Qualys Cloud Platform v3.x

Release Notes

Version 3.16
August 24, 2023

What's New

CA **Cloud Agent**

Asset Architecture Type in Asset Summary

Updated Permissions for On-demand Scans

New Tokens in Cloud Agent

New Feature - Cloud Agent as a Passive Sensor

New Feature—Software Composition Analysis

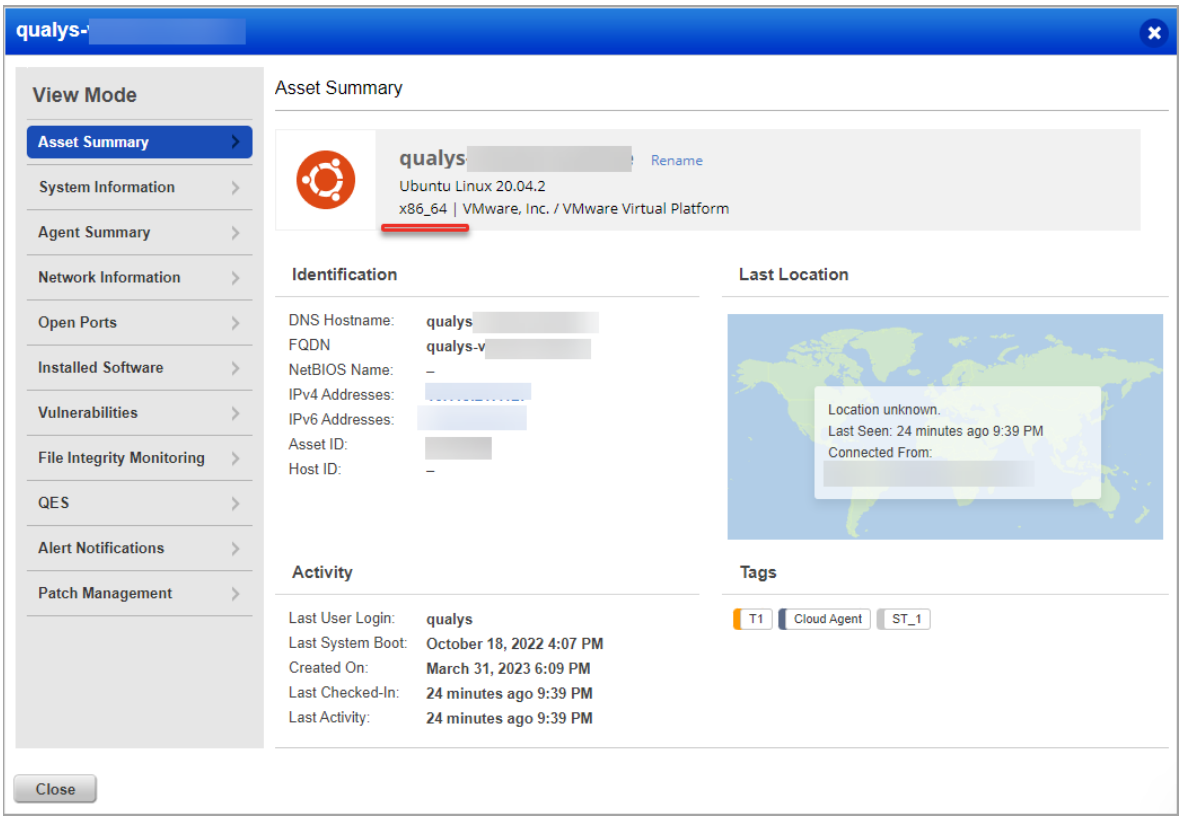
Static Tag Removal from Activation Key and Associated Agents

Qualys Cloud Platform 3.16 brings you many more improvements and updates! Learn more

CA Cloud Agent

Asset Architecture Type in Asset Summary

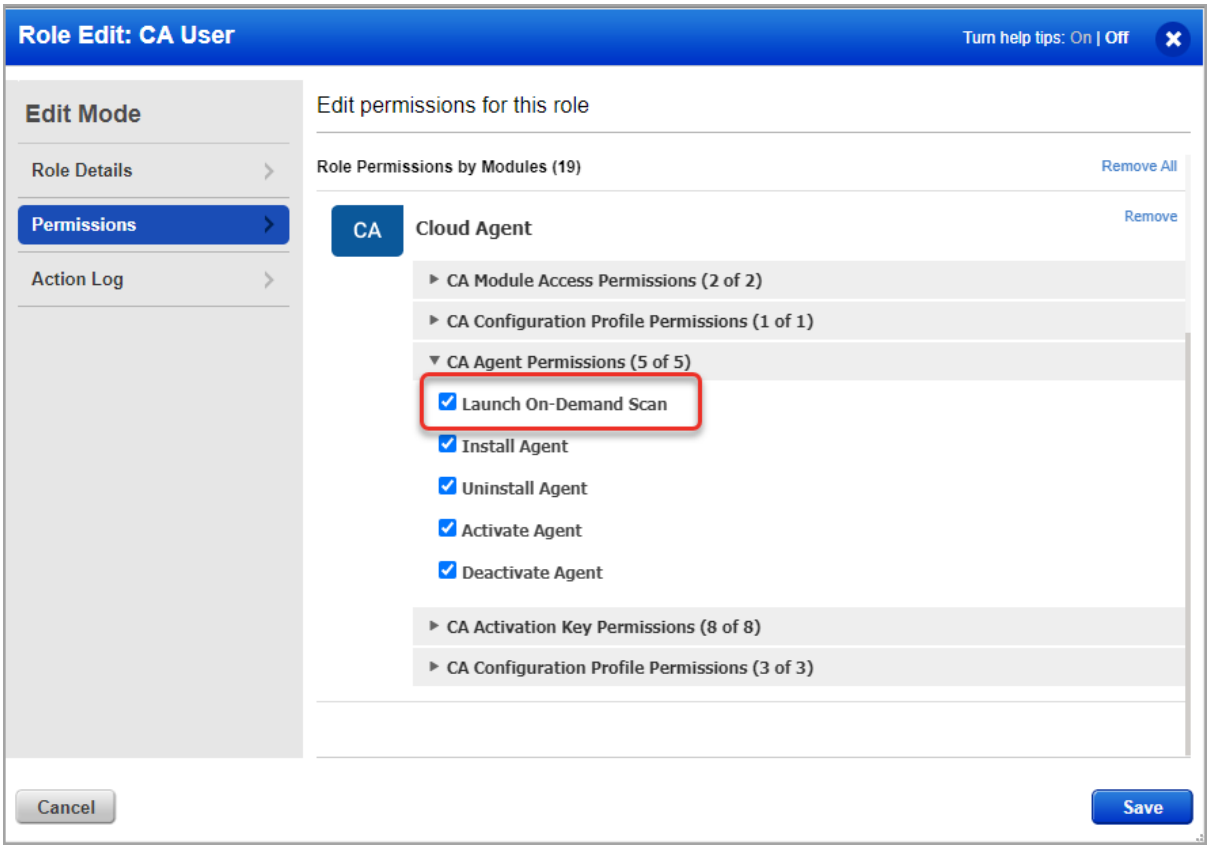
With this release, the **Asset Summary** tab displays the asset architecture type. The following screenshot is an example of the Asset Summary:



Updated Permissions for On-demand Scans

With this release, the permissions to launch on-demand scans can be assigned to a user role from the Admin module.

A new permission is added under the Role Management in the **CA Agent Permissions** section.



With the new permission, a user can launch an On-Demand Scan even if the user does not have CA Manager role access.

New Tokens in Cloud Agent

The following tokens are added to the Cloud Agent:

Token Name	Description
azure.vm.state	Find Azure VM instances in the selected state: DEALLOCATED, DEALLOCATING, DELETED, RUNNING, STARTING, STOPPED, STOPPING.
gcp.compute.state	Find GCP instances in the selected state: PENDING, RUNNING, STOPPED, TERMINATED, STOPPING, SHUTTING_DOWN, DEALLOCATED.
aws.tags	Find EC2 instances with specific tags.
aws.tags.key	Find EC2 instances with specific AWS tag keys.
aws.tags.value	Find EC2 instances with specific AWS tag values.
lastComplianceScanDate:	Find compliance scans performed on a specific date or within the specific date range.
aws.ec2.launchDate	Find EC2 instances launched on a specific date or within a specific date range.

New Feature—Cloud Agent as a Passive Sensor

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.

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.

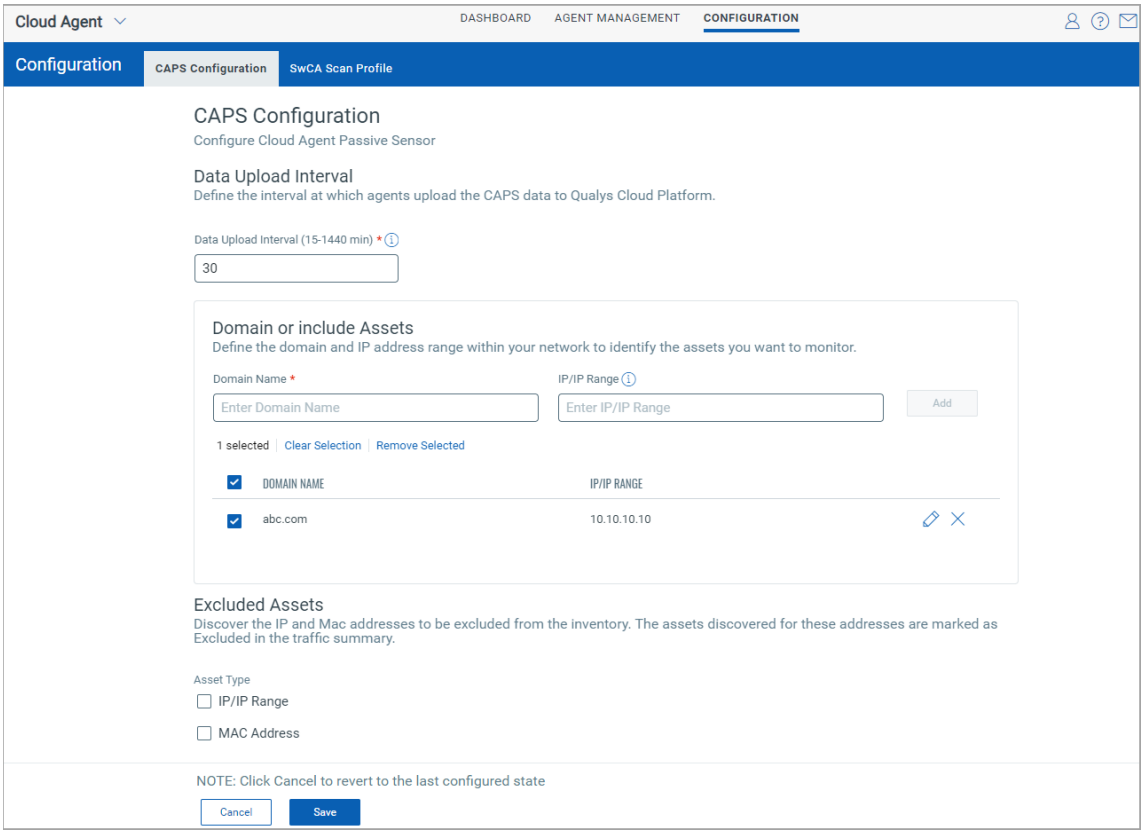
This provides you with real-time visibility to all managed and unmanaged across your global, hybrid IT environment.

The CAPS module applies only to the Windows platform. You must perform CAPS configuration before activating the CAPS module for an agent host.

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.

Configure CAPS Settings

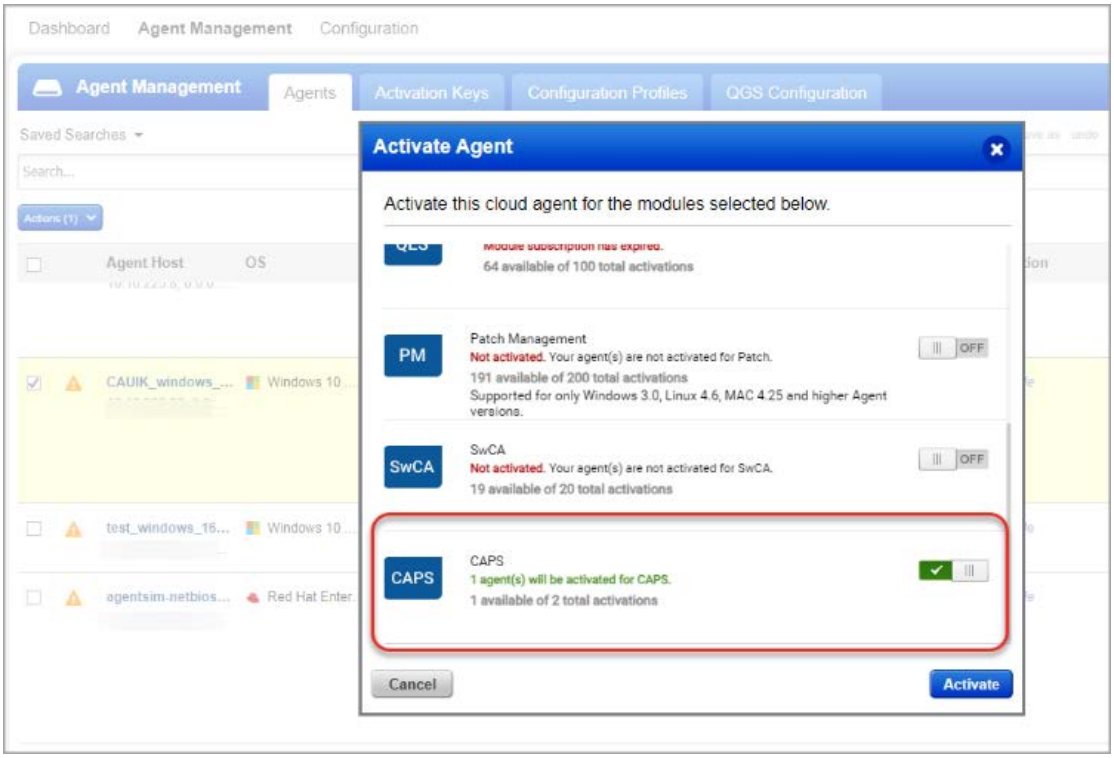
To define the settings for the Cloud Agent to work as a passive sensor, such as the interval at which data is uploaded, and the scope of passive scanning, in the Cloud Agent application, go to the **Configuration** tab and click **CAPS configuration**.



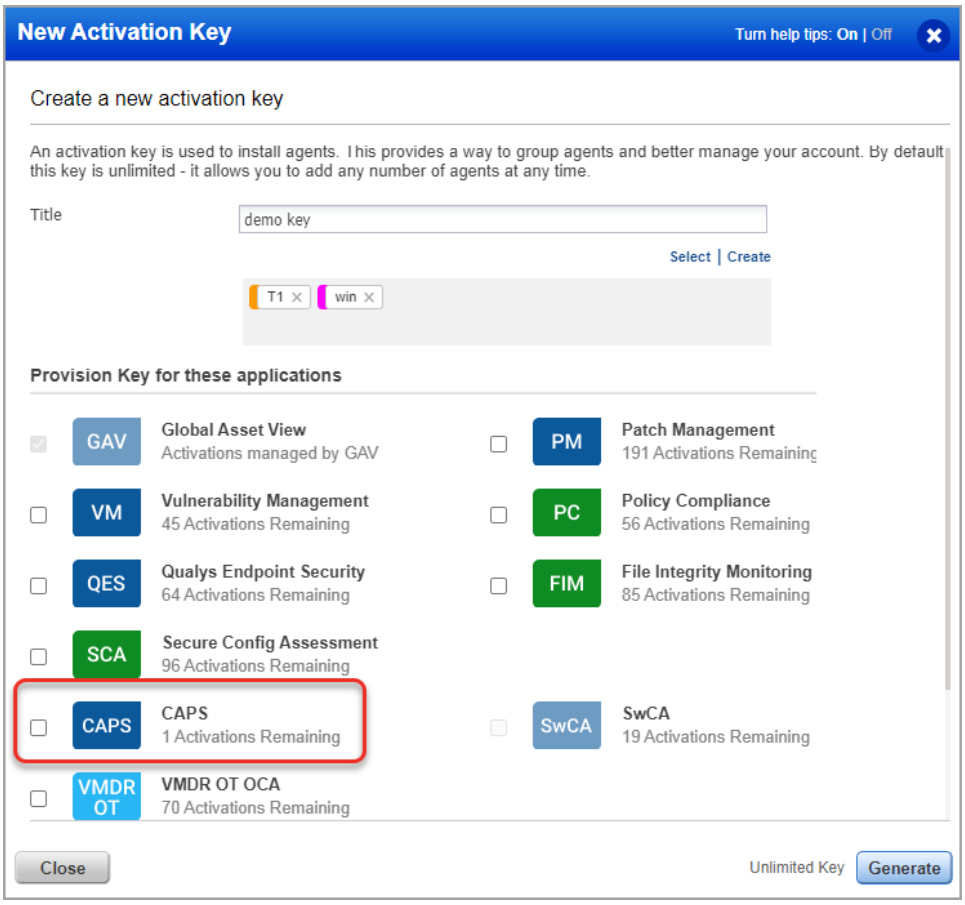
Activate CAPS Feature

To enable this functionality, you must activate the CAPS module on a single or multiple-agent host. You can activate the CAPS feature from the Agents or Activation Keys tab.

To activate the module, go to **Agent Management** > **Agents** tab, and click **Activate** for <modules> from the **Quick Actions** menu.



The following screenshot is an example that displays activating the CAPS module while creating or editing the activation key.



New Feature—Software Composition Analysis

With the software composition analysis (SwCA) feature, Cloud Agent can discover and report vulnerabilities associated with the third-party or open-source dependent software used by Qualys applications.

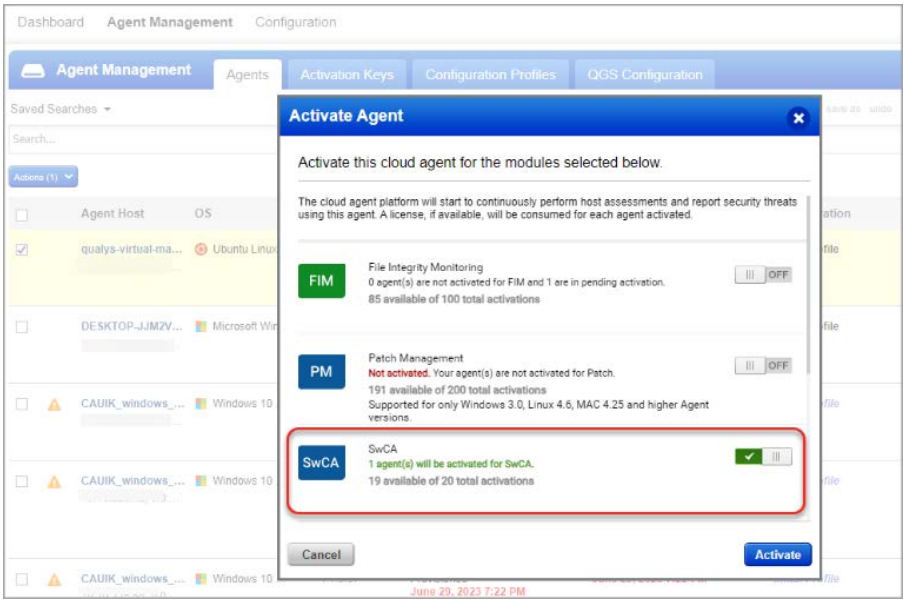
You can schedule a SwCA scan or launch the scan on demand. With the SwCA scan profile, you can define the scan scope, scan interval, and scan timeout.

SwCA is supported only for Windows and Linux Platforms and can be activated only when VM is activated for the agent.

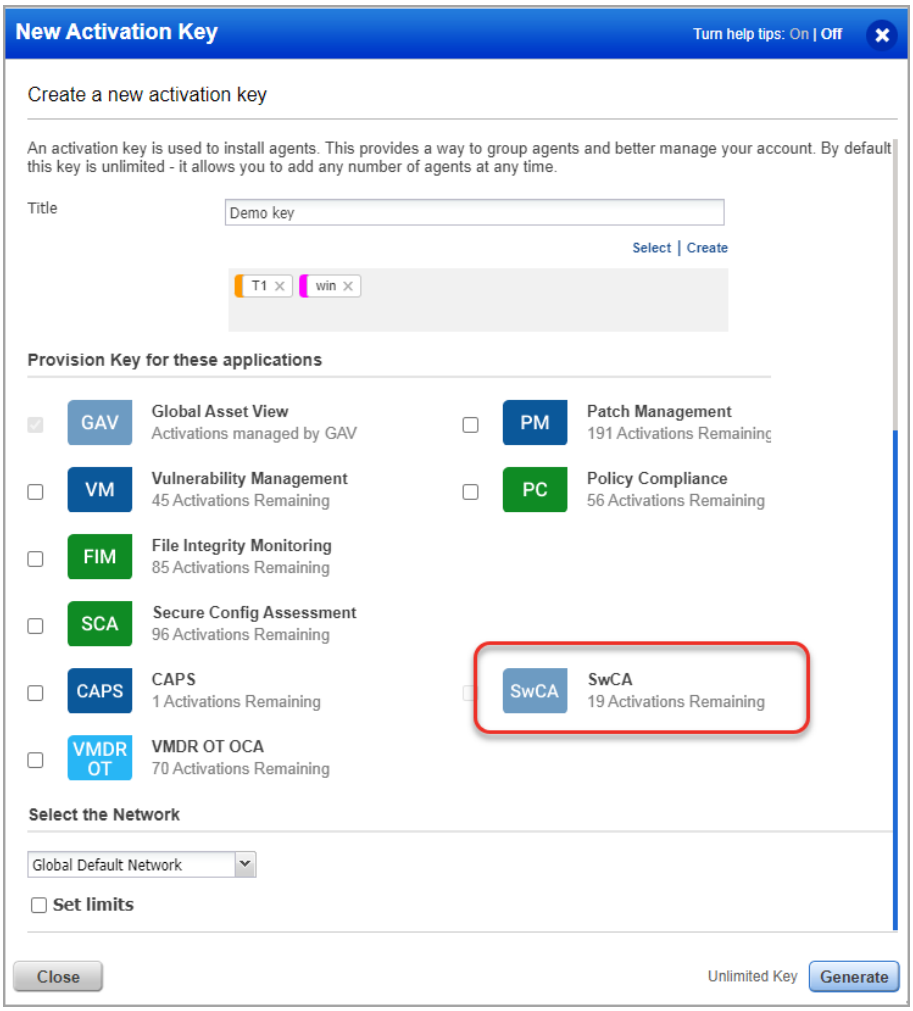
Note: This feature will be available only when the Windows and Linux agent binaries with SwCA scan support are available. For supported agent versions, refer to the *Features by Agent Version* section in the Cloud Agent Platform Availability Matrix.

Activate SwCA Feature

To enable this functionality, you must activate the SwCA 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 SwCA module while creating or editing the activation key.



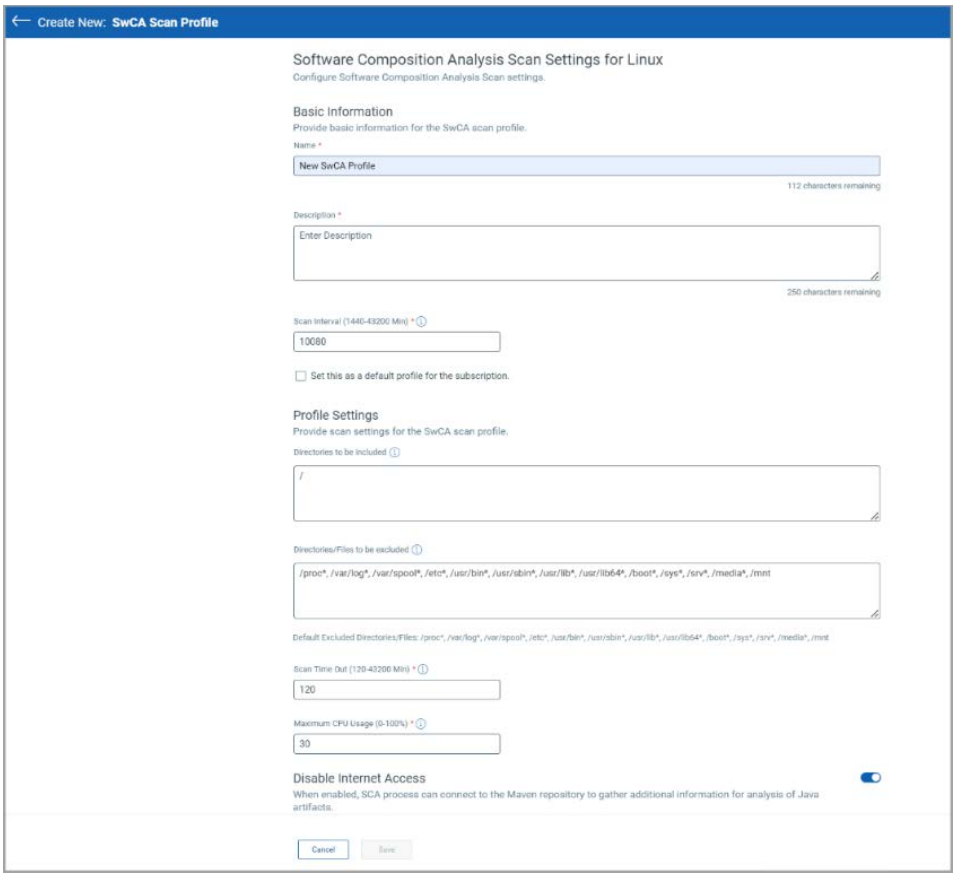
Configure SwCA Scan Settings

The default scan profile that includes scan settings and scan scope for Windows and Linux agents is provided.

You can create customized SwCA scan profile for Windows and Linux assets. To create a customized profile for the SwCA scan:

1. Go to the **Configuration** tab and click **SwCA Scan Profile**.
2. Click **Create** > **Linux Scan Profile** or **Windows Scan Profile**.
3. Enter the required values, and click **Save**.

For example, SwCA scan profile for Linux agent:



Static Tag Removal from Activation Key and Associated Agents

With this release, if a static tag attached to an activation key is removed, the tag is removed from the agents associated with the activation key when the update to the activation key is saved.

Note: This is applicable only if the **Apply changes to all the existing agents** check box is selected.

Issues Addressed

AV Asset View

- Due to differences between the VM asset name and OS computer name, the Azure VM asset name showed incorrect data. We have given priority to display the computer name as the asset name in such instances.
- We have fixed an issue where the connector was updating the hostname of the VM with an incorrect name despite VMScan being enabled.
- We fixed the tag searchability issue where a special character '&' was included in the tag name.
- A create asset purge rule failure was observed when multiple values were entered in the “agentActivationKey” attribute, as they exceeded the column width. We have now fixed this issue by increasing the column width from 2K characters to 4K characters.
- We fixed the issue wherein creating an asset purge rule using "ActivationKey" failed as extensive page loading time was taken.

CA Cloud Agent

- We have fixed an issue where the user could not deactivate the EDR (Endpoint Detection and Response) module after the subscription was removed for the respective application.
- We have fixed an issue where the agent was working with the Qualys applications. But, in the Agent Summary, the status of the field 'Last Activity' was not updated.
- We have updated the Cloud Agent online help for purge rule behavior for the following scenarios:
    - the agent is not available for more than 15 days
    - the agent becomes available within 15 days
- During merging assets, duplicate agent host entries were created in Vulnerability Management. The issue is fixed. Now, while asset merging, the reactivation is triggered after the completion of provisioning actions. This will add a delay between merge and reactivation, and chances of the creation of duplicate host ID will be minimized.

CM Continuous Monitoring

- We have updated the Continuous Monitoring online help with an example while setting notifications.

MD Web Malware Detection

- We have fixed an issue where the Manager user with full permissions could not delete a site from the Web Malware Detection application. Now, a user with Allow Edit Or Delete Malware Domains permission can delete a site.

SAQ Security Assessment Questionnaire

- We have improved the email message that users receive when someone else reassigns or delegates a questionnaire to them.

VMDR Vulnerability Management, Detection, and Response

- We have fixed an issue where an incorrect query result was generated when the user selected the Not Selected - 30 Days widget from Qualys Insights under the Vulnerabilities tab.

- We have fixed an issue where the search results for the VulnPatchable column for query vulnerabilities.vulnerability.qualysPatchable: TRUE would generate incorrect output.

- Previously, when the user downloaded the CSV report from the Vulnerabilities tab of the VMDR application, the generated downloaded report did not display any results. The issue is fixed now.

- In some QIDs, the user encountered discrepancies with the Change Log section of the Knowledgebase and Modified Dates of the Vulnerabilities tab in the VMDR application. We have fixed this issue, and the data is in sync.

- We have fixed the issue where even though the user excluded the Non-Running Kernel count for vulnerabilities in the trending widget, the search result would include the Non-Running Kernel results.

- The Customized Solution comments in the General information of Vulnerabilities details page have been enhanced to show HTML content (without converting special characters ('<', '>') into code annotations ('&lt', '&gt').

- Previously, when the user ran the QQL for a particular vulnerability severity, the search results displayed vulnerabilities with different severities. Now the QQL returns vulnerabilities with the correct severity.

WAS Web Application Scanning

- We have fixed an issue where the HTML, PDF, and PPT WAS Reports did not have the Qualys logo.

- We fixed an issue for an error occurrence faced by the user at the time of removing a web application.

- We have fixed an issue in a scan report with multiple scans where the user encountered incorrect status for vulnerabilities.

- We have fixed an issue where the user could not create the scorecard reports when specific QIDs were reported in detection.

- We have fixed an issue where the user encountered a discrepancy in the number of web applications in Web Applications Scanning (WAS) and Global Asset View (GAV) or CyberSecurity Asset Management (CSAM) application.