Qualys Global AssetView/CyberSecurity Asset Management v2.x

Release Notes

Version 2.15
April 06, 2023

What’s New

Here's what's new in Global AssetView/CyberSecurity Asset Management 2.15!

GAV CSAM Global AssetView/CyberSecurity Asset Management

Visibility to Alibaba Cloud Instance Details
New QQL Tokens for Alibaba Cloud Instances
Added support to View and edit tags from the Asset Details Page
Introduced Default Purge Rules
Added Purge Assets Support for Additional Inventory Sources
Introduced New Asset Purge Criteria
Enhanced Select Tags Page
Visibility to Third-Party Vuln Imported Assets

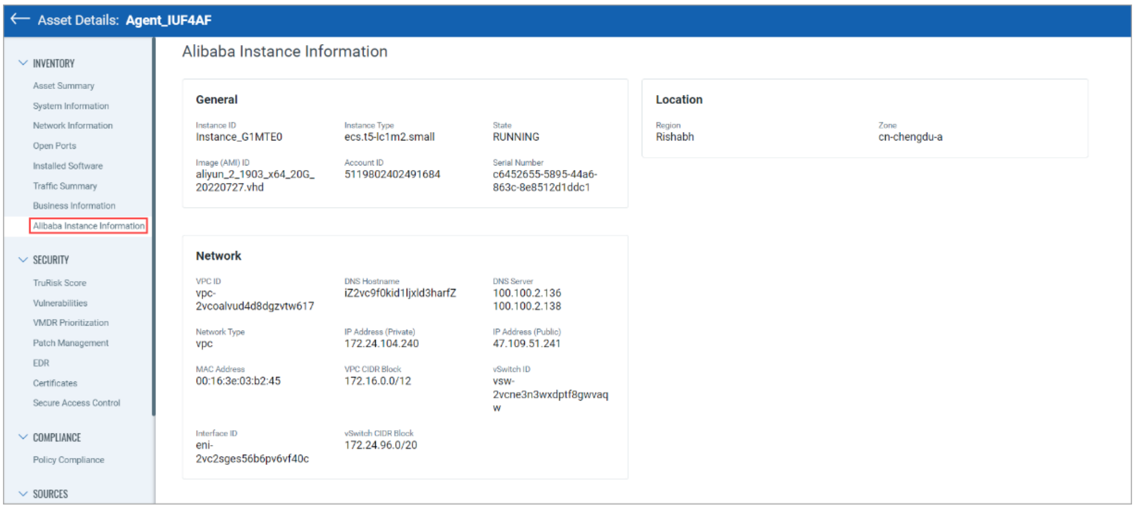
CSAM CyberSecurity Asset Management

Introduced a Configuration Tab
Added ‘CDN’ Type in Exclude Filter of EASM Configuration
Added New Report Template
Enhanced the EASM Page
New EASM QQL Tokens
Changed the Shodan Tags Label to EASM Tags
Introduced DNS SINKHOLE Tag

Global AssetView/CyberSecurity Asset Management 2.15 brings you many more improvements and updates! Learn more

Visibility to Alibaba Cloud Instance Details GAV CSAM

With this release, you can get an insight into the Alibaba instances. When you go to the **Inventory** > **Assets** tab and view the details of the Alibaba instance, you can see the **Alibaba Instance Information** tab in the Inventory section for Alibaba instances. You can find the details about the Alibaba instance from this tab, such as Hostname, FQDN, Host ID, and so on.



Alibaba Instance Information

General

Instance ID: Instance_G1MTE0
Instance Type: ecs.t5-lc1m2.small
State: RUNNING
Image (AMI) ID: aliyun_2_1903_x64_20G_20220727.vhd
Account ID: 5119802402491684
Serial Number: c6452655-5895-44a6-863c-8e8512d1ddc1

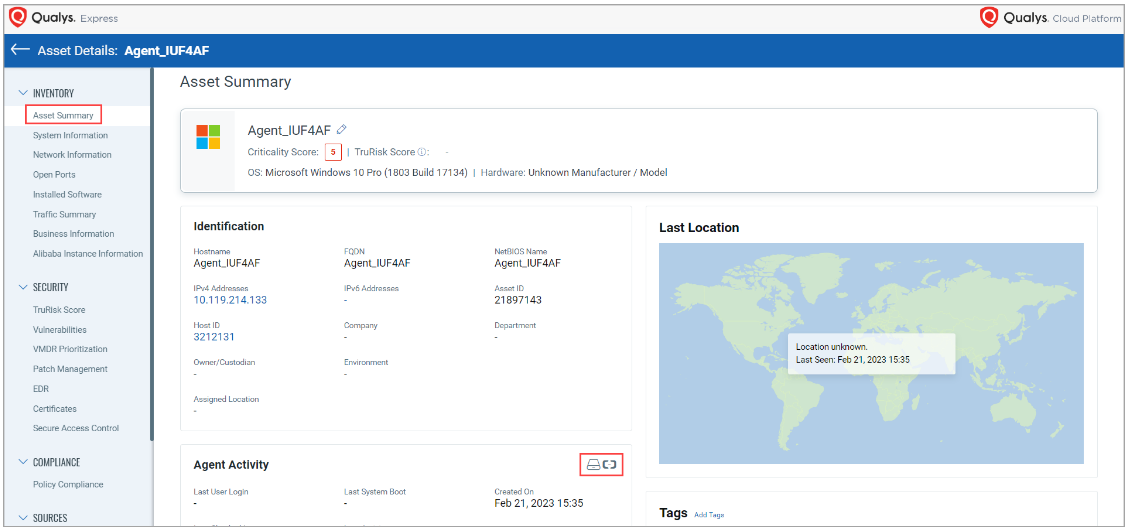
Location

Region: Rishabh
Zone: cn-chengdu-a

Network

VPC ID: vpc-2vcoalvud4d8dgzvtw617
DNS Hostname: iZ2vc9f0kid1ljxld3harfZ
DNS Server: 100.100.2.136
100.100.2.138
Network Type: vpc
IP Address (Private): 172.24.104.240
IP Address (Public): 47.109.51.241
MAC Address: 00:16:3e:03:b2:45
VPC CIDR Block: 172.16.0.0/12
vSwitch ID: vsw-2vcne3n3wxdptf8gwvaqw
Interface ID: eni-2vc2sges56b6pv6vf40c
vSwitch CIDR Block: 172.24.96.0/20

You can also see **Cloud Agent** and **ALIBABA** icons in the Agent Activity section from the **Asset Summary** tab.



Asset Summary

Agent_IUF4AF

Criticality Score: 5 | TruRisk Score: -

OS: Microsoft Windows 10 Pro (1803 Build 17134) | Hardware: Unknown Manufacturer / Model

Identification

Hostname: Agent_IUF4AF
FQDN: Agent_IUF4AF
NetBIOS Name: Agent_IUF4AF
IPv4 Addresses: 10.119.214.133
IPv6 Addresses: -
Asset ID: 21897143
Host ID: 3212131
Company: -
Department: -
Owner/Custodian: -
Environment: -
Assigned Location: -

Last Location

Location unknown.
Last Seen: Feb 21, 2023 15:35

Agent Activity

Last User Login: -
Last System Boot: -
Created On: Feb 21, 2023 15:35

New QQL Tokens for Alibaba Cloud Instances GAV CSAM

With this release, you can use the following Alibaba tokens from the **Dashboard**, **Inventory**, **Tags**, and **Responses** tab. You can filter your Alibaba instances using these tokens in the QQL queries. To know more about these tokens, see Online Help.

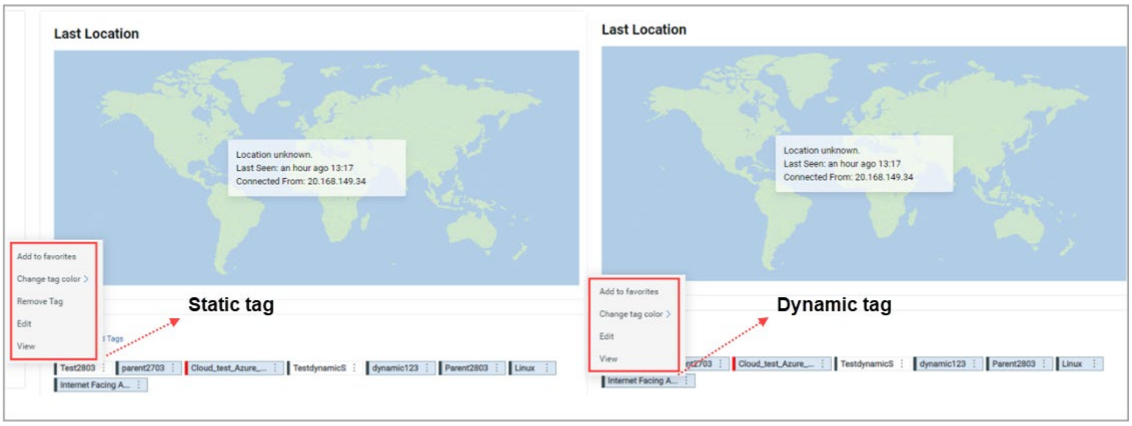
Token Name	Description
alibaba.instance.accountId	Find Alibaba cloud instances with a particular account Id.
alibaba.instance.dnsServer	Find Alibaba cloud instances associated with the Domain Name System (DNS) configuration.

alibaba.instance.hasAgent	Find Alibaba instances that have a cloud agent installed.
alibaba.instance.hostName	Find Alibaba cloud instances associated with the hostname.
alibaba.instance.imageId	Find Alibaba cloud instances with the specified image Id used during instance creation.
alibaba.instance.instanceId	Find an Alibaba cloud instance with a specific Id.
alibaba.instance.instanceType	Find Alibaba cloud instances with a specific instance type.
alibaba.instance.interfaceId	Find Alibaba cloud instances by the Id of network interface controllers (NICs).
alibaba.instance.instanceState	Find Alibaba cloud instances of the selected state. Examples of the instance's state are, RUNNING, STARTED, STOPPED, TERMINATED, and so on.
alibaba.instance.macAddress	Find Alibaba cloud instances with the specific MAC address.
alibaba.instance.networkType	Find Alibaba cloud instances of the selected network type. The network type can be vpc or classic.
alibaba.instance.privateIpAddress	Find Alibaba cloud instances with private IPv4 addresses or a range of IPs assigned to NIC.
alibaba.instance.publicIpAddress	Find Alibaba cloud instances with public IPv4 addresses or a range of IPs.
alibaba.instance.region.code	Find Alibaba cloud instances that belong to the specific region code.
alibaba.instance.region.name	Find Alibaba cloud instances that belong to the specific region name.
alibaba.instance.serialNumber	Find Alibaba cloud instances that belong to the specific serial number.
alibaba.instance.vpcCidrBlock	Find Alibaba cloud instances that belong to the CIDR block of the VPC network.
alibaba.instance.vpcId	Find Alibaba cloud instances that belong to the specific virtual private clouds (VPC) Id.
alibaba.instance.vswitchId	Find the Alibaba cloud instance that is connected to the vSwitch Id.
alibaba.instance.vswitchCidrBlock	Find Alibaba cloud instances that are connected to the CIDR block of vSwitch.
alibaba.instance.zoneId	Find Alibaba cloud instances that belong to the specific zone Id.

Added support to View and edit tags from the Asset Details Page GAV CSAM

With this release, you can view and edit static and dynamic tags from the **Asset Summary** tab on the "Asset Details" page. When you click **View**, a new "Tag Details" page opens, unlike the earlier release, wherein you could see the tag details in the pop-up window.

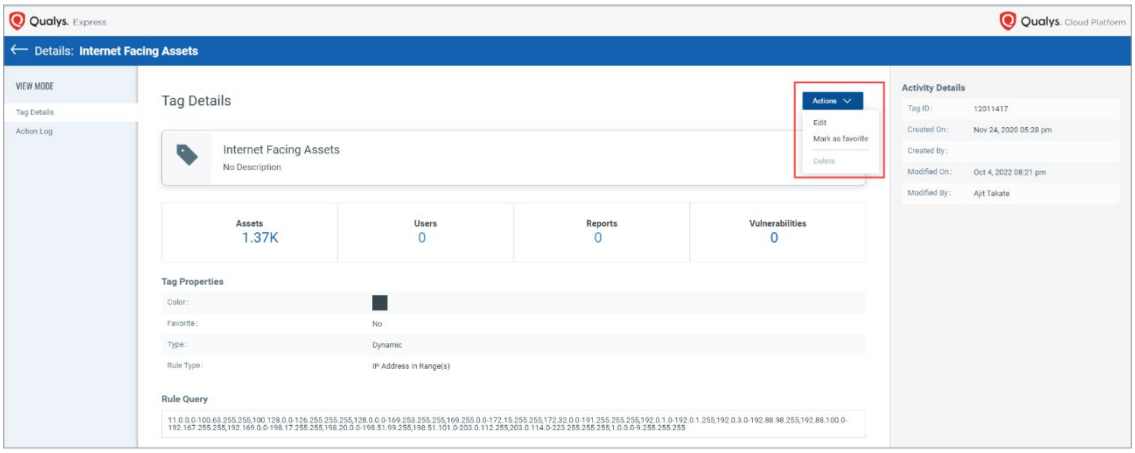
Note: When you click **ctrl +View**, the "Tag Details" page opens in the next tab.



Last Location

Location unknown.
Last Seen: an hour ago 13:17
Connected From: 20.168.149.34

You can see the tag details on the "Tag Details" page. Also, you can edit or mark the tag as a favorite by clicking **Actions** from the “Tag Details” page.



Details: **Internet Facing Assets**

Tag Details

Internet Facing Assets
No Description

Assets	Users	Reports	Vulnerabilities
1.37K	0	0	0

Tag Properties

Color:	■
Favorite:	No
Type:	Dynamic
Rule Type:	IP Address In Range(s)

Rule Query

```
11.0.0.0-100.63.255.255,100.128.0.0-126.255.255.255,128.0.0.0-169.253.255.255,169.255.0.0-172.15.255.255,172.32.0.0-191.255.255.255,192.0.1.0-192.0.1.255,192.0.3.0-192.88.98.255,192.88.100.0-
192.167.255.255,192.169.0.0-198.17.255.255,198.20.0.0-198.51.99.255,198.51.101.0-203.0.112.255,203.0.114.0-223.255.255.255,1.0.0.0-9.255.255.255
```

Activity Details

Tag ID:	12011417
Created On:	Nov 24, 2020 05:28 pm
Created By:	
Modified On:	Oct 4, 2022 08:21 pm
Modified By:	Ajit Takate

Introduced Default Purge Rules GAV CSAM

With this release, we have introduced the following seven default purge rules. By default, these rules are disabled. You can enable these rules to purge or delete assets from your asset inventory.

The following table explains the purge rules and their use.

Purge Rule	Description
Terminated GCP assets and not updated in 3 days	Delete GCP assets that are in a terminated state and updated older than 3 days.
Terminated AWS assets and not updated in 3 days	Delete AWS assets that are in a terminated state and updated older than 3 days.
Terminated Azure assets and not updated in 3 days	Delete Azure terminated assets in either a terminated or a deleted state and updated older than 3 days.
Assets not scanned in 90 days	Delete the scan-based assets with IP or NETBIOS tracking method and older than 90 days.
AWS instances and all states not updated in 90 Days	Delete AWS assets older than 90 days, irrespective of the asset states.

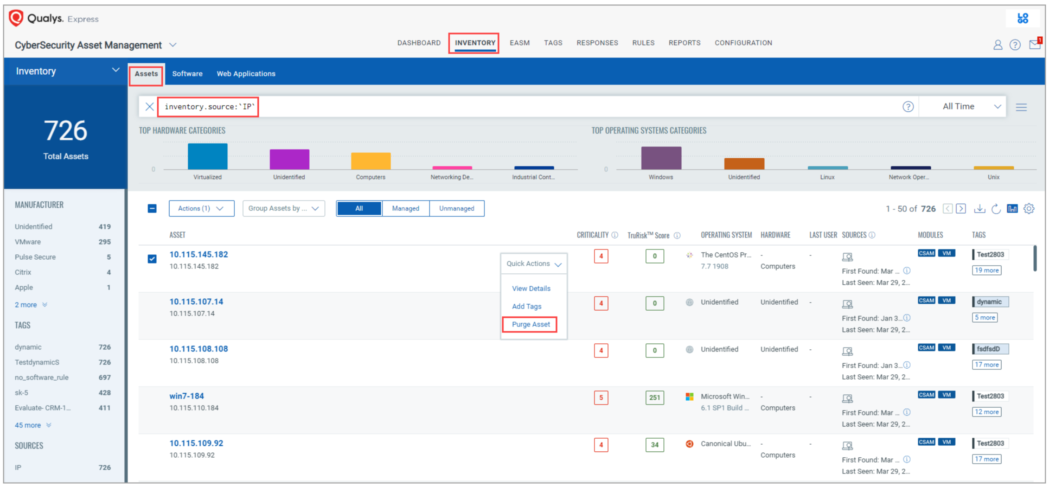
Azure VMs and all states not updated in 90 days	Delete AZURE assets older than 90 days, irrespective of the asset states.
GCP machines and all states not updated in 90 days	Delete GCP assets with all states older than 90 days, irrespective of the asset states.

Added Purge Assets Support for Additional Inventory Sources GAV CSAM

With this release, purge assets support is now available for DNSNAME, IP, and NETBIOS inventory sources. For example, refer to the following screen captures, wherein the inventory source is IP.

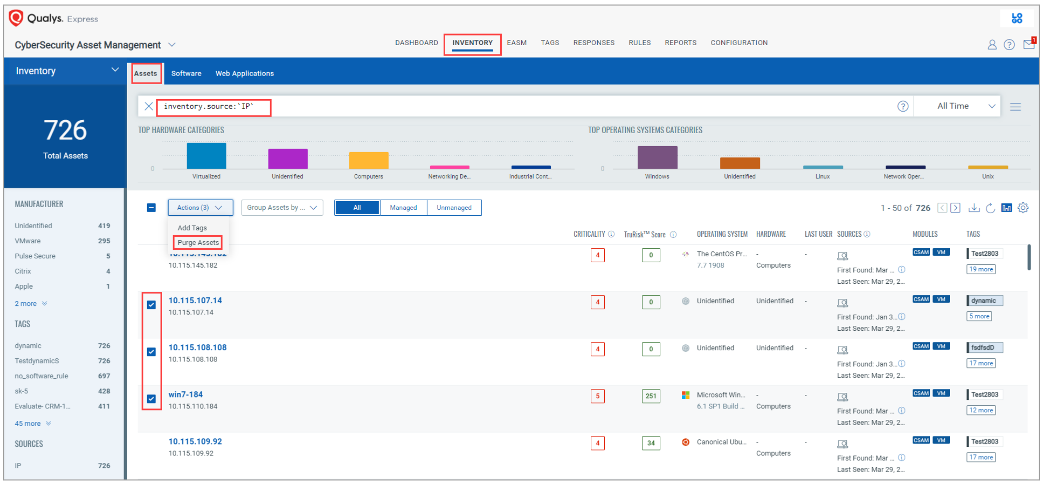
Complete the following steps to purge assets:

1. Go to the **Inventory** > **Assets** tab, filter your assets based on the required inventory source, and choose the assets you want to purge.
2. Select the check box next to the asset you want to purge, and from the Quick Actions menu, click **Purge Asset**.



inventory.source:`IP`

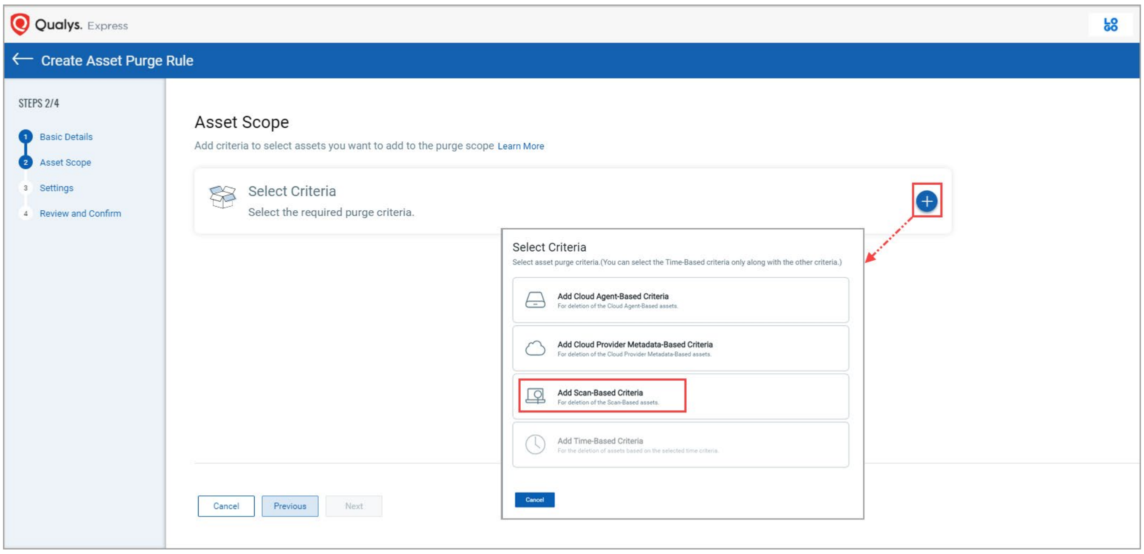
To purge multiple assets, select the check boxes next to the assets you want to purge, and from the Actions list, click **Purge Assets**.



inventory.source:`IP`

Introduced New Asset Purge Criteria GAV CSAM

With this release, we have introduced Add Scan-Based Criteria to the Create Asset Purge Rule steps. As a result, you can now delete or purge scan-based assets with IP, DNSNAME, and NETBIOS tracking methods. For more details, refer to the Online Help.



Add criteria to select assets you want to add to the purge scope

Select the required purge criteria.

Select asset purge criteria.(You can select the Time-Based criteria only along with the other criteria.)

For deletion of the Cloud Agent-Based assets.

For deletion of the Cloud Provider Metadata-Based assets.

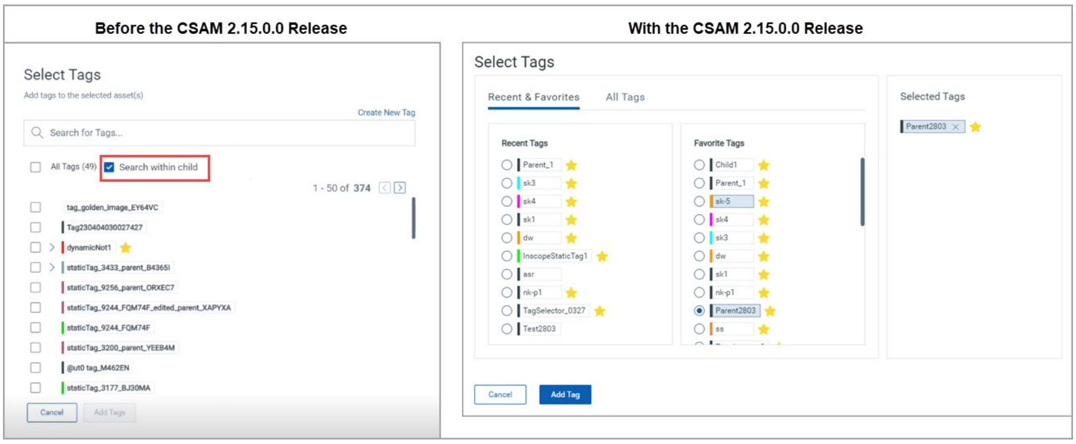
For deletion of the Scan-Based assets.

For the deletion of assets based on the selected time criteria.

Enhanced Select Tags Page GAV CSAM

With this release, the "Select Tags" page is modified that enhances the user experience. This page is used from multiple tabs to execute various operations. Also, the "Select Tags" page is used across Qualys products.

See the following screen capture that shows the "Select Tags" page.



Add tags to the selected asset(s)

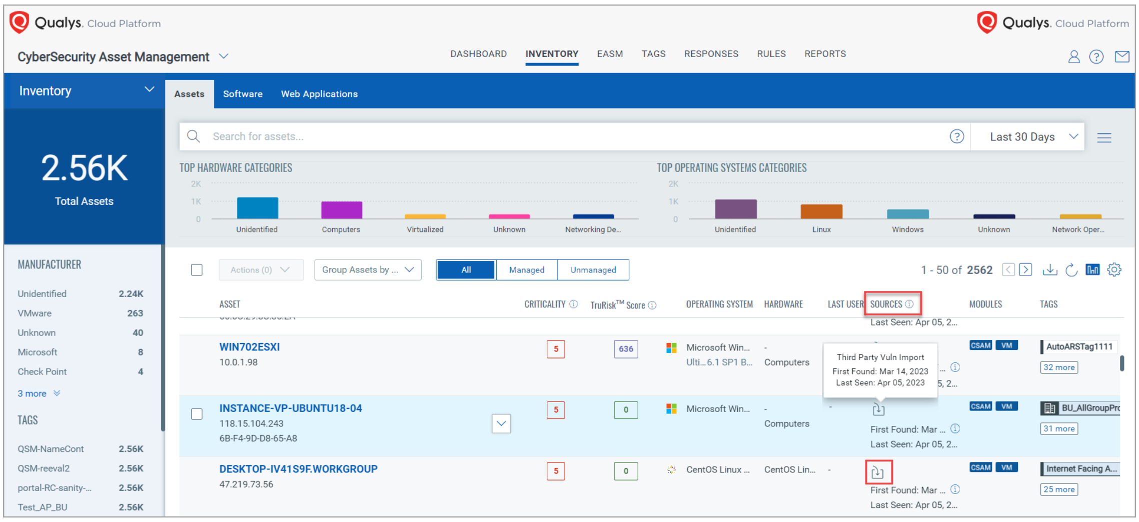
- A **Recent & Favorites** tab is added to the Select Tags page. As shown in the screen capture, from the **Recent & Favorites** tab, you can see tags categorized as **Recent Tags** and **Favorite** Tags. After selecting the required tag, it is also shown in the **Selected Tags** section.
- No changes are made to the search functionality from the **All Tags** tab. You can search for the tag by entering a complete tag name or its substring, and parent and child tags for which the search string matches are shown.

- The **Search within child** check box is removed from the "Select Tags" page.

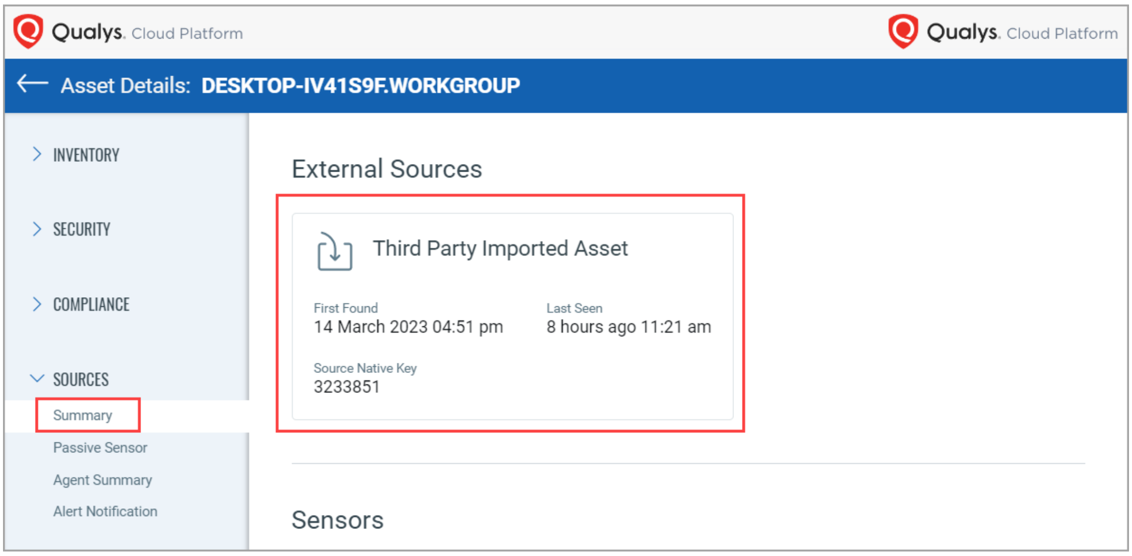
Visibility to Third-Party Vuln Imported Assets GAV CSAM

With this release, you can see the third-party vuln imported assets from the **Inventory** > **Assets** tab.

As shown in the following screen capture, you can see a specific icon, **Third Party Vuln Import**, for the third-party vuln imported asset in the **Sources** column. When you hover over that icon, you can see the first found and last seen details of that asset in the tooltip.



When you go to the "Asset Details" page of that asset and click the **Summary** tab from the **Sources** section, you can see the details of third-party vuln imported assets.



Third Party Imported Asset

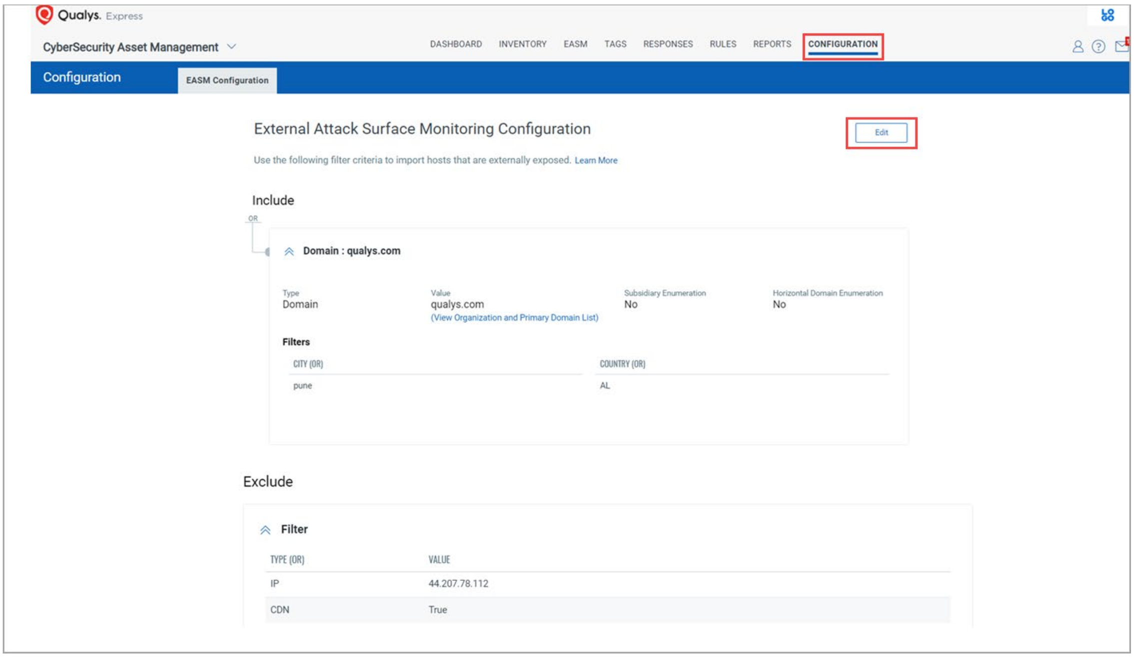
First Found
14 March 2023 04:51 pm

Last Seen
8 hours ago 11:21 am

Source Native Key
3233851

Introduced a Configuration Tab CSAM

With this release, we have added a new tab, **Configuration**, which provides a more user-friendly view of the EASM configuration. When EASM is enabled, and you want to configure EASM, you are now pointed to the **Configuration** tab. You can edit the existing EASM configuration by clicking **Edit**.



External Attack Surface Monitoring Configuration

Use the following filter criteria to import hosts that are externally exposed. Learn More

Include

Domain : qualys.com

Type	Value	Subsidiary Enumeration	Horizontal Domain Enumeration
Domain	qualys.com (View Organization and Primary Domain List)	No	No

Filters

CITY (OR)	COUNTRY (OR)
pune	AL

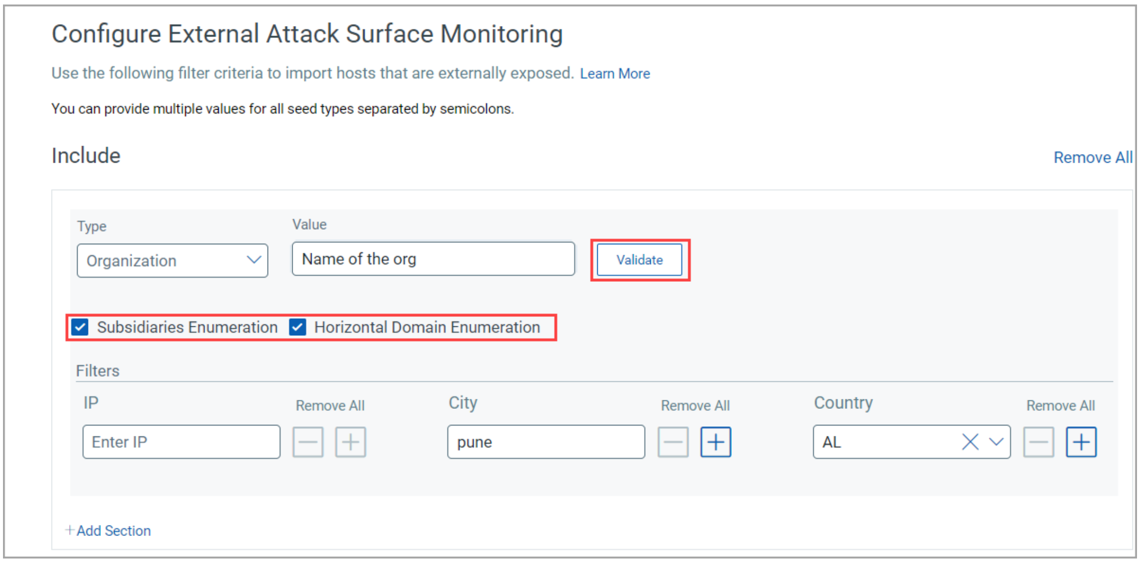
Exclude

Filter

TYPE (OR)	VALUE
IP	44.207.78.112
CDN	True

When you edit the EASM configuration, you can see the newly introduced **Validate** button. This button is available only for the **Domain** and **Organization** Include Types.

- The **Validate** button is displayed only after entering the details in the **Value** field.
- The validation support is available for only one domain and Organization value.



Configure External Attack Surface Monitoring

Use the following filter criteria to import hosts that are externally exposed. Learn More

You can provide multiple values for all seed types separated by semicolons.

Include

Type: Organization

Value: Name of the org

☑ Subsidiaries Enumeration ☑ Horizontal Domain Enumeration

Filters

IP: Enter IP

City: pune

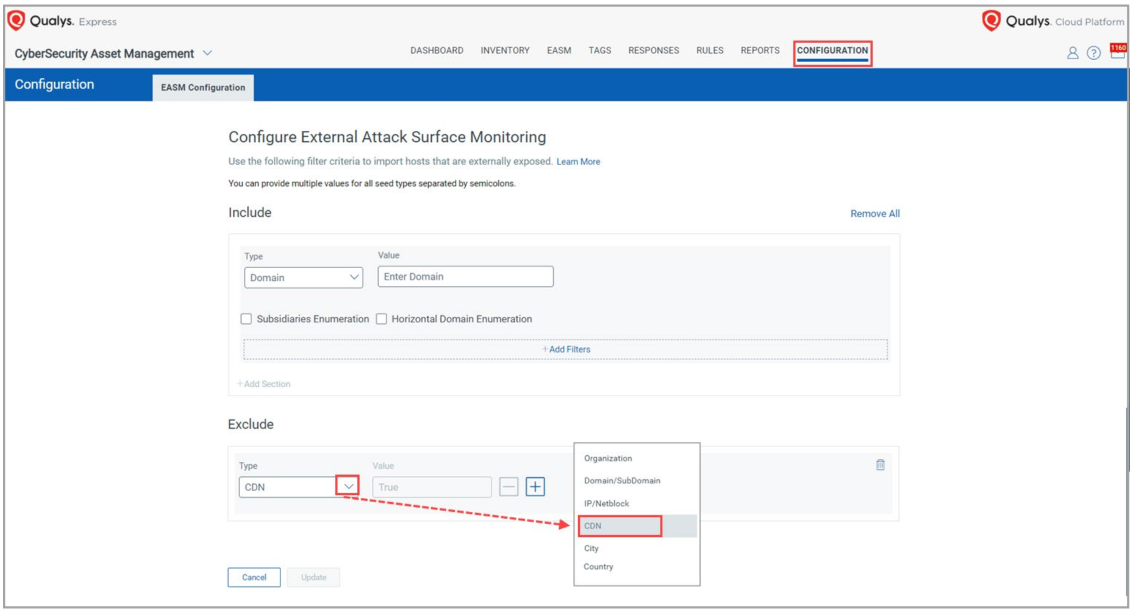
Country: AL

If you choose to validate based on Domain or Organization, you can see a list of Organizations and Domains for which the data will be available. The data will be synced only if you select the Subsidiaries Enumeration and Horizontal Domain Enumeration check boxes. For more information, refer to the Online Help.

Added ‘CDN’ Type in Exclude Filter of EASM Configuration CSAM

With this release, we have added a new filter criterion, ‘CDN’, in global exclusion for managing EASM configurations. By using this criterion, you can exclude the CDN from the EASM configuration, and the excluded CDN is not shown after the immediate next scan. The default value selected for CDN is ‘True’.

You cannot add the CDN criterion multiple times like the rest of the exclude filter criteria.



Configure External Attack Surface Monitoring

Use the following filter criteria to import hosts that are externally exposed. Learn More

You can provide multiple values for all seed types separated by semicolons.

Include

Type: Domain

Value: Enter Domain

□ Subsidiaries Enumeration □ Horizontal Domain Enumeration

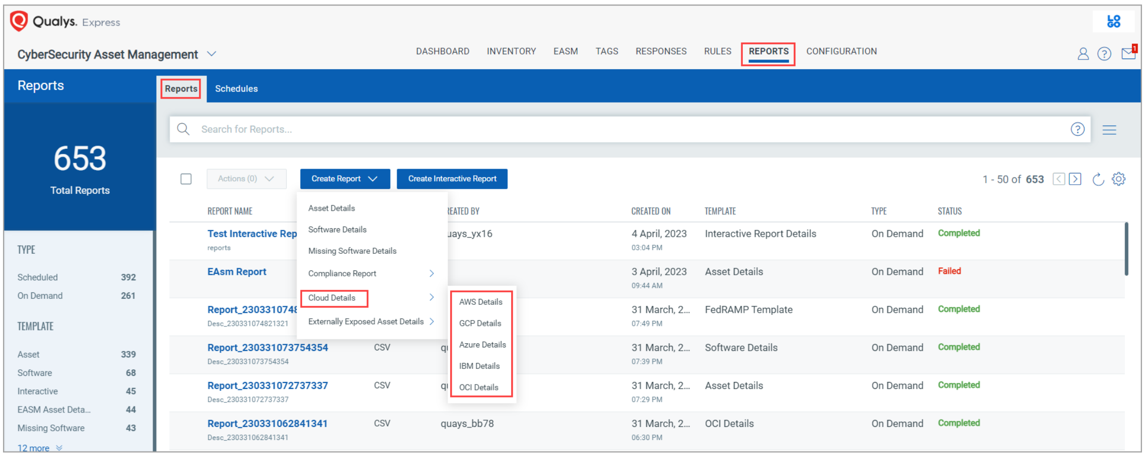
Exclude

Type: CDN

Value: True

Added New Report Template CSAM

With this release, we have added a new **Cloud Details** option to the **Generate Report** list. Upon clicking **Generate Reports**, you can see the available templates for various cloud asset types, such as **AWS Details**, **GCP Details**, **Azure Details**, **IBM Details**, and **OCI Details**. You can generate the report for a particular cloud asset type using the required template.



653 Total Reports

TYPE	
Scheduled	392
On Demand	261

TEMPLATE	
Asset	339
Software	68
Interactive	45
EASM Asset Deta...	44
Missing Software	43
12 more	

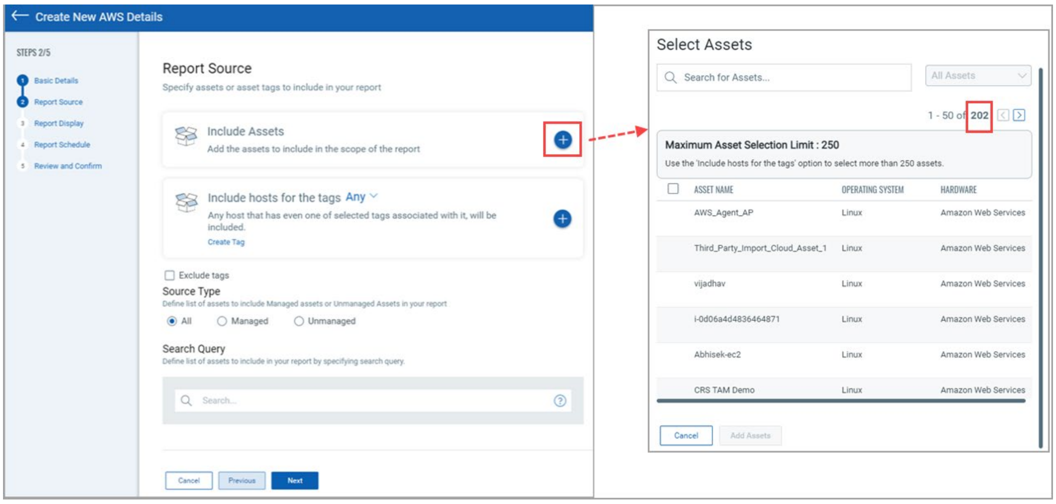
1 - 50 of 653

REPORT NAME		REATED BY	CREATED ON	TEMPLATE	TYPE	STATUS
Test Interactive Rep reports		uays_yx16	4 April, 2023 03:04 PM	Interactive Report Details	On Demand	Completed
EAsm Report			3 April, 2023 09:44 AM	Asset Details	On Demand	Failed
Report_2303310748 Desc_230331074821321			31 March, 2... 07:49 PM	FedRAMP Template	On Demand	Completed
Report_230331073754354 Desc_230331073754354	CSV	q	31 March, 2... 07:39 PM	Software Details	On Demand	Completed
Report_230331072737337 Desc_230331072737337	CSV	q	31 March, 2... 07:29 PM	Asset Details	On Demand	Completed
Report_230331062841341 Desc_230331062841341	CSV	quays_bb78	31 March, 2... 06:30 PM	OCI Details	On Demand	Completed

Note:

- While creating a report, when you add assets to include in the report’s scope, only the assets for the selected cloud asset type are shown in the “Select Assets” window.

  As shown in the following screen capture, the AWS cloud assets are shown in the “Select Assets” window while creating an AWS details report.



Report Source

Specify assets or asset tags to include in your report

Include Assets

Add the assets to include in the scope of the report

Include hosts for the tags Any

Any host that has even one of selected tags associated with it, will be included.

□ Exclude tags

Source Type

Define list of assets to include Managed assets or Unmanaged Assets in your report

● All ○ Managed ○ Unmanaged

Search Query

Define list of assets to include in your report by specifying search query.

Select Assets

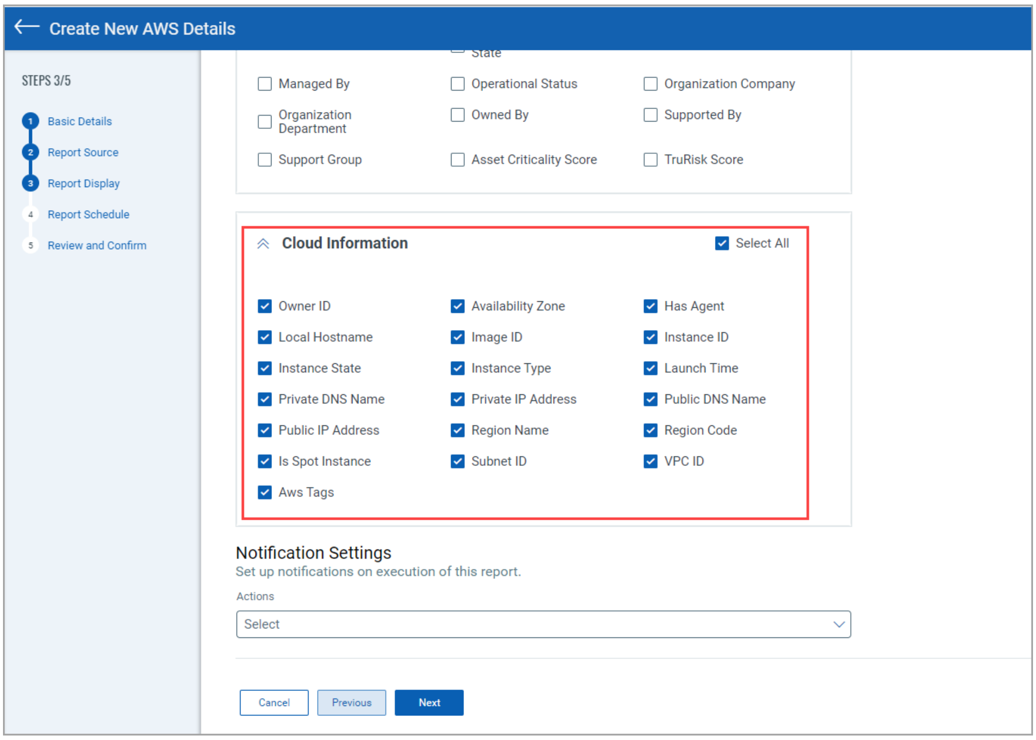
1 - 50 of 202

Maximum Asset Selection Limit : 250

Use the 'Include hosts for the tags' option to select more than 250 assets.

ASSET NAME	OPERATING SYSTEM	HARDWARE
AWS_Agent_AP	Linux	Amazon Web Services
Third_Party_Import_Cloud_Asset_1	Linux	Amazon Web Services
vijadhav	Linux	Amazon Web Services
i-0d06a4d4836464871	Linux	Amazon Web Services
Abhisek-ec2	Linux	Amazon Web Services
CRS TAM Demo	Linux	Amazon Web Services

- The columns specific to the selected cloud asset are shown in the Report Display step. See the following screen capture that shows the columns specific to AWS cloud assets.



State

□ Managed By □ Operational Status □ Organization Company

□ Organization Department □ Owned By □ Supported By

□ Support Group □ Asset Criticality Score □ TruRisk Score

Cloud Information ☑ Select All

☑ Owner ID ☑ Availability Zone ☑ Has Agent

☑ Local Hostname ☑ Image ID ☑ Instance ID

☑ Instance State ☑ Instance Type ☑ Launch Time

☑ Private DNS Name ☑ Private IP Address ☑ Public DNS Name

☑ Public IP Address ☑ Region Name ☑ Region Code

☑ Is Spot Instance ☑ Subnet ID ☑ VPC ID

☑ Aws Tags

Notification Settings

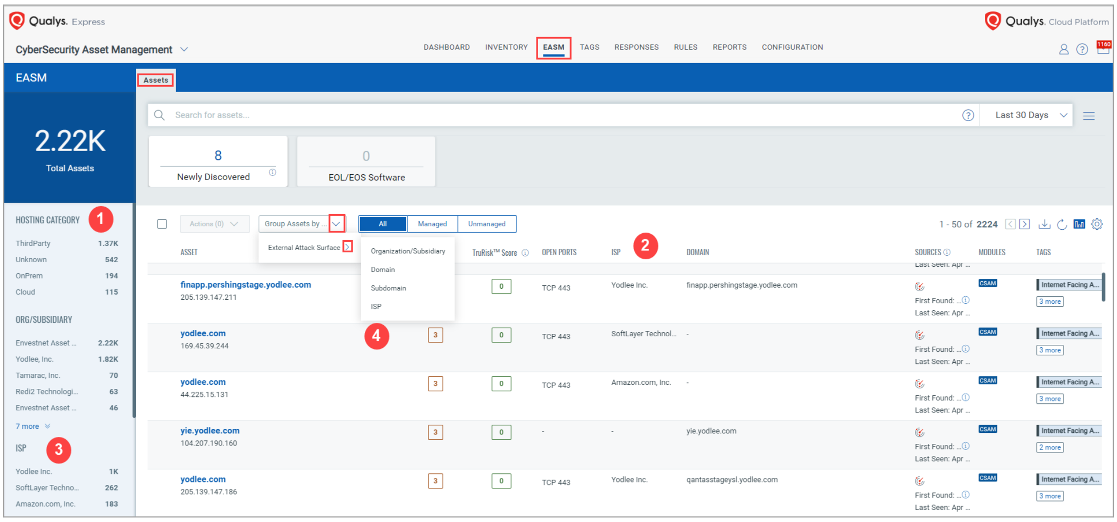
Set up notifications on execution of this report.

Actions

Select

Enhanced the EASM Page CSAM

With this release, we made the following enhancements to the EASM page:



HOSTING CATEGORY

ThirdParty	1.37K
Unknown	542
OnPrem	194
Cloud	115

ORG/SUBSIDIARY

Envestnet Asset ...	2.22K
Yodlee, Inc.	1.82K
Tamarac, Inc.	70
Redi2 Technologi...	63
Envestnet Asset ...	46

7 more

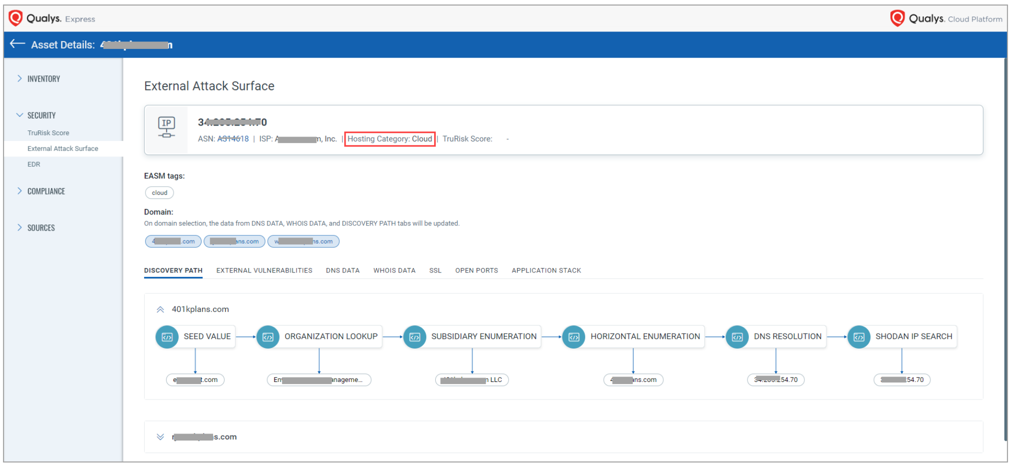
ISP

Yodlee Inc.	1K
SoftLayer Techno...	262
Amazon.com, Inc.	183

ASSET		TruRisk™ Score	OPEN PORTS	ISP	DOMAIN	SOURCES	MODULES	TAGS
finapp.pershingstage.yodlee.com 205.139.147.211		0	TCP 443	Yodlee Inc.	finapp.pershingstage.yodlee.com	First Found: ... Last Seen: Apr ...	CSAM	Internet Facing A... 3 more
yodlee.com 169.45.39.244	3	0	TCP 443	SoftLayer Technol...	-	First Found: ... Last Seen: Apr ...	CSAM	Internet Facing A... 3 more
yodlee.com 44.225.15.131	3	0	TCP 443	Amazon.com, Inc.	-	First Found: ... Last Seen: Apr ...	CSAM	Internet Facing A... 3 more
yie.yodlee.com 104.207.190.160	3	0	-	-	yie.yodlee.com	First Found: ... Last Seen: Apr ...	CSAM	Internet Facing A... 2 more
yodlee.com 205.139.147.186	3	0	TCP 443	Yodlee Inc.	qantasstageysl.yodlee.com	First Found: ... Last Seen: Apr ...	CSAM	Internet Facing A... 3 more

(1) Added the **HOSTING CATEGORY** section in the left pane. You can filter the EASM assets by clicking the required hosting category.

When you go to the “Assets Details” page of a particular asset from the **External Attack Surface** tab, you can see the hosting category of that asset.



Asset Details: [redacted]

External Attack Surface

[redacted]

ASN: [redacted] | ISP: [redacted] | Hosting Category: Cloud | TruRisk Score: -

EASM tags:

cloud

Domain:

On domain selection, the data from DNS DATA, WHOIS DATA, and DISCOVERY PATH tabs will be updated.

[redacted] [redacted] [redacted]

401kplans.com

[redacted] [redacted] [redacted] [redacted] [redacted] [redacted]

[redacted]

(2) The HOSTING column is now renamed as ISP.

(3) The HOSTING section from the left pane is renamed as ISP.

(4) The Hosting option from the Group Assets by list is renamed as ISP.

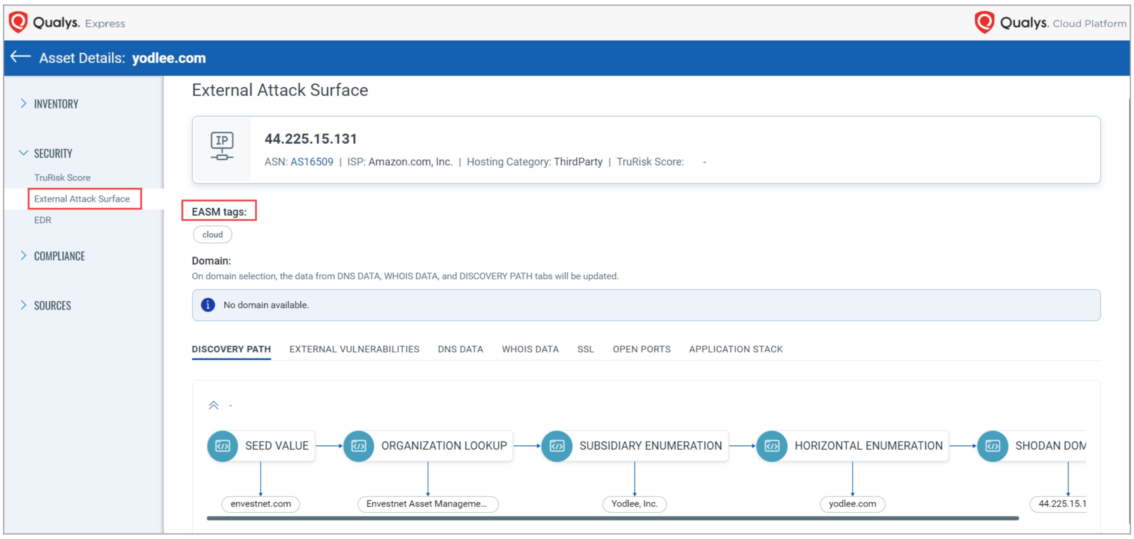
New EASM QQL Tokens CSAM

With this release, we have added the following EASM tokens. You can access them from the **EASM** and **Dashboard** tabs.

- **easm.tags.name:** This token enables you to filter asset based on tags discovered through EASM.
- **asset.hostingCategory1:** This token enables you to filter your assets based on the hosting category you provided.

Changed the Shodan Tags Label to EASM Tags CSAM

With this release, we changed the label Shodan tags to the EASM tags. Go to **EASM** > **Assets** tab and view the details of a particular asset. You are navigated to **the External Attack Surface** tab, where you can see the new label, EASM tag.



External Attack Surface

44.225.15.131

ASN: AS16509 | ISP: Amazon.com, Inc. | Hosting Category: ThirdParty | TruRisk Score: -

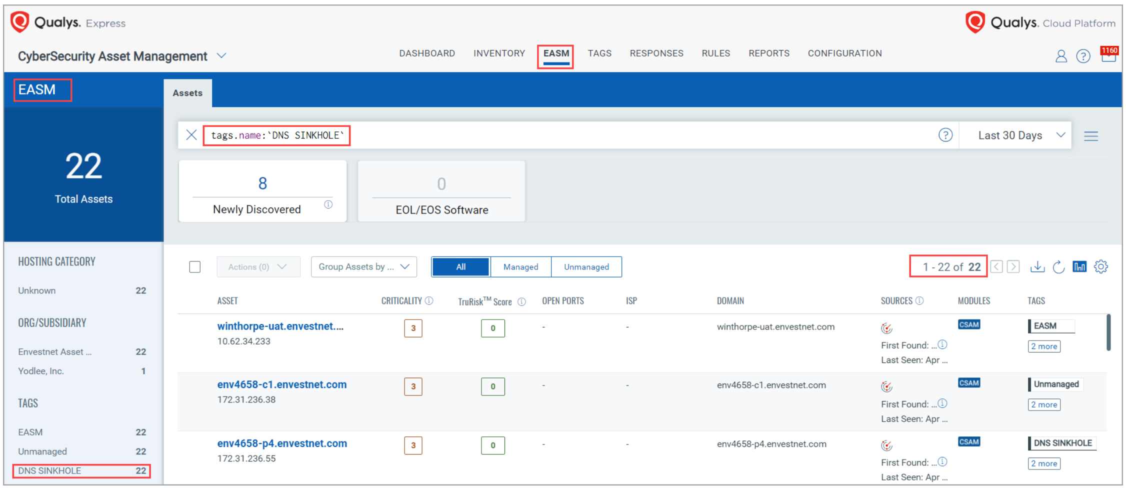
EASM tags: cloud

Domain:
On domain selection, the data from DNS DATA, WHOIS DATA, and DISCOVERY PATH tabs will be updated.

No domain available.

Introduced DNS SINKHOLE Tag CSAM

With this release, we have introduced the “DNS SINKHOLE” tag. This tag is applied to the private IPs discovered in the EASM scan. When you click the DNS SINKHOLE tag from the **Tags** section from the left pane, from the “Inventory” or the “EASM” page, you can see the list of private IPs discovered in the EASM scan.



```
tags.name:`DNS SINKHOLE`
```

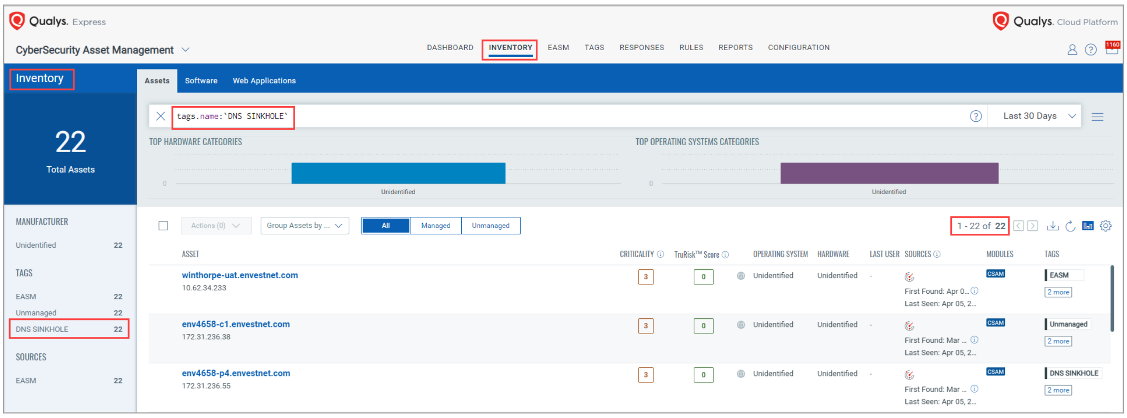
22 Total Assets

8 Newly Discovered

0 EOL/EOS Software

HOSTING CATEGORY	
Unknown	22
ORG/SUBSIDIARY	
Envestnet Asset ...	22
Yodlee, Inc.	1
TAGS	
EASM	22
Unmanaged	22
DNS SINKHOLE	22

ASSET	CRITICALITY	TruRisk™ Score	OPEN PORTS	ISP	DOMAIN	SOURCES	MODULES	TAGS
winthorpe-uat.envestnet.... 10.62.34.233	3	0	-	-	winthorpe-uat.envestnet.com	First Found: ... Last Seen: Apr ...	CSAM	EASM 2 more
env4658-c1.envestnet.com 172.31.236.38	3	0	-	-	env4658-c1.envestnet.com	First Found: ... Last Seen: Apr ...	CSAM	Unmanaged 2 more
env4658-p4.envestnet.com 172.31.236.55	3	0	-	-	env4658-p4.envestnet.com	First Found: ... Last Seen: Apr ...	CSAM	DNS SINKHOLE 2 more



```
tags.name:`DNS SINKHOLE`
```

22
Total Assets

MANUFACTURER	
Unidentified	22

TAGS	
EASM	22
Unmanaged	22
DNS SINKHOLE	22

SOURCES	
EASM	22

ASSET	CRITICALITY	TruRisk™ Score	OPERATING SYSTEM	HARDWARE	LAST USER	SOURCES	MODULES	TAGS
winthorpe-uat.envestnet.com 10.62.34.233	3	0	Unidentified	Unidentified	-	First Found: Apr 0... Last Seen: Apr 05, 2...	CSAM	EASM 2 more
env4658-c1.envestnet.com 172.31.236.38	3	0	Unidentified	Unidentified	-	First Found: Mar ... Last Seen: Apr 05, 2...	CSAM	Unmanaged 2 more
env4658-p4.envestnet.com 172.31.236.55	3	0	Unidentified	Unidentified	-	First Found: Mar ... Last Seen: Apr 05, 2...	CSAM	DNS SINKHOLE 2 more

Issues Addressed

- We fixed the issue where the Software report file size was exceptionally huge.
- We fixed the issues where characters from Nordic and German languages were not supported in the EASM Configuration domain names.
- We have fixed the issue where the CSAM application crashed when generating reports because the TimeZone value was not getting auto populated.
- We fixed the issue where the 'Unable to activate CMDB trial' error message was shown for a user despite having the Full/Purchased type license for the CMDB sync.
- We have fixed the issue where the results of the existing QQL query for application Software type showed a discrepancy in the assets count.