



Qualys Cloud Platform (VM, PC) 10.x

Release Notes

Version 10.23

July 14, 2023

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

Qualys Cloud Platform

User-Specific Session Timeout

Allow Administrator User to Create Another Administrator User

Enhanced Validation: Unique Email ID while Creating or Editing Users

Qualys Vulnerability Management (VM)

Search for Scans using NetBIOS/DNS/FQDN/Cloud Instance

Show Unique Hosts Scanned in the Last 90 Days

Support for Active OT Scanning

Asset Risk Score (ARS) Renamed TruRisk Score in Scan Reports

Enhancements Related to Subscription Activation

Qualys Policy Compliance (PC/SCAP/SCA)

Support for New Technologies for UDCs

Support for New Authentication Technologies

Support for Red Hat OpenShift Container Platform 4.x on CoreOS Agent

API Changes

Refer to the [Cloud Platform 10.23 API Release Notes](#) for API changes in this release.

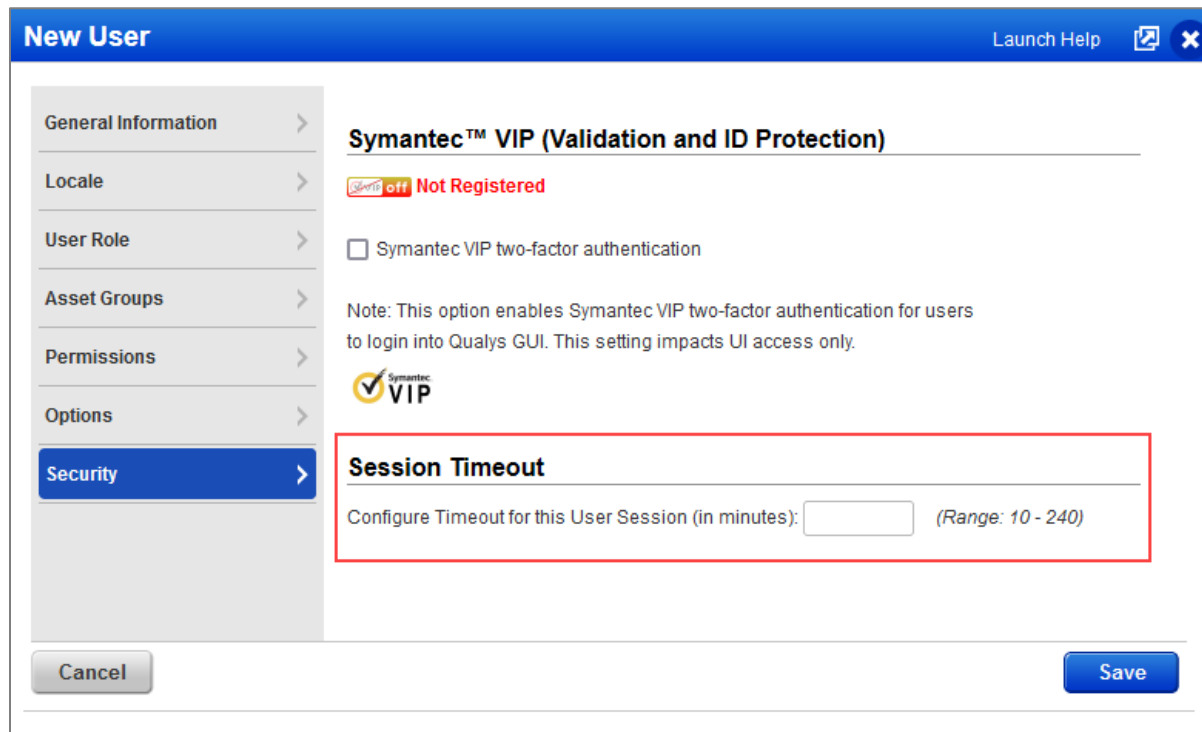
Qualys 10.23 brings you many more improvements and updates! [Learn more](#)

What's New?

User-Specific Session Timeout

Manager users can now define session timeout for individual users, allowing a more granular level of control over user access. When creating or editing a user, navigate to the **Security** section and set the required session timeout for that specific user.

Note that this user-specific timeout takes precedence over the role-based timeout.



The screenshot shows the 'New User' configuration window. On the left is a sidebar with tabs: General Information, Locale, User Role, Asset Groups, Permissions, Options, and Security (which is selected and highlighted in blue). The main content area is titled 'Symantec™ VIP (Validation and ID Protection)'. It contains a status indicator 'Not Registered' with a red 'off' button, a checkbox for 'Symantec VIP two-factor authentication' (which is unchecked), and a note: 'Note: This option enables Symantec VIP two-factor authentication for users to login into Qualys GUI. This setting impacts UI access only.' Below this is the Symantec VIP logo. A red rectangular box highlights the 'Session Timeout' section, which includes the text 'Configure Timeout for this User Session (in minutes):' followed by an input field and the range '(Range: 10 - 240)'. At the bottom of the window are 'Cancel' and 'Save' buttons.

Allow Administrator User to Create Another Administrator User

With this release, an administrator user can create another administrator user. The email ID assigned to the new user must be distinct from the email ID currently associated with the existing administrator user.

This feature is not activated by default. Contact Qualys Support or your technical account manager to activate this feature for your subscription.

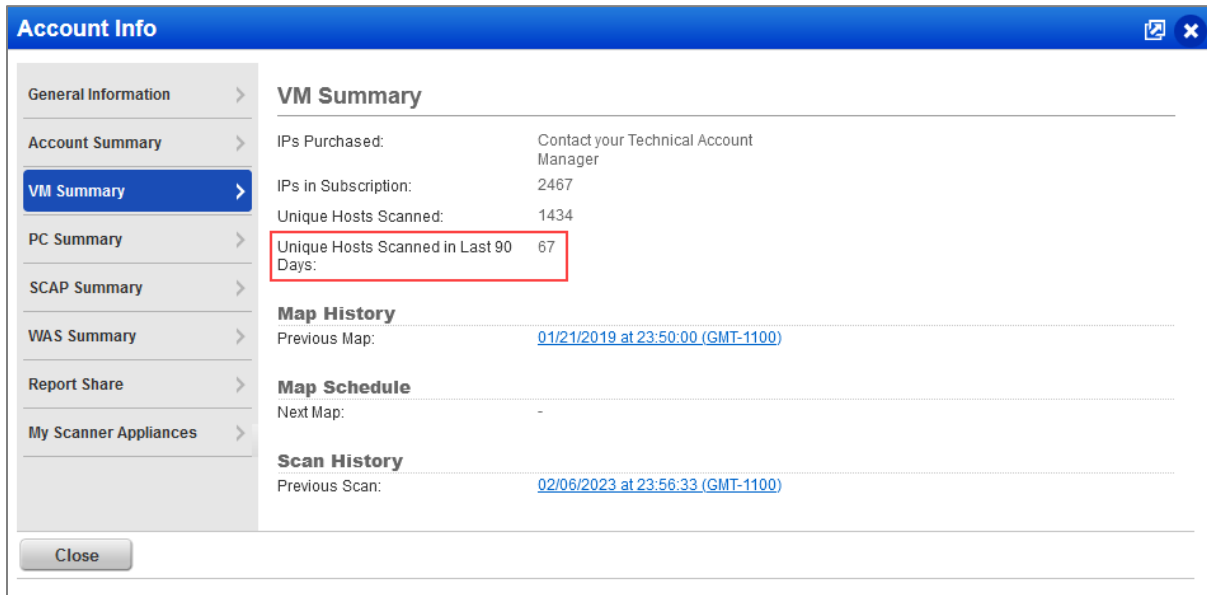
Enhanced Validation: Unique Email ID while Creating or Editing Users

While creating or editing a user, a new validation check is now added to ensure that a unique email ID is used for each user. If the specified email ID is already associated with another user, an error message is displayed to prompt you to provide a different email ID.

This feature is not activated by default. Contact Qualys Support or your technical account manager to activate this feature for your subscription.

Show Unique Hosts Scanned in the Last 90 Days

You can now view the unique hosts scanned for vulnerabilities in the last 90 days. Navigate to **Help > Account Info > VM Summary** to view the details.



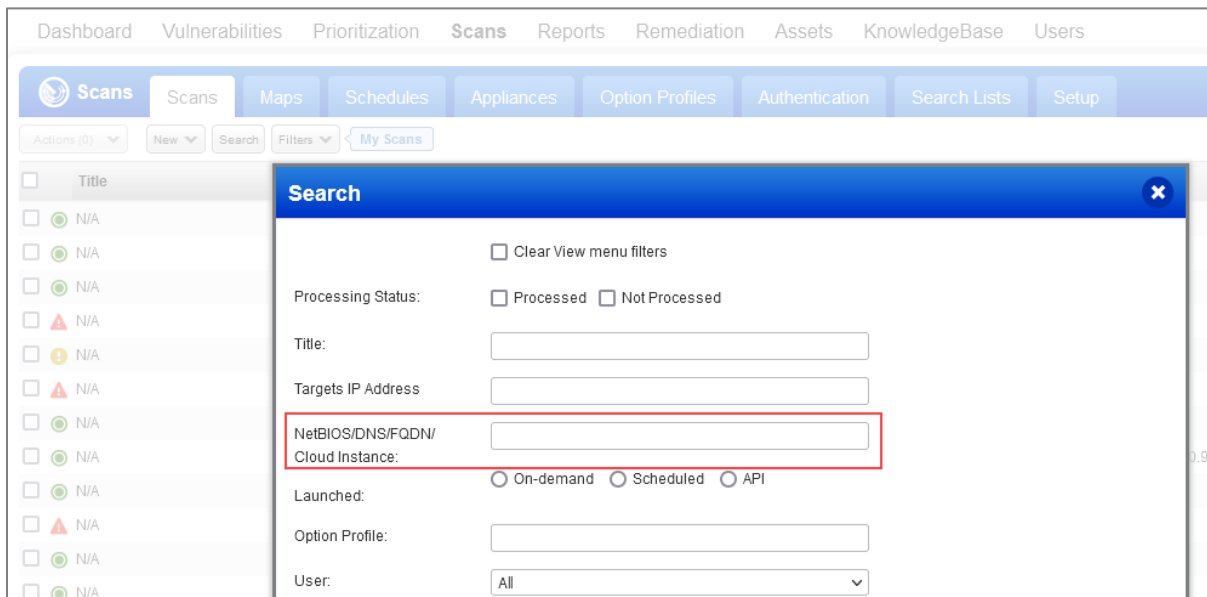
The screenshot shows the 'Account Info' window with the 'VM Summary' tab selected. The left sidebar contains a list of summary tabs: General Information, Account Summary, VM Summary (highlighted), PC Summary, SCAP Summary, WAS Summary, Report Share, and My Scanner Appliances. The main content area displays the following information:

- VM Summary**
 - IPs Purchased: Contact your Technical Account Manager
 - IPs in Subscription: 2467
 - Unique Hosts Scanned: 1434
 - Unique Hosts Scanned in Last 90 Days: 67 (highlighted with a red box)
- Map History**
 - Previous Map: [01/21/2019 at 23:50:00 \(GMT-1100\)](#)
- Map Schedule**
 - Next Map: -
- Scan History**
 - Previous Scan: [02/06/2023 at 23:56:33 \(GMT-1100\)](#)

A 'Close' button is located at the bottom left of the window.

Search for Scans using NetBIOS/DNS/FQDN/Cloud Instance

With this release, you can now search for scans using NetBIOS, DNS, FQDN, or Cloud Instance. Previously, you could search for a scan by using only IP addresses.



The screenshot shows the 'Scans' section of the application. The top navigation bar includes: Dashboard, Vulnerabilities, Prioritization, Scans (active), Reports, Remediation, Assets, KnowledgeBase, and Users. Below this is a sub-navigation bar with: Scans (active), Maps, Schedules, Appliances, Option Profiles, Authentication, Search Lists, and Setup. The main interface has a left sidebar with a list of scan entries, each with a checkbox and a status icon (green circle for 'N/A', red triangle for 'N/A', yellow circle for 'N/A'). The main content area is titled 'Search' and contains the following search criteria:

- ☐ Clear View menu filters
- Processing Status: ☐ Processed ☐ Not Processed
- Title:
- Targets IP Address:
- NetBIOS/DNS/FQDN/Cloud Instance: (highlighted with a red box)
- Launched: ☐ On-demand ☐ Scheduled ☐ API
- Option Profile:
- User:

Support for Active OT Scanning

With this release, OT device scans are now supported for Asset Group Management Service (AGMS) enabled accounts. You can launch OT device scans and get up-to-date views on your OT assets and security posture using Qualys VMDR OT. For more details, refer to VM/VMDR Online help: [Start OT Device Scans](#).

Asset Risk Score (ARS) Renamed TruRisk Score in Scan Reports

With this release, the ARS (Asset Risk Score) related fields in scan reports and report templates are renamed to replace ARS with TruRisk Score.

The following changes are made:

- The **ARS** column in the vulnerability report is renamed **TruRisk Score**.
- The **TruRisk Details (ARS, ACS, QDS)** option in the **Display** tab of the scan report template is renamed **TruRisk Details (TruRisk Score, ACS, QDS)**.

Important: The old columns with ARS will be retained in scan reports for the next few releases. However, there will be a future update where these columns will be removed with advance notification.

Enhancements Related to Subscription Activation

The email notification for subscription activation is now improved to enhance the user experience. Additionally, the OTP included in the email now remains valid for 72 hours, compared to its previous validity of only 30 minutes.

Support for New Technologies for UDCs

With this release, UDCs are now supported for the following new technologies on Scanner and Agent:

Technology	Supported for Agent and Scanner	Supported only for Agent
Mac OS X 10.15, 11.x, 12.x, and 13.x	-	<ul style="list-style-type: none">• File/Directory Existence• File/Directory Permission• File Content Check• File Integrity Check• Unix Directory Search Check• File Content Check
Rocky Linux 8.x/9.x Alma Linux 8.x/9.x	<ul style="list-style-type: none">• File/Directory Existence• File/Directory Permission• File Content Check• File Integrity Check• Directory Search Check• Directory Integrity Check• Script Execution	-

Support for New Authentication Technologies

With this release, the following technologies are now supported for Policy Compliance authenticated scans using scanners:

- Oracle 21c (Multitenant)
- NetApp Data ONTAP 9.x
Note: NetApp Data ONTAP 9.x is supported only for share access-related controls. It is recommended to perform a full scan instead of a policy-specific scan that includes only the supported controls.
- Cisco Firepower Threat Defense (Cisco FTD 6.x & 7.x)
- Cisco ISE 2.x/3.x
- Microsoft SQL Server 2022 (Supported on Windows and Linux)
- ArubaOS Switch 16.x
- ArubaOS CX 10.x
- VMware Photon OS 4.x
- Amazon Linux 2023

For more information, see [Authentication Technologies Matrix](#).

Support for Red Hat OpenShift Container Platform 4.x on CoreOS Agent

The support for middleware technologies is extended to include Red Hat OpenShift Container Platform 4.x for Linux CoreOS Agent.

For more information, see [Middleware Technologies Auto-discovered by Cloud Agents for PC](#).

Issues Addressed

The following issues are fixed with this release:

- We have fixed the issue where QIDs were mistakenly associated with certain CVEs, falsely indicating the presence of a weaponized exploit when no such exploit was actually available. With this release, we have removed the references to the incorrect CVEs. For the list of QIDs that were fixed, refer to [QIDs Fixed to Remove Incorrect Exploit References](#).
- We have fixed an issue where users were redirected to the Vulnerability Management application on selecting the SCA application on the home page.
- We have fixed an issue where the Policy List API was returning error code 999.
- We have fixed the policy processing issue where policy evaluation was getting stuck.
- We have fixed an issue where the tags information was not included in the Compliance Scan result PDF.
- We have fixed an issue where the Host Detection API did not respond even after 10 hours. With this release, if no response is achieved within 4 hours, the API gets aborted. Contact your technical account manager or Qualys Support to change the default execution time, as per your requirement. The default time is 4 hours.
- We have fixed an issue where the Dynamic Search list filters, **Exploitability** and **Authentication Type**, got reset upon saving or reopening the search list. This issue occurred due to selecting a large set of exploitability. To fix this, we increased the character limit for these filters to 4000 for Exploitability and 500 for Authentication Type. Additionally, an error message is now displayed to notify you when you exceed the maximum character limit.
- We have fixed an issue where users did not receive EC2 metadata when making an API call to scan using the Windows EC2 Cloud Agent. All reports in CSV, PDF, HTML, and XML formats now include the EC2 metadata.
- We have fixed an issue where the details page of the VMWare ESXi Authentication record with VCenter Authentication displayed “Not Attempted” for all hosts, despite authentication being successful. The users can now view authentication data in scans and VMWare ESXi Authentication records.
- We have fixed an issue where users while adding the IP from MAP scan results to an asset group did not get the message stating "The IP addresses listed below are not currently in this account and thus not available for processing. You may add them to the account or cancel the action and try again." Now, the message is displayed properly.
- We have fixed an issue where the report for Cloud Agents got stuck and failed to complete at 13%.
- We have fixed an issue where users were able to run API calls even after deactivating their API access.
- We have fixed an issue where the QDS score and severity were not available in the CSV report but were visible in the XML report.
- We have fixed an issue where no remediation tickets were generated after a scan, even though the correct parameters were set.
- We have fixed an issue where users were unable to launch OT scan on IPs.
- We have fixed an issue where users faced a problem with IP network scanned assets that have tracking method QAgent. It did not export any of the user-defined fields when selecting **Export All** from Address Management.

- We have fixed an issue where activity logs intermittently showed the Unit Manager as the Manager.
- We have fixed an issue where reports got interrupted and errored due to UTF-8-incompatible special characters.