



# Qualys Cloud Platform v3.x

## Release Notes

Version 3.16.2

December 08, 2023 (Updated on February 6, 2024)

### What's New?

**VMDR**

**Vulnerability Management Detection and Response**

[MITRE ATT&CK Matrix in VMDR](#)

[New Token in VMDR](#)

[Updated Tokens in VMDR](#)

**CA**

**Cloud Agent**

[New Tokens in Cloud Agent](#)

[New Feature – Agent Version Control](#)

Qualys Cloud Platform 3.16.2 brings you many more improvements and updates! [Learn more](#)



### MITRE ATT&CK Matrix in VMDR

To enhance the defensive mechanism of your network security, we have introduced the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework to improve your organization's network security. Qualys provisioned Enterprise MITRE ATT&CK Matrix identifies security architecture gaps, instantly suppresses the threat, and protects your organization from new attacks.

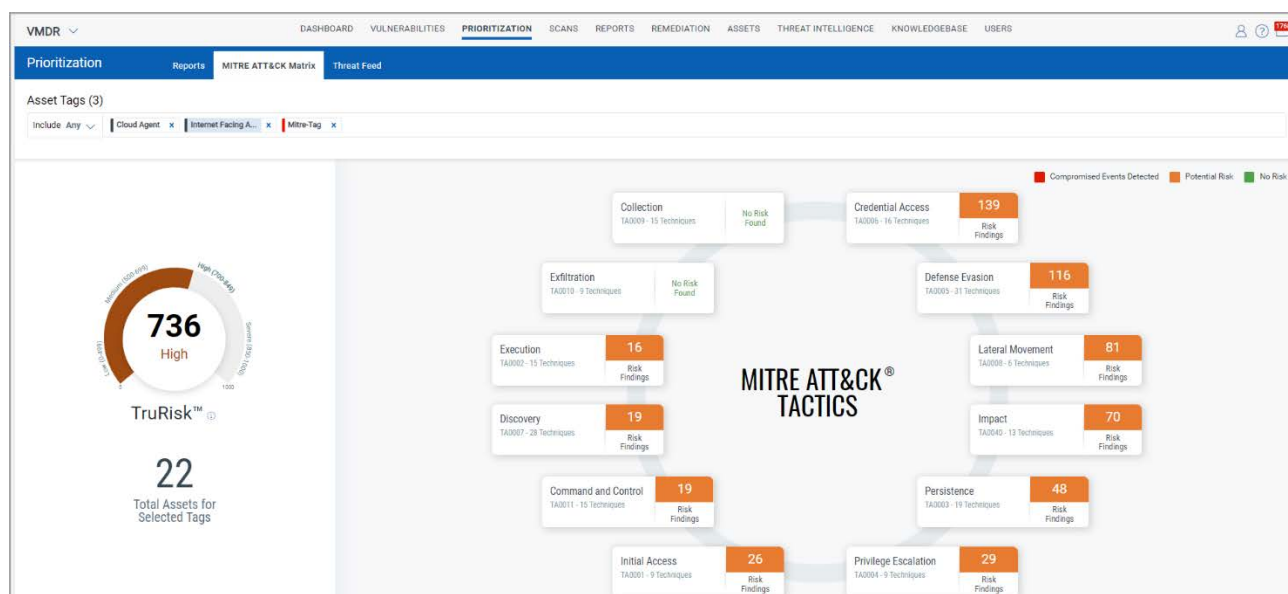
Prerequisites for MITRE ATT&CK Matrix:

- VMDR Full subscription
- VMDR Manager User

Additionally, with the Qualys Policy Compliance (PC) subscription, you can reduce internal and external threats by scanning the compliance check of your systems against your policies. Qualys Endpoint Detection and Response (EDR) subscription leverages you to get the list of compromised events.

To evaluate, determine, and remediate such attacks the MITRE ATT&CK Matrix in the **Prioritization** tab helps you enhance the robustness of your organization's products and services.

The following screenshot is an example of Tactics and Techniques on the vulnerabilities (QID), misconfiguration (CID), and Endpoint Detection and Response (EDR) events:



For more information, see MITRE ATT&CK in VMDR Prioritization in *VMDR Online Help*.

## New Token in VMDR

- **agent.swCAIdealCandidate:** Use this token to identify assets on which at least one of the software components from Ruby, Node.js, Go, Rust, PHP, Python, Java Platform, Standard Edition (Java SE) is identified. The supported values are 'true' and 'false'.

For more information, see Search Tokens for VMDR in *VMDR Online Help*.

## Updated Tokens in VMDR

- **activatedForModules:** SwCA has been added to the activatedForModules token. From the drop-down, select the type of activated module.
- **pendingActivationForModules:** SwCA has been added to the pendingActivationForModules token. From the drop-down, select the modules that are pending for activation.

For more information see Search Tokens for VMDR in *VMDR Online Help*.

## New Tokens in Cloud Agent

The following tokens are added to the Cloud Agent:

Token Name	Description
vmManifestVersion	Find the host assets, where the VM scan is performed with the specified manifest version.
pcManifestVersion	Find the host assets, where the PC scan is performed with the specified manifest version.
scaManifestVersion	Find the host assets, where the SCA scan is performed with the specified manifest version.
udcManifestVersion	Find the host assets, where the UDC scan is performed with the specified manifest version.
middlewareManifestVersion	Find host assets, where the middleware scan is performed using the specified manifest version.
swCAIdealCandidate	Find the host assets on which at least one of the software components—Ruby, Node.js, Go, Rust, PHP, Python, Java Platform, and Standard Edition (Java SE), is identified. The token uses the boolean values— True or False.

## New Feature — Agent Version Control

The Agent Version Control gives you control and flexibility to manage the Cloud Agent versions across your organization. It ensures that all endpoints have the same security measures by preventing unintended variations in software versions.

By locking specific agent versions, organizations can control updates and patches to align with the organization's operational needs, reducing the risk of compatibility issues and simplifying the task of managing security protocols.

**Note:** This feature is not available by default. To enable the feature, contact your Qualys representative.

### Agent Version Control (AVC) Profile Creation

Only one AVC profile can be configured for each subscription. However, you can edit or delete the system-provided AVC profile and create a new AVC profile.

To create a new agent version control profile or edit an existing profile, click **Configuration > Agent Version Control Profile**.

← Create: Agent Version Control Profile

### Agent Version Control Profile Details

Provide information for the Agent Version Control profile.

AVC Profile Name \*

Subscription Level Profile

Description

new cloud agent version profile

69 characters remaining

### Agent Versions

Select a platform and corresponding agent version for this AVC profile.

Platform

Select Platform

Agent Version

Select Agent Version

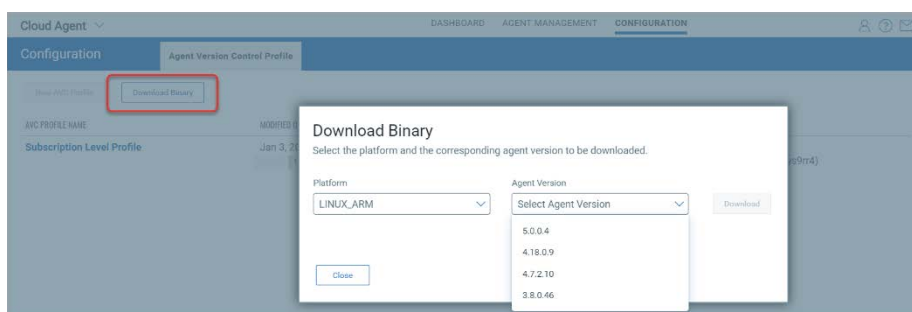
Add

PLATFORM	AGENT VERSION	
WINDOWS	5.3.0.16	
MACOSX	4.30.0.26	
MACOSX_M1	4.40.0.43	

Cancel Save

## Support for non End-of-Support (EOS) Agent Versions

You can now download previous non end-of-support (EOS) Cloud Agent binaries for your specific use cases, even if a newer version is available.



For more information, see *Cloud Agent Online Help*.

## Issues Addressed


### CA

#### Cloud Agent

- We have updated the online help for setting up exclusion to avoid conflict with antivirus or HIPS software on Windows systems. The page is updated with the files, directories, and processes that need to be excluded.
- If the user had marked a custom SwCA profile as a default profile when the user edited and saved it, the profile was not shown as the default profile. Instead, the system-generated SwCA profile was marked as the default profile. This issue is resolved. Now, the custom SwCA profile, if marked as the default profile, is retained after editing.
- We have fixed an issue where users with the CA Manager role could not see the Disable self-protection and Troubleshoot options with all necessary permissions. Now, users can access those permissions with the CA manager role for newly created subscriptions.
- We have fixed the issue where the tags were not applied to some host assets, although the assets were meeting the dynamic tagging criteria.
- We have fixed an issue where the instance State was not displayed for some GCP instances.
- In the earlier version, when the Software Composition Analysis (SwCA) feature is enabled in a trial mode for a user, the subscription for the Cloud Agent application also changed to the Trial mode. This issue is resolved.

### VMDR

#### Vulnerability Management, Detection, and Response

- The latency issue of downloading detailed reports from the Vulnerabilities tab of the VMDR application is now fixed. You can view the report download progress since the report is directly downloaded from the new tab.
- We have fixed an issue for all widgets with Trending enabled where the gear icon  did not reflect the changes selected by the user.

### WAF

#### Web Application Firewall

- We have fixed an issue where the user could not add a web application with the URL containing .lat extension for Top-Level Domains (TLD) through the Web Application Firewall application.

### WAS

#### Web Application Security

- We have fixed the delay in response to the get web application details API. Now, the response time is improved.

The impacted API- GET: <APIServer name>/qps/rest/3.0/get/was/webapp/[id] API

- We have fixed an issue where the user could not generate the scan report for some scans, where one of the scans was deleted, and the reference scan ID had been deleted from the database. Now, the user can generate the scan report even when the corresponding scan ID is deleted.