Qualys Cloud Platform v2.x

Release Notes

Version 2.44

February 25, 2020 (Updated March 11, 2020)

Here's what's new in Qualys Cloud Suite 2.44!

CA Cloud Agent

WAS Web Application Scanning

Qualys Cloud Platform

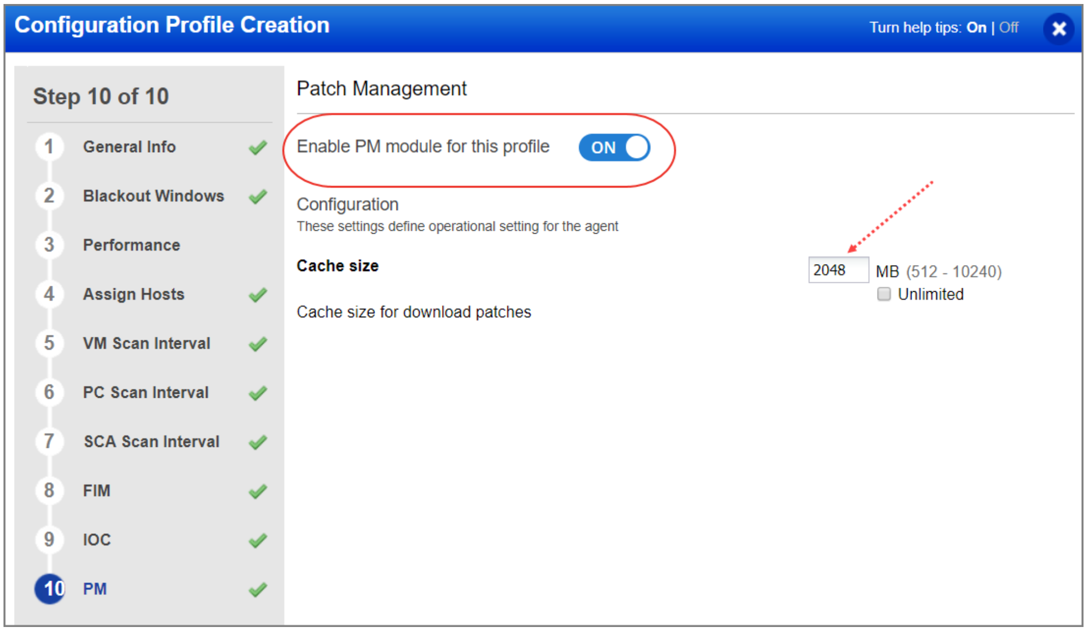
Qualys Cloud Platform 2.44 brings you many more Improvements and updates! Learn more

CA Cloud Agent

Enhancements to Configuration Profile

The Cloud Agent Configuration Profile is now enabled for Patch Management by default, and the default value of the cache size is increased to 2048 MB.

The cache size determines how much space the agent should allocate to store downloaded patches on the asset.



Configuration Profile Creation

Turn help tips: On | Off

Step 10 of 10

1 General Info ✓
2 Blackout Windows ✓
3 Performance
4 Assign Hosts ✓
5 VM Scan Interval ✓
6 PC Scan Interval ✓
7 SCA Scan Interval ✓
8 FIM ✓
9 IOC ✓
10 PM ✓

Patch Management

Enable PM module for this profile ON

Configuration

These settings define operational setting for the agent

Cache size 2048 MB (512 - 10240)

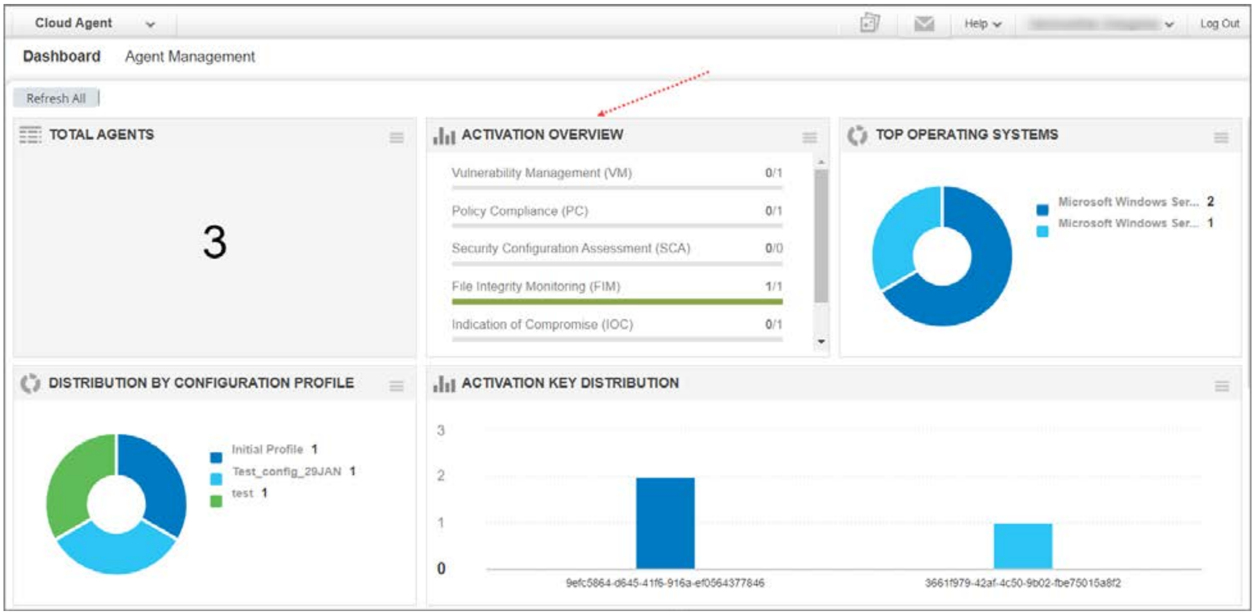
□ Unlimited

Cache size for download patches

‘Licenses’ to ‘Activation’ changes

Each Qualys App will now manage its own licenses. Therefore the word “Licenses” is now changed to “Activation” at a few places on the Cloud Agent UI. This means the Cloud Agent UI will now show agents activated for ‘n’ number of apps, instead of showing ‘n’ licenses being consumed.

For example, on the Cloud Agent dashboard, the widget "License Overview" is now called "Activation Overview". Similar changes are done at other places on the UI.


Cloud Agent
Help
[redacted]
Log Out
Dashboard
Agent Management
Refresh All
TOTAL AGENTS
3
ACTIVATION OVERVIEW
TOP OPERATING SYSTEMS
Microsoft Windows Ser... 2
Microsoft Windows Ser... 1
DISTRIBUTION BY CONFIGURATION PROFILE
Initial Profile 1
Test_config_29JAN 1
test 1
ACTIVATION KEY DISTRIBUTION
3
2
1
0
9efc5864-d645-41f6-916a-ef0564377846
3661f979-42af-4c50-9b02-fbe75015a8f2

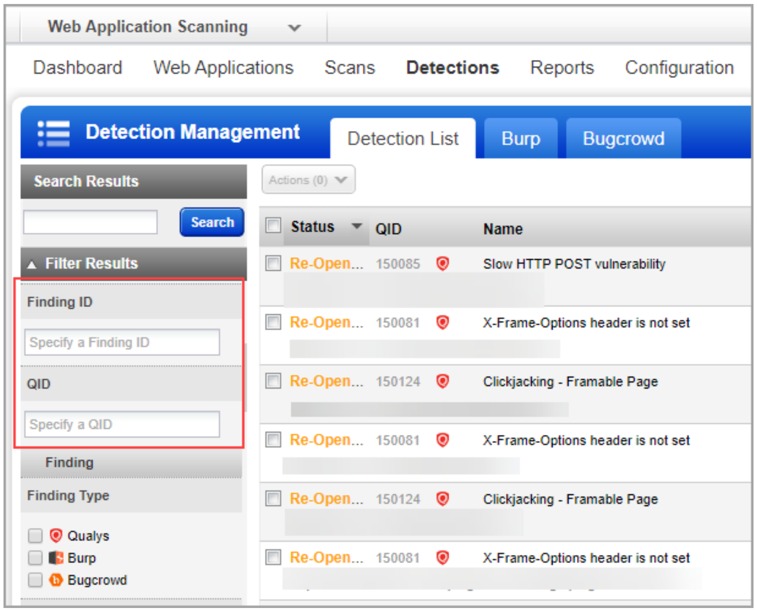
Vulnerability Management (VM)	0/1
Policy Compliance (PC)	0/1
Security Configuration Assessment (SCA)	0/0
File Integrity Monitoring (FIM)	1/1
Indication of Compromise (IOC)	0/1

WAS **Web Application Scanning**

Detection Search Simplified with New Filters

We have now introduced two new filters in Detections tab for you to quickly search the required detections. You could either directly specify the QID or Finding ID and view the finding details.

Go to Detections tab and in the left pane, you can view the new filters. Type the QID or Finding ID and narrow down your search results.



□	Status	QID	Name
□	Re-Open...	150085	Slow HTTP POST vulnerability
□	Re-Open...	150081	X-Frame-Options header is not set
□	Re-Open...	150124	Clickjacking - Framable Page
□	Re-Open...	150081	X-Frame-Options header is not set
□	Re-Open...	150124	Clickjacking - Framable Page
□	Re-Open...	150081	X-Frame-Options header is not set

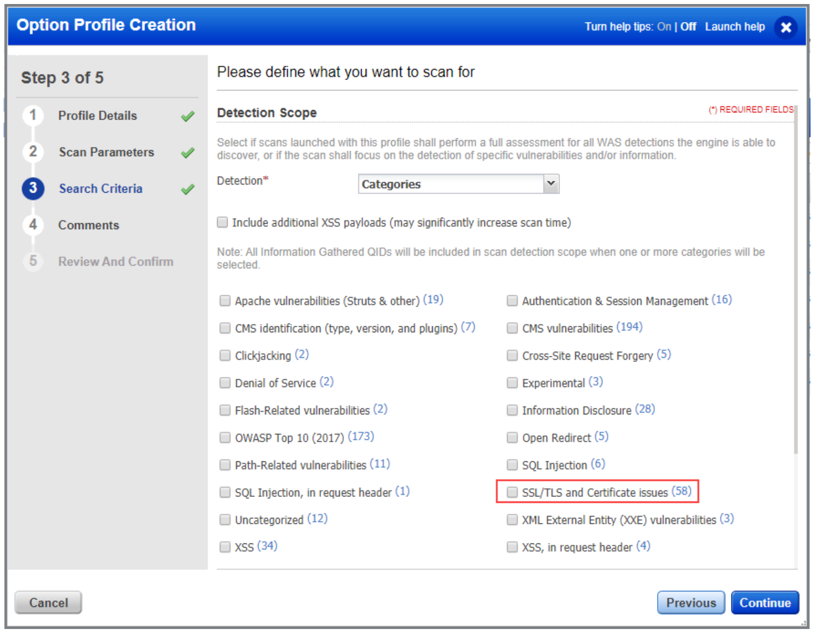
Support for SSL Lab Information

We now support detection and reporting of SSL/TLS and certificate related vulnerabilities in WAS. To include SSL/TLS and certificate related vulnerabilities in your scan, you need to choose the correct detection scope when you define or update the option profile for the scan.

Scans

Go to Configuration > Option Profiles and click New or you could update an existing option profile. When you define the detection scope for an the option profile, you could choose any of the options except XSS Power Mode.

For example, if you choose Categories as detection scope, we have now added a new category for SSL/TLS and certificate related vulnerabilities.



Option Profile Creation

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*: Categories

☐ Include additional XSS payloads (may significantly increase scan time)

Note: All Information Gathered QIDs will be included in scan detection scope when one or more categories will be selected.

☐ Apache vulnerabilities (Struts & other) (19)
☐ CMS identification (type, version, and plugins) (7)
☐ Clickjacking (2)
☐ Denial of Service (2)
☐ Flash-Related vulnerabilities (2)
☐ OWASP Top 10 (2017) (173)
☐ Path-Related vulnerabilities (11)
☐ SQL Injection, in request header (1)
☐ Uncategorized (12)
☐ XSS (34)
☐ Authentication & Session Management (16)
☐ CMS vulnerabilities (194)
☐ Cross-Site Request Forgery (5)
☐ Experimental (3)
☐ Information Disclosure (28)
☐ Open Redirect (5)
☐ SQL Injection (6)
☐ SSL/TLS and Certificate issues (58)
☐ XML External Entity (XXE) vulnerabilities (3)
☐ XSS, in request header (4)

Reports

The scan report includes the different types of SSL/TLS and Certificate issues. Depending on the finding type, the details are listed in the Information Gathered or Information Disclosure section of the report.

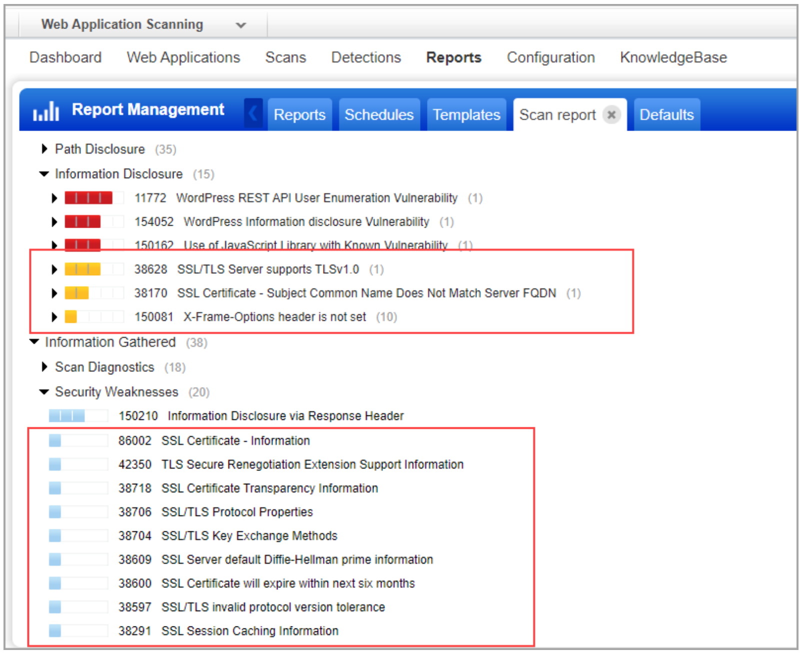
The different types of SSL/TLS and certificate issues that we support are:

- SSL Data with Certificate Fingerprint

- SSL Data with Prop

- SSL Data with Kex

- SSL Data with Ciphers



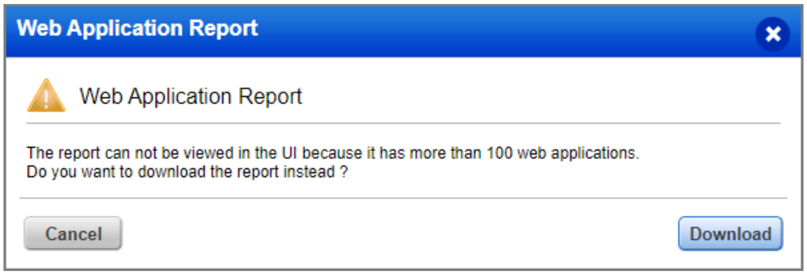
Path Disclosure (35)
Information Disclosure (15)
11772 WordPress REST API User Enumeration Vulnerability (1)
154052 WordPress Information disclosure Vulnerability (1)
150162 Use of JavaScript Library with Known Vulnerability (1)
38628 SSL/TLS Server supports TLSv1.0 (1)
38170 SSL Certificate - Subject Common Name Does Not Match Server FQDN (1)
150081 X-Frame-Options header is not set (10)
Information Gathered (38)
Scan Diagnostics (18)
Security Weaknesses (20)
150210 Information Disclosure via Response Header
86002 SSL Certificate - Information
42350 TLS Secure Renegotiation Extension Support Information
38718 SSL Certificate Transparency Information
38706 SSL/TLS Protocol Properties
38704 SSL/TLS Key Exchange Methods
38609 SSL Server default Diffie-Hellman prime information
38600 SSL Certificate will expire within next six months
38597 SSL/TLS invalid protocol version tolerance
38291 SSL Session Caching Information

Notification for Huge Reports

Report generation may sometimes fail if the report is generated for large number of web applications. To avoid such failures, we have now categorized report generation as per the number of web applications being included in the report. The categorization is as follows:

Number of Web Applications/Scans	Online Report	Download Report
Less than or equal to 100	Yes	Yes
101 to 500	No	Yes
More than 500	No	No

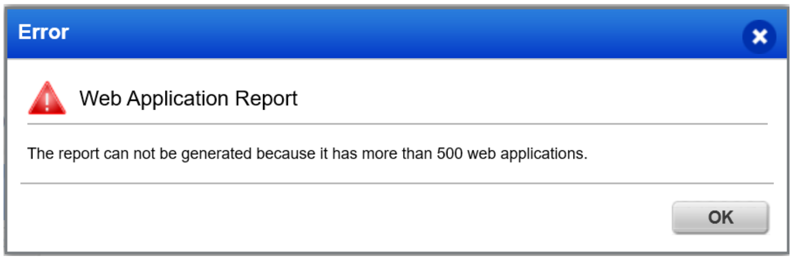
For web applications in the range of 101 to 500, the report is not available online on UI but can be directly downloaded.



Web Application Report

The report can not be viewed in the UI because it has more than 100 web applications.
Do you want to download the report instead ?

But if the number of web applications exceeds 500, report cannot be generated and error message is displayed in such cases.



Web Application Report

The report can not be generated because it has more than 500 web applications.

For web applications less than 100, you can view the report on the UI as well as download it.

Patch Vulnerabilities from Asset Details

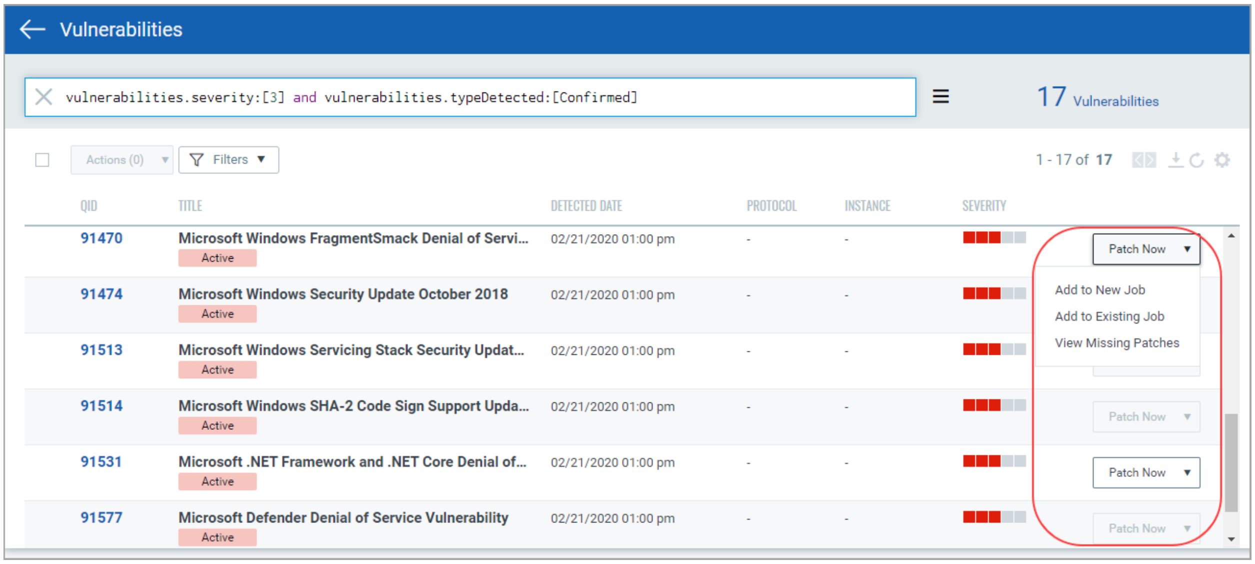
We now provide you with an option to directly patch vulnerabilities for an asset from the Asset Details page of the following modules:

- Vulnerability Management in case the new VM Dashboard Beta is enabled
- Global IT Asset Inventory

Patching of vulnerabilities is possible only if you have subscribed for Patch Management module and have activated the asset for Patch Management.

To patch the vulnerabilities for an asset, simply go to Asset Details of that asset and view the list of vulnerabilities. Click Patch Now against the vulnerability to initiate the patching process.

Note: The Patch Now button is enabled only when Qualys can automatically patch the vulnerability.



```
vulnerabilities.severity:[3] and vulnerabilities.typeDetected:[Confirmed]
```

17 Vulnerabilities

1 - 17 of 17

QID	TITLE	DETECTED DATE	PROTOCOL	INSTANCE	SEVERITY
91470	Microsoft Windows FragmentSmack Denial of Servi... Active	02/21/2020 01:00 pm	-	-	🟥🟥🟥⬜⬜
91474	Microsoft Windows Security Update October 2018 Active	02/21/2020 01:00 pm	-	-	🟥🟥🟥⬜⬜
91513	Microsoft Windows Servicing Stack Security Updat... Active	02/21/2020 01:00 pm	-	-	🟥🟥🟥⬜⬜
91514	Microsoft Windows SHA-2 Code Sign Support Upda... Active	02/21/2020 01:00 pm	-	-	🟥🟥🟥⬜⬜
91531	Microsoft .NET Framework and .NET Core Denial of... Active	02/21/2020 01:00 pm	-	-	🟥🟥🟥⬜⬜
91577	Microsoft Defender Denial of Service Vulnerability Active	02/21/2020 01:00 pm	-	-	🟥🟥🟥⬜⬜

Issues addressed in this release

Qualys Cloud Platform 2.44 brings you many more improvements and updates.

AV AssetView

- Fixed an issue where an error was shown while converting an already existing static tag into a dynamic tag.
- Purge Rule UI performance is now improved.

SAQ Security Assessment Questionnaire

- When a user was re-assigned any template as part of a campaign and the pre-fill option was selected, the invitee user got an error while opening that questionnaire. We have fixed this issue and the invitee user is now able to see pre-filled answers along with attachments from the user's earlier response.
- In the Attach File window, an appropriate number attachments are now displayed as per the count selected in Rows Shown option.
- The Qualys Logo was not displayed properly in the Questionnaire email. We have fixed this issue and now the user can see Qualys logo in Questionnaire email notifications.
- We fixed an issue where on saving the Vendor Risk Assessment (288 questions) template in the questionnaire, the symbols " " (double quotes), > (greater than) and < (less than) within the template were showing their corresponding HTML names, such as &quot for double quotes, &lt for less than and &gt for greater than. Now, these symbols are shown appropriately after saving the template.

WAS Web Application Scanning

- Deleting a web application reflected in multiple errors for the web application in catalog. We have now fixed the issues so that despite a web application is deleted, you can now successfully use "Add to Subscription" option and also change the status of the web application.
- We have now fixed an issue so that the comment you add to a QID in Knowledgebase is automatically wrapped and does not overflow from the comment box. The maximum limit for the comment is 1024 characters.
- We have now fixed a spelling of increased that was incorrectly displayed after editing the severity of a QID in Knowledgebase and also in Detections list.
- We have now updated our syntax to dynamically adapt to changes made by POSTMAN for collection file upload and thus prevent the upload failure error.
- We have now fixed the Remove button functionality for POSTMAN collection environment variables so that it removes only the required environment variable and not all other variables.
- We have now fixed all issues so that the auto-generated scan notification email now correctly displays the WAS Scan URL.
- The text content of POST and GET data in Vulnerability Details (for detections) is now automatically wrapped to display it correctly.

WAF Web Application Firewall

- Fixed an issue in the Events tab where the UI did not display the correct results upon clicking the events bar chart to drill down further.

Qualys Cloud Platform

- Fixed an issue where the text on the "Log out" button was inconsistent on different Qualys Cloud Platforms.