



Qualys Cloud Platform v3.x

Release Notes

Version 3.6

May 11, 2021 (Updated: May 19, 2021)

Here's what's new in Qualys Cloud Suite 3.6!

VMDR Vulnerability Management Detection and Response

[View Thread Feed List](#)

UD Unified Dashboard

[Zoom into View Count Card Details](#)

[Use Advanced Filters to Add Data to a Widget](#)

[Select Columns to Sort Data for a Widget](#)

SAQ Security Assessment Questionnaire

[User ID Hidden in Questionnaire Details for the Recipient](#)

WAS Web Application Scanning

[Assign System and Dynamic tags from the UI and API for the WAS](#)
(FORMAL DEPRECATION NOTICE)

MD Web Malware Detection

[Option to Delete WAS Managed Malware Detection Sites](#)

[Assign System and Dynamic tags from the UI for the MD](#)
(FORMAL DEPRECATION NOTICE)

Administration Module

[Global Option to Enable Geolocation](#)

Qualys Cloud Platform 3.6 brings you many more Improvements and updates! [Learn more](#)

View Thread Feed List

You can view the threat feed list right from VMDR module. Simply go to **Prioritization > Threat Feed**. The **Thread Feed** tab shows the High Rated Feeds, Medium/Low Rated Feed, and thread feeds marked as favorite by you.


You can use the and/or tokens combined with these tokens for searching a threat feed.

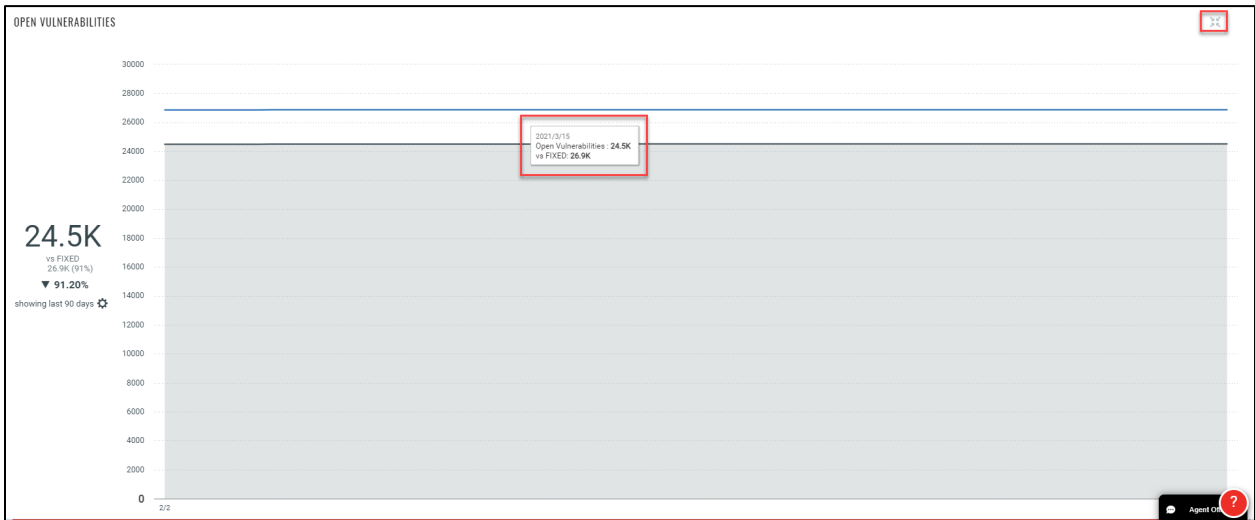
- categories
- contents
- publishDate

You can also save your search query and view the recent strings that you have searched. If you have saved search in Threat Protection, the same feed is shown on the **Thread Feed** tab. You can also filter the threat feeds using the Asset tags.

The screenshot shows the VMDR interface with the 'Prioritization' tab selected. The 'Threat Feed' sub-tab is active, displaying a search bar and filter options. Below the search bar, there are three main sections: 'HIGH RATED FEED' (398 items), 'MEDIUM / LOW RATED FEED' (34.9K items), and 'FAVORITES' (7 items). Each section contains a list of threat entries. The first entry in the 'HIGH RATED FEED' section is 'Google Chrome and Microsoft Edge Zero-day Remote Code Execution...' dated April 15, 2021, with 0 impacted assets. The first entry in the 'MEDIUM / LOW RATED FEED' section is 'PoC Exploit available for CVE-2021-27928' dated April 14, 2021, with 0 impacted assets. The first entry in the 'FAVORITES' section is 'PoC Exploit available for CVE-2020-14882' dated January 26, 2021, with 0 impacted assets.

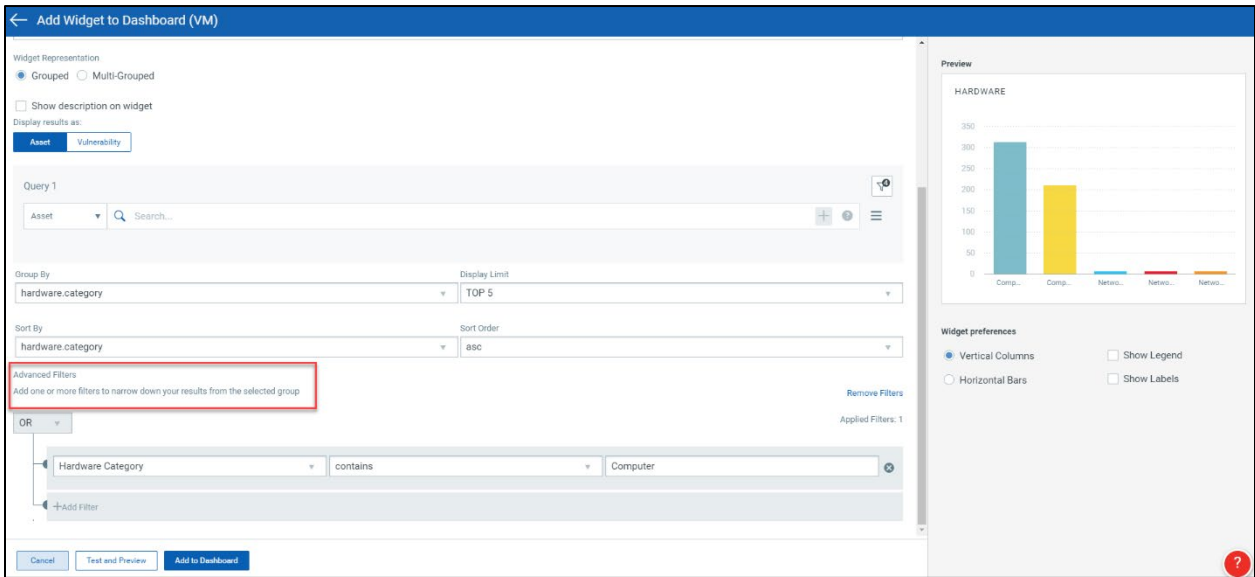
Zoom into View Count Card Details

You can now zoom into view details for the Count widget type. Simply clicking the zoom icon  on a widget card to view the trend lines clearly.



Use Advanced Filters to Add Data to a Widget

You can now add advanced filters for Table, Column, and Pie widget types. You can use one or more tokens to filter data displayed on a widget. If you add multiple token filters, the latest filter gets the precedence.



Select Columns to Sort Data for a Widget

You can now choose the columns by which you want to sort the data displayed on a widget. You can choose to display the data in an ascending or a descending order.

← Add Widget to Dashboard (VM)

Count Table Column Pie

Custom Count: Perform a mathematical operation such as Count, Min or Max. Supports comparison between multiple queries.

Name *

Hardware

Widget Representation:

☒ Grouped ☐ Multi-Grouped

☐ Show description on widget

Display results as:

Asset Vulnerability

Query 1

Asset Search...

Group By

hardware.category

Display Limit

TOP 10

Sort By

hardware.category

Sort Order

ASC

Advanced Filters

Add one or more filters to narrow down your results from the selected group

+ Add Filter

Preview

HARDWARE

300
250
200
150
100
50
0

Comp. Comp. Unide. Storage. Network. Network. Storage. System. Power.

Widget preferences

☒ Vertical Columns ☐ Show Legend

☐ Horizontal Bars ☐ Show Labels

SAQ

Security Assessment Questionnaire

User ID Hidden in Questionnaire Details for the Recipient

On the **Questionnaire** tab of the Security Assessment Questionnaire module, recipients can view and respond to the questionnaires assigned to them. Earlier, on this screen, right below the name of a questionnaire, the recipient could see the username and the user ID of the campaign manager who created a questionnaire for the recipient. From this release onwards, only the username of the campaign manager will be visible. For security reasons, we've decided not to show the user ID.

Qualys. Enterprise

Security Assessment Questionnaire

QUESTIONNAIRE

Questionnaire

7 Total Questionnaires

TIMEFRAME

Due within 2 wee... 0

Idle (No answers ... 7

Overdue 7

STATE

NAME STATE PROGRESS UPDATED DATE DUE DATE RISK RATING

Questionnaire for PCI Mandate Readin... In Progress 50% Apr 19, 2021 Apr 20, 2021 6 days overdue -

Created by John Rudman on Apr 19, 2021

Questionnaire for SCIT Conference Pr... In Progress 50% Apr 19, 2021 Apr 20, 2021 6 days overdue -

Created by John Rudman on Apr 19, 2021

GDPR Awareness Questionnaire In Progress 50% Apr 19, 2021 Apr 21, 2021 6 days overdue -

Created by John Rudman on Apr 19, 2021

Assign System and Dynamic tags from the UI and API for the WAS (FORMAL DEPRECATION NOTICE)

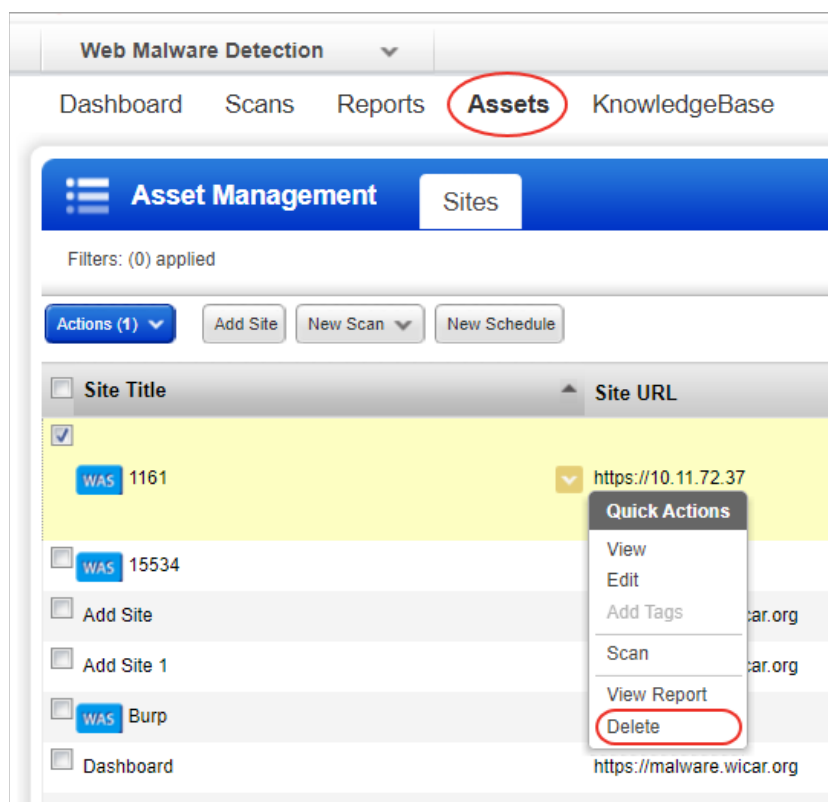
In the WAS module, you can now assign system and dynamic tags from the UI and API again. However, this is in violation of the defined Qualys Platform Tag behavior. Consider this as a formal deprecation notice. 60 days on, you will no longer be able to assign system and dynamic tags in the WAS module either from the UI and API.

Option to Delete WAS Managed Malware Detection Sites

With this release, the user with “Malware Manager “ role can now delete web sites that are enabled from WAS for Malware monitoring from the Assets tab. A new permission “MDS Asset Delete” is added. This permission will be assigned to Malware Manager user role by default. To assign this permission to other user roles, please contact Qualys Support.

When you delete a WAS managed web application from Web MD, the web site and its scan schedules are also deleted, and malware monitoring is disabled for the web application.

If you remove a WAS managed web application from subscription from WAS, then the we will delete the associated asset and its scan schedules from MD also.



Assign System and Dynamic tags from the UI for the MD (FORMAL DEPRECATION NOTICE)

In the Web Malware Detection module, you can now assign system and dynamic tags from the UI again. However, this is in violation of the defined Qualys Platform Tag behavior. Consider this as a formal deprecation notice. 60 days on, you will no longer be able to assign system and dynamic tags in the Malware Detection module from the UI.



Administration Module

Global Option to Enable Geolocation

We have now added an option for you to enable geolocation for widgets and maps across your subscription. Once you enable the geolocation option, it is enabled for all the users in your subscription.

Go to **Administration > Users > Defaults** and click **Edit** to enable the geolocation option.

The screenshot shows the Qualys Cloud Platform Administration interface. At the top, there is a navigation bar with 'Administration' and a dropdown arrow. Below this, there are tabs for 'Users' and 'Action Log'. The 'Users' tab is active, and within it, there are sub-tabs for 'User Management', 'Role Management', and 'Defaults'. The 'Defaults' sub-tab is selected. On the left side, there is a sidebar with 'Edit Setting' and a dropdown menu for 'Locale'. The main content area is titled 'Define user defaults values' and contains several settings. The 'Locale' section has two radio buttons: 'Use browser time zone' (selected) and 'Use custom time zone'. Below this is the 'CSV List Separator*' section, which has a text input field. The 'Geolocation' section has a text input field and a checkbox labeled 'Enable Geolocation', which is currently unchecked and highlighted with a red rectangle. At the top right of the main content area, there are 'Cancel' and 'Save' buttons.

By default, the **Enable Geolocation** option is disabled. The option is available to users who have permissions for the Administration utility.

Issues Addressed

We have fixed the following issues in this current release-

AV

AssetView

- We have now fixed an issue where the purge rule for GCP displayed "undefined" for its assets. It now correctly reflects the details instead of "undefined".
- We have now added a close button to the banner in AssetView.
- We now support drag and drop for system-based tags in AssetView. Prior to this release, system-based tags could not be dragged and dropped.
- Group-By Tag on an asset search query, click on the asset count and redirection to the asset search query failed. We have now fixed this issue so that the redirection asset details and redirection works successfully on Group-By Tag assets.
- We now support listing an asset via only NetBIOS name in Asset view.
- A user with VM and AV enabled for subscription displayed an error for asset activation from the AssetView module. We have now fixed the issue so that the assets are activated without any error being displayed for users.
- We have updated the "Support for EC2 Scanning" topic in the AssetView online help to include information about AWS assets: Status and behavior.

CA

Cloud Agent

- Fixed an issue where the installer downloaded for AIX was showing the rpm file. After this fix, a proper installer file with .bff.gz extension is getting downloaded.
- Fixed an issue where multiple agents were showing 'Provisioned' status with 'Pending Assignment' configuration for a long time.

VMDR

Vulnerability Management Detection and Response

- We have fixed an issue where if you downloaded the VM Scan Report in the CSV format, for some QIDs, the Solution Section format was not displayed correctly.
- We have fixed an issue where on a VM Dashboard, you could not search a tag that contained square brackets.
- We have fixed an issue where the Dashboard Trending stopped if you added the QID QQL token to the Dashboard.
- We have fixed an issue where the "threatIntelFacade" API request with the "remoteCodeExecution" token was showing null response.

UD

Unified Dashboard

- We have fixed an issue where if you tried to click on the VM dashboard widgets count, an error occurred. Also, if you tried to edit the same widget, a blank page was displayed.
- We have fixed an issue where on a VM dashboard, if you tried to create the same widget that was already on ITAM dashboard, the widget displayed no data. This issue occurred only if the ITAM widget was set for software tokens.
- We have fixed an issue where the Widget Query box did not expand to accommodate multi-line queries.

- We have rectified the image format for the GET action of web application report API from PNG to JPEG in WAS API User Guide.
- We have now fixed an issue where the scans failed due to an issue in password of authentication records. We have now fixed the issue so that the scan failure due to authentication record password is prevented.
- Some scans that are in "processing" status caused other scans to be blocked. We have now fixed an issue so that even if the current scan is in the "Processing" state, other scans in parallel are not blocked.
- Generating a scan report failed in the absence of a web application ID. We have now rectified the issue so that you can generate a scan report despite the absence of web application ID.
- When the performance attribute was updated using WAS API, despite successful response, the update was not reflected. We have now fixed the issue so that update of the performance attribute using Option profile API is correctly reflected.
- A web application report successfully generated using API, had report ID missing on the WAS UI and was not downloadable either. We have now fixed this issue so that the web application report generated from API reflects correct ID on the UI and is downloadable as well.
- We fixed an issue where the "WAS Finding Count API" returned an incorrect finding count when the user after tagging several applications used the Finding Count API to find the total number of findings for the tagged web applications. After the fix, the Finding Count API is returning a correct number of findings for the tagged web applications.
- We fixed an issue where the user was getting an error when trying to download a particular Scan Report using the API: "qps/rest/3.0/download/was/wasscan/<id>". After the fix, the WAS Scan report is downloadable from API.
- We fixed an issue where the Scan report in the XML format was not showing the body element under <REQUEST>. After the fix, the report in the XML and CSV format will now show the body element and the payload information in the SCAN report. The data in this body element in the Scan report in the CSV/XML format matches with the complete data shown in the PDF format of the report.
- We fixed an issue where the same vulnerabilities are flagged in different colors under the Web Applications tab and in the Web application Online Report. After the fix, the same vulnerabilities are flagged in the same colors under the Web Applications tab and in the Web application Online Report.

Qualys Cloud Platform

- During search query formation, pressing enter caused [and] operator to be automatically appended to the search query resulting in incorrect search query formation. We have now fixed an issue so that the [and] operator is not automatically appended to the search query.