Qualys.

Qualys Cloud Platform v2.x

Version 2.32
March 23, 2018

Here’s what’s new in Qualys Cloud Platform 2.32!

AV AssetView

TP ThreatPROTECT

AWS EU Region (Paris) support

FIM File Integrity Monitoring

IOC Indication of Compromise

Import / Export Dashboards

FIM Improvements for Managing Events and Incidents

SAQ Security Assessment Questionnaire

New User Interface for Responders

WAS Web Application Scanning

Option Profile Enhanced to Define Detection Scope

New Feature to Test Authentication Records

Exclude Parameters from Scan

Update to 2017 OWASP Top 10

Support for Latest Burp Version

New CSV_V2 format for WAS Reports

WAF Web Application Firewall

Support for Microsoft Azure and Google Cloud

Schedule auto-update for appliances registered to a cluster

Add trusted proxies for a Cluster

Validate XML/JSON payload

Qualys Cloud Platform 2.32 brings you many more Improvements and updates! Learn more

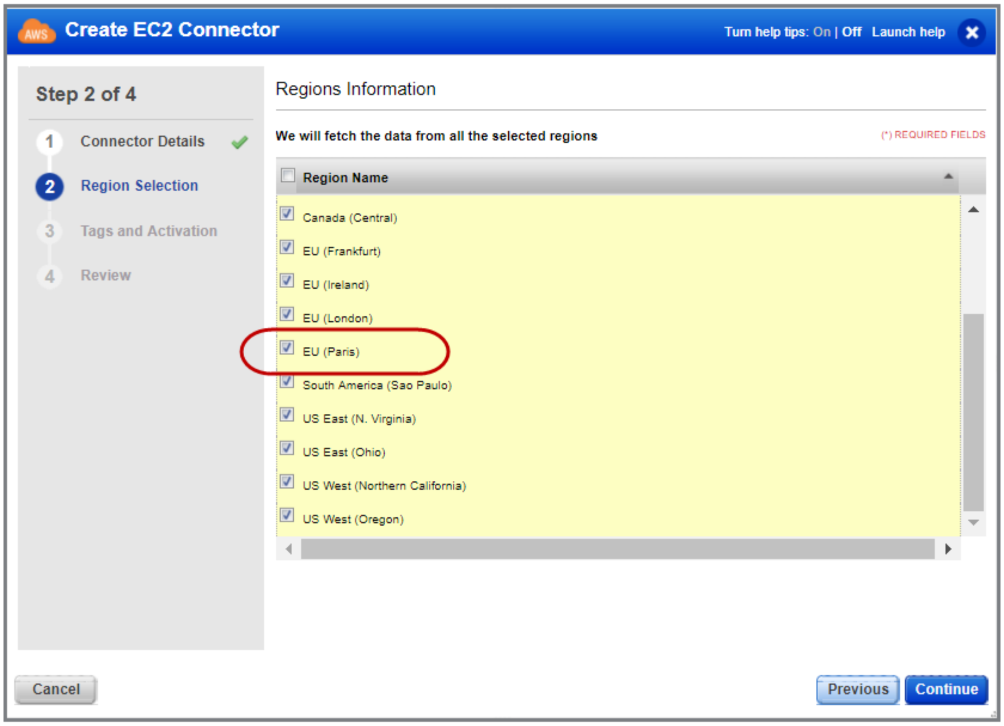
AV AssetView

TP ThreatPROTECT

AWS EU Region (Paris) support

Region name “EU (Paris)” with Region Code “eu-west-3” is now supported by the EC2 Connector.

Now you can easily scan EC2 instances included in the AWS EU (Paris) region for vulnerabilities and policy compliance using the Qualys Cloud Platform. You can create/update EC2 connectors to pull instance info from the Paris region, activate discovered instances for the VM, PC or SCA module, and scan them using our EC2 scan workflow. When setting up your EC2 connector using AssetView choose EU (Paris) in the wizard.



Regions Information

We will fetch the data from all the selected regions

(*) REQUIRED FIELDS

☐ Region Name

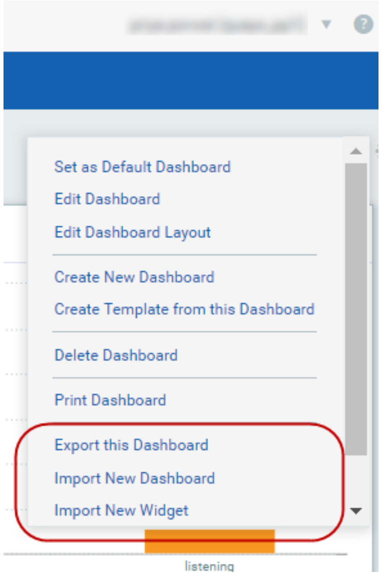
☑ Canada (Central)
☑ EU (Frankfurt)
☑ EU (Ireland)
☑ EU (London)
☑ EU (Paris)
☑ South America (Sao Paulo)
☑ US East (N. Virginia)
☑ US East (Ohio)
☑ US West (Northern California)
☑ US West (Oregon)

FIM File Integrity Monitoring

IOC Indication of Compromise

Import / Export Dashboards

You can now import and export Dashboards with their corresponding widgets, and import widgets that you can then add to your Dashboards. Now it's easy to share Dashboards and widgets. You'll see the new options on the Dashboard tools menu.



FIM Improvements for Managing Events and Incidents

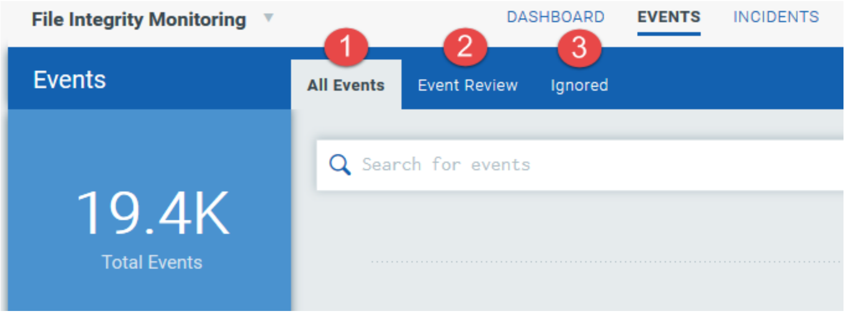
We've made several improvements in FIM including new workflows for ignoring events and grouping related changes into incidents.

Use the new sub-tabs in the Events section to quickly identify:

(1) All events detected across all of your assets, except ignored events.

(2) Events waiting to be reviewed. You can choose to ignore events or create incidents.

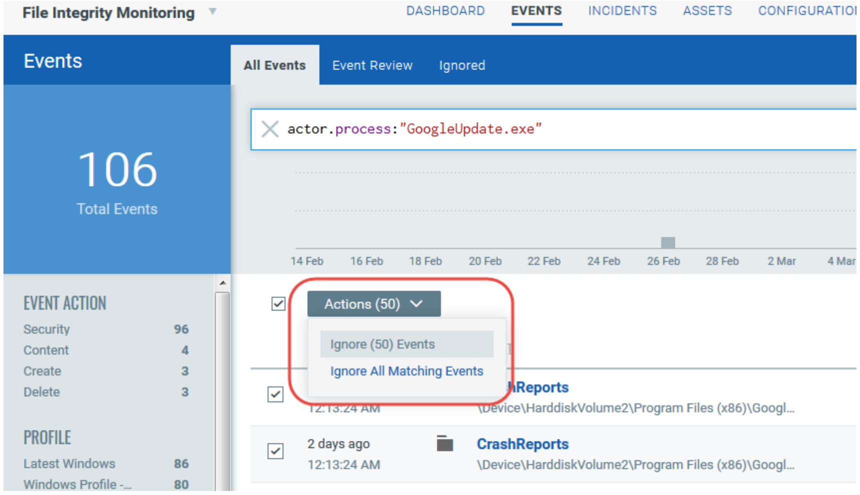
(3) Ignored events.



Ignore Events

Have an event you don't need to track? Ignore it to move it out of your list.

Select specific events and choose Ignore Events from the Actions menu. Choose Ignore All Matching Events to ignore all events that are currently matching your query for the timeframe that you've selected. Ignored events are moved to the Ignored list. Note - You may get similar events in the future that will appear in your Events list and you'll want to ignore those too.



actor.process:"GoogleUpdate.exe"

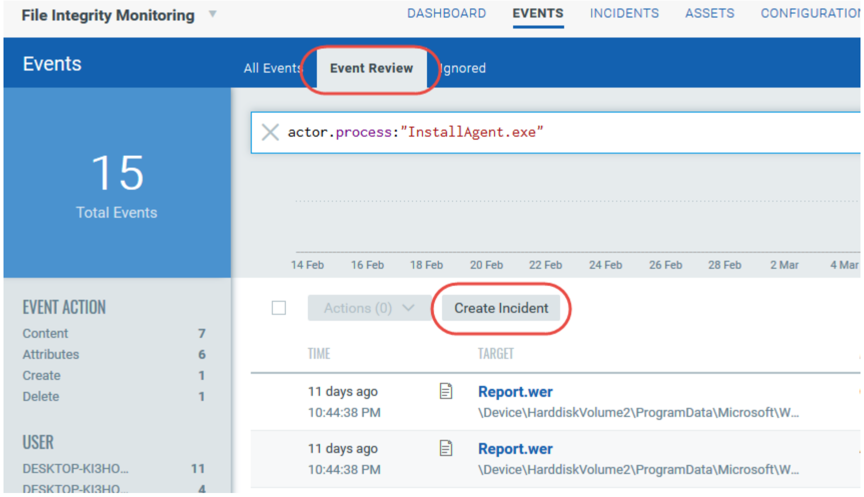
☑	12:13:24 AM	hReports \Device\HarddiskVolume2\Program Files (x86)\Googl...
☑	2 days ago 12:13:24 AM	CrashReports \Device\HarddiskVolume2\Program Files (x86)\Googl...

Did you ignore an event by mistake? No worries. You can easily restore any ignored event from the Ignored list.

Create Incidents

Group related changes into incidents. Then review your incidents to determine if they're valid.

On the Event Review tab, run a query to find related events, click Create Incident and give your incident a name. Your new incident will be saved on the Incidents list where you can view and add details. All events matching your query will be included.

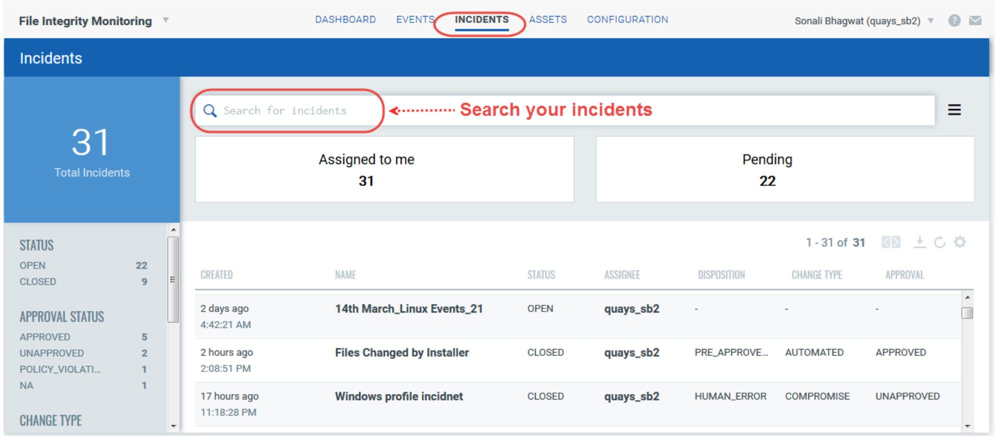


actor.process:"InstallAgent.exe"

TIME	TARGET
11 days ago 10:44:38 PM	Report.wer \Device\HarddiskVolume2\ProgramData\Microsoft\W...
11 days ago 10:44:38 PM	Report.wer \Device\HarddiskVolume2\ProgramData\Microsoft\W...

Your Incidents List

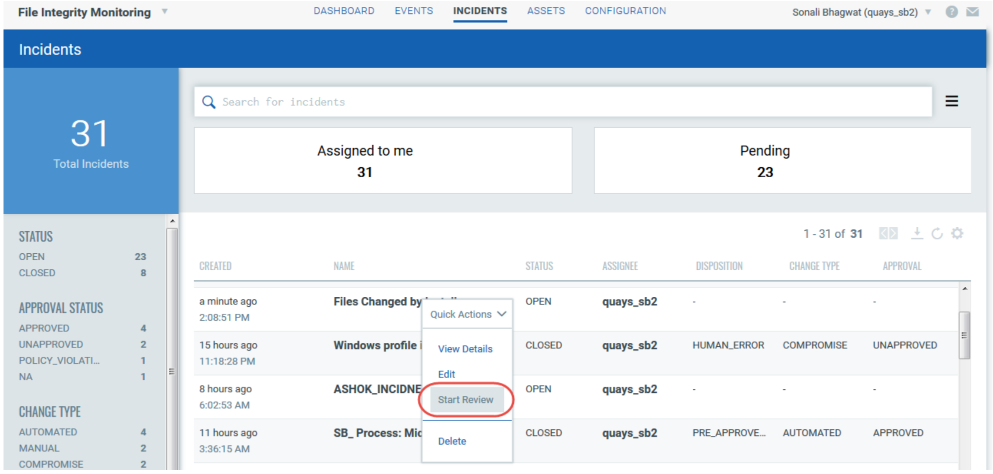
This is where you'll search and take actions on your incidents. View details for any incident to get a break-down of the events by severity, action and user. Edit any incident to rename it or change the events associated with it by modifying the query or timeframe.



CREATED	NAME	STATUS	ASSIGNEE	DISPOSITION	CHANGE TYPE	APPROVAL
2 days ago 4:42:21 AM	14th March_Linux Events_21	OPEN	quays_sb2	-	-	-
2 hours ago 2:08:51 PM	Files Changed by Installer	CLOSED	quays_sb2	PRE_APPROVE...	AUTOMATED	APPROVED
17 hours ago 11:18:28 PM	Windows profile incidnet	CLOSED	quays_sb2	HUMAN_ERROR	COMPROMISE	UNAPPROVED

Start Incident Review

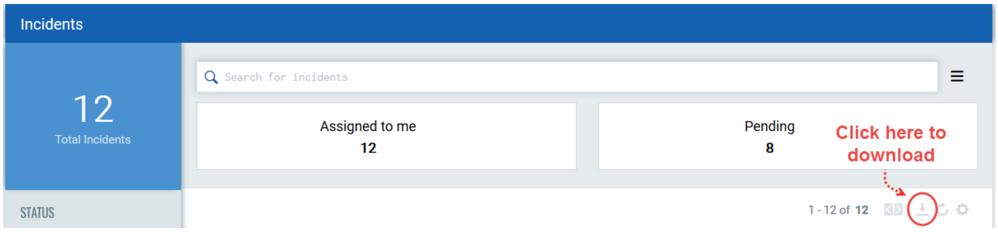
We'll guide you through this process. You'll review the events associated with the incident and then mark the incident Approved or Unapproved. You'll also classify the events by disposition category (e.g. Pre-Approved by Change Control, Patching, Data Corruption, Human Error, etc.) and indicate the type of change (e.g. Manual, Automated, etc.)



CREATED	NAME	STATUS	ASSIGNEE	DISPOSITION	CHANGE TYPE	APPROVAL
a minute ago 2:08:51 PM	Files Changed by	OPEN	quays_sb2	-	-	-
15 hours ago 11:18:28 PM	Windows profile i	CLOSED	quays_sb2	HUMAN_ERROR	COMPROMISE	UNAPPROVED
8 hours ago 6:02:53 AM	ASHOK_INCIDNE	OPEN	quays_sb2	-	-	-
11 hours ago 3:36:15 AM	SB_ Process: Mic	CLOSED	quays_sb2	PRE_APPROVE...	AUTOMATED	APPROVED

Download Your Incidents

It's easy. Just click the Download icon above the list and choose a download format.

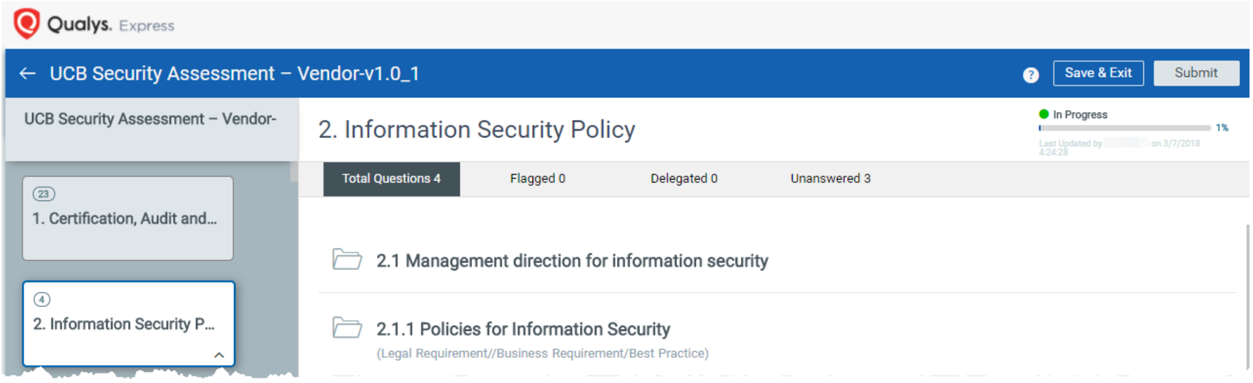


SAQ Security Assessment Questionnaire

New User Interface for Responders

We now have a new interface to make it easier for you to respond to questionnaires.

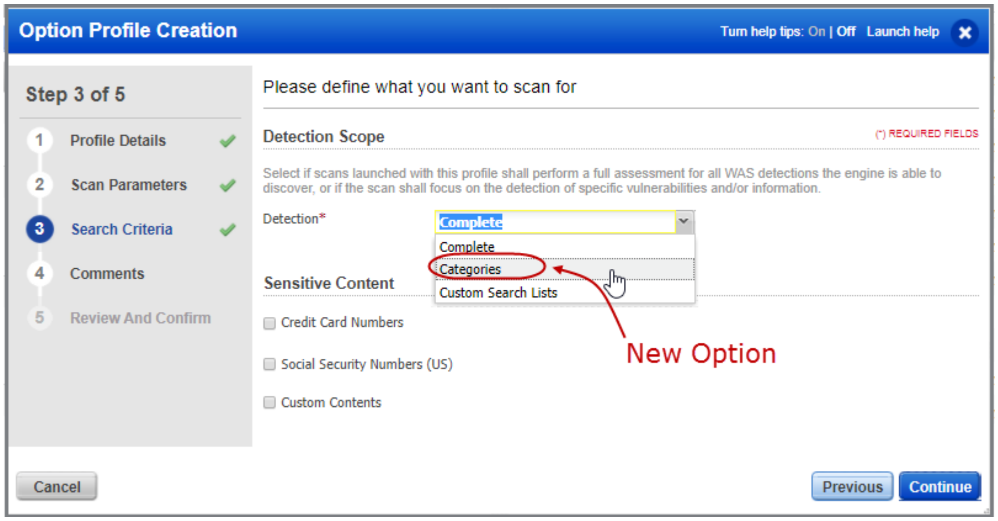
It's easy to get started. Just login with the credentials provided to you and choose a questionnaire from your list. Click View Questions from the Quick Actions menu, answer all questions and submit your completed questionnaire.


Qualys. Express
← UCB Security Assessment – Vendor-v1.0_1
?
Save & Exit
Submit
UCB Security Assessment – Vendor-
23
1. Certification, Audit and...
4
2. Information Security P...
2. Information Security Policy
In Progress
1%
Last Updated by on 3/7/2018 4:24:28
Total Questions 4
Flagged 0
Delegated 0
Unanswered 3
2.1 Management direction for information security
2.1.1 Policies for Information Security
(Legal Requirement//Business Requirement/Best Practice)

WAS Web Application Scanning

Option Profile Enhanced to Define Detection Scope

We now provide different categories of vulnerabilities that can now be selected for detection scope within an option profile. This allows for targeted scans and offers an alternative to using static and dynamic search lists.



Option Profile Creation

Turn help tips: On | Off Launch help

Step 3 of 5

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

Please define what you want to scan for

Detection Scope (*) REQUIRED FIELDS

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

Detection*: Complete
- Complete
- Categories
- Custom Search Lists

New Option

Sensitive Content

☐ Credit Card Numbers

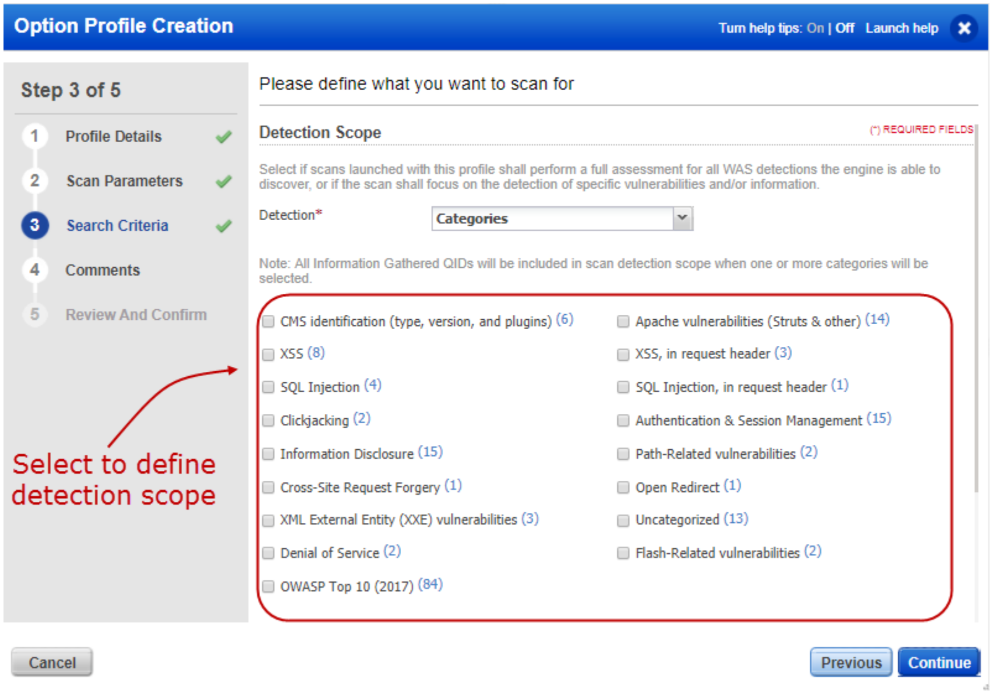
☐ Social Security Numbers (US)

☐ Custom Contents

Go to Configuration > Option Profile. Let us create a new option profile. In addition to Complete and Custom Search Lists, we now provide a new option "Categories".

Once you select Categories, we list various detection categories and you can select the categories to define the detection scope for a scan.

To view the detections/QIDs included in a particular category, click the View link next to the category listed.



Option Profile Creation

Turn help tips: On | Off Launch help

Step 3 of 5

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

Select to define detection scope

Please define what you want to scan for

Detection Scope (*) REQUIRED FIELDS

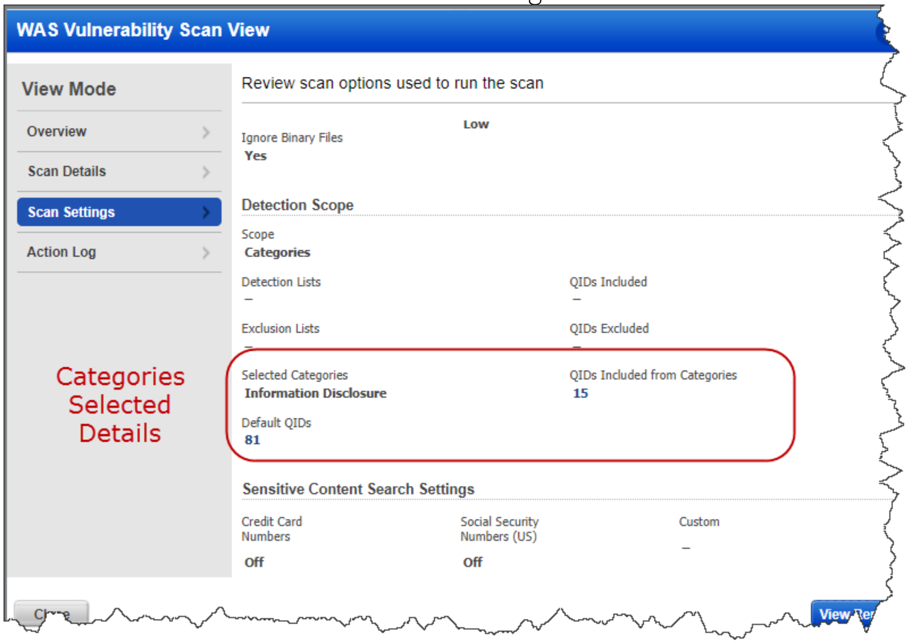
Select if scans launched with this profile shall perform a full assessment for all WAS detections the engine is able to discover, or if the scan shall focus on the detection of specific vulnerabilities and/or information.

Detection*: Categories

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

☐ CMS identification (type, version, and plugins) (6)
☐ XSS (8)
☐ SQL Injection (4)
☐ Clickjacking (2)
☐ Information Disclosure (15)
☐ Cross-Site Request Forgery (1)
☐ XML External Entity (XXE) vulnerabilities (3)
☐ Denial of Service (2)
☐ OWASP Top 10 (2017) (84)
☐ Apache vulnerabilities (Struts & other) (14)
☐ XSS, in request header (3)
☐ SQL Injection, in request header (1)
☐ Authentication & Session Management (15)
☐ Path-Related vulnerabilities (2)
☐ Open Redirect (1)
☐ Uncategorized (13)
☐ Flash-Related vulnerabilities (2)

You could view the details in Scan Settings of Scan View.



Review scan options used to run the scan

Low

Ignore Binary Files
Yes

Detection Scope

Scope
Categories

Detection Lists
–

QIDs Included
–

Exclusion Lists
–

QIDs Excluded
–

Selected Categories
Information Disclosure

QIDs Included from Categories
15

Default QIDs
81

Sensitive Content Search Settings

Credit Card Numbers
Off

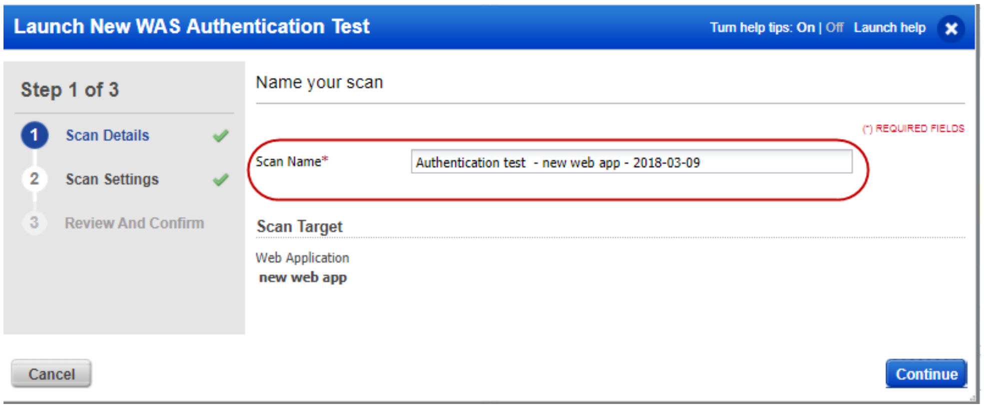
Social Security Numbers (US)
Off

Custom
–

Categories Selected Details

New Feature to Test Authentication Records

We have now introduced a new option in the quick actions menu that allows you to quickly test the scanner's ability to authenticate to a web application. You can now immediately test authentication records for web applications you define without having to run a Discovery scan.



Name your scan

(*) REQUIRED FIELDS

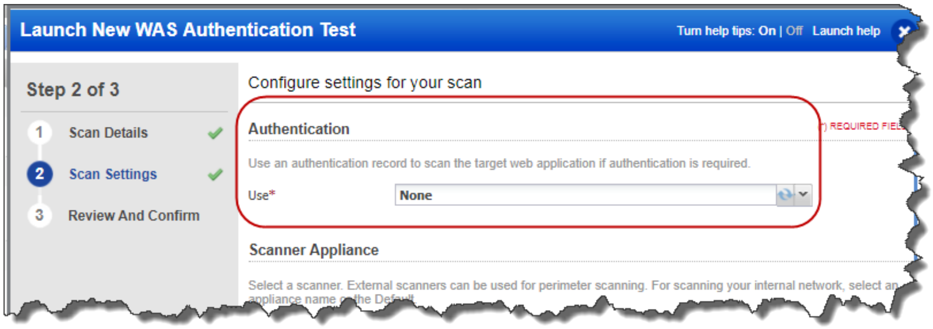
Scan Name* Authentication test - new web app - 2018-03-09

Scan Target

Web Application
new web app

Go to Web Applications > Web Applications and select the web application and select Test Authentication from the quick actions menu.

By default, we use the following format for the name of the authentication test.
Authentication test - <name of the web application> - <date in yyyy-mm-dd format>



Configure settings for your scan

(*) REQUIRED FIEL

Authentication

Use an authentication record to scan the target web application if authentication is required.

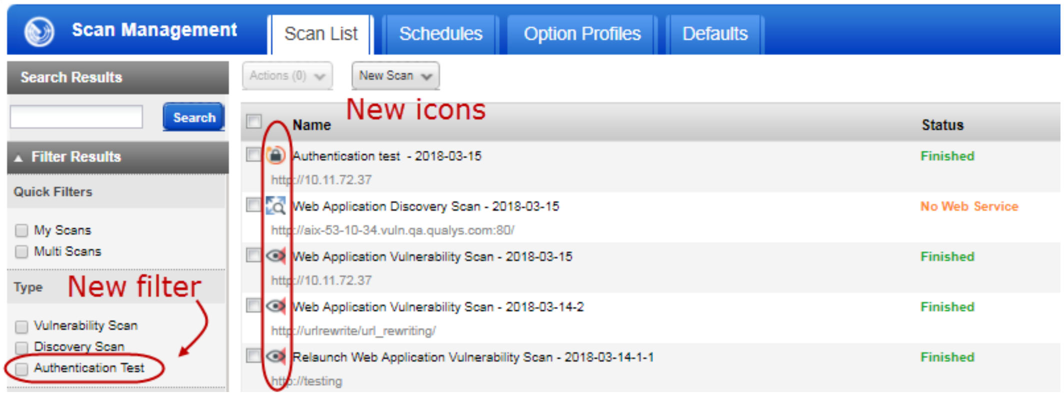
Use* None

Scanner Appliance

Select a scanner. External scanners can be used for perimeter scanning. For scanning your internal network, select an appliance name or the Default

You can then choose the authentication record to be tested in Authentication section and configure other settings similar to scan settings.

Authentication test can be only configured for a single scan. You cannot configure authentication test for a multi-scan or a scheduled scan. The authentication test scans that you execute are listed in scans.



Quick Filters

□ My Scans
□ Multi Scans

Type — New filter

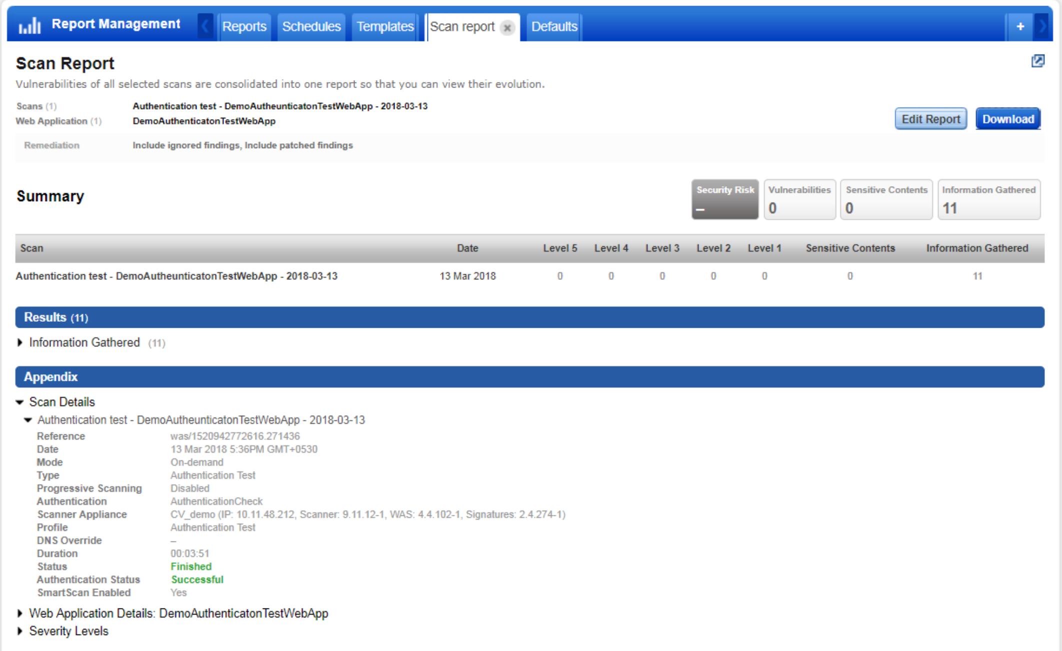
□ Vulnerability Scan
□ Discovery Scan
□ Authentication Test

New icons

Name	Status
Authentication test - 2018-03-15 http://10.11.72.37	Finished
Web Application Discovery Scan - 2018-03-15 http://aix-53-10-34.vuln.qa.qualys.com:80/	No Web Service
Web Application Vulnerability Scan - 2018-03-15 http://10.11.72.37	Finished
Web Application Vulnerability Scan - 2018-03-14-2 http://urlrewrite/url_rewriting/	Finished
Relaunch Web Application Vulnerability Scan - 2018-03-14-1-1 http://testing	Finished

You can use the new filter ‘Authentication Test’ in Type that we added to view only authentication test scans. You could also identify them with the icon associated with the authentication test. You will notice that we also introduced new icons for scans.

You could view the report as well. Let us see an example of authentication test report.



Scan Report

Vulnerabilities of all selected scans are consolidated into one report so that you can view their evolution.

Scans (1) Authentication test - DemoAutheunticatonTestWebApp - 2018-03-13
Web Application (1) DemoAuthenticatonTestWebApp
Remediation Include ignored findings, Include patched findings

Summary

Security Risk	Vulnerabilities	Sensitive Contents	Information Gathered
–	0	0	11

Scan	Date	Level 5	Level 4	Level 3	Level 2	Level 1	Sensitive Contents	Information Gathered
Authentication test - DemoAutheunticatonTestWebApp - 2018-03-13	13 Mar 2018	0	0	0	0	0	0	11

Results (11)

- Information Gathered (11)

Appendix

- Scan Details
  - Authentication test - DemoAutheunticatonTestWebApp - 2018-03-13

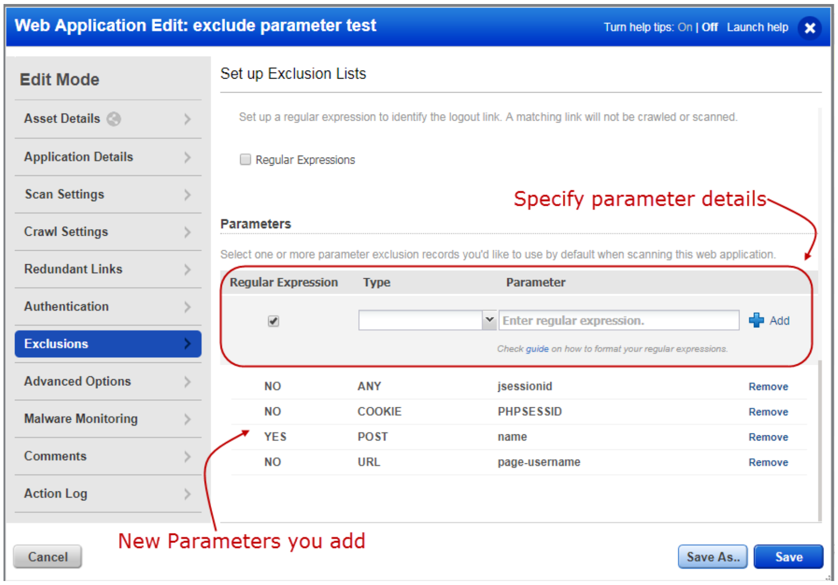
Reference	was/1520942772616.271436
Date	13 Mar 2018 5:36PM GMT+0530
Mode	On-demand
Type	Authentication Test
Progressive Scanning	Disabled
Authentication	AuthenticationCheck
Scanner Appliance	CV_demo (IP: 10.11.48.212, Scanner: 9.11.12-1, WAS: 4.4.102-1, Signatures: 2.4.274-1)
Profile	Authentication Test
DNS Override	–
Duration	00:03:51
Status	Finished
Authentication Status	Successful
SmartScan Enabled	Yes

- Web Application Details: DemoAuthenticatonTestWebApp
- Severity Levels

Test authentication feature is available only if it is enabled for your subscription. If you want to enable the feature, please contact Qualys Support.

Exclude Parameters from Scan

You can now exclude specific parameters from testing to improve a scan's efficiency and effectiveness. Exclusions can be defined for URL parameters, request body parameters, or cookies.



Set up Exclusion Lists

Set up a regular expression to identify the logout link. A matching link will not be crawled or scanned.

□ Regular Expressions

Specify parameter details

Parameters

Select one or more parameter exclusion records you'd like to use by default when scanning this web application.

Regular Expression	Type	Parameter	
☑		Enter regular expression.	Add
NO	ANY	jsessionid	Remove
NO	COOKIE	PHPSESSID	Remove
YES	POST	name	Remove
NO	URL	page-username	Remove

Check guide on how to format your regular expressions.

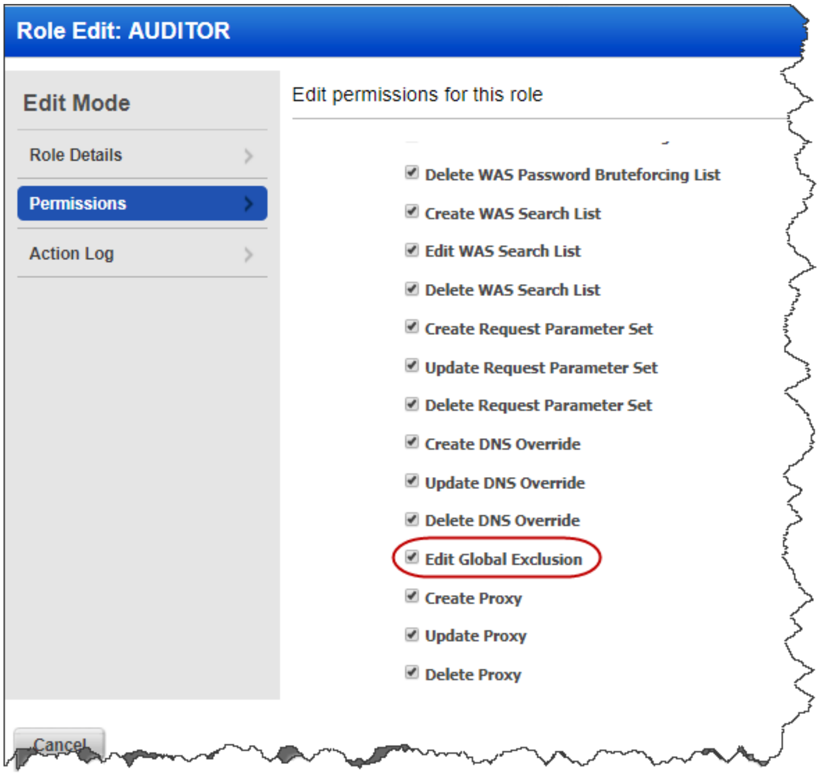
New Parameters you add

Go to Configuration > Global Settings and click Edit to add the parameters to be excluded from scan.

To add a parameter,
---select the check box to indicate if it is regular expression
---select the type of parameter: ANY, COOKIE, POST, URL
---type the parameter name
---click Add

The parameter is successfully added and listed below.

If you are Manager and want to configure permissions for exclude parameter settings, you need to go to Administration Utility and select the Edit Global Exclusion setting.



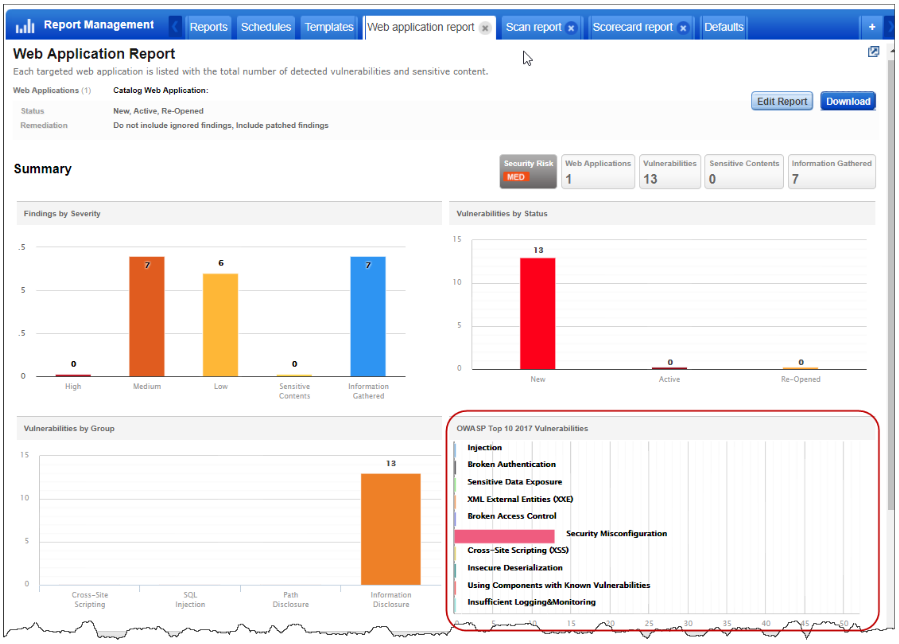
Edit permissions for this role

☑ Delete WAS Password Bruteforcing List
☑ Create WAS Search List
☑ Edit WAS Search List
☑ Delete WAS Search List
☑ Create Request Parameter Set
☑ Update Request Parameter Set
☑ Delete Request Parameter Set
☑ Create DNS Override
☑ Update DNS Override
☑ Delete DNS Override
☑ Edit Global Exclusion
☑ Create Proxy
☑ Update Proxy
☑ Delete Proxy

Update to 2017 OWASP Top 10

The OWASP Top 10 is one of the most common ways to categorize web application risks and vulnerabilities. The vulnerability detection in Qualys Web Application Scanning (WAS) are now mapped to the 2017 edition of the OWASP Top 10 replacing the 2013 edition.

We have updated web application report, scan report as well as scorecard report.



Web Application Report

Each targeted web application is listed with the total number of detected vulnerabilities and sensitive content.

Web Applications (1) Catalog Web Application:

Status New, Active, Re-Opened

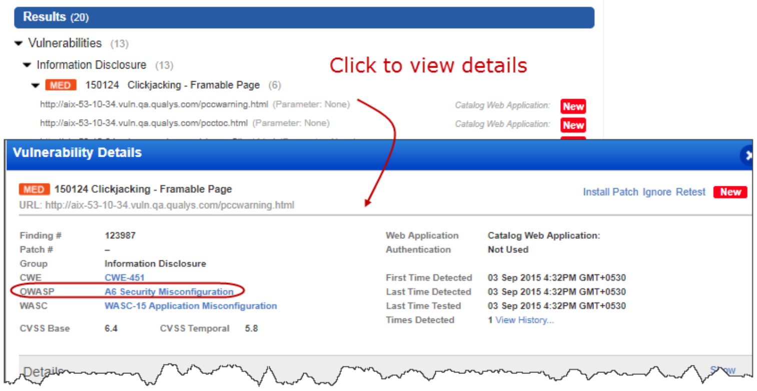
Remediation Do not include ignored findings, Include patched findings

Let us generate a web application report and view the changes.

The report provides a graph listing the OWASP top 10 vulnerabilities.

The Vulnerability Details in the report also provides a clickable link with OWASP details. You can click the link and view the further details about the vulnerability.

You could also view the vulnerability details in the Detection List.



Results (20)

Vulnerabilities (13)

Information Disclosure (13)

MED 150124 Clickjacking - Framable Page (6)

http://aix-53-10-34.vuln.qa.qualys.com/pccwarning.html (Parameter: None) Catalog Web Application: New

http://aix-53-10-34.vuln.qa.qualys.com/pcctoc.html (Parameter: None) Catalog Web Application: New

Click to view details

Vulnerability Details

MED 150124 Clickjacking - Framable Page

URL: http://aix-53-10-34.vuln.qa.qualys.com/pccwarning.html

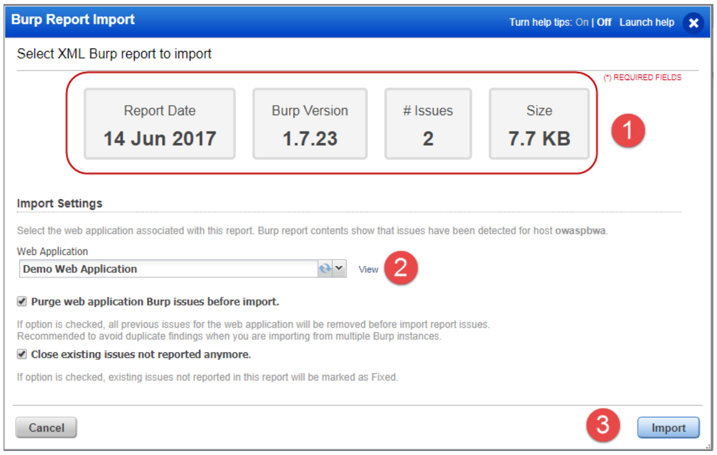
Install Patch Ignore Retest New

Finding #	123987	Web Application	Catalog Web Application:
Patch #	–	Authentication	Not Used
Group	Information Disclosure		
CWE	CWE-451	First Time Detected	03 Sep 2015 4:32PM GMT+0530
OWASP	A6 Security Misconfiguration	Last Time Detected	03 Sep 2015 4:32PM GMT+0530
WASC	WASC-15 Application Misconfiguration	Last Time Tested	03 Sep 2015 4:32PM GMT+0530
		Times Detected	1 View History...
CVSS Base	6.4 CVSS Temporal 5.8		

Details

Support for Latest Burp Version

We now support import of the latest version of Burp 1.7.24. You can now successfully import Burp files that belong to version 1.7.24.



Select XML Burp report to import

(*) REQUIRED FIELDS

Report Date	Burp Version	# Issues	Size
14 Jun 2017	1.7.23	2	7.7 KB

Import Settings

Select the web application associated with this report. Burp report contents show that issues have been detected for host **owaspbwa**.

Web Application: Demo Web Application

☑ **Purge web application Burp issues before import.**

If option is checked, all previous issues for the web application will be removed before import report issues.
Recommended to avoid duplicate findings when you are importing from multiple Burp instances.

☑ **Close existing issues not reported anymore.**

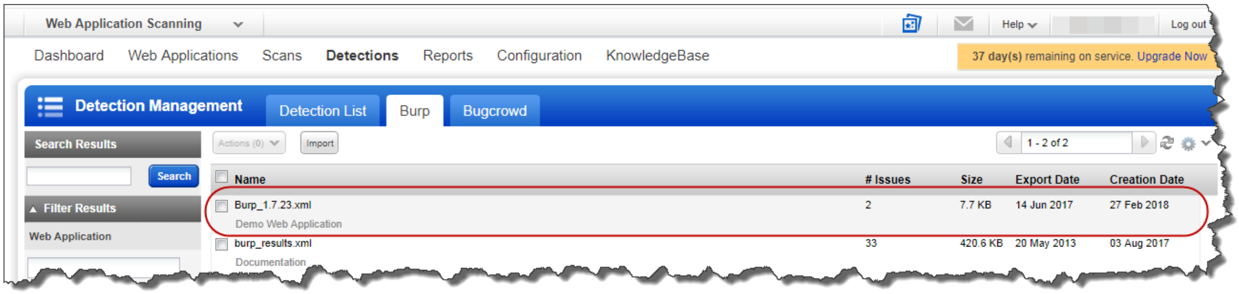
If option is checked, existing issues not reported in this report will be marked as Fixed.

Go to Detections > Burp and click Import.
1-You can then select the Burp file that contains the issues.

2- Select the web application. Let us know your other preferences.

3- Click Import.

Burp Report After Import



37 day(s) remaining on service. Upgrade Now

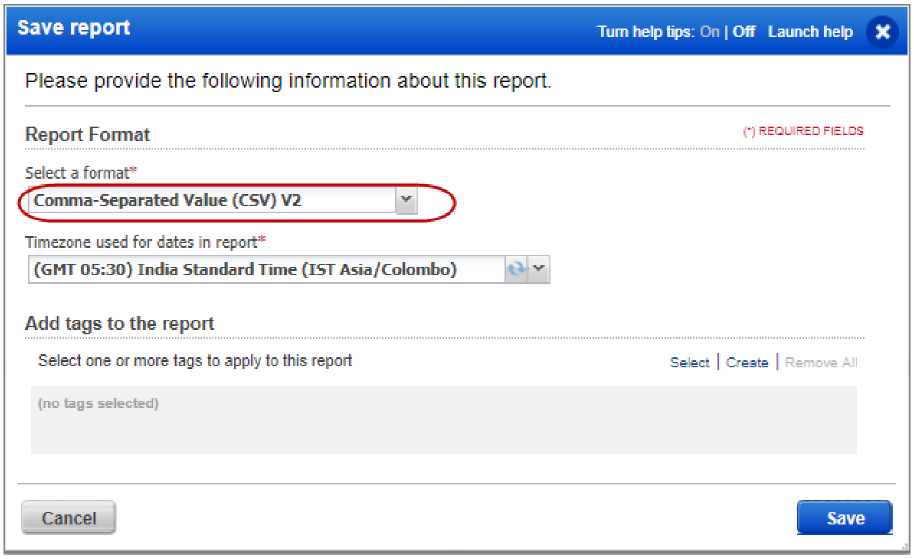
Name	# Issues	Size	Export Date	Creation Date
Burp_1.7.23.xml Demo Web Application	2	7.7 KB	14 Jun 2017	27 Feb 2018
burp_results.xml Documentation	33	420.6 KB	20 May 2013	03 Aug 2017

New CSV_V2 format for WAS Reports

We have now introduced a new CSV V2 report format for Web application report and Scan report. The CSV_V2 report format provides you information about 12 new fields in addition to all the fields that exist in CSV format.

How do I generate the report?

Let us generate a scan report in the new CSV-v2 format.



Save report

Please provide the following information about this report.

Report Format

(*) REQUIRED FIELDS

Select a format*: Comma-Separated Value (CSV) V2

Timezone used for dates in report*: (GMT 05:30) India Standard Time (IST Asia/Colombo)

Add tags to the report

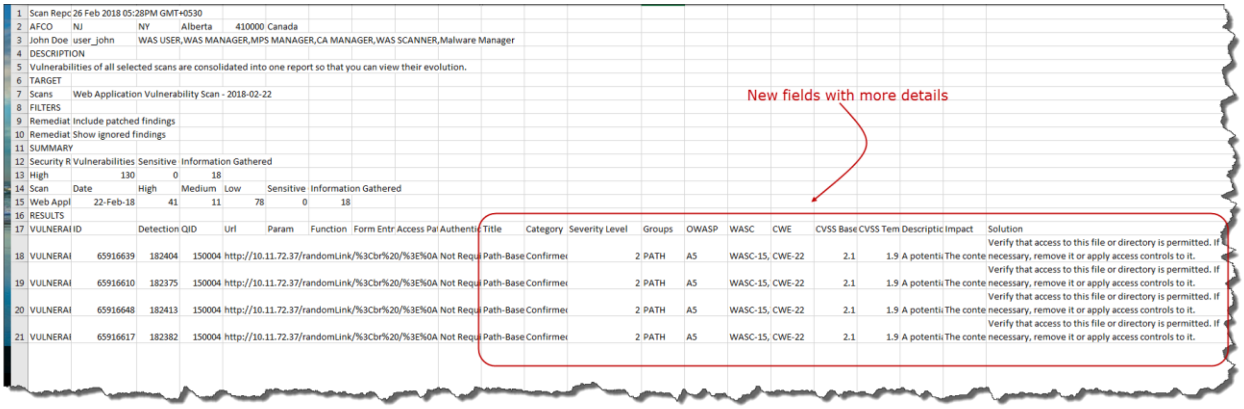
Select one or more tags to apply to this report

(no tags selected)

Go to Scans > Scan List, select one or more scans of a single web application and then select View Report from the Quick Actions menu.

Once the scan report is displayed, click Download and select Comma Separated Value (CSV) v2 as the report format.

The new report format provides details on the following fields:



1	Scan Repc	26 Feb 2018 05:28PM GMT+0530																			
2	AFCO	NJ	NY	Alberta	410000	Canada															
3	John Doe	user_john	WAS USER,WAS MANAGER,MPS MANAGER,CA MANAGER,WAS SCANNER,Malware Manager																		
4	DESCRIPTION																				
5	Vulnerabilities of all selected scans are consolidated into one report so that you can view their evolution.																				
6	TARGET																				
7	Scans	Web Application Vulnerability Scan - 2018-02-22																			
8	FILTERS																				
9	Remediat	Include patched findings																			
10	Remediat	Show ignored findings																			
11	SUMMARY																				
12	Security R	Vulnerabilities	Sensitive	Information Gathered																	
13	High	130	0	18																	
14	Scan	Date	High	Medium	Low	Sensitive	Information Gathered														
15	Web Appl	22-Feb-18	41	11	78	0	18														
16	RESULTS																				
17	VULNERAI	ID	Detection	QID	Url	Param	Function	Form Entr	Access Pat	Authentic	Title	Category	Severity Level	Groups	OWASP	WASC	CWE	CVSS Base	CVSS Tem	Descriptic	Impact	Solution
18	VULNERAI	65916639	182404	150004	http://10.11.72.37/randomLink/%3Cbr%20/%3E%0A					Not Requi	Path-Base	Confirmec	2	PATH	A5	WASC-15,	CWE-22	2.1	1.9	A potentia	The conte	Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.
19	VULNERAI	65916610	182375	150004	http://10.11.72.37/randomLink/%3Cbr%20/%3E%0A					Not Requi	Path-Base	Confirmec	2	PATH	A5	WASC-15,	CWE-22	2.1	1.9	A potentia	The conte	Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.
20	VULNERAI	65916648	182413	150004	http://10.11.72.37/randomLink/%3Cbr%20/%3E%0A					Not Requi	Path-Base	Confirmec	2	PATH	A5	WASC-15,	CWE-22	2.1	1.9	A potentia	The conte	Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.
21	VULNERAI	65916617	182382	150004	http://10.11.72.37/randomLink/%3Cbr%20/%3E%0A					Not Requi	Path-Base	Confirmec	2	PATH	A5	WASC-15,	CWE-22	2.1	1.9	A potentia	The conte	Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

-Title	-Category
-Severity Level	-Groups
-OWASP	-WASC
-CWE	-CVSS Base
-CVSS Temporal	-Description
-Impact	-Solution

WAF Web Application Firewall

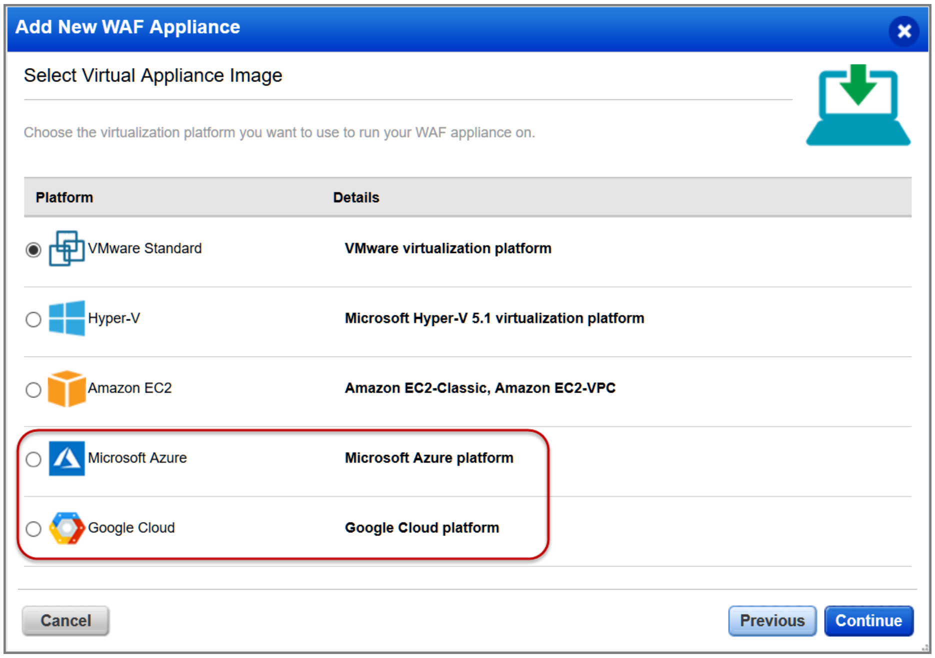
Support for Microsoft Azure and Google Cloud

WAF now extends support to two more cloud providers: Microsoft Azure and Google Cloud.

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 Microsoft Azure or Google Cloud and click Continue to get a link which will take you to the respective marketplaces.

You can then deploy, register and start using the WAF appliance from Azure or Google Cloud.

Note: At the time this document is written, approvals for Amazon AWS, Google Cloud and Microsoft Azure marketplaces are still pending for WAF appliance image 1.4.x. As soon as the approval for each marketplace is received, the option for provisioning the respective appliance will be available.



Add New WAF Appliance

Select Virtual Appliance Image

Choose the virtualization platform you want to use to run your WAF appliance on.

Platform	Details
● VMware Standard	VMware virtualization platform
○ Hyper-V	Microsoft Hyper-V 5.1 virtualization platform
○ Amazon EC2	Amazon EC2-Classic, Amazon EC2-VPC
○ Microsoft Azure	Microsoft Azure platform
○ Google Cloud	Google Cloud platform

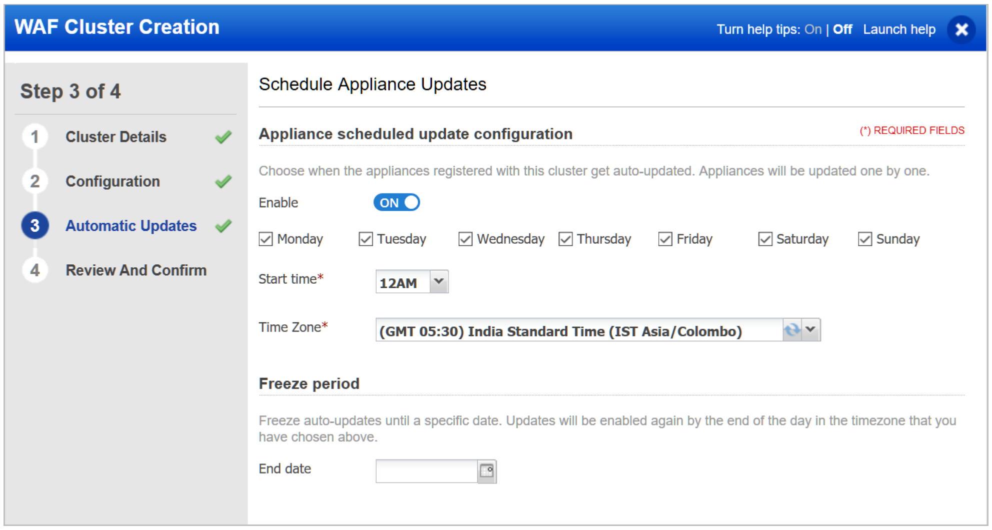
Refer to the WAF Getting Started Guide for details.

Schedule auto-update for appliances registered to a cluster

You can now choose when the appliances registered with a cluster get auto-updated. Select days of the week and the start time. By default, auto-update is enabled for all days of the week.

You can choose to freeze auto-updates until a specific date. Auto-updates are stopped up to the end date and then resumed.

Simply go to WAF Appliances > WAF Cluster, create a new cluster or edit an existing cluster, and then click Automatic Updates.



WAF Cluster Creation

Turn help tips: On | Off Launch help

Step 3 of 4

1 Cluster Details ✓
2 Configuration ✓
3 Automatic Updates ✓
4 Review And Confirm

Schedule Appliance Updates

Appliance scheduled update configuration

(*) REQUIRED FIELDS

Choose when the appliances registered with this cluster get auto-updated. Appliances will be updated one by one.

Enable: ON

☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

Start time*: 12AM

Time Zone*: (GMT 05:30) India Standard Time (IST Asia/Colombo)

Freeze period

Freeze auto-updates until a specific date. Updates will be enabled again by the end of the day in the timezone that you have chosen above.

End date:

In the clusters table, hovering over the 📅 icon under the deployment status shows the time when the next scheduled update is planned.

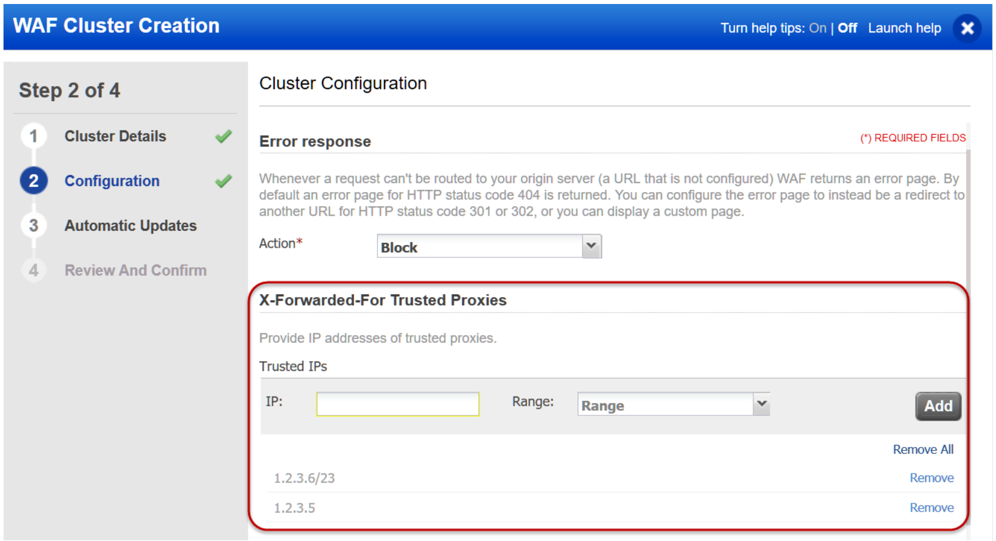
The Upgrade option in clusters Quick Actions Menu is not available until the time you have chosen to freeze auto-updates.

Add trusted proxies for a Cluster

While configuring a cluster you can now provide the IP address/range/network of trusted origin proxies or load balancers configured in full-proxy mode. Enter an IP address between 1.0.0.0 - 223.255.255.254 excluding 127.x.x.x. Optionally, you can provide a range for the IP address between 1 - 32.

For example, `1.2.3.6/23`

If the request is not from a trusted source the X-Forwarded-For header values are automatically discarded. If you do not provide IP addresses for trusted origin proxies or load balancers, then IP addresses as per RFC1918 are trusted.



WAF Cluster Creation

Turn help tips: On | Off Launch help

Step 2 of 4

1 Cluster Details ✓
2 Configuration ✓
3 Automatic Updates
4 Review And Confirm

Cluster Configuration

Error response

(*) REQUIRED FIELDS

Whenever a request can't be routed to your origin server (a URL that is not configured) WAF returns an error page. By default an error page for HTTP status code 404 is returned. You can configure the error page to instead be a redirect to another URL for HTTP status code 301 or 302, or you can display a custom page.

Action*: Block

X-Forwarded-For Trusted Proxies

Provide IP addresses of trusted proxies.

Trusted IPs

IP: Range: Range Add

Remove All

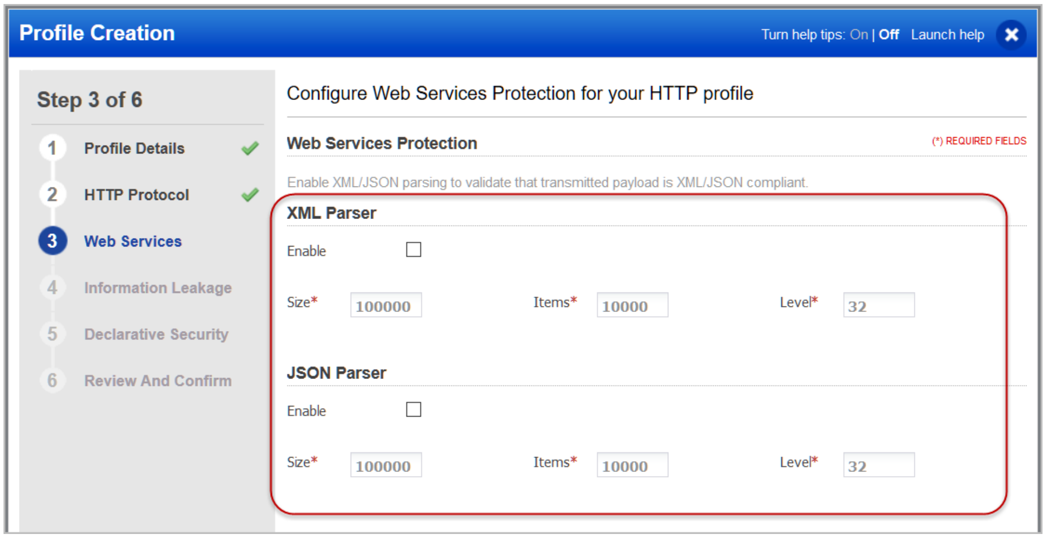
1.2.3.6/23 Remove

1.2.3.5 Remove

Validate XML/JSON payload

You can enable XML/JSON parsing in HTTP profiles to validate that transmitted payload is XML/JSON compliant. Parsing is not enabled by default.

Provide values for:
Size: Maximum size of XML/JSON buffer accepted. Default is 100000 characters.
Item: Maximum object count to parse (XML tag or JSON node). Default is 10000.
Level: Maximum hierarchy level accepted for structured content. Default is 32.



Configure Web Services Protection for your HTTP profile

Web Services Protection (*) REQUIRED FIELDS

Enable XML/JSON parsing to validate that transmitted payload is XML/JSON compliant.

XML Parser

Enable □

Size* 100000 Items* 10000 Level* 32

JSON Parser

Enable □

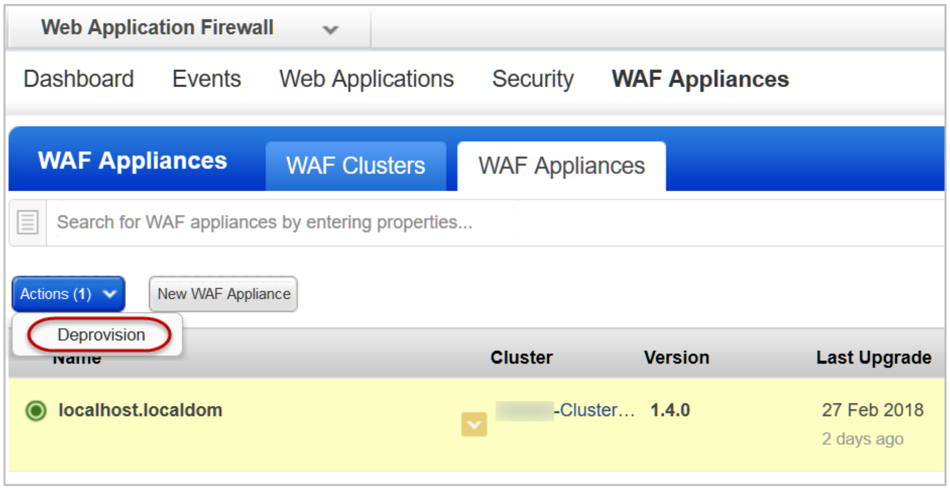
Size* 100000 Items* 10000 Level* 32

Deprovision WAF appliance

You can now deprovision (remove) a WAF appliance from the Qualys Cloud Platform.

To remove a WAF appliance, go to the WAF Appliances tab, select the appliance that you want to remove, and then click **Deprovision** in the Actions menu or the Quick Actions menu of that appliance. Click **confirm** at the message asking you to confirm the removal.

This deregisters the appliance from Qualys Cloud and removes the appliance from the Qualys Cloud Platform. The appliance is however retained on the host in unregistered mode.



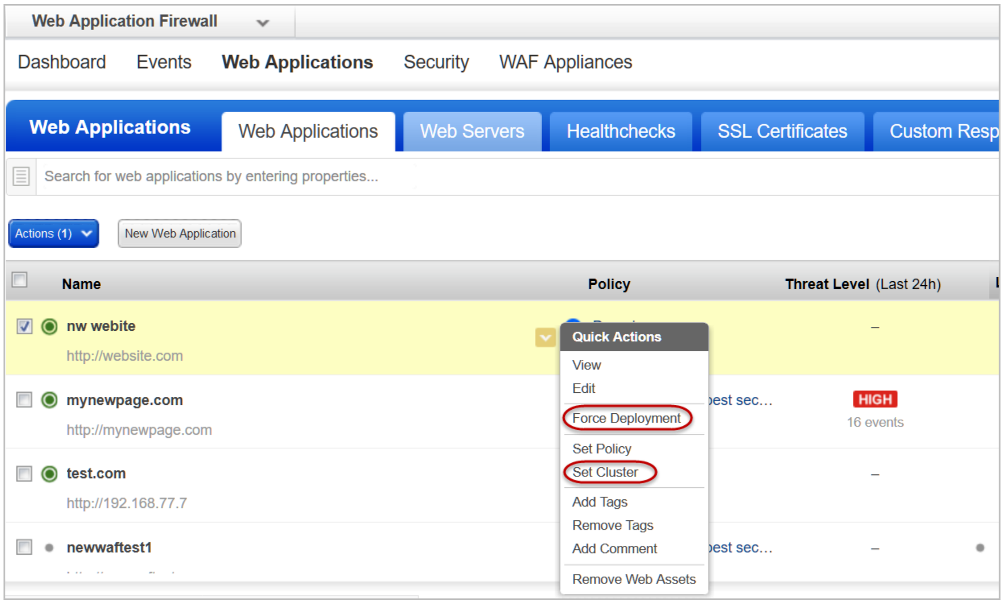
Name	Cluster	Version	Last Upgrade
localhost.localdom	[redacted]-Cluster…	1.4.0	27 Feb 2018 2 days ago

User must have "Manage WAFs" permission in order to deprovision an appliance.

New Quick Actions for Web Applications

This release of WAF introduces two new quick actions for Web applications.

- Force Deployment
- Set Cluster



Name	Policy	Threat Level (Last 24h)
☑ nw webite http://website.com		–
□ mynewpage.com http://mynewpage.com	est sec...	HIGH 16 events
□ test.com http://192.168.77.7		–
□ newwaftest1	est sec...	–

Force Deployment

Force Deployment lets you push a web application and its configurations to associated WAF clusters and registered appliances. The deployment status gets updated once the Web application and configurations are deployed.

To use the Force Deployment option, go to the Web Applications tab, and from the Quick Actions menu of a web application, click **Force Deployment**. Click **confirm** at the message asking you to confirm the force deployment.

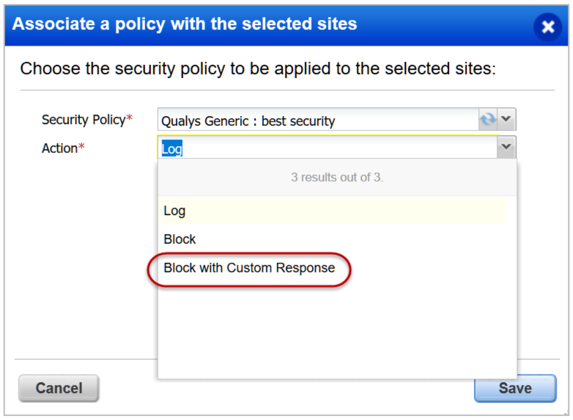
Set Cluster

Set Cluster lets you associate a cluster to a Web application without the need to launch the Web Application Edit wizard.

To associate a cluster, go to the Web Applications tab, and from the Quick Actions menu of a web application, click **Set Cluster**. Select a cluster from the list and then click **Save**. Clusters already associated with the Web application are checked by default.

Custom Page for Set Policy

You can now provide a custom page while using the set policy option from a web application's quick action menu.


Associate a policy with the selected sites

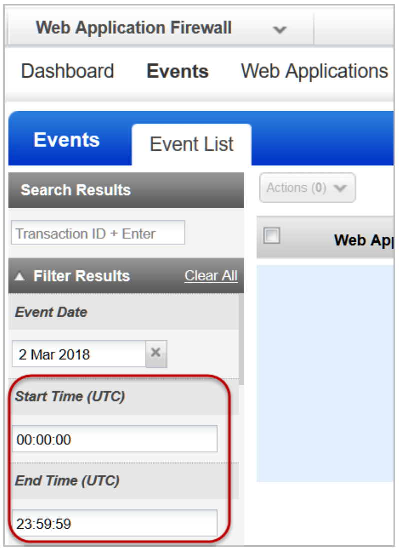
Choose the security policy to be applied to the selected sites:

Security Policy*: Qualys Generic : best security

Action*: Log

Time filter enhancements for Events

You can now filter events not just by Date, but by time as well. The start time and end time filters for Event List let you enter precise time in the form of hours:minutes:seconds (hh:mm:ss).


Event Date: 2 Mar 2018

Start Time (UTC): 00:00:00

End Time (UTC): 23:59:59

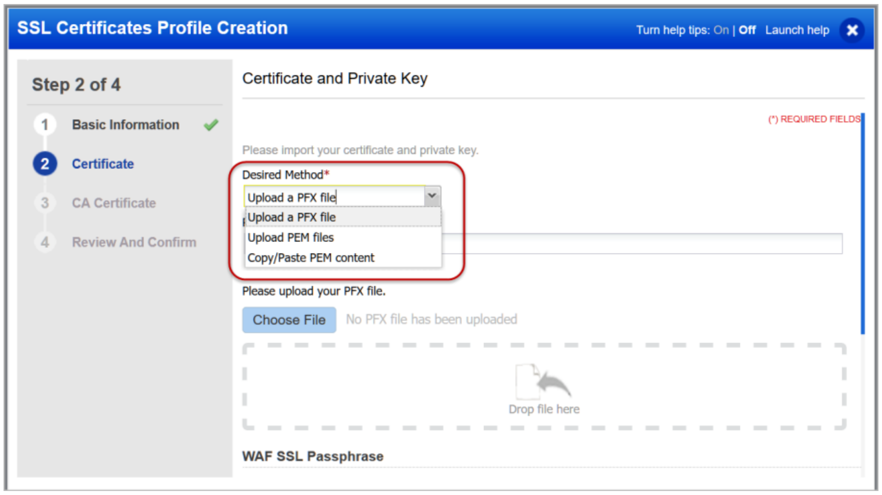
Tip: Pressing Enter after you specify Hours/Minutes automatically sets Minutes or Seconds to zero. For example, if you specify 22 for Hours and then press enter, the time will be 22:00:00.

.

Simplified SSL Certificates Profile wizard

The SSL Certificates Profile wizard is now simplified to only provide fields related to a chosen certificate format.

Choose the required certificate format whether PFX (PKCS12) or PEM and then provide the related information.



SSL Certificates Profile Creation

Step 2 of 4

1 Basic Information ✓
2 Certificate
3 CA Certificate
4 Review And Confirm

Certificate and Private Key

(*) REQUIRED FIELDS

Please import your certificate and private key.

Desired Method*: Upload a PFX file

Please upload your PFX file.

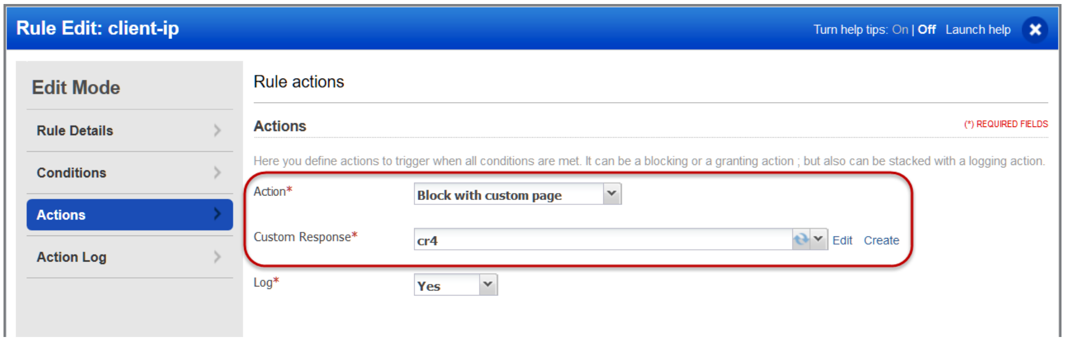
No PFX file has been uploaded

WAF SSL Passphrase

In the CA Certificate section, provide chained / intermediate certificate in PEM format.

Display custom page for custom rule

You can now display a custom page if events match a specific condition in a rule. If you wish to use custom page, select Block with custom page from Action, and then select a custom response page that you have created. Click Edit to modify the selected custom response page, or click Create to add a new custom response page.
Ensure that you create the custom page before you associate it with a custom rule.



Rule Edit: client-ip

Edit Mode

Rule actions

Actions

(*) REQUIRED FIELDS

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

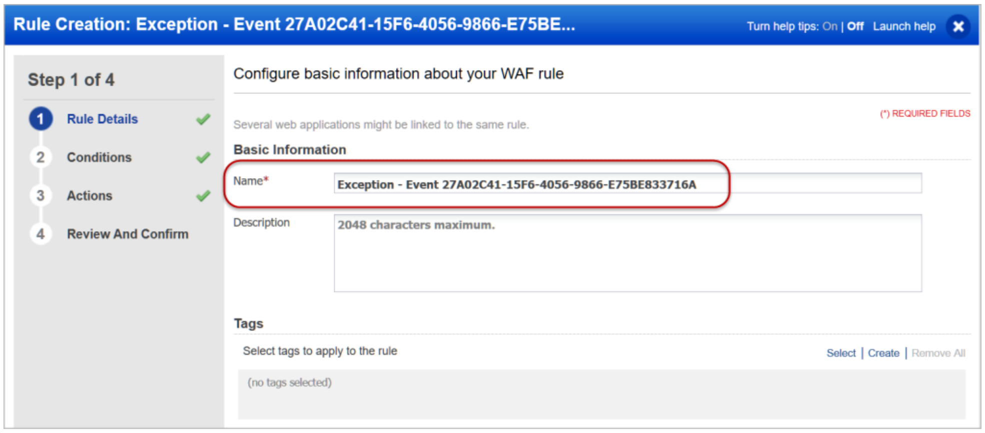
Action*: Block with custom page

Custom Response*: cr4

Log*: Yes

Exceptions and Virtual Patches are now Custom Rules

While creating an exception for a WAF event or installing a patch for a WAS detection, the custom rule wizard now appears instead of different wizards for exceptions or virtual patches as before.



Rule Creation: Exception - Event 27A02C41-15F6-4056-9866-E75BE...

Step 1 of 4

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

Configure basic information about your WAF rule

(*) REQUIRED FIELDS

Several web applications might be linked to the same rule.

Basic Information

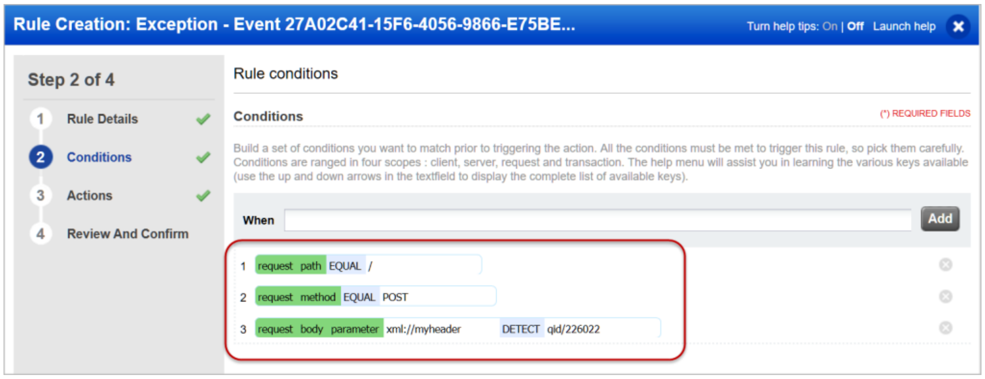
Name*: Exception - Event 27A02C41-15F6-4056-9866-E75BE833716A

Description: 2048 characters maximum.

Tags

Select tags to apply to the rule

(no tags selected)



Rule Creation: Exception - Event 27A02C41-15F6-4056-9866-E75BE...

Step 2 of 4

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

Rule conditions

Conditions

(*) REQUIRED FIELDS

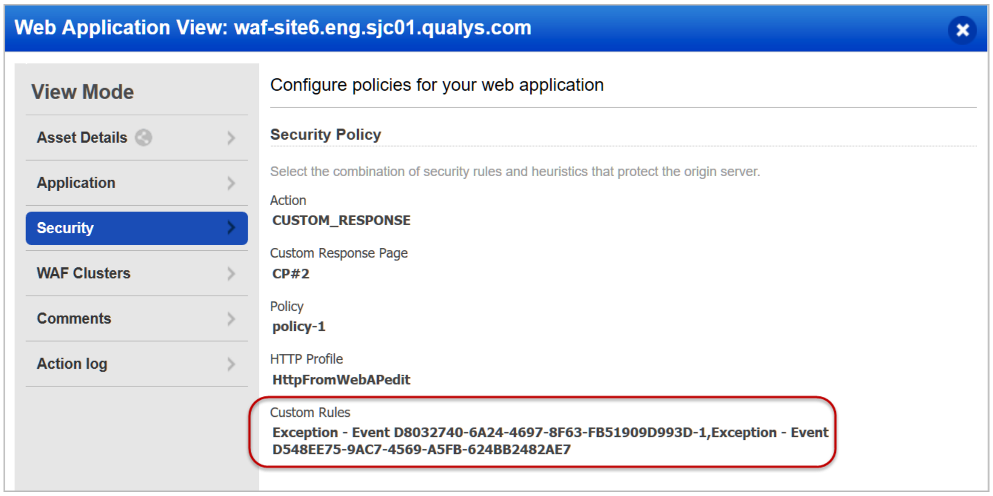
Build a set of conditions you want to match prior to triggering the action. All the conditions must be met to trigger this rule, so pick them carefully. Conditions are ranged in four scopes : client, server, request and transaction. The help menu will assist you in learning the various keys available (use the up and down arrows in the textfield to display the complete list of available keys).

When

1 request path EQUAL /
2 request method EQUAL POST
3 request body parameter xml://myheader DETECT qid/226022

Rule Details and Conditions are auto populated based on the event or detection.

By default, the action for an exception is **Allow** or **Block** (the opposite of the original event's action) and for virtual patch is **Block**.



Web Application View: waf-site6.eng.sjc01.qualys.com

View Mode

Configure policies for your web application

Security Policy

Select the combination of security rules and heuristics that protect the origin server.

Action: CUSTOM_RESPONSE

Custom Response Page: CP#2

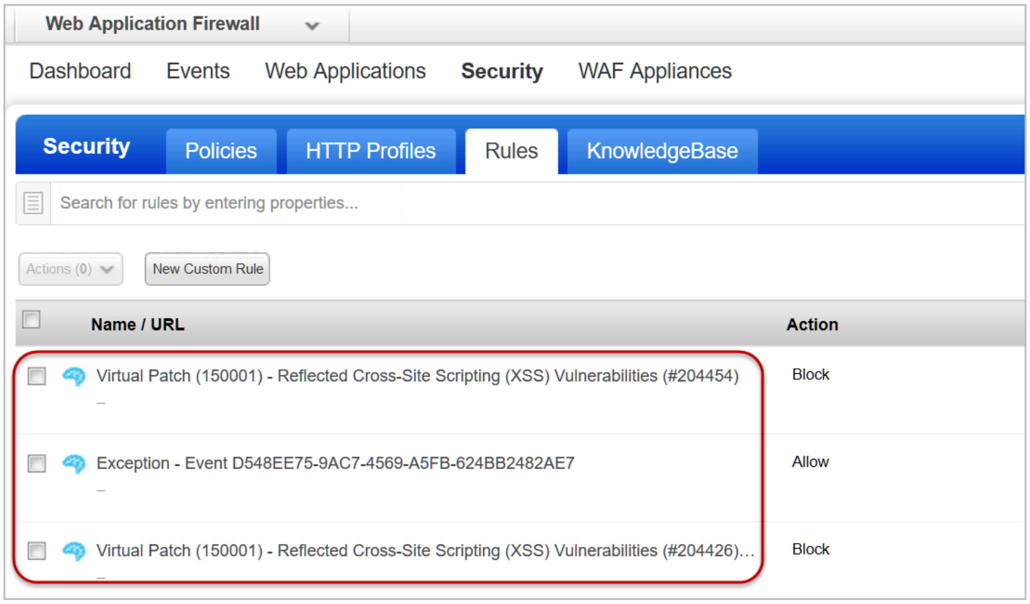
Policy: policy-1

HTTP Profile: HttpFromWebAPedit

Custom Rules: Exception - Event D8032740-6A24-4697-8F63-FB51909D993D-1,Exception - Event D548EE75-9AC7-4569-A5FB-624BB2482AE7

Exceptions or virtual patches once created are linked to the Web application. To view them, simply click View in the Quick Actions for a Web application, and then click the **Security** pane.

All your existing exceptions and virtual patches have now got converted to custom rules. However, your existing exceptions and virtual patches are still visible in the old form along with the newly created custom rules.



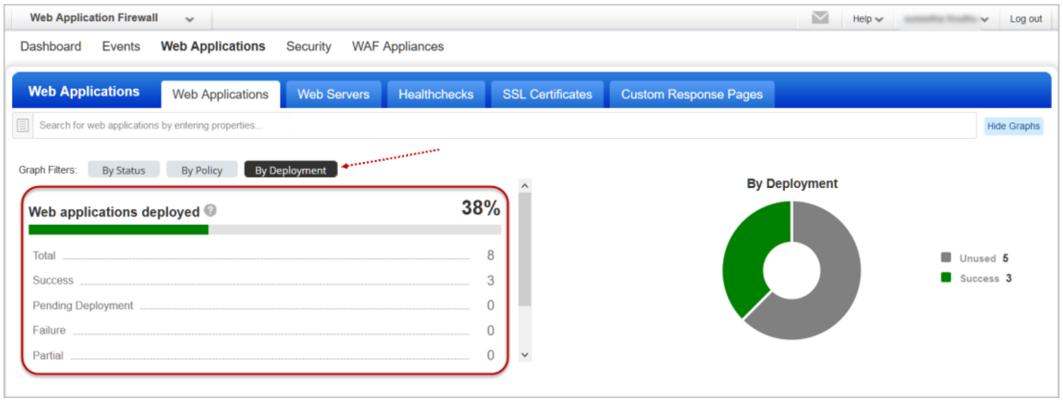
□	Name / URL	Action
□	Virtual Patch (150001) - Reflected Cross-Site Scripting (XSS) Vulnerabilities (#204454) –	Block
□	Exception - Event D548EE75-9AC7-4569-A5FB-624BB2482AE7 –	Allow
□	Virtual Patch (150001) - Reflected Cross-Site Scripting (XSS) Vulnerabilities (#204426)... –	Block

Deleting an exception from WAF events list or a virtual patch from WAS detections list, does not remove the associated custom rule. You can use the custom rule in the future for similar Web applications.

Deployment status in overview panels

You can now view deployment status for web applications, clusters, and appliances in the overview panels and beside the Last Update column in their respective tabs.

For example, here is the deployment status for web applications:



Web applications deployed 38%

Total	8
Success	3
Pending Deployment	0
Failure	0
Partial	0

The deployment status for web applications, clusters, and appliances is as follows:

Web Applications

Status	Description
Success	Web application successfully deployed.
Pending Deployment	Deployment of a Web application is pending.
In Progress	Deployment of Web application on cluster is in progress.
Partial	Deployment failed on at least one cluster or appliance assigned to the Web application.
Failure	Deployment of Web application configuration has failed on all associated clusters.
Unused	Web application is not deployed on any WAF cluster or the Web application is deployed on a cluster having no appliances registered to it.

Clusters

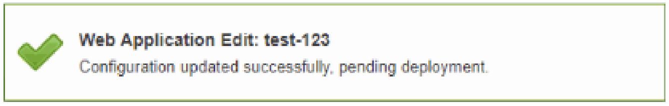
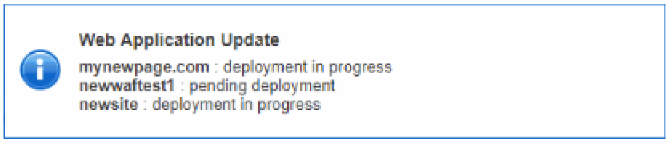
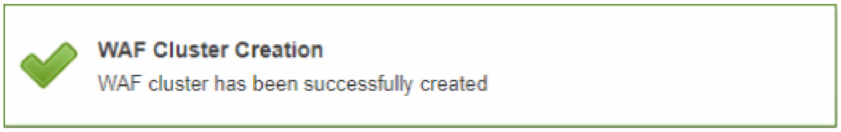
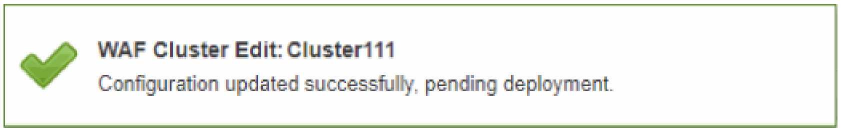
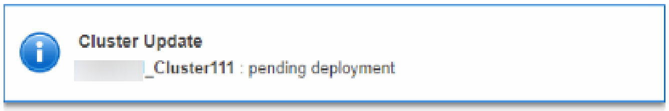
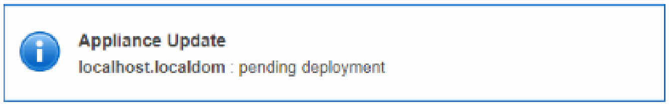
Status	Description
Success	Configuration deployment is successful on all appliances in a cluster.
Pending Deployment	Configuration deployment has been requested but not yet started.
In Progress	Configuration deployment is in progress on all appliances in a cluster.
Partial	Configuration deployment is successful on some appliances but failed on other appliances in a cluster.
Failure	Configuration deployment has failed on all appliances in a cluster.
Unused	Web application is not deployed on any WAF cluster, or the Web application is deployed on a cluster having no appliances registered to it.

Appliances

Status	Description
Success	Appliance configuration deployed successfully.
Pending Deployment	Appliance configuration deployment has been requested but not yet started.
In Progress	Appliance configuration deployment is in progress.
Partial	Deployment of Web application failed on at least one cluster or appliance assigned to the Web application.
Failure	Appliance configuration deployment has failed.
Unused	No Web application is deployed on the Appliance.

Apart from the overview panels, deployment status is also shown as part of messages that briefly appear on top of the Qualys Cloud Platform UI.

Here are a few examples,

Status	Message
Web application configuration updated, pending deployment	 ✓ **Web Application Edit: test-123** Configuration updated successfully, pending deployment.
Web application updated, deployment in progress	 **Web Application Update** **mynewpage.com** : deployment in progress **newwaftest1** : pending deployment **newsite** : deployment in progress
WAF cluster created	 ✓ **WAF Cluster Creation** WAF cluster has been successfully created
WAF cluster configuration updated, pending deployment	 ✓ **WAF Cluster Edit: Cluster111** Configuration updated successfully, pending deployment.
WAF Cluster/Appliance updated, pending deployment	 **Cluster Update** [redacted]**_Cluster111** : pending deployment  **Appliance Update** **localhost.localdom** : pending deployment

Issues addressed in this release

Qualys Cloud Platform 2.32 brings you many more improvements and updates.

AV AssetView

TP ThreatPROTECT

- We have fixed the issue with interfaces.hostname token and now interfaces.hostname token also supports prefix and suffix for search queries.
- Accurate results are now returned for search using the following queries:
  - activatedForModules:"WAS"
  - activatedForModules:"WAF"
- We've implemented controls in query parsing for queries containing the operators AND, OR. The maximum depth allowed for an AND/OR query cannot cross 1000 levels. If you run a query having more than 1000 levels of depth, an error is returned.
  This query has level of depth 2
  vulnerabilities.vulnerability: (severity: "5" AND category: "CGI")
  This query has level of depth 5
  (operatingSystem: windows OR operatingSystem: linux) AND (openPorts.port: 80 OR openPorts.port:8080) AND NOT updated <= "2018-01-20"
- You can now view modules that have activation status pending, no profile found, or queued for manifest in Asset View.
- A note is now added on the create widget screen informing the user that the last rule is applied in case more than one rules are applicable for the widget.
- We've now fixed an issue and the Threat Protect app loads within reasonable time for account with large number of tags.

CA Cloud Agent

- Now a query using the token configurationProfile returns expected results. For example configurationProfile:MyProfile finds agents having the custom profile MyProfile.
- Now the user will see the label "Secure Configuration Assessment"' instead of "Secure Config Assessment" on Activate Agent page.
- User will be able to activate VM, PC, SCA, if the "Do not enforce license count" option is enabled for the subscription level.
- Now SCA activation will fail if the SCA manifest is missing.
- Now the user can see the full value of the installed software version.
- Now users can search for agents using the token lastVMScandate.
- Now the user can see the correct syntax help for the search token lastVMScanDate.

SAQ Security Assessment Questionnaire

- Notification mails sent for questionnaires are now displayed accurately.
- We've fixed the template import issue and now the imported template is displayed appropriately.

WAS Web Application Scanning

- We have now introduced a new report format: CSV_V2. It provides additional information about 12 fields in addition to the information provided by CSV report format.
- We have identified and fixed missing help tips across the Web Application Scanning module.
- We have now fixed an issue where users in a subscription with certain settings can now edit a WAS scan schedule.
- We have now improved the text descriptions and user-facing error messages for Form Training section when you create or edit a web application.
- We have now fixed the issue with the custom attribute filter so that it now functions as expected.
- We have now fixed an issue to correctly display the logged-in user's email address to configure notifications when the user tries to edit a schedule from quick action menu.
- We have now fixed the issue with the Scanner Not Available filter so that it now functions as expected.
- We now include Burp and Bugcrowd findings along with Qualys detections in the response for Search finding API.
- Name Uniqueness for schedule scans is applicable to active schedules. If you have deleted a schedule scan for an existing web application, and created a new schedule for the same web application, the scheduled scan name need not be unique with respect to the deleted schedule.
- We have now rectified the XSD to correctly fetch GET request for Finding API and support IGNORED, PATCHED, and PROTECTED types of findings in the response.
- We now correctly display the correct icon in the Type column for authentication records on Authentication List Panel.

WAF Web Application Firewall

- The event details tab has improved UI for expanding various sections like Event Summary, Event Inspection and Transaction Details.
- Appliance details - CPU information is now sorted and well aligned.
- Custom rules - server.ip.address help tip example is now improved to match the supported operators.
- Web Applications wizard now displays a proper error message if a chosen system policy is not available in the backend.
- The Web application wizard now validates the input for failure response code.
- Fixed an issue where the create link was not enabled for custom response page while editing a WAF cluster.
- Fixed an issue where the graphs on WAF appliances tab did not reflect the correct appliance statuses.
- WAF cluster wizard - configuration pane now shows improved labels and description.

MD Malware Detection

- Now customers will see a correct display of dates in the Summary Report.

FIM File Integrity Monitoring

- We'll now show an informational error message when the user tries to add a new monitoring profile with the same name as an existing profile.
- On the dashboard, when the user clicks the Tags icon next to "Last 30 days" the tags shown have proper layout.
- Users will not able to assign cross platform OS monitoring profiles. For example a Windows monitoring profile can't be assigned to a Linux asset.
- When adding or editing a rule, leading white spaces for "Directory Path" are trimmed and ignored (a "Directory Path" cannot start with white spaces).
- When adding or editing the Advanced Options for a monitoring profile, the white spaces at the beginning of the pattern are ignored, and trimmed.
- Profile name with special characters is now displayed properly on the dashboard.
- Now the Create Incident button is disabled when there are no events in the user's account.
- Under Events, the tab "Recent" was renamed to "Event Review".
- On the Events list we renamed column from Event to Action.
- On Assign a Monitoring Profile page we added a tooltip for long profile names. Now users can choose to view the entire profile name when the name is long.
- On the Assets tab we've added a hyperlink for asset name. When clicked the user views the Asset Details.
- Query gives correct result when the user edits an incident and changes the query.
- We changed text in Asset Details on the Tags list page. The page name changed to Tag Selector (from Asset Selector).

IOC Indication of Compromise

- We've added background color for chart tooltips on dashboards for better readability.
- Now users will not be able to create widgets using same name.
- We've added a tool-tip for the score icon.
- You can now view accurate data for registry.data in group by dropdown in the widget.
- The asset name link is enabled for active assets only.
- Filters now appear on the Assets tab.
- Fixed an issue where improper occurrences were displayed on the Hunting tab.
- Label text in now displayed correctly without being truncated.
- A note is now added on the create widget screen informing the user that the last rule is applied in case more than one rules are applicable for the widget.
- Icons in Customize widget screen are now resized for better visibility.
- We've fixed alignment of filters in the Hunting tab.
- We've fixed an issue and the IOC tab in Asset Details loads accurately.
- Users will see a success confirmation message when saving or deleting a query.
- Now users who create widget templates can easily find their templates for future use in the Add Widget workflow under Templates > Shared.
- User will be searched with proper key-value.
  Now when the user add a custom Table type widget to a dashboard and clicks the widget, the query is performed as expected and shows the same count as the dashboard.
- On the Hunting tab now the user will see a bar chart of events count against the days axis.

- Under Incidents > Malware now users can click the Indicators and Impacted Assets links to explore associated results.
- Under Incidents > Hosts now users will see graph indicators of incident count against the days axis.
- Asset links are now disabled when the asset has a cloud agent that is no longer active.

Qualys Cloud Platform

- We've fixed an issue and the following message is now displayed if the EC2 tag resolution fails: "Error in resolving EC2 Assets Tags."
- Fixed an issue where user was not able to scan with All scanners in Tagset when included tag was associated with a deleted scanner.