Qualys Cloud Suite 2.21

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

AV AssetView

TP ThreatPROTECT

Better Visibility to Vulnerability Information
Use Filters to Redesign Table Widget

CA 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

SAQ Security Assessment Questionnaire

Customize Questionnaire invitation emails
Preview a Report before Generating

WAS 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

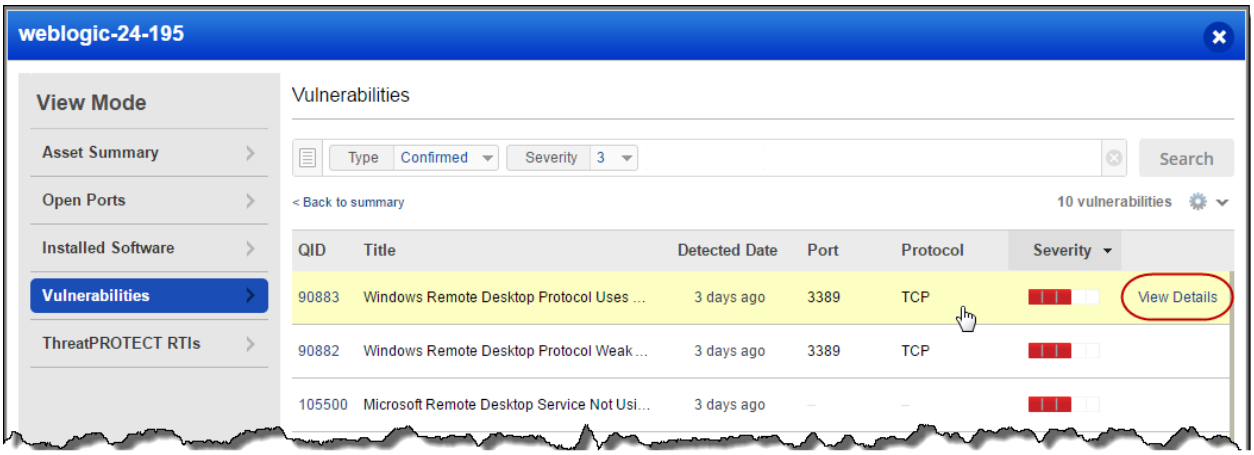
AV AssetView

TP ThreatPROTECT

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.



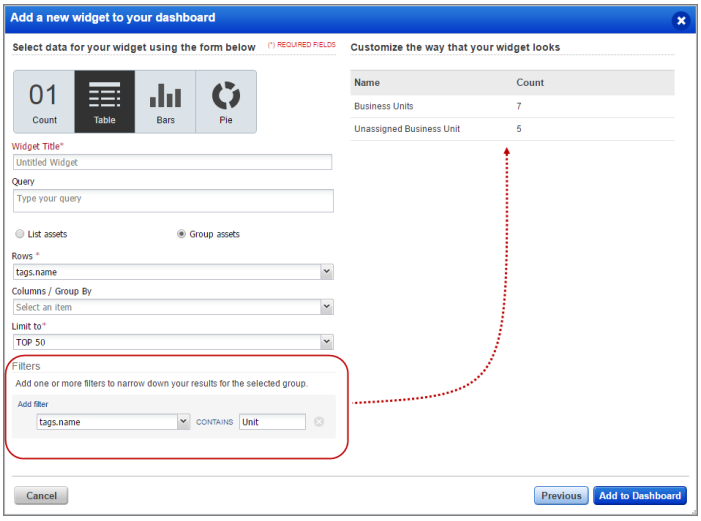
Use Filters to Redesign Table Widget

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.

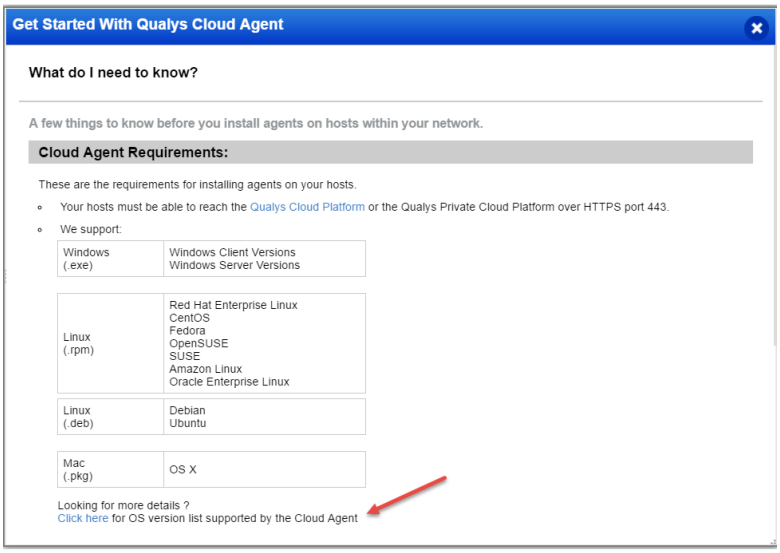


CA Cloud Agent

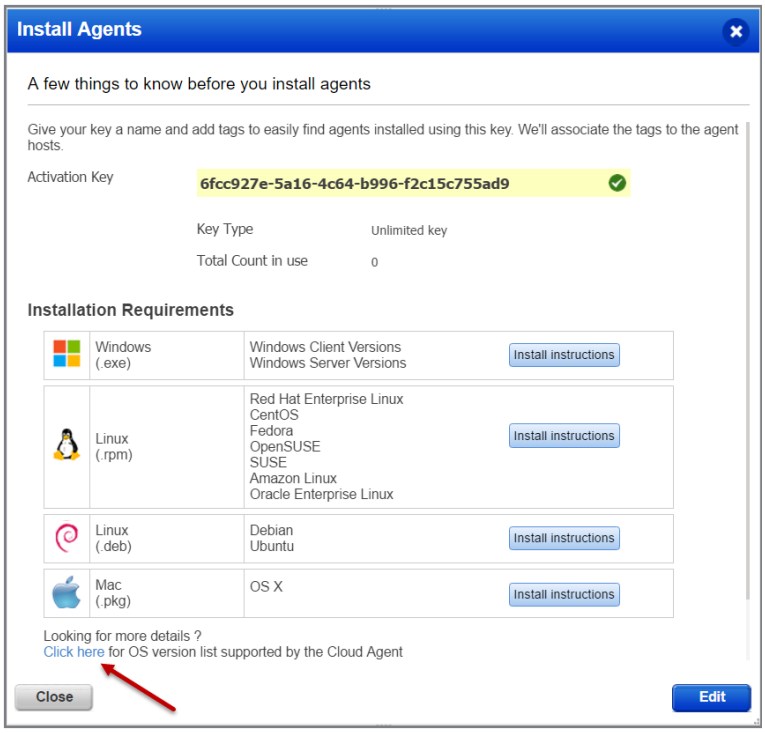
Easily view supported OS versions

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

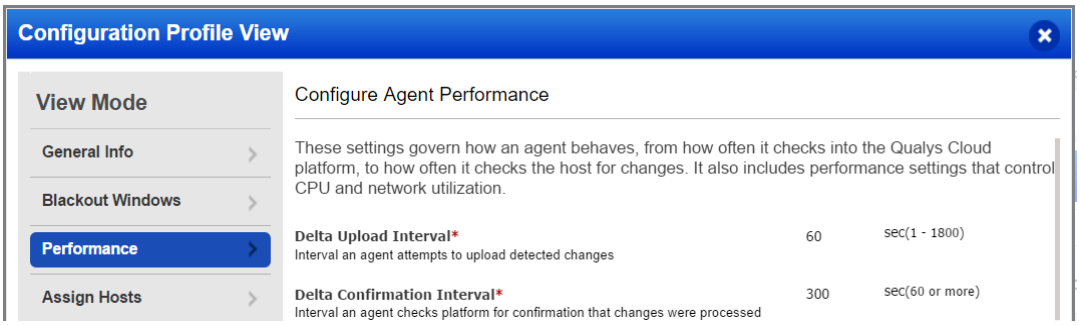


Install Agent wizard



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).



We've changed the default values

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

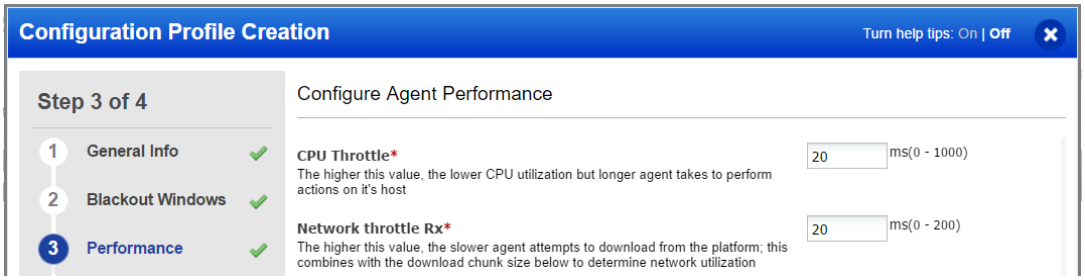
Good to know

- 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

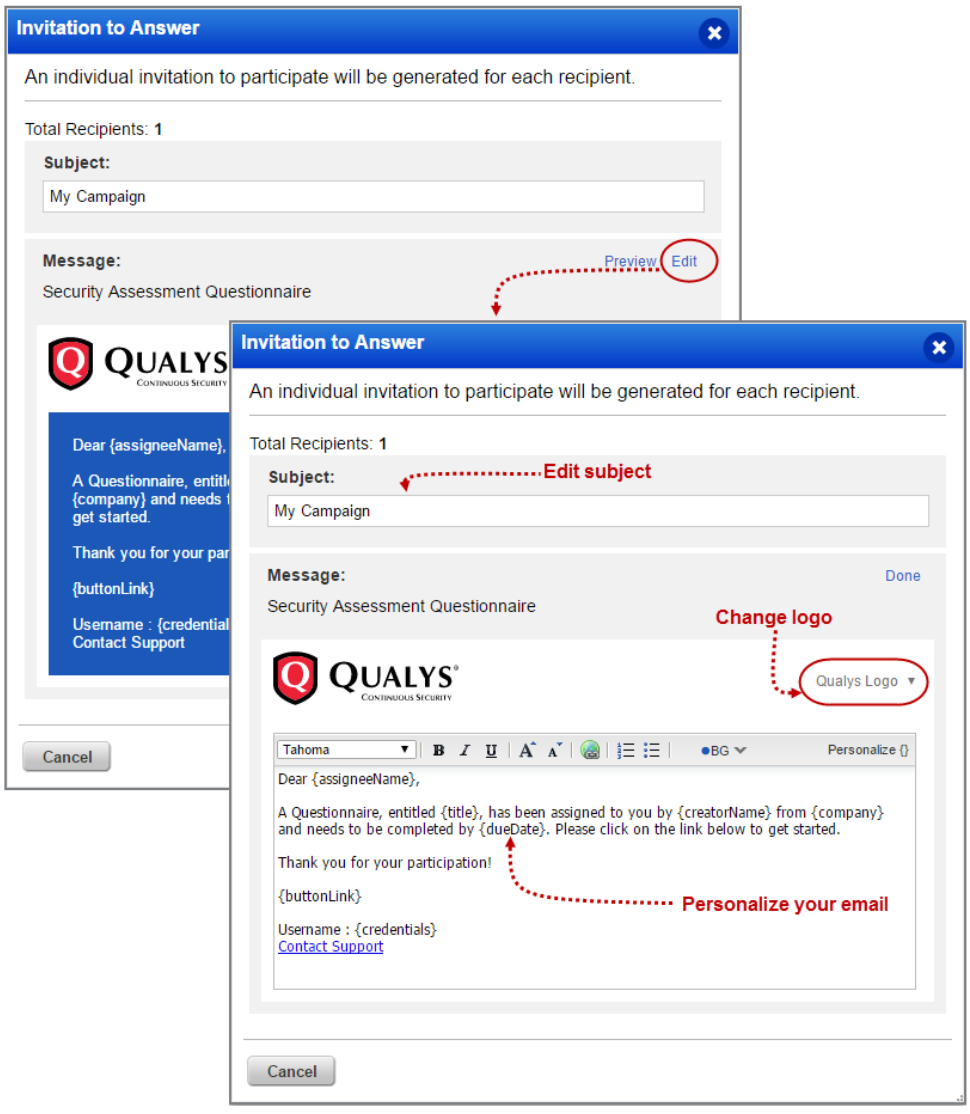
When you run out of Qualys VM licenses we'll let you know by displaying a message on your virtual machines in the Azure Security Center (ASC).

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.

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.

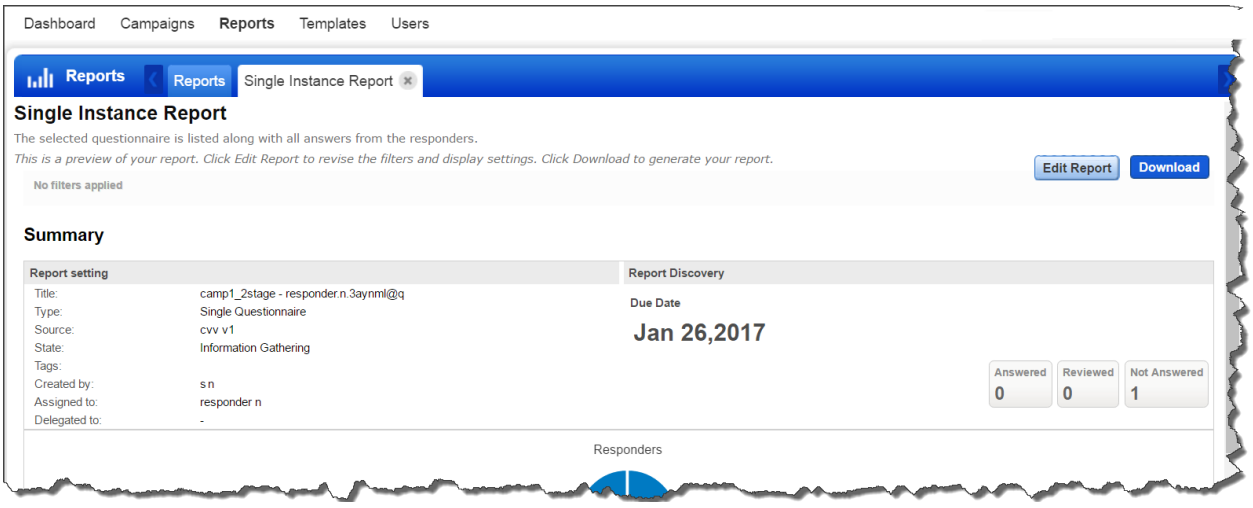


Preview a Report before Generating

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.

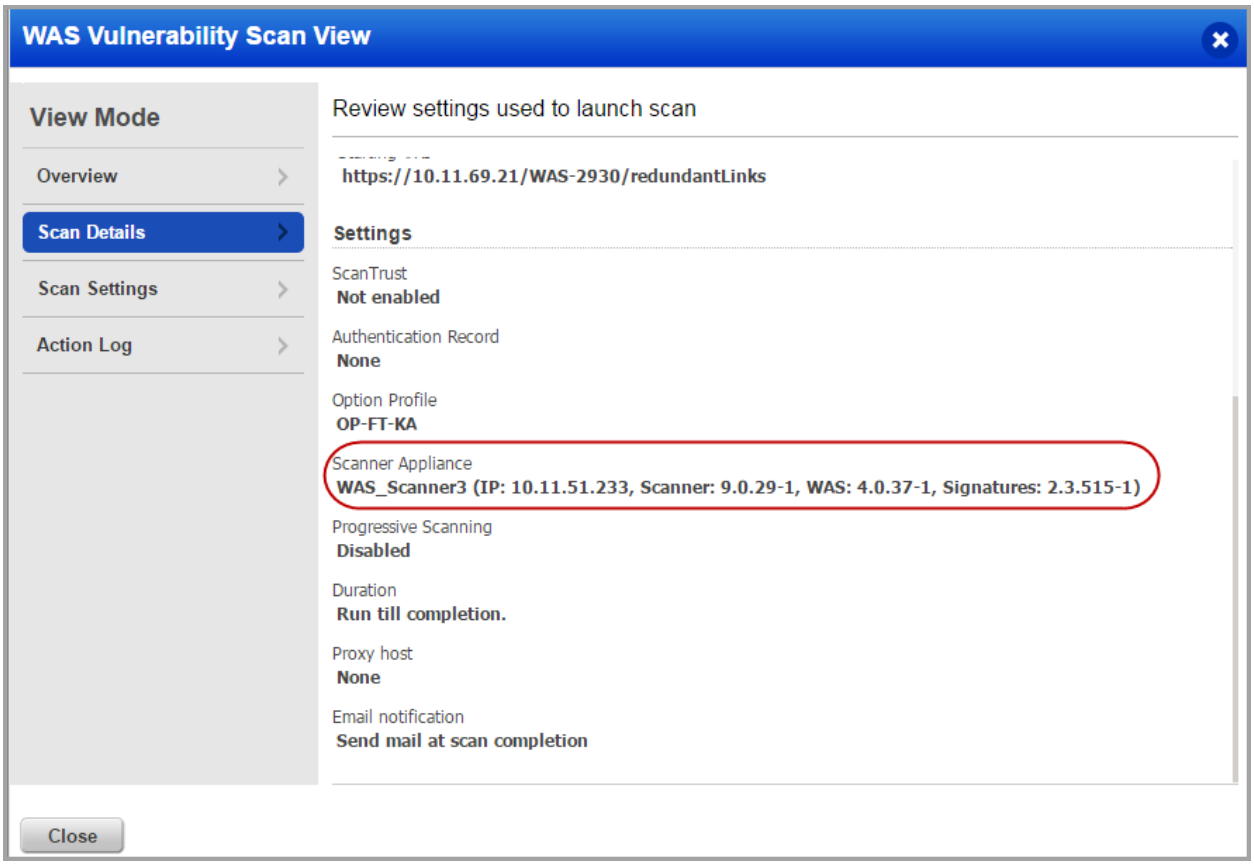


Your report is now generated and is downloaded in the desired format. Once the final report is generated it is added to the data list in the Reports tab.

Web Application Scanning

Easily find Scanner Appliance Details

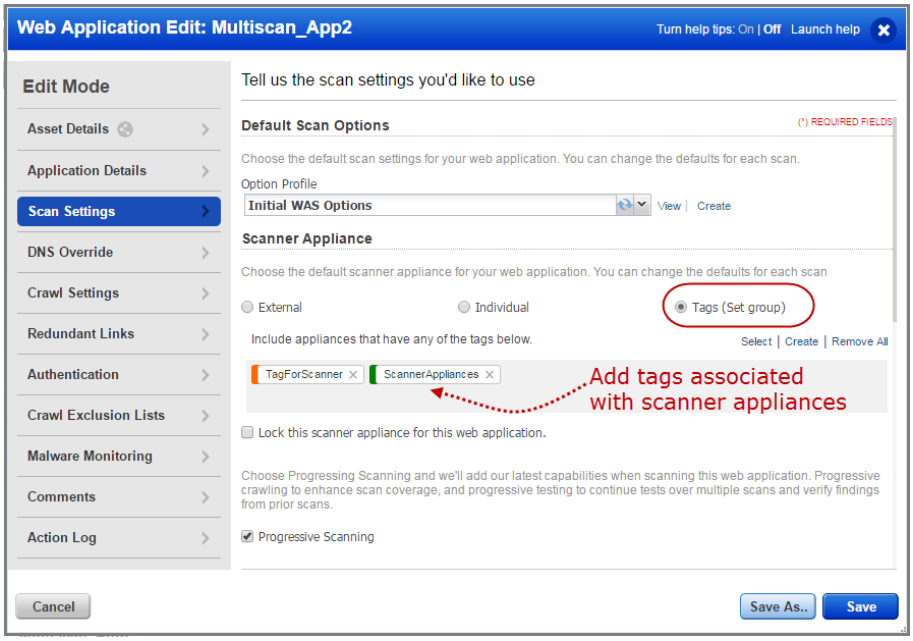
Knowing scanner appliance details is key to troubleshooting. Go to Scans > Scan List, choose the scan and select View from the quick actions menu, you'll see the scanner appliance details such as scanner name, IP address, scanner version, WAS version, and signature version in the Scan Details.



Scanner Appliance Pool

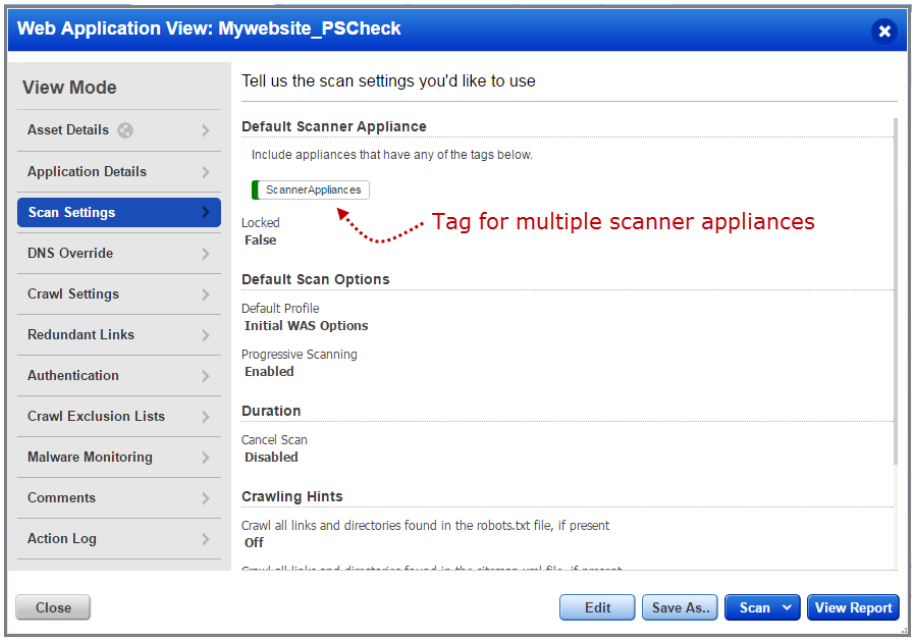
We now give you the flexibility to allocate multiple scanner appliances clubbed in a group to a web application or during scan configuration. You can group the scanner appliances by tagging them with single or multiple asset tags and add the tags to the web application or scan configuration. During scan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

Web Application



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.

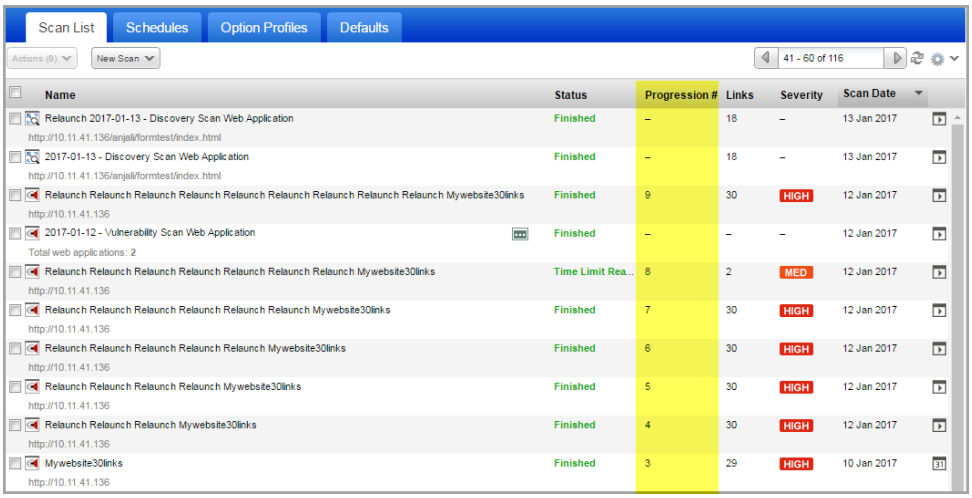


Similarly, you can assign the multiple scanner appliances to a scan or when you launch or schedule a scan. Add the tag (used to group multiple scanner appliances) using Select Tags option in Scan Settings.

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

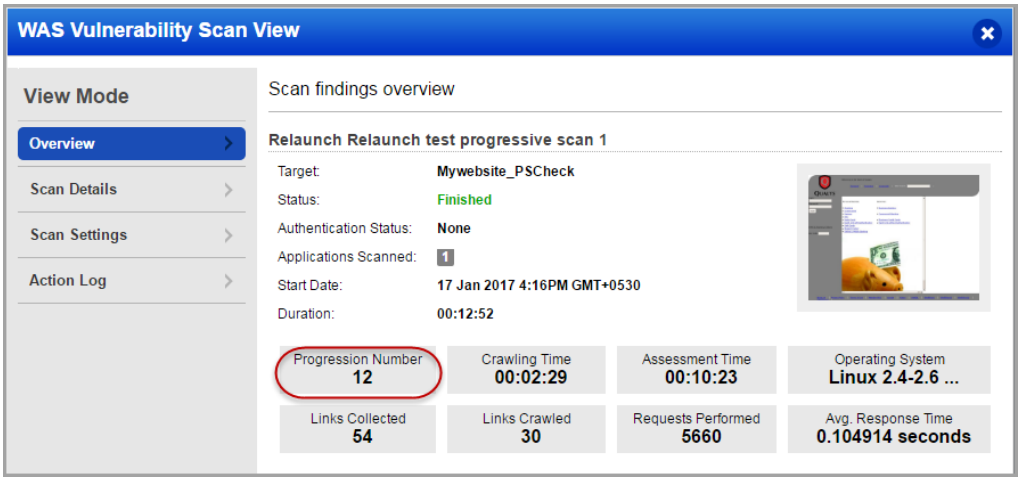


Go to Scans > Scans List and the Progression # column displays in the Scan Datalist displays the scan progression number.

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

Select a scan, choose View from the quick actions menu and the progression number is displayed in the Overview section of the Scan View.

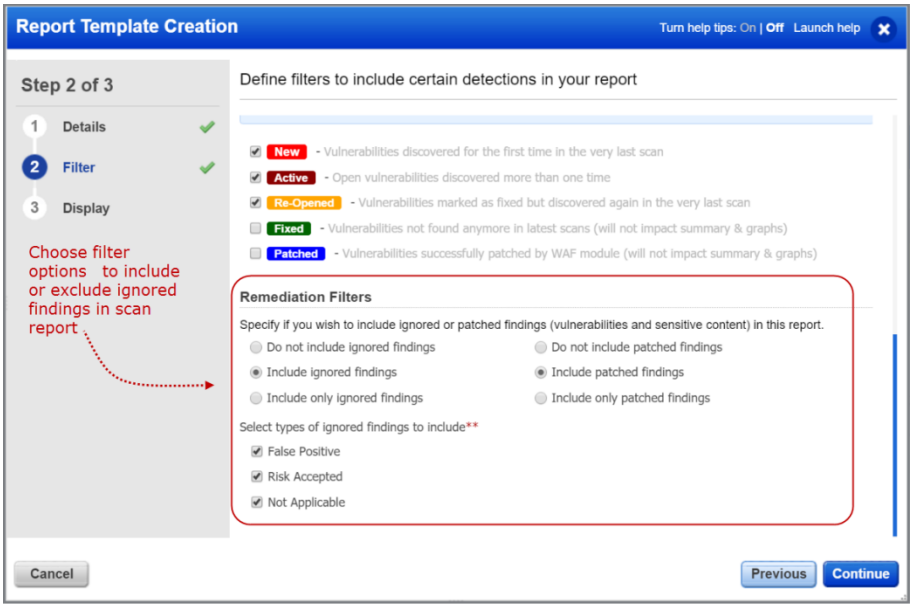


Scan Report

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.

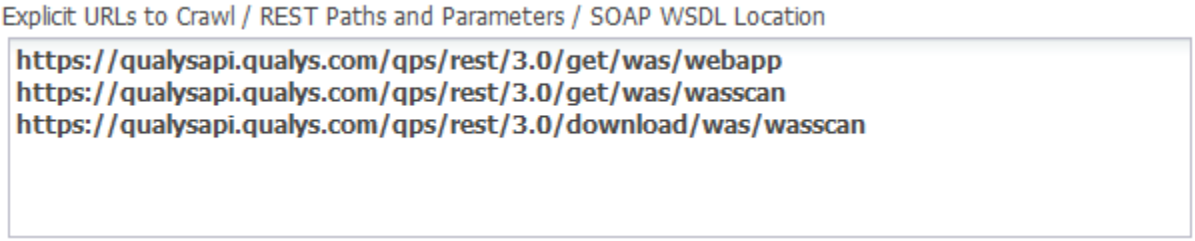


Go to Reports > Templates and New Template or edit an existing template. The Filter section includes the new options for Remediation Filter. The types of ignored findings are displayed for selection only if you opt to include ignored findings in the scan report.

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.



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.

- 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.

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

- 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.