Qualys Cloud Platform (VM, PC) 10.x

Release Notes

Version 10.24

October 06, 2023

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

What's New

Qualys Vulnerability Management (VM)

Partial SSL/TLS Auditing

Support for Private Key Format, PKCS8

Additional Information in Scan Results

Increased Data Retention Period for PCI Scan Results

Qualys Policy Compliance (PC/SCAP/SCA)

Support for New Authentication Technologies

New Authentication Records

Qualys 10.24 brings you many more improvements and updates! Learn more

Partial SSL/TLS Auditing

With this release, you can partially scan SSL/TLS endpoints with an incomplete handshake. An incomplete handshake occurs when SSL/TLS endpoints require client certificates to complete SSL/TLS handshake. Only a limited set of QIDs is checked in this mode and any QIDs that are typically reported as confirmed vulnerabilities are now reported as potential vulnerabilities. Due to this enhancement, the following changes have been made:

- A new scan setting, **Perform Partial SSL/TLS Auditing**:
    1. Navigate to **Scans**> **Option Profiles**>**New Option Profile**>**Scan**.
    2. Select or deselect the **Enable partial SSL/TLS auditing** checkbox to enable or disable partial auditing of SSL/TLS endpoints with an incomplete handshake.

- Modified the following APIs. For more information, refer to Cloud Platform 10.24 API release notes and notifications.
    - Option Profile Export
    - Option Profile Import
    - Create VM Option Profile
    - Update VM Option Profile

Added Support for Private Key Format, PKCS8

You can now create/edit Unix and Network SSH authentication records in FIPS mode with private keys in PKCS8 format. The support for PKCS8 private key format has been added to resolve validation errors while creating or editing authentication records with private keys in FIPS mode.

When you create or edit authentication records, select the newly added PKCS8 option from the **Private Key Type** list (**Private Keys/Certificates** tab> **Add Private Key Certificate**> **Private Key Type** list).

Additional Information in Scan Results

To enhance the user experience, the following links to the troubleshooting articles have been added to the scan results page for the VM scans with no host alive:

- https://success.qualys.com/support/s/article/000002839
- https://success.qualys.com/support/s/article/000006204

Increased Data Retention Period for PCI Scan Results

PCI-DSS ASV Program Guide 3.0 recommends storing PCI scan results for three years. Previously, this retention period was of two years. To align with this, Qualys VM/VMDR now stores PCI scan results for three years from the date of scan launch.

Support for New Authentication Technologies

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

- Mongo DB 6.x
- PostgreSQL 15.x

For more information, see Authentication Technologies Matrix.

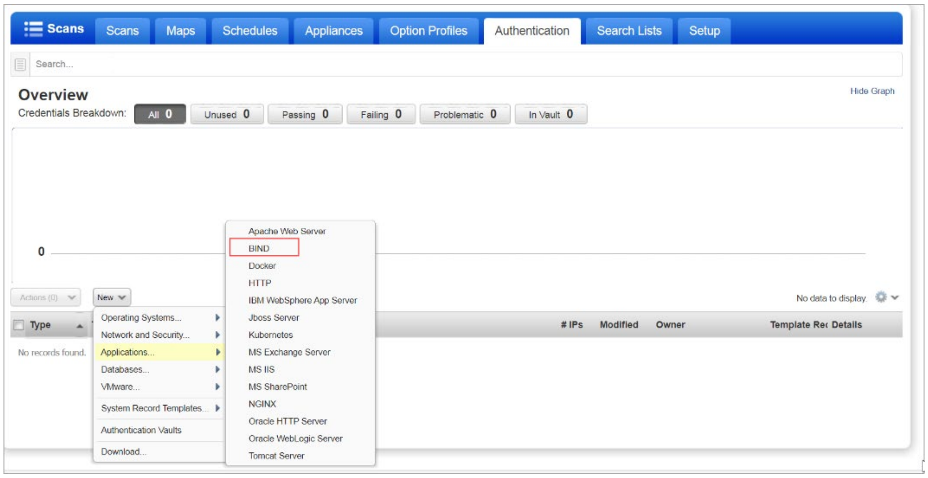
New Authentication Records

With this release, the following Authentication Records are now supported for Policy Compliance authenticated scans:
The record types are only available in accounts with PC/SCA module and are only supported for compliance scans.

- DNS BIND

  Berkeley Internet Name Domain (BIND) is the most popular Domain Name System (DNS) server in use today and responsible for performing domain-name-to-IP conversion on Linux-based DNS servers. The BIND package provides the named service. It reads the configuration from the /etc/named and /etc/named. conf files.

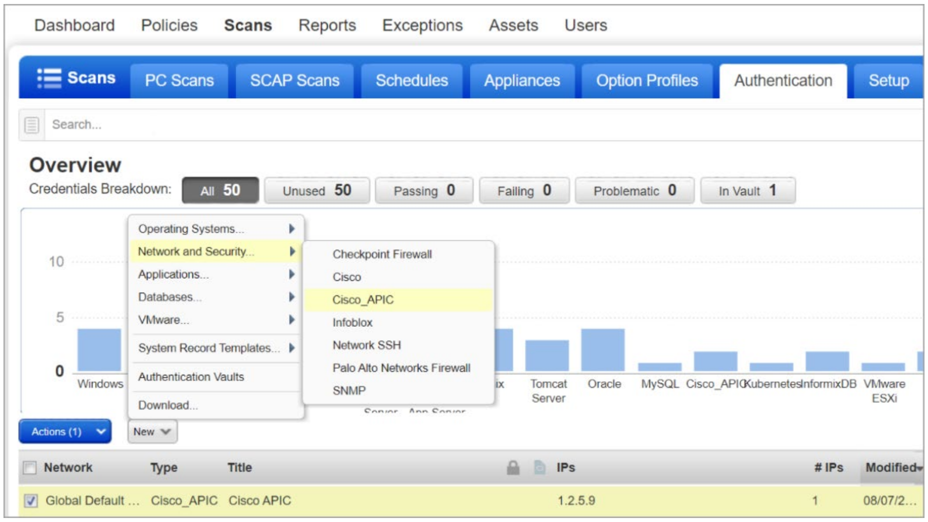
  To create a DNS BIND authentication record, go to **Scans** > **Authentication** > **New** > **Applications** > **BIND**.



- Cisco_APIC

  The Cisco Application Policy Infrastructure Controller (Cisco_APIC) is the main architectural component of the Cisco ACI solution. It is the unified point of automation and management for the Cisco ACI fabric, policy enforcement, and health monitoring. The controller optimizes performance, manages, and operates a scalable multitenant Cisco ACI fabric.

  To create a Cisco_APIC authentication record, go to **Scans** > **Authentication** > **New** > **Network and Security** > **Cisco_APIC**.



☐ Network	Type	Title	IPs	# IPs	Modified
☑ Global Default ...	Cisco_APIC	Cisco APIC	1.2.5.9	1	08/07/2...

Issues Addressed

The following issues are fixed with this release:

- The QDS factors were not available in the CSV report but were visible in the XML report.
- The host-based scan report displays source information for non-ETM-enabled subscriptions. Now, the source information is visible only to ETM-enabled subscriptions.
- The user was unable to create or update vCenter authentication record due to an error encountered while saving the authentication record.
- The vulnerabilities on dead hosts were not closed after scan completion due to an error during scan processing.
- There was a mismatch between the activity logs displayed in the VMDR module and the Administration module.
- When a user with access only to the KnowledgeBase tried to use the host list detection API, a response code of 999 with an Incident signature was generated. However, we have updated the error message to be more user-friendly and informative.
  The following message will be displayed instead of the incident signature.
  "Your permissions or account settings do not allow you to access this API."
- The Policy Summary tab encountered an error and did not show a dashboard view of the compliance status for the selected policy.
- The asset tags were not applied consistently when <DNS_HOSTNAME> and <FQDN> tags were present for Cloud Agent.
- Users were unable to add/remove IPs from the Unix authentication record due to an error encountered while adding or removing IPs.
- There was a mismatch between the number of scans listed on the Scans tab (VM>Scans>Scans tab), and the number of scans downloaded in the Excel file.
- Users were unable to edit and save the schedule as adding and deleting asset groups from a schedule was taking longer time.
- Users were getting the wrong time zone in the policy report. Users need to set the time zone from the user profile to get the same desired time zone for both API and UI reports.
- The total host count in the VM scan summary was reflecting zero for large number of ips.
- The PCI links were not getting unlinked from the VM subscription when FO/BO user account was deleted.
- The user was unable to view the created date in the report template and scan option profile.
- Schedule scan was getting deactivated, and users were getting an error when any IP from the IP range added in the tag was not present in the subscription.

- Users were unable to import Script UDC via policy import API using Qualys Session ID and were getting an error message Control ID: Found invalid script.

- Agent IP was still visible under SCA IP scorecard report section even if the SCA module was not enabled for the same.

- Authentication Records API failed to generate a regular response and showed 999 error code in the output.

- There was a delay in receiving weekly vulnerability emails. The emails were received on Wednesday, instead of Monday.

- Preview section of PC Scans showed incorrect Total Hosts Alive count as "0" (Zero) even when a few hosts were in operation.

- Scanner Preview failed to display additional scanner information, such as its CPU, Memory, and Region, even when the Show Additional Scanner Information feature was enabled.

- When a user removed an IP address from Address Management on which a scan was running, the IP address was still visible in Asset Search Report. This is as per the design as a new host ID will be created after the completion of a scan and will be visible in a Asset Search Report.

  We have added a note on the UI and updated the Online Help to inform about this behaviour. The following message is displayed in the UI, in the **Remove IPs from Subscription** window.

  “If you remove IP of an ongoing scan, the IP may get partially removed and the asset may still appear at different places, such as in the asset search report.”

- The user encountered an incident signature while generating an Asset Search report (Reports>New>Asset Search Report) for over 4000 IPs. Now, instead of showing the incident signature, the following message is displayed:
  The string size for the IPs cannot exceed 4000 number of characters.

- The user was unable to create a CyberArk AIM authentication record with the same Application ID.