

Qualys Cloud Suite 2.21

We're excited to tell you about new features and improvements in Qualys Cloud Suite 2.21.



AssetView

ТР

ThreatPROTECT

Better Visibility to Vulnerability Information Use Filters to Redesign Table Widget



Cloud Agent

Easily view supported OS versions Delta Upload Interval - Performance improvement CPU Throttle – Increased upper limit New License Message for Azure Security Center users



Security Assessment Questionnaire

Customize Questionnaire invitation emails Preview a Report before Generating



Web Application Scanning

Easily find Scanner Appliance Details Scanner Appliance Pool Know your Scan Progression New Filters for Ignore Findings in Scan Reports Support for REST based Testing

Qualys Cloud Suite Update 2.21 brings you many more Improvements and updates! Learn more



Better Visibility to Vulnerability Information

Vulnerability details are now more accessible to you while you're looking through vulnerabilities shown in asset details.

Hover over a vulnerability you're interested in and click View Details option. (We've moved View Detail out of quick actions)

The View Details option also appears in your ThreatPROTECT RTIs list when the module is enabled.

weblogic-24-195							8
View Mode		Vulnera	abilities				
Asset Summary	>	E	Type Confirmed Severity 3				Search
Open Ports	>	< Back to s	summary				10 vulnerabilities 🐳 🗸
Installed Software	>	QID	Title	Detected Date	Port	Protocol	Severity 👻
Vulnerabilities	>	90883	Windows Remote Desktop Protocol Uses	3 days ago	3389	TCP	View Details
ThreatPROTECT RTIs	>	90882	Windows Remote Desktop Protocol Weak	3 days ago	3389	TCP	
		105500	Microsoft Remote Desktop Service Not Usi	3 days ago		_	

Use Filters to Redesign Table Widget

You can now add one or more filters to narrow down your results for the selected group while creating a table type custom widget.

Simply navigate to Dashboard > Add Widget > Custom Table and select the Group assets option.

Filters section is enabled which allows you to add filters for your group.

Filters can be added only for Bar and Pie charts type widgets.

Add a new widget to your dashboard		8
Select data for your widget using the form below (") REQURED FIELDS	Customize the way that your wi	dget looks
	Name	Count
	Business Units	7
Count Table Bars Pie	Unassigned Business Unit	5
Widget Title*		
Untitled Widget		
Query		
Type your query		
Uut assets Group assets Rows * tags.name Columns / Group By Select an item Umit to * To 50		
Filters	. / .	
Add one or more filters to narrow down your results for the selected group.		
Add Rer Tags.name CONTAINS Unit)	
Cancel		Previous Add to Dashboard



Easily view supported OS versions

Get the information you need as you are installing Cloud Agents. Just click the link to view the OS version list supported by the Cloud Agent.

Quick Start Guide Overview

et Si	t Started With Qualys Cloud Agent						
Wha	at do I need t	to know?					
A fe	w things to kno	now before you install agents on hosts within your network.					
Cl	oud Agent R	Requirements:					
°	ese are the requi Your hosts mus We support:	irements for installing agents on your hosts. st be able to reach the Qualys Cloud Platform or the Qualys Private Cloud Platform over HTTPS port -	443.				
	Windows (.exe)	Windows Client Versions Windows Server Versions					
	Linux (.rpm)	Red Hat Enterprise Linux CentOS Fedora OpenSUSE SUSE Amazon Linux Oracle Enterprise Linux					
	Linux (.deb)	Debian Ubuntu					
	Mac (.pkg)	OS X					

Install Agent wizard

Give you nosts.	ur key a name a	nd add tags to easily find agen	ts installed using this key. We'll associate the tags to the age
Activatio	n Key	6fcc927e-5a16-4c64-	b996-f2c15c755ad9
		Key Type	Unlimited key
		Total Count in use	0
nstalla	ation Requi	rements	
	Windows (.exe)	Windows Client W Windows Server V	ersions Install instructions
0	Linux (.rpm)	Red Hat Enterpris CentOS Fedora OpenSUSE SUSE Amazon Linux Oracle Enterprise	e Linux Install instructions
0	Linux (.deb)	Debian Ubuntu	Install instructions
	Mag	OS X	Install instructions

Delta Upload Interval - Performance improvement

Now you can set the Delta Upload Interval performance setting in the configuration profile to something smaller than the minimum 60 seconds (in previous releases) to 1 second minimum. This lets you speed up the rate your agents upload changes to the Qualys Cloud Platform. Also we've added the upper limit of 1800 seconds (30 minutes).

Configuration Profile View							
View Mode		Configure Agent Performance					
General Info	>						
Blackout Windows	>	CPU and network utilization.					
Performance	\rightarrow	Delta Upload Interval* Interval an agent attempts to upload detected changes	60	sec(1 - 1800)			
Assign Hosts	>	Delta Confirmation Interval* Interval an agent checks platform for confirmation that changes were processed	300	sec(60 or more)			

We've changed the default values

Performance profile	Default
Low	10 seconds
Medium	5 seconds
High	1 second

Good to know

- Only new performance profiles you create use the new values (1-1800 seconds)

- It's best practice to go ahead and lower this setting in your existing profiles, similar to the default performance profile ranges: 1, 5 or 10 seconds

CPU Throttle - Increased upper limit

For the CPU Throttle performance setting in the configuration profile, you can now set a value from 0 to 1000 ms. We've increased the upper limit to 1000 ms (from 200 ms).



New License Message for Azure Security Center users

This update applies to the Qualys Vulnerability Management integration with Azure Security Center

When you run out of Qualys VM licenses we'll let you know by displaying a message on your virtual machines in the Azure Security Center (ASC).

This update will populate a message alerting you if there are no more licenses for Vulnerability Management module from Qualys, when you try to look for Vulnerabilities for Virtual Machines under Azure Security Center. This applies to you, if you are using Qualys "vulnerability assessment" solution integration from within Azure Security Center.

It's possible that you've deployed cloud agents on virtual machines within ASC but those machines are not collecting vulnerability information from Qualys because you have no Qualys VM licenses remaining in your subscription. Now you'll see a message on your virtual machines when this happens. Once more licenses are added, the virtual machines that were blocked will start collecting vulnerability information.



Security Assessment Questionnaire

Customize Questionnaire invitation emails

While sending out questionnaire invitation emails for a campaign, you can now be easily customize the email content, email subject, and company logo.

Invitation to Answer	8
An individual invitation to	participate will be generated for each recipient.
Total Recipients: 1 Subject:	
My Campaign	
Message: Security Assessment Que	estionnaire
	Invitation to Answer
Dear {assigneeName}, A Questionnaire, entitle {company} and needs i get started.	Total Recipients: 1 Subject: My Campaign
Thank you for your par {buttonLink} Usemame : {credential Contact Support	Message: Done Security Assessment Questionnaire Change logo
Cancel	Tahoma IB I II A^* I $B \subseteq \Xi$ I $B \subseteq \Psi$ Personalize () Dear {assigneeName}, Image: A = A = A = A = A = A = A = A = A = A
	A Questionnaire, entitled {title}, has been assigned to you by {creatorName} from {company} and needs to be completed by {dueDate}. Please click on the link below to get started. Thank you for your participation! {buttonLink} Username : {credentials} <u>Contact Support</u>
	Cancel

Preview a Report before Generating

You can now preview and edit SAQ report results before you generate the final report.

Just create a new report from the Reports tab, select the type of report you want, select targets and click Preview. The preview is displayed in a new tab, where you can review the information in the report.

Click Edit Report and change any filter or display settings and click Download.

I Reports	Reports Single Instance Report 💌				
ngle Instanc	e Report				
e selected questionr	aire is listed along with all answers from the responders.				
s is a preview of yo	ur report. Click Edit Report to revise the filters and display setti	ngs. Click Download to generate your report.			
No filtere emplied			E	dit Report	Download
No filters applied					
oummary					
Report setting		Report Discovery			
Title:	camp1_2stage - responder.n.3aynml@q	Due Date			
Туре:	Single Questionnaire	Due Date			
Source:	cvv v1	Jan 26.2017			
State:	Information Gathering				
Tags:			Answered	Reviewed	Not Answered
Created by:	sn		0	0	1
Assigned to:	responder n		0	U	•
Delegated to:	-				
		D			

Your report is now generated and is downloaded in the desired format. Once the final report is generated it is added to the data list in the Reports tab.



Web Application Scanning

Easily find Scanner Appliance Details

Knowing scanner appliance details is key to troubleshooting. Go to Scans > Scan List, choose the scan and select View from the quick actions menu, you'll see the scanner appliance details such as scanner name, IP address, scanner version, WAS version, and signature version in the Scan Details.

WAS Vulnerabilit	ty Scan	View	×
View Mode		Review settings used to launch scan	
Overview	>	https://10.11.69.21/WAS-2930/redundantLinks	
Scan Details	>	Settings	
Scan Settings	>	ScanTrust Not enabled	
Action Log	>	Authentication Record None	
		Option Profile OP-FT-KA	1
		Scanner Appliance WAS_Scanner3 (IP: 10.11.51.233, Scanner: 9.0.29-1, WAS: 4.0.37-1, Signatures: 2.3.515-1)	
		Progressive Scanning Disabled	
		Duration Run till completion.	
		Proxy host None	
		Email notification Send mail at scan completion	
Close			

Scanner Appliance Pool

We now give you the flexibility to allocate multiple scanner appliances clubbed in a group to a web application or during scan configuration. You can group the scanner appliances by tagging them with single or multiple asset tags and add the tags to the web application or scan configuration. During scan run time, the best available scanner gets selected from the group of tagged scanners.

Web Application

Web Application E	dit: M	ultiscan_App2	Turn help tips: On Off Launch help 🗙
Edit Mode		Tell us the scan settings you'd like to use	
Asset Details 🔇	>	Default Scan Options	(') REQUIRED FIELDS
Application Details	>	Choose the default scan settings for your web application. Yo Option Profile	'ou can change the defaults for each scan.
Scan Settings	>	Initial WAS Options	View Create
DNS Override	>	Scanner Appliance	ion. You can channe the defaults for each scan
Crawl Settings	>	External Individual	Tags (Set group)
Redundant Links	>	Include appliances that have any of the tags below.	Select Create Remove All
Authentication	>	TagForScanner X ScannerAppliances X	Add tags associated
Crawl Exclusion Lists	>	Lock this scapper appliance for this web application	with Sedimer appliances
Malware Monitoring	>		
Comments	>	Choose Progressing Scanning and we'll add our latest capa crawling to enhance scan coverage, and progressive testing from prior scans.	abilities when scanning this web application. Progressive g to continue tests over multiple scans and verify findings
Action Log	>	Progressive Scanning	
Cancel			Save As Save

You can add a single tag or multiple tags using Select Tags option in Scan Settings when you create or edit a web application. All the scanner appliances associated with the tags form a pool for the web application.

The assigned asset tags are displayed when you view the web application settings or scan settings.

Web Application Vi	iew: M	lywebsite_PSCheck	×
View Mode		Tell us the scan settings you'd like to use	
Asset Details 📀	>	Default Scanner Appliance	
Application Details	>	Include appliances that have any of the tags below.	
Scan Settings	>	Locked	
DNS Override	>	False	
Crawl Settings	>	Default Scan Options	
Redundant Links	>	Initial WAS Options	
Authentication	>	Progressive Scanning Enabled	
Crawl Exclusion Lists	>	Duration	
Malware Monitoring	>	Cancel Scan Disabled	
Comments	>	Crawling Hints	
Action Log	>	Crawl all links and directories found in the robots.but file, if present Off	
Close		Edit Save As Scan 🗸 View R	eport

Similarly, you can assign the multiple scanner appliances to a scan or when you launch or schedule a scan. Add the tag (used to group multiple scanner appliances) using Select Tags option in Scan Settings.

Know your Scan Progression

You can now view the scan progression number in the Scan Datalist, Scan View as well as in the scan reports. Progressive scanning adds the ability to prioritize the crawling of new pages over those that were crawled in a previous successful scan. The scan progression number is updated only after successful scan.

Scan Data List

Scan List Schedules Option Profiles Defaults						
Actions (0) V New Scan V				41 - 60 of 1	16	₽ \$ ~
Name Name	Status	Progression #	Links	Severity	Scan Date	Ŧ
Relaunch 2017-01-13 - Discovery Scan Web Application http://10.11.41.136/anjali/formtest/index.html	Finished	-	18	-	13 Jan 2017	•
Image: State	Finished	-	18	-	13 Jan 2017	Þ
Relaunch Relaunch Relaunch Relaunch Relaunch Relaunch Relaunch Relaunch Relaunch Mywebsite30links http://10.11.41.136	Finished	9	30	HIGH	12 Jan 2017	₽
Total web applications : 2	Finished	-	-	-	12 Jan 2017	▶
Relaunch Relaunch Relaunch Relaunch Relaunch Relaunch Relaunch Mywebsite30links http://10.11.41.136	Time Limit Rea	8	2	MED	12 Jan 2017	∢
Relaunch Relaunch Relaunch Relaunch Relaunch Relaunch Mywebsite30links http://10.11.41.136	Finished	7	30	HIGH	12 Jan 2017	Þ
Relaunch Relaunch Relaunch Relaunch Mywebsite30links http://10.11.41.136	Finished	6	30	HIGH	12 Jan 2017	Þ
Relaunch Relaunch Relaunch Mywebsite30links http://10.11.41.136	Finished	5	30	HIGH	12 Jan 2017	Þ
Image: The second sec	Finished	4	30	HIGH	12 Jan 2017	Þ
Mywebsite30links	Finished	3	29	HIGH	10 Jan 2017	31

Go to Scans > Scans List and the Progression # column displays in the Scan Datalist displays the scan progression number.

If a dash is displayed in the progression number column, it could be because:

-progressive scanning is not enabled. The scan progression number is displayed only if you have enabled progressive scanning for the web application.

-it is a discovery scan.

-it is a multi-scan. For multiple scans, the progression number is displayed only for the child scans. Choose View Scans from the quick actions menu to view the progression number for the child scans.

Scan View

choose View from WAS Vulnerability Scan View	×
the quick actions menu and the Scan findings overview	
progression Overview > Relaunch Relaunch test progressive scan 1	
number is displayed in the Overview section of the Scan View. Scan Details Target Mywebsite_PSCheck Scan Details Status: Finished Action Log Statt Date: 17 Jan 2017 4:16PM GMT+0530 Duration: 00:12:52	
Progression Number Crawling Time Assessment Time Operating Sys 12 00:02:29 00:10:23 Linux 2.4-2	em . 6
Links Collected Links Crawled Requests Performed Avg. Response 54 30 5660 0.104914 set	Time conds

		Ceponts	Scriedules	Templates	Scan report ×	Defaults	
Broken Authentication	and Session M	anagemen	nt				
	Crore Site Seri	inting (VCC					
	cross-site scri	pung (XSS	»)				
Insecure Direct Object References Security Misconfiguration							
Missing Function Level Access Control							
Cross-Site Request Forgery (CSRF) Using Components with Known Vulnerabilities							
Unvalidated Redirects an	d Forwards						
onvaridated recurrents an	d i official dis						
10 20	30	40	50 60	70	80 90		
an					Date	Level 5	Level
esults (108)							
esults (108) Aulnerabilities (90)							
esults (108) Aulnerabilities (90) nformation Gathered (18)						
esults (108) Aulnerabilities (90) nformation Gathered (ppendix	18)						
esults (108) Aulnerabilities (90) nformation Gathered (ppendix Scan Details	18)						
esuits (108) Autherabilities (90) Information Gathered (ppendix Scan Details Relaunch Relaunch test	18)	an 1					
esuits (108) Aulnerabilities (90) nformation Gathered (ppendix Scan Details Relaunch Relaunch test	18) progressive so	:an 1	1055000				
esuits (108) Vulnerabilities (90) nformation Gathered (ppendix Relaunch Relaunch test Reference Date	18) progressive sc was/14846	:an 1 19993612. 7 41684	1956899 3MT+0530				
esuits (108) vulnerabilities (90) information Gathered (ppendix Scan Details Relaunch Relaunch test Reference Date Mode	18) progressive so was/148464 17 Jan 2017	: an 1 19993612. 7 4:16PM (1956899 3MT+0530				
esuits (108) vulnerabilities (30) information Gathered (ppendix Scan Details Reference Date Mode Turon	18) progressive so was/148464 17 Jan 2017 On-demand Vulnorzbilit	:an 1 19993612. 7 4:16PM 0	1956899 3MT+0530				
esuits (108) Vulnerabilities (90) Information Gathered (ppendix Scan Details Relaunch Relaunch test Reference Date Date Date Programming Scamping	18) progressive so was/148464 17 Jan 2017 On-demand Vulnerability Enabled	:an 1 19993612. 7 4:16PM 0	1956899 3MT+0530				
esuits (108) Aulierabilities (90) nformation Gathered (ppendix Scan Details Relaunch Relaunch test Reference Detence Mode Type Progressive Scanning Dronzessive Scanning	18) progressive sc was/148464 17 Jan 2017 On-demand Vulnerability Enabled	:an 1 19993612. 7 4:16PM 0 7	1956899 GMT+0530				
esuits (108) Autherabilities (90) Information Gathered (ppendix Scan Details Relaunch Relaunch test Reference Date Mode Type Progression Number Authentifeation	18) progressive sc was/14846 17 Jan 2017 On-demand Vulnerability Enabled 12 Nons	:an 1 9993612. 7 4:16PM 0 7	1956899 3MT+0530				
esuits (108) Aulinerabilities (90) nformation Gathered (ppendix Scan Details Relaunch Relaunch test Reference Date Mode Type Progression Number Authentication Scannar Amilance	18) progressive sc was/148464 17 Jan 2017 On-demand Vulnerability Enabled None Scapper W	:an 1 19993612. 7 4:16PM C 7	1956899 3MT+0530	nner 9.0.29.1 M	405-4072-1 Sinnah	res: 2.2.515-1)	
esuits (108) vulnerabilities (90) information Gathered (ppendix Scan Details Reference Date Mode Type Progression Number Progression Number Scanner Appliance Profile	18) progressive sc was148464 17 Jan 2017 On-demand Vulnerability Enabled None Scanner_W Scanner_W	:an 1 19993612. 7 4:16PM 0 7 AS (IP: 10.	1956899 3MT+0530 11.51.230, Sca	nner: 9.0.29-1, W	WAS: 4.0.37-1, Signatu	res: 2.3.515-1)	
esuits (108) vulnerabilities (90) information Gathered (ppendix Scan Details Relaunch Relaunch test Reference Date Mode Type Progression Number Authentication Scanner Appliance Profile DN S Querrite	18) progressive sc was/148464 17 Jan 2017 On-demand Vulnerability Enabled 12 None Scanner_W 30Links	:an 1 19993612. 7 4:16PM 0 7 AS (IP: 10.	1956899 3MT+0530 11.51.230, Sca	nner: 9.0.29-1, W	WAS: 4.0.37-1, Signatu	res: 2.3.515-1)	
tesuits (108) Vulnerabilities (90) Information Gathered (ppendix Scan Details Reference Date Mode Type Progression Number Progression Number Authentication Scanner Appliance Profile DNS Override DNS Override	18) progressive sc wast14864 17 Jan 2017 On-demand Vulneability Table None Scanner_W Scanner_W Scanner_G On-12-52	:an 1 19993612. 7 4:16PM 0 7 AS (IP: 10.	1956899 3MT+0530 11.51.230, Sca	nner: 9.0.29-1, W	WAS: 4.0.37-1, Signatu	res: 2.3.515-1)	
esuits (108) vulnerabilities (90) information Gathered (ppendix Scan Details Pelaunch Relaunch test Reference Date Mode Type Progressive Scanning Progression Number Authentication Scanner Appliance Profile DNS Override Duration	18) progressive sc was/148464 17 Jan 2017 On-demand Vulnerability Enabled 12 None Scanner_W 30Links - 00:12:52 Enabled	:an 1 19993612. 7 4:16PM 0 7 AS (IP: 10.	1956899 3MT+0530 11.51.230, Scar	nner: 9.0.29-1, W	WAS: 4.0.37-1, Signatu	res: 2.3.515-1)	
tesuits (108) Vulnerabilities (90) information Gathered (ppendix Scan Details Reference Date Mode Type Progression Number Progression Number Progression Number Drofile DNS Override DNS Override DNS override Duration Status	18) progressive sc was148464 17 Jan 2017 On-demand Vulnerability Enabled None Scanner_W 30Links – 00:12:52 Finished None	:an 1 19993612. 7 4:16PM C 7 AS (IP: 10.	1956899 3MT+0530 11.51.230, Sca	nner: 9.0.29-1, W	WAS: 4.0.37-1, Signatu	res: 2.3.515-1)	

Scan Report

You can also view the scan progression number in the appendix section of the scan report also displays.

Remediation Filters for Ignored Findings in Scan Reports

We have added remediation filters to include or exclude ignored findings in scan reports. By default, the scan report exclude ignored findings. We now provide an option in the scan report template to include ignored vulnerabilities and sensitive contents in addition to or instead of non-ignored findings.

Step 2 of 3	Define filters to include certain	detections in your report					
1 Details	¥						
2 Filter	 New - Vulnerabilities discovered Active - Open vulnerabilities dis 	d for the first time in the very last scan					
3 Display	Re-Opened - Vulnerabilities man	ReOpened Vulnerabilities marked as fixed but discovered again in the very last scan					
Choose filter options to include or exclude ignored findings in scan report.	Patched - Vulnerabilities succes Remediation Filters Specify if you wish to include ignored or	Petched - Vulnerabilities successfully patched by WAF module (will not impact summary & graphs) Remediation Filters Specify if you wish to include inported or patched findings (vulnerabilities and sensitive content) in this report					
	Do not include ignored findings Include ignored findings Include only ignored findings	Do not include patched findings Include patched findings Include patched findings Include only patched findings					
	Select types of ignored findings to includ False Positive Risk Accepted	de**					

Go to Reports > Templates and New Template or edit an existing template. The Filter section includes the new options for Remediation Filter. The types of ignored findings are displayed for selection only if you opt to include ignored findings in the scan report.

To include or exclude ignored findings in an existing scan report, click Edit Report and configure the remediation filter options in Filter section.

Support for REST based Testing

We now include initial support for REST based testing. You can now test your REST based APIs regardless of descriptor used simply by pasting API parameters as shown below and scan as you normally would.

Explicit URLs to Crawl / REST Paths and Parameters / SOAP WSDL Location

```
https://qualysapi.qualys.com/qps/rest/3.0/get/was/webapp
https://qualysapi.qualys.com/qps/rest/3.0/get/was/wasscan
https://qualysapi.qualys.com/qps/rest/3.0/download/was/wasscan
```

Issues Addressed in this release



- Queries are now generated correctly when you click on a dashboard widget which is grouped by vulnerability.
- Sorting your assets list by the modules column is disabled.
- Queries will now be generated correctly when you click Group By view count.
- Query for tags is now updating correctly to show accurate results.
- We have fixed an issue so that duplicate dates are now not displayed in the trending widgets.
- Updated online help to clarify that you can use single or double quotes for string matching, and backticks for exact matching.
- Fixed an issue where edits made to a tag's rule fields were not retained when switching from view mode to edit mode.
- Updated online help to add more helpful information about nested queries and added examples.
- Now the tag selection widget allows the user to add only one tag in the Parent tag panel.
- A saved search name is now displayed truncated to limited characters, and the full name is displayed as a tooltip.
- Saved searches now list the top 50 saved searches.
- ThreatPROTECT: Published dates are now displayed in accurate time zone.
- ThreatPROTECT: Fixed issue with Impacted Assets filter on the Live Feed page. Now the Impacted Assets count in Live Feed articles reflects the user's asset tag selection within the Impacted Assets configuration.
- Preferences such as limitresults were not getting considered if URL parameters were supplied in search APIs using Asset Management API. Now <preferences> in the message body are considered when URL parameters are supplied.
- Qualys Asset Management API v2 User Guide was updated to correct the parameter to startFromId.

CA

- We now display a tool tip in the configuration column during the config agent upgrade for better understanding. Once the upgrade is completed, the new configuration is displayed.
- The Refresh All button is now fixed at top of dashboard and remains visible even on scroll.
- The Distribution by Configuration Profile graph on the dashboard now reflects the correct agent count for configuration profile.
- Qualys Cloud Agent API User Guide is now updated to clarify which APIs do not have optional input parameters.

SAQ

• Comments added to the answers while responding to a questionnaire can now be edited or deleted.

WAS

• When using progressive scanning in WAS to scan web applications, scan results are now displayed accurately in the web application report, when the scan status is "time limit reached".

Qualys Cloud Platform

- The activation job progress bar for activating modules will now show a hide button when the job is finished running successfully.
- The activation job progress bar for activating modules will now show 100% complete, only when the job is finished running successfully.