Cloud Agent as Passive Sensor (CAPS)

User Guide

March 05, 2024

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

Introduction

With the Cloud Agent as Passive Sensor (CAPS) feature, the Qualys Cloud Agent can collect the data in the subnet passively without any active probing of the device that it is monitoring. The Cloud Agent can monitor all network traffic and flag any asset activity. You can add one or more domains to detect whether the asset is on or off-premises.

The Cloud Agent listens to broadcasts and multicasts traffic for building the asset inventory and fingerprinting the operating systems and the device information of the assets. CAPS currently supports analysis of the following protocols —DHCP, ARP, NetBIOS, SSDP, mDNS.

The asset metadata is sent to the Qualys Cloud Platform for analysis, with which you can classify the unmanaged assets by operating system and hardware. CAPS considers split tunneled assets as off-premises and, therefore, will be in an inactive state.

This provides real-time visibility to all managed and unmanaged across your global, hybrid IT environment.

The CAPS module applies only to the Windows platform and is available as part of the CSAM application. The assets discovered by CAPS are displayed in CSAM. For details, see Assets Discovered by CAPS in CyberSecurity Asset Management.

You must perform CAPS configuration before activating the CAPS module for an agent host.

Important

When multiple cloud agents within the same subnet are configured to act as passive sensors, one cloud agent is elected as a leader and discovers assets, and those assets are shown in the CSAM inventory. In this case, the CAPS Leader tag is added to that cloud agent. The standby ensures continuity in case the Leader leaves the network.

The leader CAPS-enabled agent:

- passively senses network traffic

- sends the asset metadata to Qualys Platform

The Standby CAPS-enabled agent:

- does not sense network traffic passively

- does not send data to Qualys Platform

Note: This feature will be available only when the Windows agent binary with CAPS support is available. For supported agent versions, refer to the *Features by Agent Version* section in the Cloud Agent Platform Availability Matrix.

Prerequisites

For the CAPS feature, the Cloud Agent must connect to the corresponding Qualys Content Delivery Network (CDN) URLs directly or using the proxy.

For the list of Cloud Agent Server and CDN URLs, refer to https://www.qualys.com/platform-identification/.

System Resource Usage

The following section presents the CPU and disk usage by CAPS hosts.

CPU Usage

On active and standby CAPS hosts use 1 to 1.5% of CPU. Other CAPS hosts use less than 0.5 CPU.

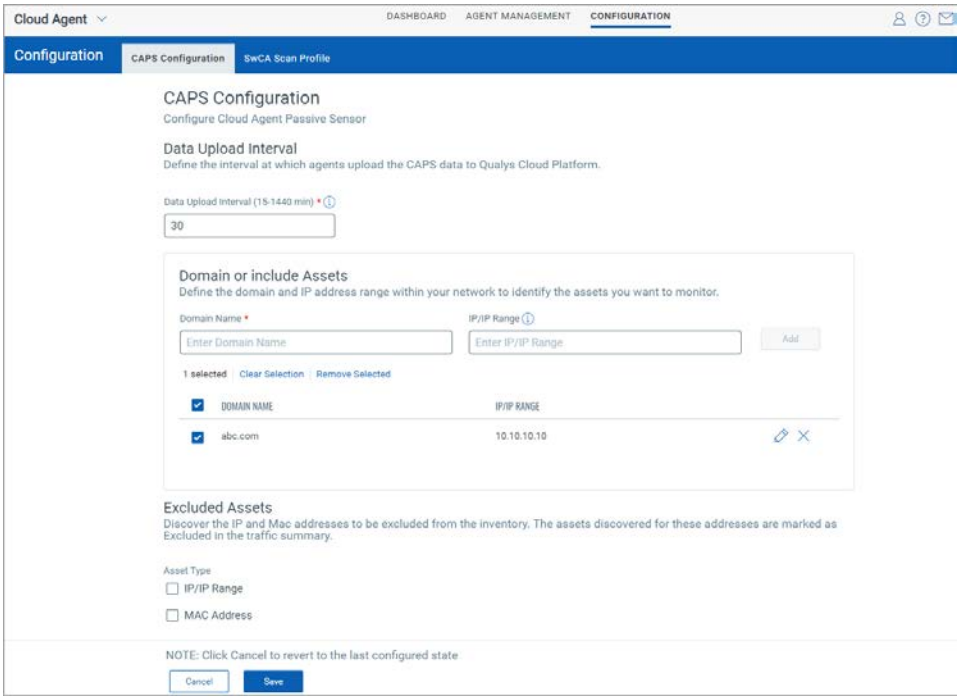
Disk Space Usage

- The binary image is approximately 10MB.
- 20 uncompressed log files – 10 MB
- Two uncompressed log file – 20 MB
- 2-3 temporary payload files each few MB. The size depends on the number of assets in the subnet.

Note: CAPS memory usage is a function of how many assets are present in the subnet. Per Asset, the average memory usage is below 100 KB. If the host is in a fully populated /22 subnet, that is, 1000 assets, then the memory usage can be 100 MB. Only the active and standby CAPS hosts will use this memory.

Configure CAPS Settings

To define the settings for the Cloud Agent to work as a passive sensor, such as the interval at which data is uploaded, and the scope of passive scanning, in the Cloud Agent application, go to the **Configuration** tab and click **CAPS configuration**.



In the **CAPS Configuration** page, define the following settings:

Data Upload Interval

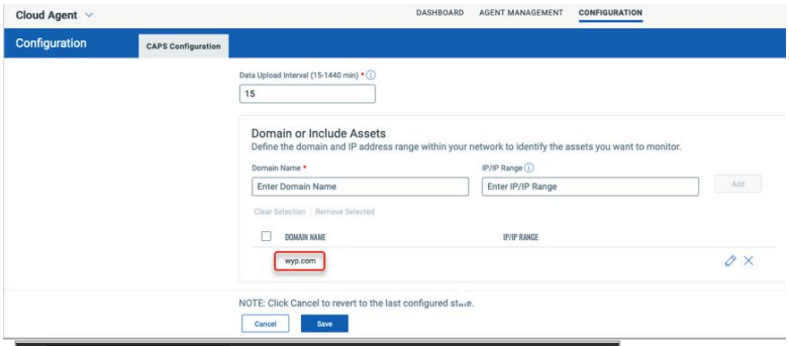
Define the time interval, in minutes, at which the agent uploads CAPS data to Qualys Cloud Platform. The valid range is 15 to 1440 minutes. The default value is 30.

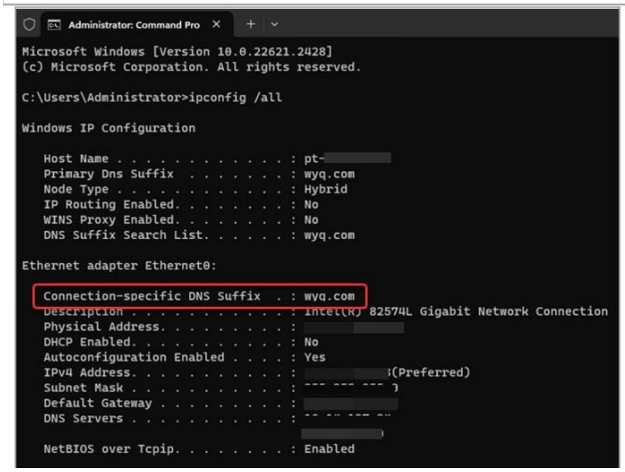
Scan Scope

In the **Domain or Include Asset** section, you can define the scanning scope by defining a domain name. You can also add specific IP addresses or a range of IP addresses in the domain to be added to the scan scope.

- **Domain Name** - Add a domain name. The scan scope includes all the assets that are part of the specified domain name. This is a mandatory field.

Note: The Domain Name must be an exact match with the Connection-specific DNS Suffix found on the endpoint. For example,





To discover the configured domain name, you can use one of the following methods:

- use QID 45606 : Network Interface Domain Name System (DNS) Suffix Information Extracted Through WMI
- run the `ipconfig /all` command at the endpoint

- **IP/IP Range** - Add one or more IP addresses, separated by a comma or IP address range for the specified domain name.

Click **Add**.

Assets to be Excluded

You can define some assets to exclude from the scan by specifying the IP, Mac address, or range. The assets are excluded from the Inventory.

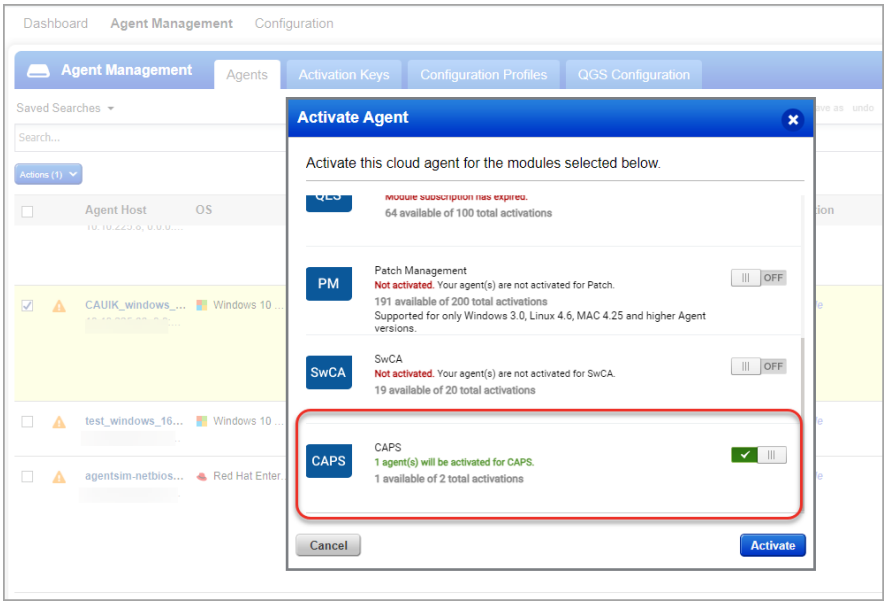
- To exclude the assets with the specified IP addresses or IP range, select the **IP/IP Range** check box, enter the IP addresses or IP range, and click **Add**.
- To exclude Mac assets, select the **Mac Address** check box, enter the Mac addresses or IP range, and click **Add**.

Click **Save** to save the CAPS configuration.

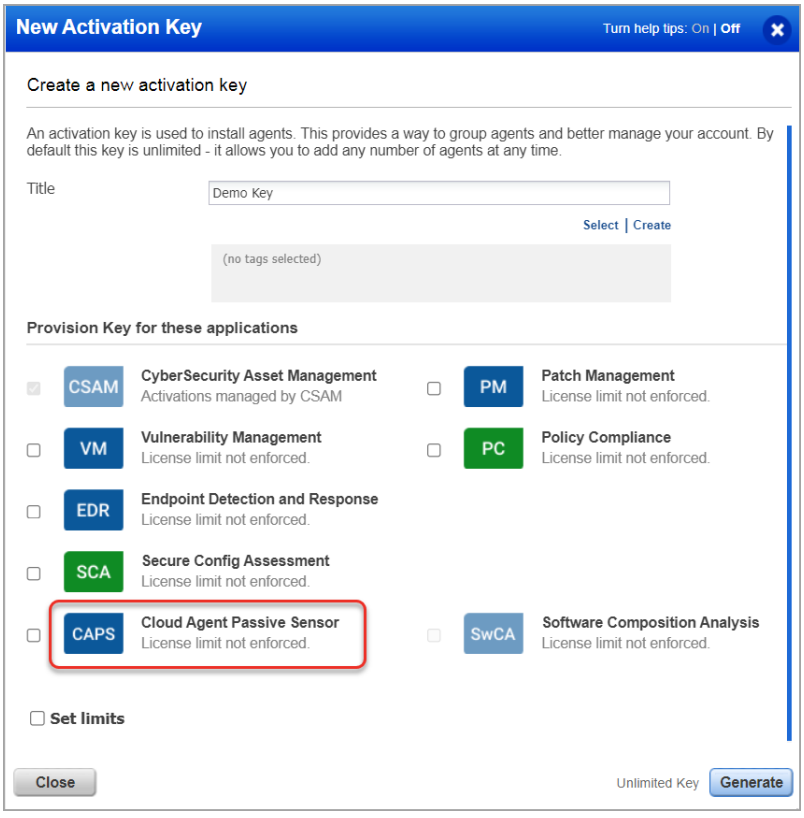
To revert the changes made in the CAPS configuration, click **Cancel**.

Activate CAPS Feature

To enable this functionality, you must activate the CAPS module on a single or multiple agent hosts. To activate the module, go to **Agent Management** > **Agents** tab, and click **Activate for <modules>** from the **Quick Actions** menu.



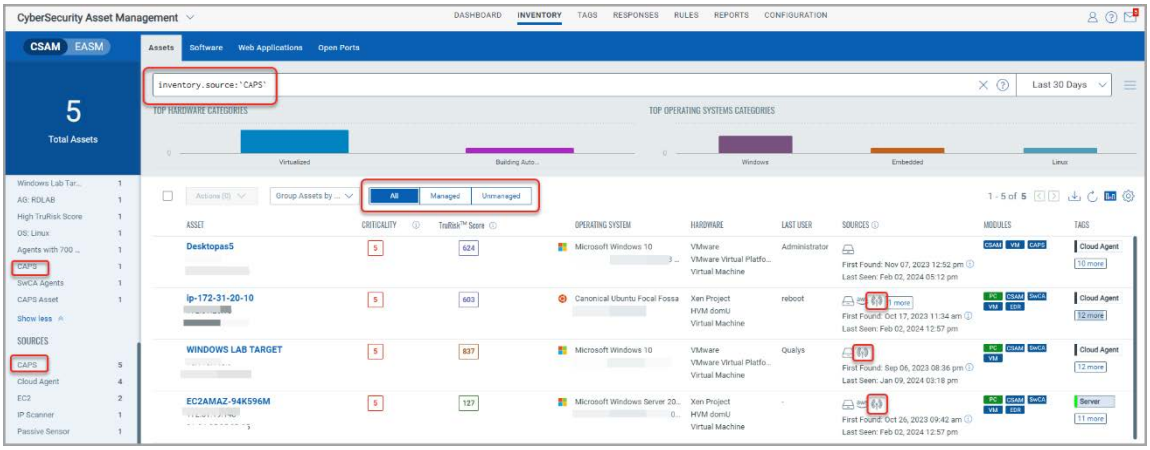
You can also activate the CAPS module while creating or editing the activation key.



Assets Discovered by CAPS in CyberSecurity Asset Management

You can see the assets discovered by Cloud Agent as Passive Sensor (CAPS) on the **Inventory** page in CyberSecurity Asset Management (CSAM).

You can use the search token `inventory.source:`CAPS`` to search assets discovered by CAPS. You can also view the assets grouped into managed and unmanaged and take action on the unmanaged assets.



You can see detailed information about the asset discovered by CAPS from the **Inventory** > **Sources** > **CAPS** tab, such as Agent UUID, First Found, Last Seen, and so on.