



# Qualys Connector v1.5.0

Version 1.5.0

May 20, 2023

## What's new?

### Common Features

[Enhancements to the Connector Listing Page](#)

[New Cloud Perimeter Scan Period](#)

### Amazon Web Services

[Introduce Support for Snapshot Based Assessment for AWS](#)

[New Tokens](#)

**Qualys Connector 1.5.0 brings you improvements and updates! [Learn More](#)**

## Common Features

### Enhancements to the Connector Listing Page

The Connector listing page in the Connector application is improved with additional functionalities for existing columns. We have made the Assets/Resources column clickable.

- The Assets column redirects you to the CSAM/GAV app with your connector Assets listed. The list shows assets up to 30 days prior.
- The Resources column redirects you to the CloudView Resources tab with your account's resources listed.

**Note:** The asset column update only applies to AWS and Azure CloudType, as GCP CloudType only displays resources.

### New Cloud Perimeter Scan Period

We have introduced a new schedule for launching Cloud Perimeter Scans. You can run a Perimeter scan for your assets every four hours. This update applies to both on-demand and scheduled scans.

## Amazon Web Services

Listed below are the updates and features applicable to the connectors in both the Connector and TotalCloud applications.

### Introducing Support for Snapshot Based Assessment for AWS

Qualys is introducing a new agentless approach to vulnerability management to utilize Snapshot images of your instances for vulnerability assessments. The Snapshot assessment ensures scans over large volumes of data do not slow down your running workloads. Additionally, you can add multiple AWS accounts for snapshot scans, allowing you to perform large volumes of vulnerability scans together.

Snapshot Based Assessment is available in both Connector Application and TotalCloud Application.

#### Enable Snapshot Based Assessment for AWS

You will need two AWS accounts to avail Snapshot Based scan functionality. One is your registered service account and the other is your target account.

The pre-requisites for enabling Snapshot-based scans for Connectors can be found in the [Connector online help](#).

- 1) To enable Snapshot scans in Connector Application, start configuring an AWS connector in the target account.
- 2) Proceed with the connector creation steps until you reach **Tags and Activation**.
- 3) Select the **Automatically activate all assets for VM Scanning application** checkbox.
- 4) Select **Enable Zero-touch Snapshot Based Scan** (you will need to register a service account to check the box. [Learn more](#)).

← Edit: Target account connector

Edit Mode

Basic Details

Authentication Details

Region Selection

Tags and Activation

Assign Tags

Asset Tags and Activation

Activate and tag the discovered assets during scans on application.

Select Activation

☒ Automatically activate all assets for VM Scanning application
 

☐ Enable Zero-touch Cloud Perimeter Scan
 ☐ Enable Zero-touch API Based Scan ⓘ
 

☐ Enable Zero-touch Snapshot Based Scan ⓘ

☐ Automatically activate all assets for PC Scanning application
 ☐ Automatically activate all assets for SCA Scanning application
 ☐ Automatically activate all assets for CertView Scanning application

Select Asset Tags

Select Tags to automatically add the selected tags to the discovered assets.

+

Cancel

Save

## New Tokens

We have introduced the following new tokens for Connectors and TotalCloud to search for connectors with specified scan types.

**scanType.isCPSEnabled:** Use values true/false to find Connectors with Cloud Perimeter Scan type enabled.

**scanType.isInstantAssessmentEnabled:** Use values true/false to find Connectors with API-Based Scan type enabled.

**scanType.isSnapshotScanEnabled:** Use values true/false to find Connectors with Snapshot-Based scan type enabled.

## Issues Addressed

- We fixed an issue where the GCP Organization connectors were failing to create member connectors
- We fixed an issue where GCP member connectors were automatically going to a disabled state on the org connector run while fetching projects for selected folders from gcp
- We fixed an issue where the org connector was unable to create member connectors due to duplication of data in the backend
- We fixed an issue where the customer could not edit the Organization connectors of multiple cloud providers.
- We fixed an issue where GCP Org level connectors showed a timeout error when viewing folder listing.
- We have temporarily disabled the account reconciliation of deleted assets to stop the false termination of assets which triggers the purge rule. This may lead to a miscount of total running assets. Customers must manually purge assets in CSAM as a temporary solution until a permanent fix is deployed.
- We fixed an issue where running EC2 connectors changed the operating system of an asset in AssetView. The fix will be available as part of the Portal 3.15.1.0 release.