Qualys Global AssetView/CyberSecurity Asset Management v2.x

Release Notes

Version 2.15.2
June 2, 2023

What's New

Here's what's new in Global AssetView/CyberSecurity Asset Management 2.15.2!

GAV **CSAM** **Global AssetView/CyberSecurity Asset Management**

Introduced Automated External Attack Surface Summary Report

CSAM **CyberSecurity Asset Management**

EASM Summary Report Template
Tag Set Creation

Global AssetView/CyberSecurity Asset Management 2.15.2 brings you many more improvements and updates! Learn more

Introduced Automated External Attack Surface Summary Report `GAV` `CSAM`

With this release, we have provided support to generate an automated, on-demand external attack surface summary report. Contact your Technical Account Manager (TAM) for the EASM summary report.

From the external attack surface summary report, you get an insight into the risk of internet-facing assets, cloud instances with risk, top risky domains, subdomains, open ports, and so on.

This insight enables you to secure your internet-facing assets using other Qualys products, such as Vulnerability Management, Detection and Response (VMDR), and Web Application Scanning (WAS).

- If you are a Global Asset View (GAV) user, the CSAM trial is activated, and the EASM summary report is generated.
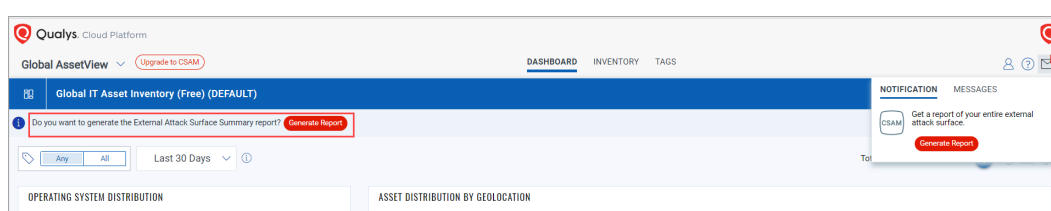
- If you are a Cybersecurity Asset Management (CSAM) trial user, EASM is activated, and the EASM summary report is generated.
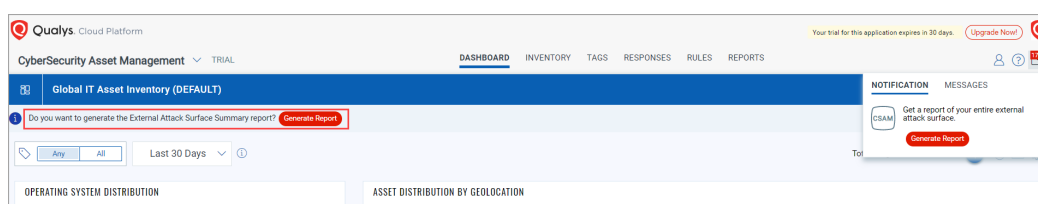

- If you are a Cybersecurity Asset Management (CSAM) paid user and have not activated EASM, EASM is activated, and the EASM summary report is generated.
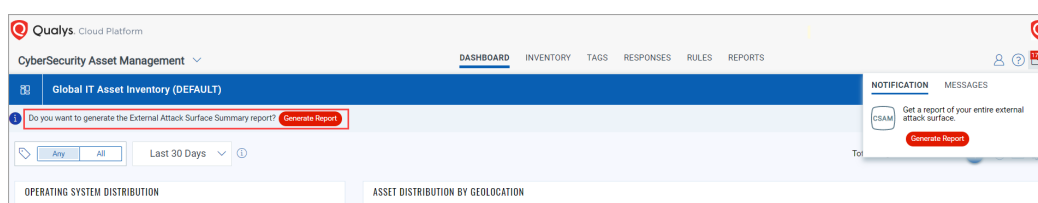
Note: This is a one-time process. After you click **Generate Report** and complete all the steps, the EASM summary report is generated for you. After that, the **Generate Report** is not shown again.

To know more about the EASM Summary Report creation steps, refer to the Online Help.

After the report is ready, you receive a notification. You can download the report from the link provided in the notification or by clicking **Download Report** from the **Dashboard** tab.
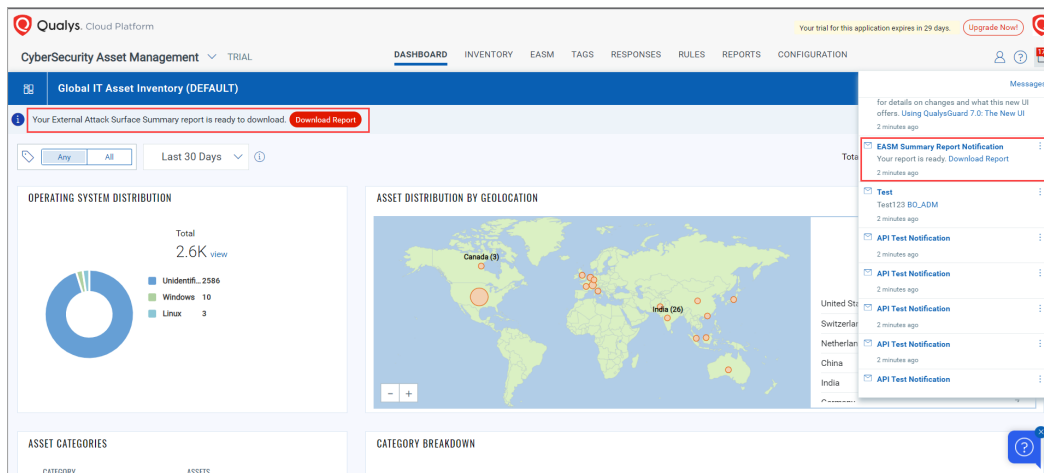
You are then navigated to the **Reports** tab, and you can download the report from the **Reports** tab.

Example: Download the EASM summary report from the CSAM trial version.
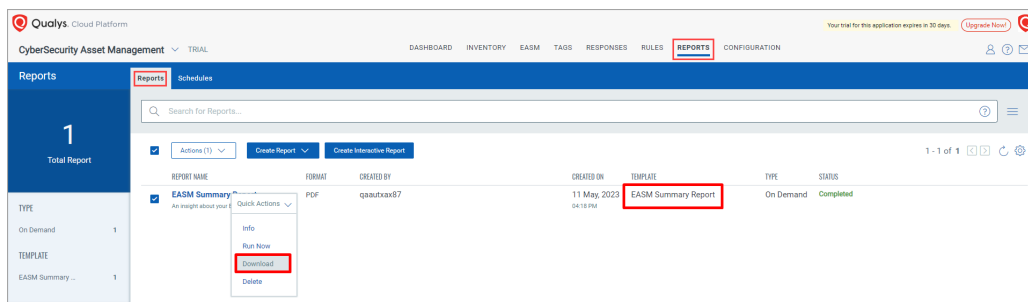
EASM Summary Report Template CSAM

With this release, we have added the EASM Summary Report template. The users already using EASM can use this new report template and generate the report to get visibility into the summary of your external attack surface.
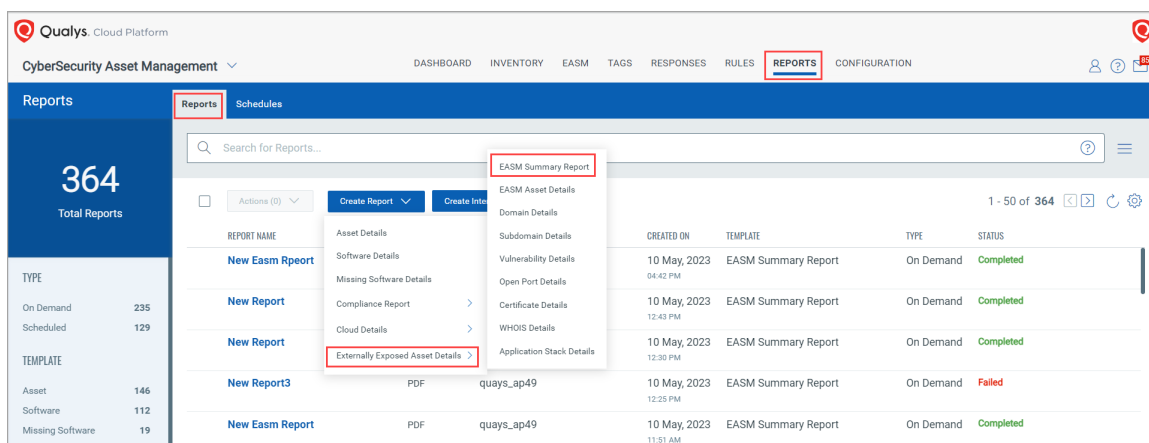
You can create an On Demand or a scheduled EASM summary report. You can choose to send the notification after the report is executed through email. Optionally, you can limit the number of times the report can be downloaded from the link sent through the email notification.

Example of report generation steps:

Tag Set Creation CSAM

With this release, you can now create a tag set by including tags in a tag set. Also, you can choose to exclude tags. The assets tagged with such tags are brought under such a unique tag set. You can also mark the tag set as Favorite.

Go to **Tags** > **Create New** > **Tag Set** to create a new tag set. For more information about tag set creation steps, refer to the Online Help.

The type of tag set is dynamic, but you can include static and dynamic tags in the tag set. Similarly, you can exclude static and dynamic tags while creating a tag set. Note that you can include or exclude a maximum of 20 tags. Also, you can create a maximum of 100 tag sets from your account.

When the tag set gets evaluated, and assets are added to the tag set, you can see the 'Completed' status under the **Reveal Status** column.

After the tag set is created, you can view, edit, and delete the tag set. Also, remove the tag set from the Favorite, and find assets that are part of a tag set.

Note: The tag sets created from QWEB are also shown on the CSAM UI. These tag sets are denoted with the highlighted icon. As these tag sets are created from QWEB, you can't edit or delete them. You can only view them and mark them as Favorites.

Issues Addressed

- We have fixed an issue where the CSAM rule alerts did not generate the Account ID and Instance ID.
- We have fixed an issue where upon clicking View Install List with the All Time filter selected, the software count was shown as 0.