Qualys Global AssetView/CyberSecurity Asset Management v2.x

Release Notes

Version 2.13
November 14, 2022

What's New

Here's what's new in Global AssetView/CyberSecurity Asset Management 2.13!

CyberSecurity Asset Management

General Availability of External Attack Surface Management (EASM)
Inventory of Externally Exposed Assets from the EASM Tab
VMDR Activation for Externally Exposed Unmanaged Assets
Asset Risk Score for EASM Unmanaged Assets
Enhancements to the EASM Dashboard
Grouping Externally Exposed assets
New EASM Tokens
Additional Details in Reports Downloaded for EASM Assets
Exclusion of IP Addresses from the EASM Discovery
Addition of a New template to the External Attack Surface Reports

Global AssetView/CyberSecurity Asset Management 2.13 brings you many more improvements and updates! Learn more

Copyright 2022 by Qualys, Inc. All Rights Reserved.

General Availability of External Attack Surface Management (EASM) CSAM

With the CSAM 2.13.0.0 release, External Attack Surface Management (EASM) is now generally available.

Before this release, it was a Beta feature, which was in an early preview.

You can now get visibility in the form of External Attack Surface Management (EASM) that gives an outside-in view of your external-facing IT infrastructure to continuously monitor your organization's external attack surface and internet-connected assets, track changes, and receive notifications when new assets, unknown assets, or critical issues are found.

EASM allows you to continuously identify and assess the security and compliance gaps in your organization’s network.

The following EASM-specific new features are delivered as part of this release:

- Inventory of Externally Exposed Assets from the EASM Tab
- VMDR Activation for Externally Exposed Unmanaged Assets
- Asset Risk Score for EASM Unmanaged Assets
- Enhancements to the EASM Dashboard
- Grouping Externally Exposed assets
- New EASM Tokens
- Additional Details in Reports Downloaded for EASM Assets
- Exclusion of IP Addresses from the EASM Discovery
- Addition of a New template to the External Attack Surface Reports

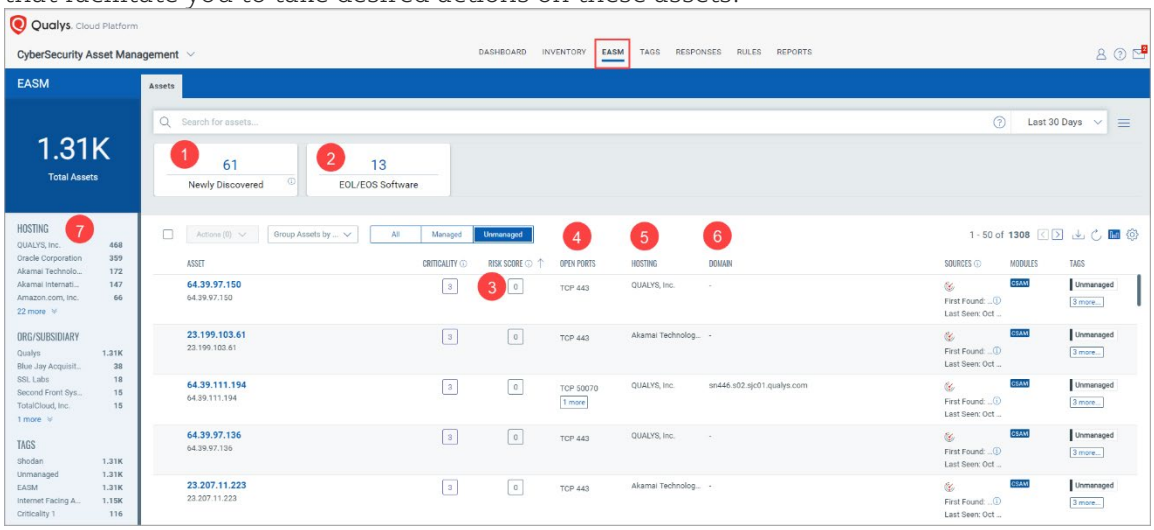
Inventory of Externally Exposed Assets from the EASM Tab CSAM

Before the CSAM 2.13.0.0 release, the externally exposed assets were shown from the **Inventory** tab.

With the CSAM 2.13.0.0 release, we have added a new tab **EASM**. You can now see the externally exposed assets from this newly added **EASM** tab as well.

The **EASM** tab is specifically designed to highlight the metadata of externally exposed assets, such as domains, subdomains, ports, and so on.

From the **EASM** tab, you can find detailed information about the externally exposed assets that facilitate you to take desired actions on these assets.



(1) On the **Newly Discovered** tile, you can see the newly discovered externally exposed assets from the latest scan.
(2) On the **EOL/EOS Software** tile, you can see the count of EOL and EOS software for externally exposed assets.
(3) **Risk Score:** You can see the Asset Risk Score (ARS) for assets on which vulnerabilities are detected.
(4) **Open Ports:** You can see the protocol type and count of open ports for the externally exposed assets.
(5) **Hosting**: You can see the hosting providers' names.
(6) **Domain**: You can see domain and subdomain details of the externally exposed assets.
(7) **EASM-specific quick filters:** In the left pane, you can see the EASM-specific quick filters, such as **HOSTING**, **ORG/SUBSIDIARY**, and **TAGS**.

Note: The inventory of externally exposed assets gets refreshed after every 48 hours.

To learn more about the inventory of externally exposed assets, refer to the Online Help.

VMDR Activation for Externally Exposed Unmanaged Assets CSAM

EASM capability discovers the externally exposed assets that are unknown to you.
Since such assets are not scanned by Qualys VMDR, they are classified as unmanaged assets.
You can see them from the **EASM** tab.

With this release, you can bring these assets to your security assessment program. To do so, activate 'Vulnerability Management, Detection and Response (VMDR)' on such externally exposed unmanaged assets.

Note:

- Only Superusers can activate VMDR on the externally exposed unmanaged assets. Also, VMDR can be activated only if your customer account is AGMS.
- VMDR activation can be done for all assets, except:
  - Managed assets
  - Assets with IPv6 and IP 0.0.0.0 addresses

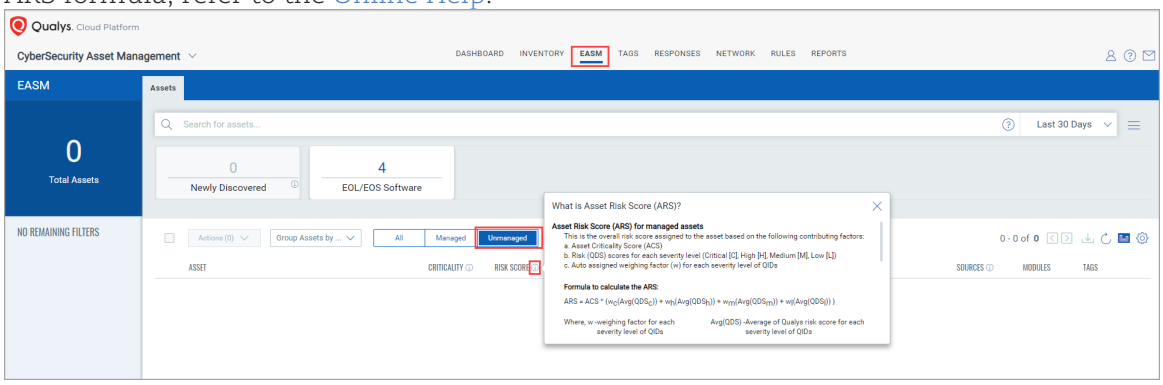
To learn how to activate VMDR on individual and multiple externally exposed assets, refer to the Online Help.

Asset Risk Score for EASM Unmanaged Assets CSAM

Before the CSAM 2.13.0.0 release, the Asset Risk Score (ARS) was calculated for managed assets only.

With this release, we calculate the ARS for externally exposed unmanaged assets too. The ARS for these assets is calculated based on the Asset Criticality Score (ACS) and Qualys Vulnerability Score (QVS). The QVS is calculated based on vulnerabilities that are reported by Shodan.

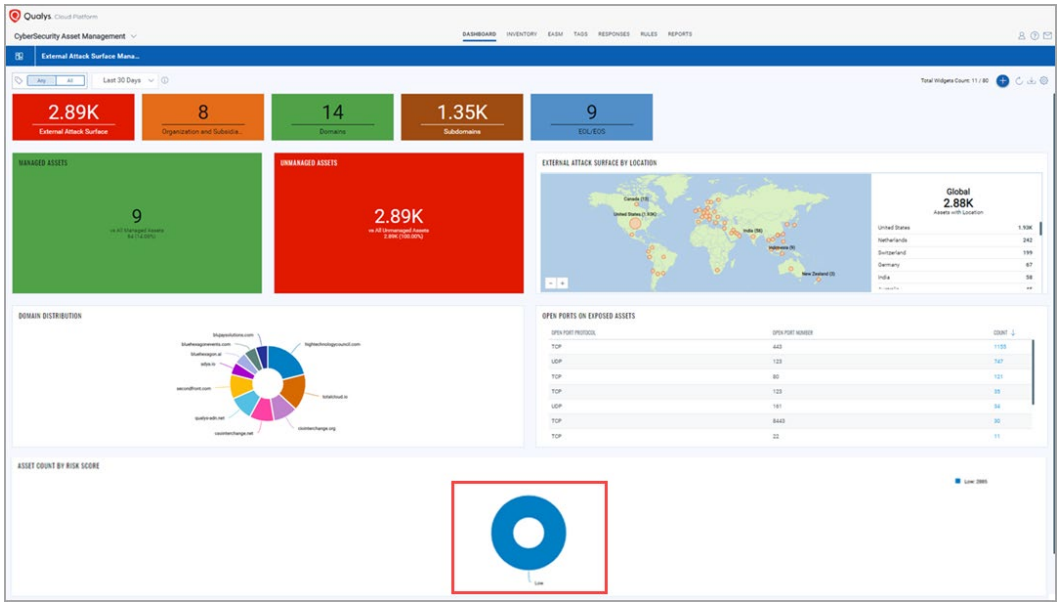
The ARS helps you prioritize the assets that you should consider for VMDR activation. You can view the ARS for **All**, **Managed**, and **Unmanaged** assets from the **EASM** tab. You can see the ARS-related details, such as the ARS formula, contributing factors, and ARS range by clicking the info icon from the Risk Score column. To find more details about the ARS formula, refer to the Online Help.



Enhancements to the EASM Dashboard CSAM

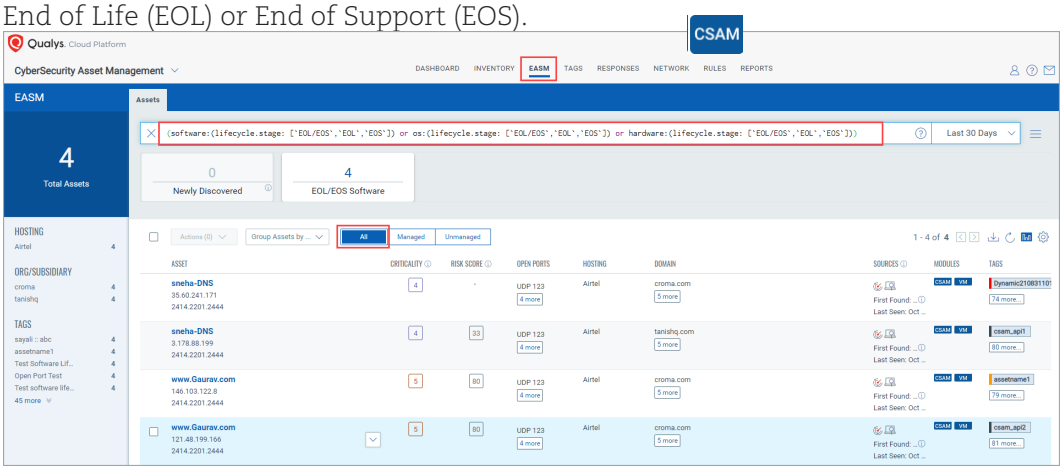
Before the CSAM 2.13.0.0 release, the EASM dashboard template 'EXTERNAL ATTACK SURFACE MANAGEMENT' was in place.

With the CSAM 2.13.0.0 release, we have renamed the EASM dashboard template as 'EXTERNAL ATTACK SURFACE MANAGEMENT(V2)'.



In this template, the following 5 new tiles are added:

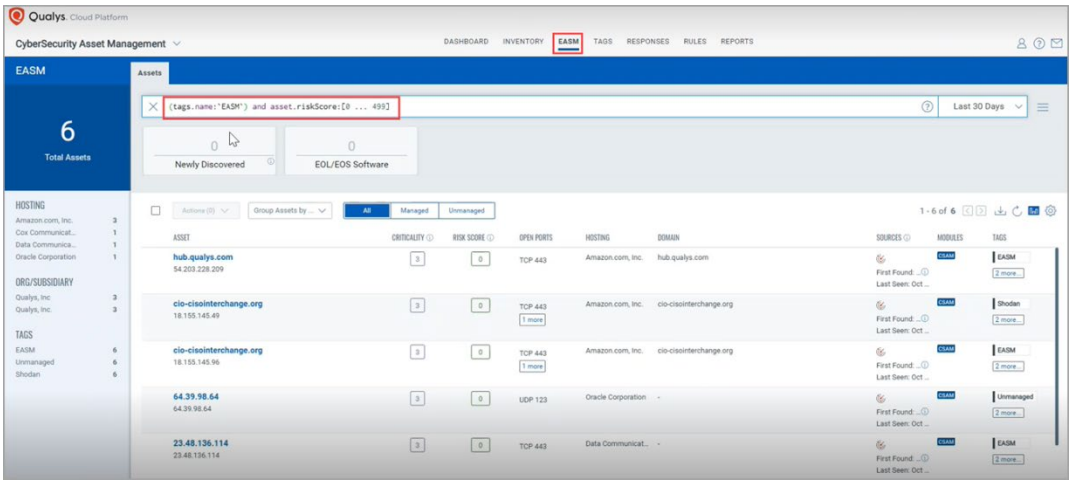
- **External Attack Surface:** When you click the count from this tile, you are navigated to the **EASM** tab with the (tags.name: `EASM`) QQL. The EASM assets are shown based on this QQL.
- **Organization and Subsidiaries:** When you click the count from this tile, you are navigated to the **EASM** tab, and the **Group Assets by : Organization/Subsidiary** query is selected by default.
- **Domains:** When you click the count from this tile, you are navigated to the **EASM** tab, and the **Group Assets by : Domain** query is selected by default.
- **Subdomains:** When you click the count from this tile, you are navigated to the **EASM** tab, and the **Group Assets by : Subdomain** query is selected by default.
- **EOL/EOS:** When you click the count from this tile, you are navigated to the **EASM** tab > **All** assets. The EOL/EOS count includes a count of software, OS, or Hardware that is End of Life (EOL) or End of Support (EOS).



- Asset Count by Risk Score: From the 'Asset Count by Risk Score' widget, you can see the asset count based on the following Asset Risk Score (ARS) range:

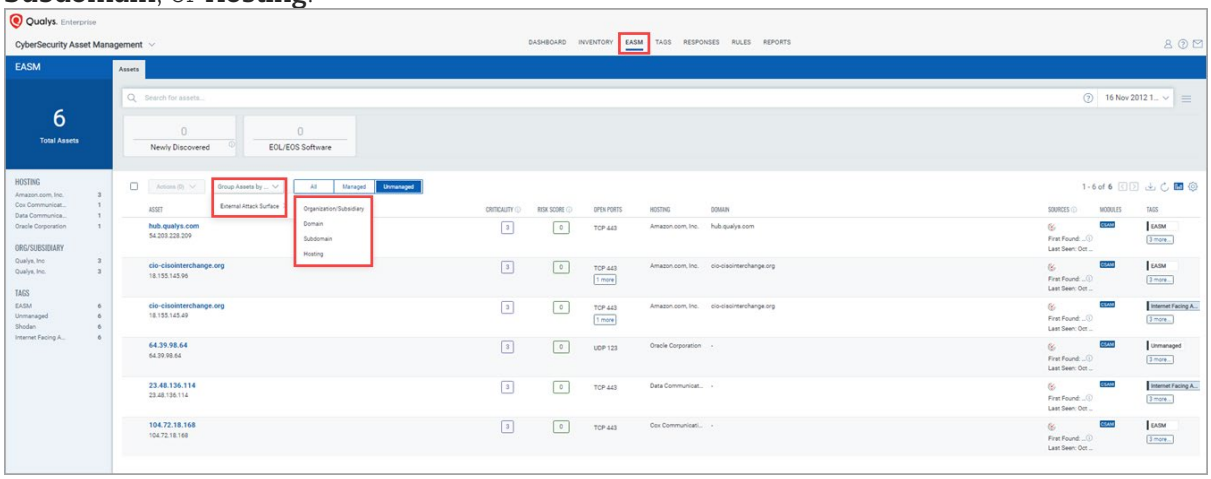
- Low: ARS between 0-499
- Medium: ARS between 500-699
- High: ARS between 700-849
- Severe: ARS between 850-1000

Upon clicking a particular risk score category from the pie chart from this widget, you are navigated to the **EASM** tab, and assets shown based on that particular risk score are shown.



Grouping Externally Exposed assets CSAM

With this release, like the **Inventory** tab, the **Group Assets by** list is now available from the **EASM** tab too. You can now group your assets by **Organization/Subsidiary**, **Domain**, **Subdomain**, or **Hosting**.

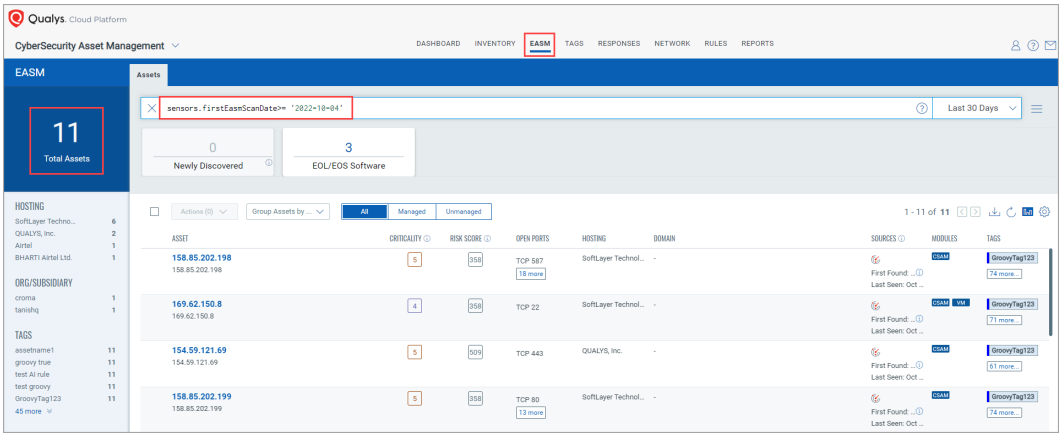


New EASM Tokens CSAM

With this release, we have added two new tokens, ‘sensors.lastEasmScanDate’ and ‘sensors.firstEasmScanDate’. You can use these tokens from the **EASM**, **Inventory**, and **Dashboard** tabs.

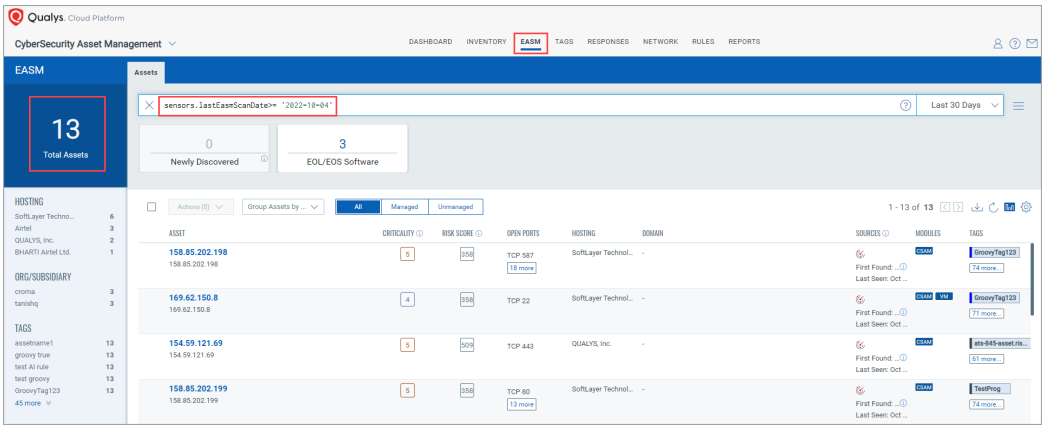
- **sensors.firstEasmScanDate:** This token helps you find the list of externally exposed assets based on their first scan date.

  As shown in the following screen capture, the externally exposed assets are displayed based on the first scan date that you entered. Also, the asset count is shown in the left pane.



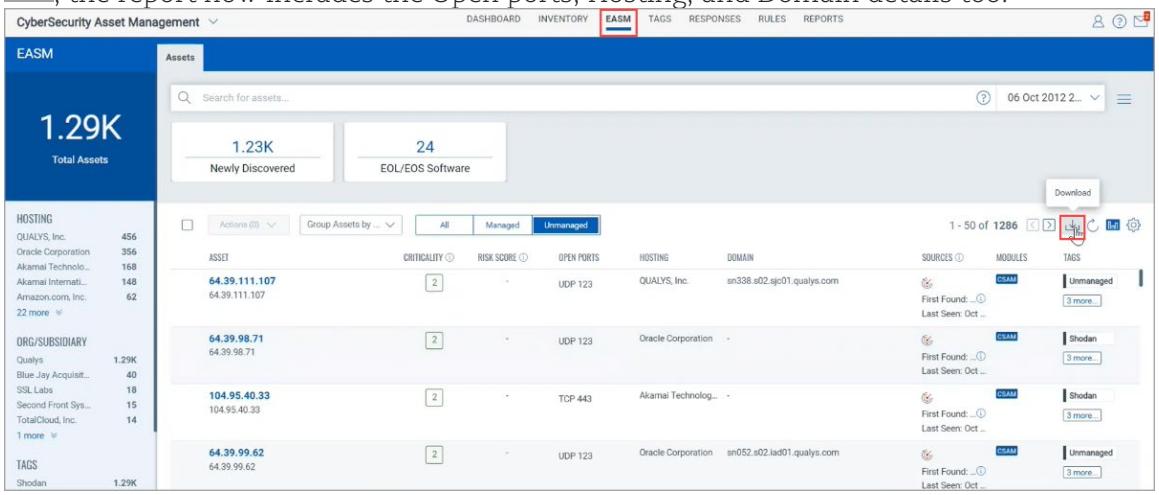
- **sensors.lastEasmScanDate:** This token helps you find the list of externally exposed assets based on their latest scan date.

  As shown in the following screen capture, the externally exposed assets are displayed based on the last scan date that you entered. Also, the asset count is shown in the left pane.



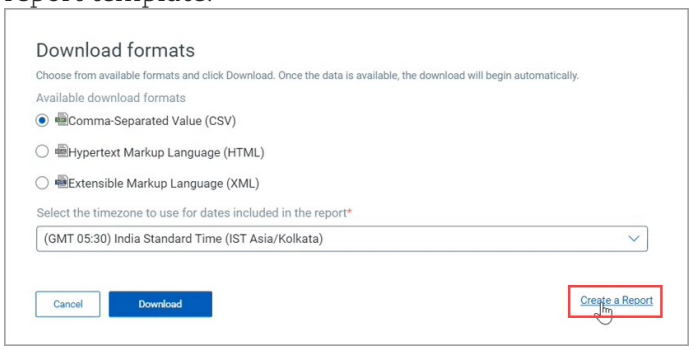
Additional Details in Reports Downloaded for EASM Assets CSAM

With this release, when you download the EASM assets report by clicking the **Download** icon , the report now includes the Open ports, Hosting, and Domain details too.



These details are included in all three (CSV, HTMN, XML) download formats that you select.

When you click a **Create a Report** link, by default, you are navigated to a Domain Details report template.



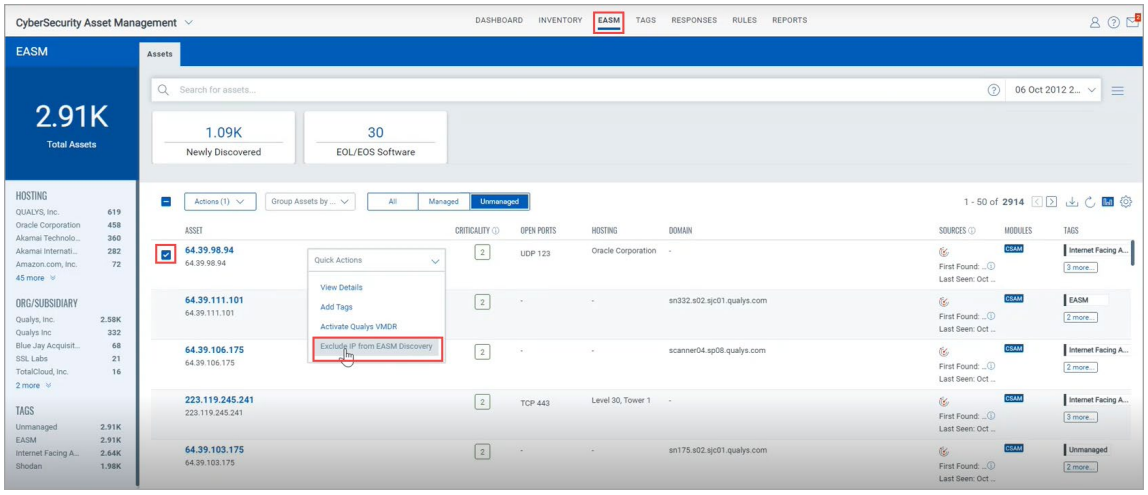
Exclusion of IP Addresses from the EASM Discovery CSAM

With this release, you can now exclude individual or multiple IP (IPv4 and IPv6) addresses for managed and unmanaged assets from the EASM discovery.

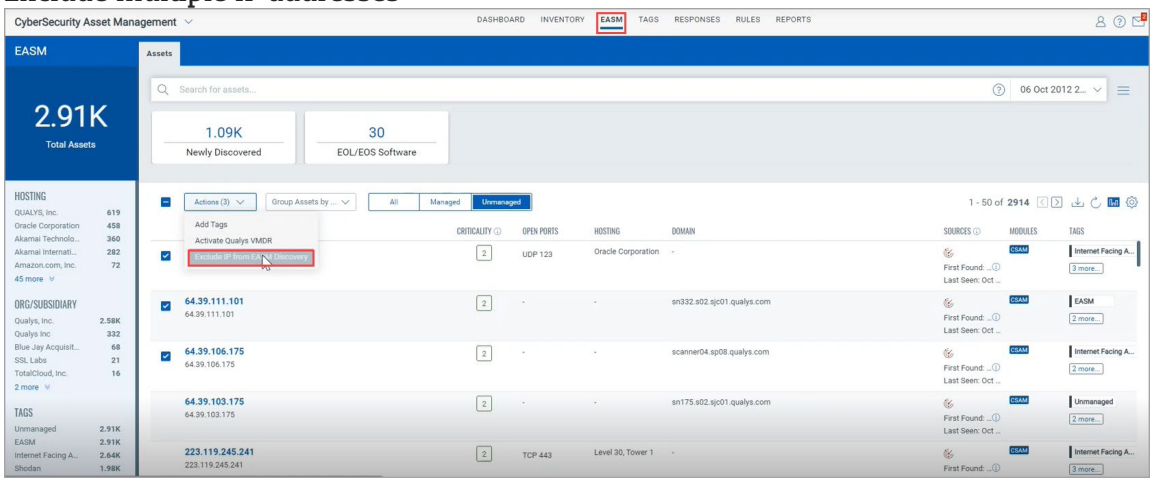
By excluding these IP addresses, you can monitor the most crucial subset of your external attack surface. If you want to include these IP addresses back in the inventory, remove the **Exclude** filter.

Note: Only Superusers can exclude IP addresses from the EASM discovery.

Exclude an individual IP address



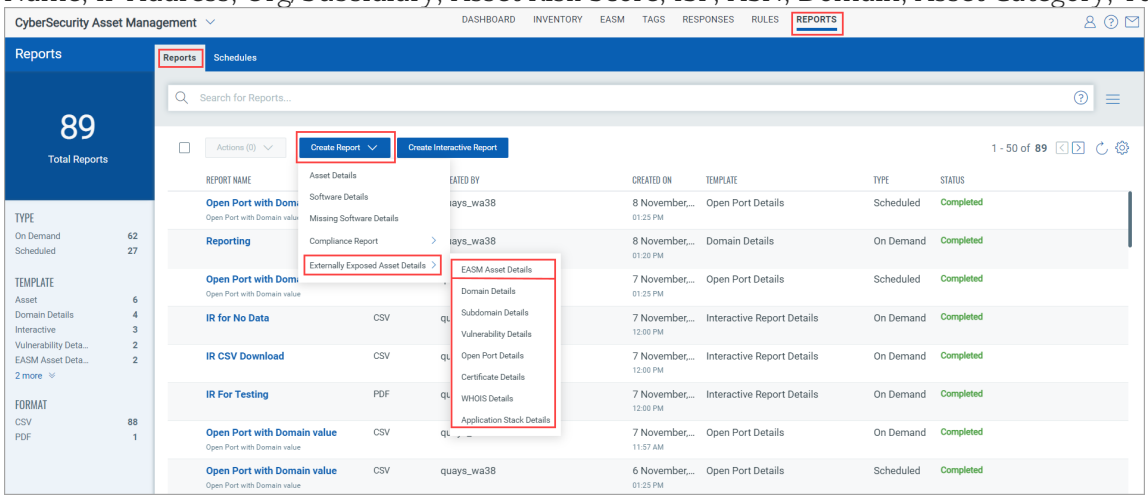
Exclude multiple IP addresses



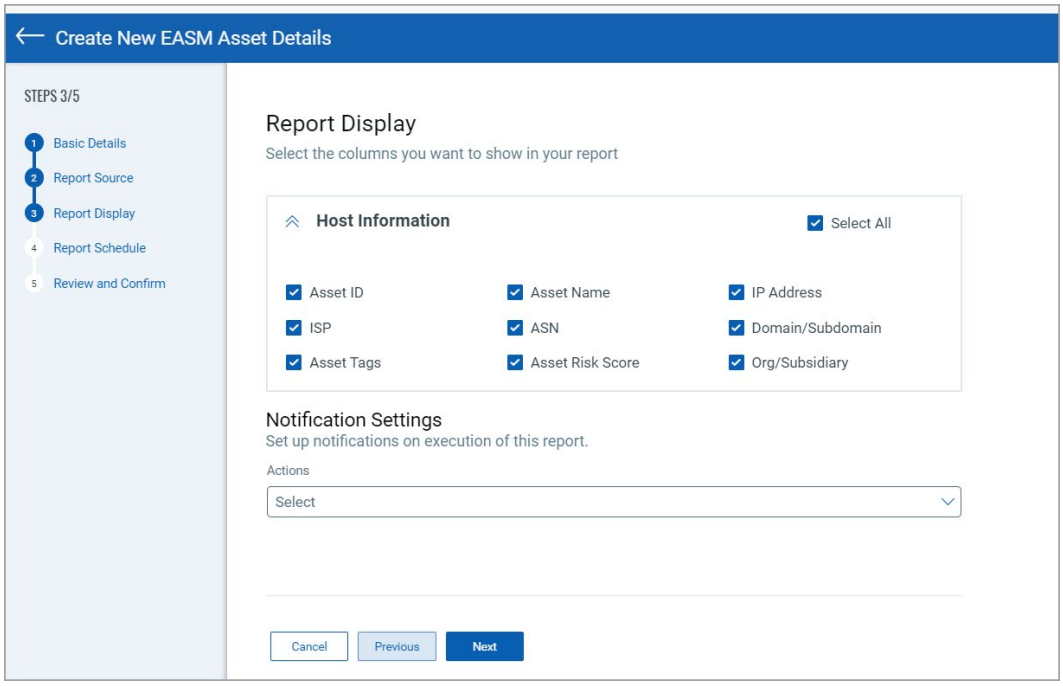
To know more details about how to exclude the IP addresses, refer to the Online Help.

Addition of a New template to the External Attack Surface Reports CSAM

With the CSAM 2.13.0.0 release, we have added an **EASM Asset Details** report template to the **Externally Exposed Asset Details** section. Using this template, you can generate the EASM asset details report, which includes EASM-specific asset details, such as Asset ID, Asset Name, IP Address, Org/Subsidiary, Asset Risk Score, ISP, ASN, Domain, Asset Category, Tags.



Also, new columns, **Asset Risk Score** and **Org/Subsidiary** are added to the Report Display option, which displays the asset risk score and org/subsidiary information in your report.


Create New EASM Asset Details
STEPS 3/5
1 Basic Details
2 Report Source
3 Report Display
4 Report Schedule
5 Review and Confirm
Report Display
Select the columns you want to show in your report
Host Information
Select All
Asset ID
Asset Name
IP Address
ISP
ASN
Domain/Subdomain
Asset Tags
Asset Risk Score
Org/Subsidiary
Notification Settings
Set up notifications on execution of this report.
Actions
Select
Cancel
Previous
Next

Issues Addressed

- We fixed an accessing issue with the "Installed Software" and "System Information" tab through the CSAM module, where the pages were blank and only showed No Records found.

- We fixed an issue where the users saw the slash (/) with the IPV4 IPV6 address (/IPV4 IPV6) in the CSV report downloaded from CSAM.

- We fixed an issue for the Dynamic Tag Rule Engine Asset Inventory for the QQL tokens Operating System and Hardware. The tag was getting toggled in the case of an asset that can be discovered from two different sources, which caused the removal of the tag for a discovered asset that had a particular tag already attached to it.

- We fixed an issue for CSAM widgets trending data by supporting new tokens, wherein the CSAM widgets trendline was showing no trending data.

- We fixed an issue with the create tag API where two dynamic tags, one parent dynamic tag and one child dynamic tag were using the API. These tags are evaluated now.