Qualys Cloud Platform v3.x

Release Notes

Version 3.12
June 16, 2022

Here's what's new in Qualys Cloud Suite 3.12!

WAS Web Application Scanning

YAML Support for Swagger File

CA Cloud Agent

OCI BYOL Support
Disable Self Protection Feature for Windows Agent

VMDR Vulnerability Management, Detection, and Response

Qualys TruRisk
New Risk Score Widget for the Dashboard
KB Security Level
Remediate Microsoft Vulnerabilities with a Patch and a Configuration Change
New Tokens for VMDR

Qualys Cloud Platform 3.12 brings you many more improvements and updates! Learn more!

WAS Web Application Scanning

YAML Support for Swagger File

With this release, while creating a web application, you can upload a swagger/OpenAPI file in YAML format to scan REST APIs for vulnerabilities.

Note: To upload the YAML file, you must have the following permissions granted in the Administration module in addition to the WAS subscription:

- UI Access and Access WAS module permissions
- Create, edit, and view permissions for web applications

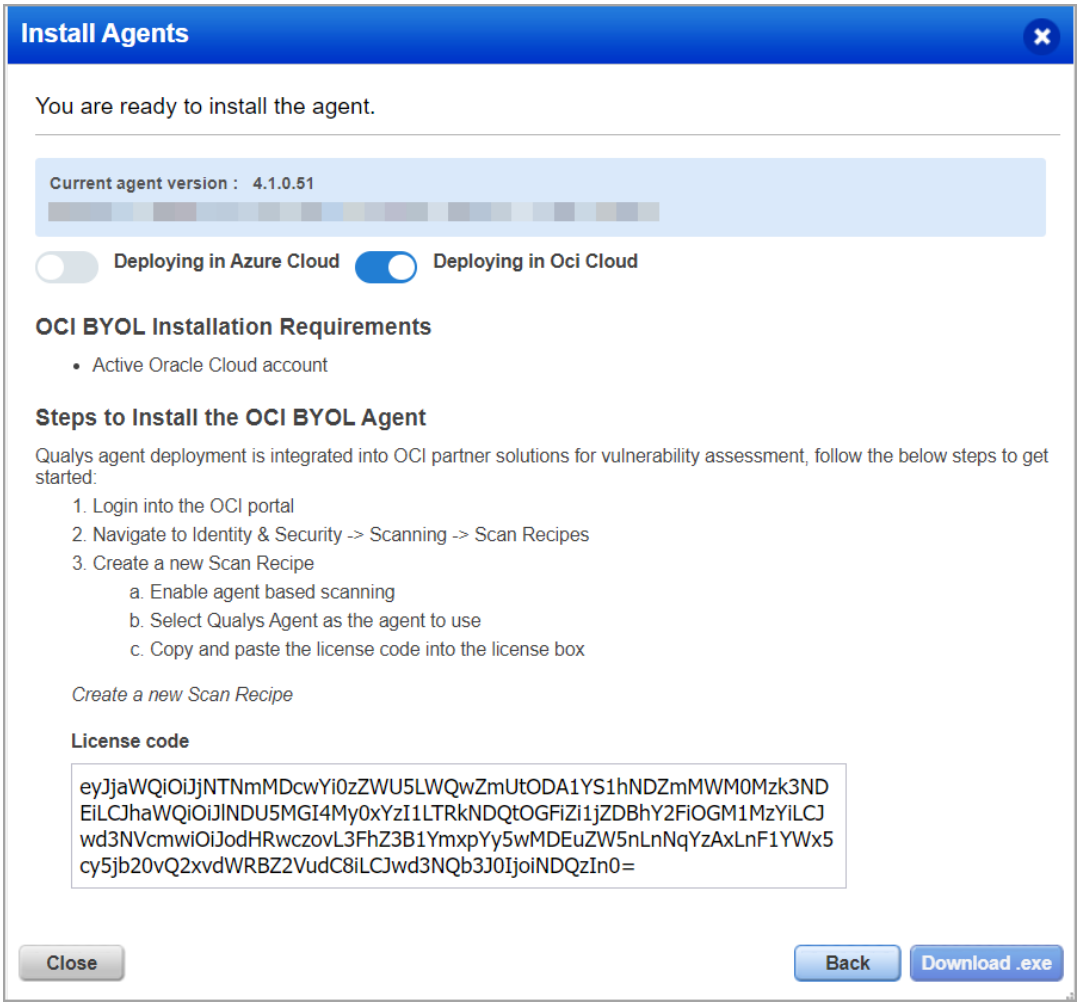
CA Cloud Agent

OCI BYOL Support

With this release, we have added Bring Your Own License (BYOL) support for Oracle Cloud Infrastructure (OCI) to enable Qualys VM scanning for instances on OCI.

To register these instances in the Qualys platform, you need a license code. To view the license code:

- Navigate to **Agent Management** > **Activation Keys**
- Select the activation key, and click **Install Agent** from the **Actions** menu.
- In the **Install Agents** screen, click **Install instructions** for the required agent > **Deploying in OCI Cloud**.



You can follow the instructions and use the license code to install the agent in your OCI.

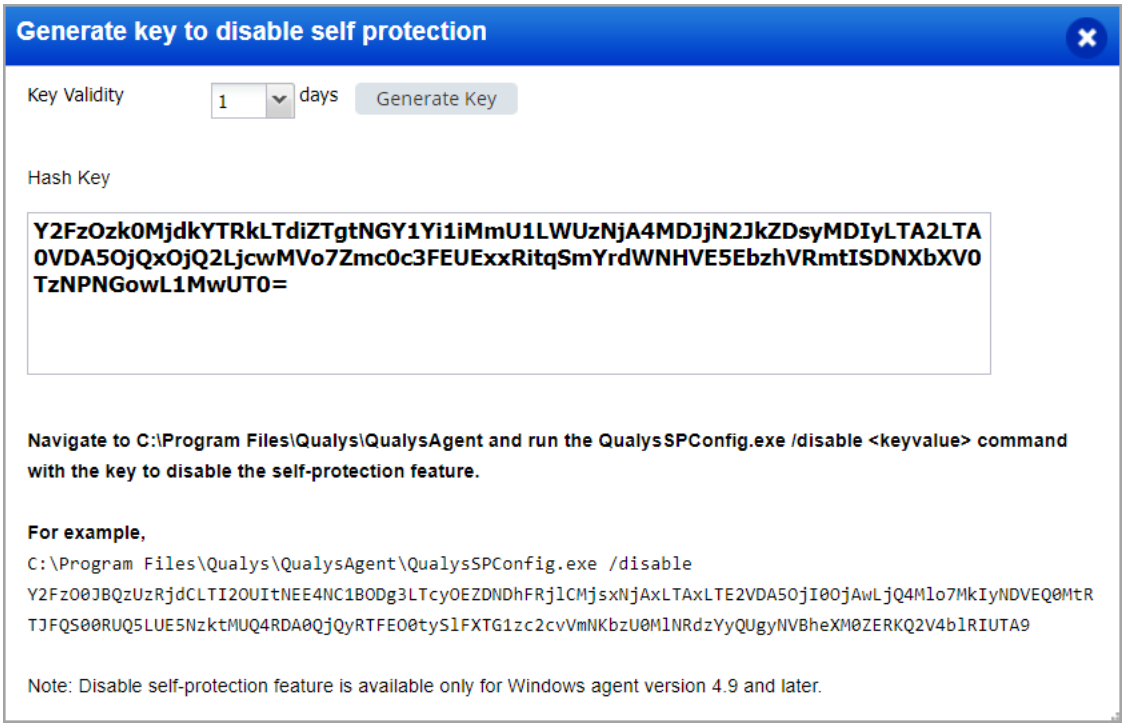
Disable Self Protection Feature for Windows Agent

With this release, you can generate a key to disable the self-protection feature for Windows Agent. By disabling the self-protection feature, you can access the agent data and artifacts that are required for debugging purposes, such as log files.

By default, the self-protection feature is enabled for all Windows agents. With this enhancement, you can generate a key to disable self-protection for a defined time interval for Windows Agent. By default, the generated key is valid for one day. However, you can define the validity of the key.

Note: Users with the Managers and Unit Managers role have permission to generate the self-protection key.

To disable self-protection on an agent, in the Agent tab, select agent, and click Disable Self Protection.



In the **Generate key to disable self protection** screen, click **Generate Key** and follow the process to disable the self-protection on the selected agent.

Note: This feature is available only for Windows agent version 4.9 or later.

VMDR **Vulnerability Management, Detection, and Response**

Qualys TruRisk™

With this release we have introduced Qualys VMDR with TruRisk. Qualys TruRisk provides integration between CMDB's ITSM tools such as ServiceNow, and patch management solutions. Qualys TruRisk also offers an automated consolidated version of the prioritization workflow. It proactively estimates risk across vulnerabilities, assets, and groups of assets to provide remediation. It provides data for Asset Criticality Score (ACS), Qualys Detection Score (QDS), and Asset Risk Score (ARS).

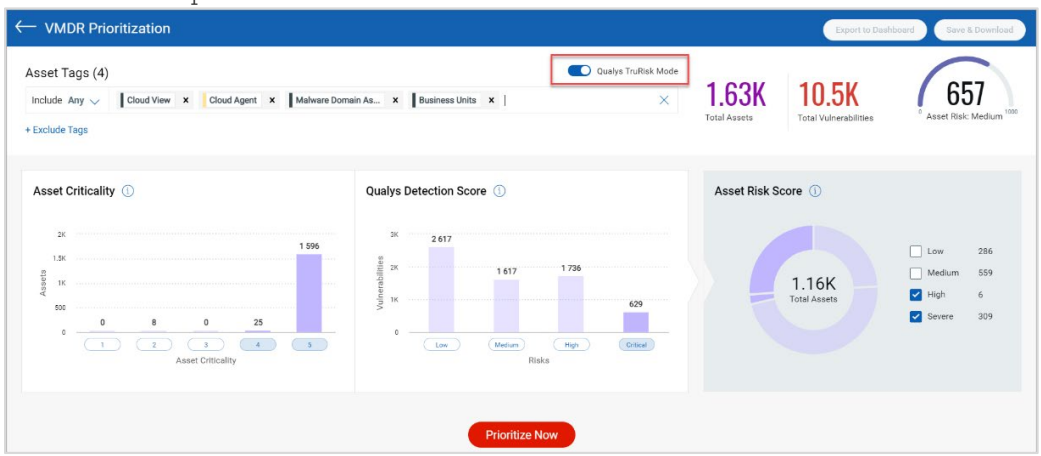
- **ACS**: You can select the range of Asset Criticality (1-5) using the Asset Criticality bar graph. The highest score is considered if multiple tags are assigned to the asset.
- **QDS**: You can select the range of Risks (Low-Critical) in its bar graph. The risk scores generated prioritize the assets and vulnerabilities.
- **ARS**: It helps you prioritize your vulnerabilities based on the risk to your assets and not just the technical severity. If no risk is detected the value of ARS is shown as 1 (Low Risk).

  The ARS range is between 0 to 1000, and is divided as follows:
  - Critical (c): 850-1000
  - High (h) : 700-849
  - Medium (m) : 500-699
  - Low (l): 0-499

NOTE: If no vulnerabilities are detected on any assets the risk score is set to 1.

To enable the Qualys TruRisk Mode in the **Prioritization** tab:

- Click **Reports** > **Start Prioritizing**
- Click → to proceed with Prioritization.
- In the Asset Tags field select Include or Exclude options and add tags.
- Toggle the **Qualys TruRisk Mode** to enable it.
- The result displays the Asset Criticality, Qualys Detection Score and Asset Risk score.
- Click **Prioritize Now** to enable threat intelligence. This will prioritize the riskiest vulnerabilities on your netowrk for the selected assets.
- You can patch the vulnerabilities if Patch Management application is enabled in your subscription.

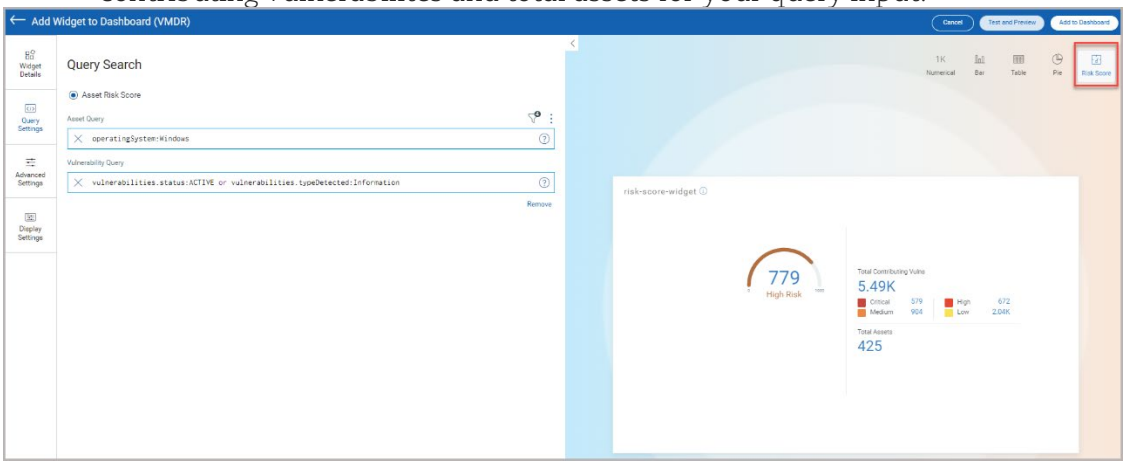


For more information, see VMDR online help(link to be added)

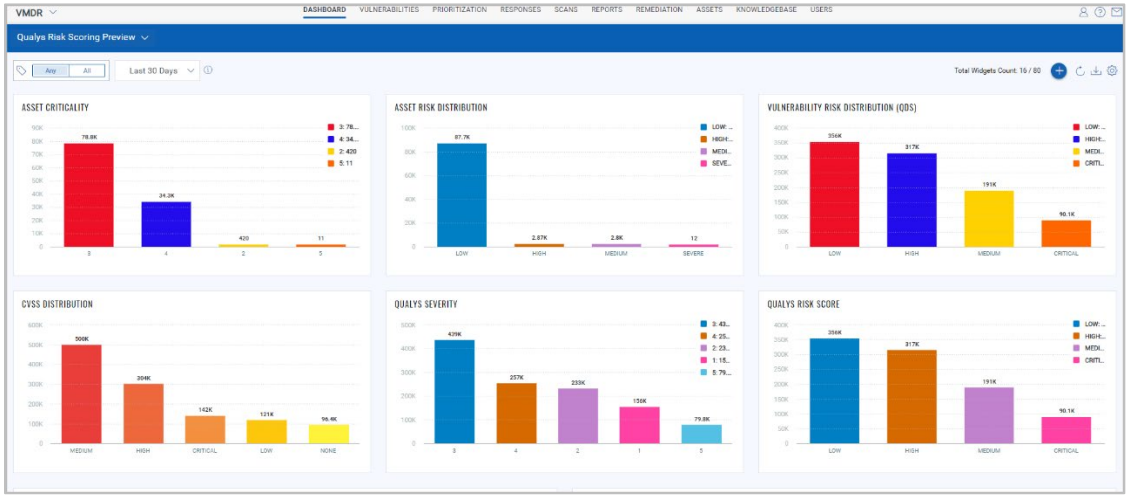
New Risk Score Widget for the Dashboard

We have introduced Risk Score widget to show data based on the risk score of the assets in your environment. The widget displays the contributing factors which helps you prioritize the vulnerabilities. To generate a risk score widget dashboard from the **Build your widget** option perform the following steps for the Vulnerability Management application:

- Click **Query Settings** and select **Risk Score**
- In the **Asset Risk Score** choose **Asset Query** or **Vulnerability Query**.
- Optionally, you can click **Advance Settings** and enable **Contributing Factors** to view the contributing vulnerabilites and total assets for your query input.



- Click Add to Dashboard to complete the widget creation and view the widget on dashboard.



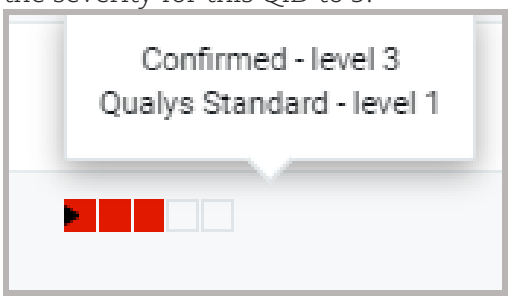
KB Severity Level

With this release, you can now view the severity level set by Qualys. It will help you differentiate the severity levels set by you and Qualys for a particular QID.

⟶ : Indicates custom severity higher than Qualys severity.

⟵ : Indicates custom severity lower than Qualys severity.

Example:
Consider a QID with Qualys severity as 1 and custom severity as 3. The severity bar indicates the right arrow at 1. The right arrow implies that Qualys severity level is 1, but you have increased the severity for this QID to 3.



Remediate Microsoft Vulnerabilities with a Patch and a Configuration Change

With this release, you will be able to view if the vulnerabilities require a patch or a configuration change. If the selected vulnerabilities require a patch and a configuration change the job will be pre-populated with the relevant patches and the required configuration changes. You can perform the remediation action from the **VMDR Prioritization** page.

- Click **Start Prioritizing** and add asset tags to proceed.
- Click **Prioritize Now**.

Available Remediation column has **Patches** and **Fixes for Misconfiguration** The **Patches** are based on the Qualys Patchable, and **Fixes for Misconfiguration** includes the pre and post config changes.

- Click **Patch Now** for the QID you want to apply patches and then select **Add to new Job.**

You will be redirected to Patch Management application. Based on the script config you select (pre or post) the script window will display.

New Tokens for VMDR

We have updated the information for the Vulnerability, Assets and Search tokens to enhance your search results:

- **vulnerabilities.vulnerability.severity:** Select this token to view the severity level set by Qualys.
- **vulnerabilities. severity:** Select this token to view the severity level set by you.

Issues Addressed

AM Asset Management

- We have updated the Asset Management online help with the correct ruleType parameters for the Search Tag API.

AV Asset View

- We have fixed an issue where the Azure VM with multiple NICs was unable to fetch IP from all the NICs.

- We have fixed an issue where the createdDate parameter for EC2 was not in sync with the Launch Date.

CA Cloud Agent

- We fixed an issue where the note regarding the deactivation of modules on the Deactivate Agent screen was confusing. After the fix, the note on the Deactivate Agent screen provides the correct information.

- We fixed an issue where the Asset Summary tab in host details displayed DNS short name instead of FQDN name. We now support the FQDN value in the Asset name attribute sequence at PBO. Thus, you can set the asset name as FQDN value if required.

AV Asset View

VM Vulnerability Management

- We have fixed the backend implementation of the following query results to avoid any discrepancies in the Asset View and Vulnerability Management. You might expect some spike in the trending widgets if the following tokens are used:
    - operatingSystem
    - operatingSystem.name
    - software.name
    - software.version

VM Vulnerability Management

- In the Asset list of the Vulnerabilities tab, the IP address was shown as unknown IP though the IP addresses were assigned to the assets. We fixed this issue, and now the assets display the correct assigned IP address.

- We fixed an issue about the discrepancy results of the agent.lastCheckedIn and agent.lastActivity QQL.

- We fixed an issue where the asset numbers displayed in the Ratio widget would not match the existing assets after applying tags.

- We fixed an issue where the QQL results for vulnerabilities.vulnerability.title, group by Vulnerability if downloaded as CSV would not show the data.

TP Threat Protection

- The following three Threat Protection (TP) tokens are removed from the "Search Tokens for IT Assets" topic of the online help as these tokens are not supported in the product:
    - vulnerabilities.vulnerability.threatIntel.privilegeEscalation
    - vulnerabilities.vulnerability.threatIntel.remoteCodeExecution
    - vulnerabilities.vulnerability.threatIntel.unauthenticatedExploitation

WAS Web Application Scanning

- We have updated the online help with information for Experimental QID.