



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!

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](#)

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

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.

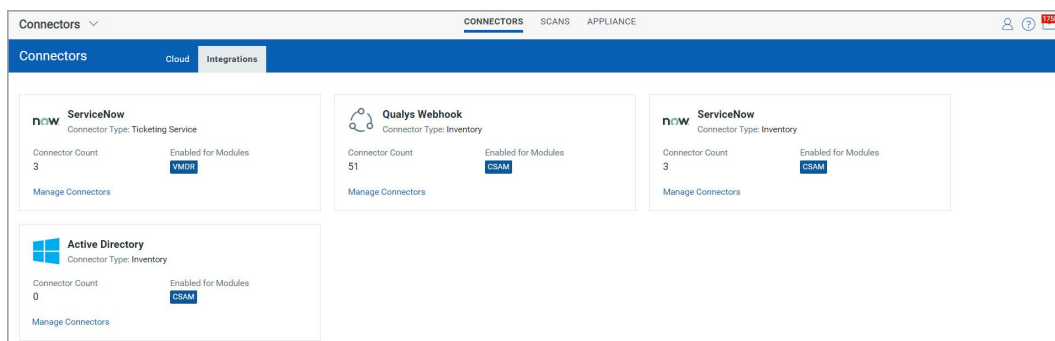
To understand the end-to-end feature workflow, refer to the [Online Help](#).

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.



- **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.

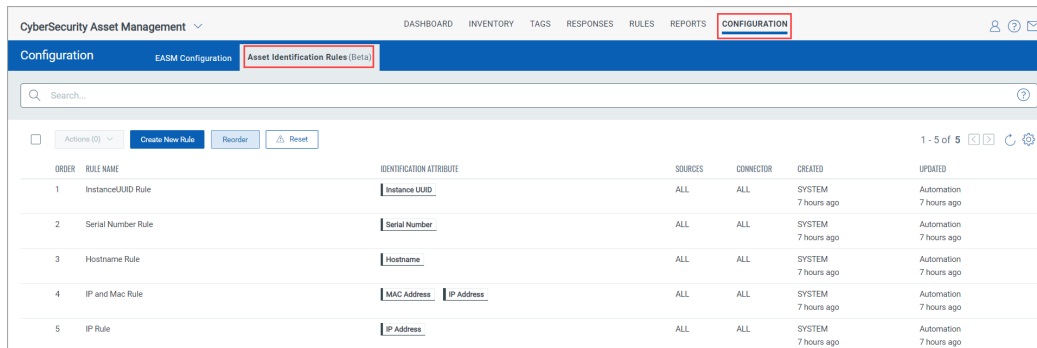
- **ServiceNow:** The ServiceNow Inventory connector lets you connect and discover resources of ServiceNow inventories. You can then view the discovered assets in the CSAM application.

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](#).

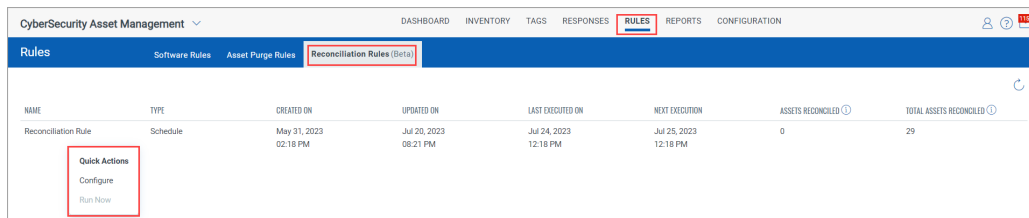


ORDER	RULE NAME	IDENTIFICATION ATTRIBUTE	SOURCES	CONNECTOR	CREATED	UPDATED
1	Instance/UUID Rule	Instance/UUID	ALL	ALL	SYSTEM 7 hours ago	Automation 7 hours ago
2	Serial Number Rule	Serial Number	ALL	ALL	SYSTEM 7 hours ago	Automation 7 hours ago
3	Hostname Rule	Hostname	ALL	ALL	SYSTEM 7 hours ago	Automation 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](#).



NAME	TYPE	CREATED ON	UPDATED ON	LAST EXECUTED ON	NEXT EXECUTION	ASSETS RECONCILED	TOTAL ASSETS RECONCILED
Reconciliation Rule	Schedule	May 31, 2023 02:18 PM	Jul 24, 2023 08:21 PM	Jul 24, 2023 12:18 PM	Jul 25, 2023 12:18 PM	0	29

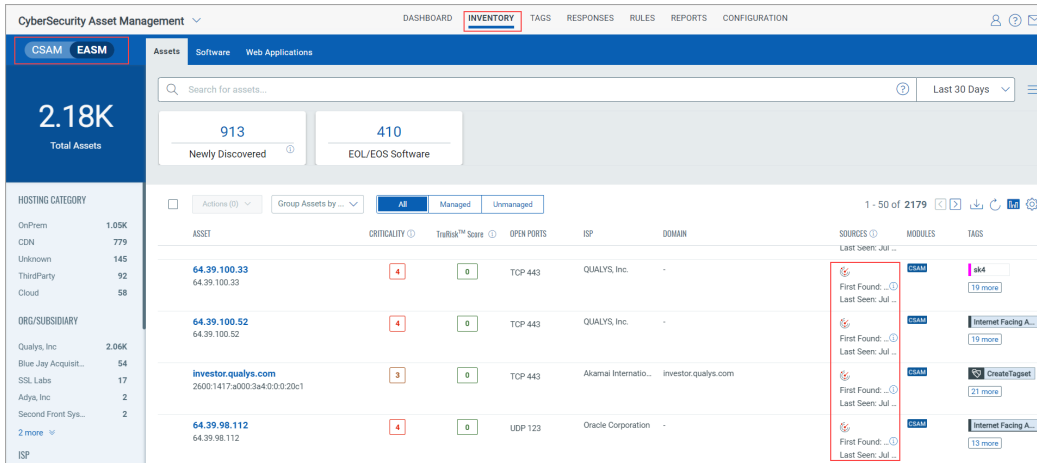
You can also [purge assets discovered by third-party connectors](#), such as Webhook, ServiceNow, and Active Directory connectors.

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.



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.

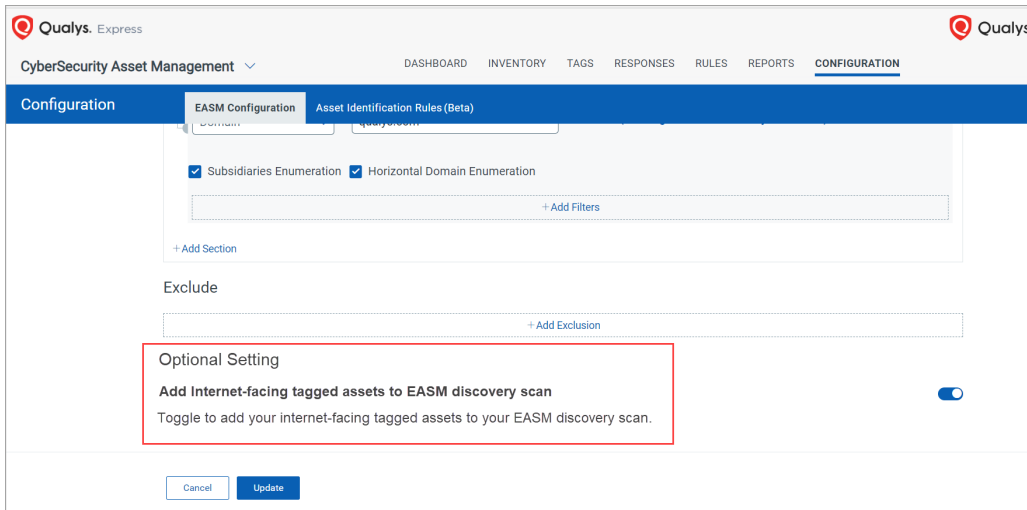
You can use the following new QQL tokens from the **Asset Identification Rules (Beta)** tab. For more information, refer to [Search Tokens for IT Assets](#).

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 CSAM

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



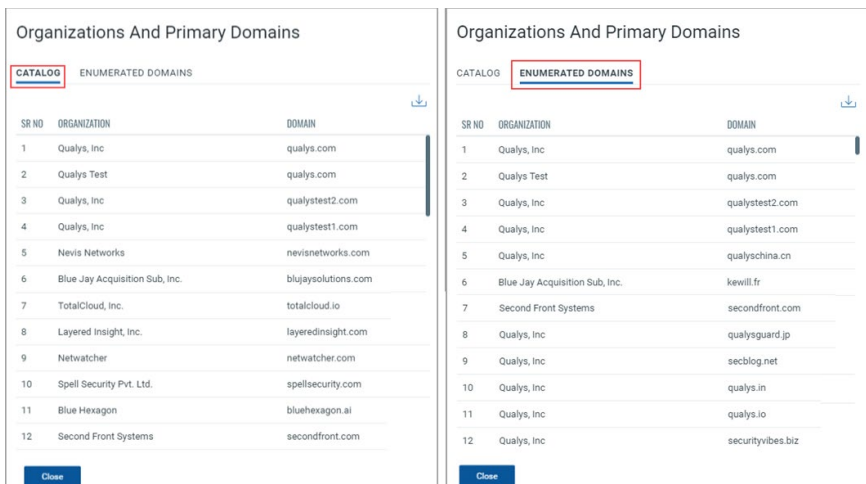
Typically, when you source the data from our EASM third-party sources, all the internet-facing assets might not be available for various reasons. For example, only the Internet-facing asset allowed by firewalls is accessible to Qualys scanners, or your Internet-facing assets don't have enough attribution, 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 CSAM

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.



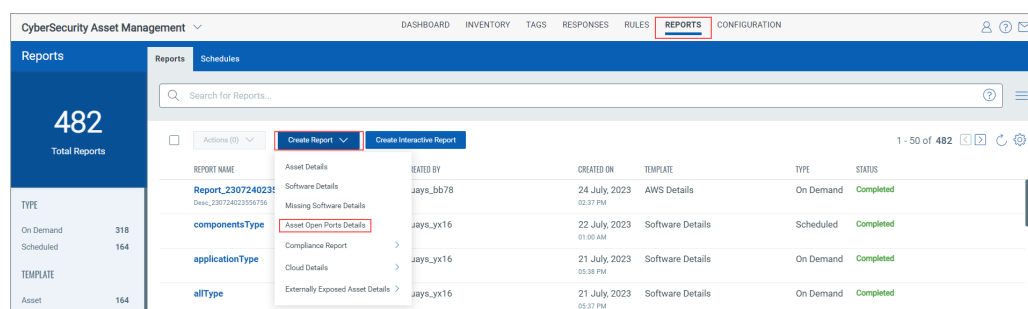
You can see a list of domains and organizations available in the EASM catalog DB from the **CATALOG** tab.

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](#).

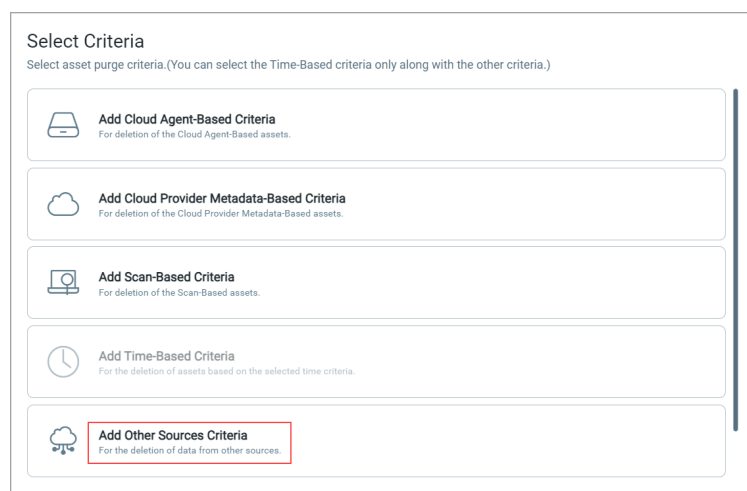


Purge Assets Identified by Third-Party Connectors GAV CSAM

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](#).

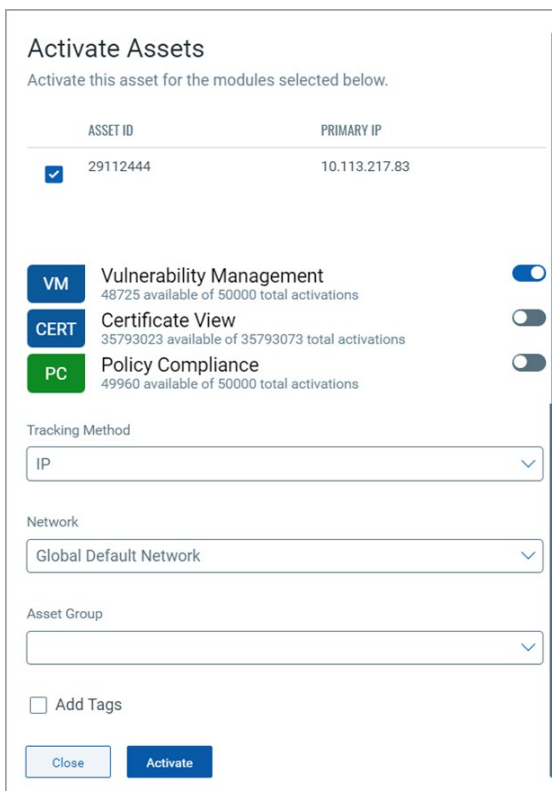
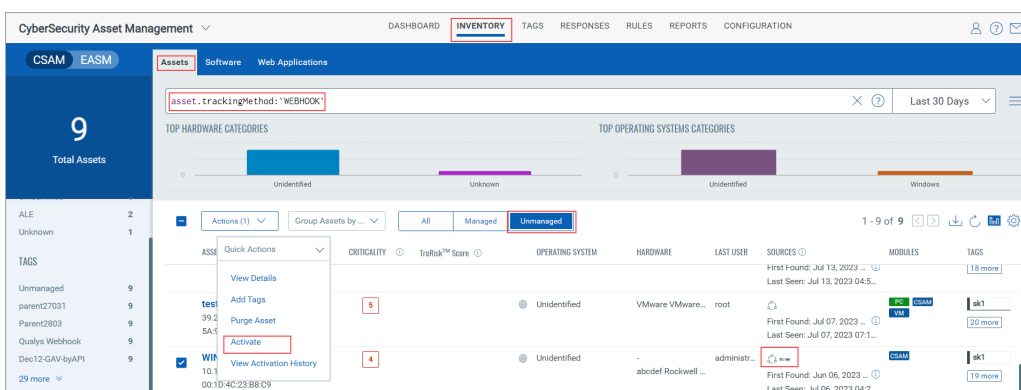


Activate Assets for VM, PC, and CERT Modules GAV CSAM

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.



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**.

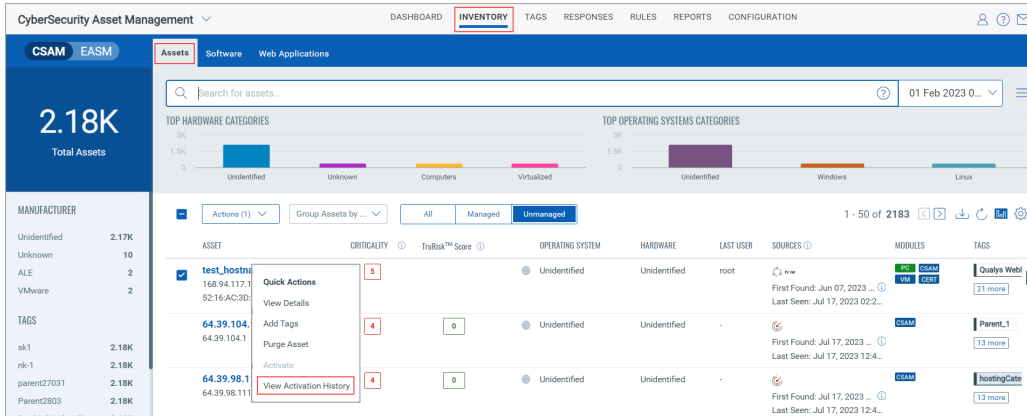
Once you activate the asset for the required modules, the IP address of that asset is added for the respective module scan.

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.



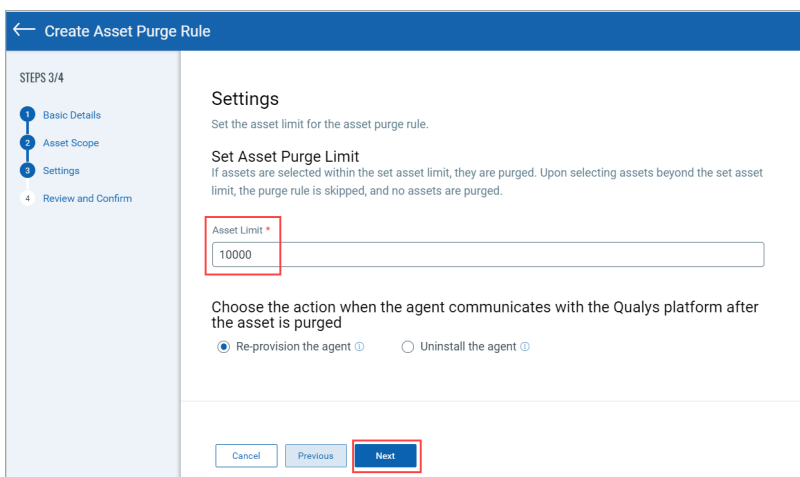
You can see the activation details, such as the asset ID, activated modules, status, etc.

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.



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.