it (for …). Else, select **Starter Pipeline**.



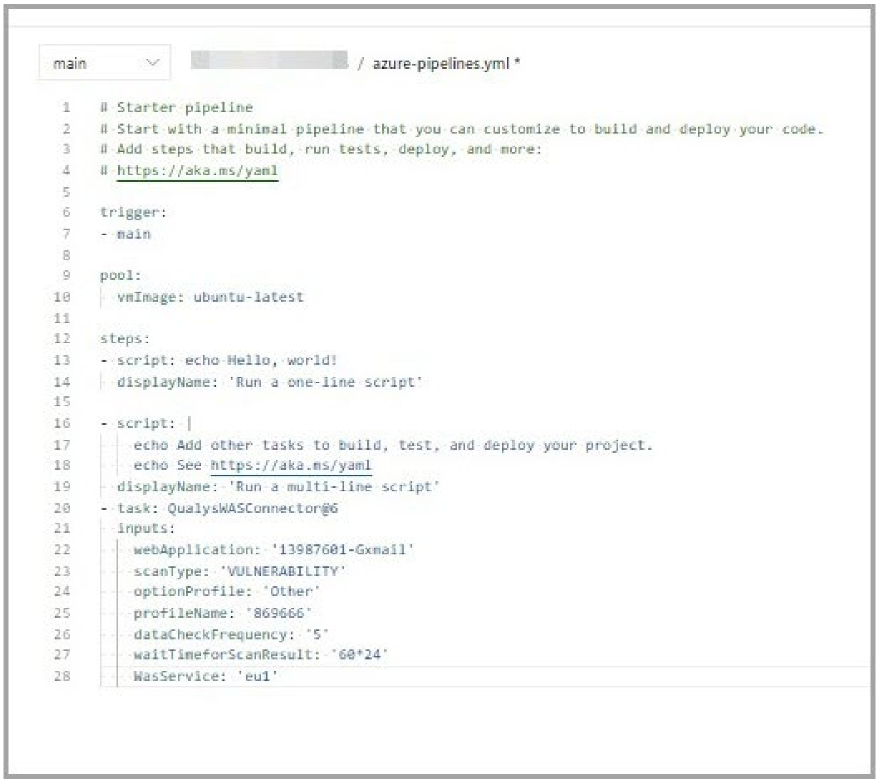
New pipeline

Configure your pipeline

Starter pipeline
Start with a minimal pipeline that you can customize to build and deploy your code.

Existing Azure Pipelines YAML file
Select an Azure Pipelines YAML file in any branch of the repository.

7. Type **Qualys** in the search bar.
8. Select **Scan Web Applications with Qualys WAS**.
9. Configure the Qualys WAS plugin. For more information, refer to Configure the Plugin.
10. Add the configuration steps generated by the plugin into the pipeline file.



[redacted] / azure-pipelines.yml *

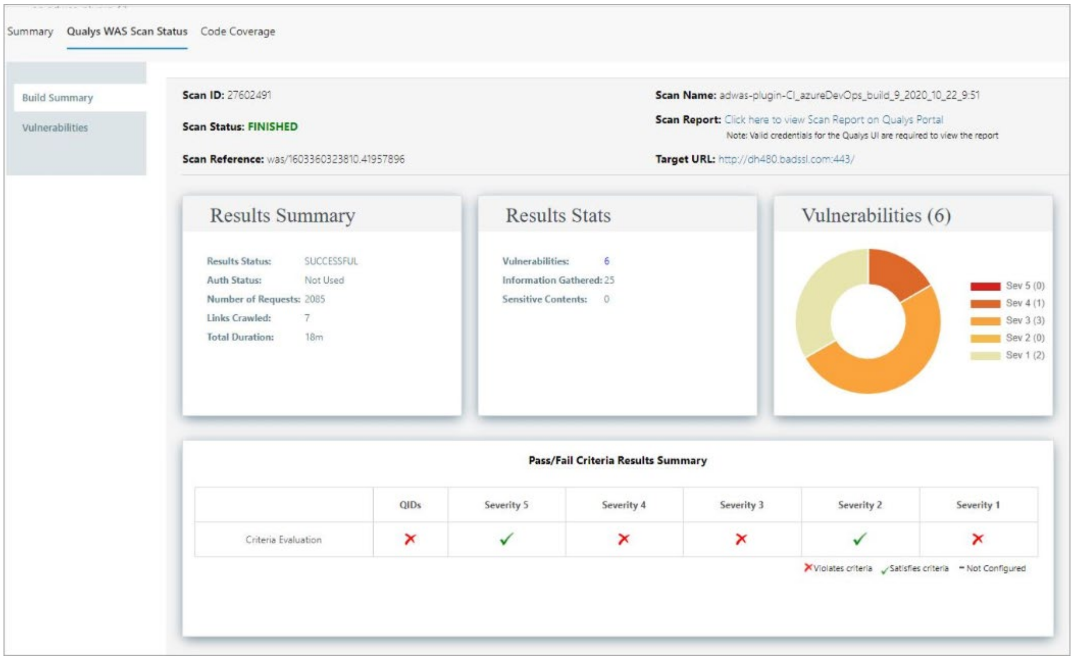
```yaml
# Starter pipeline
# Start with a minimal pipeline that you can customize to build and deploy your code.
# Add steps that build, run tests, deploy, and more:
# https://aka.ms/yaml

trigger:
- main

pool:
  vmImage: ubuntu-latest

steps:
- script: echo Hello, world!
  displayName: 'Run a one-line script'

- script: |
    echo Add other tasks to build, test, and deploy your project.
    echo See https://aka.ms/yaml
  displayName: 'Run a multi-line script'
- task: QualysWASConnector@6
  inputs:
    webApplication: '13987601-Gxmail'
    scanType: 'VULNERABILITY'
    optionProfile: 'Other'
    profileName: '869666'
    dataCheckFrequency: '5'
    waitTimeforScanResult: '60*24'
    WasService: 'eu1'
```

11. Click **Save and run**.

## 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.



**Scan ID:** 27602491

**Scan Status:** FINISHED

**Scan Reference:** was/1603360323810.41957896

**Scan Name:** adwas-plugin-CI_azureDevOps_build_9_2020_10_22_9:51

**Scan Report:** Click here to view Scan Report on Qualys Portal

Note: Valid credentials for the Qualys UI are required to view the report

**Target URL:** http://dh480.badssl.com:443/

Results Summary

| | |
|---|---|
| Results Status: | SUCCESSFUL |
| Auth Status: | Not Used |
| Number of Requests: | 2085 |
| Links Crawled: | 7 |
| Total Duration: | 18m |

Results Stats

| | |
|---|---|
| Vulnerabilities: | 6 |
| Information Gathered: | 25 |
| Sensitive Contents: | 0 |

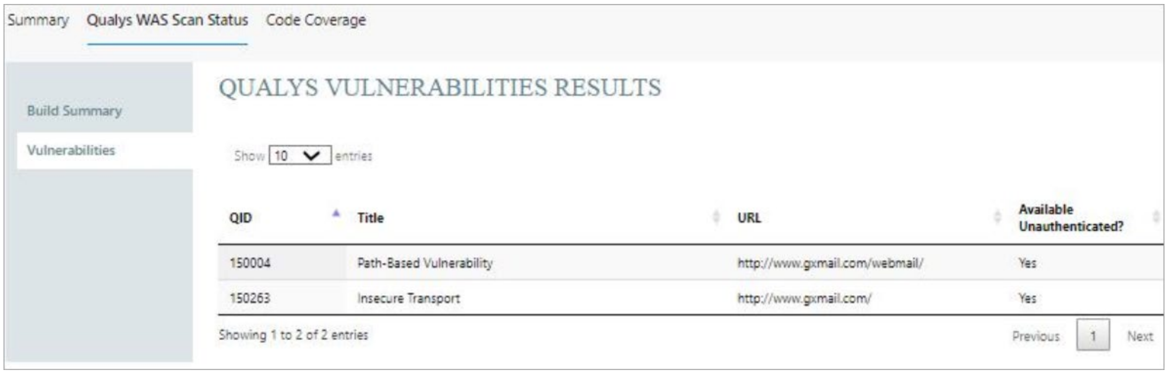
Pass/Fail Criteria Results Summary

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

✗ Violates criteria ✓ Satisfies criteria − Not Configured

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.



QUALYS VULNERABILITIES RESULTS

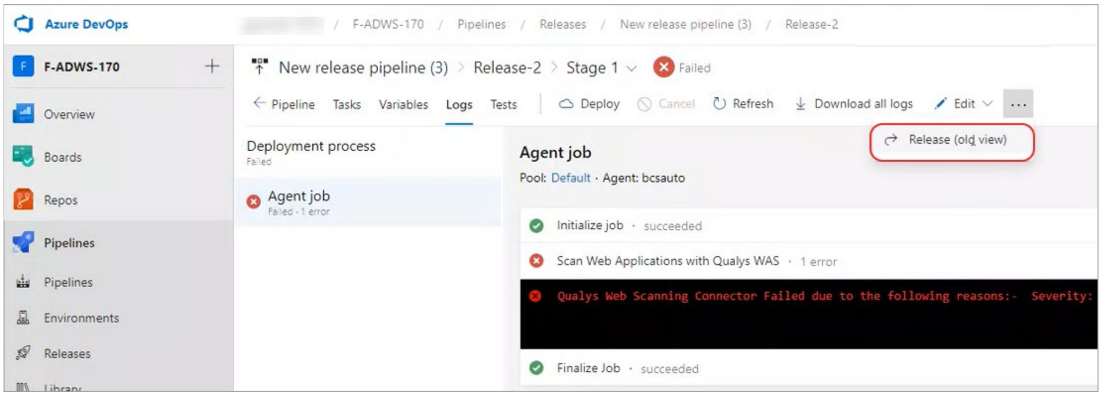
Show 10 entries

| 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

### 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.



Deployment process
Failed

Agent job
Failed · 1 error

Agent job
Pool: Default · Agent: bcsauto

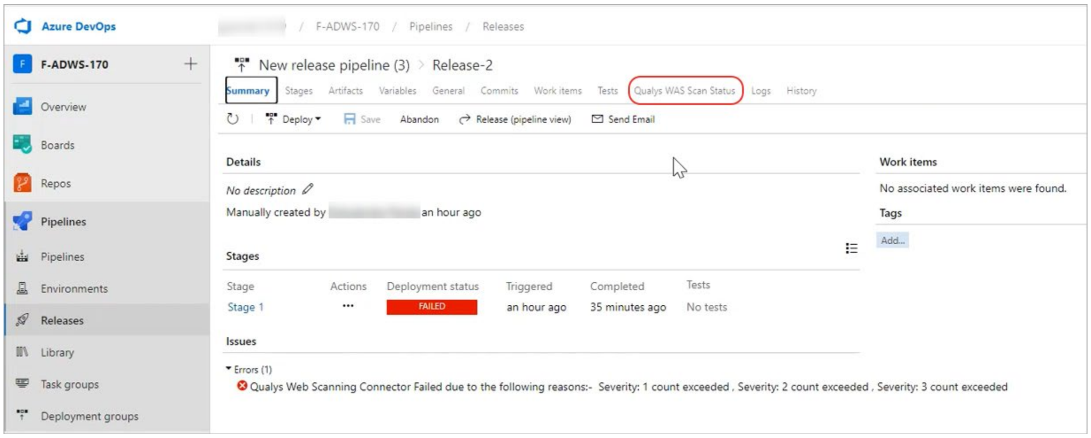
Initialize job · succeeded

Scan Web Applications with Qualys WAS · 1 error

```
Qualys Web Scanning Connector Failed due to the following reasons:-  Severity:
```

Finalize Job · succeeded

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



Details

*No description*

Manually created by [redacted] an hour ago

Work items

No associated work items were found.

Tags

Add...

Stages

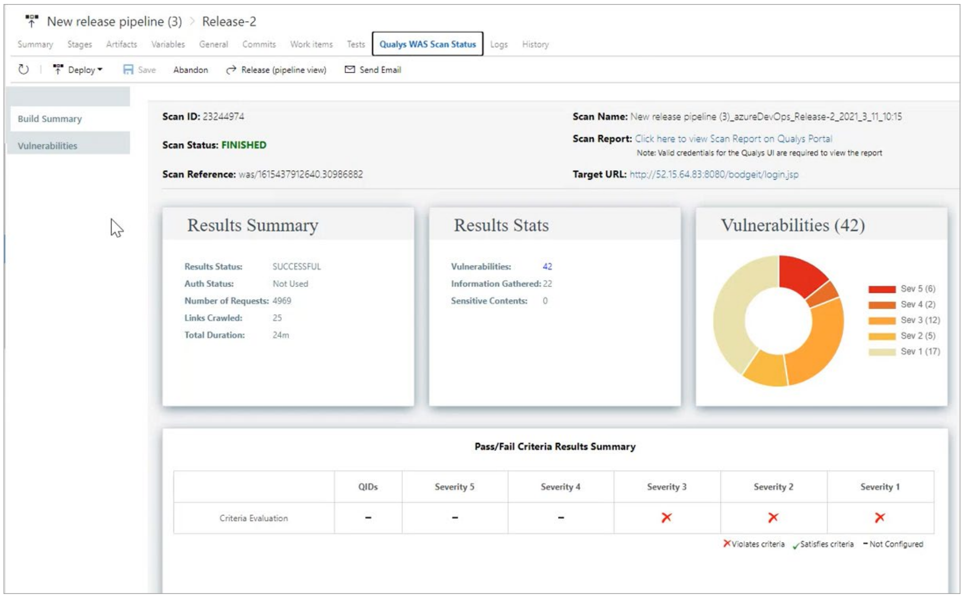
| Stage | Actions | Deployment status | Triggered | Completed | Tests |
|---|---|---|---|---|---|
| Stage 1 | ··· | FAILED | an hour ago | 35 minutes ago | No tests |

Issues

Errors (1)

Qualys Web Scanning Connector Failed due to the following reasons:- Severity: 1 count exceeded , Severity: 2 count exceeded , Severity: 3 count exceeded

A sample WAS Scan Status report generated for the release pipeline.



**Scan ID:** 23244974

**Scan Status:** FINISHED

**Scan Reference:** was/1615437912640.30986882

**Scan Name:** New release pipeline (3)_azureDevOps_Release-2_2021_3_11_10:15

**Scan Report:** Click here to view Scan Report on Qualys Portal

Note: Valid credentials for the Qualys UI are required to view the report

**Target URL:** http://52.15.64.83:8080/bodgeit/login.jsp

Results Summary

**Results Status:** SUCCESSFUL
**Auth Status:** Not Used
**Number of Requests:** 4969
**Links Crawled:** 25
**Total Duration:** 24m

Results Stats

**Vulnerabilities:** 42
**Information Gathered:** 22
**Sensitive Contents:** 0

**Pass/Fail Criteria Results Summary**

| | QIDs | Severity 5 | Severity 4 | Severity 3 | Severity 2 | Severity 1 |
|---|---|---|---|---|---|---|
| Criteria Evaluation | – | – | – | ✗ | ✗ | ✗ |

✗ Violates criteria ✓ Satisfies criteria – Not Configured

## What's New

Here's what's new in features and improvements in Qualys Web App Scanning Connector for Azure DevOps!

### What's new in v1.2.2

We have addressed the issue where **Scan Report** URL navigation was not working for newly added Qualys platforms. Now, the user can access Scan Report URL navigation correctly.

## Known Issues

- For YAML specific Azure DevOps pipeline, the Qualys WAS connector is not able to populate drop-downs post 1000 records due to the design limitation of Azure DevOps itself.
  Hence, if your target record for a web application, Option profile &/or Authentication record needs to be populated in dropdowns in YAML assistant for Qualys WAS task, then you need to add the entry manually in the YAML script for respective fields.
- If the user has switched to Qualys WAS new UI, then the Scan report URL navigated from Azure DevOps scan result will land on Qualys WAS Dashboard. Fix for the same in the pipeline from Qualys WAS side.
- Target URL on Scan result - Use mouse right-click to open the target URL.

# 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.

Verify that the 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 the account has been set up with the required roles and scope.

### When Azure DevOps users with 'Build Administrator' or any equivalent permission log in, the web application drop-down is not populating even when web applications are present on the respective Qualys account.

Developer tool Error - "You do not have permission to perform this operation on the service connection. An Endpoint Administrator should add you to the Endpoint Readers group of this service connection."

Solution -

The error occurred because the logged-in Azure user may not have permission to consume/use the service connection configured in the Qualys WAS task.

The issue can be resolved by assigning the 'USER' role to the respective Azure user for configuring service connection. This needs to be done by the Endpoint administrator (the creator of the service connection is automatically assigned with this role)
1. Navigate to Project Settings > Service Connection > Open the Service Connection entry.
2. Go to the more actions at the top-right corner and choose Security.
3. Under 'User Permissions, add the Azure user and assign the role 'User'

Ref. - *https://docs.microsoft.com/en-us/azure/devops/pipelines/library/service-endpoints?view=azure-devops&tabs=yaml#secure-a-service-connection*