

Qualys Cloud Suite 2.x

Version 2.34

August 29, 2018

Here's what's new in Qualys Cloud Suite 2.34!



Continuous Monitoring

[License Counts are enforced for Continuous Monitoring](#)



Security Assessment Questionnaire

[New User Interface for Campaigns Management](#)

[Add Tags to Campaign Questionnaires](#)

[Introducing Risk Rating](#)



Web Application Scanning

[Retrieve Partial Scan Data for Unfinished Scans](#)

[New XSS Power Mode Option Profile](#)

[Assign Tags to Web Application While Importing CSV](#)

[Scanning Swagger-based REST APIs](#)

[Qualys Browser Recorder to create a Selenium script](#)

[Improved WAS Scan Preview Text](#)

[Relaunch Single or Multiple Child Scan Slices](#)



Web Application Firewall

[New keys for custom rules](#)

[New Security Filters for Cipher Selection in Web Applications](#)

[Add SSL Certificate to Non-SSL web applications](#)



Cloud Agent

[Agent installer for FIM/IOC](#)

[Higher Agent Status Interval](#)

Qualys Cloud Platform 2.34 brings you many more
Improvements and updates! [Learn more](#)



License Counts are enforced for Continuous Monitoring

With this release licensing counts are enforced in the Continuous Monitoring (CM) app, for internal and external assets, using the UI and API. This applies to non-trial CM customers only.

- Users are restricted to viewing alerts for assets in their license
- Users can create monitoring profiles for assets in their license

After login to the CM UI, you can easily choose asset tags to be used for licensing under Configuration on the License Details tab. This allows you to select the asset tags to enforce the license counts.

The screenshot shows the Qualys Enterprise Continuous Monitoring interface. The top navigation bar includes 'Configuration', 'Monitoring Profiles', 'Rulesets', and 'License Details'. The 'License Details' tab is active, showing 'Continuous Monitoring License Details' with 'License level: Full' and 'Status: Active'. Below this, the 'License Information' section displays 'Used Licenses' at 9%. A table lists 'Total Purchased Assets' (2000), 'Purchased External Assets' (1000), 'Purchased Internal Assets' (1000), and 'Used Assets' (177). The 'Choose Tags for Monitoring' section allows selecting tags for assets to monitor. It includes a list of tags: '252', 'Groovy-23', 'sp4 - normal tag', 'Asset Groups', 'Asset Search Tags', 'IP-252', 'VM Windows', 'Linux', and 'Cloud Agent'. A red circle highlights the 'Add Tag' button, with a red arrow pointing to it and text saying 'Click to choose assets to add to your CM license'.

How it works - When asset tags are configured for your CM license under Configuration > License Details, the CM module shows alerts only for purchased assets (using CM UI and API), as shown in the license details.

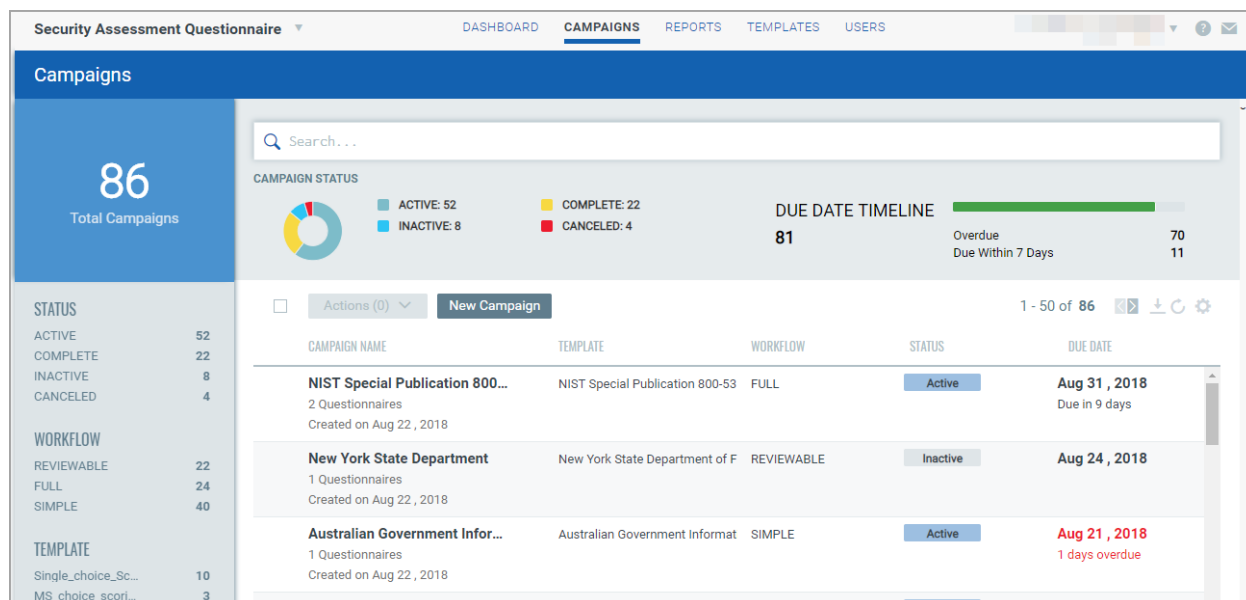
What about my existing monitoring profiles? Once licensing is configured we'll process alerts only for IP addresses in your CM license. If you have a monitoring profile containing IPs not in your CM license, the next time you edit the profile you'll be prompted to change the IPs and select only IPs in your CM license.

New User Interface for Campaign Management

We now have a new interface to make it easier for you to create and manage your campaigns.

You can easily view status and other details of your campaigns and create campaigns using the new UI.

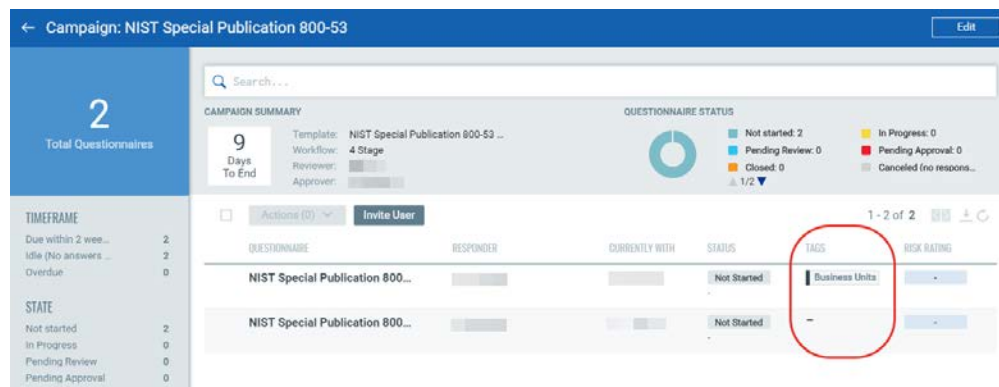
It's easy to get started! Just navigate to the Campaigns tab.



Add Tags to Campaign Questionnaires

You can now assign tags to each questionnaire in your campaign to help you organize your campaign better.

Go to View Summary from the Quick Actions menu of the desired questionnaire and assign the tag.



Introducing Risk Rating

We have enhanced our template scores and risk calculations to help you determine the risk posture of your users.

Set criticality for each question and assign risk scores to each answer while defining your templates. Campaigns launched using this template will give you the risk rating of each questionnaire in your campaign.

To set criticality and scores, go to Template > My Templates, choose a template you want to add scores and go to the Settings tab.

View Template Builder Rules **Settings**

Template Scoring

To calculate the template score we use the question criticality values and the answer scores. The final template score determines the risk rating of your template.

Question Criticality

Use the following predefined values to assign criticality to questions in your template.

None:	1	Medium:	20
Info:	5	High:	30
Low:	10	Critical:	40

Answer Scores

Configure labels and scores for you to pick from while setting scores for answers in your template.

Label	Value
LOW	0
P1	1
P2	2
P3	3
MEDIUM	50

Risk Rating

The risk rating of your template depends on where the template scores lie in the predefined risk brackets.

Very High	81%	To	100%
High	61%	To	80%
Medium	41%	To	60%

Risk Rating for each questionnaire is determined based on the template score which is calculated once the responder completes the questionnaire.

Campaign: NIST Special Publication 800-53 Edit

2 Total Questionnaires

9 Days To End

Template: NIST Special Publication 800-53 ...
Workflow: 4 Stage
Reviewer: [User]
Approver: [User]

QUESTIONNAIRE STATUS

- Not started: 2
- Pending Review: 0
- Closed: 0
- In Progress: 0
- Pending Approval: 0
- Canceled (no response): 0

1 - 2 of 2

QUESTIONNAIRE	RESPONDER	CURRENTLY WITH	STATUS	TAGS	RISK RATING
NIST Special Publication 800...	[User]	[Progress Bar]	Pending Review 4 / 6 Questions	Business Units	100% 9155/13425
NIST Special Publication 800...	[User]	[Progress Bar]	Pending Review 2 / 3 Questions	-	VERY HIGH 8830/9280

Retrieve Partial Scan Data for Unfinished Scans

We have now introduced a new quick action menu to cancel an unfinished scan and still retain the partial scan results of the unfinished scan. The option is enabled for a scan only after 20 minutes of scan goes into Running status. To view the partial data that has been retrieved by the unfinished scan (with Canceled With Results status), click View Report from the quick actions menu.

Good to Know

- The Cancel Scan with Results option is enabled only after 20 minutes of scan goes into Running status.
- The Cancel Scan with Results option is not available for multi-scan.

Tell me the steps

Go to Scans > Scan List, select the scan you want to cancel and select Cancel Scan with Results from the quick action menu. Ensure that the scan is in Running status.

The screenshot shows the 'Scan Management' interface with the 'Scan List' tab active. A table lists several scans. The scan 'Relaunch DiscScanCheckCancel' is selected, and a context menu is open showing various actions. The 'Cancel Scan with Results' option is circled in red.

Name	Status	Progression #	Link
Relaunch DiscScanCheckCancel http://10.11.72.37	Running	-	-
Relaunch Relaunch CustomOptionProfile SP https://10.11.72.37	Running	-	-
2018-07-05 - Discovery Scan Web Application https://10.11.72.37	Running	49	-
Relaunch CancelScanWithResults https://10.11.72.37	Running	433	-

The scan is now in Canceled With Results status. Click View Report to view the partial scan results of the cancelled scan.

You could also use the new status filter to view all scans with Canceled With Results status.

The screenshot shows the 'Scan Management' interface with the 'Scan List' tab active. The 'Canceled With Results' status filter is selected in the left sidebar. The table shows several scans with the status 'Canceled With Results'.

Name	Status	Progression #
10thJuly-AfterRC http://10.11.72.37	Canceled With Results	-
Relaunch Relaunch DiscScanCheckCancel-AfterFix_OnKafka http://10.11.72.37	Canceled With Results	-
ProgressiveKafkaEnabled_check https://10.11.72.37	Canceled With Results	4
Relaunch Relaunch ProgressiveScanCancel_After Fix_OnWatcherWw https://10.11.72.37	Canceled With Results	2
Relaunch ProgressiveScanCancel_After Fix_OnWatcherTest https://10.11.72.37	Canceled With Results	-
Relaunch DiscScanCheckCancel-AfterFix_OnWatcher http://10.11.72.37	Canceled With Results	-
ProgressiveScanCancel_After Fix_OnWatcher https://10.11.72.37	Canceled With Results	1
DiscScanCheckCancel-AfterFix_OnWatcher http://10.11.72.37	Canceled With Results	-
Relaunch Relaunch ProgressiveScanCancel_After Fix https://10.11.72.37	Canceled With Results	1
Relaunch Relaunch Relaunch DiscScanCheckCancel-AfterFix http://10.11.72.37	Canceled With Results	-

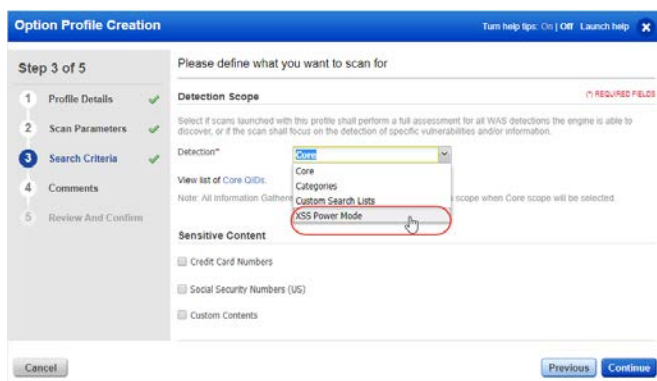
New XSS Power Mode Option Profile

You can now execute specialized scan that performs comprehensive tests for cross-site scripting vulnerabilities using the new option profile with XSS Power Mode detection scope that we have introduced.

The detection scope performs tests using the standard XSS payloads, which detect the most common instances of XSS, but also with additional payloads that can identify XSS in certain, less-common situations. Running a scan with option profile that has XSS Power Mode detection scope will provide the best assurance that your web application is free from XSS vulnerabilities.

XSS Power Mode Detection Scope

Go to Scans > Option Profiles and click New Profile or edit an existing option profile. In case of a new option profile, provide the general profile details, scan parameters and then you can choose XSS Power Mode from the detection dropdown to define the detection scope of the scan.



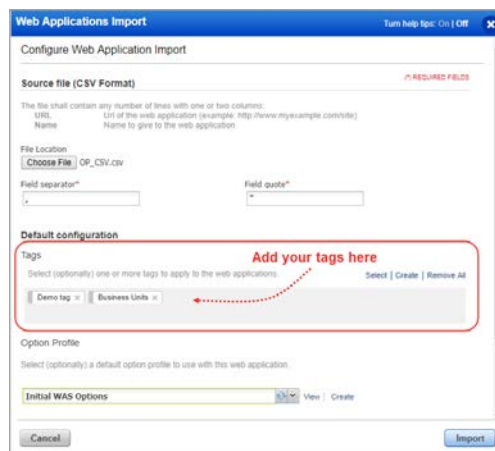
Once you create the option profile, you can use it to launch scans to detect all XSS related vulnerabilities.

Assign Tags to Web Application While Importing CSV

Tagging web applications helps you organize them according to function, location or any criteria you want. You can now tag web applications when you import a CSV file to create a web application.

Go to Web Applications > Web Applications and then click Import to create a web application using CSV file. Browse to your CSV file and define the field separator and field quote.

You could choose from existing tags to create a new tag as well. The tags you select get associated with the web application. Define option profile and the scanner appliance and then click Import.



Scanning Swagger-based REST APIs

You can scan swagger-based REST APIs as well. When you launch a scan, simply point the web application URL to the swagger file in target definition. That's it!

Go to Web Applications > Web Applications and then click New Web Application or edit an existing web application. Specify the swagger file path in the Target Definition section and you can include swagger-based REST APIs in your scan.

Web Application Creation Turn help tips: On | Off Launch help

Step 1 of 11

- 1 Asset Details
- 2 Application Details
- 3 Scan Settings
- 4 Crawl Settings
- 5 Redundant Links
- 6 Authentication
- 7 Exclusions
- 8 Advanced Options
- 9 Malware Inspection

Tell us about the asset you want to scan

Definition (*) REQUIRED FIELD

Let's start with some basic information.

Name*
My Web Application

Target Definition

Web Application URL*
http://www.example.com

For scanning Swagger-based REST APIs, the Web Application URL should point to the Swagger file. It is your responsibility to verify that you have permission to scan all web applications that you specify as scan targets.

Custom Attributes

Provide attribute information that will help you categorize this web application within your subscription.

Name	Value
------	-------

Qualys Browser Recorder to create a Selenium script

You can now use our very own Qualys browser recorder extension to create Selenium scripts and add the scripts to define the crawl scope for your web application.

Qualys Browser Recorder is a free and open source browser extension to record & play back scripts for web application automation testing. Qualys Browser Recorder includes the entire Selenium Core, allowing you to capture web elements and record actions in the browser to let you generate, edit, and play back automated test cases quickly and easily. It also allows you to select an UI element from the browser's currently displayed page and then select from a list of Selenium commands with parameters.

Web Application Edit: Documentation Turn help tips: On | Off Launch help

Edit Mode

- Asset Details
- Application Details
- Scan Settings
- Crawl Settings
- Redundant Links
- Authentication

Add Selenium scripts to help us access different parts of your web application

Selenium scripts (*) REQUIRED FIELD

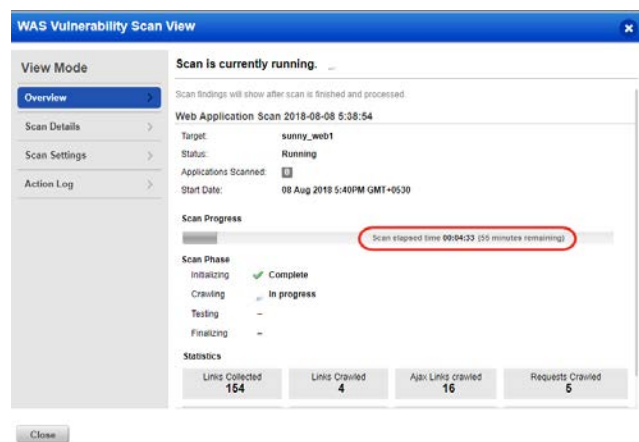
Import the Selenium scripts to be used for scanning this web application. Each script runs one time when its trigger is first encountered by our crawler. Use Qualys Browser Recorder to create a Selenium script. Want to learn more? Watch this video or visit the Qualys Browser Recorder (QBR) chrome extension.

+ Add Script

To learn more about the Qualys Browser Recorder [watch this video](#) or visit the [Qualys Browser Recorder \(QBR\)](#) chrome extension.

Improved WAS Scan Preview Text

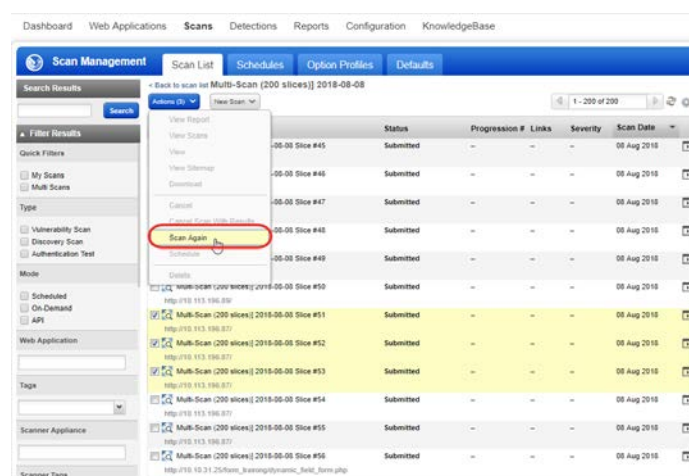
We now display the time that has elapsed since the scan was launched in the scan preview window. The elapsed time now portrays a clear picture of how long the scan has been in progress from the time it has been launched.



Relaunch Single or Multiple Child Scan Slices

We now support relaunch of single or multiple child scan slices at one go. In a multi-scan, where you can scan hundreds or even thousands of web applications in a single scan, you may want to relaunch only few of the child scans. You can now select single or multiple child scan slices of a multi-scan and rescan a scan for the selected slices.

Go to Scans > Scan List and select the multi-scan, then click View Scans from the quick action menu. All the child scans that belong to the multi-scan are displayed. You can select the required child scan and then choose Scan again from the Actions menu to relaunch the required child scans.



The title for such scans is in the format: Relaunch [original scan name] <DATE> <TIME>



New keys for custom rules

Qualys WAF now provides more keys to help you create custom rule conditions.

Here are the new keys introduced:

KEY	SUPPORTED OPERATORS
client.ssl.session.timeout	EQUAL, NOT.EQUAL, IN-RANGE, NOT.IN-RANGE, GREATER, NOT.GREATER, GREATER-EQUAL, NOT.GREATER-EQUAL, LOWER, NOT.LOWER, LOWER-EQUAL, NOT.LOWER-EQUAL
server.ssl.cipher	EQUAL, NOT.EQUAL, MATCH, NOT.MATCH
server.ssl.protocol	EQUAL, NOT.EQUAL
server.ssl.session.timeout	EQUAL, NOT.EQUAL, IN-RANGE, NOT.IN-RANGE, GREATER, NOT.GREATER, GREATER-EQUAL, NOT.GREATER-EQUAL, LOWER, NOT.LOWER, LOWER-EQUAL, NOT.LOWER-EQUAL
server.tcp.port	EQUAL, NOT.EQUAL, IN-RANGE, NOT.IN-RANGE, GREATER, NOT.GREATER, GREATER-EQUAL, NOT.GREATER-EQUAL, LOWER, NOT.LOWER, LOWER-EQUAL, NOT.LOWER-EQUAL
request.body.length	EQUAL, NOT.EQUAL, IN-RANGE, NOT.IN-RANGE, GREATER, NOT.GREATER, GREATER-EQUAL, NOT.GREATER-EQUAL, LOWER, NOT.LOWER, LOWER-EQUAL, NOT.LOWER-EQUAL
response.code	EQUAL, NOT.EQUAL, IN-RANGE, NOT.IN-RANGE, GREATER, NOT.GREATER, GREATER-EQUAL, NOT.GREATER-EQUAL, LOWER, NOT.LOWER, LOWER-EQUAL, NOT.LOWER-EQUAL
response.date	EQUAL, NOT.EQUAL, BETWEEN, NOT.BETWEEN
response.duration	EQUAL, NOT.EQUAL, IN-RANGE, NOT.IN-RANGE, GREATER, NOT.GREATER, GREATER-EQUAL, NOT.GREATER-EQUAL, LOWER, NOT.LOWER, LOWER-EQUAL, NOT.LOWER-EQUAL
response.header	EQUAL, NOT.EQUAL, MATCH, NOT.MATCH, DETECT
response.header.content-length	EQUAL, NOT.EQUAL, IN-RANGE, NOT.IN-RANGE, GREATER, NOT.GREATER, GREATER-EQUAL, NOT.GREATER-EQUAL, LOWER, NOT.LOWER, LOWER-EQUAL, NOT.LOWER-EQUAL
response.header.content-type	EQUAL, NOT.EQUAL, MATCH, NOT.MATCH, DETECT
response.header.cookie	EQUAL, NOT.EQUAL, MATCH, NOT.MATCH, DETECT
response.header.cookie.name	EQUAL, NOT.EQUAL, MATCH, NOT.MATCH, DETECT
response.header.cookie.value	EQUAL, NOT.EQUAL, MATCH, NOT.MATCH, DETECT
response.header.line.length	EQUAL, NOT.EQUAL, IN-RANGE, NOT.IN-RANGE, GREATER, NOT.GREATER, GREATER-EQUAL, NOT.GREATER-EQUAL, LOWER, NOT.LOWER, LOWER-EQUAL, NOT.LOWER-EQUAL
response.header.name	EQUAL, NOT.EQUAL, MATCH, NOT.MATCH, DETECT
response.header.value	EQUAL, NOT.EQUAL, MATCH, NOT.MATCH, DETECT
response.protocol	EQUAL, NOT.EQUAL
response.time	EQUAL, NOT.EQUAL, BETWEEN, NOT.BETWEEN
transaction.day	EQUAL, NOT.EQUAL
transaction.duration	EQUAL, NOT.EQUAL, IN-RANGE, NOT.IN-RANGE, GREATER, NOT.GREATER, GREATER-EQUAL, NOT.GREATER-EQUAL, LOWER, NOT.LOWER, LOWER-EQUAL, NOT.LOWER-EQUAL

	NOT.LOWER, LOWER-EQUAL, NOT.LOWER-EQUAL
transaction.time	EQUAL, NOT.EQUAL, BETWEEN, NOT.BETWEEN

New Security Filters for Cipher Selection in Web Applications

We have made cipher selection for your web applications simple with new security filters. You can choose one or more security filters based on your security requirements. Available security filters are Strong, Good, Weak and Unsafe.

Ciphers are now categorized based on these security filters. We recommend you to choose Strong and Good security filters and corresponding ciphers belonging to these categories for safe and secure communication between your web applications and client browsers.

Configure security filters

In the Web Application Creation/Edit wizard, go to the Application tab. Select the security filters. Selecting a filter lists the corresponding ciphers in the Add ciphers drop-down. Select the appropriate ciphers from the drop-down or click Add All.

Web Application Creation Turn help tips: On | Off Launch help

Step 2 of 6

1 Asset Details ✓
2 Application ✓
3 Security
4 WAF Clusters
5 Comments
6 Review And Confirm

Configure application and network settings

SSL Certificates

Select the profile that stores appropriate SSL materials, and pick the preferred SSL/TLS protocols and ciphers.

Certificate*
Please select a profile Edit Create

Choose the desired protocols and security levels to list the matching ciphers.

SSL/TLS Protocol
☒ TLS 1.2 ☒ TLS 1.1 ☐ TLS 1.0 ☐ SSL v3

Cipher suite security level
☒ Strong ☒ Good ☐ Weak ☐ Unsafe

Cipher Suite
Add ciphers: Search... Add All Remove All

23 ciphers selected

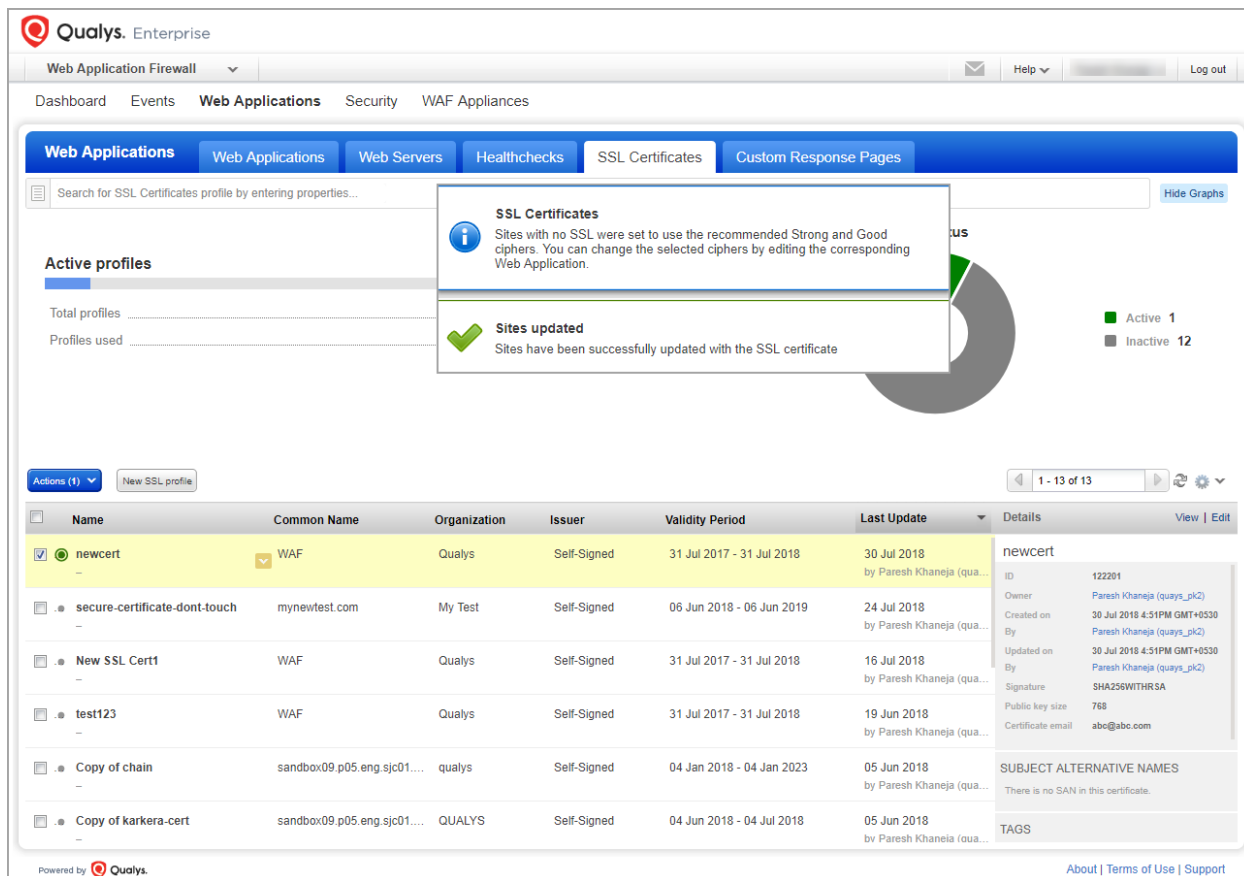
1	ECDHE-ECDSA-AES256-GCM-SHA384	Remove
2	ECDHE-ECDSA-AES128-GCM-SHA256	Remove
3	ECDHE-ECDSA-AES256-SHA384	Remove

Cancel Previous Continue

Add SSL Certificate to Non-SSL web applications

You can now add SSL certificate to non-SSL web applications. Adding the certificate converts a web application into HTTPS. The SSL web application is configured to use default protocols: TLS 1.1 and TLS 1.2 and default security filters: Strong and Good to support HTTPS communication. Later, you can edit the web application to modify these default settings.

To add an SSL certificate, go to Web Applications and click the SSL Certificates tab. Select the SSL certificate and click Add to Sites in the Quick Actions to add the certificate to HTTP web applications.



Qualys Enterprise

Web Application Firewall

Dashboard Events **Web Applications** Security WAF Appliances

Web Applications Web Applications Web Servers Healthchecks **SSL Certificates** Custom Response Pages

Search for SSL Certificates profile by entering properties...

Active profiles

Total profiles: 13
Profiles used: 13

SSL Certificates
Sites with no SSL were set to use the recommended Strong and Good ciphers. You can change the selected ciphers by editing the corresponding Web Application.

Sites updated
Sites have been successfully updated with the SSL certificate

Active 1
Inactive 12

Actions (1) New SSL profile

1 - 13 of 13

Name	Common Name	Organization	Issuer	Validity Period	Last Update	Details
<input checked="" type="checkbox"/> newcert	WAF	Qualys	Self-Signed	31 Jul 2017 - 31 Jul 2018	30 Jul 2018 by Paresh Khaneja (qua...)	newcert ID: 122291 Owner: Paresh Khaneja (quays_pk2) Created on: 30 Jul 2018 4:51PM GMT+0530 By: Paresh Khaneja (quays_pk2) Updated on: 30 Jul 2018 4:51PM GMT+0530 By: Paresh Khaneja (quays_pk2) Signature: SHA256WITHRSA Public key size: 768 Certificate email: abc@abc.com
<input type="checkbox"/> secure-certificate-dont-touch	mynewtest.com	My Test	Self-Signed	06 Jun 2018 - 06 Jun 2019	24 Jul 2018 by Paresh Khaneja (qua...)	
<input type="checkbox"/> New SSL Cert1	WAF	Qualys	Self-Signed	31 Jul 2017 - 31 Jul 2018	16 Jul 2018 by Paresh Khaneja (qua...)	
<input type="checkbox"/> test123	WAF	Qualys	Self-Signed	31 Jul 2017 - 31 Jul 2018	19 Jun 2018 by Paresh Khaneja (qua...)	
<input type="checkbox"/> Copy of chain	sandbox09.p05.eng.sjc01...	qualys	Self-Signed	04 Jan 2018 - 04 Jan 2023	05 Jun 2018 by Paresh Khaneja (qua...)	SUBJECT ALTERNATIVE NAMES There is no SAN in this certificate.
<input type="checkbox"/> Copy of karkera-cert	sandbox09.p05.eng.sjc01...	QUALYS	Self-Signed	04 Jun 2018 - 04 Jul 2018	05 Jun 2018 bv Paresh Khaneia (qua...)	TAGS

Powered by **Qualys**

About | Terms of Use | Support

Agent installer for FIM/IOC

Agent installers for FIM/IOC are different than those used for other modules. On the Install Agent window, click **Download 2.x binaries supporting FIM/IOC** to get the agent installers for FIM/IOC.

Once on the 2.x binaries page, you can click **Download 1.x binaries** to go back to the previous page, to get the agent installers for other modules.

Install Agents

A few things to know before you install agents

Give your key a name and add tags to easily find agents installed using this key. We'll associate the tags to the agent hosts.

Activation Key: **c222f**

Key Type: Unlimited key

Total Count in use: 0

[Download 2.x binaries supporting FIM/IOC](#)

Installation Requirements

	Windows (.exe)	Windows Client Versions Windows Server Versions	Install instructions
	Linux (.rpm)	Red Hat Enterprise Linux CentOS Fedora OpenSUSE SUSE Amazon Linux Oracle Enterprise Linux	Install instructions
	Linux (.deb)	Debian Ubuntu	Install instructions
	Mac (.pkg)	OS X	Install instructions
	AIX (.rpm)	IBM AIX	Install instructions

Higher Agent Status Interval

You can now specify agent status interval of up to 7200 seconds. It is the interval at which an agent requests information from the platform. Range: 900-7200 seconds. Recommended: 7200 for Low performance, 1800 for Normal performance, 900 for High performance.

Configuration Profile Creation

Turn help tips: On | Off

Step 3 of 6

1 General Info

2 Blackout Windows

3 Performance

4 Assign Hosts

5 VM Scan Interval

6 PC Scan Interval

Configure Agent Performance

These settings govern how an agent behaves, from how often it checks into the Qualys Cloud platform, to how often it checks the host for changes. It also includes performance settings that control CPU and network utilization.

Performance

Select one of the performance levels below. Keep the default settings **Customize** or customize them.

Based On: Low

Set Parameters

Agent Status Interval*

Push interval in seconds to update system with Agent's status

900 sec(900 - 7200)

Delta Upload Interval*

Interval an agent attempts to upload detected changes

7 sec(1 - 1800)

Chunk sizes for file fragment uploads*

This is the upload block size, and combined with the above Network throttle Tx, determines network utilization

1024 KB(64 - 10240)

Upgrade Reattempt Interval*

Interval an agent will retry applying a new upgrade to itself

300 sec(180 or more)

Issues addressed in this release

Qualys Cloud Platform 2.34 brings you many more improvements and updates.

AV

AssetView

TP

ThreatPROTECT

- We've added a new search token "lastInventoryDate" that supports date range queries using parameters i.e. [now-1M ... now-1s]. We recommend "lastInventoryDate" for these queries (instead of "lastInventory").
- Fixed an issue where the user was unable to export their dashboard due to backend query handling.
- Now when the user exports a dashboard containing a widget with multiple query groupings, then imports this dashboard, the grouping query displays correctly and performs as expected. Note the query language in the exported widget and imported widget will not look same but it will produce the same output. i.e. widget data will be the same.
- Fixed an issue where some widget legend data displayed incorrect counts. Now legend data displays correct counts.
- Fixed an issue where a nested queries starting with shared value "vulnerabilities.vulnerability:(xxx)" showed incorrect results. These nested queries now show correct results.

CA

Cloud Agent

- Now you can search in Cloud Agent UI on the Azure metadata collected by agents. New search tokens were added.
- Now you can search in Cloud Agent UI on the Google Cloud Platform metadata collected by agents. New search tokens were added.
- Now you can search in Cloud Agent UI on the AWS metadata collected by agents. New search tokens were added.
- Now the query below returns assets without agents installed as expected:
aws.ec2.hasAgent: "false"

WAS

Web Application Scanning

- Fixed a performance issue with downloading a CSV report from the WAS Detections tab.
- We have now improved the description of scan title format in default section of scan tab to "Default value of the scan title, you can use <TYPE> or <DATE> or <WEBAPP_NAME> to include respectively the type, date or web application name in the scan title."
- We have now revised the schedule notification email to allow "&" in the email addresses.
- We have now replaced the old obsolete links on the WAS Welcome page with correct links to the new, self-paced training videos.
- The help tip for "File Extensions" in Scan Parameter Details while creating or editing of an Option Profile is now correctly displayed.

- We have now fixed the formatting issue for the web application name and further data to be displayed under their appropriate columns in the CSV report.
- In the scan launch API request, existing scan ID is returned instead of NameUniquessException exception for the scan with same title if scan entry was created in past 2 hours, regardless of scan status.
- The scan report is now successfully generated even when the Timeout Error Threshold and Unexpected Error Threshold settings in option profile are unchecked.
- We have now fixed issue during launch of a schedule and now schedules are launched without any errors.

WAF

Web Application Firewall

- WAF doesn't allow a web application to have the same name or URL (primary/secondary) of an existing web application. If you want to add the name/URL of an already existing asset, you must provision the web application from Asset View, or delete the existing web application from Asset view, and then create a new one from WAF.
- Fixed an issue where upon selecting a custom response page, the details pane did not show the clusters or rules the custom page is assigned to.
- Web Servers tab overview panel now displays a progress bar and a pie chart to show servers of different type, whether docker or regular (classic).
- Rules overview panel now displays all actions by default, irrespective of any rules configured with them.
- Rules tab filters now do not contain the Type filter, as virtual patches and exceptions have now been converted to only one type - custom rules.
- Fixed an issue where editing an existing custom response page or HTTP profile, and then saving as another profile, did not save any changes made before doing the Save As.
- We've removed all instances of "partial" status for appliances throughout the application.
- You can now sort Web Applications, WAF Clusters, and WAF Appliances according to the deployment status.
- Fixed an issue where searching an existing WAF appliance by Name (as in the Name column in the list view), did not return any results.
- Fixed an issue where during web applications edit, users were not able to select certain certificates from the certificate drop-down in Web Applications wizard.
- Fixed the Name column title in Rules tab.
- Event details now display the name of a custom rule instead of the rule UUID, but displays the rule UUID if the custom rule doesn't exist anymore.
- Security policy name is now restricted to 128 characters using the WAF API.
- Fixed an issue where the help tip for Actions in Rule Create/Edit wizard did not match the options shown in the Action drop-down.

Qualys Cloud Platform

- Now an asset tag created using the VM app (Assets > Asset Search) can be edited using the AssetView app by user who created the tag.
- Now you can search for users by tags associated with the user under User Management in the Administration utility.
- Qualys PCP users now have the option to enter their base account credentials, instead of using default Qualys account, for connectors. This capability is available for PCP customers.
- We have now fixed the authentication issue for upgrade connector: when the user switches from access and secret key authentication to ARN authentication, ARN authentication gets successfully implemented.

- Fixed an issue in AssetView where a customer could not view Host ID details for assets in Asset Details under Asset Summary.
- Fixed an issue where Host Asset Search API request failed intermittently (<base URL>/qps/rest/2.0/search/am/hostasset/).
- We've added asset tokens for searching docker information: isDockerHost (true|false), docker.dockerVersion, docker.noOfContainers, docker.noOfImages.