Qualys Cloud Platform (VM, PC) v8.x

Release Notes

Version 8.22

December 13, 2019

(Updated January 30, 2020)

This new release of the Qualys Cloud Platform (VM, PC) includes improvements to Vulnerability Management and Policy Compliance.

Qualys Cloud Platform

Include or Exclude Micro/Nano/Small EC2 Instances in Cloud Perimeter Scan
Include or Exclude Public Load Balancers from Selected Connectors in Cloud Perimeter Scan

Qualys Vulnerability Management

Edit Action Supported for WAS QIDs in KnowledgeBase

Qualys Policy Compliance

Support for New OCA Technologies
DNS Tracking Support
Optimized Cloud Agent Data Processing

Qualys 8.22 brings you many more improvements and updates! Learn more

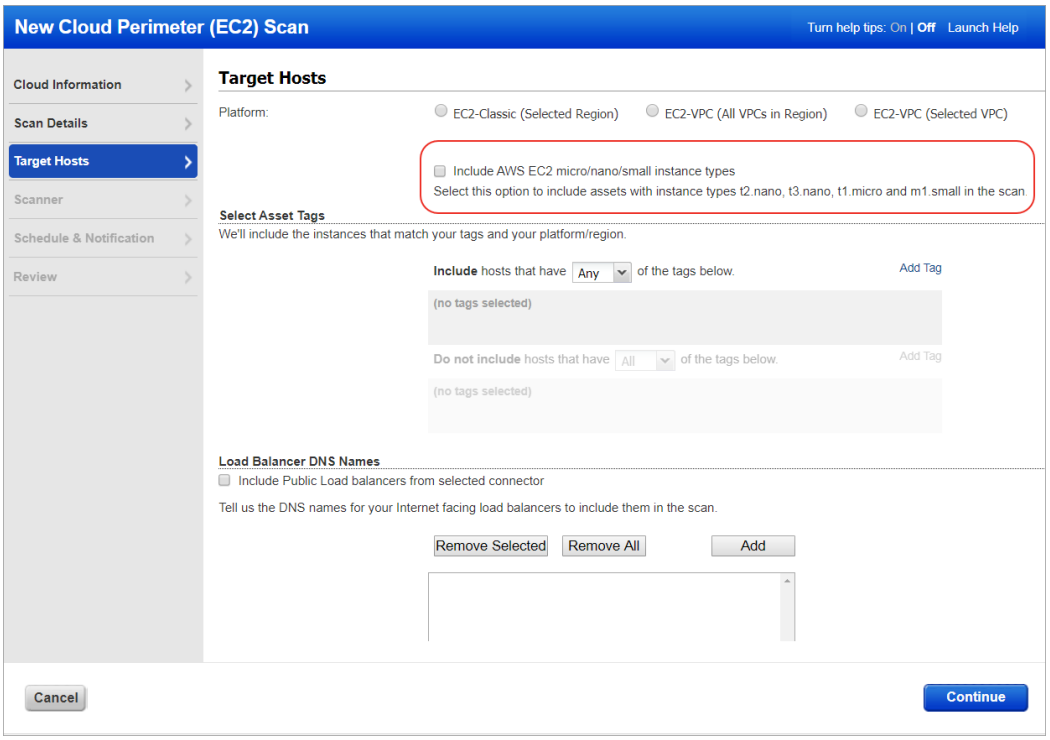
Qualys Cloud Platform

Include or Exclude Micro/Nano/Small EC2 Instances in Cloud Perimeter Scan

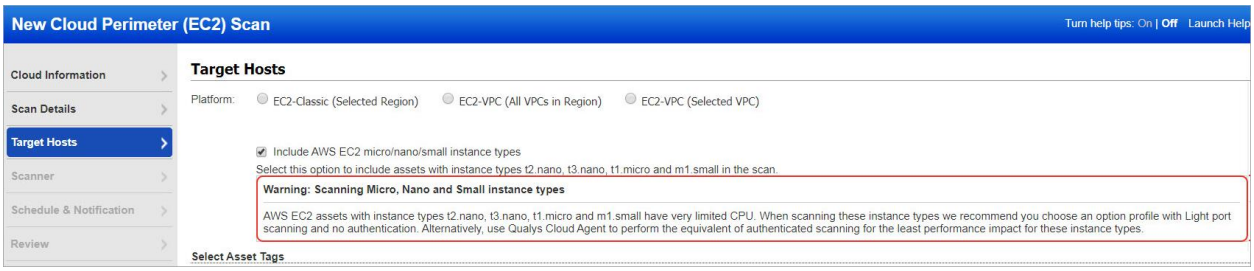
It's now possible to include EC2 assets with instance types t2.nano, t3.nano, t1.micro and m1.small when creating a Cloud Perimeter scan job for EC2 instances.

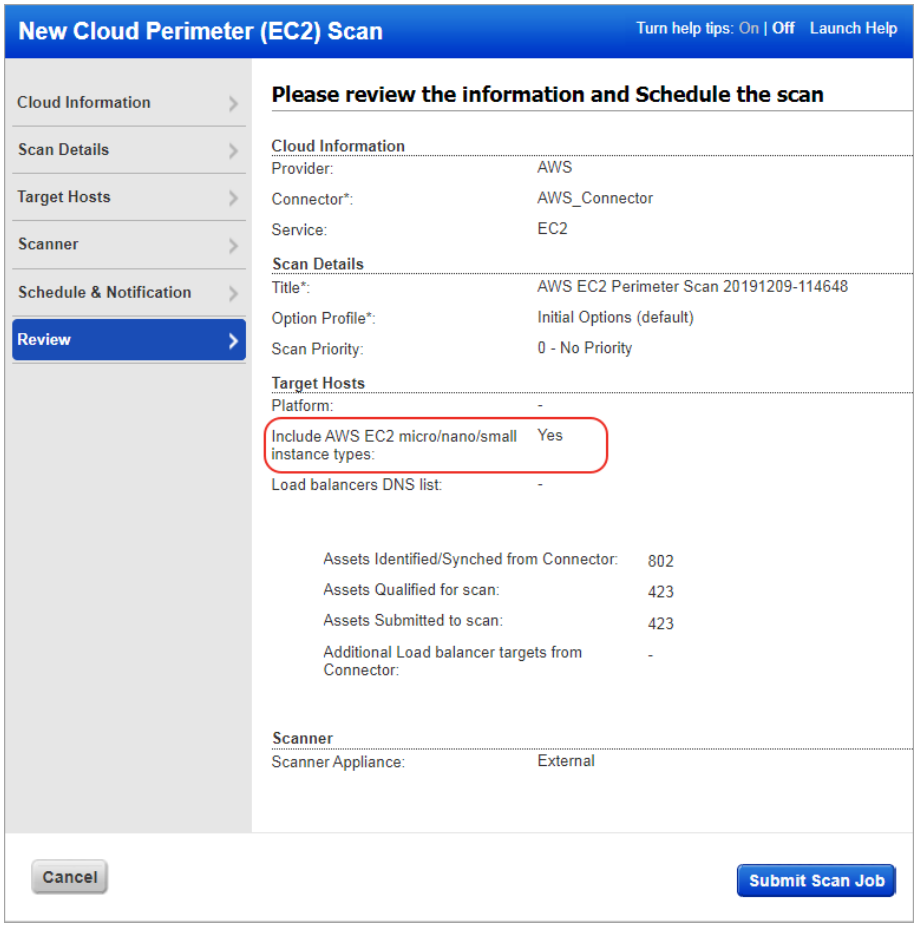
Note - This option is only available if micro, nano and small instance types are activated for your account. You'll see these changes in your account only when available on your platform. Please reach out to Qualys Support if you need more information.

To support this option, we added an optional check box field " Include AWS EC2 micro/nano/small instance types" on the Scans > Scans > Cloud Perimeter Scan > Target Hosts screen.



Select the checkbox to include these instances in the scan job. When you select the checkbox, we show a warning message recommending you to perform no authentication, light port scanning for these instances.

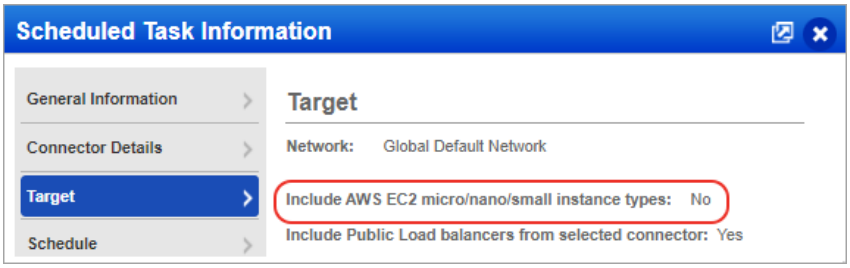




On the Scans > Scans > Cloud Perimeter Scan > Review screen, we added a field " Include AWS EC2 micro/nano/small instance types" in the Review tab to show your selection for the checkbox.

The “Assets qualified for scan” and “Assets submitted to scan” will now show counts depending on whether you have chosen to include or exclude the micro/nano/small instances.

You will also see your selection choice for including the micro/nano/small instances in the Target tab when viewing the scheduled cloud perimeter scan from Quick Actions menu.

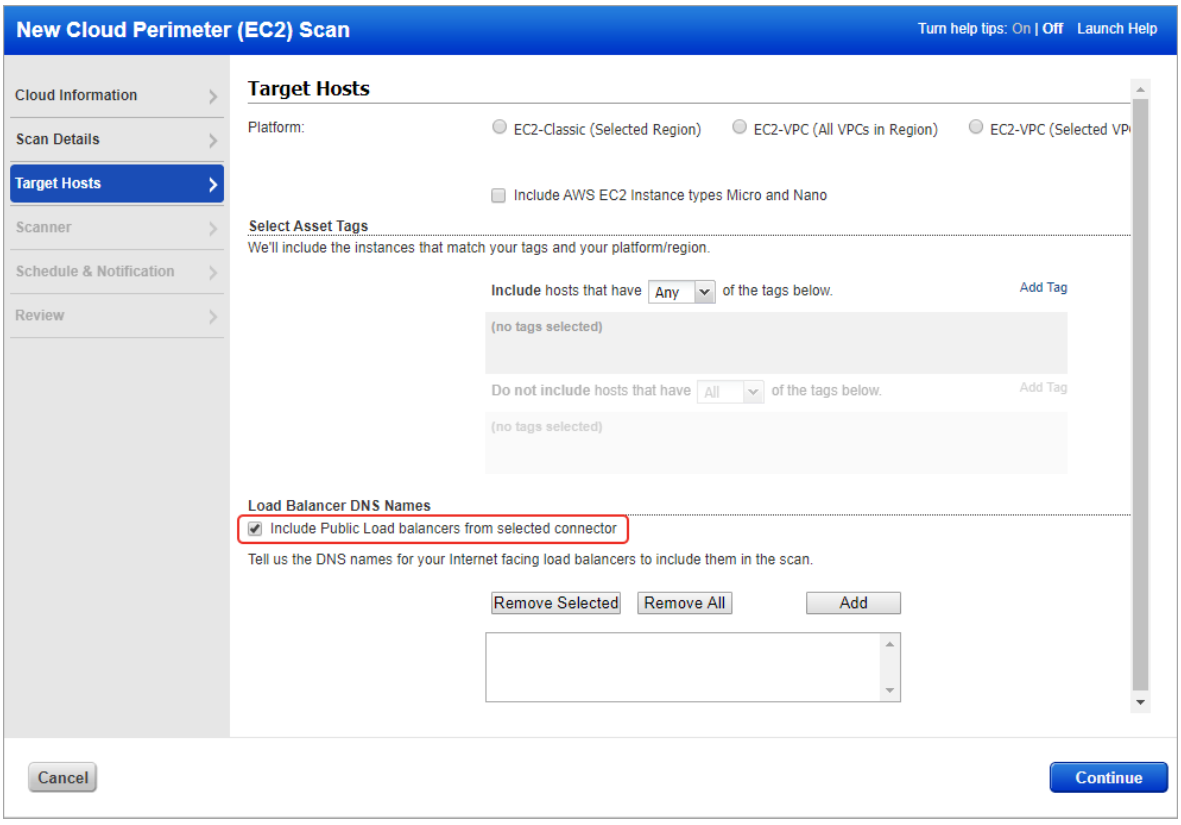


Include or Exclude Public Load Balancers from Selected Connectors in Cloud Perimeter Scan

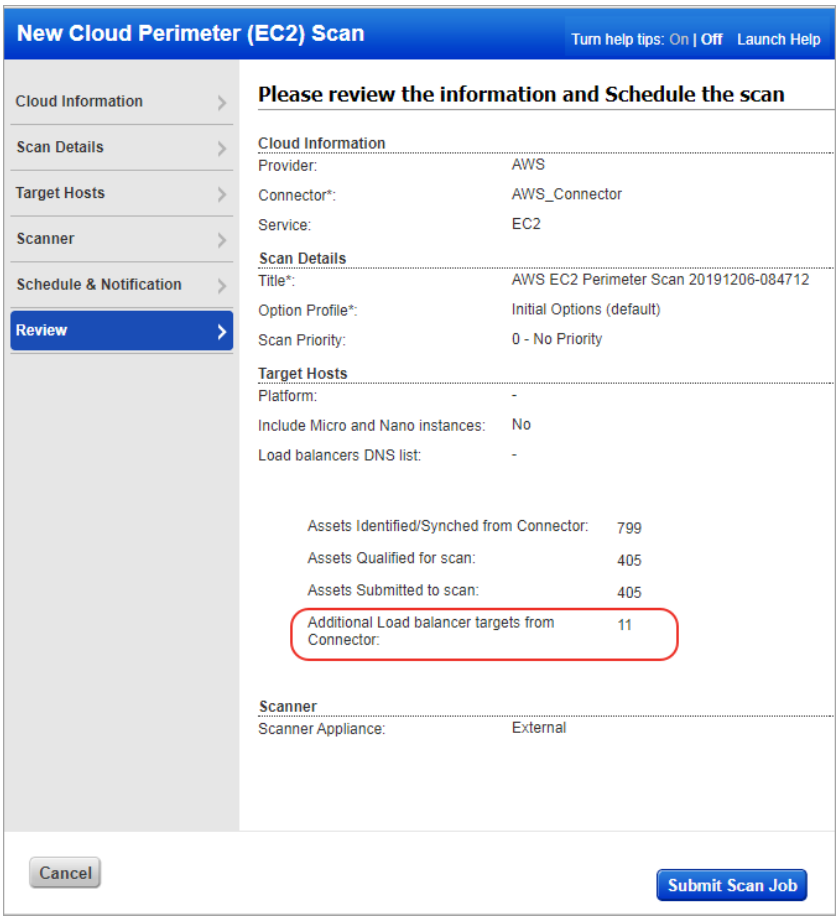
You can now choose to include or exclude public load balancers from the selected connector in the Cloud Perimeter Scan job. To support this option, we added an optional check box field "Include Public Load balancers from selected connector" on the "Scans > Scans > Cloud Perimeter Scan > Target Hosts" screen.

Note - This option is available only if your account has CloudView subscription and your platform has access to CloudView base URL "qweb_cloud_view_base_url". Please reach out to Qualys Support if you need more information.

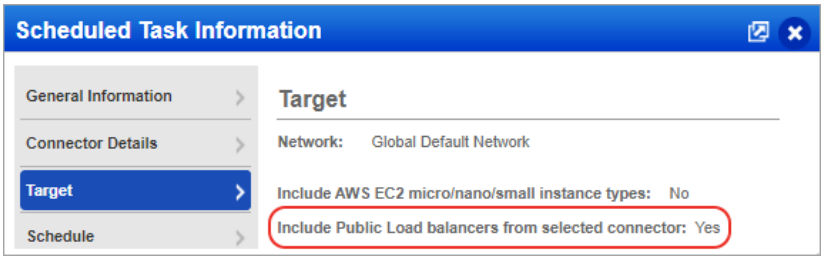
Select this checkbox to include public load balancers from the selected connector. By default, this check box is not selected. The option to add load balancer DNS names manually in the scan job is also available with this option.



On the Scans > Scans > Cloud Perimeter Scan > Review screen, we will show you the number of public load balancers discovered by the selected connector in the “Additional Load balancers targets from Connector” field in the Target Hosts section.



You will also see the selection choice for including the public load balancers in the Target tab when viewing the scheduled cloud perimeter scan from Quick Actions menu.



Qualys Vulnerability Management

Edit Action Supported for WAS QIDs in KnowledgeBase

The previous version of the published release notes had an error when describing this feature. You can now take actions on QIDs from the Web Application Scanning and Malware Detection applications when this feature is enabled. You cannot edit WAS QIDs from Vulnerability Management. Please refer to the Cloud Platform 2.42.2 Release Notes to learn more.

Qualys Policy Compliance (PC)

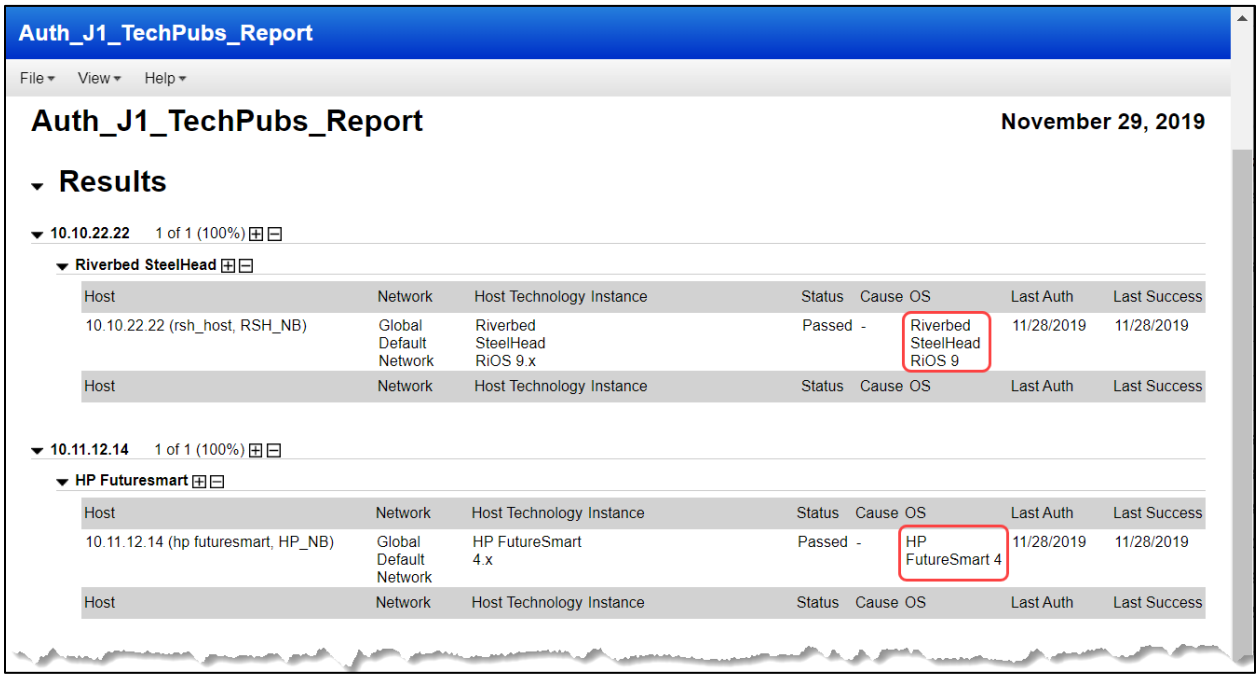
Support for New OCA Technologies

We now support the following new technologies on assets for which data is collected using Out-of-Band Configuration Assessment (OCA) tracking.

- Riverbed SteelHead RiOS
- HP Futuresmart

Simply navigate to the Reports tab and run the Policy Compliance Reports and Authentication Report on these technologies to view your compliance posture.

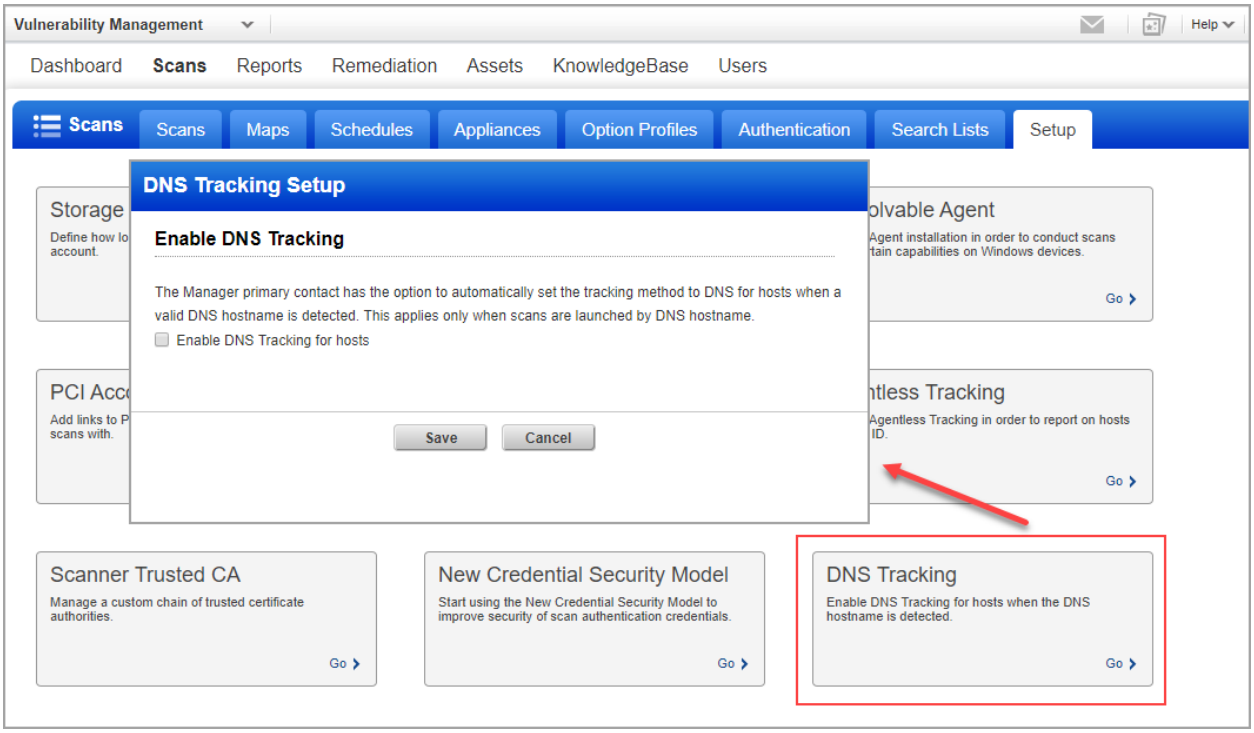
Sample: Authentication Report for Riverbed SteelHead RiOS and HP Futuresmart



DNS Tracking Support

Now you can automatically set the tracking method to DNS for hosts when a valid DNS hostname is detected at scan time. This option applies only when scans are launched by DNS hostname.

The new setting "DNS Tracking" appears under Scans > Setup. The Manager primary contact for the subscription can choose the "Enable DNS Tracking for hosts" option in the Setup page to enable this scan feature. Then hosts with a valid DNS hostname detected at scan time will be tracked by DNS.

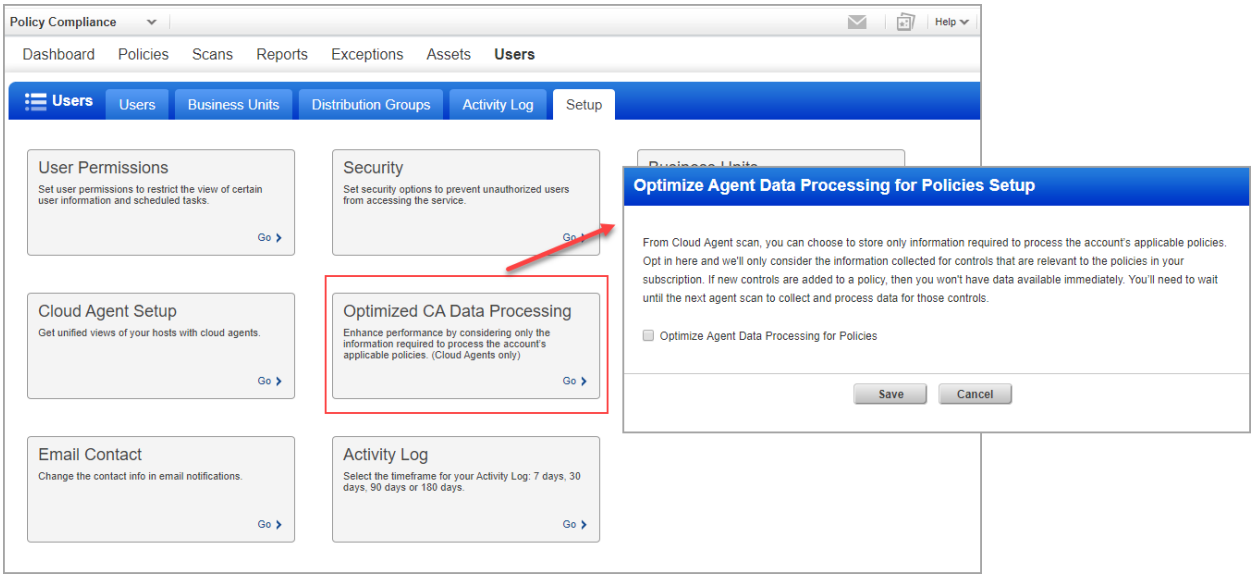


Note – If you want to enable an option to track all assets by DNS if valid hostnames are found, contact Qualys Support.

Optimized Cloud Agent Data Processing

You can now optimize and enhance performance of the cloud agent data by choosing to consider only the information required to process the account's applicable policies.

Simply navigate to Users > Setup > Optimized CA Data Processing and enable the option Optimize Agent Data Processing for Policies.



Once enabled, we will store only the information from the cloud agent scan that is required to process the account's applicable policies. That means, only the information collected for controls that are relevant to the policies in your subscription is considered.

However, if new controls are added to a policy, then you won't have data available immediately. You'll need to wait until the next agent scan to collect and process data for those controls.

Issues Addressed

- We fixed an issue on the Host Information page that displayed zero count for fixed vulnerabilities.
- We fixed an issue where the user found that PC scans scheduled for a policy that has asset tags were not running accurately. This issue occurred because asset tags were getting removed by PC from these policies. Now the asset tags are not removed and host assets in asset tags are getting scanned as expected.
- We are now able to render text from <ERR> tag for policy reports in HTML and PDF formats.
- We fixed an issue where a user with the Unit Manager role was getting permission error on selecting the "View All" option while viewing EC2 Scan Results.
- We fixed an issue where when the user was re-saving or deleting a scheduled compliance policy report, the asset tags associated with the policy were getting deleted from the policy. This issue was observed if the target type was "All Assets" and the policy specified for the report had asset tags.
- We fixed an issue where incorrect control count was shown on the Host Information page. Now, we have excluded the inactive controls to show the correct control count.
- We fixed an issue where all database records were pulled and not as per authentication records. After fix, database records are pulled as per authentication records.
- We fixed an issue where leading zero was not retaining for External ID field.
- We are now updating the evaluation date in reports even if the value of the compliance data was observed to be unchanged during latest scan.
- We fixed an issue where the count for Asset Groups from UI was not matching with the count returned by asset group list API. The reason for the mismatch was due to deleted asset groups being included in the API count. We have now added a check for the deleted asset group in the asset group list API to show only the asset group which are not deleted.
- Asset Tag names were getting truncated in csv and pdf reports. We have now fixed this issue and tag names are displayed correctly.
- Added validation in UDC for max length of 4000 characters to File Name Include, File Name Exclude, Directory Name Include, and Directory Name Exclude fields.
- We fixed an issue where compliance report for Mozilla Firefox technology was generated as blank report.
- We fixed an issue where compliance report for Google Chrome (Windows) technology was generated as blank report.
- We fixed an issue where test evaluation gave incorrect results when the IP was provided manually.
- We have now increased the timeout duration to 15 minutes so that even tags with a larger number of assets associated with them load appropriately.
- We fixed an issue for unprocessed PC scans and it is processed successfully after fix.
- We updated the online help to explain that the map duration that appears in the Map Summary email notification is greater than the duration that appears in the UI because it includes results uploading and processing time.
- We updated the online help for VM scan report templates to explain that the Status filters only apply when Host Based Findings is also selected in the template.
- We added a new setup guide for MariaDB authentication. You can download it from within the online help or from Help > Resources.