Qualys Cloud Platform (VM, PC) 10.x

Release Notes

Version 10.21

December 15, 2022

What's New

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

Qualys Cloud Platform

Enhanced Accessibility of Scan Best Practices & Troubleshooting

Scanner Appliance Syslog Forwarding

API Changes

Refer to the Cloud Platform 10.21 API Release Notes for API changes in this release.

Qualys 10.21 brings you many more improvements and updates! Learn more

Enhanced Accessibility of Scan Best Practices & Troubleshooting

We have now made information on best practices for scans and troubleshooting scans easily available. To ease the accessibility of the information, we have introduced:

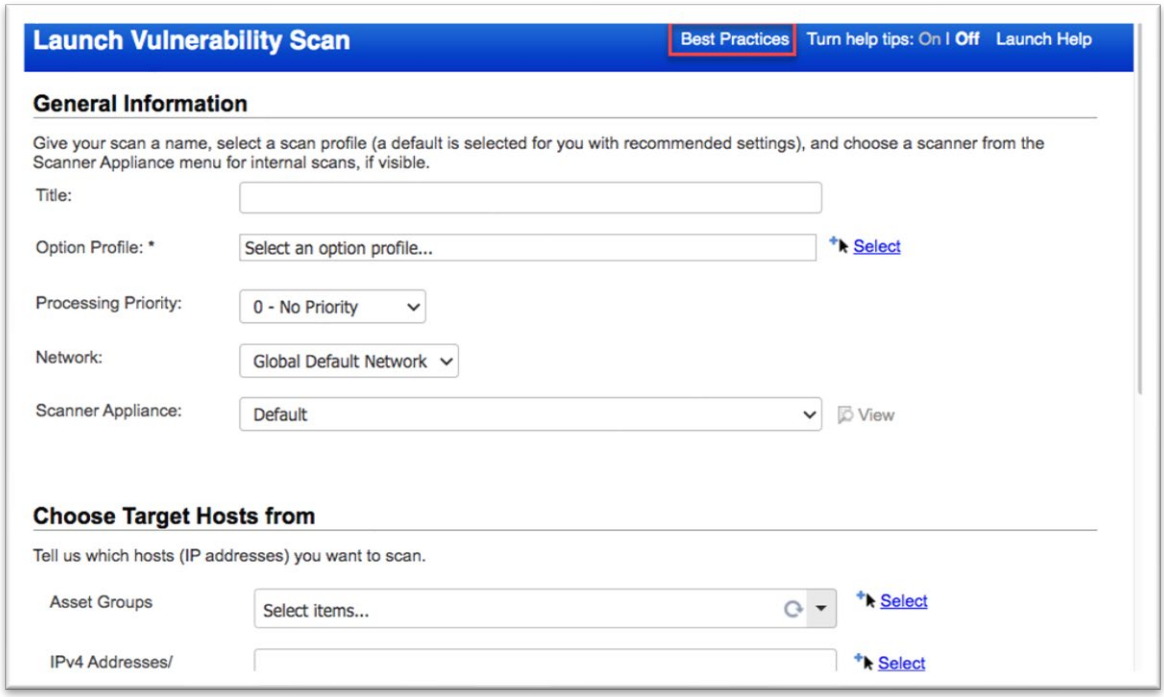
- a **Best Practices** link for **VM and PC/SCA scan**
- a **Scan Troubleshooting** link for **VM scan**

Use these links to quickly glance through recommendations on optimal scanning or find quick resolutions to some of the issues you may encounter when scanning.

Best Practices for VM and PC/SCA scan

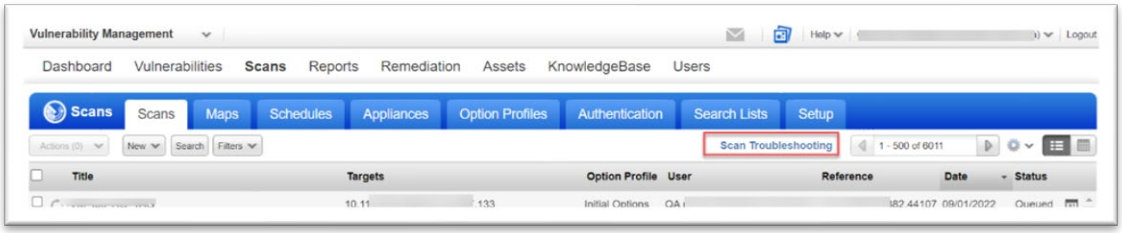
The **Best Practices** link is available when you launch any type of vulnerability scan, including regular vulnerability scans, cloud perimeter scans, and EC2 scans. The link opens an article with topics around scanning, including the events that take place during a scan job, how scanners work, the scanner capacity/sizing, and other recommendations. Use this link to optimize your scanning experience.

A link with similar information is also available for PC/SCA scans.



Scan Troubleshooting for VM scans

On the VM Scans tab, we now have a **Scan Troubleshooting** link that offers solutions to some of the common scan issues. When running scans, if you run into issues, use the information on this link to self-resolve the issues.



Scanner Appliance Syslog Forwarding

Now, you can automatically have scan related syslog messages (/var/log/messages syslog stream) forwarded from your scanner appliances to a remote syslog server that you define. This feature can be enabled for the subscription by any Manager user. Once enabled, syslog forwarding is turned on for all scanner appliances (virtual and physical) that are currently in the subscription and also for new scanners that get added later.

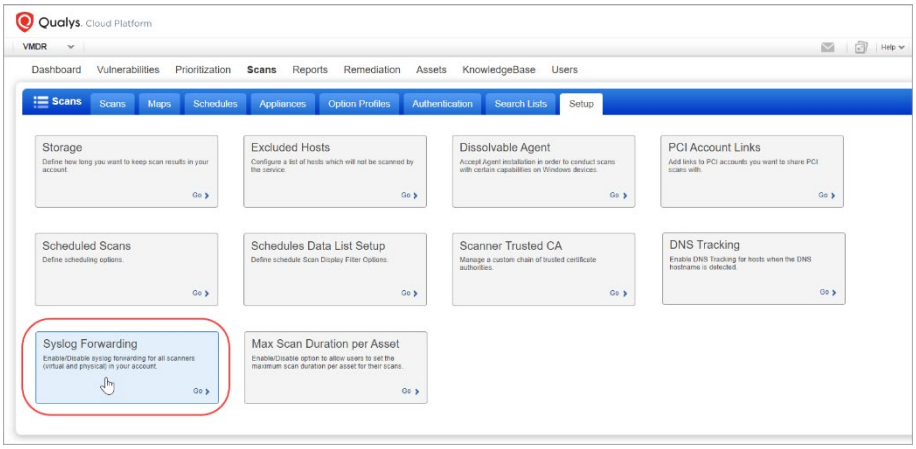
Prerequisites

- The remote syslog server you configure must be reachable from the scanner's LAN, native VLAN or WAN gateways.
- You must be a Manager user to enable Syslog Forwarding.

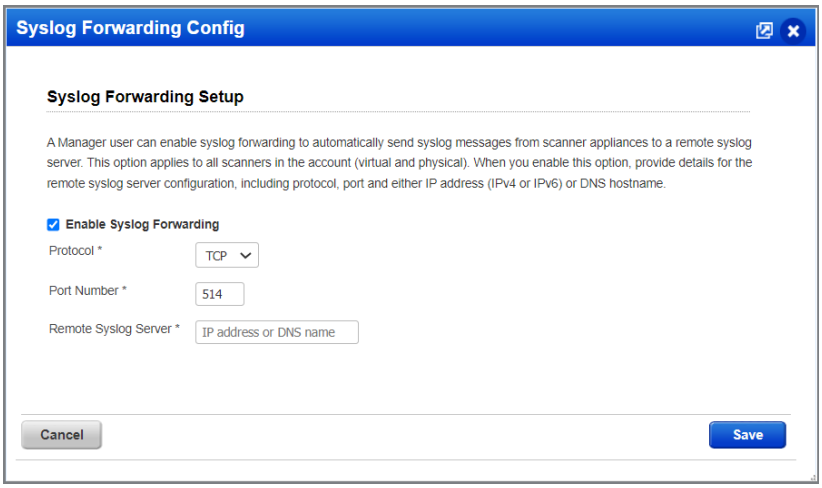
How to Enable Syslog Forwarding

Follow these steps to enable syslog forwarding:

1) Go to **Scans** > **Setup** > **Syslog Forwarding**.



2) Select the option **Enable Syslog Forwarding** and provide details for the remote syslog server, including the protocol (TCP or UDP), port number (default is 514), and either the IP address (IPv4 or IPv6) or DNS hostname. Then hit **Save**.



Issues Addressed

- For subscriptions with AGMS enabled, we improved performance for the Scans list for all the sub-users when the "Show in Scope Scan List" option is selected.
- For subscriptions with AGMS enabled, we fixed an issue where the incorrect number of rows was shown on the Address Management tab. Now the user will see the correct number of rows based on the Rows Shown value they select for the list.
- We fixed an issue with tag creation based on QID from Asset Search. Now the tag is created with the correct tag rule.
- When updating authentication records using the API, a valid error message will now appear when an IP is being added to a record and the same IP already exists in another record of the same type for the same network (when Network Support feature is enabled).
- We fixed an issue where the Update action for Unix authentication record using the API returned an error when multiple record IDs were specified in the API request.
- We have fixed an issue where customers with AGMS-enabled accounts couldn't run the 'Update Schedule Scan API' due to an internal ORA error.
- We fixed an issue when a user edits the schedule scan report and if removes a tag, the tag does not appear in the Asset Tags section.
- We fixed an issue where a deleted user will not be the sender of email notifications for scheduled reports. When scheduling a report, you can select the group of people to whom an email notification will be sent upon report completion. If the user from which the email has to be sent is deleted before the scheduled report launch, then the email notification should not be sent from the deleted user. While deleting the user, you have the option to transfer the ownership to any other superior user. The email notification will be sent from the user to whom ownership has been transferred and not from the user who was deleted.
- We have fixed the issue where the “IP”, “Total vulnerabilities”, and “Security Risk” data was present in reports but the “IP”, "Total Vulnerabilities", "Security Risk" header was missing from all types of vulnerability reports where this header was supposed to be present.
- We have updated the description for 'Exclude superseded patches' to accurately reflect the possible QIDs that can be excluded. The prior description mentioned only OS-level QIDs could be excluded when there were exceptions. Click the 'Learn more' hyperlink to view the updated description.
- We have fixed the issue where users were unable to run a scan if they selected “Global Default Network” and “All Scanners in Network” while launching a scan from the Scan tab. The “Scanner versions are mixed” error was shown.
- When selecting a control for the Control Pass/Fail Interactive Report, we added text on the screen to inform users that they can search by multiple control IDs (CIDs) and other criteria, but only one control can be selected for the report.
- We fixed an issue where the SQL Statements in Database User Defined Controls (UDCs) were cleared in error as the result of changes to UDC technologies.
- We have fixed the issue where the **Evidence** column was blank in the Policy Compliance report (CSV format) for large evidence data. The evidence data is now correctly displayed in the report.

- We have fixed the issue where the generation of policy compliance reports in CSV format was failing due to time-out. The reports are now generated successfully.
- In the Policy Compliance **Posture** tab, the asset tag name used to get removed from the **Asset** QQL field when users performed the following actions in the given sequence:
    - On the **Dashboard** tab, applied an asset tag and navigated from a widget to the **Posture** tab for more details.
    - On the **Posture** tab, clicked **Assets** to view the asset list or applied a **Group by** filter

  This issue has been fixed and now the asset tag is retained in the Asset QQL box even if the user navigates to the Assets list or applies Group by filters.

- Fixed an issue in Policy Compliance, wherein a discrepancy was observed in the posture data displayed in the Policy Editor and the enhanced PC user interface.

- We fixed an issue where the "Cause of Failure" is visible in Policy Compliance reports in CSV format when the users re-enable the Policy Compliance Report Service. The "Cause of Failure" is now visible in both PDF and CSV report formats and the users now do not need to disable the Policy Compliance Report Service every time.

- We fixed the behavior of PosturStreamingAPI output when the user changes the criticality label name from policy setup. Users are now able to see the correct criticality label names in JSON and XML reports.