Qualys Cloud Platform v2.x

Release Notes

Version 2.37
March 13, 2019

Here’s what’s new in Qualys Cloud Suite 2.37!

AV AssetView

Activate EC2 Assets for CertView Scanning

SAQ Security Assessment Questionnaire

New User Permissions

WAS Web Application Scanning

Configure Email Frequency for Multi-Scan
Recommendation to Use Burp Extension for Burp Import
External References available for All

MD Malware Detection

Application to Delete Older Scans with no Detections

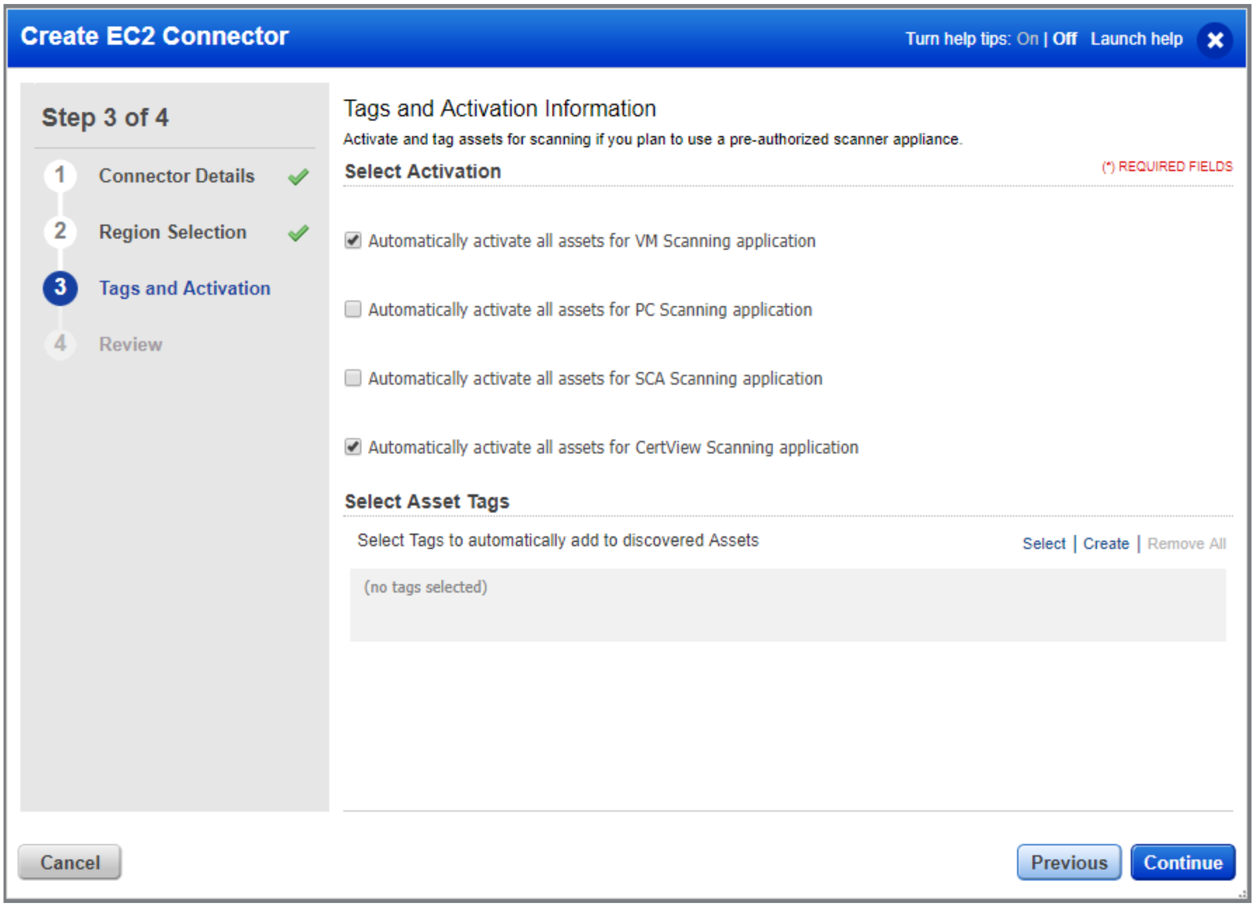
Qualys Cloud Platform 2.37 brings you many more Improvements and updates! **Learn more**

Activate EC2 Assets for CertView Scanning

We can now activate EC2 assets to automatically scan CertView Scanning application. Just configure the Tags and Activation within the EC2 connector wizard and we'll activate them automatically as they are discovered.

Simply go to AssetView > Connectors > AWS > Create EC2 Connector. In the Tags and Activation tab select the option: Automatically activate all assets for CertView Scanning application

Since this option has to go hand in hand with VM Scanning application we will pre-select the Automatically activate all assets for VM Scanning application option for you.



Tags and Activation Information

Activate and tag assets for scanning if you plan to use a pre-authorized scanner appliance.

Select Activation (*) REQUIRED FIELDS

☑ Automatically activate all assets for VM Scanning application

☐ 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 to discovered Assets

(no tags selected)

SAQ Security Assessment Questionnaire

New User Permissions

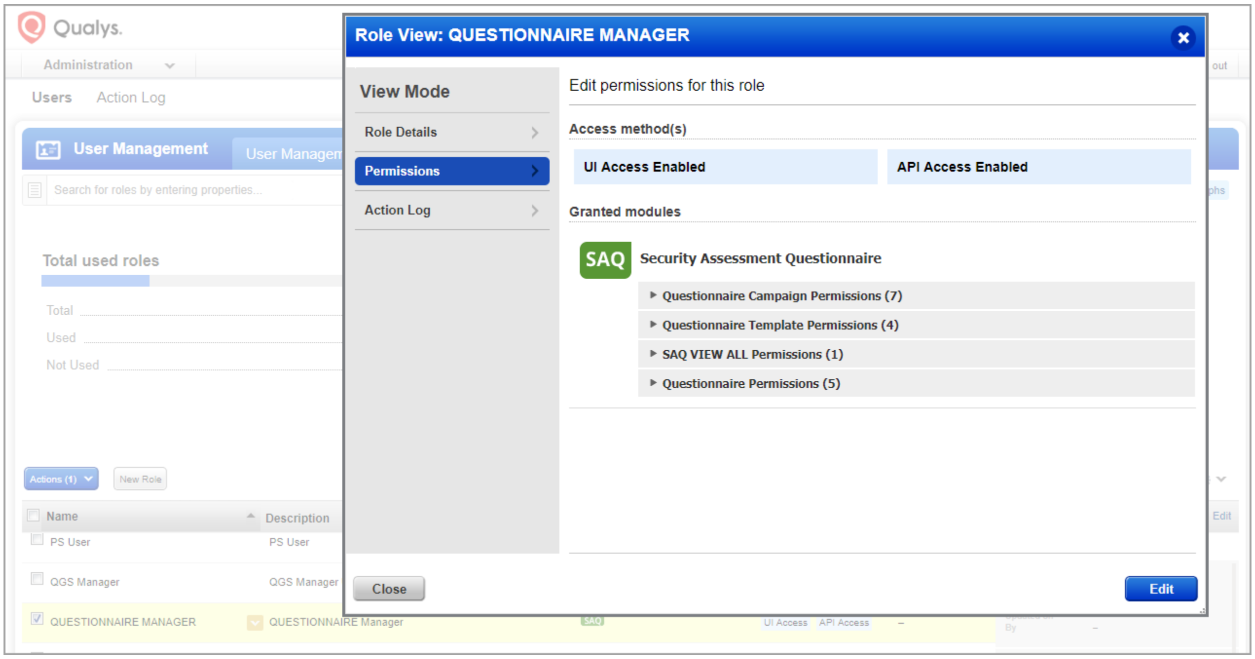
We have added new user permissions to help you better manage role based access control for various users in your subscription.

From the Administration Utility you can create custom roles to control which permissions should be assigned to a user with that role.

For example, a user can be given specific access to only to launch Campaigns but not create or publish templates. You can also choose to give permission to a user to view campaigns created by other users in your subscription.

Navigate to Module Picker > Utilities > Administration. Within the Administration utility, you'll find roles and their related permissions in the Role Management section.

Go to the Permissions tab to view all permissions assigned to the default Questionnaire Manager user.



Role View: QUESTIONNAIRE MANAGER

Edit permissions for this role

Access method(s)

UI Access Enabled | API Access Enabled

Granted modules

SAQ Security Assessment Questionnaire

- Questionnaire Campaign Permissions (7)
- Questionnaire Template Permissions (4)
- SAQ VIEW ALL Permissions (1)
- Questionnaire Permissions (5)

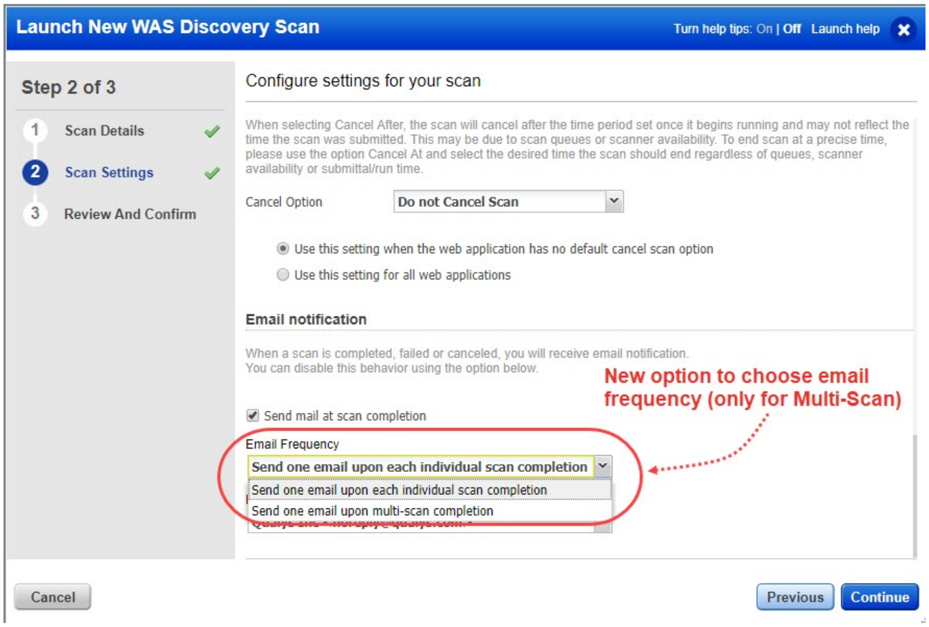
Configure Email Frequency for Multi-Scan

We have now introduced a new option for multi-scan where you can configure the frequency of notification email to be sent on completion of multi-scan. You could choose to send email after every scan is completed in multi-scan or completion of all scans in a multi-scan.

The new option Email Frequency is available only when:
-Scan involves multiple web applications (multi-scan)
-Email notification is enabled for the multi-scan

How do I configure the Email Frequency?

Go to Scans > Scan List and launch a new scan (discovery or vulnerability). When you enable Send mail at scan completion check box, you can choose one of the options in the Email notification frequency in Scan Settings.



Configure settings for your scan

When selecting Cancel After, the scan will cancel after the time period set once it begins running and may not reflect the time the scan was submitted. This may be due to scan queues or scanner availability. To end scan at a precise time, please use the option Cancel At and select the desired time the scan should end regardless of queues, scanner availability or submittal/run time.

Cancel Option: Do not Cancel Scan

● Use this setting when the web application has no default cancel scan option
○ Use this setting for all web applications

Email notification

When a scan is completed, failed or canceled, you will receive email notification.
You can disable this behavior using the option below.

☑ Send mail at scan completion

Email Frequency: Send one email upon each individual scan completion
- Send one email upon each individual scan completion
- Send one email upon multi-scan completion

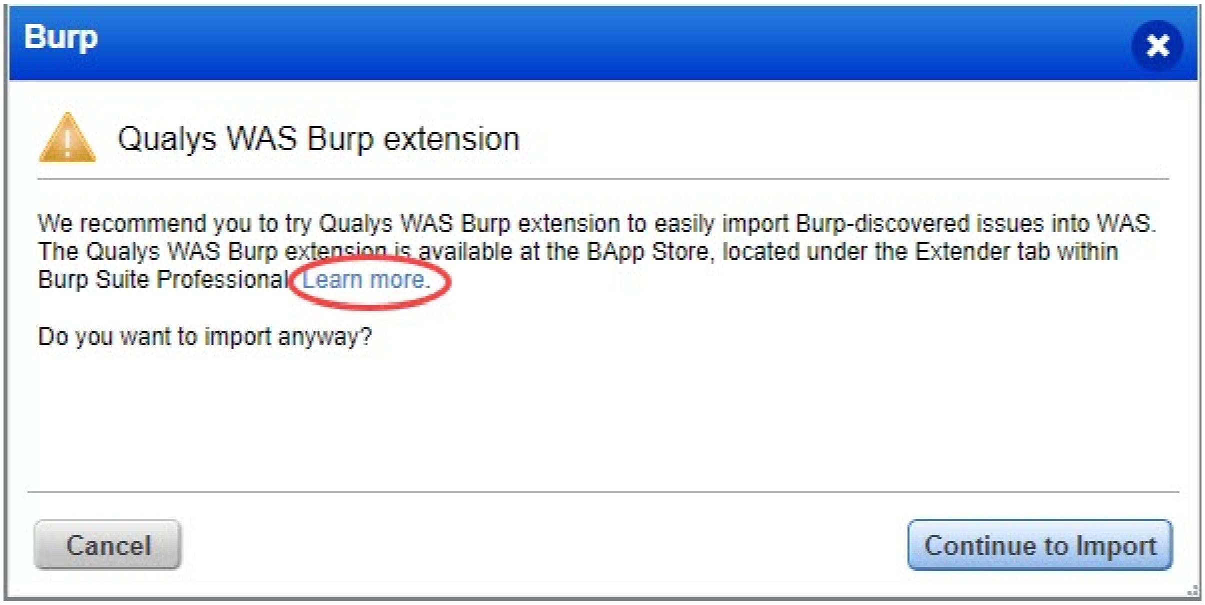
New option to choose email frequency (only for Multi-Scan)

The new option is available when you launch or edit a multi-scan and when you create or update a schedule.

Recommendation to Use Burp Extension for Burp Import

We recommend you to use the newly added Burp extension for Qualys WAS to import Burp issues. We have now added a new screen during Burp import steps that recommends you to use the Burp extension for Qualys WAS.

Go to Detections > Burp and click Import.



Qualys WAS Burp extension

We recommend you to try Qualys WAS Burp extension to easily import Burp-discovered issues into WAS. The Qualys WAS Burp extension is available at the BApp Store, located under the Extender tab within Burp Suite Professional. Learn more.

Do you want to import anyway?

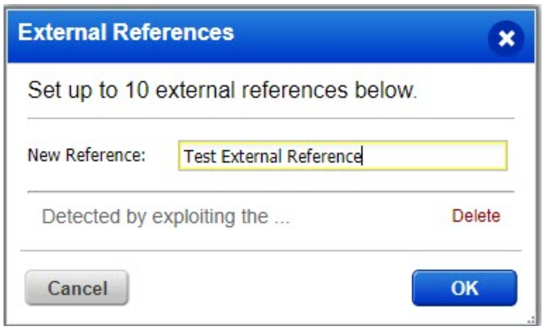
For more information on the extension and how to go about using the extension, click the Learn more link. Alternately, you could click Continue to Import and import Burp issues as supported in previous releases.

External References available for All

We have now made external references for QID available to all by default. You could add any external references such as IDs, comments or any other reference you want to associate with the QID. You can now add and view external references that are added to a QID or search for QIDs with specific external references.

Add External References

Go to Detections > Detection List, pick the QID you would want to add external references to and then select External References from the quick action menu. Type the content you want to add in New Reference and then click OK. You could add upto maximum 10 references for a QID. Use Delete link to remove the reference associated with the QID.



External References

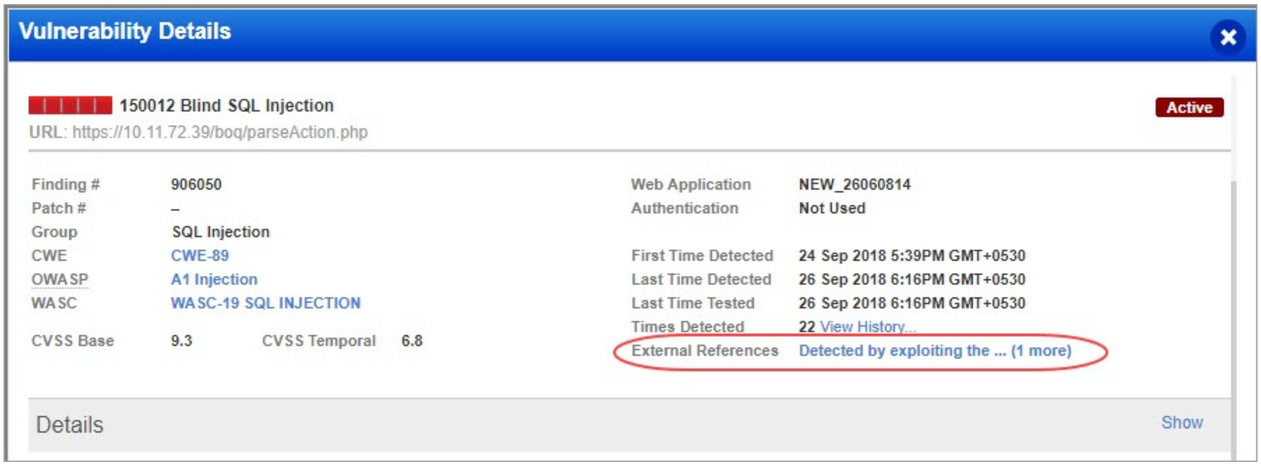
Set up to 10 external references below.

New Reference: Test External Reference

Detected by exploiting the ... Delete

View External References

To view the references associated with a QID, go to Detections > Detection List, pick the QID and then select view from the quick actions menu. The QID details now lists the external references associated with the QID. If there are multiple references, click more link to view all the references.



Vulnerability Details

150012 Blind SQL Injection

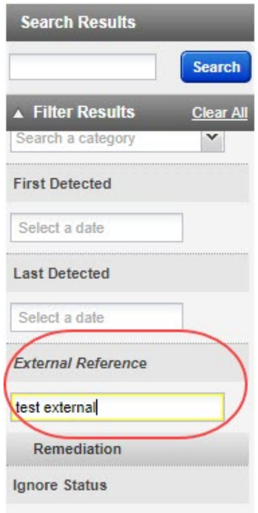
Active

URL: https://10.11.72.39/boq/parseAction.php

Finding #	906050	Web Application	NEW_26060814
Patch #	–	Authentication	Not Used
Group	SQL Injection		
CWE	CWE-89	First Time Detected	24 Sep 2018 5:39PM GMT+0530
OWASP	A1 Injection	Last Time Detected	26 Sep 2018 6:16PM GMT+0530
WASC	WASC-19 SQL INJECTION	Last Time Tested	26 Sep 2018 6:16PM GMT+0530
		Times Detected	22 View History...
CVSS Base 9.3	CVSS Temporal 6.8	External References	Detected by exploiting the ... (1 more)

Search External References

We have also added a new filter to ease your search for a QID using the external references you add to a QID.

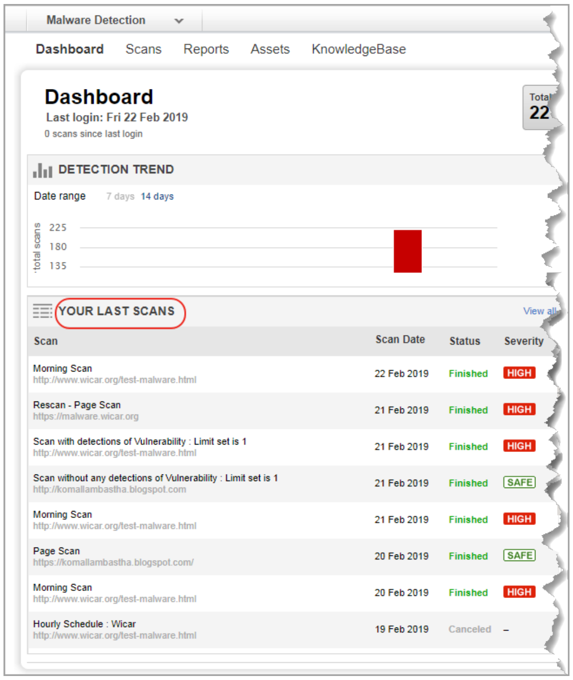


test external

Application to Delete Older Scans with no Detections

The Scans with no detections and that are older than a predefined period in days will get deleted automatically. Default settings are: delete scans older than 90 days for users with full subscription accounts, delete scans older than 60 days for trial accounts and delete scans older than 14 days for free accounts. Contact support to change the default value for deleting scans with no detections. Note that the scans with threats detected are saved for one year for all account types.

Deleted scans are not shown on the dashboard in "Your Last Scans" and on the scan list page. As the number of scans to be loaded are less after deletion, you may experience faster dashboard loading.

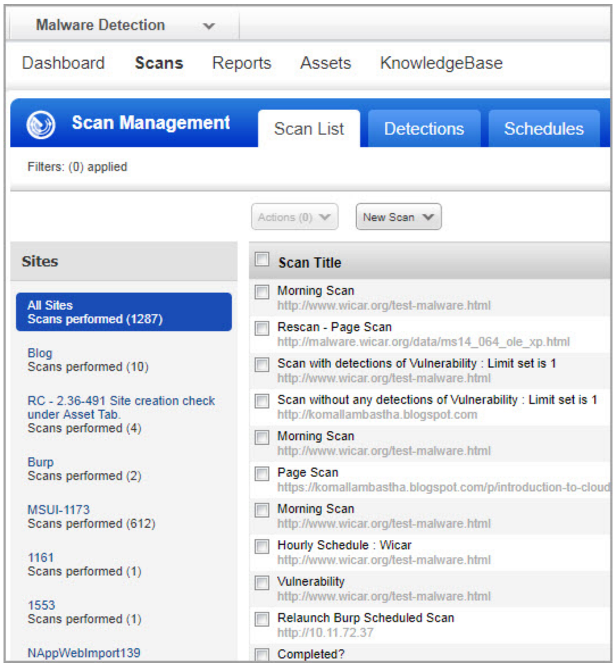


Dashboard

Last login: Fri 22 Feb 2019

0 scans since last login

Scan	Scan Date	Status	Severity
Morning Scan http://www.wicar.org/test-malware.html	22 Feb 2019	Finished	HIGH
Rescan - Page Scan https://malware.wicar.org	21 Feb 2019	Finished	HIGH
Scan with detections of Vulnerability : Limit set is 1 http://www.wicar.org/test-malware.html	21 Feb 2019	Finished	HIGH
Scan without any detections of Vulnerability : Limit set is 1 http://komallambastha.blogspot.com	21 Feb 2019	Finished	SAFE
Morning Scan http://www.wicar.org/test-malware.html	21 Feb 2019	Finished	HIGH
Page Scan https://komallambastha.blogspot.com/	20 Feb 2019	Finished	SAFE
Morning Scan http://www.wicar.org/test-malware.html	20 Feb 2019	Finished	HIGH
Hourly Schedule : Wicar http://www.wicar.org/test-malware.html	19 Feb 2019	Canceled	–



Filters: (0) applied

Sites

All Sites
Scans performed (1287)

Blog
Scans performed (10)

RC - 2.36-491 Site creation check under Asset Tab.
Scans performed (4)

Burp
Scans performed (2)

MSUI-1173
Scans performed (612)

1161
Scans performed (1)

1553
Scans performed (1)

NAppWebImport139

□ Scan Title
□ Morning Scan http://www.wicar.org/test-malware.html
□ Rescan - Page Scan http://malware.wicar.org/data/ms14_064_ole_xp.html
□ Scan with detections of Vulnerability : Limit set is 1 http://www.wicar.org/test-malware.html
□ Scan without any detections of Vulnerability : Limit set is 1 http://komallambastha.blogspot.com
□ Morning Scan http://www.wicar.org/test-malware.html
□ Page Scan https://komallambastha.blogspot.com/p/introduction-to-cloud
□ Morning Scan http://www.wicar.org/test-malware.html
□ Hourly Schedule : Wicar http://www.wicar.org/test-malware.html
□ Vulnerability http://www.wicar.org/test-malware.html
□ Relaunch Burp Scheduled Scan http://10.11.72.37
□ Completed?

Issues addressed in this release

Qualys Cloud Platform 2.37 brings you many more improvements and updates.

AV AssetView

TP Threat Protection

- The “vulnerabilities.vulnerability.exploitability” search token is no longer available in AssetView.
- Fixed an issue in AssetView where searching tags using underscore did not work.
- Fixed an issue in AssetView where the “Last Inventory” column for a Cloud Agent CSV report was appearing blank. The CSV report for Cloud Agent will now contain appropriate data in the “Last Inventory” column.
- Fixed an issue in AssetView where the “Activate” option under Actions was available even though a non-EC2 asset was part of multiple selection of assets for activation. The “Activate” option is now available only when all the selected assets are EC2 assets only.
- Fixed an issue in AssetView where clicking a live feed in the Threat Protection RTIs pane of Asset Details, displayed a blank page. Clicking the live feed will now take the user to the appropriate page.
- Fixed an issue in Threat Protection where the Threat Protection widget wasn't displaying for the user roles: Auditor, Malware Manger, WAS Scanner User, WAS Manager User, Unit Manager User, and Scanner User. The Threat Protection widget now displays for these roles.

CA Cloud Agent

- We fixed an issue on the Agents tab in the Cloud Agent UI where users were not able to sort the list by the Last Activity column.
- Scanned data by the SCA agent is now displayed appropriately in the Compliance tab.

VM Vulnerability Management

- The VM Dashboard help is updated to mention that the NOT operator can be used only with Asset search tokens. Vulnerability search tokens do not support the NOT operator.
- Fixed an issue in VM Dashboard where the tag search in Dashboard did not work.
- Fixed an issue in VM Dashboard, where an icon under the Detection Summary of Vulnerability Details was not displayed correctly.

SAQ Security Assessment Questionnaire

- We have updated the UI text to list all the file types supported as attachments in the questionnaire.
- Fixed an issue where a questionnaire in a Campaign in SAQ failed to open when clicked. The questionnaire now opens in a single click.

WAF Web Application Firewall

- We have updated the content of the downloaded data lists. The rules data list now shows the rule types in the Type column, new Status column to show the status of the rule as active/inactive. The appliance data list now also shows Platform of the appliance and Last Upgrade date.
- Now the View Details button for Exception and Virtual patch linked to a web application is visible to the sub-user only if the web application is in sub-user's scope.

WAS Web Application Scanning

- We have fixed an issue where Default DNS record (if configured from superuser web application), is now visible in scan configuration when same web application is scanned through sub-user's account.
- We have now enabled the cancel scan option even if the scan is in submitted state. Earlier, cancelling a submitted scan was not possible.
- We have now removed the fields: “First Time Detected”, “Last Time Detected”, and “Last Time Tested” from the downloaded scan report. Instead, it displays only “Detection Date” as per the online scan report.
- The customized dashboard when set to default is now correctly displayed as default dashboard. Previously, despite configuring custom dashboard as default, the Qualys configured default dashboard was displayed.
- We have now added a new error message for retest finding: “Retest cannot be done due to vulnerability age and recommend to purge the application and run a brand new scan.” The error message is displayed when the finding being retested is too old and the required data for retest is not available.
- We have now fixed the issue so that when you configure scanner pool (based on tags) to be used during the launch of a scan/schedule for a web application, the scan/schedule gets launched using the scanner appliance from the scanner pool (based on tags). Earlier, the scan/schedule was launched using an external scanner appliance.
- The Scan cancellation using cancelScansAfterNHours parameter now functions correctly through API.

Qualys Cloud Platform

- The “Click here to configure asset correlation” link is removed from the Configuration page of Threat Protection. This link is still shown on the Dashboard tab if no tags are included for correlation.
- Fixed an issue where the Asset Management & Tagging API (qps/rest/2.0/search/am/hostasset) did not return the element “Vulnsupdated”, which shows the dateTime on which the vulnerabilities were last updated for a host asset.
- The “View” option in CertView email templates is now changed to “View Request”.
- Fixed an issue in Continuous Monitoring where users were unable to remove a distribution group from the Notifications pane of the Monitoring Profile Creation wizard.