



Qualys IaC Security Extension for Azure DevOps

User Guide

Version 1.1.0

April 1, 2022

Copyright 2022 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 will show you how to install and use the Qualys IaC Security extension to see your Infrastructure as Code (IaC) 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 are 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 IaC Security Extension Documentation

This document provides information about using the Qualys IaC Security extension for Azure DevOps.

For supported templates, other integrations, and features of CloudView IaC Security, refer to [CloudView User Guide](#) and [CloudView API User Guide](#).

Introduction

The Qualys IaC Security extension empowers DevOps teams to build Infrastructure as Code (IaC) scans into their existing CI/CD processes. By integrating scans in this manner, cloud misconfigurations are detected and remediated earlier in the SDLC to catch and eliminate security flaws.

Pre-requisites


Ensure that you have the required subscription and permissions as stated below.

- The current version of the Qualys IaC Security extension supports only “Azure DevOps Services”. You can use self-hosted agents or out-of-box agents by Microsoft.
- You must have valid account credentials for Qualys CloudView (Cloud Security Assessment) app. The user must have API access enabled and a role assigned with all the necessary permissions.
- Ensure that the Azure DevOps user account for configuring Qualys IaC Security extension is part of the Project Collection Administrators group. To view the Project Collection Administrators group, go to Organization Settings > Permissions > Project Collection Administrators.

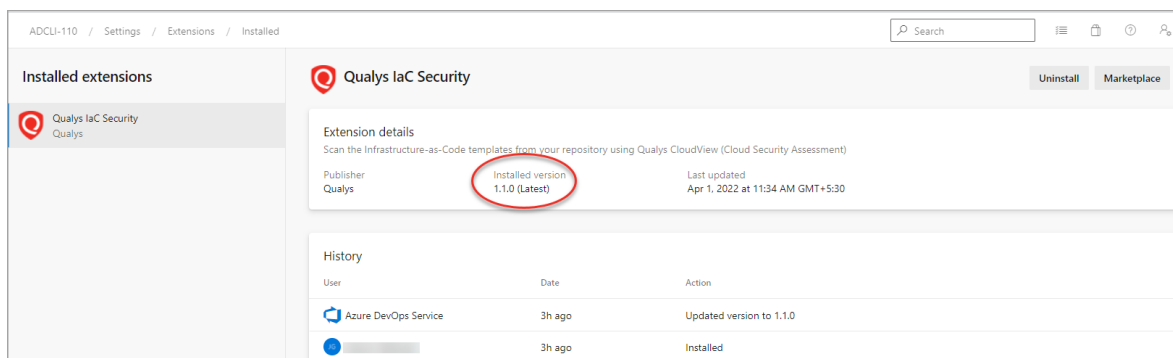
Install the Extension from Azure DevOps Marketplace

You can install the Qualys IaC Security extension for Azure DevOps from [Azure DevOps Marketplace](#).


Install the extension

1. To install the extension from the Azure DevOps marketplace, log in to your Azure DevOps instance.
2. Click the  icon on the upper-right side of the page and click **Browse marketplace**. A new browser opens to show you the extensions for Azure DevOps.
3. Enter Qualys in the search bar to search for all the Qualys extensions.
4. Click the Qualys IaC Security extension in the extensions 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 extension in your Azure DevOps instance.

You can see the extension version in the **Installed** tab when you navigate to **Organization Settings > Extension**.



The screenshot shows the 'Installed extensions' page in Azure DevOps. The extension 'Qualys IaC Security' is listed. The 'Installed version' is highlighted with a red circle and is '1.1.0 (Latest)'. The 'Publisher' is 'Qualys'. The 'Last updated' date is 'Apr 1, 2022 at 11:34 AM GMT+5:30'. Below the extension details is a 'History' table with columns 'User', 'Date', and 'Action'.

User	Date	Action
Azure DevOps Service	3h ago	Updated version to 1.1.0
	3h ago	Installed

The installation is now complete.

Note: If you have already installed version 1.0.0, the extension will be automatically updated to the version 1.1.0.

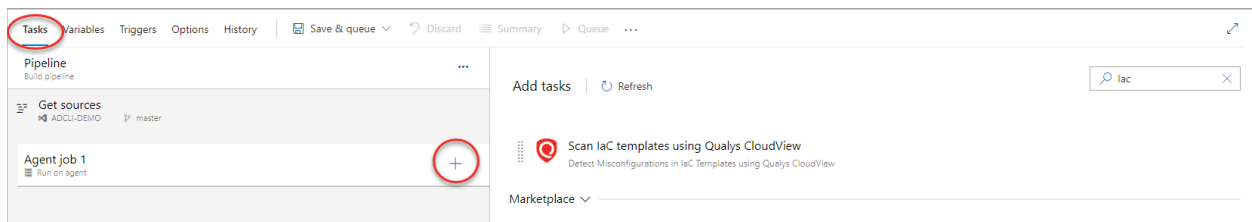
Configure the Extension

The Qualys IaC Security extension can be added as a task in your Build pipeline.

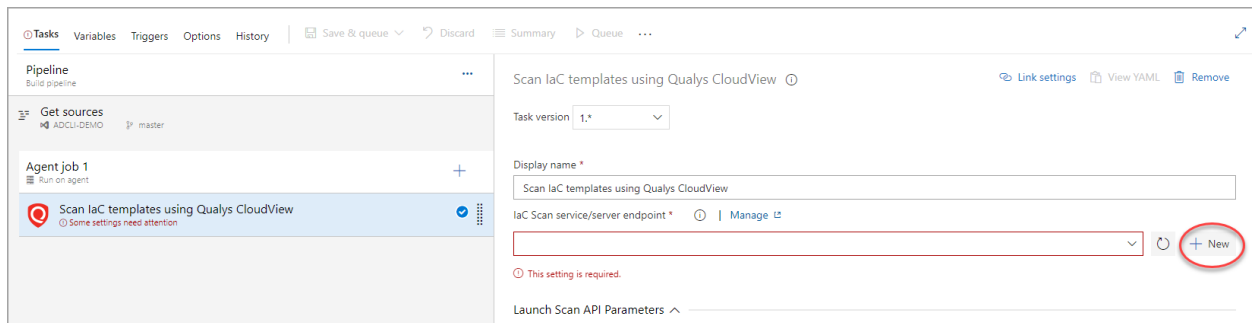
Configure the Extension for Build Pipelines Projects

You can use the Qualys IaC Security extension as a pre-deployment task in your project pipeline. After installing, you can see the Qualys IaC Security extension as a task in your pipeline.

In the **Tasks** tab, click **+** icon under your agent job, and search for **Scan IaC templates using Qualys CloudView**. Click **Add** to add the extension as a task in the build pipeline.

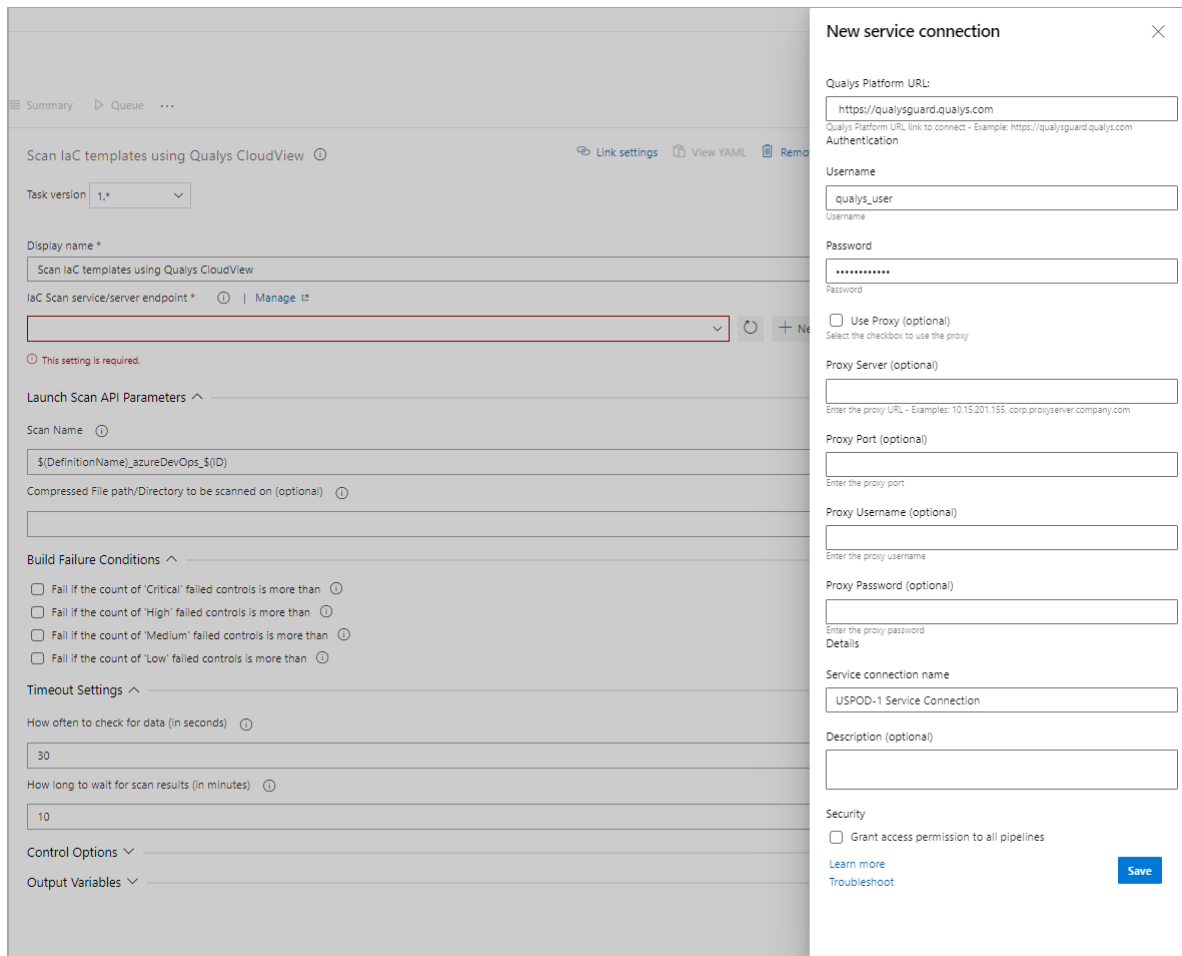


Click the task under the agent job to configure the extension.



After entering the display name, you need to provide the IaC scan service endpoint to connect to CloudView APIs. You can use the preconfigured IaC scan service endpoint or configure a new service endpoint.

To configure a new service endpoint, go to the **IaC Scan service/server endpoint** field and click **New**.



In the **New service connection** screen, enter the **Qualys platform URL**, **Username**, and **Password**. Provide a **Service connection name** and click **Save**. Once added, the service endpoint is listed in the **IaC Scan service/server endpoint** drop-down field.

Note: The Qualys platform URL that you use here depends on the Qualys platform your organization is using. To identify the platform URL, refer to [Identify your Qualys platform](#).

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

Launch Scan API Parameters

In the **Launch Scan API Parameters**, provide a scan name and file path or directory that you want to scan.



The Scan Name is populated automatically. By default, the scan name is `$(DefinitionName)_azureDevOps_$(ID)`. However, you can update the scan name.

Enter the file name or directory path to be scanned. If you do not specify the path, the entire repository is scanned.

Note: By default, `.tf`, `.yaml`, `.yml`, `.json`, and `.template` files in the directory are scanned. If you want to scan any compressed file, add the path and name of the compressed file. For example, `.zip`, `.7z`, `.tar`, `.tar.gz`, and `.gz`.

Build Failure Conditions

Configure the criteria to fail a build job based on the number of controls that failed for each severity.

Build Failure Conditions ^

Fail if the count of 'Critical' failed controls is more than ⓘ

Enter Count * ⓘ

2

Fail if the count of 'High' failed controls is more than ⓘ

Enter Count * ⓘ

3

Fail if the count of 'Medium' failed controls is more than ⓘ

Enter Count * ⓘ

1

Fail if the count of 'Low' failed controls is more than ⓘ

Enter Count * ⓘ

2

The build fails if the number of failed controls exceed the specified number for one or more severity types in scan results.

Timeout Settings

In the **Timeout** settings, specify the polling frequency in seconds for collecting the IaC scan result data. By default, it is set to 30 seconds.

Note: We recommend you to set this value to minimum 10 seconds.

You can also specify the timeout duration for a running scan. By default, it is set to 10 minutes.

Timeout Settings ^

How often to check for data (in seconds) ⓘ

30

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

10

Save the configuration and click **Queue** to run the pipeline.

Qualys IaC Scan Result

After the scan is complete, the **Summary** tab displays the details of the scan, such as the git repository that is scanned, errors (failures), scan time, and job details.

The screenshot shows the 'Summary' tab of a Qualys IaC Scan Result. It includes a 'Manually run by' section, repository and version information, time started and elapsed, related work items, and tests and coverage. Below this, there is an 'Errors' section with one error: 'Qualys IaC Security Failed due to the following reasons: -terraform checkType - Failed High controls count exceeded .terraform checkType - Failed Medium controls count exceeded .terraform checkType - Failed Low controls count exceeded Scan IaC templates using Qualys CloudView'. A 'Jobs' table at the bottom shows one job: 'Agent job 1' with a status of 'Failed' and a duration of '47s'.

To view the detailed IaC scan results, go to **Qualys IaC Scan Result** tab. The tab shows graphical data of cloud misconfigurations by criticality, number of controls causing build failure, and Pass/Fail Criteria Results Summary.

The screenshot shows the detailed view of the Qualys IaC Scan Result. It features a 'Cloud Misconfigurations (42)' donut chart with a legend: Critical (0), High (29), Medium (9), and Low (4). A 'Controls causing Build Failure' box displays '42 of 42 (Failed)'. Below these is a 'Pass/Fail Criteria Results Summary' table.

	Critical	High	Medium	Low
Criteria Evaluation	✓	✗	✗	✗

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

The Pass/Fail Criteria Result 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.

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 **IaC Posture** section displays the details of cloud misconfigurations, such as control IDs, name, criticality, result, file path, and resource.

Summary [Qualys IaC Scan Result](#)

Qualys

TERRAFORM CLOUDFOR...

Qualys CloudView IaC Posture

Show 10 entries Show Only: Criticality All

Control Id	Control Name	Criticality	Result	File Path	Resource
41	Ensure no security groups allow ingress from 0.0.0.0/0 to port 22	HIGH	FAILED	/security-group.tf	aws_security_group.project1-sg
42	Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389	HIGH	PASSED	/security-group.tf	aws_security_group.project1-sg
286	Ensure all data stored in the Launch configuration EBS is securely encrypted	HIGH	FAILED	/inputs_tf_files/main.tf	aws_instance.app_server
286	Ensure all data stored in the Launch configuration EBS is securely encrypted	HIGH	FAILED	/inputs_tf_files/whitelisted_files/main.tf	aws_instance.app_server
286	Ensure all data stored in the Launch configuration EBS is securely encrypted	HIGH	FAILED	/main.tf	aws_instance.app_server
289	Ensure every security groups rule has a description	LOW	FAILED	/security-group.tf	aws_security_group.project1-sg

The **Remediation** section displays the control IDs and associated remediation.

Summary [Qualys IaC Scan Result](#)

Qualys

TERRAFORM CLOUDFOR...

Remediation

Show 10 entries

Control Id	Remediation
41	Ensure aws_security_group or aws_security_group_rule resource does not have ingress cidr_blocks argument set to 0.0.0.0/0
42	Ensure aws_security_group or aws_security_group_rule resource does not have ingress cidr_blocks argument set to 0.0.0.0/0
286	Ensure aws_instance resource or aws_launch_configuration has encrypted argument set to True for the root_block_device
286	Ensure aws_instance resource or aws_launch_configuration has encrypted argument set to True for the root_block_device
286	Ensure aws_instance resource or aws_launch_configuration has encrypted argument set to True for the root_block_device
289	Ensure aws_security_group or aws_security_group_rule resource or aws_db_security_group or aws_elasticache_security_group or aws_redshift_security_group has description argument configured for the egress and the ingress objects.
301	Remove hard-coded secrets added to user data of EC2 Launch configurations
301	Remove hard-coded secrets added to user data of EC2 Launch configurations
301	Remove hard-coded secrets added to user data of EC2 Launch configurations
320	Ensure aws_athena_database resource has arguments encryption_option and kms_key configured for the encryption_configuration object.

You can download the published artifact file which has all the scan details in the JSON file format.

ADCLI / Azure_DevOps_Extension / Pipelines / Pipeline-GithubAction-Repo / 415 / Published artifacts

Search

← Artifacts

Published Consumed

Name	Size
Qualys_IaC_Extension_Artifacts	74 KB
Qualys_IaC_Scan_result_415.json	74 KB

What's New

Improvements in 1.1.0

We have added Qualys IaC Scan Result tab to the Summary that shows the IaC scan results. You can also view the IaC scan results for the jobs that were run before the extension upgrade to version 1.1.0.