



# Qualys Global AssetView/CyberSecurity Asset Management v2.x

## Release Notes

Version 2.14

January 11, 2023

### What's New

Here's what's new in Global AssetView/CyberSecurity Asset Management 2.14!

#### **CyberSecurity Asset Management**

Asset Risk Score Renamed as TrueRisk Score

Added 'Domain/SubDomain' Filter Criterion to Manage EASM Configurations

Added a New 'All Time' Timeframe Option

Added a New 'All Time' Filter

Added Support for EASM Tokens from the Tag Creation Wizard

#### **Global AssetView/CyberSecurity Asset Management**

Web Application Scanning (WAS) Integration with CSAM

Added ICS\_OCA Source Type for ICS Assets

Download Support for Installed Software

Assets Listing and Assets Count Based on User Scope

New tokens

Global AssetView/CyberSecurity Asset Management 2.14 brings many more improvements and updates! [Learn more](#)


## Asset Risk Score Renamed as TrueRisk Score CSAM

With the CSAM 2.14.0.0 release, the Asset Risk Score is renamed as TruRisk Score. As a result, the Asset Risk Score instances from multiple User Interface (UI) pages are renamed with TruRisk Score.

When you go to **INVENTORY > Assets** and **EASM > Assets** tab, you can see the “TruRisk Score” column, previously called “Asset Risk Score”.

The screenshot displays the Qualys Cloud Platform interface for the INVENTORY > Assets section. The main table lists various assets, including 'newVM', 'c5.ca.559e.ip4.static.sl-reverse.com', 'win7patch', and '10.115.78.162'. The 'TruRisk™ Score' column is highlighted with a red box, showing scores like 3, 0, 348, and 345. The 'Managed' filter button is also highlighted with a red box. The left sidebar indicates 90 Total Assets.

The screenshot displays the Qualys Cloud Platform interface for the EASM > Assets section. The main table lists assets such as '169.62.150.13', '158.85.202.196', '51.178.133.187', and 'c5.ca.559e.ip4.static.sl-reverse.c...'. The 'TruRisk™ Score' column is highlighted with a red box, showing scores like 3, 4, 3, and 0. The 'Managed' filter button is also highlighted with a red box. The left sidebar indicates 10 Total Assets.

From the **INVENTORY > Assets** and **EASM > Assets** tab, when you select **All**, **Managed**, or **Unmanaged** and click the info icon  next to the TruRisk Score, the TruRisk score details are shown.

The screenshot displays the Qualys Cloud Platform interface for the EASM > Assets section. A tooltip is shown over the 'TruRisk™ Score' column, providing details on how the score is calculated. The tooltip text is as follows:

**What is TruRisk Score?**  
**TruRisk Score for managed assets**  
This is the overall risk score assigned to the asset based on the following contributing factors:  
a. Asset Criticality Score (ACS)  
b. Risk (QDS) scores for each severity level (Critical [C], High [H], Medium [M], Low [L])  
c. Auto assigned weighing factor (w) for each severity level of QDS

**Formula to calculate the TruRisk Score:**  
$$\text{TruRisk Score} = \text{MIN}(\text{ACS} * (\text{w} * \text{Avg}(\text{QDS})) * \text{np.power}(\text{Count}(\text{QDS}), 1/100) + \text{w} * \text{Avg}(\text{QDS}) * \text{np.power}(\text{Count}(\text{QDS}), 1/100) + \text{w} * \text{Avg}(\text{QDS}) * \text{np.power}(\text{Count}(\text{QDS}), 1/100), 1000)$$

**TruRisk Score**

The TruRisk Score is derived from the business criticality of an asset, its risk factors and its location within the network.

Asset Name	IP	Asset Type	Owner	OS
169.62.150.13	169.62.150.13	HOST	Doctor Strange	Unidentified

**Contributing Factors**

- Business Criticality:** Asset criticality rating 2 out of 5
- Asset Exposure:** Externally Exposed with ip | Internal facing A | Intranet | DMZ
- Risk Factors:** Total 12 Vulnerabilities

**Vulnerabilities**

CVSS  
VDB  
CVE  
CWE  
NVD  
NIST  
OWASP  
SANS  
SECWiki  
TTPs  
WPM

**Formula**

$$\text{TruRisk Score} = \min(\text{Asset exposure}) * ACS * (\frac{1}{\log_2(Avg(QVLS)) + 1}) * \log_{10}(Count(QVLS) / 11000) + \\ m_A * Avg(QVLA) * \log_{10}(Count(QVLS) / 11000) + \\ m_I * Avg(QVLI) * \log_{10}(Count(QVLS) / 11000) + \\ m_E * Avg(QVLE) * \log_{10}(Count(QVLS) / 11000) + 1000$$

NOTE: External assets are weighted 20% higher than internal assets

**Calculation**

$$\text{TruRisk Score (428)} = \min(1+2+3+(1.0+95)*power(1,1/1000)) * (0.6+0+power(1,1/1000)) * ((0.4+41)*power(2,1/1000)) * (0.2+30*power(1,1/1000),1000)$$

**VULNERABILITIES (12)**

CVE	QID	TYPE	SUMMARY
CVE-2015-6111	[H]	Potential	An issue was discovered in OpenSSH 7.5. Due to the app implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the app client only performs syntax validation of the object name returned (only directory traversal attacks are prevented). A malicious app server (or ...)
CVE-2015-6110	[H]	Potential	In OpenSSH 7.5, due to accepting and displaying arbitrary output from the server, a malicious user (or Man-in-the-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.
CVE-2014-23945	[H]	Potential	In OpenSSH 7.5, app in the app client allows remote SSH servers to bypass intended access restrictions via the filename of - or an empty filename. The impact is modifying the permissions of the target directory on the client side.
CVE-2014-1439	[H]	Potential	An issue was discovered in OpenSSH 7.5. Due to missing character encoding in the progress display, a malicious user (or Man-in-the-Middle attacker) can inject crafted object names to manipulate the client output, e.g. by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_re...
CVE-2020-15776	[L]	Potential	= DISPUTED CVE in OpenSSH through Sftp allows command injection in the app's command function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great ch...

For more details, refer to the [Viewing Inventory of External Attack Surface Discovered Assets from the EASM Tab](#) and [TruRisk Score Calculation](#).

With the CSAM 2.14.0.0 release, we have added a new filter criterion, '**Domain/SubDomain**', in global exclusion for managing EASM configurations. By using this criterion, you can exclude the specified Domain/SubDomain of the EASM assets from all the included seeds to manage EASM configurations. Refer to the [CSAM Online Help](#) to learn more details about the filter criteria in External Attack Surface Management (EASM) Configuration.

Qualys Cloud Platform

Manage EASM Configurations

Configure External Attack Surface Monitoring

Use the following filter criteria to import hosts that are externally exposed. [Learn More](#)

Include

Remove All

Type

Value

Domain

sjrb.ca

☐ Subsidiaries Enumeration ☐ Horizontal Domain Enumeration

+ Add Filters

+ Add Section

Exclude

Type

Value

Select Type

Enter Value

-

+

Type

Domain/SubDomain

Organization

Domain/SubDomain

IP/Netblock

City

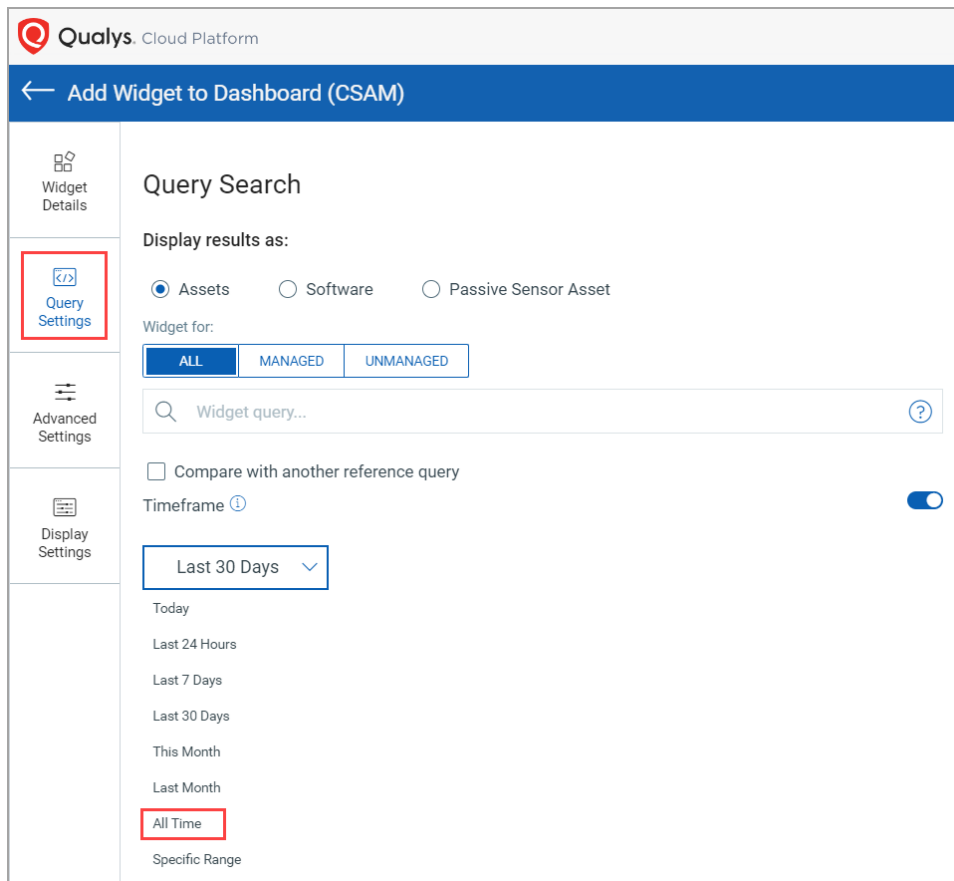
Country

Cancel

Update

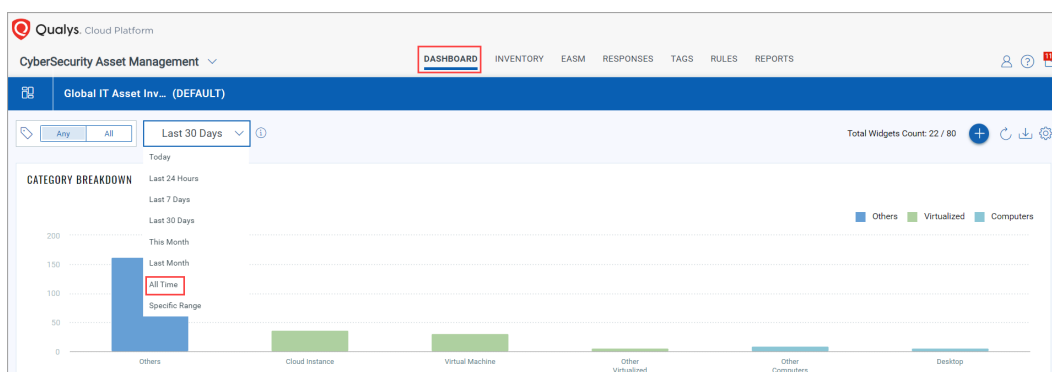
## Added a New 'All Time' Timeframe Option CSAM

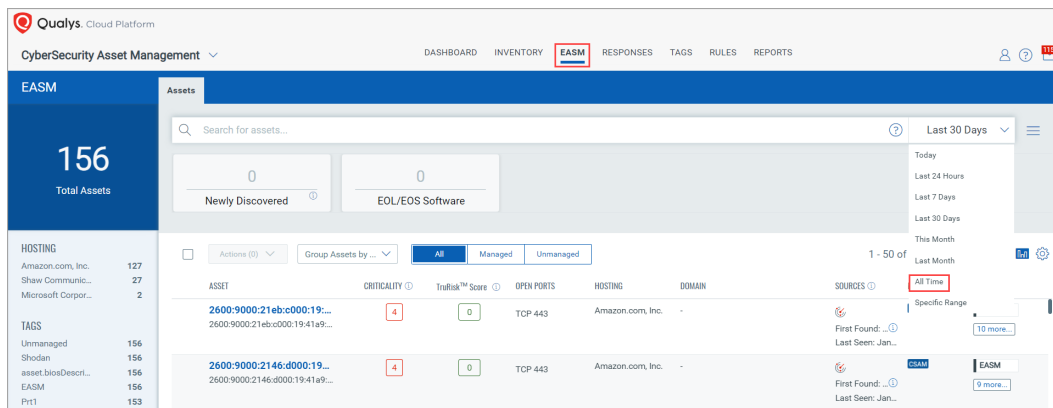
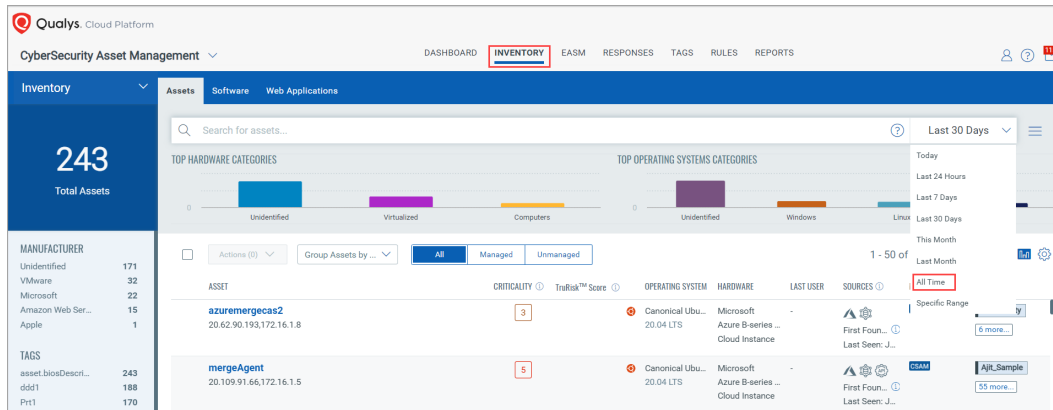
With the CSAM 2.14.0.0 release, we have added a new timeframe filter option, "All Time" to the **Add Widget to Dashboard (CSAM)** page. By applying this filter, you can see all-time data in the widgets.



## Added a New 'All Time' Filter CSAM

With the CSAM 2.14.0.0 release, we have added a new filter called the 'All Time' filter to the **DASHBOARD**, **INVENTORY**, and **EASM** tabs. By applying this filter, the all-time data is shown.





## Added Support for EASM Tokens from the Tag Creation Wizard

Before the CSAM 2.14.0.0 release, you could use the following EASM search tokens from the **EASM**, **INVENTORY**, **TAGS**, and **DASHBOARD** tabs only.

With the CSAM 2.14.0.0 release, you can also use these tokens in the tag creation wizard (Dynamic tag > Asset Inventory rule). For more information, refer to the [Search Tokens for Tag Rules](#) topic from the online help.

- **asset.domain:** This token enables you to find the assets with their domain.
- **asset.subdomain:** This token enables you to find the assets using their subdomains.
- **asset.org.name:** This token enables you to find assets with the organization name you're looking for.
- **asset.isp:** This token enables you to find assets with the Internet Service Provider (ISP) name you're looking for.
- **asset.asn:** This token enables you to find the assets with the ASN value you are looking for.
- **whoIs.registrantEmailId:** This token enables you to find all the assets using the registrant email id of the domain or subdomain.
- **whoIs.registrantOrg:** This token enables you to find all the assets by using the registrant organization of the domain or subdomain.
- **whoIs.registrar:** This token helps you to find all the assets using the registrar.

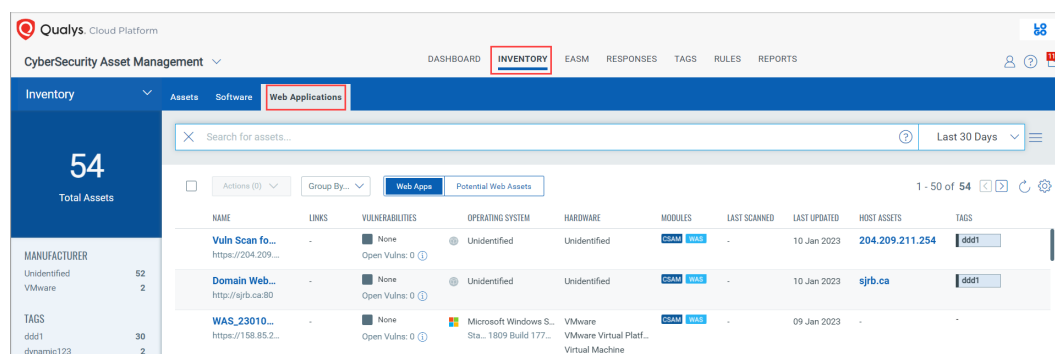
## Web Application Scanning (WAS) Integration with CSAM GAV CSAM

With the CSAM 2.14.0.0 release, we have introduced WAS integration with CSAM. With this integration, you can identify and manage security risks and vulnerabilities in web applications and APIs anywhere and anytime.

### Prerequisite:

WAS must be enabled for you. To get it enabled, contact Support.

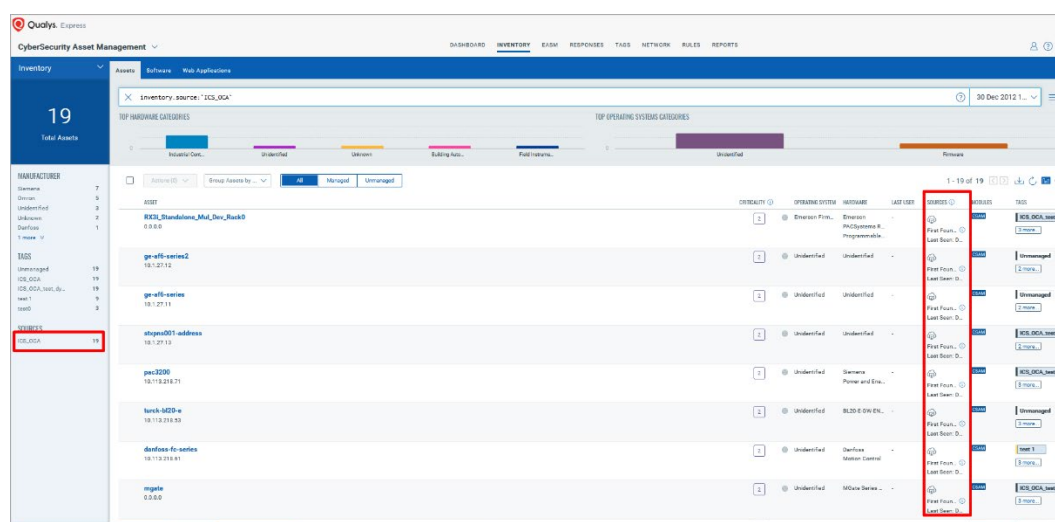
A new tab **Web Applications** is added. After WAS is enabled for you, you can create Web apps, activate WAS on the potential Web Assets, and deactivate WAS from the Web App. To know more details, refer to the [online help](#).

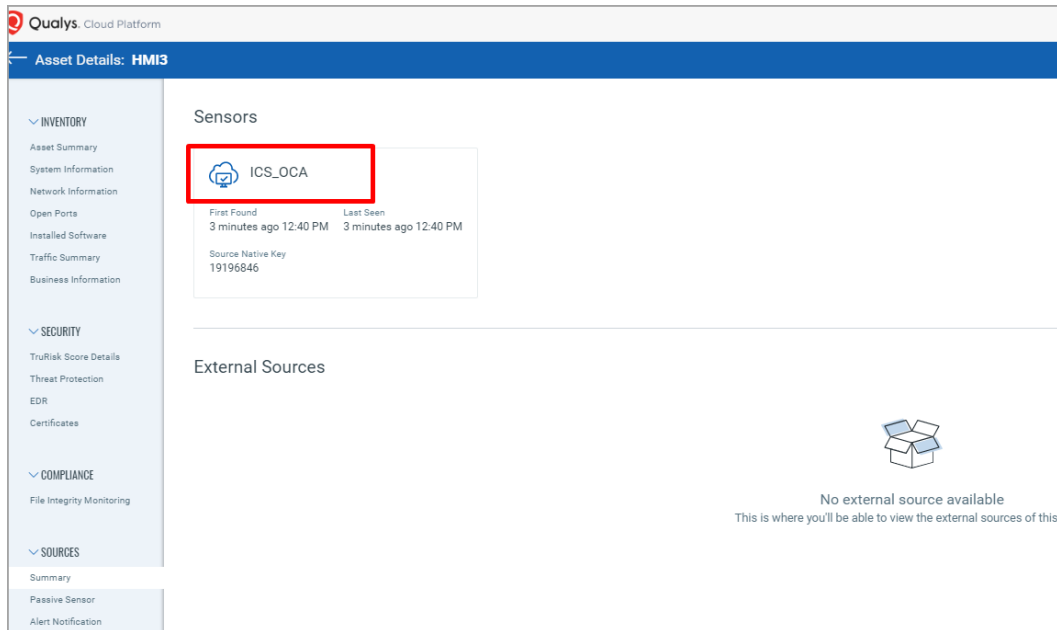


## Added ICS\_OCA Source Type for ICS Assets GAV CSAM

With the CSAM 2.14.0.0 release, we have added the ICS\_OCA source type for ICS assets. You might notice a discrepancy in the counts of assets with the ICS\_OCA tag and assets with the ICS\_OCA source. This is because the source tracking of assets imported from project files is changed to ICS\_OCA from PASSIVE\_SENSOR.


**Note:** This change does not automatically apply to assets imported earlier. It applies to only the assets imported from project files after that. To correct the discrepancy, delete the project files and upload them again.

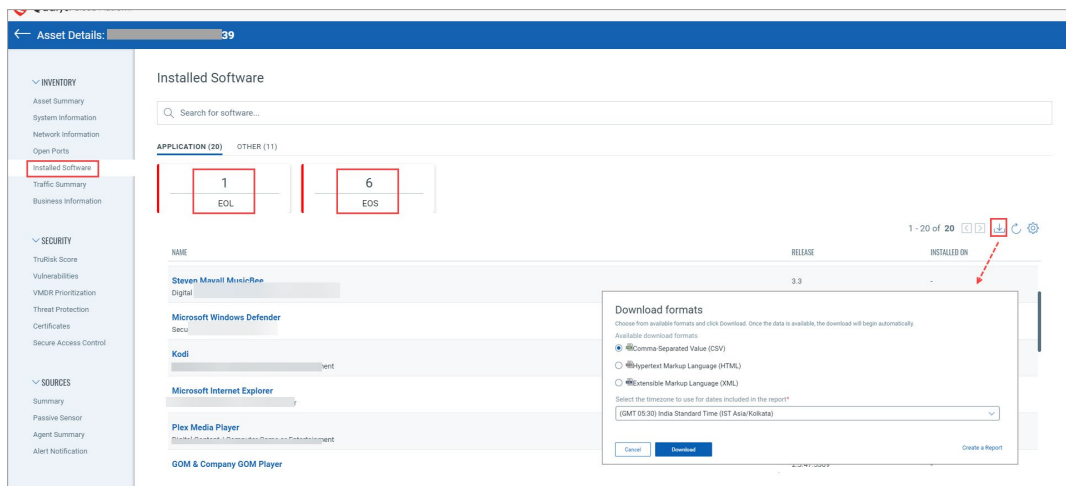




## Download Support for Installed Software GAV CSAM

With the CSAM 2.14.0.0 release, you can now download details about the software in the Application/Others category installed on the asset from the Installed Software page. From the downloaded report, you can identify the software version, end of license date, etc.

To download the report, from the Asset Details page, click the **Installed Software** tab and click the download  icon.

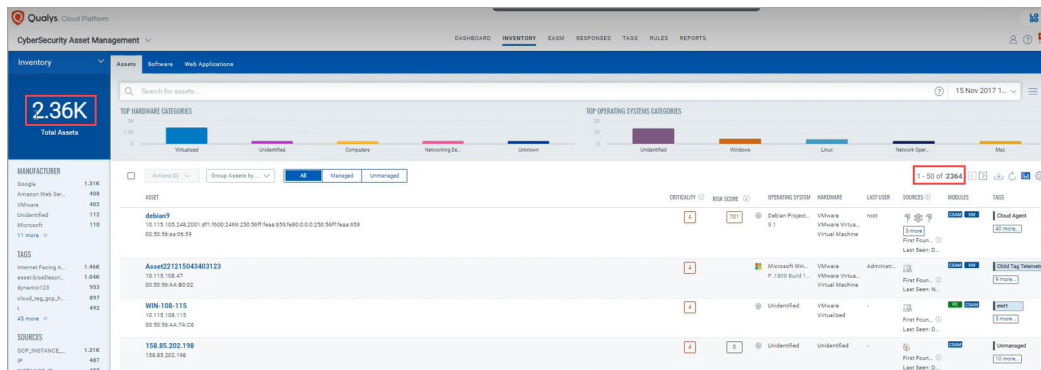


## Assets Listing and Assets Count Based on User Scope GAV CSAM

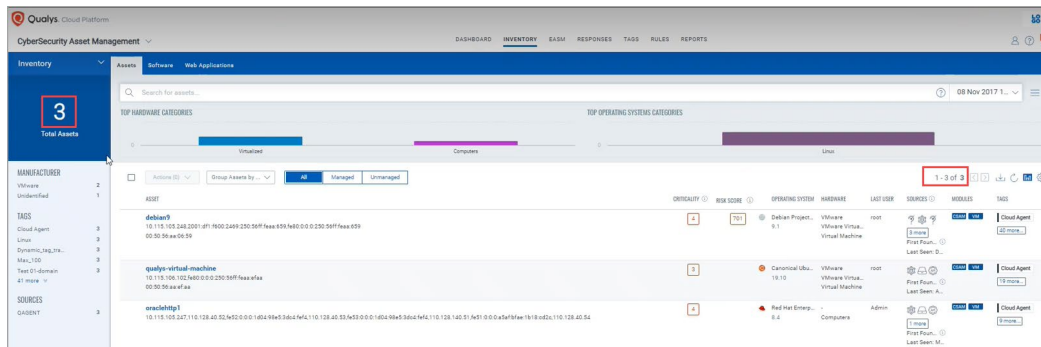
The assets list and count are now shown based on the scope defined for the respective user. After the scope is defined for a respective user, that user can access only the assets, which are tagged by the specified tags.

**Note:** Before the CSAM 2.14.0.0 release also, it was possible to define the user scoping for the public V2 APIs only, and the assets list and count were shown based on the scope defined for the respective user.

Hence, though there is no change in the user experience, with the CSAM 2.14.0.0 release, the user scoping can be defined for the public V1 APIs too, which is noteworthy. For more information, refer to the [API Release Notes](#).



**Note:** See the following screen capture, wherein the assets associated with only the “Cloud Agent” tag are in scope for this user, and hence, only those assets are shown on the UI.



## New tokens

With the CSAM 2.14.0.0 release, you can use the following new WAS tokens from the **INVENTORY > Web Applications** tab:

- **asset.links:** This token enables you to filter web assets based on crawled links.
- **asset.url:** This token enables you to filter web assets based on the IP, domain, subdomain, or URL used during Web Application creation.



## Issues Addressed

- A discrepancy was found in the assets count when trending was enabled. The assets count shown in the CSAM widget and the assets count shown on the Inventory page were different. The issue was observed because though no timeframe was selected, the 30 days timeframe was considered when showing the data on the Inventory page, which led to this discrepancy. With this release, we fixed this issue by adding the "All Time" timeframe on the Trending widget, which is the default timeframe. Thus, when no timeframe is selected, results from the trending widget also show all-time data.
- An issue was observed where an incorrect result was shown when the user changed the timeframe from enable to disable for the trending widget. We have now fixed the issue, and the correct result is shown. This issue might exist in the case of the previously added widgets. To fix the issue, either edit and save the impacted widgets or delete the impacted widgets and new ones.
- An issue was observed where, upon the expiry of the GAV license, the GAV-specific dashboard was no more available for the user. We have now fixed this issue, and as a result, though the GAV license expires and changes from full to free, the default GAV-specific free dashboard will be available for the user.
- An issue was observed where, though a higher central API subscription was purchased, and the user upgraded the CSAM subscription from free to trial from the CSAM UI, the concurrency limit and rate limit was set based on the default trial version API subscription instead of the central API subscription. Now, these subscriptions are compared first, and the higher one is considered to set the concurrency and rate limits.
- We have fixed the issue where the geolocation automated query didn't provide correct results for the country name that included "and" in its name.
- We have fixed the issue, wherein upon detection of multiple Microsoft Teams versions on the asset, the latest updated version was not shown in the Installed software list of that asset.
- We have fixed the issue observed for the sub-user, wherein upon clicking the "View all" option of the VM widget added to the CSAM dashboard, the VM DR application was not opening.
- We have fixed the issue where the scheduled report creation and saving from only the Firefox browser used to fail.
- We have fixed the issue where a user could not search for assets associated with tag names that included a special character using the tags.name QQL.