



Qualys Cloud Platform v3.x

Release Notes

Version 3.3

November 12, 2020

Here's what's new in Qualys Cloud Suite 3.3!

AV

AssetView

New Regions Supported for AWS Connectors

Purge Cloud Agent and GCP Assets

VMDR

Vulnerability Management Detection and Response

New Count Widget Card

Enhanced Multi-Grouped Table Widget

Token Updates

CVE Details for Vulnerabilities in CSV

UD

Unified Dashboard

New Templates for Dashboards

Hover and View Count Value in Widget

New Widgets for AssetView Discontinued from Widget Builder

SAQ

Security Assessment Questionnaire

Support for Campaign Scheduler

Support for Campaign Creation from VENDORS Tab

WAS

Web Application Scanning

Added Custom Attributes Information to Reports

Added New Search List "Core QIDs" and Option to Copy QIDs

Ability to Filter Catalog Entries using Wildcards in IP Address

Qualys Cloud Platform 3.3 brings you many more Improvements and updates! [Learn more](#)

New Regions Supported for AWS Connectors

During the connector creation process, you can now select the newly supported regions and start discovering assets from each region. The newly supported regions are Europe (Milan) eu-south-1 and Africa (Cape Town) af-south-1.

Purge Cloud Agent and GCP Assets

You can define purge rules to automatically purge GCP assets and cloud agents based on the criteria you define. When you purge an asset you remove the asset and the data associated with it.

We have now enabled the “Purge cloud agent assets matching criteria” option for GCP to remove the cloud agent and its license for matching assets.

The screenshot displays the 'Purge Rule Creation' dialog box, currently on 'Step 2 of 4: Rule Definition'. The interface includes a sidebar with four steps: 1. Rule Details (checked), 2. Rule Definition (active), 3. Purge Limits, and 4. Review And Confirm. The main area is titled 'Rule Definition' and contains the following elements:

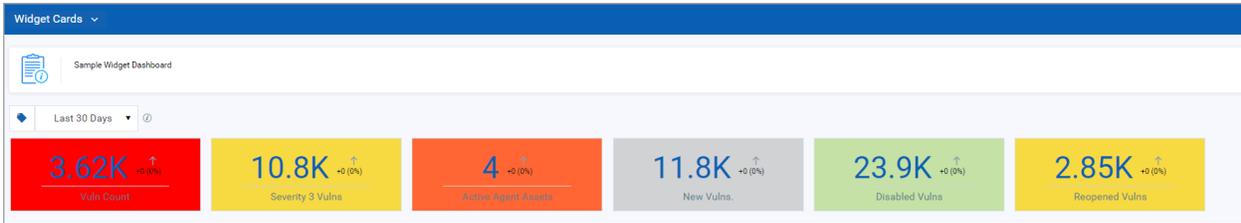
- A header: 'Add criteria to permanently remove cloud based assets' with a red asterisk and '(*) REQUIRED FIELDS'.
- A sub-header: 'All matching assets will be purged'.
- A filter section titled 'Cloud Provider Metadata Based Filter' with a 'Remove' button.
- Instructions: 'Select a cloud provider and choose rule criteria.'
- A dropdown for 'Assets match all of the following conditions for' set to 'GCP'.
- A filter rule: 'gcp.compute.zone' IN 'europe-west4-a'.
- A checkbox labeled 'Purge cloud agent assets matching criteria' which is currently unchecked. Below it, a note states: 'When selected, we will remove the asset, the cloud agent and its license from your subscription.'
- An 'Add Criteria' button with a plus icon.

At the bottom of the dialog, there are three buttons: 'Cancel', 'Previous', and 'Continue'.

New Count Widget Card

We have now introduced widget cards that display count of the data. The count widget cards are compact in size to give you a quick glance of the data point to be monitored.

Due to its compact size, you can accommodate more widgets and data in a dashboard.



How to Create a Count Widget Card?

On the dashboard, click the **Add Widget** button. In the widget builder, select **Vulnerability Management** application from the left pane and click **Create Widget**.

Choose the **Count** Widget Type. Provide a name for the widget that is displayed on the widget below the count.

Choose Summary as the Widget Representation.

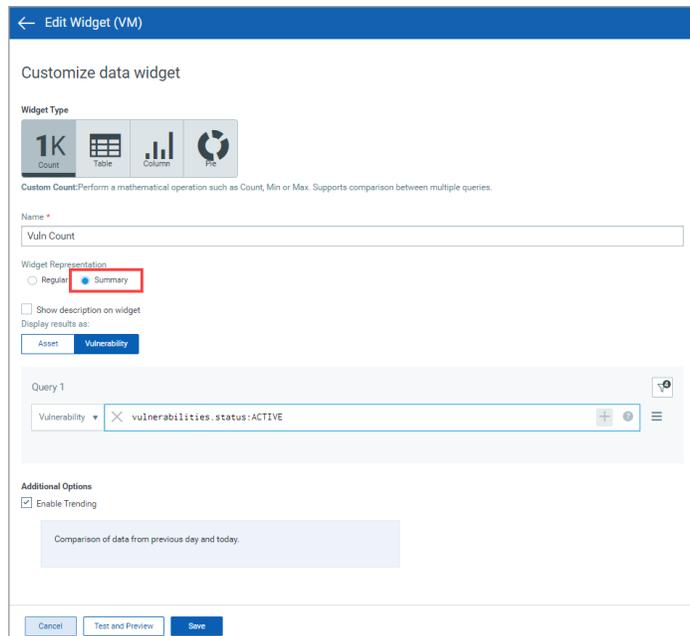
Define the search query to populate the data in the widget.

The widget card also displays trending data as comparison of data from previous and today. If there is no change in data, the trend is displayed as 0 percent.

Because the widgets are compact, you cannot resize the widget.

You can view the preview of the widget and configure the parameters as per your requirement. Click **Add to Dashboard** to complete widget creation and view the widget on the dashboard.

Example: Count of Vulnerabilities detected.



Enhanced Multi-Grouped Table Widget

We have enriched our table widget builder with new options to give you the flexibility to view grouped or ungrouped data in a table widget. With Multi-grouped table widget, you can not only monitor multiple data points in a single widget, but also choose to represent the multiple data points in a grouped or ungrouped manner.

Note: The enhanced table widget options are available only for Vulnerability Management app.

When you create Multi-Grouped Table Widget, choose from the new options that we provide for the data representation you want in the table.

← Add Widget to Dashboard (VM)

Customize data widget

Widget Type

1K Count | **Table** | Column | Pie

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

Name *

Vulnerability Data

Widget Representation

Simple List Grouped Multi-Grouped

Data Representation

Expanded Collapsed

Note: Toggle between Collapsed and Expanded to view information as grouped or ungrouped in your tables.

Show description on widget

Display results as:

Asset | **Vulnerability**

- **Expanded:** The data points you choose to add in the widget are ungrouped to be listed as separate columns in the table widget.

The values of data points selected through Group By 2 and Group By 3 fields are added as separate columns in the table. For example, if you choose to the table to grouped by Type Detected, Severity (Group 2), and Status (Group 3). The values for Type Detected (Confirmed, Potential) are listed as rows in the table, while the values for Severity (Severity 1, Severity 2, and so on) and Status (Re-opened, Active, Fixed) are listed as separate columns in the table.

TYPE DETECTED	Group By 2 Columns in Expanded Form					Group By 3 Columns in Expanded Form			
	SEVERITY 1	SEVERITY 2	SEVERITY 3	SEVERITY 4	SEVERITY 5	NEW	REOPENED	ACTIVE	FIXED
Confirmed	-	33	78	187	123	-	-	421	-
Potential	4	1	2	2	-	-	-	9	-

- **Collapsed:** The data points you choose to add in the widget are ungrouped to be listed as separate columns in the table widget.

The data points selected through Group By fields are added as columns in the table. For example, if you choose to the table to grouped by Status, Severity (Group 2), and Type Detected (Group 3). The data points Severity and Type Detected are grouped as columns in the table.

The screenshot shows a table widget titled 'COLLAPSED WIDGET'. The table has four columns: 'STATUS', 'SEVERITY', 'TYPE DETECTED', and 'COUNT'. The 'SEVERITY' column is labeled 'GroupBy 2' and the 'TYPE DETECTED' column is labeled 'GroupBy 3'. The data is as follows:

STATUS	SEVERITY	TYPE DETECTED	COUNT
ACTIVE	4	Confirmed	187
ACTIVE	5	Confirmed	123
ACTIVE	3	Confirmed	78
ACTIVE	2	Confirmed	33
ACTIVE	1	Potential	4
ACTIVE	3	Potential	2
ACTIVE	4	Potential	2

Token Updates

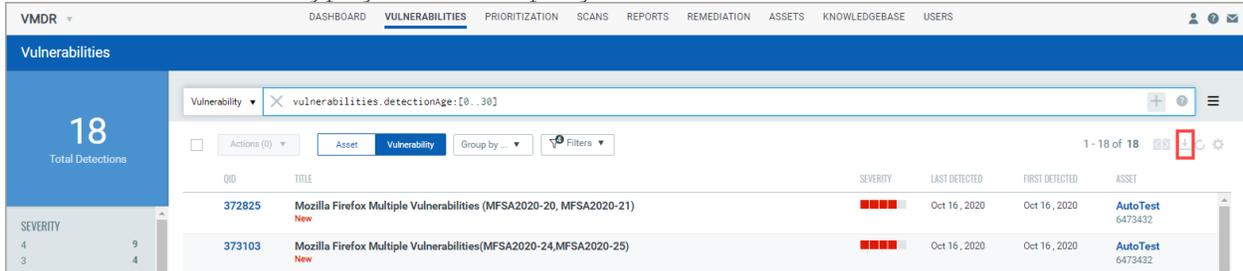
We have updated the names of vulnerabilities.vulnerability.cvssInfo.* tokens for better clarity.

Old Token Name	Updated Token Name
vulnerabilities.vulnerability.cvssInfo.accessVector	vulnerabilities.vulnerability.cvss2Info.accessVector
vulnerabilities.vulnerability.cvssInfo.baseScore	vulnerabilities.vulnerability.cvss2Info.baseScore
vulnerabilities.vulnerability.cvssInfo.temporalScore	vulnerabilities.vulnerability.cvss2Info.temporalScore

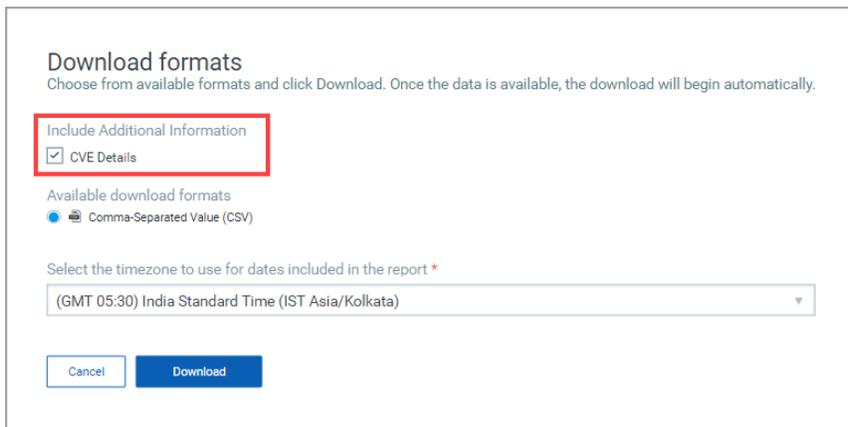
CVE Details for Vulnerabilities in CSV

You can now choose to include additional information about CVE details for a vulnerability when you download vulnerability details in CSV format.

On Vulnerabilities tab, type your search query and click Download icon.



The Download formats dialog box is displayed. To include the CVE information in the CSV file, select the **CVE Details** check box and click **Download**.



The CSV file is downloaded with CVE details.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
1	Asset Vuln	12 Nov 2020	18																		
2	qualys	Sample	sample	None	34343	India															
3	Joh Doe	User_john	CA MANAGER	Global AI User,Global AI Manager,CS User,EDR User,VM User,PC User,CA UI Access,CA API Access,FIM User,PATCH MANAGER																	
4	CVE	CVE-Desct	CVSSv2 Ba	CVSSv3 Ba	QID	TITLE	SEVERITY	TYPE	DETE	LAST DETE	FIRST DETE	PROTOCO	PORT	ASSET ID	ASSET NA	STATUS	ASSET IP	SOLUTION	RESULTS	DISABLED	IGNORED
5	CVE-2020-	Mozilla de	9.3	8.8	372825	Mozilla Fii	4	Confirme	16-Oct-20	16-Oct-20	-	-	-	6473432	AutoTest	NEW	10.115.10	Vendor has released fix	-	No	No
6	CVE-2020-	NSS has st	1.2	4.4	372825	Mozilla Fii	4	Confirme	16-Oct-20	16-Oct-20	-	-	-	6473432	AutoTest	NEW	10.115.10	Vendor has released fix	-	No	No
7	CVE-2020-	Mozilla de	9.3	8.8	372825	Mozilla Fii	4	Confirme	16-Oct-20	16-Oct-20	-	-	-	6473432	AutoTest	NEW	10.115.10	Vendor has released fix	-	No	No
8	CVE-2020-	Mozilla de	9.3	8.8	372825	Mozilla Fii	4	Confirme	16-Oct-20	16-Oct-20	-	-	-	6473432	AutoTest	NEW	10.115.10	Vendor has released fix	-	No	No
9	CVE-2020-	When bro	2.6	5.3	372825	Mozilla Fii	4	Confirme	16-Oct-20	16-Oct-20	-	-	-	6473432	AutoTest	NEW	10.115.10	Vendor has released fix	-	No	No
10	CVE-2020-	When usit	6.8	8.8	372825	Mozilla Fii	4	Confirme	16-Oct-20	16-Oct-20	-	-	-	6473432	AutoTest	NEW	10.115.10	Vendor has released fix	-	No	No
11	CVE-2020-	When con	4.3	6.5	372825	Mozilla Fii	4	Confirme	16-Oct-20	16-Oct-20	-	-	-	6473432	AutoTest	NEW	10.115.10	Vendor has released fix	-	No	No
12	CVE-2020-	Mozilla de	2.6	6.5	372825	Mozilla Fii	4	Confirme	16-Oct-20	16-Oct-20	-	-	-	6473432	AutoTest	NEW	10.115.10	Vendor has released fix	-	No	No
13	CVE-2020-	Due to cor	9.3	8.8	373103	Mozilla Fii	4	Confirme	16-Oct-20	16-Oct-20	-	-	-	6473432	AutoTest	NEW	10.115.10	Vendor has released fix	-	No	No
14	CVE-2020-	A Video st	9.3	8.8	373103	Mozilla Fii	4	Confirme	16-Oct-20	16-Oct-20	-	-	-	6473432	AutoTest	NEW	10.115.10	Vendor has released fix	-	No	No
15	CVE-2020-	When %	4.3	6.5	373103	Mozilla Fii	4	Confirme	16-Oct-20	16-Oct-20	-	-	-	6473432	AutoTest	NEW	10.115.10	Vendor has released fix	-	No	No
16	CVE-2020-	Mozilla de	9.3	8.8	373103	Mozilla Fii	4	Confirme	16-Oct-20	16-Oct-20	-	-	-	6473432	AutoTest	NEW	10.115.10	Vendor has released fix	-	No	No
17	CVE-2020-	Due to cor	4.3	6.5	373103	Mozilla Fii	4	Confirme	16-Oct-20	16-Oct-20	-	-	-	6473432	AutoTest	NEW	10.115.10	Vendor has released fix	-	No	No
18	CVE-2020-	When pro	9.3	8.8	373103	Mozilla Fii	4	Confirme	16-Oct-20	16-Oct-20	-	-	-	6473432	AutoTest	NEW	10.115.10	Vendor has released fix	-	No	No
19	CVE-2020-	Manipulat	4.3	6.5	373103	Mozilla Fii	4	Confirme	16-Oct-20	16-Oct-20	-	-	-	6473432	AutoTest	NEW	10.115.10	Vendor has released fix	-	No	No
20	CVE-2020-	When tryi	9.3	8.8	373103	Mozilla Fii	4	Confirme	16-Oct-20	16-Oct-20	-	-	-	6473432	AutoTest	NEW	10.115.10	Vendor has released fix	-	No	No
21	CVE-2020-	During RS	1.2	4.4	373103	Mozilla Fii	4	Confirme	16-Oct-20	16-Oct-20	-	-	-	6473432	AutoTest	NEW	10.115.10	Vendor has released fix	-	No	No
22	CVE-2020-	When con	4.3	6.5	373103	Mozilla Fii	4	Confirme	16-Oct-20	16-Oct-20	-	-	-	6473432	AutoTest	NEW	10.115.10	Vendor has released fix	-	No	No
23	CVE-2020-	When the	6.9	7.8	373103	Mozilla Fii	4	Confirme	16-Oct-20	16-Oct-20	-	-	-	6473432	AutoTest	NEW	10.115.10	Vendor has released fix	-	No	No
24	CVE-2020-	The r	4.3	6.5	372277	Mozilla Fii	2	Confirme	16-Oct-20	16-Oct-20	-	-	-	6473432	AutoTest	NEW	10.115.10	Vendor has released fix	-	No	No

New Templates for Dashboards

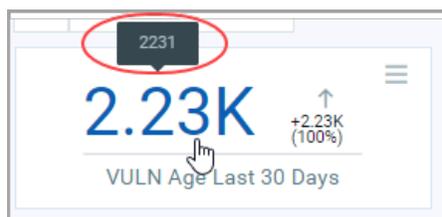
We have now enriched our template library with addition of several new templates. You can use these pre-defined template dashboard to have a single-pane-of-glass view on the dashboard for assets with specific areas of concern.

The new templates that we have introduced in this release are:

- **High RTI 4-5 Severity Summary:** Provides a set of indicators based on RTI data that allow you to measure the real level of risk in your infrastructure, and to provide a summary of the VM data with specific indicators related to the ignored vulnerabilities.
- **Microsoft RCE SMBv3 Advisory-CVE-2020-0796:** Lets you track all the hosts impacted by CVE-2020-0796 vulnerability in their environment.
- **Top10 Exploited Vulns | Alert-AA20-133A:** Helps you to identify the most exploited vulnerabilities in the last 5 years.
- **F5 | BIG IP – Vulnerabilities:** Provides a view all the F5 vulnerabilities and highlights the following CVEs for remediation:
CVE-2020-5902
CVE-2020-5902
CVE-2020-5903
- **CISCO IOS | XE: Vulnerabilities:** Use template to visualize exposure to the new/Cisco REST API Container for IOS XE Software Authentication Bypass Vulnerability (CVE-2019-12643).
- **OpenBSD Vulnerabilities:** Use template to envision exposure to multiple authentication vulnerabilities in OpenBSD and highlights the following CVEs:
CVE-2019-19522
CVE-2019-19521
CVE-2019-19520
CVE-2019-19519

Hover and View Count Value in Widget

The count widgets display shortened values for big numbers in the widget. We have now enhanced the count widget to quickly display the complete actual value of the count rather than the shortened value. Simply hover the mouse over the number and the actual count is displayed as a tool tip.



New Widgets for AssetView Discontinued from Widget Builder

We have removed the support for new widget creation for AssetView module from the widget builder. All your existing widgets and dashboards remain unaffected.

AssetView will be end-of-life by early 2021. We are replacing it with our feature rich Global IT Asset Inventory.

Support for Campaign Scheduler

Now, you can schedule your campaigns and run them automatically on a particular date and time. With this change, you can now automate and manage your assessment workflow even better.

You can schedule a campaign to run only once, or set it as a recurring job. You must set a due date for your campaign.

The screenshot shows the 'Create Campaign' interface with a sidebar on the left containing six steps: 1 Campaign Details, 2 Workflows, 3 Recipients, 4 Schedule (highlighted), 5 Notifications, and 6 Review and Confirm. The main content area is titled 'Schedule Campaign' and includes the instruction 'Set up your campaign to run on demand or schedule it for later'. There are two radio buttons: 'On Demand' and 'Schedule' (which is selected and highlighted with a red box). Below these are input fields for 'Start Date *' (15-11-2020), 'Start Time' (12:00am), and 'Due Date *' (15-12-2020). A 'Recurring Job' checkbox is also present. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.

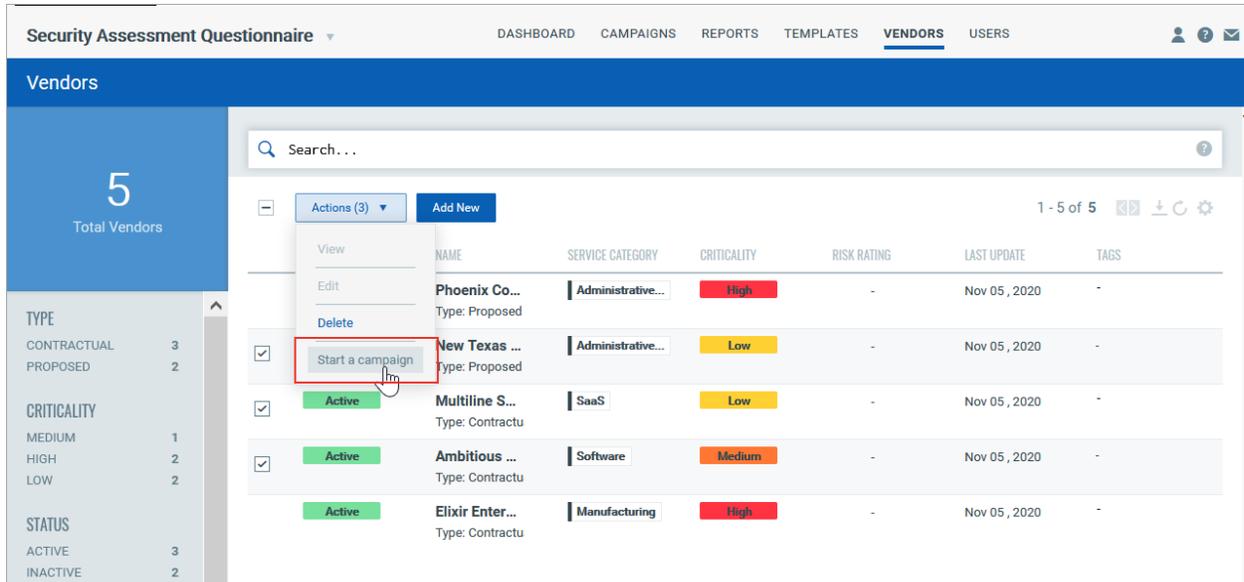
As a recurring job, choose the options for the recurrence pattern. You must set an end date for your recurrence schedule. You can set the day on which you want to notify the campaign manager about the initialization of a campaign. You can also view the next schedule date, which is calculated based on the recurrence options that you set.

The screenshot shows the 'Create Campaign' interface. The sidebar on the left indicates the current step is '4 Schedule'. The main content area is titled 'Schedule Campaign' and includes the following elements:

- Buttons for 'On Demand' and 'Schedule' (selected).
- Start Date: 15-11-2020
- Start Time: 11:00am
- A red box highlights the 'Recurring Job' checkbox, which is checked.
- Radio buttons for 'Day of the Month' (unselected) and 'Day of the Week' (selected).
- Recurrence Day: 1
- Week Day: MONDAY
- Start Time: 11:00am
- Due Date: 30 days after campaign initialization
- Notify Campaign Manager: 7 days prior to initialization
- End Date: 31-05-2021
- A link to 'View next schedule date' with the calculated date: Dec 14, 2020 11:00:00 AM
- Navigation buttons: Cancel, Previous, Next.

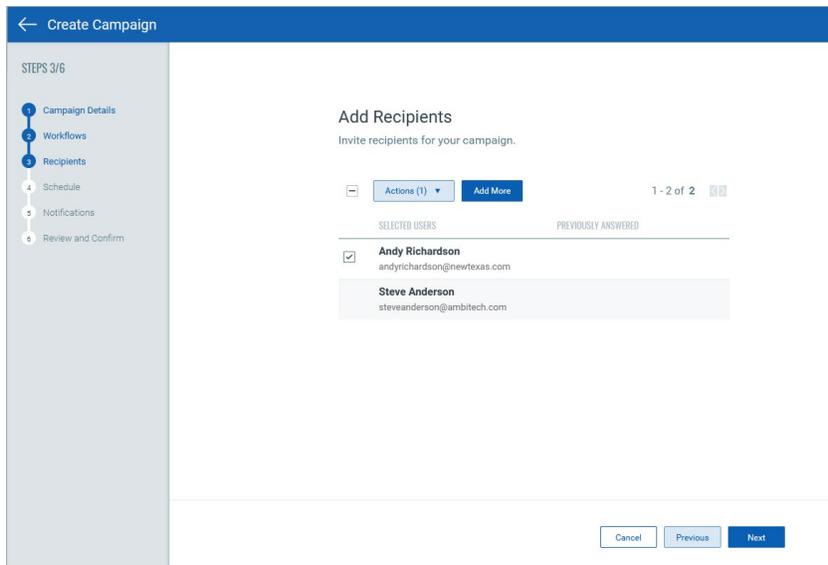
Support for Campaign Creation from VENDORS Tab

From this release onwards, you can create a campaign from the Vendors page as well. Select vendors for whom you want to create an assessment campaign and then, from the **Actions** tab, click **Start a campaign**.



On the Create Campaign page, provide the required details and launch your campaign.

The users that you choose as single points of contact (SPOC) during vendor onboarding are displayed in the list of potential recipients for your campaign automatically. You can select these SPOCs as the intended recipients. This saves you an effort of manually adding users to the list of recipients.



If you want to invite users other than SPOCs or if a SPOC is not assigned for a selected vendor, you can manually add the intended recipients.

Added Custom Attributes Information to Reports

When you set up a web application, you have the option to add custom attributes (name/value) and apply tags to your web application. We now show the custom attributes and tag information in the Appendix section of the Web application and Scan reports. The report lets you quickly find the custom attributes added or the tags that are applied to a web application.

Web application report shows the Tag and Custom Attributes information.

The screenshot shows the 'Appendix' section of a web application report. Under 'Web Application Details', there is a section for 'Varun-custAttributes'. A table lists the following attributes:

Name	Value
Contact Email	john@abc.com
Contact Person	John Doe

Scan report shows the Tags and Custom Attributes information.

The screenshot shows the 'Appendix' section of a scan report. Under 'Web Application Details: Varun-custAttributes', there is a table listing tags and custom attributes:

Tags	Value
Tag1	1582696957250

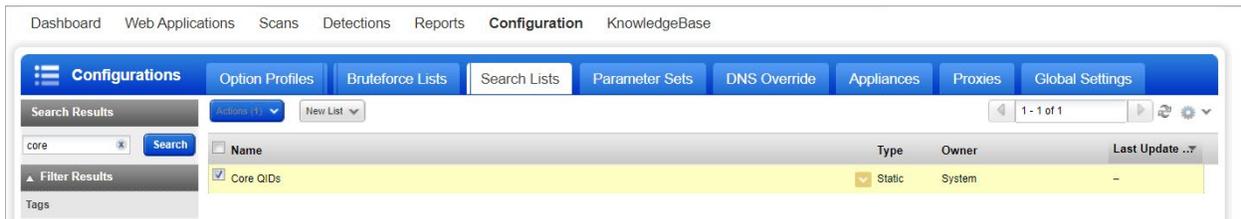
Custom Attributes	Name	Value
	Contact Email	john@abc.com
	Contact Person	John Doe

For Web application and Scan report in the CSV form, we have added the Tags and Custom Attributes columns to show the tag and custom attributes information.

APPENDIX																		
Scan Name	Reference	Start Date	End Date	Mode	Type	Progressive	Progressive	Web Appli	Authentic	Profile	DNS Overri	Scanner A	Status	Authentication Status				
Prasanjit - was/1604	09 Nov 20	09 Nov 20	09 Nov 20	Vulnerabil	Manual	Disabled		1	Varun-cus	None	Test 10 links	External (I	Finished	No Authentication specified				
Form Subr	Form Crav	Maximum	User Agen	Request P	Document	SmartScar	SmartScar	Timeout E	Unexpecte	Scan Inter	Bruteforce	Detection	Include ad	Credit Car	Social Seci	Custom		
Post & Get	Do not inc	10		Initial Para	Ignore cor	Disabled		5	100	300	Low	Disabled	Core	Off	Off	Off		
Web Appli URL	Owner	Scope	ID	Tags	Custom Attributes													
Varun-cus	http://10.	Anjali Ping	Limit to UF	3622184	Tag1 1582	"Contact Email=john@abc.com", "Contact Person=John Doe", "Jane=Doe", "Joe=Harris"												

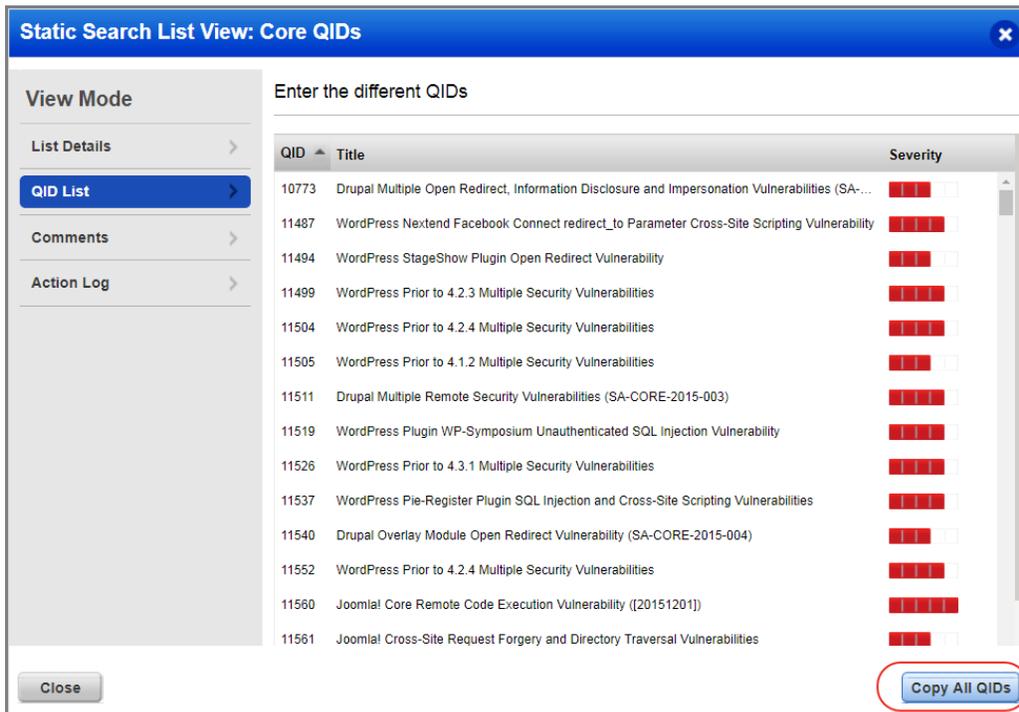
Added New Search List “Core QIDs” and Option to Copy QIDs

You can now view the core QIDs and customize the Core detection scope from the search list. We added a new static search list for core QIDs with the name “Core QIDs” in **Configuration > Search Lists**. This is a default search list created by the system. The search list is synched with the core QIDs of the core category to keep the QIDs in the search list updated. As the search list is system created, you cannot edit but only view the QIDs in the search list.



While viewing the QIDs, you can copy the core QIDs from the Core QID search list using the Copy All QIDs button. When you click Copy All QIDs button, we copy all the QIDs into the clipboard. Next, paste the QIDs into a text file, add or remove QIDs from the list as desired, and then create a new search list with these QIDs.

The “Copy all QIDs” option is available for all the search lists. To copy the QIDs from the search list, select a search list and click **View** from the **Quick Action** menu. Go to the **QIDs list** tab and click **Copy All QIDs**.



The “Copy all QIDs” option is also available from option profile (for core, categories, XSS Power Mode, and Custom Search Lists detection scope) and scan settings.

You can copy the Core QIDs from the option profile when you create or edit an option profile with Detection scope set as Core. To copy the core QIDs from the option profiles, go to the create/ edit option profile screen, and then go to the **Search Criteria** tab. If you are creating a new option profile, set the detection scope to **Core** and then click the link **View list of Core QIDs**.

Option Profile Creation Turn help tips: On | Off Launch help

Step 3 of 5

- 1 Profile Details ✓
- 2 Scan Parameters ✓
- 3 Search Criteria ✓
- 4 Comments
- 5 Review And Confirm

Please define what you want to scan for

Detection Scope (*) REQUIRED FIELDS

Select if scans launched with this profile shall perform a full assessment for all WAS detections the engine is able to discover, or if the scan shall focus on the detection of specific vulnerabilities and/or information.

Detection*

Include additional XSS payloads (may significantly increase scan time)

[View list of Core QIDs.](#)

Note: All Information Gathered QIDs will be included in scan detection scope when Core scope will be selected.

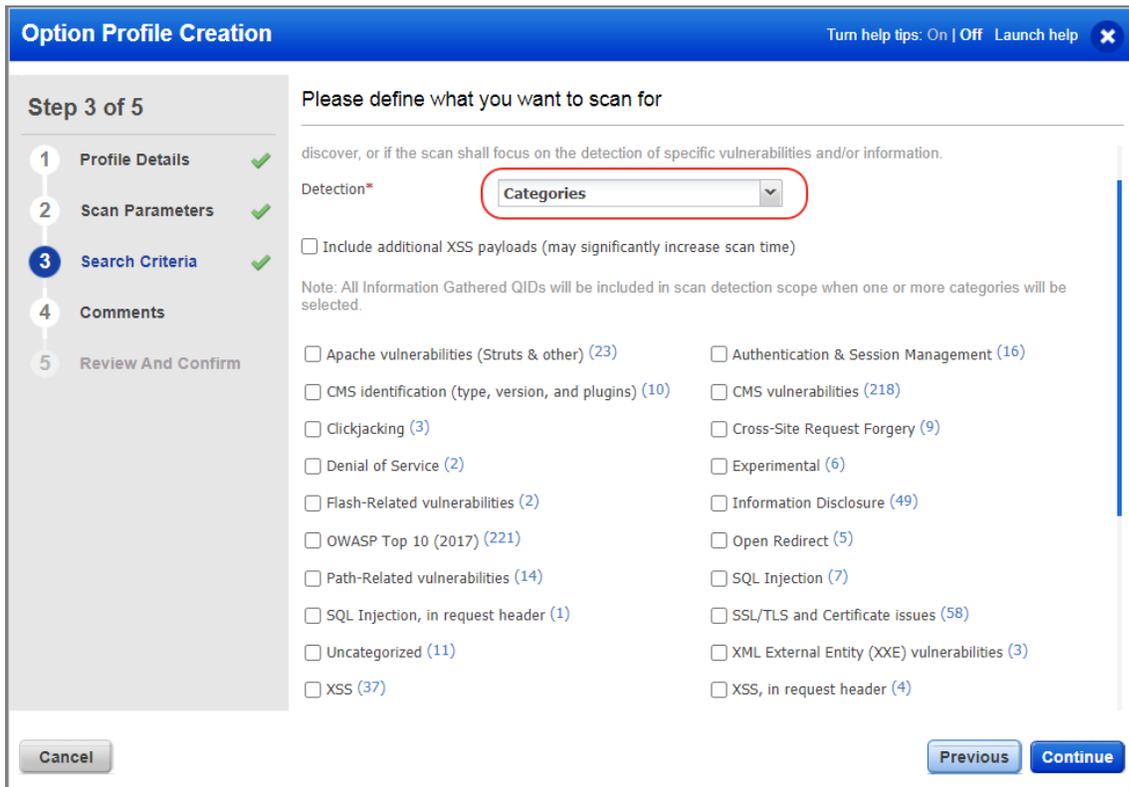
The **QIDs included in Core Detection Scope** screen shows the **Copy All QIDs** button. Click this button to copy the QIDs from list.

QIDs included in Core Detection Scope

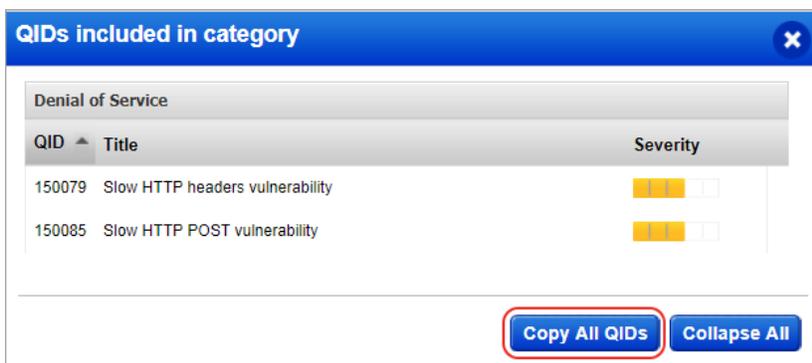
QID	Title	Severity
10773	Drupal Multiple Open Redirect, Information Disclosure and Impersonation Vulnerabilities (SA-CORE-2015-002)	■■■■
11487	WordPress Nextend Facebook Connect redirect_to Parameter Cross-Site Scripting Vulnerability	■■■■
11494	WordPress StageShow Plugin Open Redirect Vulnerability	■■■■
11499	WordPress Prior to 4.2.3 Multiple Security Vulnerabilities	■■■■

[Copy All QIDs](#) [Collapse All](#)

To copy the QIDs for detection categories, select **Categories** in the Detection Scope and click the number showing the total number of QIDs for a category.



The **QIDs included in category** screen shows the **Copy All QIDs** button. Click this button to copy the QIDs from list.



You can copy the QIDs from the Scan settings. Go to **Scans > Scan List**. Select a scan, then click **View Scans** from the **Quick Actions** menu. Select a child scan and choose **View** from the **Quick Actions** menu. On the **WAS Vulnerability Scan View** screen, go to scan settings and then click the QIDs shown for the QIDs included, QIDs excluded, QIDs included from categories, and Default QIDs.

WAS Vulnerability Scan View

View Mode

- Overview >
- Scan Details >
- Scan Settings >**
- Action Log >

Review scan options used to run the scan

Crawling Settings

Form Submissions GET and POST	Form Crawl Scope Do not include 'Form Action URI'	Maximum links tested 300
User Agent -		
Ignore Binary Files Yes		

Detection Scope

Scope Core	Include additional XSS payloads No
Detection Lists -	QIDs Included 289
Exclusion Lists -	QIDs Excluded -
Selected Categories -	QIDs Included from Categories -
Default QIDs 77	

Buttons: Close, View Report

The **Default QIDs included** screen shows the **Copy All QIDs** button. Click this button to copy the QIDs from list.

Default QIDs included

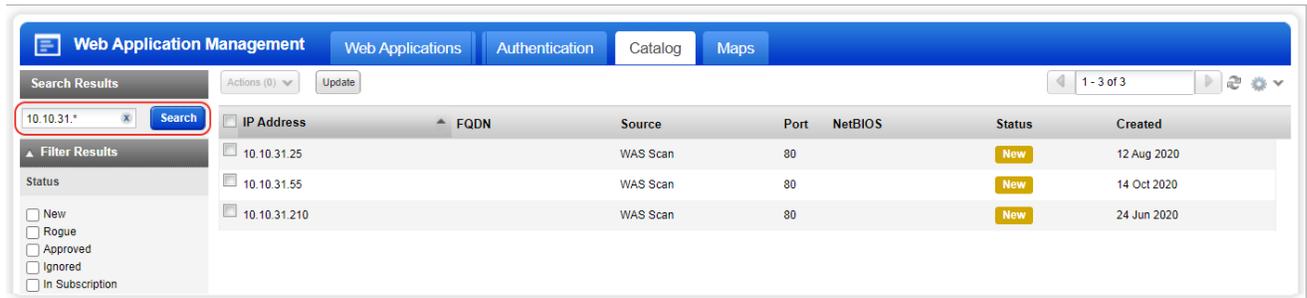
All Information Gathered QIDs

QID	Title	Severity
6	DNS Host Name	<input type="checkbox"/>
38116	SSL Server Information Retrieval	<input type="checkbox"/>
38291	SSL Session Caching Information	<input type="checkbox"/>
38597	SSL/TLS invalid protocol version tolerance	<input type="checkbox"/>
38600	SSL Certificate will expire within next six months	<input type="checkbox"/>
38609	SSL Server default Diffie-Hellman prime information	<input type="checkbox"/>

Buttons: Copy All QIDs, Collapse All

Ability to Filter Catalog Entries using Wildcards in IP Address

You can now use wildcard character * in IP address when searching for catalog entries by IP address. We support wild card character * for numbers in IP Address. For example, 10.11.196.* or 10.11.*.* are valid patterns for IP address. Examples of Invalid patterns: *1.123.123.123, 1*1.123.123.123 and 1*.123.123.123. You can combine one or more filters with IP address to search for a specific entry.



The screenshot displays the 'Web Application Management' interface, specifically the 'Catalog' tab. A search bar at the top left contains the text '10.10.31.*' and a 'Search' button. Below the search bar, a table lists the search results. The table has columns for 'IP Address', 'FQDN', 'Source', 'Port', 'NetBIOS', 'Status', and 'Created'. Three entries are shown, all with a status of 'New' and a source of 'WAS Scan'. The 'Created' dates are 12 Aug 2020, 14 Oct 2020, and 24 Jun 2020. On the left side, there is a 'Filter Results' section with a 'Status' filter and several checkboxes: 'New', 'Rogue', 'Approved', 'Ignored', and 'In Subscription'. The 'New' checkbox is checked.

IP Address	FQDN	Source	Port	NetBIOS	Status	Created
10.10.31.25		WAS Scan	80		New	12 Aug 2020
10.10.31.55		WAS Scan	80		New	14 Oct 2020
10.10.31.210		WAS Scan	80		New	24 Jun 2020

Issues addressed in this release

We have fixed the following issues in this current release-

UD Unified Dashboard

- We have now fixed an issue so that the long queries in the search bar of the widget builder are displayed without being truncated. Earlier, the long query text was truncated behind the preview pane.
- We have now fixed an issue so that when you print a dashboard, the tag selection for the dashboard is correctly reflected on the dashboard.

CA Cloud Agent

- Fixed an issue where 'Network Information' for asset details was not showing any information.
- Fixed an issue where the error was occurring while editing the configuration profile.
- Fixed an issue where only VM and PC were getting enabled with Create Activation Key API for "ALL" value in the "modules" parameter.
- Fixed an issue where column sorting on a list of configuration profiles if the number of configuration profiles is more than 20.

WAS Web Application Scanning

- We now show on the UI under the help > Account Information, the settings (On/Off) for marking a detection fixed when the vulnerable URL is not found on the Web Application Scanning tab.
- We fixed an issue where values in the reported QID 150300 in the scan report were shown on the same line instead of on new lines. Now we show QID 150300 values in the scan report separated by new lines.
- We fixed an issue where we were not showing the correct value in the Cookie tag in the web app and scan report in the XML format for QIDs that have cookies. Now the XML report for web apps shows the correct values of the cookies for QIDs that have cookies.
- We fixed an issue where for web application with scan trust enabled on both WAS and WAF, the user was not able to see the vulnerabilities that were detected by Qualys WAF in WAS Detections when the Protected filter was selected. Now you can see the vulnerabilities detected by Qualys WAF when you select the Protected filter in WAS Detections.
- We fixed an issue where the user was getting an error when canceling an On Demand or a Scheduled scan that was in the running state. Now, the user can cancel the On Demand or Scheduled scans that are in the running state.
- We fixed an issue where the user was shown non-supported report formats when saving an MDS scan report. Now you will see only the valid formats: PDF, EPDF, ZIP, CSV when saving the scan report.
- We fixed an issue where scans scheduled in the user account were launched even after the MDS module was disabled for the user. Now, scheduled scans are not launched if the MDS module is disabled for the user account.
- We fixed an issue where the user was getting an error when trying to save a copy of a malware scan schedule using the "Save As" option. Now, you can use the "Save As" option to save a copy of the scan schedule.