Qualys Cloud Platform (VM, PC) 10.x

Release Notes

Version 10.22
April 03, 2023

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

Qualys Policy Compliance (PC/SCAP/SCA)

New UDC Technology Support for Ubuntu 22.x and RHEL 9.x

Qualys Cloud Platform

Extended CVE Search Ability in Knowledge Base for "Exact Match" and "Contains"

Automated Debug Scan for VM Internal Scanner

Qualys 10.22 brings you many more improvements and updates! Learn more

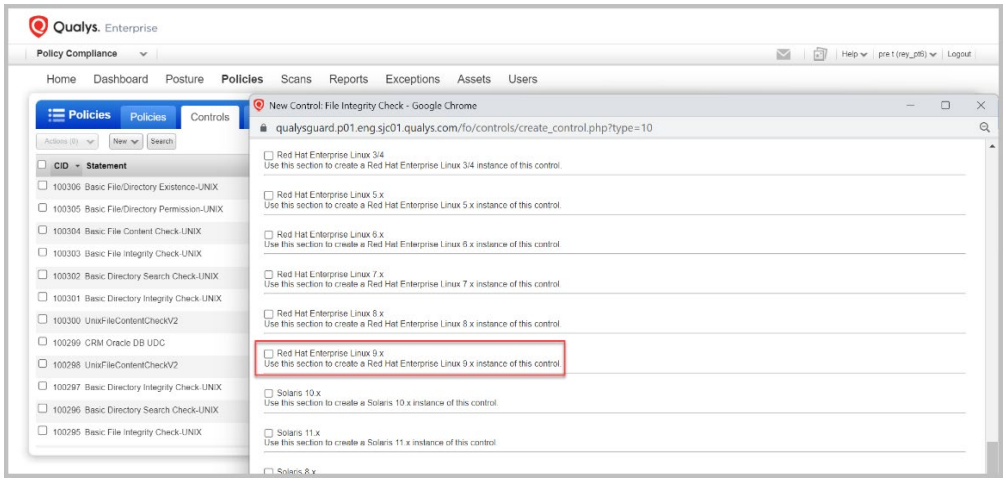
New UDC Technology Support for Ubuntu 22.x and RHEL 9.x

This release introduces new User Defined Control technology support for Ubuntu 22.x and RHEL 9.x. You can create a new UDC where you can select and use Ubuntu 22.x and RHEL 9.x under **Control Technologies**.

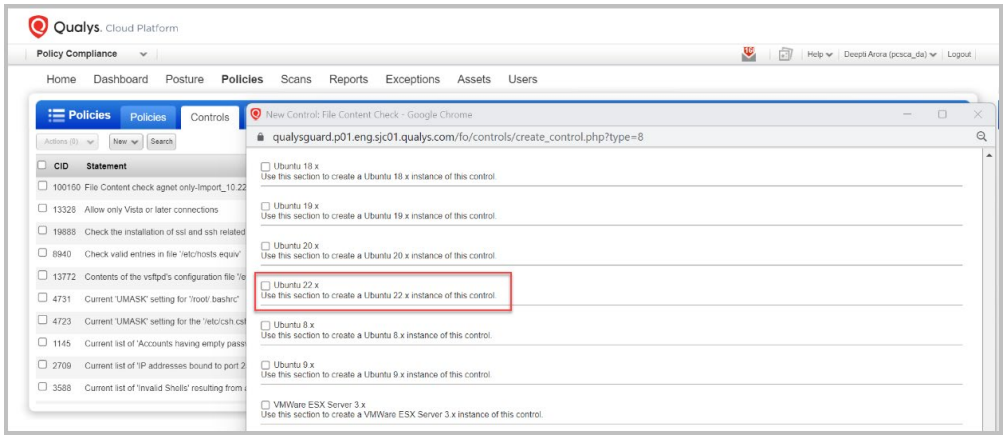
How it works

Here is the basic flow to create a new User Defined Control using new control technology support:

1. In **Policy Compliance**, navigate to **Policies** > **Controls**.
   Here, you can choose from several available controls and create your own User Defined Controls.
2. Click **New** and select **Controls**.
   The **New User Defined Control** window appears.
3. Select **Unix Control Types** from the side pane.
4. Select a control type from **Unix Control Types** list.
5. Provide the mandatory information and you can see the newly added support for Ubuntu 22.x and RHEL 9.x under **Control Technologies**.



RHEL 9.x under Control Technologies



Ubuntu 22.x under Control Technologies

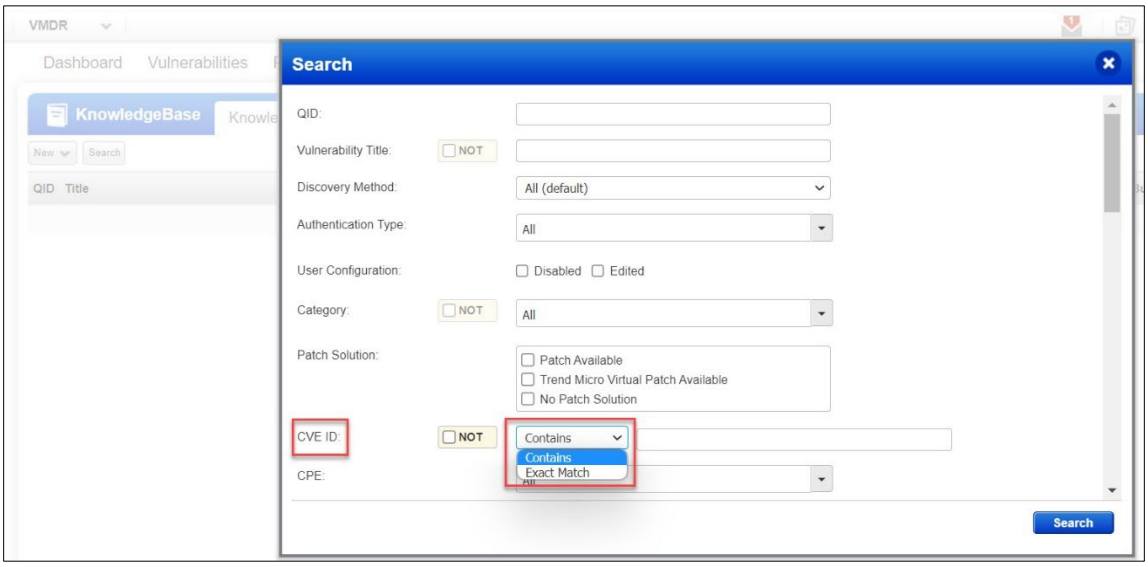
Extended CVE Search Ability in KnowledgeBase for "Exact Match" and "Contains"

With this release, you can use the extended CVE search options **Exact Match** and **Contains** to filter the QIDS based on selected search criteria. A new drop-down is added in the existing CVE ID box, containing two menus: **Contains** and **Exact Match**.

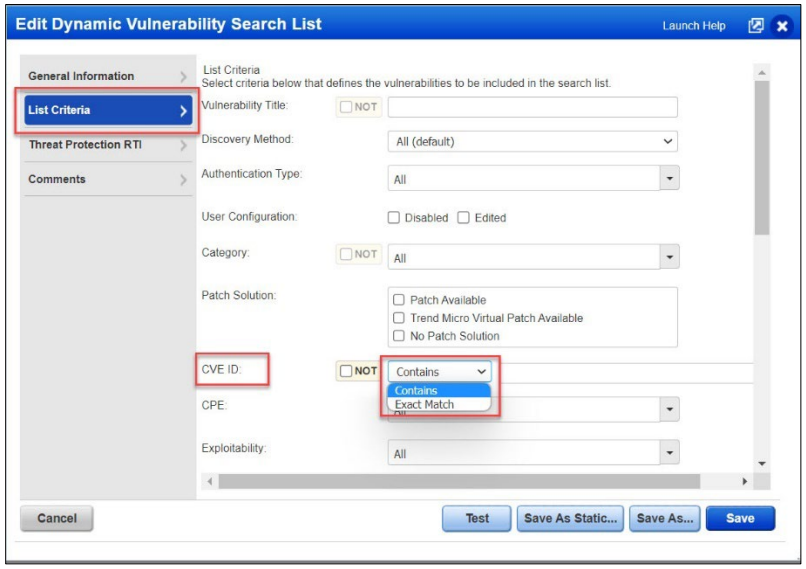
- The **Exact Match** option shows the QIDs that exactly match the CVEs provided in the search criteria.
- The **Contains** option shows the QIDs that exactly match the CVEs and the CVEs that contain the given CVE's name in the search criteria.

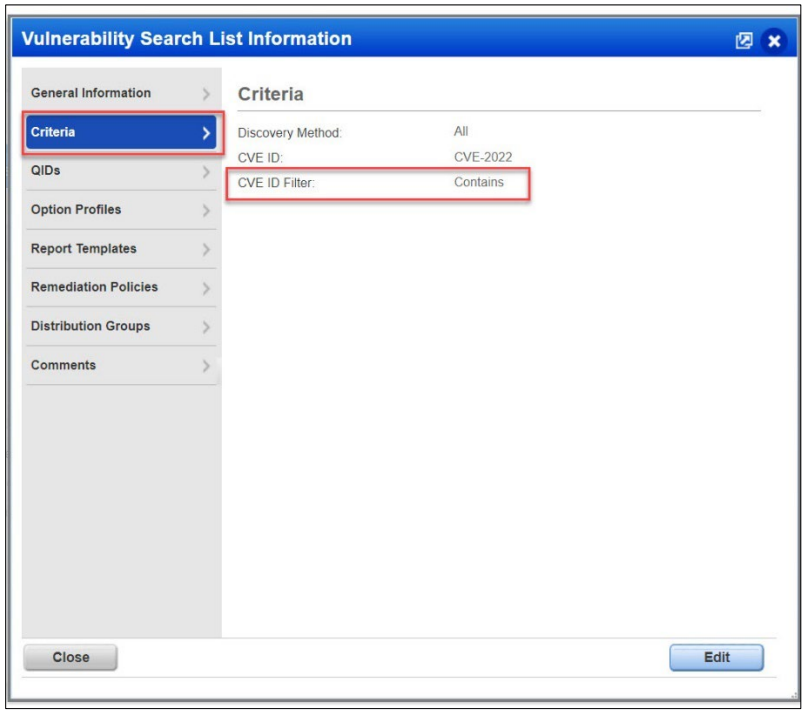
This option is provided in the KnowledgeBase Search option. You can create a new Dynamic Search List that can be imported into different sections such as **Reports**, **Scans**, and **Remediation**. It is available on KnowledgeBase and Dynamic Search List Pages.

Go to **VM/VMDR > KnowledgeBase** > **Search > CVE ID.**



This change also applies to the **Edit Dynamic Vulnerability Search List** and **Vulnerability Search List Information** UI for any existing dynamic search list.

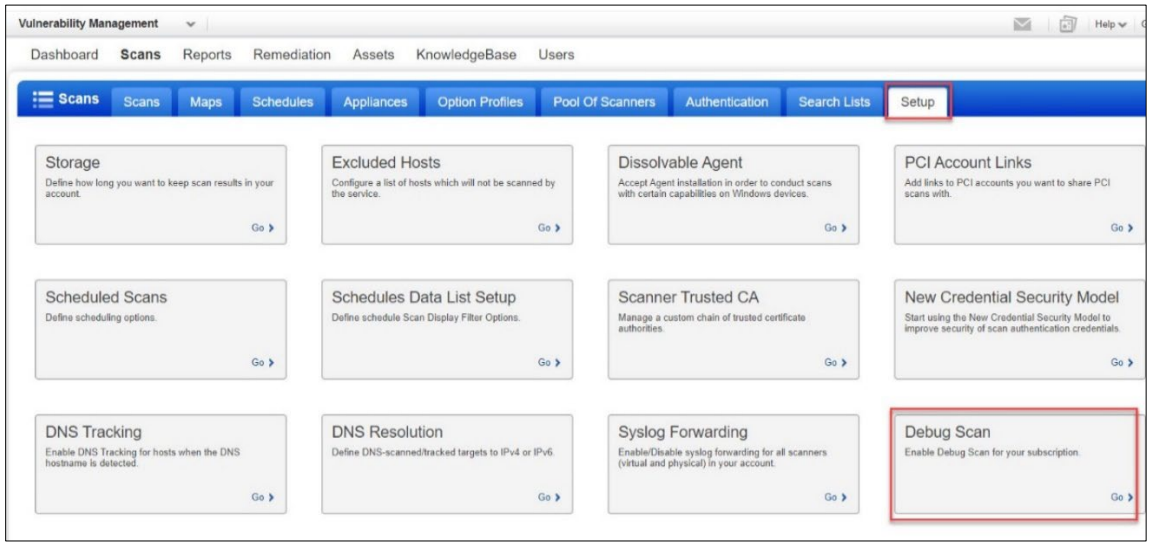




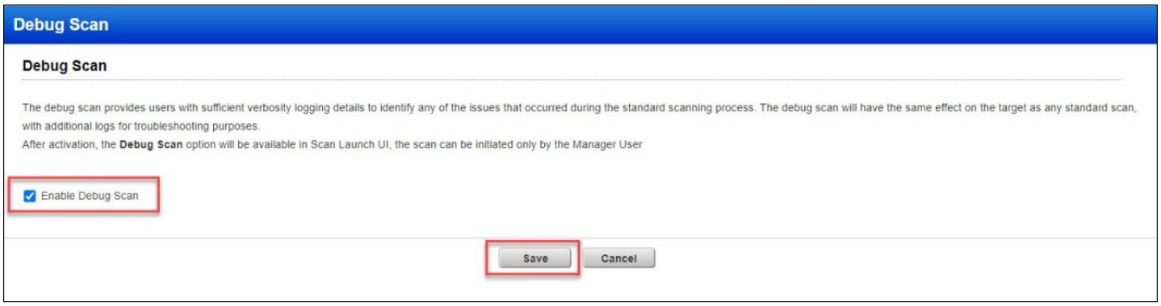
Automated Debug Scan for VM Internal Scanner

With this release, you can now perform Automated Debug scans. You can launch the Debug Scan from the Scan Launch Screen with only one IP Address. With this, the scanner is automatically set into Debug mode, and post the completion of the scan, the scanner will automatically revert to the Standard operation mode. You can continue with their traditional scanning activity planned during that time.

Note: The "Debug Scan" feature needs to be enabled for your subscription. Contact your POC Manager user.
Once enabled, go to **Setup > Debug Scan**.

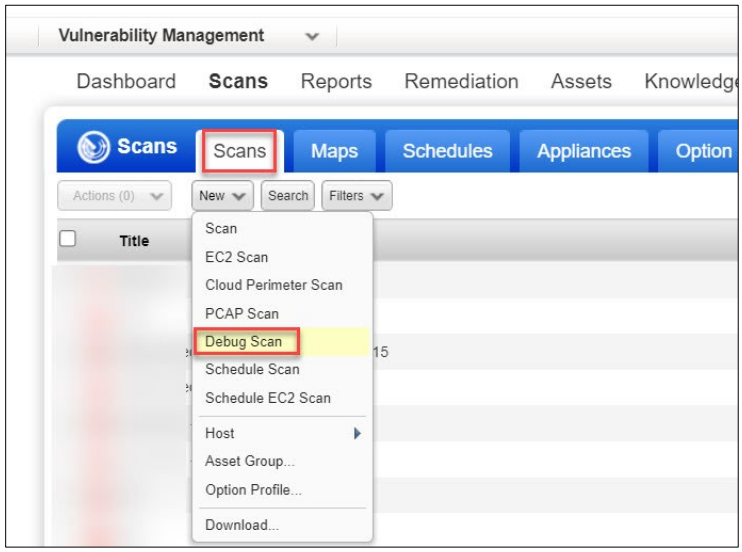


Select **Enable Debug Scan** and click **Save**.



After activation, the Debug Scan option will be available in Scan Launch UI. The scan can be initiated only by the Manager User.

To launch a Debug scan, go to **VM/VMDR > Scans > Scans > New > Debug Scan.**



Post Completion of Debug Scans

After completing the Debug Scans, the Scanner Appliance will automatically revert to normal.

You must manually download the Scan Results in PDF format (for the Debug Scans) and then share it with the Qualys Support team at support@qualys.com. Qualys Support will leverage backend tooling and reference numbers from the Scan PDF to retrieve, decompress, and de-obfuscate that log file which could potentially contain sensitive information.

Issues Addressed

- Hosts that were not part of the PC license were incorrectly included in the Scorecard report. We have now fixed this issue to exclude hosts from the scorecard report that are not included in PC license.
- In some cases, when trying to update an IBM DB2 Authentication Record, a duplication error message was thrown stating that the IP/Port combination being used is already present in another IBM DB2 Authentication record. This issue is now resolved.
- We fixed an issue, where the user was not getting the scan processed even if the status of the scan showed Finished.
- In a few cases, when the user having access only to the PC module was logged in to QWEB, the user was redirected to the VMDR portal landing page and got an error in the UI. We have fixed the issue; the user is now redirected to QWEB's default dashboard page when logging in
- "We have fixed an issue where customers could not create a network with the same name as a deleted network. Now, customers can create a network of the same name after the database is updated successfully, which may take around an hour."
- We fixed an issue where Cloud Agent with custom EC2 network/Custom network was getting overridden with global default network after scans.
- We fixed an issue where upon purging only the Certview data, the vulnerability data was also getting purged.
- We fixed the issue where upon running and downloading a scan-based report on auth records, incorrect host details were shown under the "Windows authentication was successful for these hosts" section.
- We fixed an issue with the business function of the asset group where the changes made by the user in the business function were not getting logged in activity logs.
- We fixed an issue with the vCenter ESXi data mapping where the mapping data was not getting populated in the map table.
- We have fixed an issue where any update to a scheduled scan with multiple asset groups caused an indefinite wait time and non-completion.
- We have fixed an issue for Asset Search Report having QIDs with results selection and containing filter. The Search Criteria was displaying the containing filter parameters incorrectly.
- The asset counts obtained from API and UI searches for assets scanned between specific dates were different. It was possibly due to differences in the search queries used. Please note the following:
    - The "vm_scan_date_before" parameter displays results on or before the specified date, whereas the "vm_scan_date_after" parameter displays results after the specified date.
    - The date-related tokens in the search are evaluated based on UTC format, with the search results showing the date as per your time zone.

  To investigate the difference between the API and UI search results, it may be necessary to examine the specific search queries and relevant search parameters.