



Qualys Cloud Platform v3.x

Release Notes

Version 3.8

September 21, 2021

Here's what's new in Qualys Cloud Suite 3.8!

VMDR Vulnerability Management, Detection, and Response

[In-app guided tours for better user assistance \(Beta\)](#)

AM AssetView

[Detection of Terminated Instances](#)

UD Unified Dashboard

[New Application Dashboard Template Library](#)

[Share Dashboard based on Asset Tags](#)

[Enhancements](#)

WAS Web Application Scanning

[Introducing a New Vulnerability Category "Potential Confirmed"](#)

Administration

[Updates to User Management](#)

Qualys Cloud Platform 3.8 brings you many more improvements and updates! [Learn more](#)



In-app guided tours for better user assistance (Beta)

You can now use the in-app guided tours to learn about various features and how to use them. The guided tours provide step-by-step help, ensuring optimum user assistance within the app. Currently, this feature is Beta and is available only for VMDR.

To launch a guided tour, click  on the VMDR Home page and choose a specific topic to start with the step-by-step help.

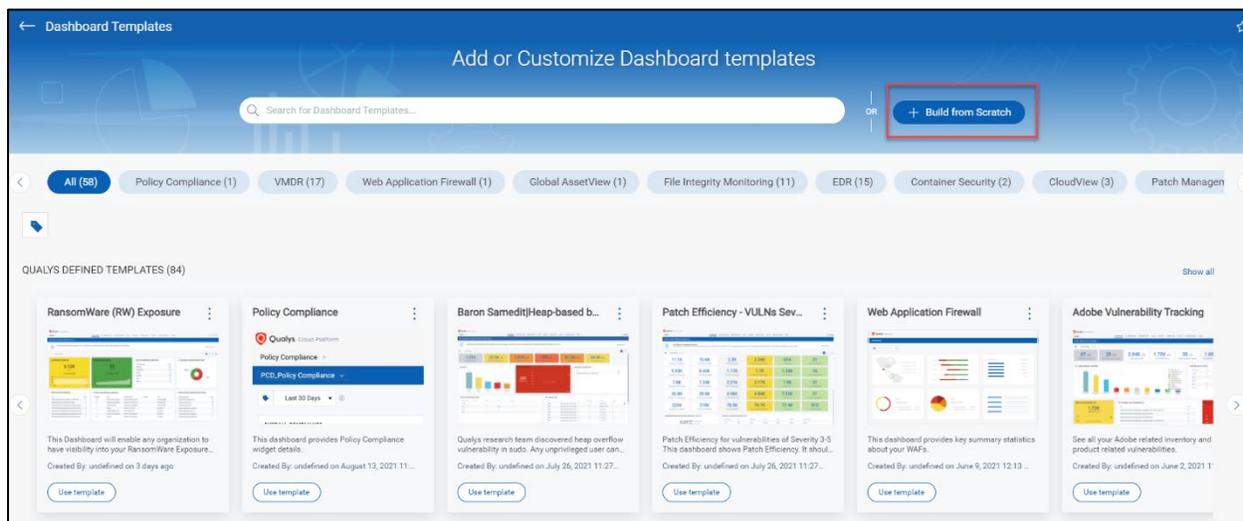
Detection of Terminated Instances

Currently, in AssetView, the connectors for Amazon Web Services (AWS) did not process terminated (any instance in a terminated state when discovered), AutoScaling, and EMR instances. We have now changed this behavior so that the terminated, AutoScaling, or EMR instances in the AWS cloud are detected by our connectors. The detection of such assets is also reflected in the asset inventory.

During our connector run, the asset inventory will now update to include instances that are in the terminated state. The instances exist in our asset inventory only till the time the instances exist in the AWS cloud environment.

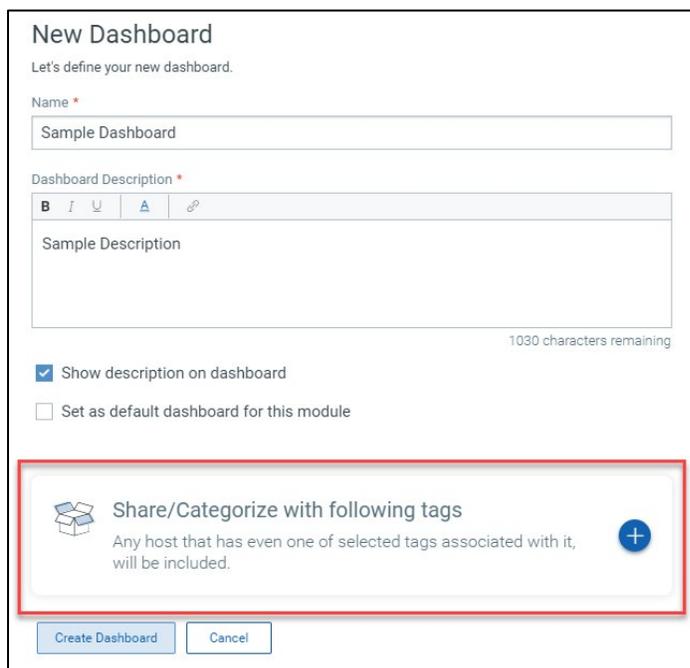
New Application Dashboard Template Library

The Dashboard library allows you to create your dashboard using existing widget templates, customize existing widgets or create your widgets to suit your need. The templates are segregated based on the subscription to other Qualys products.



Share Dashboard based on Asset Tags

You can restrict users from viewing your dashboard based on user tags. While creating a dashboard using a template or creating it from scratch, you can select the asset tags for the dashboard. Only the users who have permissions to the asset tags can view the dashboard.



Enhancements

The following enhancements have been added for the Unified Dashboard:

- You can now add static values for the Count Ratio widget while comparing queries.
- Ratio values for Count widgets are now supported.
- For the Column and Pie type of widgets, you use the color library to assign custom color schemes for the data.
- While creating a VMDR widget, you can customize the color mapping for the predefined values of these tokens for some token values in the Group By menu.

Introducing a New Vulnerability Category “Potential Confirmed”

The KnowledgeBase has vulnerabilities that may be confirmed in some cases and not confirmed in others because of various factors affecting scan results. With this release, we will show the severity level of such vulnerabilities as half red/half yellow in the KnowledgeBase. These QIDs are also known as Potential Confirmed Vulnerability.

Dashboard Web Applications Scans Detections Reports Configuration KnowledgeBase

KnowledgeBase KnowledgeBase

Search Results Actions (0) 1 - 165 of 165

SSL	Search	QID	Name	Information	Category	Severity
		38139	SSL Server Has SSLv2 Enabled Vulnerability	+	General remote services	Half Red / Half Yellow
		38140	SSL Server Supports Weak Encryption Vulnerability	+	General remote services	Half Red / Half Yellow
		38141	SSL Server May Be Forced to Use Weak Encryption Vulnerability	+	General remote services	Half Red / Half Yellow
		38142	SSL Server Allows Anonymous Authentication Vulnerability	+	General remote services	Half Red / Half Yellow
		38143	SSL Server Allows Cleartext Communication Vulnerability	+	General remote services	Half Red / Half Yellow

Filter Results: Identification, Severity Level, Scan Information, Exploit Information, CVSS V3 Information

QIDs with the half red/half yellow severity match both confirmed and potential. That means these QIDs would match search lists for both confirmed and potential.

Dynamic Search List View: Confirmed Vulnerabilities with severity 1-5

View Mode: List Details, Search Criteria, QID List, Comments, Action Log

Review QIDs included in this list

Status	QID	Title	Severity
	38168	SSL Certificate - Future Start ...	Half Red / Half Yellow
	38169	SSL Certificate - Self-Signed ...	Half Red / Half Yellow
	38170	SSL Certificate - Subject Com...	Half Red / Half Yellow
	38173	SSL Certificate - Signature Va...	Half Red / Half Yellow
	38284	Netscape/OpenSSL Cipher F...	Red

Dynamic Search List View: Potential Vulnerabilities with severity 1-5

View Mode: List Details, Search Criteria, QID List, Comments, Action Log

Review QIDs included in this list

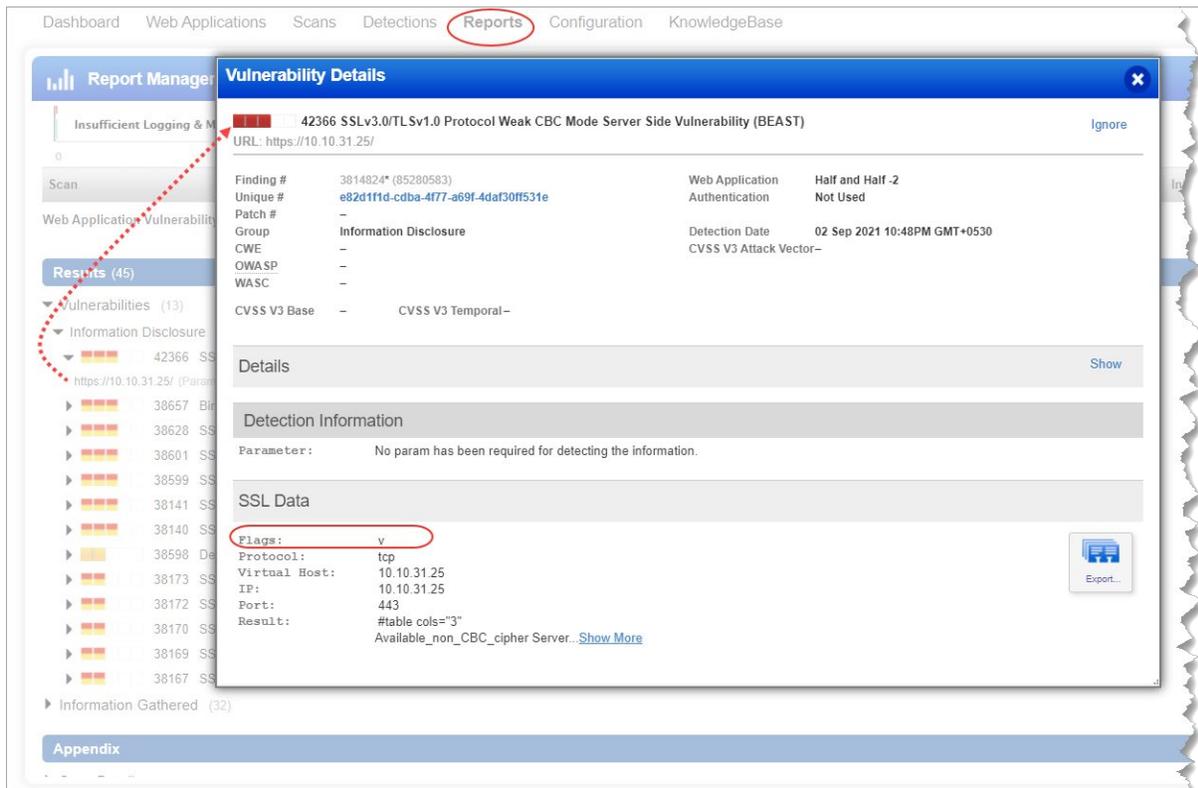
10829	Drupal News Message HTML ...	CGI	Half Red / Half Yellow
11556	Zen Cart Multiple Security Vul...	CGI	Half Red / Half Yellow
11933	Drupal Multiple Security Vuln...	CGI	Half Red / Half Yellow
12265	WordPress user_login Colum...	CGI	Half Red / Half Yellow
12460	WordPress XML-RPC Remot...	CGI	Half Red / Half Yellow
12598	WordPress Multiple Cross-Sit...	CGI	Half Red / Half Yellow
38167	SSL Certificate - Expired	General remote services	Half Red / Half Yellow
38168	SSL Certificate - Future Start ...	General remote services	Half Red / Half Yellow
38169	SSL Certificate - Self-Signed ...	General remote services	Half Red / Half Yellow
38170	SSL Certificate - Subject Com...	General remote services	Half Red / Half Yellow
38173	SSL Certificate - Signature Va...	General remote services	Half Red / Half Yellow
38477	SSL Insecure Protocol Negoti...	General remote services	Half Red / Half Yellow
38592	Server Supports SSLv2 Proto...	General remote services	Half Red / Half Yellow
38606	SSL Server Has SSLv3 Enabl...	General remote services	Half Red / Half Yellow

Page 1 of 10 Displaying 1 - 20 of 197

Copy All QIDs Save As.. Edit

If our service confirms the vulnerability during a scan, it appears as a red vulnerability in the finding. If it cannot be confirmed, it appears as a yellow potential vulnerability in the finding. This change primarily impacts TLS/SSL QIDs. We set a “v” value in the **Flags** fields if a finding of a Potential Confirmed QID is confirmed.

The sample scan report shows the Potential Confirmed QIDs as half red/half yellow; when you click any of the findings of the QID, we show the category as potential or confirmed.



When our service fetches the QIDs from the KnowledgeBase, we show Potential Confirmed QIDs as half red/half yellow, such as in search lists, option profiles with detection categories as TLS/SSL Certificate, and scans when we view QIDs included in a scan. But you will see these QIDs as either confirmed or potential vulnerabilities when we show them as detections.

If the scan result has a Potential Confirmed QID and if you create a dynamic search list to filter confirmed vulnerabilities and add that search list to the exclusion list when generating a report, we will exclude only the confirmed findings of the QID from the scan report. The potential findings of the QIDs are not excluded. In the case of a static search list, if you include a Potential Confirmed QID in the list and add the search list to the exclusion list, we will remove the QID and all its findings irrespective of their finding types from the scan report.



Administration

Updates to User Management

We have made minor updates to the User Management screen of the Administration app. The changes are listed below:

- **Number of Rows** to be displayed: We have removed 100 and 200 options from the Number of rows to be shown on the screen. We now support only 20 or 50 users to be displayed on one page.
Note: We are working on improving performance for the options that we have removed for now.
- **Sort by Modules:** We have removed the Sort by Modules option for better sorting of users. The other sort options are available: Username, First Name, Last Name, Email Address, Last Update Date, Last Login Date.
- **New Data Columns in CSV download:** We have now added new columns of user data when you download the user's list in CSV format. The new columns that we added are: Modules, Roles, Tags, Scope, and Status.

	A	B	C	D	E	F	G	H	I	J
1	ADMIN Us	21 Sep 20		28						
2	Info1	Sector 63	California	XYZ	54321	USA				
3	John Doe	nf_mt11	CM User,	VM User						
4	Username	First Name	Last Name	Email Address	Modules	Roles	Tags	Scopes	Status	
5	nf_aa3	john	doe	ldoe@example.com	ASSET, ITAM, CA, VM, PV	ADMINISTRATOR	Unassigned Business U	Default Dashboard Access Tag, Clou	ACTIVE	
6	nf_aa4	john	doe	ldoe@example.com	ASSET, ITAM, CA, VM, PV	CM User, VM User, UNI	all_BU	Default Dashboard Access Ta	ACTIVE	
7	nf_aa5	john	doe	ldoe@example.com	Admin, ASSET, ITAM, CA, CM	User	Unassigned Business Unit		ACTIVE	
8	nf_ag7	Adam	Gilly	jdoe@example.com	ASSET, ITAM, CA, PM, CO	VM User, CM User, AU	Unassigned Business U	Unassigned Business Unit, Default D	ACTIVE	
9	nf_an	Auditor	New Issue	jdoe@example.com	ASSET, ITAM, CA, PM, CO	AUDITOR, CM User	Unassigned Business Unit		ACTIVE	
10	nf_an1	Administr	New	jdoe@example.com	Admin, ASSET, ITAM, CA, CM	User, Administratic	Unassigned Business U	Default Dashboard Access Tag	ACTIVE	
11	nf_as4	Auditor	11787	jdoe@example.com	ASSET, ITAM, CA, PM, CO	CM User, AUDITOR	Unassigned Business U	Default Dashboard Access Tag	ACTIVE	
12	nf_au	Auditor	User	jdoe@example.com	ASSET, ITAM, CA, PM, CEI	PC/SCA User, VM User	Unassigned Business U	Default Dashboard Access Tag	ACTIVE	
13	nf_bb	Boom	Boom	jdoe@example.com	ASSET, ITAM, CA, VM, PV	PC/SCA User, SCANNER	Unassigned Business U	Default Dashboard Access Tag	ACTIVE	
14	nf_du	Dashboar	User	jdoe@example.com	ASSET, ITAM, CA, VM, PV	CM User, VM User, SCA	Unassigned Business U	Default Dashboard Access Tag	ACTIVATION	
15	nf_mt11	Mohit	Tester	aporwal@example.com	Admin, ASSET, ITAM, CA, VM	User, CM User	Unassigned Business Unit		ACTIVE	
17	nf_pc2	Pointing	Clark	jdoe@example.com	ASSET, ITAM, CA, PM, CO	PC/SCA User, AUDITOR	Unassigned Business U	Default Dashboard Access Tag	ACTIVATION	
22	nf_rr	Read	Reader	jdoe@example.com	ASSET, ITAM, CA, VM, PV	PC/SCA User, READER,	Unassigned Business U	Default Dashboard Access Tag	ACTIVE	
23	nf_rr1	Reed	Reader 1	ldoe@example.com	ASSET, ITAM, CA, VM, PV	PC/SCA User, CM User,	Unassigned Business U	Default Dashboard Access Tag	ACTIVATION	

Issues Addressed

AM AssetView

- We fixed an issue where you could not update the Azure connectors by using the API.
- We fixed an issue where if the password contained a colon (:), API endpoint authentication failed.
- We fixed an issue where the terminated instances which no longer existed in AV Azure cloud were incorrectly shown as running.
- We fixed an issue where the terminated instances which no longer existed in AWS cloud were incorrectly shown as running.
- We fixed an issue where the UI showed a generic error message if you created a connector with an existing Tenant ID.

VMDR Vulnerability Management, Detection, and Response

- We fixed an issue where the documentation did not mention that the fixed vulnerability filters are not applicable for the QID token.

UD Unified Dashboard

- We fixed an issue where the data on the second page of a downloaded dashboard was not reflecting correct data on the Firefox or Safari browsers.
- We fixed an issue where the widget's position was not retained after you rearranged the widgets.
- We fixed an issue where you could not sort widget data in an ascending or descending order for vulnerability tokens.
- We fixed an issue where if you used ampersand (&) in the widget title, the word amp was repeated multiple times in the title while hovering on the graph of the saved widget.
- We fixed an issue where the dashboard widget size increased five times while using the Edit Dashboard Layout option.

CA Cloud Agent

- We fixed an issue where the query containing `aws.ec2.hasAgent:"false"` was not showing the correct result.
- We fixed an issue where 'OTHER_ERROR' was displayed when the performance settings tags were not provided in the `/qps/rest/1.0/update/ca/agentconfig/` endpoint.
- We fixed an issue where the `/qps/rest/2.0/get/am/hostasset/` API call was returning multiple vNIC for Oracle assets even if a single vNIC was installed on the system.



Administration

- We have now fixed an issue during the download of the user's list in the User Management tab of the Admin app.