

Release Notes

Version 3.16 August 24, 2023 (Updated on November 15, 2023)

What's New

CA

Cloud Agent

Asset Architecture Type in Asset Summary Updated Permissions for On-demand Scans New Tokens in Cloud Agent New Feature - Cloud Agent as a Passive Sensor New Feature—Software Composition Analysis Static Tag Removal from Activation Key and Associated Agents

Qualys Cloud Platform 3.16 brings you many more improvements and updates! Learn more

Cloud Agent

CA

Asset Architecture Type in Asset Summary

With this release, the **Asset Summary** tab displays the asset architecture type. The following screenshot is an example of the Asset Summary:

qualys-					*
View Mode		Asset Summary			
Asset Summary System Information	>		ualys Rename		
Agent Summary	>		66_64 VMware, Inc. / VMware Virtual Platfor	m	
Network Information	>	Identification		Last Loca	ation
Open Ports	>	DNS Hostname: FQDN	qualys qualys₋v		
Installed Software	>	NetBIOS Name:	-		Start - And Children
Vulnerabilities	>	IPv4 Addresses: IPv6 Addresses:			Location unknown. Last Seen: 24 minutes ago 9:39 PM
File Integrity Monitoring	>	Asset ID: Host ID:	-		Connected From:
QES	>				
Alert Notifications	>	A - 41 - 14 -		Taura	<i>L</i> .
Patch Management	>	Activity Last User Login: Last System Boot: Created On: Last Checked-In: Last Activity:	qualys October 18, 2022 4:07 PM March 31, 2023 6:09 PM 24 minutes ago 9:39 PM 24 minutes ago 9:39 PM	Tags	oud Agent ST_1
Close					

Updated Permissions for On-demand Scans

With this release, the permissions to launch on-demand scans can be assigned to a user role from the Admin module.

A new permission is added under the Role Management in the **CA Agent Permissions** section.

Role Edit: CA Use	er		Turn help tips: On Off
Edit Mode		Edit permissions for this role	
Role Details	>	Role Permissions by Modules (19)	Remove All
Permissions	>	CA Cloud Agent	Remove
Action Log	>	CA Module Access Permissions (2 of 2)	
		CA Configuration Profile Permissions (1 of 1)	
		CA Agent Permissions (5 of 5)	
		✓ Launch On-Demand Scan✓ Install Agent	
		✓ Uninstall Agent	
		Activate Agent	
		✓ Deactivate Agent	
		CA Activation Key Permissions (8 of 8)	
		CA Configuration Profile Permissions (3 of 3)	
Cancel			Save

With the new permission, a user can launch an On-Demand Scan even if the user does not have CA Manager role access.

New Tokens in Cloud Agent

The following tokens are added to the Cloud Agent:

Token Name	Description	
azure.vm.state	Find Azure VM instances in the selected state: DEALLOCATED, DEALLOCATING, DELETED, RUNNING, STARTING, STOPPED, STOPPING.	
gcp.compute.state	Find GCP instances in the selected state: PENDING, RUNNING, STOPPED, TERMINATED, STOPPING, SHUTTING_DOWN, DEALLOCATED.	
aws.tags	Find EC2 instances with specific tags.	
aws.tags.key	Find EC2 instances with specific AWS tag keys.	
aws.tags.value	Find EC2 instances with specific AWS tag values.	
lastComplianceScanDate:	Find compliance scans performed on a specific date or within the specific date range.	
aws.ec2.launchDate	Find EC2 instances launched on a specific date or within a specific date range.	

New Feature—Cloud Agent as a Passive Sensor

With the Cloud Agent as Passive Sensor (CAPS) feature, the Qualys Cloud Agent can collect the data in the subnet passively without any active probing of the device that it is monitoring. The Cloud Agent can monitor all network traffic and flag any asset activity.

The asset metadata is sent to the Qualys Cloud Platform for analysis, with which you can classify the unmanaged assets by operating system and hardware.

This provides you with real-time visibility to all managed and unmanaged across your global, hybrid IT environment.

The CAPS module applies only to the Windows platform and is available as part of the CSAM application. You must perform CAPS configuration before activating the CAPS module for an agent host.

Note: This feature will be available only when the Windows agent binary with CAPS support is available. For supported agent versions, refer to the Features by Agent Version section in the Cloud Agent Platform Availability Matrix.

Configure CAPS Settings

To define the settings for the Cloud Agent to work as a passive sensor, such as the interval at which data is uploaded, and the scope of passive scanning, in the Cloud Agent application, go to the **Configuration** tab and click **CAPS configuration**.

Cloud Agent \smallsetminus	DASHBOARD AGENT MANAGEMENT CONFIGURATION	2 @ 🗹
Configuration	CAPS Configuration SwCA Scan Profile	
	CAPS Configuration Configure Cloud Agent Passive Sensor Data Upload Interval Define the interval at which agents upload the CAPS data to Qualys Cloud Platform. Data Upload Interval (15-1440 min) * 30	
	Domain or include Assets Define the domain and IP address range within your network to identify the assets you want to monitor.	
	Domain Name * IP/IP Range ①	Add
	Enter Domain Name Enter IP/IP Range	Add
	1 selected Clear Selection Remove Selected	
	✓ DOMAIN NAME IP/IP RANGE	
	✓ abc.com 10.10.10.10	\diamond ×
	Excluded Assets Discover the IP and Mac addresses to be excluded from the inventory. The assets discovered for these addresse Excluded in the traffic summary. Asset Type IP/IP Range MAC Address	es are marked as
	NOTE: Click Cancel to revert to the last configured state	
	Cancel Save	

Activate CAPS Feature

To enable this functionality, you must activate the CAPS module on a single or multiple-agent host. You can activate the CAPS feature from the Agents or Activation Keys tab.

To activate the module, go to **Agent Management** > **Agents** tab, and click **Activate** for <modules> from the **Quick Actions** menu. Once CAPS is activated, you can see the detailed

information about the assets discovered in the CSAM application from the **Inventory** > **Sources** > **CAPS** tab.

	Searches 👻		Activate Agent 🗙	100.20
arch			Activate this cloud agent for the modules selected below.	
10	Agent Host	OS	Accuracy and the second	son
1	CAUIK_windows_	📲 Windows 10	PM Patch Management Not activated. Your agent(s) are not activated for Patch. 191 available of 200 total activations Supported for only Windows 3.0, Linux 4.6, MAC 4.25 and higher Agent versions:	1.14
			SwCA SwCA Not activated. Your agent(s) are not activated for SwCA.	
1	test_windows_16	📕 Windows 10	CAPS	la.
1	agentsim-netbios	🔌 Red Hat Enter.	CAPS 1 agent(s) will be activated for CAPS.	9

The following screenshot is an example that displays activating the CAPS module while creating or editing the activation key.

Acti	vation K	(ey		Tum	help tips: On Off	×
Edit	t the activ	ation key				
		y is used to install agents. This provides a ws you to add any number of agents at an	group agent	s and better manage your accoun	t. By default this ke	ey is
Title	l.	demo_key				
				Select Create		
		EDR-UI X 10_Nov_23 X				
Pro	vision Key	for these applications				
	CSAM	CyberSecurity Asset Management Activations managed by CSAM	PM	Patch Management 10096 Activations Remaining		
	VM	Vulnerability Management 9996 Activations Remaining	PC	Policy Compliance 9998 Activations Remaining		
	EDR	Endpoint Detection and Response 64 Activations Remaining	FIM	File Integrity Monitoring 99 Activations Remaining		
	XDR	Extended Detection and Response 100 Activations Remaining	SCA	Secure Config Assessment 9999 Activations Remaining		
	CAPS	Cloud Agent Passive Sensor 50000 Activations Remaining				
	Set limits					
	Apply cha	nges to all the existing agents				
Clo	ose			U	nlimited Key 🗧 Si	ave

New Feature–Software Composition Analysis

With the software composition analysis (SwCA) feature, Cloud Agent can discover and report vulnerabilities associated with the third-party or open-source dependent software used by Qualys applications.

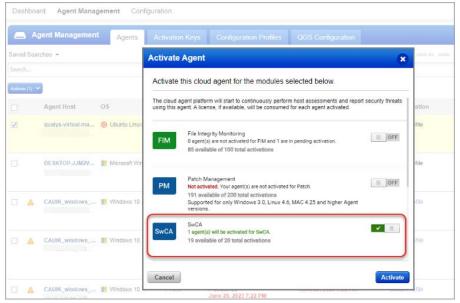
You can schedule a SwCA scan or launch the scan on demand. With the SwCA scan profile, you can define the scan scope, scan interval, and scan timeout.

SwCA is supported only for Windows and Linux Platforms and can be activated only when VM is activated for the agent.

Note: This feature will be available only when the Windows and Linux agent binaries with SwCA scan support are available. For supported agent versions, refer to the *Features by Agent Version* section in the Cloud Agent Platform Availability Matrix.

Activate SwCA Feature

To enable this functionality, you must activate the SwCA module on a single or multiple agent hosts. To activate the module, go to **Agent Management** > **Agents** tab, and click Activate for <modules> from the **Quick Actions** menu.



You can also activate the SwCA module while creating or editing the activation key.

New Activat	ion Key			Turn help tips: On Off	×
Create a new	activation key				
	y is used to install agents. This provides a ited - it allows you to add any number of a			s and better manage your account. By defau	ılt
Title	Demo Key				
				Select Create	
	(no tags selected)				
Provision Key	for these applications				
CSAM	CyberSecurity Asset Management Activations managed by CSAM		РМ	Patch Management License limit not enforced.	
D VM	Vulnerability Management License limit not enforced.		PC	Policy Compliance License limit not enforced.	
EDR	Endpoint Detection and Response License limit not enforced.				
SCA	Secure Config Assessment License limit not enforced.	_			
	Cloud Agent Passive Sensor License limit not enforced.		SwCA	Software Composition Analysis License limit not enforced.	
□ Set limits					
Close				Unlimited Key Generat	e

Configure SwCA Scan Settings

The default scan profile that includes scan settings and scan scope for Windows and Linux agents is provided.

You can create customized SwCA scan profile for Windows and Linux assets. To create a customized profile for the SwCA scan:

- 1. Go to the **Configuration** tab and click **SwCA Scan Profile**.
- 2. Click **Create** > **Linux Scan Profile** or **Windows Scan Profile**.
- 3. Enter the required values, and click **Save**.

For example, SwCA scan profile for Linux agent:

← Create New: SwCA Scan Profile	
	Software Composition Analysis Scan Settings for Linux Configure Software Composition Analysis Scan settings.
	Basic Information Provide basic information for the SwCA scan profile. Nome +
	New SwCA Profile
	112 characters remaining
	Description *
	Enter Description
	1
	250 characters remaining
	Scan Interval (1440-43200 Min) * ()
	10080
	Set this as a default profile for the subscription.
	Profile Settings Provide scan settings for the SwCA scan profile.
	T
	Envectories/Files to be excluded ()
	[proc*, /wa/log*, /var/spcol*, /etc*, /us/jbin*, /usr/sbin*, /usr/lb6*, /boot*, /oye*, /srv*, /media*, /met
	20 Default Excluded Directories, Files: /proc*, /we/log*, /we/log*, /etc*, has/bin*, /ws/bin*, /ws/bin*
	Issan Time Dut (120-42200 Mile) * ① 120
	Maximum CFU Usage (0-1074) * ()
	Disable Internet Access When enabled, SCA process can connect to the Maven repository to gather additional information for analysis of Java artifacts.
	Center

Static Tag Removal from Activation Key and Associated Agents

With this release, if a static tag attached to an activation key is removed, the tag is removed from the agents associated with the activation key when the update to the activation key is saved.

Note: This is applicable only if the **Apply changes to all the existing agents** check box is selected.

Issues Addressed

AV

Asset View

- Due to differences between the VM asset name and OS computer name, the Azure VM asset name showed incorrect data. We have given priority to display the computer name as the asset name in such instances.
- We have fixed an issue where the connector was updating the hostname of the VM with an incorrect name despite VMScan being enabled.
- We fixed the tag searchability issue where a special character '&' was included in the tag name.
- A create asset purge rule failure was observed when multiple values were entered in the "agentActivationKey" attribute, as they exceeded the column width. We have now fixed this issue by increasing the column width from 2K characters to 4K characters.
- We fixed the issue wherein creating an asset purge rule using "ActivationKey" failed as extensive page loading time was taken.

CA Cloud Agent

- We have fixed an issue where the user could not deactivate the EDR (Endpoint Detection and Response) module after the subscription was removed for the respective application.
- We have fixed an issue where the agent was working with the Qualys applications. But, in the Agent Summary, the status of the field 'Last Activity' was not updated.
- We have updated the Cloud Agent online help for purge rule behavior for the following scenarios:
 - o the agent is not available for more than 15 days
 - o the agent becomes available within 15 days
- During merging assets, duplicate agent host entries were created in Vulnerability Management. The issue is fixed. Now, while asset merging, the reactivation is triggered after the completion of provisioning actions. This will add a delay between merge and reactivation, and chances of the creation of duplicate host ID will be minimized.

CM Continuous Monitoring

• We have updated the Continuous Monitoring online help with an example while setting notifications.

MD Web Malware Detection

• We have fixed an issue where the Manager user with full permissions could not delete a site from the Web Malware Detection application. Now, a user with Allow Edit Or Delete Malware Domains permission can delete a site.

SAQ Security Assessment Questionnaire

• We have improved the email message that users receive when someone else reassigns or delegates a questionnaire to them.

VMDR Vulnerability Management, Detection, and Response

- We have fixed an issue where an incorrect query result was generated when the user selected the Not Selected 30 Days widget from Qualys Insights under the Vulnerabilities tab.
- We have fixed an issue where the search results for the VulnPatchable column for query vulnerabilities.vulnerability.qualysPatchable: TRUE would generate incorrect output.
- Previously, when the user downloaded the CSV report from the Vulnerabilities tab of the VMDR application, the generated downloaded report did not display any results. The issue is fixed now.
- In some QIDs, the user encountered discrepancies with the Change Log section of the Knowledgebase and Modified Dates of the Vulnerabilities tab in the VMDR application. We have fixed this issue, and the data is in sync.
- We have fixed the issue where even though the user excluded the Non-Running Kernel count for vulnerabilities in the trending widget, the search result would include the Non-Running Kernel results.
- The Customized Solution comments in the General information of Vulnerabilities details page have been enhanced to show HTML content (without converting special characters ('<', '>') into code annotations ('<', '>').
- Previously, when the user ran the QQL for a particular vulnerability severity, the search results displayed vulnerabilities with different severities. Now the QQL returns vulnerabilities with the correct severity.

WAS Web Application Scanning

- We have fixed an issue where the HTML, PDF, and PPT WAS Reports did not have the Qualys logo.
- We fixed an issue for an error occurrence faced by the user at the time of removing a web application.
- We have fixed an issue in a scan report with multiple scans where the user encountered incorrect status for vulnerabilities.
- We have fixed an issue where the user could not create the scorecard reports when specific QIDs were reported in detection.
- We have fixed an issue where the user encountered a discrepancy in the number of web applications in Web Applications Scanning (WAS) and Global Asset View (GAV) or CyberSecurity Asset Management (CSAM) application.