



Qualys Cloud Platform v2.x

Release Notes

Version 2.33

June 25, 2018 (updated on November 19, 2020)

Here's what's new in Qualys Cloud Suite 2.33!

[Grant Dashboard Permissions to a user role](#)

[View Cloud Provider metadata collected by Cloud Agents](#)

SAQ Security Assessment Questionnaire

[Import questions from Question Bank or Library](#)

WAS Web Application Scanning

[Enhancements to Scan View and Scan Phases](#)

[Case-Sensitive Name Sorting](#)

[New Filter for Retesting Detections](#)

[Retest Multiple Findings with same QID](#)

[Granular Filters for Scheduled Web Applications](#)

[Enhancements to Scan Report](#)

WAF Web Application Firewall

[Install WAF appliance on Docker](#)

[Web Server profile for containers](#)

[Securing your web applications with http headers](#)

[New detection categories in security policy](#)

[Upgrade specific WAF appliances](#)

[UI improvements](#)

Qualys Cloud Platform 2.33 brings you many more Improvements and updates! [Learn more](#)

Grant Dashboard Permissions to a user role

We have now added three new permissions to allow a user to add, edit and delete dashboards. You can now configure these permissions for a user role on need basis.

Following are the default permission settings:

- For the existing subscriptions, all the roles have these permissions enabled.
- New Managers and Unit Managers have all the permissions enabled for new subscriptions.
- New Scanner role only has the create permission enabled for new subscriptions.

Where do I configure the permissions?

Choose the Administration utility on the module picker. Then Go to Role Management.

Role Edit: SCANNER Turn help tips: On | Off

Edit Mode

- Role Details
- Permissions**
- Action Log

Edit permissions for this role

Select how users would access this application

☒ UI Access ☐ API Access

Select modules which this role should have access. For each role you can define which permissions would be granted

Modules

Role Permissions by Modules (15) [Remove All](#)

AM Asset Management [Remove](#)

- Tag Permissions (4 of 4)
- Asset Management Permissions (5 of 5)
- Dashboard Permissions (3 of 3)**
 - ☒ Create Dashboards(and Edit/Delete for user's created Dashboard)
 - ☒ Edit any Dashboard(includes Widget editing)
 - ☒ Delete any Dashboard

new permissions for dashboards and widgets

[Cancel](#) [Save](#)

Edit the role for which you want to configure permissions. Search for the Asset Management module and click Dashboard Permissions.

To enable or disable a permission, select or clear a checkbox.

The Edit and Delete Dashboards permissions allow you to take these actions on dashboards created by other users as long as those dashboards are visible to you.

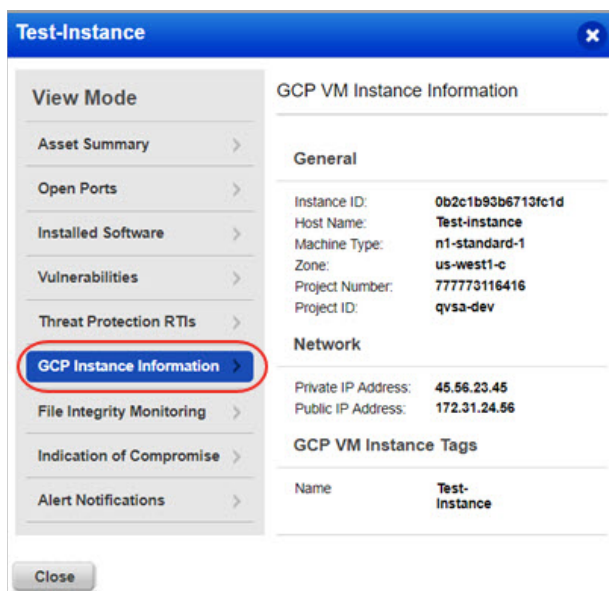
View Cloud Provider metadata collected by Cloud Agents

Your cloud agents will now collect virtual machine instance information for Amazon AWS, Azure and Google Cloud Platform. This information will appear in Asset Details in Cloud Agent (CA) and AssetView (AV). Based on the cloud provider, the instance information includes details like the instance ID and name, machine type, location, operating system, IP address and more.

How to view instance information

In Cloud Agent, go to Agent Management > Agent and choose View Asset Details for the agent host that you are interested in. In AssetView, go to Assets > Assets and choose View Asset Details for the asset you are interested in. Then locate the tab of your cloud provider to view instance information collected by cloud agents.

Sample GCP instance information



The screenshot shows a window titled "Test-Instance" with a sidebar on the left and a main content area on the right. The sidebar contains a "View Mode" section with several options: "Asset Summary", "Open Ports", "Installed Software", "Vulnerabilities", "Threat Protection RTIs", "GCP Instance Information" (highlighted with a red circle), "File Integrity Monitoring", "Indication of Compromise", and "Alert Notifications". The main content area displays "GCP VM Instance Information" with two sections: "General" and "Network".

GCP VM Instance Information	
General	
Instance ID:	0b2c1b93b6713fc1d
Host Name:	Test-instance
Machine Type:	n1-standard-1
Zone:	us-west1-c
Project Number:	777773116416
Project ID:	qvsa-dev
Network	
Private IP Address:	45.56.23.45
Public IP Address:	172.31.24.56
GCP VM Instance Tags	
Name	Test-Instance

A "Close" button is located at the bottom left of the window.

Sample Azure VM information

The screenshot shows a window titled 'rhel73' with a sidebar on the left and a main content area on the right. The sidebar contains a 'View Mode' section with several options: Asset Summary, System Information, Agent Summary, Network Information, Open Ports, Installed Software, Vulnerabilities, File Integrity Monitoring, Alert Notifications, and Azure VM Information. The 'Azure VM Information' option is highlighted with a red circle. The main content area displays the 'Azure VM Information' for a VM named 'rhel73'. The information is organized into sections: VM Details, Network, and Azure VM Tags.

VM Details	
VM Name:	rhel73
Platform (OS Type):	Linux
Size:	Basic_A1
Image Offer:	RHEL
Image Publisher:	RedHat
Image Version:	7.3.2017090723
Subscription ID:	2c92b89c-3427-42de-9c47-ece6eb8cb620
Location:	SouthIndia
Resource Group Name:	azureqa

Network	
Private IP Address:	10.0.0.5
Public IP Address:	104.211.218.183
MAC Address:	000D3AF2AAAD
Subnet:	10.0.0.0

Azure VM Tags	
Project:	qU@LY\$
CreatedBy:	GK
ComputerName:	RHEL7.3
ENV:	DevTestLab
ResourceGroup:	azureqa
Location:	South India

Close

Sample EC2 information

The screenshot shows a window titled 'test-instance' with a sidebar on the left and a main content area on the right. The sidebar contains a 'View Mode' section with several options: Asset Summary, Open Ports, Installed Software, Vulnerabilities, Threat Protection RTIs, Compliance, EC2 Information, File Integrity Monitoring, Indication of Compromise, and Alert Notifications. The 'EC2 Information' option is highlighted with a red circle. The main content area displays the 'EC2 Information' for an instance named 'test-instance'. The information is organized into sections: General, Location, and Network.

General	
Instance ID:	i-0e3eea08949075f43
Instance Type:	t2.micro
Created Date:	2017-12-20 05:46:19.0
State:	STOPPED
Spot Instance:	Yes
Image (AMI) ID:	ami-58d65b3b
Account ID:	205767712438

Location	
Region:	Asia Pacific (Singapore)
Availability Zone:	ap-southeast-1b
Zone:	VPC
Subnet ID:	subnet-9dddb8f8

Network	
VPC ID:	vpc-c9f643ec
DNS (Private):	ip-172.30.1.59.ap-southeast.1.compute.internal
DNS (Public):	-
IP Address (Private):	172.30.1.59
IP Address (Public):	-
Group ID:	sg-a184f9c4
Group Name:	default

Close

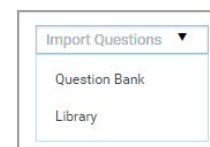


Security Assessment Questionnaire

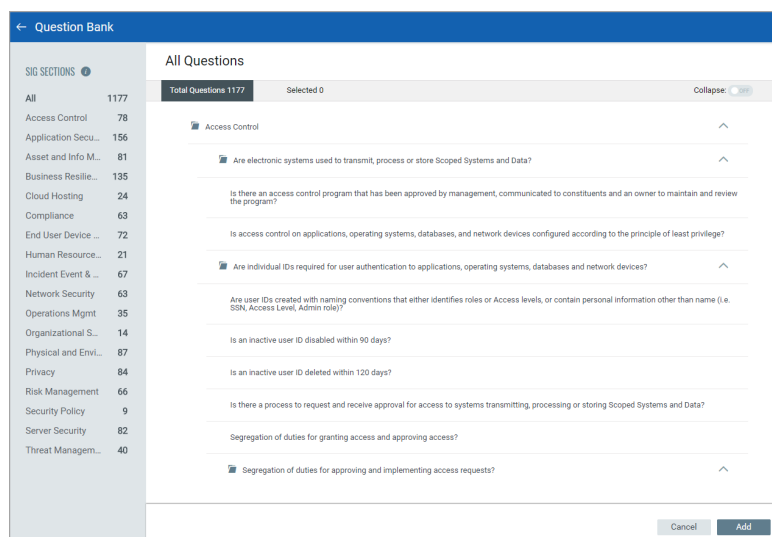
Import questions from Question Bank or Library

We now provide a ready list of questions and answers based on sections from Shared Assessments Standardized Information Gathering (SIG) Question Bank and from out of box templates in our Library.

While adding questions to your template just select Question Bank or Library from the Import Questions drop down.



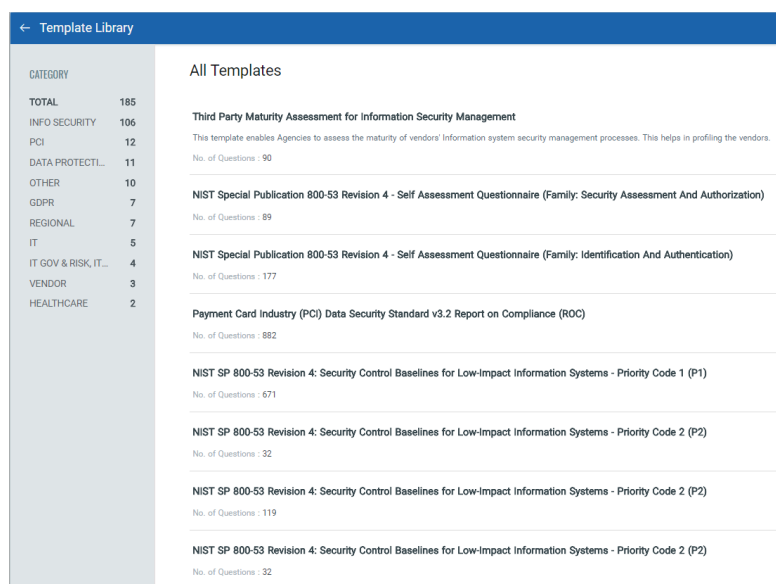
Question Bank



The Question Bank consist of ready to use questions and answers based on Shared Assessments Program for SIG questionnaire, used to perform an initial assessment of your vendors.

Simply pick the ones applicable to you and add them to your questionnaire template.

Library



Library lists all the questions available in our library of out of box templates that cover common compliance standards such as ISO, PCI-DSS, HIPAA, NIST, GDPR, and vendor risk guidelines.

Pick the relevant sections or questions to create your own questionnaire

Enhancements to Scan View and Scan Phases

We now display more information in the scan view to give you a better picture about the scan progress by displaying the scan phases along with the status. We now also display additional scan statistics during the scan.

Scan Phases

Let us launch a scan and view the scan progress. Go to Scans > Scan List > New Scan. Define the scan details, settings and then launch the scan. Once the scan is launched, go to the quick actions menu and select View. You can view the scan progress and the various phases it undergoes before the scan is completed.

We now display the progress of each phase for you to know the scan status.

- Initializing
- Crawling
- Testing
- Finalizing

We also display the scan progress bar that tells you the expected time to complete the scan.

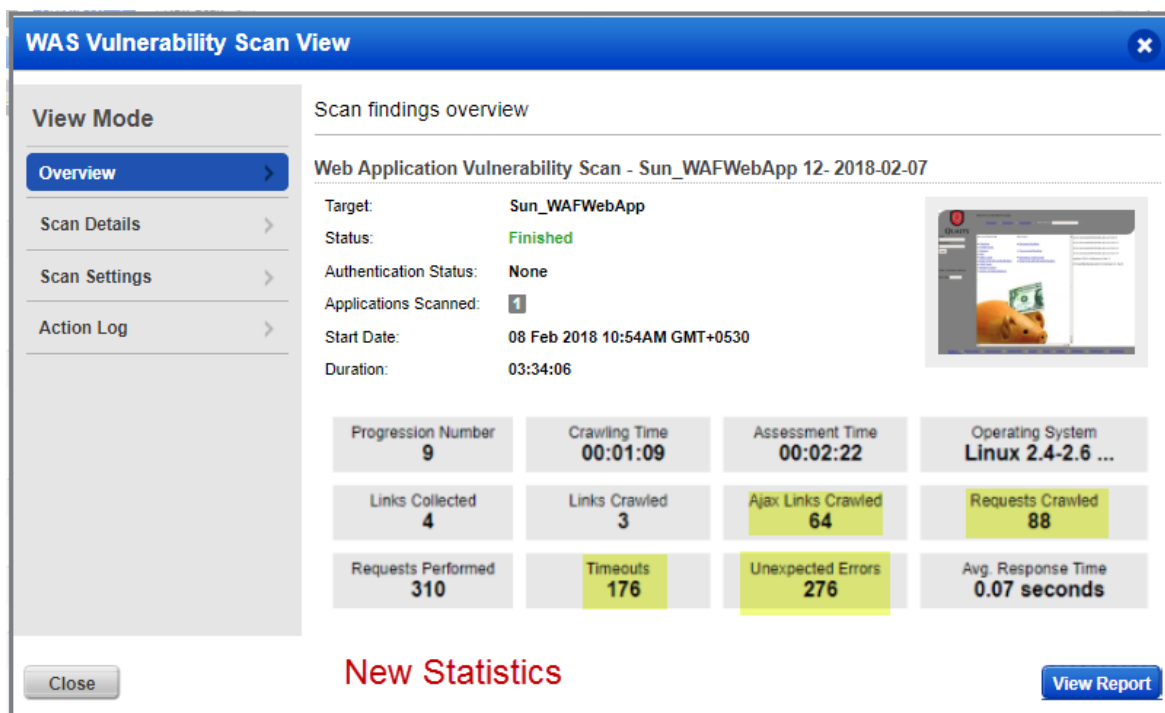
The screenshot displays the 'WAS Vulnerability Scan View' window. On the left is a 'View Mode' sidebar with options: Overview (selected), Scan Details, Scan Settings, and Action Log. The main content area shows 'Scan is currently running.' with a status of 'Running'. It lists 'Target: CheckProgressiveScan', 'Applications Scanned: 0', and 'Start Date: 22 May 2018 5:33PM GMT+0530'. A 'Scan Progress' section, highlighted with a red box, shows a progress bar for 'Scan running since -6:36:-58 (6 hours remaining)' and a table of scan phases: Initializing (Complete), Crawling (In progress), Testing (—), and Finalizing (—). Below this is a 'Statistics' section with eight metrics in a grid: Links Collected (5544), Links Crawled (146), Ajax Links crawled (0), Requests Crawled (0), Requests Performed (272), Timeouts (0), Unexpected Errors (0), and Avg. Response Time (0.55 seconds). A 'Close' button is at the bottom left.

Statistics			
Links Collected	Links Crawled	Ajax Links crawled	Requests Crawled
5544	146	0	0
Requests Performed	Timeouts	Unexpected Errors	Avg. Response Time
272	0	0	0.55 seconds

Additional Scan Statistics

We now display few more scan statistics to help you analyze your scan in a better manner.

Once the scan achieves Finished status, you can select View from quick actions menu and view the scan statistics. We now also display: Ajax Links Crawled, Request Crawled, Timeout Errors, Unexpected Errors for the scan.

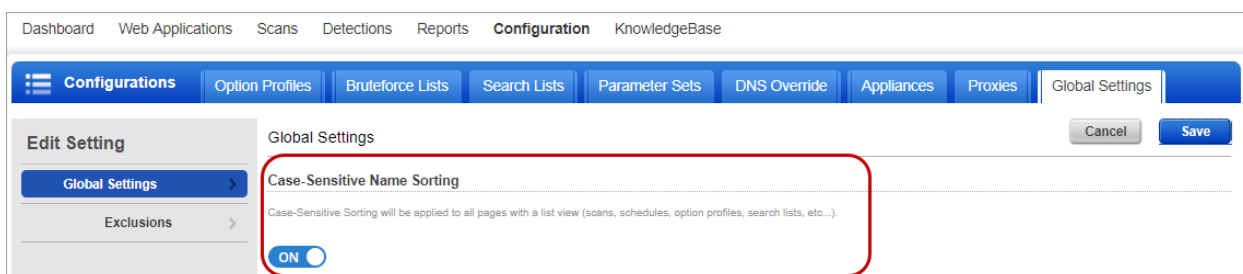


Case-Sensitive Name Sorting

We have now introduced configurable case-sensitive name sorting of your data list. Enable case-sensitive name sorting from Global Settings and then you can sort names of scans, schedules, option profiles, search lists, and such other data lists.

How do I configure the setting?

Go to Configuration > Global Settings. By default, the Case-Sensitive Name Sorting is enabled. To change the setting, click Edit. You can then toggle and configure the sorting to enable or disable as per your need. Click Save to save your changes.



The case-sensitive name sorting setting is visible to you only if "Edit Global Settings" permission is enabled for you.

We have now added a new filter to easily filter detections that are being retested.

Dashboard Web Applications Scans **Detections** Reports Configuration KnowledgeBase

Detection Management Detection List Burp Bugcrowd

Search Results

Filter Results

☐ 1
 ☐ 2
 ☐ 3
 ☐ 4
 ☐ 5

Status

☐ New
☐ Active
☐ Re-Opened
☐ Protected
☐ Fixed
☒ Retesting

Group

You can now club the multiple findings that belong to the same QID and web application and launch a retest in a single batch. The retest scan is launched with settings used in the latest scan on the web-application.



Go to Detections > Detections List. You can use filters in the left-pane to view all findings of same QID and web application. Select the findings to be retested.

From the Actions menu, select Retest. Once you confirm, the retest scan would be launched on all the selected findings at one go.

If the retest scan is launched for multiple findings, and if you cancel the retest for any of the findings, the retest scan is cancelled for the entire batch of findings.

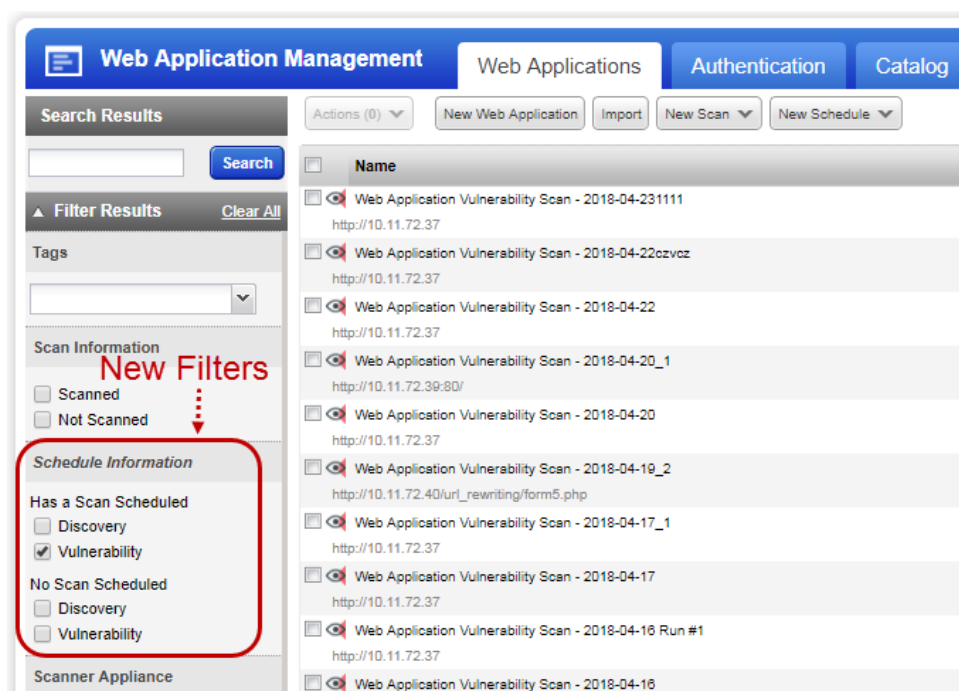
Granular Filters for Scheduled Web Applications

New granular filters are now added for quick filtering of Web application schedules. The new filters: Has a Scan Scheduled and No Scan Scheduled are available for discovery as well as vulnerability scan schedules.

Go to Web Applications > Web Applications and you can see four new filters in Schedule Information section.

- Has a Scan Scheduled: Choose this filter to view web applications with active scheduled scans. You could further filter web applications depending on the type of scan: discovery or vulnerability.

- No Scan Scheduled: Choose to filter to view all the web applications except the one for which the scan schedules exist. You could further filter web applications depending on the type of scan: discovery or vulnerability.

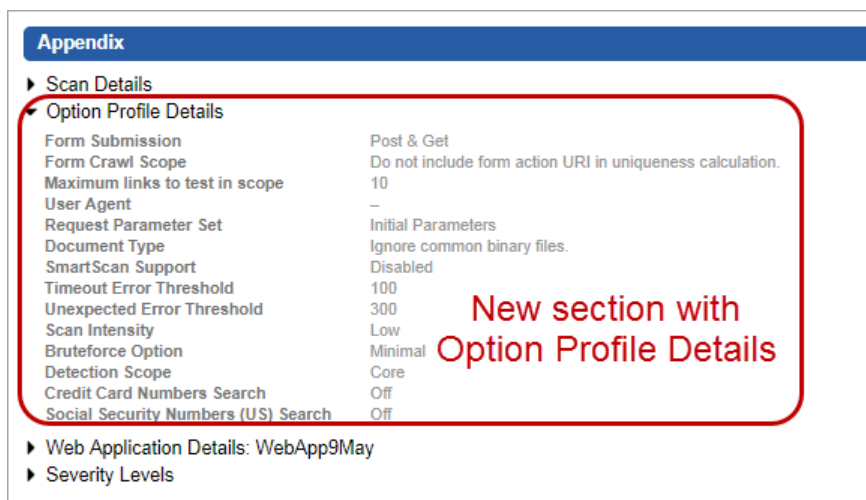


Enhancements to Scan Report

The Scan Report now gives you more information as we have now added a new section titled “Option Profile Details”. The information is available all report formats.

Let us generate the scan report and view the details.

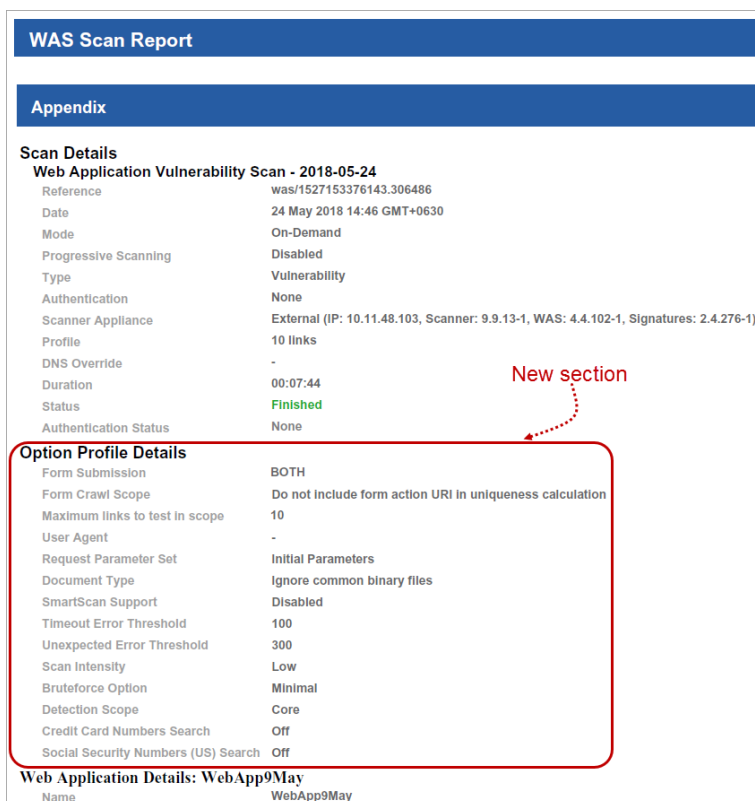
Go to Reports > New Report > Scan Report. Choose a report template and the scan for which you would want to view the report. Click Finish.



The Appendix section lists the new section.

The new section is displayed in all report formats.

For example, let us see PDF report format.

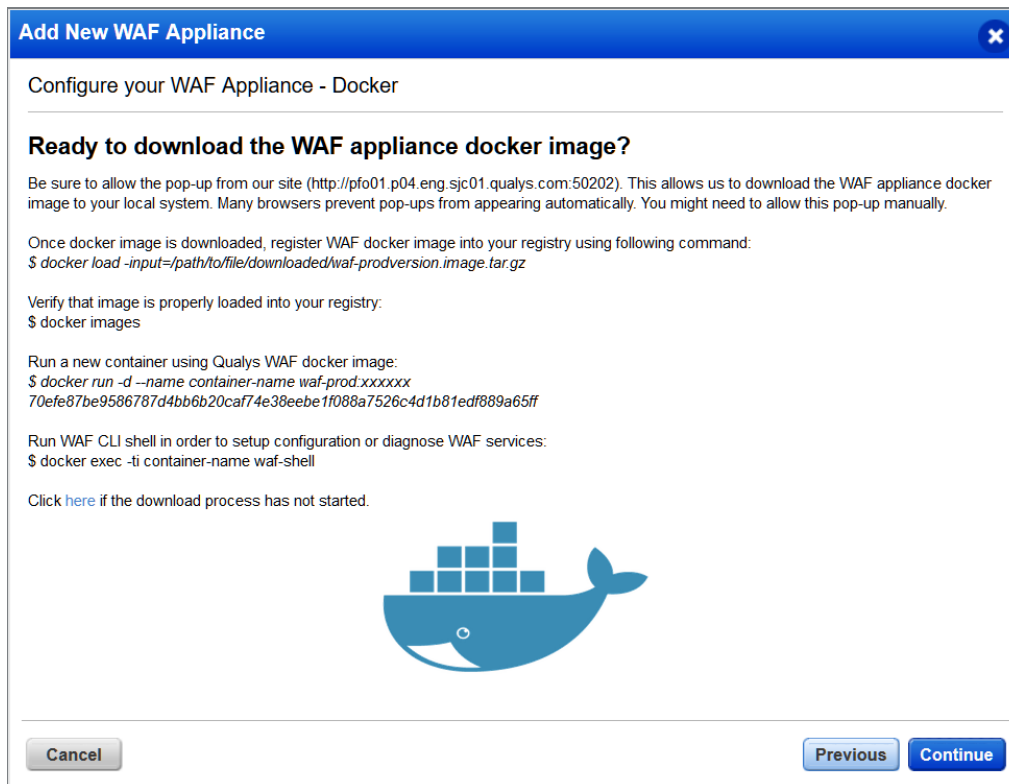




Install WAF appliance on Docker

You can now install the WAF appliance on a Docker container.

Go to WAF Appliances > WAF Appliances, and click New WAF Appliance. Select an existing WAF cluster or create a new one. In the Add New WAF Appliance wizard, select Docker and click Continue to download the Docker image file.



Refer to the onscreen instructions to create a container from the Docker image. Click Continue to get the registration code of the cluster to register the WAF appliance to. See the WAF Getting Started Guide for information on using the WAF CLI for registering the WAF appliance.

Ensure that the Docker container has proper network connectivity for WAF appliance to communicate and register with the Qualys Cloud Platform (WAF_SERVICE_URL) in order to start sending WAF events.

Web Server profile for containers

Now that WAF provides support for Docker (container), you can create a web server profile to load balance traffic between web applications installed on containers.

To create a web server profile for containers, go to Web Applications > Web Servers. Create a new Web Server profile or edit an existing one to provide the Docker image id and name.

The web server profile will create a pool of all containers spawned from the Docker image.

The screenshot shows the 'Web Servers Creation' interface, specifically 'Step 2 of 3'. The left sidebar indicates the current step is 'Configuration'. The main area is titled 'Web Servers configuration' and 'Application Servers'. It includes a description: 'Here you define the server-side properties. Select a port, protocol (http or https), and a list of servers along with a load-balancing method.' The configuration fields are: 'Port*' with value '80', 'Protocol HTTPS' with a radio button 'OFF', 'Docker platform' with a toggle 'ON', 'Docker properties' section containing 'Docker image*' with 'Example: /home/tomcat' and 'Docker name' with '(optional)', and 'Load-balancing' with a dropdown set to 'roundrobin'. A red rectangular box highlights the 'Docker platform' and 'Docker properties' section.

Docker image ID is required. Optionally, you can provide the Docker name.

Once created, you can associate this Web Server profile to a Web application.

Note that a single Web Server profile can be used to create a container pool or a server pool, but not a combination of both.

Securing your web applications with http headers

You can now secure your web application through HTTP headers. Security headers instructs the browser exactly how to behave when it handles your website's content and data. You can add appropriate HTTP headers to a response from your server, based on conditions met in a custom rule.

The Actions panel of the Rule Creation wizard allows you to specify HTTP headers you want to add, set (modify), or delete when events match conditions in a custom rule.

An example of a security header could be an XFO header to mitigate clickjacking attacks:

x-frame-options: SAMEORIGIN

Rule Creation

Step 3 of 4

- 1 Rule Details ✓
- 2 Conditions ✓
- 3 **Actions** ✓
- 4 Review And Confirm

Rule actions

Actions

Here you define actions to trigger when all conditions are met. It can be a blocking or a granting action ;

Action* **Allow**

Log*

Actions

Here you define actions to trigger when all conditions are met. It can be a blocking or a granting action ; but also can

Action* **Add header**

Header Name*

Header Value

Log* **No**

New detection categories in security policy

Four new sliders for detection categories are introduced in the security policy. You can set the minimum confidence rating for each of these categories.

This allows you to filter out events. Events that are filtered out will not be considered during correlation and a final decision. Clear (un-check) a category if you do not want to apply any minimum confidence rating to a category.

Security Policy Creation Turn help tips: On | Off Launch help X

Step 2 of 4

- 1 Policy Details ✓
- 2 **Application Security**
- 3 Policy Controls
- 4 Review And Confirm

Configure Sensitivity Rating for detection categories

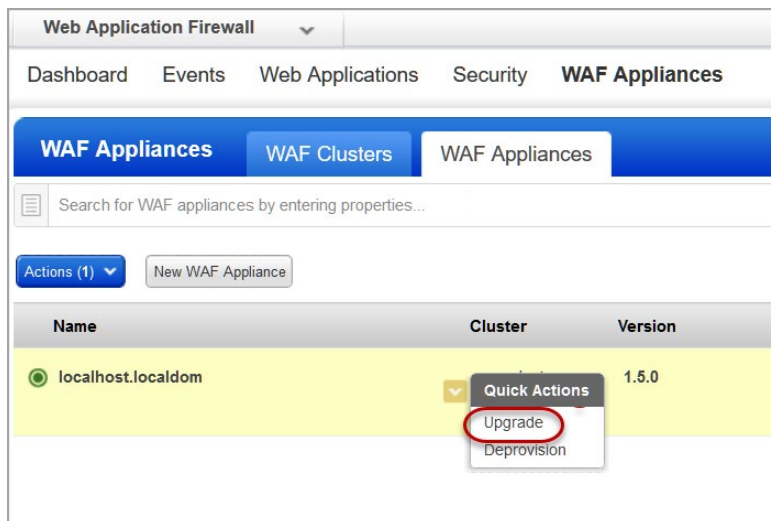
<input checked="" type="checkbox"/>	Source Code Disclosure	<div><div></div></div>	50
<input checked="" type="checkbox"/>	SQL Injection	<div><div></div></div>	50
<input checked="" type="checkbox"/>	SSI Injection	<div><div></div></div>	50
<input checked="" type="checkbox"/>	XPath Injection	<div><div></div></div>	50
<input checked="" type="checkbox"/>	Relative path overwrite	<div><div></div></div>	50
<input checked="" type="checkbox"/>	XML Injection	<div><div></div></div>	50
<input checked="" type="checkbox"/>	Expression Language Injection	<div><div></div></div>	50
<input checked="" type="checkbox"/>	Code Injection	<div><div></div></div>	50

Upgrade specific WAF appliances

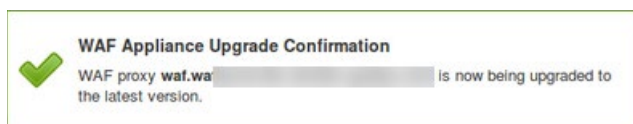
You can now upgrade specific WAF appliances manually. This is in addition to the existing functionality of updating all appliances associated with a cluster through auto-update.

It is recommended not to upgrade a WAF appliance if the associated cluster is in freeze period.

To upgrade a specific appliance, go to WAF Appliances > WAF Appliances, and then select **Upgrade** from the Quick Actions menu of the appliance.



The following confirmation message appears when upgrade is in progress.

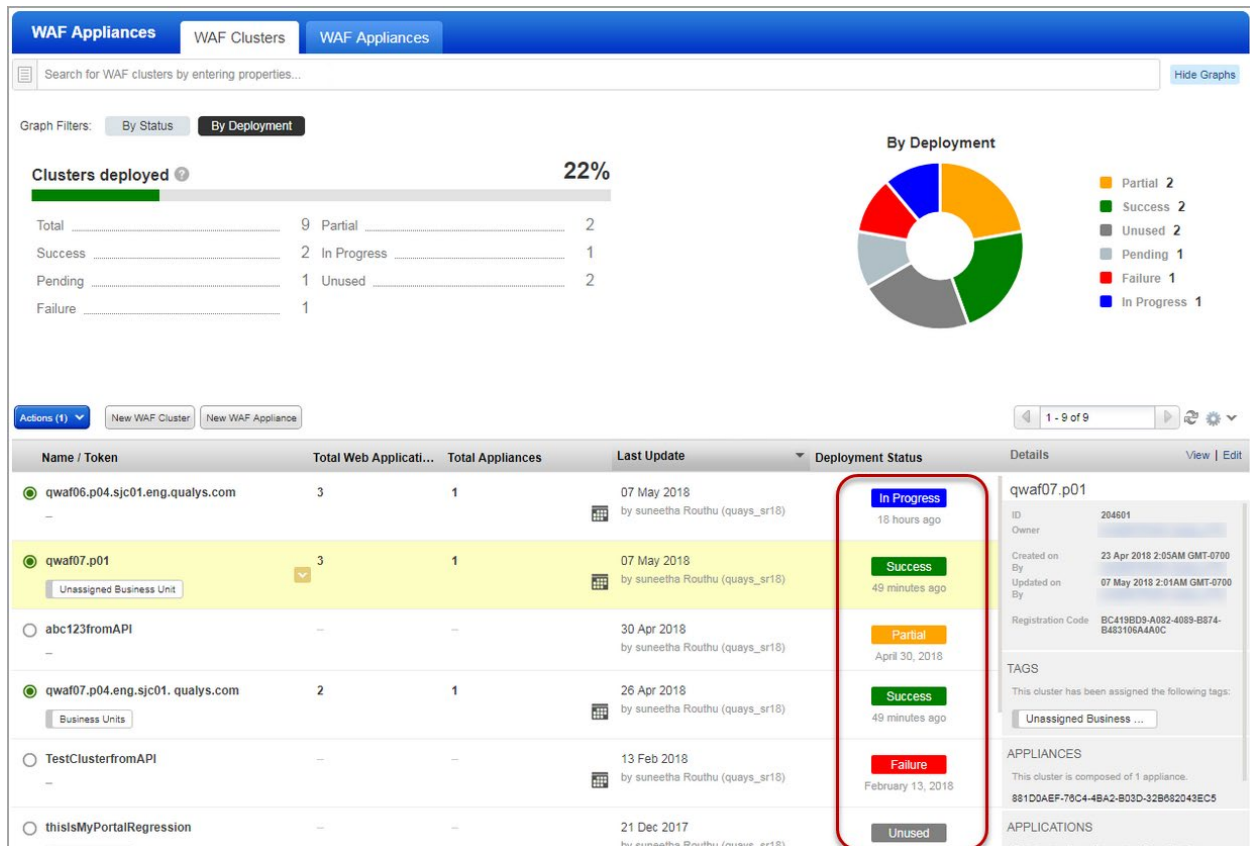


UI improvements

This release of WAF contains several improvements to the UI.

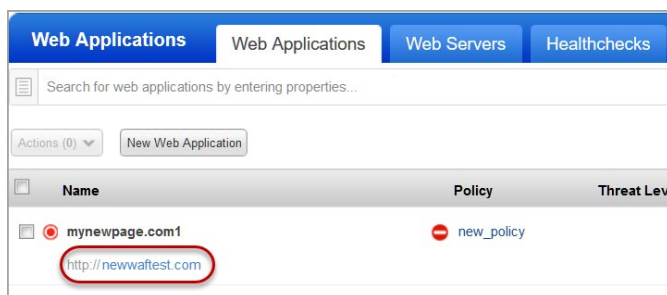
New column for deployment status

A new column called “Deployment Status” is added to Web Applications, WAF Clusters, and WAF Appliances tabs. This column now shows the deployment status in the form of text labels.



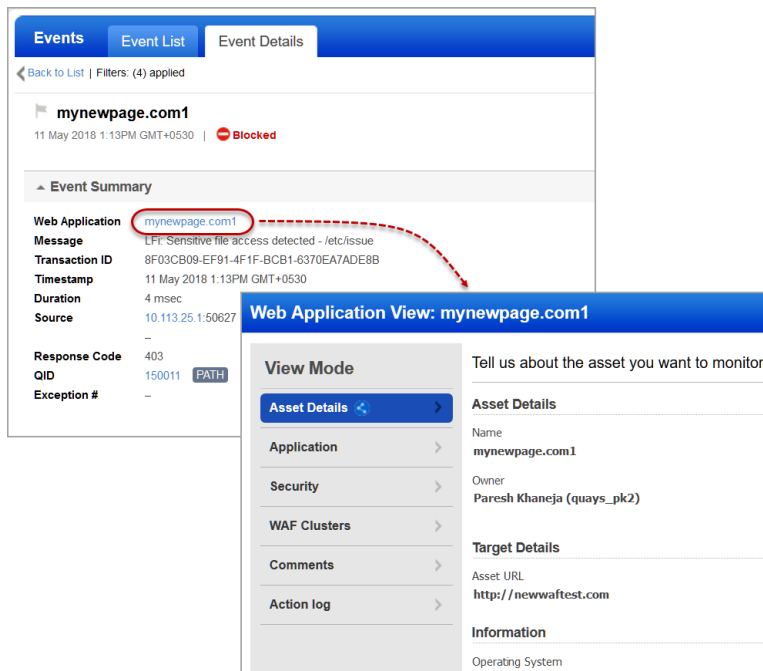
Clickable web application URL

The URL displayed under a Web application on the Web Applications tab is now clickable.



Clickable web application in Event Details

The Web application URL under Event Summary is now clickable. Clicking the web application URL launches the web application wizard where you can view/edit the web application details.



Events | Event List | Event Details

Back to List | Filters: (4) applied

mynewpage.com1
11 May 2018 1:13PM GMT+0530 | Blocked

Event Summary

Web Application mynewpage.com1

Message LFI: Sensitive file access detected - /etc/issue

Transaction ID 8F03CB09-EF91-4F1F-BCB1-6370EA7ADE8B

Timestamp 11 May 2018 1:13PM GMT+0530

Duration 4 msec

Source 10.113.25.1:50627

Response Code 403

QID 150011 **PATH**

Exception # -

Web Application View: mynewpage.com1

View Mode

Asset Details

Application

Security

WAF Clusters

Comments

Action log

Tell us about the asset you want to monitor

Asset Details

Name
mynewpage.com1

Owner
Paresh Khaneja (quays_pk2)

Target Details

Asset URL
http://newwaftest.com

Information

Operating System

Issues addressed in this release

Qualys Cloud Platform 2.33 brings you many more improvements and updates.



AssetView



ThreatPROTECT

- Now users can search for Docker attributes when Container Security (CS) is enabled in the user's subscription. We've added these new search tokens:
isDockerHost, docker.dockerVersion, docker.noOfContainers, docker.noOfImages
- We've made updates to using commas in widgets. Users can no longer create or edit a widget with commas in the widget title (an error message appears on save). When exporting an existing widget with commas in the title, all the commas are deleted.
- Fixed an issue with widget configuration when sort by set to activatedForModules
- We have removed connectedFrom and errorStatus as group by tokens, and these tokens are no longer an option in widgets (i.e. for Categories, Group by, Sort by). Now these tokens are used only for search.
- Now users can search by assetId using various methods such as exact match, range query, matching multiple values.
- "Groovy Scriptlet" will not show in drop down list (in AssetView tag creation workflow) if the groovy script option is disabled for the user's subscription.
- Now the queries activatedForModules:* and pendingActivationForModules:* will give correct results.
- We've expanded and improved user documentation on prefix and suffix matching in How to Search help file located at https://<platform>/portal-help/en/assetview/assets/asset_search_samples.htm
- Fixed an issue with Threat Protection (TP) activation once TP is expired in the user's account.
- Updated the help for interfaces.hostname to include suffix and prefix matching and better syntax examples.



Certificate View

- Accurate validations are now added for adding new certificate authority file that has multiple dot operators.



Security Assessment Questionnaire

- The User quota in Account Information summary now accurately displays the number of users provided at the time of licensing.
- The Rejected filter is now displayed even if the filter count is 0.

- Updated help with accurate information about adding company logo to email.
- The Load More button is now removed and an infinite scroll is added to the Rules tab.
- Online help is updated to with information that questions and sections can be delegated to users within the same company.
- All special characters will now be accepted by the Question and Answer fields.

WAS Web Application Scanning

- The detection list now gets correctly sorted when sorted by last detected date.
- The detection list when downloaded in CSV format displays correct time zone and data without any error.
- Usage of multiple filters now functions correctly (as expected) when applied to web application list or scan list.
- We have now fixed the issue so that the ScanTrust option is not displayed in authentication scan when WAF enabled asset is created under WAS.
- Depending on the permissions assigned to you, the "Ignore" option is now enabled/disabled in the Quick Actions menu of the Detections tabs.
- The default system-defined authentication test option profile is now displayed only if authentication scan option is enabled for your subscription.
- We have now fixed the issue to prevent the cross-site scripting from being executed when a user opens HTML report format.

WAF Web Application Firewall

- Fixed an issue where there was a mismatch between the color of appliance status icons and the color of "By Status" pie chart. Now the colors are consistent.
- Fixed an issue where in case of large number of clusters, the list of clusters in the set cluster window used to spill over outside the window frame.
- Fixed an issue where incomplete error message was displayed while adding web servers in the web server creation wizard.
- Fixed an issue where partial deployment status was displayed under Appliances tab. Partial deployment status is not applicable for appliances, hence it is now removed.

Qualys Cloud Platform

- Now the user can set a dashboard as the default using the Container Security app.