

Qualys Cloud Suite 2.30

Here's what's new in Qualys Cloud Suite 2.30!

AV AssetView

TP ThreatPROTECT

Dynamic tag support for Amazon EC2 Metadata
Search Assets by Amazon EC2 Metadata

CA Cloud Agent

Download Search Results
Enhancements to Actions Menu

SAQ Security Assessment Questionnaire

Assign Reviewers per Section or Subsection
Add Tags to Users

WAS Web Application Scanning

Normalization of Date/Time Format in CSV Reporting
Scan Result Comparison Updated

WAF Web Application Firewall

Event List enhancements
View policies by status
Custom rules - DETECT operator

Qualys Cloud Suite 2.30 brings you many more
Improvements and updates! [Learn more](#)



AssetView



ThreatPROTECT

Dynamic tag support for Amazon EC2 Metadata

We've introduced a new dynamic tag rule type that allows you to tag your EC2 instances based on EC2 metadata attributes as collected by the EC2 Connector. For each tag rule you'll provide a search query with EC2 instance information like the public and private DNS name, image ID, VPC ID, instance state, instance type and more. You can even create tags in Qualys that are based on tags in AWS.

When creating a new tag, choose "Cloud Asset Search (AWS EC2 Instances)" and enter a search query to define the rule criteria. It's easy - start typing in the Query field and we'll show you the EC2 attributes you can search.

Tag Creation Turn help tips: On | Off Launch help ×

Step 2 of 3

- 1 Tag details ✓
- 2 Tag Rule ✓
- 3 Review And Confirm

Set the tag type and rules

Rule Engine (*) REQUIRED FIELDS

Cloud Asset Search (AWS EC2 Instances) ☐ Re-evaluate rule on save

Query*

aws.ec2.instanceState:"RUNNING" and aws.ec2.region.name:"Asia Pacific (Mumbai)"

Test Rule Applicability on Selected Assets

Add Asset: Select an asset

Check out these sample queries:

Find running EC2 instances:

```
aws.ec2.instanceState:"RUNNING"
```

Find EC2 instances with type "t2.medium" in the region "US West (Northern California)":

```
aws.ec2.instanceType:"t2.medium" and aws.ec2.region.name:"US West (Northern California) "
```

Find EC2 instances with AWS tag key "department" and value "stage":

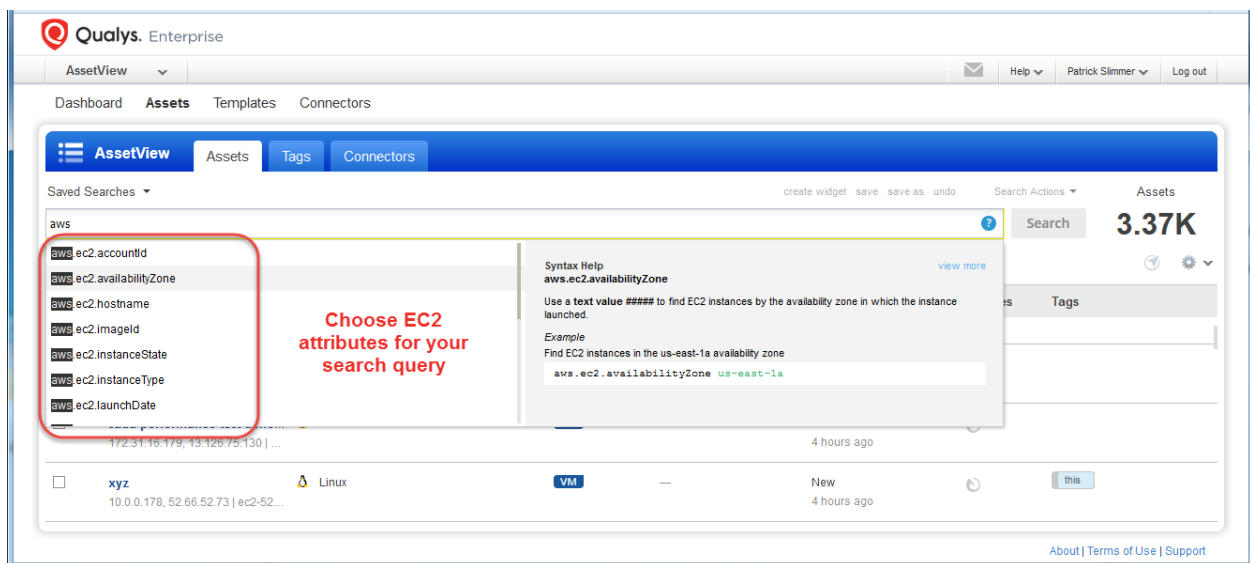
```
aws.tags.key:department and aws.tags.value:stage
```

Find EC2 instances created from pre-approved AMIs (ami-1231231 and ami-8790707):
`aws.ec2.imageId:ami-1231231 and aws.ec2.imageId:ami-8790707`

Find EC2 instances with specific criteria for scanning:
`aws.ec2.region.name:"EU (London)" and aws.ec2.vpcId: [vpc-12321213, vpc-342342] and aws.ec2.instanceState:"RUNNING"`

Search Assets by Amazon EC2 Metadata

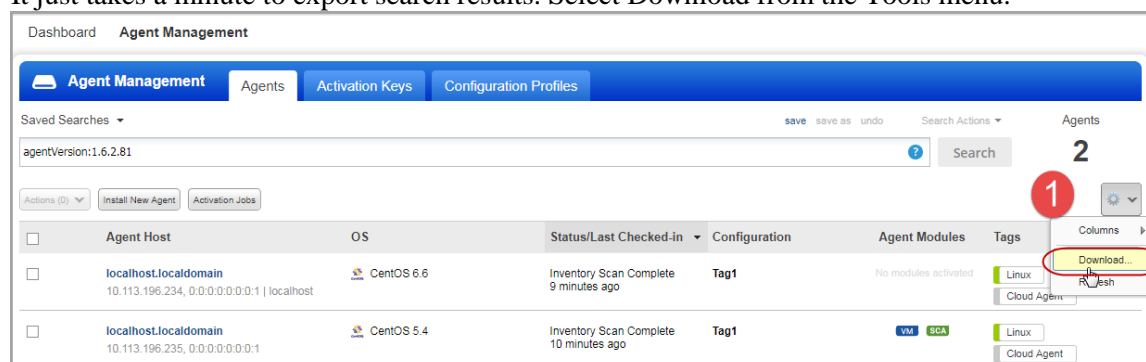
Our search capabilities have been expanded to include EC2 metadata attributes so you can easily find your Amazon EC2 instances. These new fields start with `aws.ec2`. Start typing in the Search box and we'll show you the attributes you can search like availability zone, region, hostname, image ID and more.



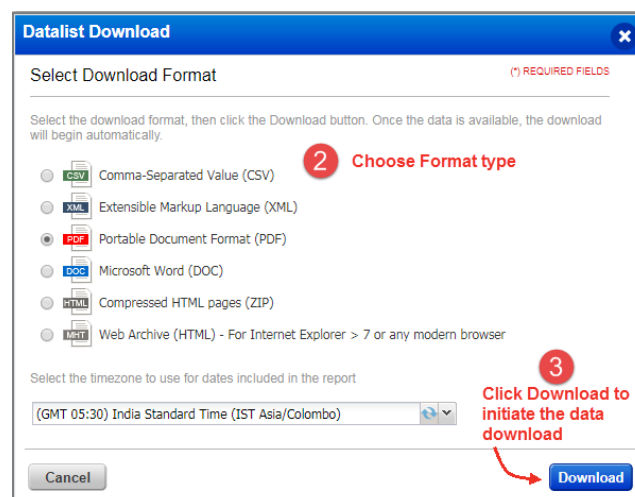
Download Search Results

With this release you can now download and export the search results in the Cloud Agent user interface similar to AssetView download results providing offline analysis of Cloud Agent deployments. By exporting agent list to your local system you can easily manage assets outside of the Qualys platform and share them with other users. You can export results in multiple formats (CSV, XML, PDF, DOC, ZIP, HTML).

It just takes a minute to export search results. Select Download from the Tools menu.




Next, choose an export format and click Download. That's it!



Agent list in PDF format

Agents

Qualys. Enterprise

Data List: Agents

Patrick Slimmer
quays_ps

Qualys, Inc.
1600 Bridge Parkway
United States of America

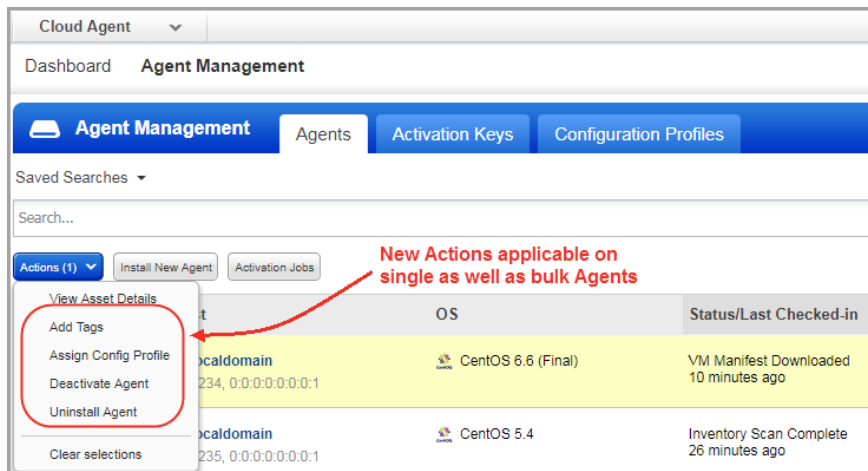
Created: 31 Aug 2017 15:14 GMT+0630

Number of records: 62

Asset Id	Errors	Agent Host	OS	Version	Status/Last Checked-in	Configuration	Agent Modules	Tags
5936055		localhost.localdomain (10.113.196.235) 10.113.196.235, 0:0:0:0:0:0:1	CentOS 5.4	1.6.2.81	Inventory Scan Complete (31 Aug 2017 02:37PM GMT+0500)	Default new	SCA,VM	Cloud Agent
5941083		localhost.localdomain (localhost) 10.113.196.234, 0:0:0:0:0:0:1 localhost	CentOS 6.6	1.6.2.81	Inventory Scan Complete (31 Aug 2017 02:26PM GMT+0500)	Default new		Cloud Agent

Enhancements to Actions Menu

We have introduced many enhancements to the Actions menu. You can now:




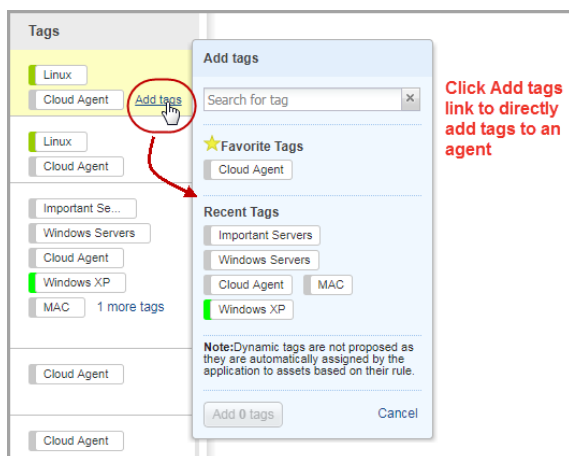
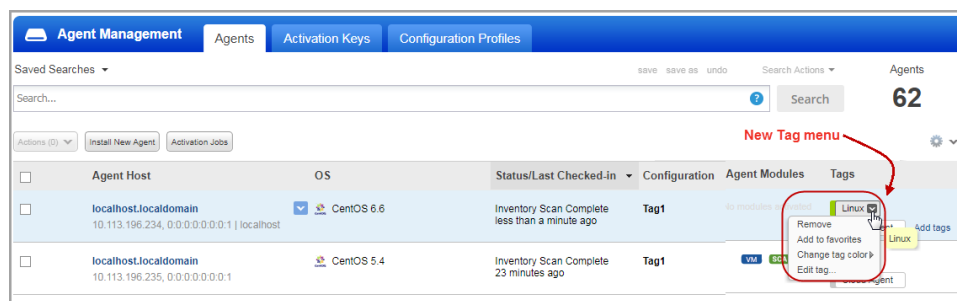
--Add tags: You can directly assign tags to the agents as per your selection. You can also create new tags.

--Assign Config Profile: You can now directly assign a configuration profile to the selected agents (single or bulk agents).

--Activate, Deactivate, and Uninstall Agents (Bulk): You can now directly perform bulk action (activate,

deactivate or uninstall) on the cloud agents that match your search query. You can now also activate/deactivate FIM and IOC modules (in addition to VM and PC) for your cloud agents. We have removed the Bulk Actions button and moved the same actions to the Actions menu.

We have also added new menu for you to perform tag related actions. Click the  icon on the required tag to view the tag menu.



You could also hover the mouse in the Tags column and click Add Tags link to add tags for the selected agent.



Security Assessment Questionnaire

Assign Reviewers per Section or Subsection

You can now have different reviewers review different sections or subsections. Only when all sections are reviewed by the assigned reviewer the campaign is marked complete.

To assign multiple reviewers, create a campaign and select a 3 or 4 stage workflow. Click Add Section or Subsection Reviewer and select reviewers for the desired sections.

Campaign Creation Turn help tips: On | Off

Step 2 of 5

- 1 Campaign Details ✓
- 2 **Workflows** ✓
- 3 Recipients
- 4 Notifications
- 5 Review And Confirm

What workflow do you want to follow? (*) REQUIRED FIELDS

Choose a workflow

A workflow refers to tasks procedural steps and the people involved need for each step in questionnaire process. Select from the defined workflows below.

Workflow* **3-Stage**

Total Stages : 3
Stages : Information Gathering / Review / Close
Notification : Email
Requirements : Review

Select Workflow Users

Select a user responsible for reviewing answers to all questions.

Reviewer* **John Doe (Jdoe@afco.com)**

+ Add Section or Subsection Reviewer

Select Workflow Users

Select a user responsible for reviewing answers to all questions.

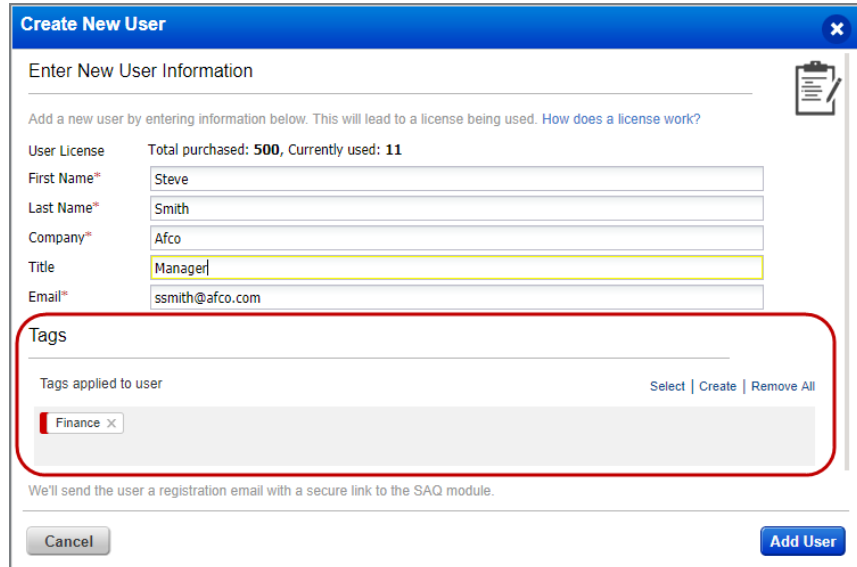
Reviewer* **John Doe (Jdoe@afco.com)**

Section or Subsection	Reviewer			
2. Control the Network	Mark Taylor (Mtaylor@afco.com)			
8. Monitor Systems	Patrick Slimmer (pslimmer@afco.com)			+

Add Tags to Users

With this release you can now configure tags, which helps you to organize and manage users in your subscription. Add tags while creating a user or edit an existing user. You can also create tags or sub tags while adding them.

Simply, navigate to Users > Users > New User and fill in the user details and assign tags to this user.



The 'Create New User' form is shown with a red box highlighting the 'Tags' section. The form includes fields for user information and a section for assigning tags.

Create New User

Enter New User Information

Add a new user by entering information below. This will lead to a license being used. [How does a license work?](#)

User License: Total purchased: 500, Currently used: 11

First Name*: Steve

Last Name*: Smith

Company*: Afco

Title: Manager

Email*: ssmith@afco.com

Tags

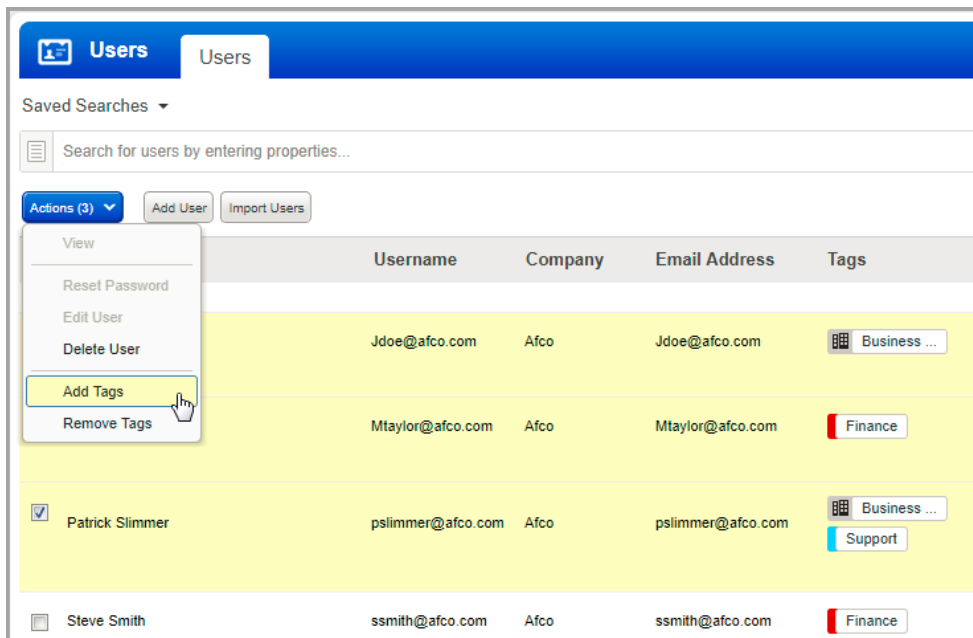
Tags applied to user: Select | Create | Remove All

Finance X

We'll send the user a registration email with a secure link to the SAQ module.

Cancel Add User

In the Users tab, select a single user or multiple users from the list, to add or delete tags from the Actions menu.



The 'Users' management interface shows a list of users with columns for Username, Company, Email Address, and Tags. The 'Actions' menu is open, showing options like View, Reset Password, Edit User, Delete User, Add Tags, and Remove Tags. The 'Add Tags' option is highlighted.

Users

Saved Searches ▾

Search for users by entering properties...

Actions (3) ▾ Add User Import Users

View

Reset Password

Edit User

Delete User

Add Tags

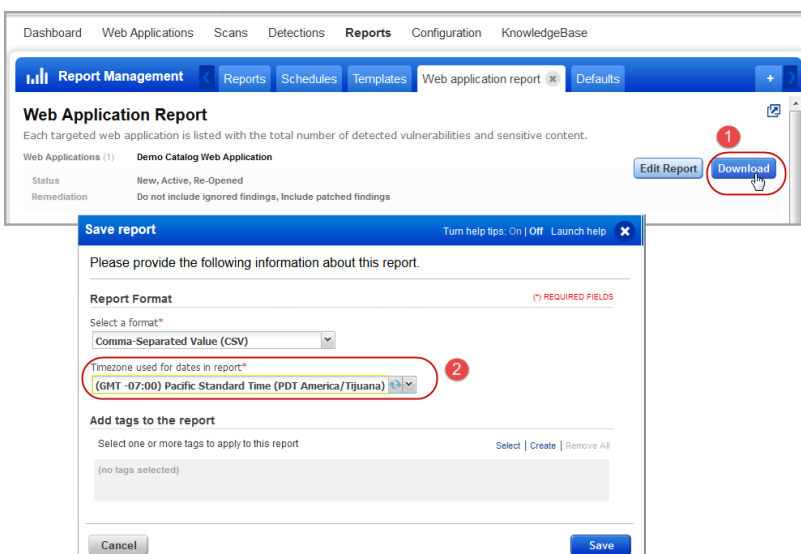
Remove Tags

	Username	Company	Email Address	Tags
<input type="checkbox"/>	Jdoe@afco.com	Afco	Jdoe@afco.com	Business ...
<input type="checkbox"/>	Mtaylor@afco.com	Afco	Mtaylor@afco.com	Finance
<input checked="" type="checkbox"/>	Patrick Slimmer	pslimmer@afco.com	pslimmer@afco.com	Business ... Support
<input type="checkbox"/>	Steve Smith	ssmith@afco.com	ssmith@afco.com	Finance

Normalization of Date/Time Format in CSV Reporting

Previously XML and CSV reports in Qualys WAS had the date/time in Zulu format. With this release Qualys has normalized the date/time format to be consistent with other reports and is presented with the respective GMT.

For example, let us download a web application report in CSV format in Pacific time zone.



The CSV Report now displays the correct time zone.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Web Appl	31 Aug 2017 11:42PM GMT-0700											
2	Qualys	Pune	Pune	None	111111	Switzerland							
3	Patrick SLI	user_ps											
4	DESCRIPTION												
5	Each targeted web application is listed with the total number of detected vulnerabilities and sensitive content.												
6	TARGET												
7	Web Appl Demo Catalog Web Application												
8	FILTERS												
9	Status	New,Active,Re-Opened											
10	Remediat	Do not show ignored findings, Include patched findings											
11	SUMMARY												
12	Security R	Web Appl	Vulnerabi	Sensitive	Information Gathered								
13	Medium	1	57	0	14								
14	Web Appl	Level 5	Level 4	Level 3	Level 2	Level 1	Sensitive	Information Gathered					
15	Demo Cat	0	0	8	20	29	0	14					
16	RESULTS												
17	Web Appl	VULNERAI	ID	QID	Url	Param	Function	Form Entr	Access Pa	Authentic	Ajax Requ	Ajax Requ	Statu
18	Demo Cat	VULNERAI	220295	150145	https://10.11.69.21/WAS-2930/applet-2/applet-2htr				Not Requi	No			New
19	Demo Cat	VULNERAI	220300	150023	https://10.11.69.21/icons/				Not Requi	No			New
20	Demo Cat	VULNERAI	220264	150146	https://10.11.69.21/WAS-2930/CSS_AS_IMAGE_GALL				Not Requi	No			New
21	Demo Cat	VULNERAI	220289	150146	https://10.11.69.21/WAS-2930/iframe/page.html				Not Requi	No			New
22	Demo Cat	VULNERAI	220287	150145	https://10.11.69.21/WAS-2930/redndantLinks/s.ht				Not Requi	No			New

The normalization of date/time format is now applicable across all CSV reports (web application reports, scan reports, and datalist) in WAS.

Scan Result Comparison Updated

We would now display comparative analysis of changes in scan results between incremental scan reports for six specific QIDs: 150009 150020 150041 150018 150152 and 150115.

For example, let us see the scan result comparison for QID 150009.

Simply navigate to the Information Gathered section in a scan report. When you expand the Results section you can see the changes from previous scans highlighted in multiple colors. Disable the Highlight changes from the previous scan option to hide the comparative analysis. By default this option is enabled.

Information Gathered Details

150009 Links Crawled

Finding #	325225* (86309522)	Web Application	Fresh_Scan
Group	Information Gathered	Authentication	Not Used
CWE	-		
OWASP	-	Detection Date	31 Aug 2017 4:08PM GMT+0530
WASC	-		

Details [Show](#)

Results

☒ Highlight changes from previous scan

- New - this link was not found in the previous scan
- Modified - this result was found by the previous scan but its value was different
- Removed - this link was not found, but was reported in the previous scan

Duration of crawl phase (seconds): 411.00
Number of links: 52
(This number excludes form requests and links re-requested during authentication.)

http://10.10.26.238/
http://10.10.26.238/crossdomain.xml
https://10.10.26.238/
https://10.10.26.238/?account=business
https://10.10.26.238/?account=personal
https://10.10.26.238/?accountcorp=corporate
https://10.10.26.238/bog/
https://10.10.26.238/bog/Ranjit/
https://10.10.26.238/bog/Ranjit/WAS-4437-secureflag.php
https://10.10.26.238/bog/Ranjit/rany-with-auth.php
https://10.10.26.238/bog/Ranjit/rany-without-auth.php

[Export...](#)



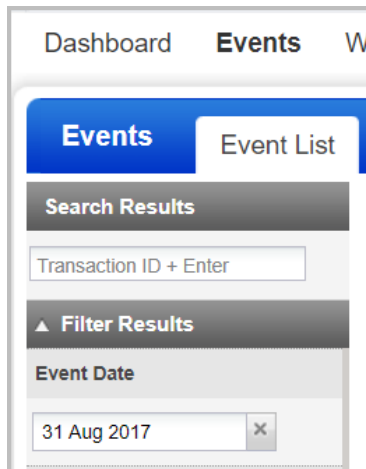
Web Application Firewall

Event List enhancements

You can now use the filters on the WAF Event List tab with better precision.

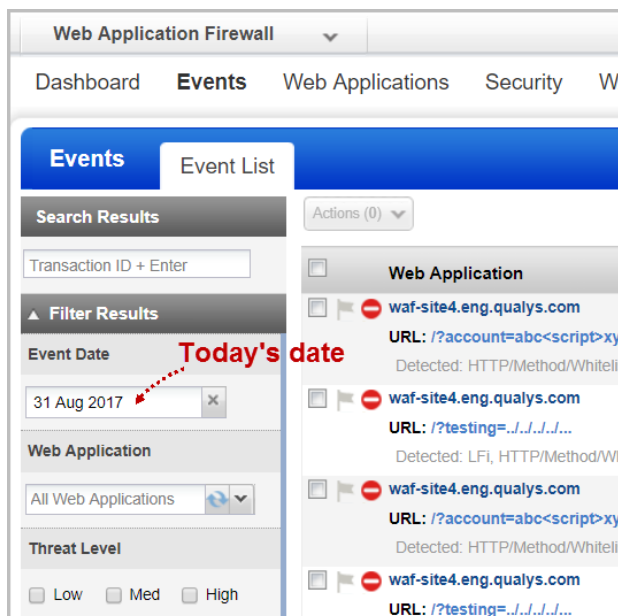
Search by Transaction ID or use Filters

You can either search an event by transaction ID or use filters, you cannot specify both.



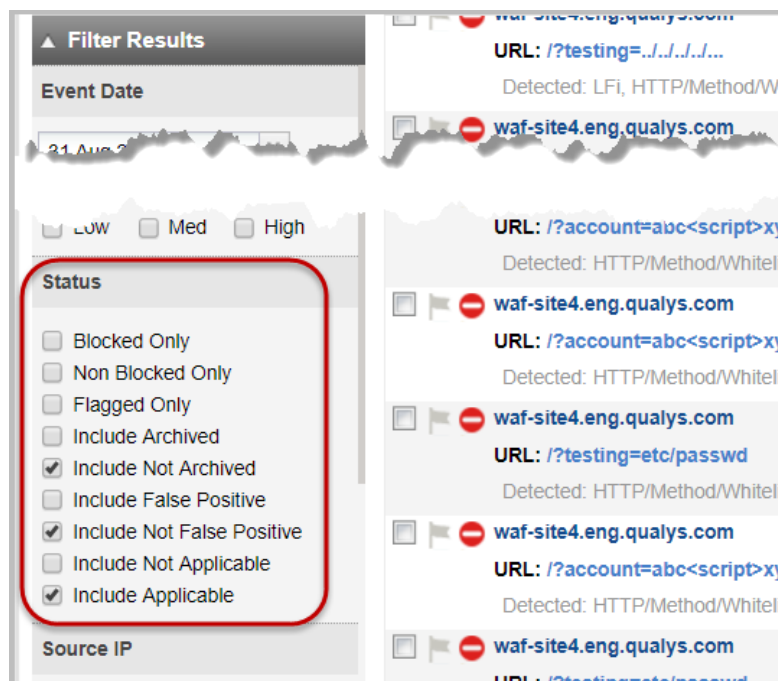
Event Date shows today's date

The Event Date filter now displays today's date. Previously the events were sorted starting with today's date, however the date was not displayed in the Event Date filter.



Improved status filters

The default filters enabled for status are now explicitly displayed as checked on the UI. Previous these were being used, but were not displayed as checked on the UI.

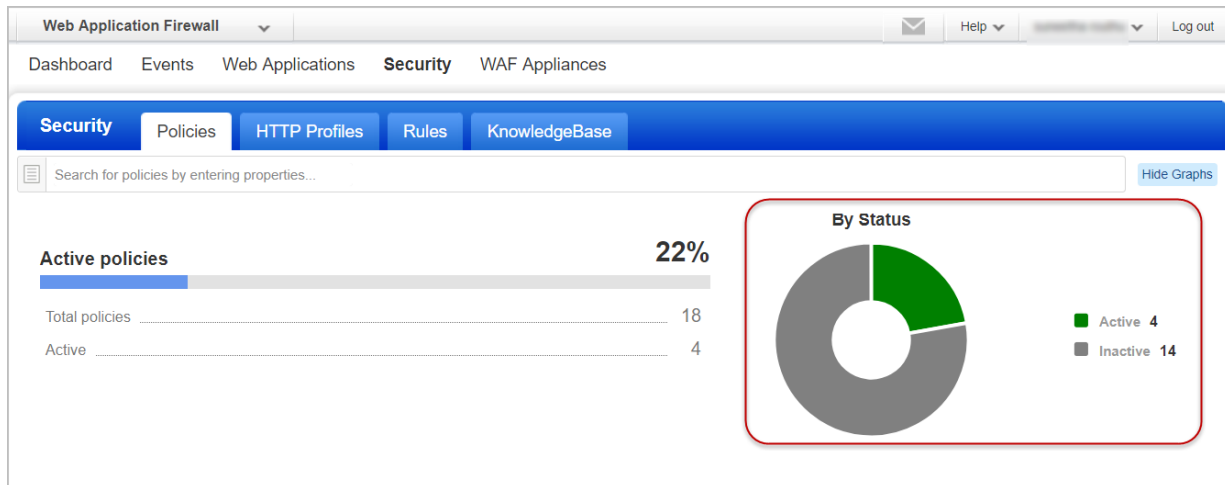


Event status filters have now become more intuitive. Filters such as Archived Only, False Positive Only, and Not Applicable Only have been removed, and new filters such as Include Not Archived, Include Not False Positive, and Include Applicable are introduced. These are the default filters.

For example if you want to see only false positive events, select Include False Positive, and uncheck Include Not False Positive.

View policies by status

The Policies tab now displays a pie chart showing policies by status (active / inactive). You can filter the list of policies according to status by clicking the active or inactive slice of the pie.



Custom rules - DETECT operator

A new operator DETECT is introduced for custom rules. This operator lets you detect incoming traffic based on QIDs.

For example, you can use the DETECT operator to detect false positives.

```
request.path DETECT "qid/150011" with action Allow
```

The above rule will look for a path that potentially exposes sensitive files (QID 150011 - Local File Inclusion), but allows this request even if it's usually blocked, as it's a false positive.

Similarly, if you create a DETECT rule with action **Block**, WAF blocks the request and applies a virtual patch for it.

Rule Creation

Step 2 of 4

1 Rule Details ✓

2 **Conditions** ✓

3 Actions

4 Review And Confirm

Rule conditions

Conditions

Build a set of conditions you want to match prior to triggering. Conditions are ranged in four scopes : client, server, request, response (use the up and down arrows in the textfield to display the available scopes).

When Type your query

1 request path DETECT qid/150011

Once you select the DETECT operator for a key, enter `qid/` followed by the QID number (all in quotes)
`request.path DETECT "qid/150011"`

The DETECT operator is available for the following keys:

```
request.body.charset
request.body.parameter
request.body.parameter.name
request.body.parameter.value
request.header
request.header.content-type
request.header.cookie
request.header.cookie.name
request.header.cookie.value
request.header.name
request.header.value
request.path
request.query-string.parameter
request.query-string.parameter.name
request.query-string.parameter.value
request.url
```

Issues addressed in this release

Qualys Cloud Suite 2.30 brings you many more improvements and updates.

AV

AssetView

TP

ThreatPROTECT

- Updated Qualys Top 10 widgets to use list-notation for QIDs in query (e.g. QID in brackets []). Now these widgets return QIDs in the filter as expected.
- Vulnerability queries will now be performed as expected when the user clicks on a dashboard chart widget point like a bar chart.
- The widget "sort by" field will now be saved after saving a widget as expected.
- When calculating trend percentage for a dashboard widget, the percentage will now always be calculated against the previous day's value rather than the last trend value, which in some cases could be for the same day.
- List of assets is downloaded successfully even when the number of assets is more than 500.

TP

ThreatPROTECT

- For a new feed article at TP > Dashboard > Feed, the New tag is displayed with the user's first visit to this page. If the user leaves this page and returns the New tag is not shown.
- When removing all columns from the table asset list dashboard widget, the widget preview now displays a message indicating that at least one column must be selected.
- Fixed an issue where deleting a tag which was assigned in the Threat Protection targeted assets would prevent the TP app from loading. Now the TP app always appears to the user when the user selects TP from the application picker.
- Now users can select "tags.businessImpact" as a category in the Add/Edit widget flow.
- Now it's not possible to add a widget with an invalid query. For example if you try to add a widget with an invalid query, an error is returned and the widget is not added.

CA

Cloud Agent

- We've added support for Secure Configuration Assessment (SCA) to Cloud Agent (CA). Users will be able to activate SCA for Cloud Agents when SCA app is enabled for their subscription.
- CA API - Fixed an issue where the Search Activation Key API (/search/ca/agentactkey) did not return the licensed modules as expected.
- User will see static tags applied through the CA activation key on the agent asset after the agent is installed.
- Now users can activate cloud agents for the SCA module.

SAQ**Security Assessment Questionnaire**

- While creating a campaign, the 'Info Security' category is displayed correctly during template selection.
- An appropriate message is displayed when the User does not have the required access permissions.
- Strong password tips are now added to the change password prompt.

WAS**Web Application Scanning**

- We have now fixed an issue to correctly display report values in “” (instead of "e) in Scan report and Web Application report.
- We now show correct information for QID 150100 (Selenium Diagnostics) on the UI as well as in the downloaded report.
- The Scorecard report now supports selection of tags for exclusion without selecting included tags.
- Now adding too many tags during launch of a scan or generation of a report displays all the tags correctly.
- To know more about WAS scans that end in No Web Service status, we now provide a community link that tells you more information about the No Web Service scan status.
- Previously XML and CSV reports had the date/time in Zulu format. With this release, we have normalized the date/time format to be consistent with other reports and is presented with the respective GMT.
- We have now fixed an issue to prevent browser from being unresponsive when an invalid path fuzzing rule is entered.
- We have now fixed an issue to reduce the time to populate information in the Web Application edit window when opened through Quick action Edit menu.
- We have now fixed the issue to view and correctly display the Selenium Crawl script in Internet Explorer browser.
- We have now fixed the issue so that when you apply the scanner appliance filter on Configuration > Appliances page, the datalist now reflects the correct scan results.
- We have now fixed an issue to prevent the error message from being displayed when the correct scanner appliance is selected during editing of web application.
- We have now fixed the issue of scheduled Web application report getting deactivated and targets empty. This was because the schedules were created with tags feature before the include and exclude tag functionality was introduced.
- We have now fixed the issue of scheduled Scorecard report getting deactivated and targets empty. This was because the schedules were created with tags feature before the include and exclude tag functionality was introduced.
- Error in processing of scan result would lead to generation of multiple emails for the same scan. We have now fixed this scenario to prevent multiple emails from being sent.

WAF

Web Application Firewall

- An appropriate error message is returned if SSL certificate has no commonName.
- An appropriate error message is returned when deleting a deprovisioned appliance.
- The input parameters createdBy.* and updatedBy.* have been removed as a search criteria from the WAF Search clusters API.
- Appropriate error messages are returned when mandatory input parameter values are not provided for the Create HTTP Profile API.
- An appropriate error message is returned when a null private key is passed during certificate update.
- An appropriate error message is returned when an invalid value is passed for the parameter tags.tag.id.
- The Creation Date column is now properly aligned on the Security > Rules tab.
- Previously, UNAUTHORIZED response code was returned when persistency was enabled for a web server pool in a web application. This was because authenticated scanning was checked even though scanTrust was not enabled. This is fixed, and now UNAUTHORIZED response code is not returned as authenticated scanning is checked only if scanTrust is enabled.

FIM

File Integrity Monitoring

- Now the user can view a long asset name on the Assets tab and access the Quick Actions drop down menu to take actions on the asset.
- Now the user has the ability to add/update tags for an asset using the View Details option.
- Now the Clear Selected Items link on the Configurations tab is available as expected. This option appears under Categories/Status.
- Dashboard widget datapoints will now be restricted to a minimum size so they are always visible and clickable.
- System-created categories will no longer show the Quick Actions menu and users can no longer edit or delete them.
- Event details permissions matrix will now reflect permissions where both Allow and Deny are checked.
- Now the user can sort profile rules by PATH RULE using the FIM Monitoring Profile wizard.
- On Events tab, fixed Last 30 days default range to be inclusive of start date.

IOC

Indication of Compromise

- When no modules are detected for a given event, we now display a simple label indicating "0 modules loaded".
- Now when the user clicks on quick filters on the Hunting tab, the app returns accurate matches and the query uses double quotes around the query value, i.e. action: "CONNECTED"

Qualys Cloud Platform

- SCA app - This is now available to the user from the app picker.
- Assets Inventory - User will be able to search assets by business impact in their assets inventory (using AssetView, FIM and IOC) using the new tags.businessImpact token.
- Assets Inventory - Secure Config Assessment (SCA) is now available as an additional option to users when activating EC2 assets.
- EC2 Connector - User can now see connector status in API response. List of responses include: PENDING, RUNNING, SUCCESS, ERROR, QUEUED, PROCESSING, FINISHED_SUCCESS, FINISHED_ERRORS
- EC2 Connector - New states are now added in API response for the connector: QUEUED, PROCESSING, FINISHED_SUCCESS, FINISHED_ERRORS. When a new connector is created, the state flow will be such:
QUEUED--> PROCESSING--> FINISHED_SUCCESS/FINISHED_ERRORS
- EC2 Connector - A new state DISABLED is added, which will appear in the API response if the connector is disabled. This disabled connector will display an icon to signify it is disabled, on the UI. Also, the connector list will now auto refresh after 5 minutes (previously it was 2 minutes).
- EC2 Connector - Region name Asia Pacific is now correctly displayed on UI.