

Qualys Global AssetView/CyberSecurity Asset Management v2.x

Release Notes

Version 2.16 August 30, 2023 (Updated on October 16, 2023)

What's New

Here's what's new in Global AssetView/CyberSecurity Asset Management 2.16!

CSAM CyberSecurity Asset Management

Third-party Asset Import CSAM EASM Toggle New QQL Tokens New Optional Setting in EASM Profile Configuration Domain and Organization Validation Enhancement Asset Open Ports Details Report

GAV CSAM Global AssetView/CyberSecurity Asset Management

Purge Assets Identified by Third-Party Connectors Activate Assets for VM, PC, and CERT Modules View Assets Activation History New Option in the Purge Rule Creation

Global AssetView/CyberSecurity Asset Management 2.16 brings you many more improvements and updates! Learn more

Third-party Asset Import CSAM

With this release, we introduced a new feature, "Third-Party Asset Import", to enhance Qualys assets data with the third-party data connectors. With this feature, you can identify the third-party assets scanned by various connectors, such as Webhook, Active Directory, and ServiceNow, and import them to CSAM.

Note: The "Third-Party Asset Import" is a new feature in the Beta phase. It's in the early stage and only available on a request basis. Contact your Technical Account Manager (TAM) for more information.

To understand the end-to-end feature workflow, refer to the Online Help.

The takeaway of this feature is that all third-party assets or data are merged with Qualys assets, or new unmanaged assets are created, and you get visibility on how assets are deduplicated.

Out-of-the-box Third-Party Connectors

Having a reliable and comprehensive inventory of all your assets is essential to manage your IT assets effectively. Using the third-party data connectors, you can find your non-agent or non-scanner assets unavailable in Qualys and create unmanaged assets in Qualys. You can then add them to your vulnerability management program.

Qualys connectors enable continuous visibility and security across all your cloud environments. You can configure your connector and discover assets in your cloud account. Connectors integrations let you create connectors for third-party services, discover resources, and pass the information to the required Qualys modules, such as CSAM.

Connectors \vee	CONNECTORS SCANS APPLIANCE	E E	3 🕐 🎦
Connectors Cloud Integrations			
Connector Type: Ticketing Service Connector Count Enabled for Modules 3 Manage Connectors	Connector Type Inventory Connector Count Evabled for Modules 51 Manage Connectors	Connector Specific Inventory Connector Count Enabled for Modules 3 Manuage Connectors	
Active Directory Connector Type: Inventory Connector Count Enabled for Modules 0 CSXX Manage Connectors			

- **Webhook:** The Webhook connector lets you connect and discover assets of third-party inventories. You can then view the discovered assets in the CSAM application. The CSAM APIs are required to establish a connection with any third-party service. In the case of Webhook connectors, you must send the API request to identify or discover the assets and bring them to the CSAM inventory. For more information, refer to the *Import Third-Party Assets* section from the API v2 User Guide.

- **Active Directory:** The Active Directory connector lets you fetch the assets data from your AD server. The connector then passes this data to the CSAM application.

- **ServiceNow:** The ServiceNow Inventory connector lets you connect and discover resources of ServiceNow inventories. You can then view the discovered assets in the CSAM application.

To know about how to create connectors, refer to the Connectors online help.

Asset Identification Rules

Go to the **Configuration** > **Asset Identification Rules (Beta)** tab to identify and import the third-party assets.

You can create asset identification rules by selecting the required identification attributes and connector sources to import the assets to CSAM. For more information, refer to the Online Help.

Cybe	rSecur	ity Asset Management 🖂	DASHBOARD	INVENTORY	TAGS	RESPONSES	RULES	REPORTS	CONFIGURATION		8 @ 🗹
Cont	igurat	ion EASM Configuration Asset Identification Rules (Beta)]								
٩	Search	la.									0
0	Acti	ons (0) V Create New Bule Reorder									1-5 of 5 🔇 🖒 💍
	ORDER	RULE NAME	IDENTIFICATION ATTRIBUTE					SOURCES	CONNECTOR	CREATED	UPDATED
	1	InstanceUUID Rule	Instance UUID					ALL	ALL	SYSTEM 7 hours ago	Automation 7 hours ago
	2	Serial Number Rule	Serial Number					ALL	ALL	SYSTEM 7 hours ago	Automation 7 hours ago
	3	Hostname Rule	Hostname					ALL	ALL	SYSTEM 7 hours ago	Automation 7 hours ago
	4	IP and Mac Rule	MAC Address IP	Address				ALL	ALL	SYSTEM 7 hours ago	Automation 7 hours ago
	5	IP Rule	IP Address					ALL	ALL	SYSTEM 7 hours ago	Automation 7 hours ago

Reconciliation Rules

The **Reconciliation Rules (Beta)** are essential when you want to merge assets that come from Qualys native sensors like Qualys agent or scanner when there are assets already identified by the third-party sources before they are discovered again through a different schedule.

Go to **Rules** > Reconciliation Rules (Beta) tab. You can configure the **On Demand** or **Recurring Reconciliation Rule** and merge such assets. For more information, refer to the Online Help.

CyberSecurity Asset Ma	nagement 🗸		DASHBOARD I	INVENTORY TAGS	RESPONSES RULES	REPORTS	CONFIGURATION	8 (2 1159
Rules	Software Rules	Asset Purge Rules Reconciliation Rul	es (Beta)						
									Ç
NAME	TYPE	CREATED ON	UPDATED ON	LAST EXE	CUTED ON	NEXT EXECUTION	ASSETS RECONCILED ①	TOTAL ASSETS RECONCILED ①	
Reconciliation Rule	Schedule	May 31, 2023 02:18 PM	Jul 20, 2023	Jul 24, 2	2023 M	Jul 25, 2023	0	29	
Quick Actions									
Configure									
Run Now									

You can also purge assets discovered by third-party connectors, such as Webhook, ServiceNow, and Active Directory connectors.

CSAM EASM Toggle CSAM

Before the CSAM 2.16.0.0 release, **EASM** and **Inventory** tabs were available. You could see assets with all inventory sources, including EASM from the **Inventory** tab and assets with EASM as one of the inventory sources tagged with the EASM tag from the **EASM** tab.

Considering the scope of future enhancements, multiple tabs might be added under both the **EASM** and **CSAM** tabs. Hence, with the CSAM 2.16.0.0 release, we replaced both these tabs by introducing a **CSAM EASM** toggle for easy navigation.

Click the **Inventory** tab, and you can see the **CSAM EASM** toggle. By default, the toggle is set to show the CSAM assets. You can see the respective asset inventory by turning the toggle to CSAM or EASM. The rest of the functionality remains the same.

CyberSecurity Asset Mana	gement V DASHBOARD INVENTORY TAGS	RESPONSES RULES REPORTS CONFIGURATION	⊘ ⊠
CSAM EASM	Assets Software Web Applications		
	Q Search for assets	() Last 30 Days ~	- ≡
2.18K Total Assets	913 410 Newly Discovered O EOL/EOS Software		
HOSTING CATEGORY	Actions (0) V Group Assets by V All Managed Unmanaged	1 - 50 of 2179 < 🔉 🕁 💍	M ()
OnPrem 1.05K CDN 779	ASSET GRITICALITY ① Trufkisk TM Soure ③ OPEN PORTS	ISP DOMAIN SOURCES () MODULES TAGS	
Unknown 145 ThirdParty 92 Cloud 58	64.39.100.33 4 0 TCP 443 64.39.100.33	QUALYS, Inc	
ORG/SUBSIDIARY Qualys, Inc 2.06K	64.39.100.52 4 0 TCP 443 64.39.100.52	QUALYS, Inc (%) Internet Fa	acing A
Blue Jay Acquisit 54 SSL Labs 17 Adya, Inc 2	investor.qualys.com 3 0 TOP 443 2600:1417.a000.3s4:0:0:20:1	Akamal Internatio investor.qualys.com (%) Trist Found:() Last Seen: Jul	æTagset
2 2 more ⊗	64.39.98.112 4 0 UDP 123 64.39.98.112	Oracle Corporation - Similar Composition - Similar Composition - Similar Composition - Simon Composition -	acing A

For example, when you toggle to **CSAM** and click the asset from the CSAM inventory list, you are redirected to the **Asset Summary** tab from the "Asset Details" page. When you toggle to **EASM** and click the asset from the EASM inventory list, you are redirected to the **External Attack Surface** tab from the "Asset Details" page.

New QQL Tokens CSAM

You can use the following new QQL tokens from the **Inventory** tab. For more information, refer to *Search Tokens for IT Assets*.

Token Name	Description
connectors.connectorId	Find assets sourced from a specific connector created by the user.
	Note: This token is for the "Third-Party Asset Import" which is a new feature in the Beta phase. It's in the early stage and only available on a request basis. Contact your Technical Account Manager (TAM) for more information.
connectors.firstDiscovered	Identify when findings were first discovered.
connectors.lastDiscovered	Identify when findings were first discovered.

You can use the following new QQL tokens from the **Asset Identification Rules (Beta)** tab. For more information, refer to *Search Tokens for IT Assets*.

Note: These tokens are for the "Third-Party Asset Import" which is a new feature in the Beta phase. It's in the early stage and only available on a request basis. Contact your Technical Account Manager (TAM) for more information.

Token Name	Description
ruleName	Get the asset identification rules by providing the
	exact rule name or a fragment of the rule name.
identificationAttribute	Get the asset identification rules created by using
	the specified attribute.

New Optional Setting in EASM Profile Configuration

A new optional setting, **Add Internet-facing tagged assets to EASM discovery scan**, is added to the EASM profile configuration.

Qualys. Express									Qualys.	
CyberSecurity Asset Management V DASHBOARD INVENTORY TAGS RESPONSES RULES REPORTS CONFIGURATION										
Configuration	EASM Configuration Asset Ident	ification Rules (Beta)								
				J						
	Subsidiaries Enumeration Horizontal Domain Enumeration									
	+ Add Filters									
	+Add Section									
	Exclude									
			+ Add	I Exclusion						
	Optional Setting									
	Add Internet-facing tagged asse	ets to EASM dis	covery scan							
	Toggle to add your internet-facing tagged assets to your EASM discovery scan.									
	Cancel Update									

Typically, when you source the data from our EASM third-party sources, all the internetfacing assets might not be available for various reasons. For example, only the Internetfacing asset allowed by firewalls is accessible to Qualys scanners, or your Internet-facing assets don't have enough attribution, like an associated domain, subdomain, or organization ASN. If so, the EASM third-party sources cannot discover such assets out of the box. In such a scenario, if you turn the toggle on, such IP addresses are considered part of your EASM discovery process. After the sync, you can see the External Attack Surface details on the "Asset Details" page.

When you turn the toggle off, all the internet-facing tagged asset information related to EASM, like tags and sources, is deleted from the "Asset Details" page.

Domain and Organization Validation Enhancement

Before the CSAM 2.16.0.0 release, you could see the organization and domain details after the successful Domain and Organization validation.

With the CSAM 2.16.0.0 release, the Organizations and Primary Domains popup is enhanced to provide the details under the **CATALOG** and **ENUMERATED DOMAINS** tabs.

Orga	anizations And Primary Dor	mains	Org	Organizations And Primary Domains					
CATALO	ENUMERATED DOMAINS		CATA	LOG ENUMERATED DOMAINS					
		4							
SR NO	ORGANIZATION	DOMAIN	SR NO	ORGANIZATION	DOMAIN				
1	Qualys, Inc	qualys.com	1	Qualys, Inc	qualys.com				
2	Qualys Test	qualys.com	2	Qualys Test	qualys.com				
3	Qualys, Inc	qualystest2.com	3	Qualys, Inc	qualystest2.com				
4	Qualys, Inc	qualystest1.com	4	Qualys, Inc	qualystest1.com				
5	Nevis Networks	nevisnetworks.com	5	Qualys, Inc	qualyschina.cn				
6	Blue Jay Acquisition Sub, Inc.	blujaysolutions.com	6	Blue Jay Acquisition Sub, Inc.	kewill.fr				
7	TotalCloud, Inc.	totalcloud.io	7	Second Front Systems	secondfront.com				
8	Layered Insight, Inc.	layeredinsight.com	8	Qualys, Inc	qualysguard.jp				
9	Netwatcher	netwatcher.com	9	Qualys, Inc	secblog.net				
10	Spell Security Pvt. Ltd.	spellsecurity.com	10	Qualys, Inc	qualys.in				
11	Blue Hexagon	bluehexagon.ai	11	Qualys, Inc	qualys.io				
12	Second Front Systems	secondfront.com	12	Qualys, Inc	securityvibes.biz				
CI	ose		c	lose					

You can see a list of domains and organizations available in the EASM catalog DB from the **CATALOG** tab.

You can see other associated domains and subdomains through horizontal enumerations and WHOIS DB From the **ENUMERATED DOMAINS** tab. The input source is the catalog DB or user-provided input.

As a result, you can differentiate between the data from our catalog and WHOIS.

Asset Open Ports Details Report CSAM

You can now create an Asset Open Ports Details report. Go to **Reports** > **Create Report** > **Asset Open Ports Details** to create the report and get the details, such as open ports, protocol, description, detected service, IP address, etc., for the selected assets. For more information, refer to the Online Help.

CyberSecurity A	sset Mana	gement	~	1	DASHBOARD	INVENTORY	TAGS	RESPONSES F	ULES	REPORTS	CONFIGURATION				8 @	
Reports		Reports	Schedules													
400	,	Q	Search for Reports												0	=
482 Total Repor	ts		Actions (0) 🗸	Create Report 🗸 Create In	teractive Report									1 - 50 of 482	()	Ø
			REPORT NAME	Asset Details	REATED BY			CREATED ON	TEMPLA	TE		TYPE	STATUS			
TYPE			Report_2307240235 Desc_230724023556756	Software Details Missing Software Details	uays_bb78			24 July, 202: 02:37 PM	AWS	Details		On Demand	Complete	1		
On Demand	318		componentsType	Asset Open Ports Details	uays_yx16			22 July, 202 01:00 AM	Softw	vare Details		Scheduled	Complete	1		
TEMPLATE			applicationType	Cloud Details >	Jays_yx16			21 July, 202 05:38 PM	Softw	vare Details		On Demand	Complete	1		
Asset	164		allType	Externally Exposed Asset Details >	uays_yx16			21 July, 202 05:37 PM	Softw	vare Details		On Demand	Complete	1		

Purge Assets Identified by Third-Party Connectors GAV CSAM

With the introduction of **Add Other Sources** criterion to Create Asset Purge Rule workflow, you can now purge assets discovered by third-party connectors, such as Webhook, ServiceNow, and Active Directory connectors.

Note: You cannot add other purge criteria with the "Add Other Sources" criterion.

For more information, refer to the Online Help.

_	Add Cloud Agent-Based Criteria For deletion of the Cloud Agent-Based assets.
\bigcirc	Add Cloud Provider Metadata-Based Criteria For deletion of the Cloud Provider Metadata-Based assets.
Q	Add Scan-Based Criteria For deletion of the Scan-Based assets.
	Add Time-Based Criteria For the deletion of assets based on the selected time criteria.

Activate Assets for VM, PC, and CERT Modules GAV CSAM

You can activate your assets discovered through sources such as EASM, PS, and Third-Party for the Vulnerability Management (VM), Policy Compliance (PC), and Certificate View (CERT) modules from CyberSecurity Asset Management (CSAM).

Note: Asset activation is not supported for AWS, Azure, and GCP cloud assets and the QAGENT assets tracking method.

You can activate the asset for an individual or all three modules simultaneously. If you activate the asset for all modules, the **Activate** option is turned off for you. Go to **Inventory** > **Assets** tab and click **Activate** from an asset's "Quick Actions" menu to activate the asset for VM, PC, or CERT modules.

CyberSecurity Asset Mar	nagement \vee	DASHBOARD INVENTO	RY TAGS RESPONSES	8 RULES REPORTS CONF	IGURATION	8 🖓 🖾
CSAM EASM	Assets Software Web Application					
٥	asset.trackingMethod:'WEBHOOK'		TO	P OPERATING SYSTEMS CATEGORIES	× ⑦ Last 30 D	ays 🗸 🔳
Total Assets	0 Unidentified	Unknow	/n	0 Unidentified	8 Windows	
ALE 2 Unknown 1	Actions (1) V Group /	ssets by V All Manage	d Unmanaged		1-9 of 9 🔇 📐	± ८ ⊡ ©
TAGS	ASSE Quick Actions View Details	CRITICALITY ① TruRisk TM Score ①	OPERATING SYSTEM	HARDWARE LAST USE	R SOURCES ① MODULES First Found: Jul 13, 2023 U Last Seen: Jul 13, 2023 Q4:5	TAGS 18 more
parent27031 9 Parent2803 9 Ousing Webbook 9	tesi Add Tags 39.2 Purge Asset 5A:5	5	Unidentified	VMware VMware root	Cound: Jul 07, 2023 Sund: Seen: Jul 07, 2023 07:1	sk1 20 more
Dec12-GAV-byAPI 9 29 more ⊗	WIN 10.1 00:1D:4C:23:B8:C9	4	Onidentified	- adminis abcdef Rockwell	۲۰ (ع) مصر المحمد المحم المحمد المحمد المحم المحمد المحمد ا	sk1 19 more



Enable the toggles next to the respective modules, choose the tracking method, network, and asset group to which you want to assign the asset.

Also, if you want, add a tag to the asset and click **Activate**.

Once you activate the asset for the required modules, the IP address of that asset is added for the respective module scan.

For more information, refer to the Online Help.

View Assets Activation History GAV CSAM

You can view the asset activation history for the asset for which you activated the VM, PC, or CERT modules.

Go to the **Inventory** > **Assets** tab and click **View Activation History** from an asset's "Quick Actions" menu.

CyberSecurity A	sset Mana	gement V DASHBOARD INVENTORY TAGS RESPONSES RULES REPORTS CONFIGURATION	8 @ 🗹
CSAM EAS	SM	Assets Software Web Applications	
2.18 Total Asset	K	Image: Comparison of the state of the st	01 Feb 2023 0 V
MANUFACTURER		Actions (1) V Group Assets by V All Managed 1 - 50 of 2183	I () 🕹 🖒 🖬 🍥
Unidentified	2.17K	ASSET CRITICALITY O THURBA ^{THIN} Schre O OPERATING SYSTEM HARDWARE LAST USER SOURCES O MODI	JULES TAGS
ALE VMware	2	test_hostin/ 158.94177) Outlet Actions 5 Unidentified root _1 == First Found un 07, 2023	CERT Qualys Webl
TAGS sk1	2.18K	64.39.104 Add Tops 4 0 Unidentified - 6/2 East First Found. Jul 17, 2023. 0 64.39.1041 Purge Asset	Parent_1 13 more
parent27031 Parent2803	2.18K 2.18K 2.18K	64.39.98.11 View Activation History 4 0 Undertified - 6/2 - First Found - 1/2 - 7/2 - 2/2 - 1/2 - 2/2	M hostingCate

You can see the activation details, such as the asset ID, activated modules, status, etc.

← View Details: View Activation History							
							Ċ
ASSET ID	ACTIVATED FOR IP	ACTIVATED MODULES	STARTED	UPDATED	STATUS	TRACKING METHOD	
29112445	168.94.117.124	CERTVIEW	Jun 12, 2023 11:32 am	Jul 15, 2023 06:50 am	Success	DNS	
29112445	168.94.117.124	PC	Jun 12, 2023 11:32 am	Jul 15, 2023 06:50 am	Success	DNS	
29112445	168.94.117.124	VM	Jun 13, 2023 06:49 am	Jul 12, 2023 11:19 am	Success	IP	
29112445	168.94.117.123	CERTVIEW	Jun 07, 2023 05:26 am	Jul 12, 2023 11:19 am	Success	IP	

New Option in the Purge Rule Creation GAV CSAM

With this release, a new option is introduced in the Asset Purge Rule creation workflow. When the agent communicates with the Qualys platform after the asset is purged, you can decide if you want the agent to create a new asset or uninstall the agent. This new option has the PORTAL 3.16.1 dependency. For more information, refer to the Online Help.

Note: By default, **Re-provision the agent** is selected, and as a result, the agent creates a new asset. If you select **Uninstall the agent**, the agent is uninstalled from the host. Also, **Re-provision the agent** is selected by default for new and existing rules.

Create Asset Purge Rule				
STIPS 3/4 Basic Details Asset Boope Settings Review and Confirm	Settings Set the asset limit for the asset purge rule. Set Assets are selected within the set asset limit, they are purged. Upon selecting assets beyond the set asset asset limit they are purged. Upon selecting assets beyond the set asset asset limit. Asset Limit* 10000 Choose the action when the agent communicates with the Qualys platform after asset asset is purged. () Reprovision the agent () () Uninstall the agent ()			

Issues Addressed

- We fixed the issue where the connector processing was completed with errors for some of the connectors.
- We fixed the issue where an incorrect version of the Oracle Web Logic server software was shown for an asset on which it's installed.
- We fixed the inconsistency issue regarding how the OS name is shown on the CSAM UI for the Cloud Agent assets.
- We fixed the issue where the QQL query using the asset.cpuCount and processors.numberOfCpu tokens were showing incorrect results.
- We fixed the issue where incorrect hash keys were generated for newly cataloged "Other" software, which caused incorrect normalization of such software as Unknown.
- An issue was observed for a customer with multiple super users, where the EASM summary report notification was sent from the super user who didn't send the generate the report request. We fixed this issue, and upon the EASM summary report generation, the notification is now sent from the super user who generated the report.