Runtime Software Composition Analysis (SwCA)

User Guide

February 15, 2024

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

Table of Contents

Introduction

While evaluating the security posture of an asset, it is important to identify all software packages present on the asset.

Qualys supports Software Composition Analysis (SwCA) scanning of assets. An SwCA scan discovers installed open-source software, libraries, and associated vulnerabilities on your asset. The SwCA scan identifies programming language-based software packages on the asset.For supported of list of supported languages, see Supported Languages section.

With SwCA feature, you can detect, manage, and proactively address the potential risk of software supply chain vulnerabilities in the production environment.

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.

The SwCA scan results are displayed in CyberSecurity Asset Management (CSAM). For details, see SwCA Scan Data in CyberSecurity Asset Management.

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.

Prerequisites

For downloading the SwCA data collector binary, the Cloud Agent must connect to the corresponding Qualys Content Delivery Network (CDN) URLs directly or using the proxy to download the SwCA data collector binary.

Qualys Cloud Agent continues to connect to the Cloud Agent server URLs for activities, such as configuration download, manifest download and delta uploads.

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

Supported Languages

The following tables present the languages and files SwCA supports on Linux and Windows assets.

Supported Languages - Linux

Language	File	Package managers/Ecosystem
Ruby	Gemfile.lock	bundler
Rust	Cargo.lock	cargo
PHP	composer.lock	composer
Python	Pipfile.lock	Pipenv
	poetry.lock	poetry
	requirements.txt	Pip
Go	go.mod	Go
Java	pom.xml	Apache Maven

Language	File	Package managers/Ecosystem
	gradle.lockfile	gradle
	jar/war/ear	jar
DotNet	packages.lock.json	Nuget
	packages.config	Nuget
	.deps.json	dotnet-core
NodeJs	package-lock.json	npm
	yarn.lock	yarn

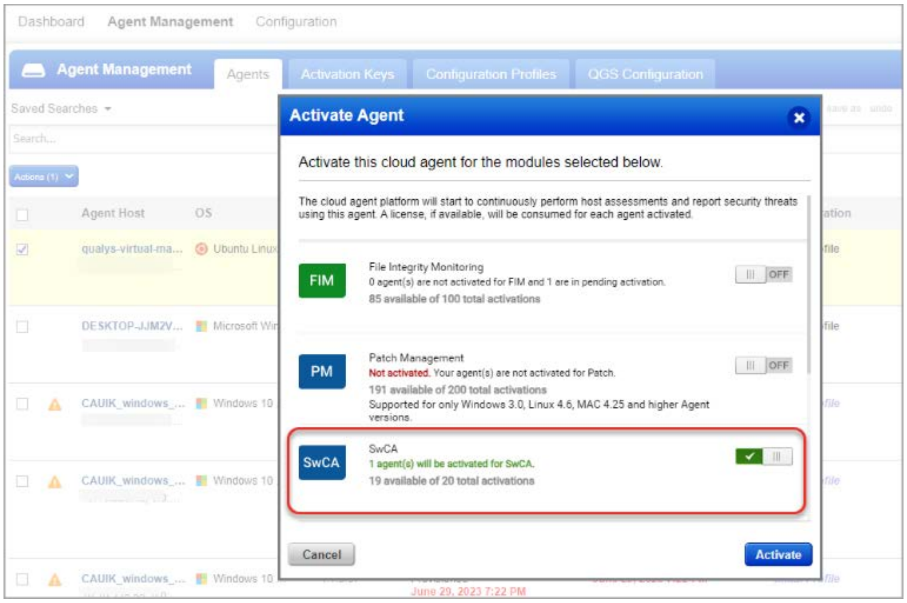
Supported Languages - Windows

Language	File
DotNet	.deps.json
	.packages.config
	nuspec
	nupkg
Go	go.sum
	go.mod
Java	jar
	war
	ear
	pom.properties
	META-INF/MANIFEST.MF
	pom.xml
	gradle.lockfile
Node.js	package.json
	.package-lock.json
	npm-shrinkwrap.json
PHP	composer.json
	composer.lock
Python	egg
	egg-info/METADATA
	egg-info\\METADATA
	egg-info/PKG-INFO
	dist-info/METADATA
	dist-info\\METADATA
	poetry.lock

Language	File
	requirements.txt
Rust	Cargo.lock
Ruby	Gemfile.lock (bundler)
	gemspec

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.



Activate this cloud agent for the modules selected below.

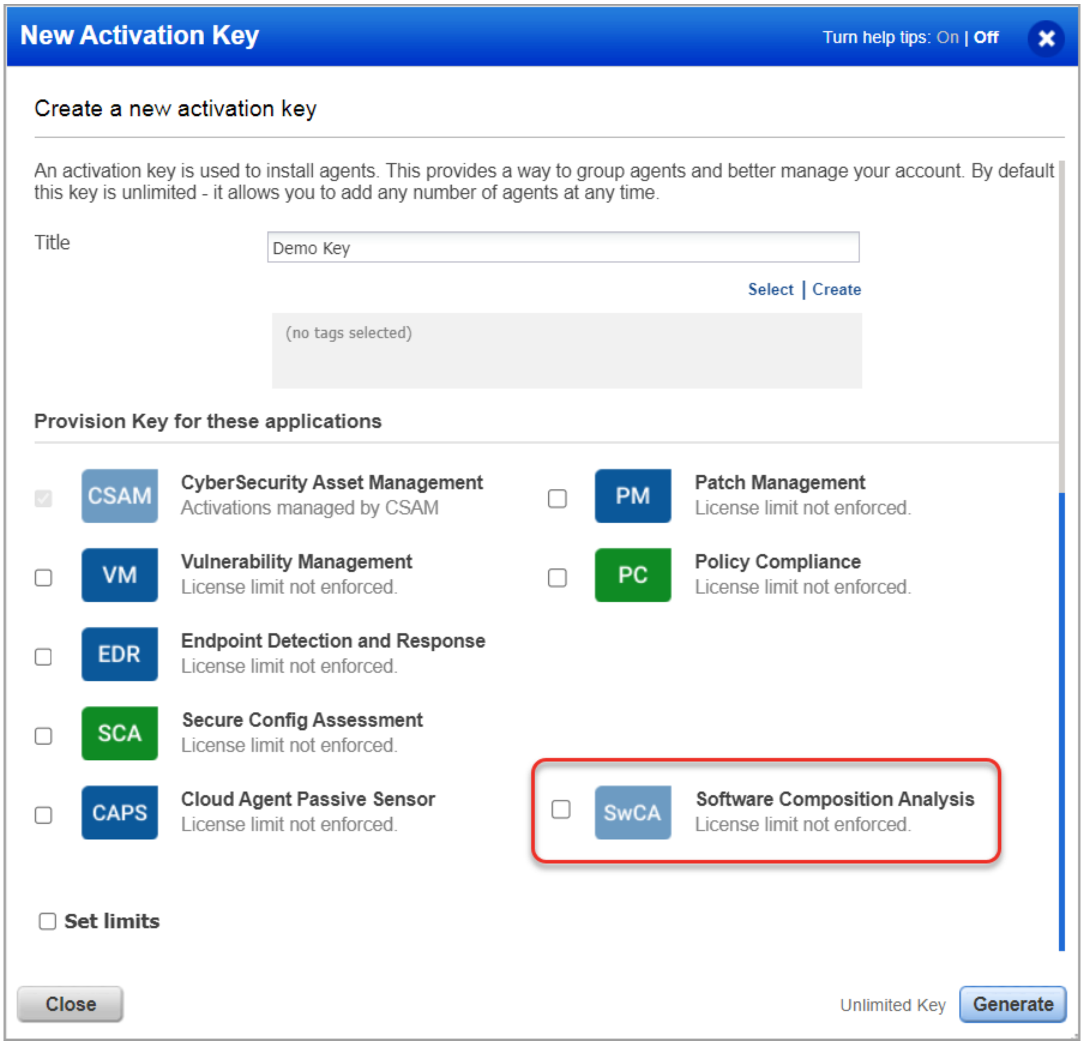
The cloud agent platform will start to continuously perform host assessments and report security threats using this agent. A license, if available, will be consumed for each agent activated.

File Integrity Monitoring
0 agent(s) are not activated for FIM and 1 are in pending activation.
85 available of 100 total activations

Patch Management
Not activated. Your agent(s) are not activated for Patch.
191 available of 200 total activations
Supported for only Windows 3.0, Linux 4.6, MAC 4.25 and higher Agent versions.

SwCA
1 agent(s) will be activated for SwCA.
19 available of 20 total activations

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



New Activation Key

Create a new activation key

An activation key is used to install agents. This provides a way to group agents and better manage your account. By default this key is unlimited - it allows you to add any number of agents at any time.

Title: Demo Key

(no tags selected)

Provision Key for these applications

☑ CSAM	CyberSecurity Asset Management Activations managed by CSAM	□ PM	Patch Management License limit not enforced.
□ VM	Vulnerability Management License limit not enforced.	□ PC	Policy Compliance License limit not enforced.
□ EDR	Endpoint Detection and Response License limit not enforced.		
□ SCA	Secure Config Assessment License limit not enforced.		
□ CAPS	Cloud Agent Passive Sensor License limit not enforced.	□ SwCA	Software Composition Analysis License limit not enforced.

□ Set limits

Unlimited Key

Installation and Uninstallation

When the SwCA application is activated for a Cloud Agent, the following files are downloaded from the Qualys CDN server and installed on the asset:

- For Linux assets—. `qualys-swca-datacollector` package. You can view the SwCA application installed as the `qualys-swca-datacollector` package in the software package manager of the operating system.
- For Windows assets— `SwCAScanner.exe` file. During the SwCA scanning process, the `SwCAScanner.exe` appears among the running processes of the operating system.

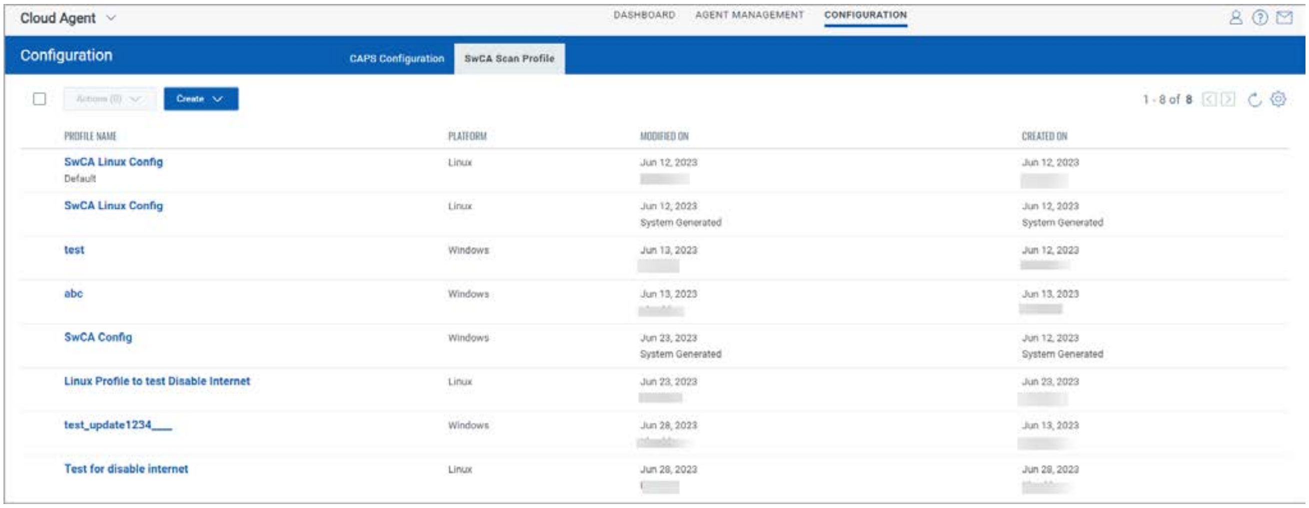
For list of Qualys CDN URLs, see the Prerequisites section.

When the SwCA application is deactivated for the Cloud Agent, the `qualys-swca-datacollector` package is uninstallaed from the Linux asset, and the `SwCAScanner.exe` file is removed from the Windows assets.

Configure SwCA Scan Settings

You can configure the software composition analysis scan settings for Windows and Linux assets. The **SwCA Scan Profile** tab under **Configuration** contains the default profiles for Windows and Linux agents.

By default, one SwCA scan profile is available for Windows and Linux each.



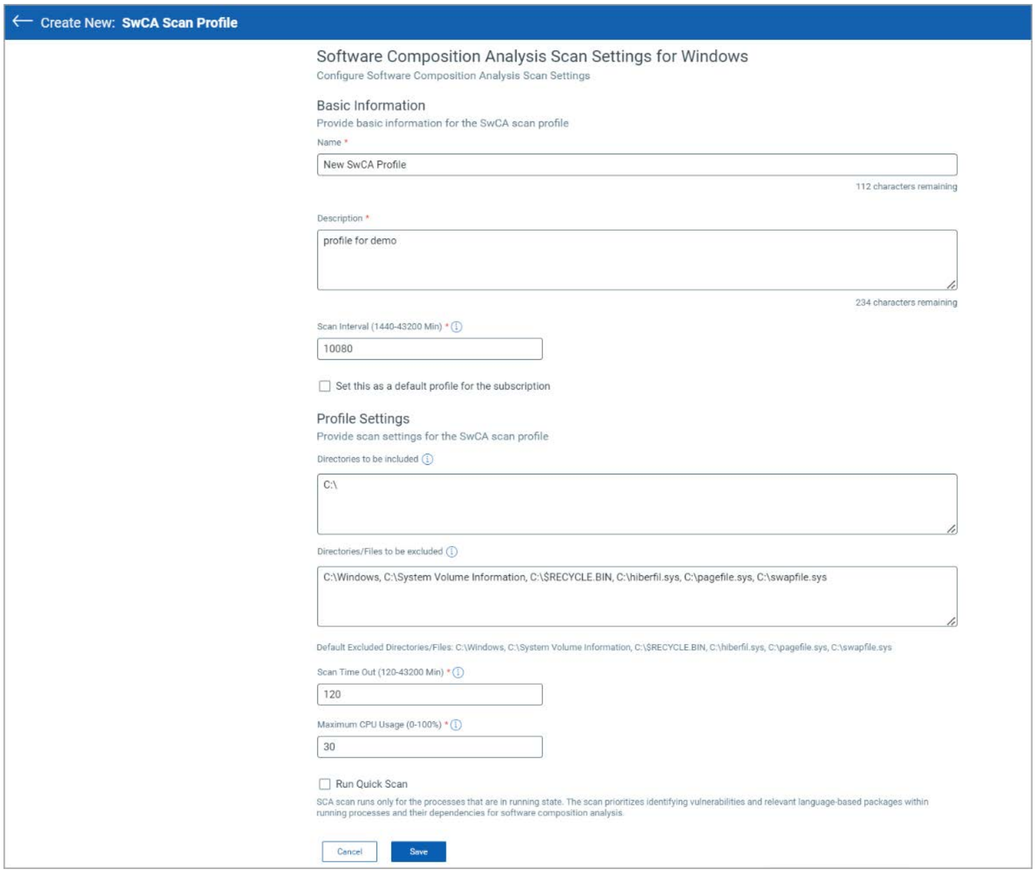
PROFILE NAME	PLATFORM	MODIFIED ON	CREATED ON
SwCA Linux Config Default	Linux	Jun 12, 2023 [redacted]	Jun 12, 2023 [redacted]
SwCA Linux Config	Linux	Jun 12, 2023 System Generated	Jun 12, 2023 System Generated
test	Windows	Jun 13, 2023 [redacted]	Jun 12, 2023 [redacted]
abc	Windows	Jun 13, 2023 [redacted]	Jun 13, 2023 [redacted]
SwCA Config	Windows	Jun 23, 2023 System Generated	Jun 12, 2023 System Generated
Linux Profile to test Disable Internet	Linux	Jun 23, 2023 [redacted]	Jun 23, 2023 [redacted]
test_update1234___	Windows	Jun 28, 2023 [redacted]	Jun 13, 2023 [redacted]
Test for disable internet	Linux	Jun 28, 2023 [redacted]	Jun 28, 2023 [redacted]

You can also create customized SwCA scan profiles 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**.

SwCA Scan Profile - Windows

To create a new profile for SwCA scan on Windows assets, click **Create** > **Windows Scan Profile**.



Software Composition Analysis Scan Settings for Windows

Configure Software Composition Analysis Scan Settings

Basic Information

Provide basic information for the SwCA scan profile

Name *: New SwCA Profile

112 characters remaining

Description *: profile for demo

234 characters remaining

Scan Interval (1440-43200 Min) *: 10080

□ Set this as a default profile for the subscription

Profile Settings

Provide scan settings for the SwCA scan profile

Directories to be included: C:\

Directories/Files to be excluded: C:\Windows, C:\System Volume Information, C:\$RECYCLE.BIN, C:\hiberfil.sys, C:\pagefile.sys, C:\swapfile.sys

Default Excluded Directories/Files: C:\Windows, C:\System Volume Information, C:\$RECYCLE.BIN, C:\hiberfil.sys, C:\pagefile.sys, C:\swapfile.sys

Scan Time Out (120-43200 Min) *: 120

Maximum CPU Usage (0-100%) *: 30

□ Run Quick Scan

SCA scan runs only for the processes that are in running state. The scan prioritizes identifying vulnerabilities and relevant language-based packages within running processes and their dependencies for software composition analysis.

In the **Create New: SwCA Scan Profile** page, enter the following information:

Basic Information

- Enter **Name** and **Description** for the new scan profile.
- **Scan Interval** - Define the interval, in minutes, at which the agent scans the assets associated with this profile. The default value is 10080 minutes.
- If you want to set this scan profile as a default software composition analysis scan profile for your subscription, select the Set this as a default profile for the subscription check box. This will be a user-defined default profile.

Profile Settings

You can define the scope for the SwCA scan by adding directories to be included in the scan. You can also specify the files or directories that you want to exclude from the scan.

- **Directories Included** - You can define the directories to be included in the scan. By default, the */ directory is included for scan. You can enter multiple directories separated by comma. SwCA scans only the local drives of Windows assets.

  Ensure that only the absolute path is supported. The field does not support wildcard characters and regular expressions.

  Note: Include only specific directories in the scan scope to reduce CPU and memory consumption.

- **Directories/Files to be excluded** - You can exclude specific files or directories from the SwCA scan. To define the files/directories to be excluded, you can enter multiple directories separated by a comma.

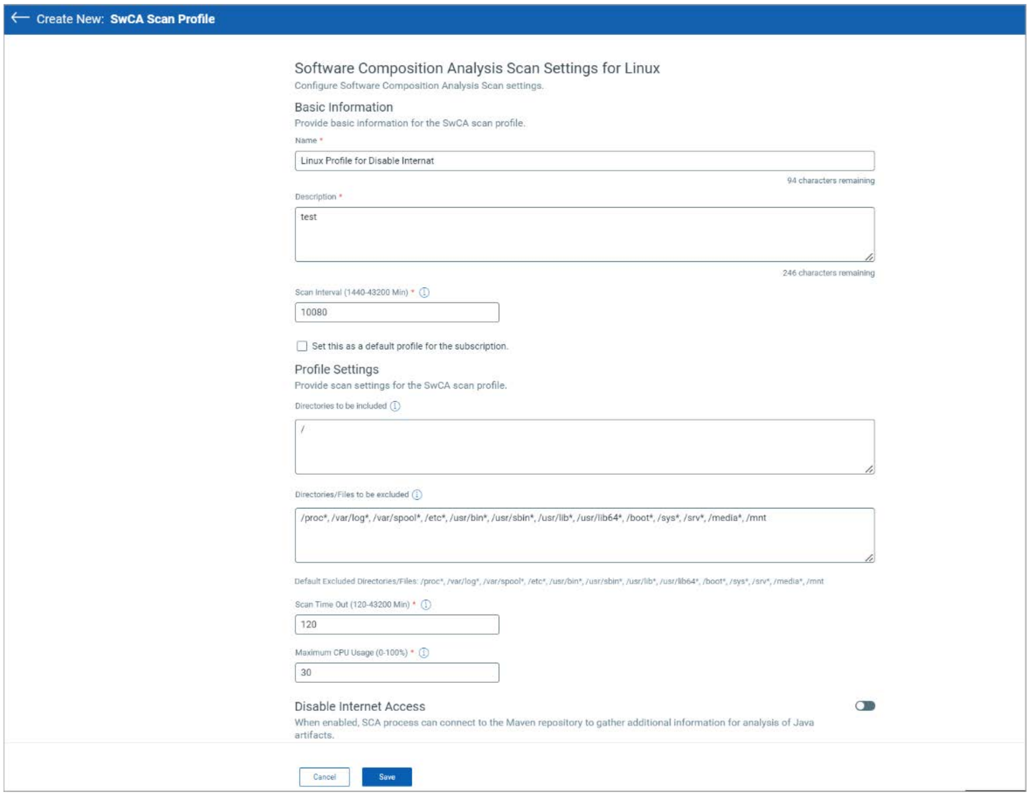
  Ensure that only the absolute path is supported. The field does not support wildcard characters and regular expressions.

  Note: Exclude the directories that do contain relevant data for SwCA scan to reduce CPU memory consumption.
- **Scan Time Out**- Define the maximum time after which the scan is terminated. The default value is 120 minutes.
- **CPU Usage**- Enter the maximum CPU consumption allowed for the SCA scan process. However, a momentary spike can occur in CPU usage.
- **Run Quick Scan**- Select the check box to run a scan on the running processes.

Click **Save** to save the scan settings configured.

SwCA Profile - Linux

To create a new profile for SwCA scan on Linux assets, click **Create** > **Linux Scan Profile**.



← Create New: **SwCA Scan Profile**

Software Composition Analysis Scan Settings for Linux

Configure Software Composition Analysis Scan settings.

Basic Information

Provide basic information for the SwCA scan profile.

Name *

Linux Profile for Disable Internat

94 characters remaining

Description *

test

246 characters remaining

Scan Interval (1440-43200 Min) *

10080

□ Set this as a default profile for the subscription.

Profile Settings

Provide scan settings for the SwCA scan profile.

Directories to be included

/

Directories/Files to be excluded

/proc*, /var/log*, /var/spool*, /etc*, /usr/bin*, /usr/sbin*, /usr/lib*, /usr/lib64*, /boot*, /sys*, /srv*, /media*, /mnt

Default Excluded Directories/Files: /proc*, /var/log*, /var/spool*, /etc*, /usr/bin*, /usr/sbin*, /usr/lib*, /usr/lib64*, /boot*, /sys*, /srv*, /media*, /mnt

Scan Time Out (120-43200 Min) *

120

Maximum CPU Usage (0-100%) *

30

Disable Internet Access

When enabled, SCA process can connect to the Maven repository to gather additional information for analysis of Java artifacts.

In the **Create New - SwCA Scan Profile** page, enter the following information:

Basic Information

- **Enter Name** and **Description** for the new scan profile.
- **Scan Interval**- Define the interval, in minutes, at which the agent scans the assets associated with this profile. The default value is 10080 minutes.

- If you want to set this scan profile as a default software composition analysis scan profile for your subscription, select the **Set this as a default profile for the subscription** check box. This will be a user-defined default profile.

Profile Settings

You can define the scope for the SwCA scan by adding directories to be included in the scan. You can also specify the files or directories that you want to exclude from the scan.

- **Directories Included** - You can define the directories to be included in the scan. By default, the */ directory is included for scan. You can enter multiple directories separated by comma.

  By default, root is included in the Linux Scan profile. However, the following common network filesystems are excluded from SwCA scan:
    - afs
    - cifs
    - fuse.sshfs
    - gfs
    - gfs2
    - nfs
    - nfs4
    - nfsd
    - safenetfs
    - secfs
    - smb2
    - smbfs
    - vxfs
    - vxodmfs

  Ensure that only absolute path is supported. The field does not support wildcard characters and regular expressions.

  Note: Include only specific directories in the scan scope to reduce CPU and memory consumption.

- **Directories/Files to be excluded** - You can exclude specific files or directories from the SwCA scan. To define the files/directories to be excluded, you can enter multiple directories separated by comma.

  Ensure that only the absolute path is supported. The field does not support wildcard characters and regular expressions.

  Note: Exclude the directories that do not contain relevant data for SwCA scan to reduce CPU memory consumption.

- **Scan Time Out** - Define the maximum time after which the scan is terminated. The default value is 120 minutes.

- **CPU** Usage - Enter the maximum CPU consumption allowed for the SCA scan process. However, a momentary spike can occur in CPU usage.

- **Disable Internet Access**- Turn the **Disable Internet Access** on or off to disconnect or connect to the Internet. When internet connectivity is enabled, the SCA process can connect to the Maven repository to gather additional information to analyze Java artifacts.

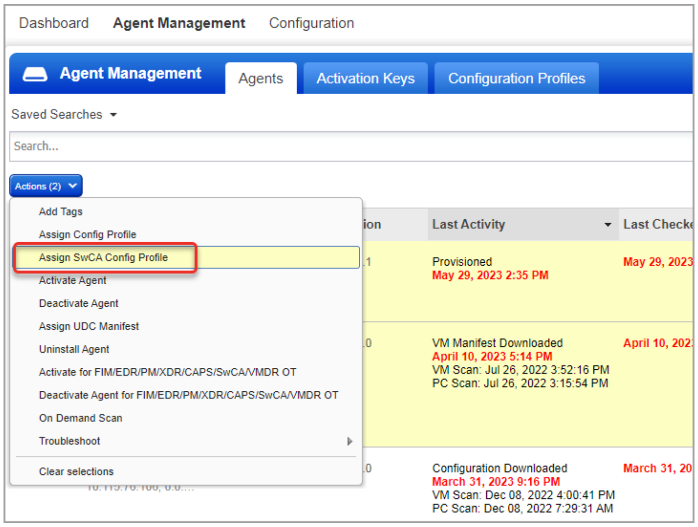
Click **Save** to save the SwCA scan settings that you have configured.

Assign Customized SwCA Configuration Profile

If you want to use a customized SwCA configuration profile, you must assign the SwCA configuration profile to the host asset.

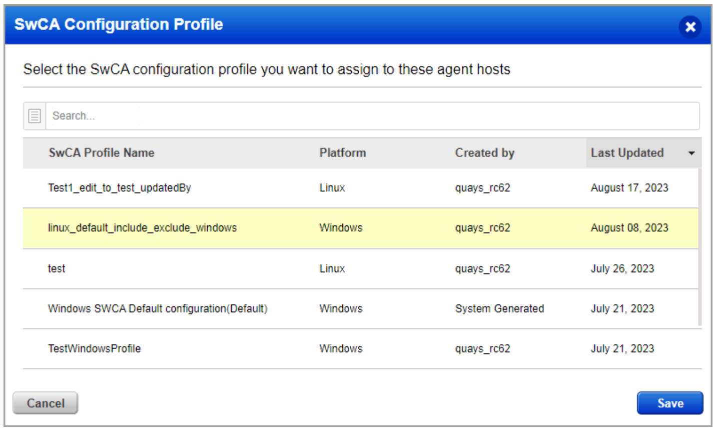
To assign the custom SwCA configuration profile:

1. From the list of assets, select host asset, and from the **Actions** menu, click **Assign SwCA Config Profile**.



ion	Last Activity	Last Checke
1	Provisioned May 29, 2023 2:35 PM	May 29, 2023
0	VM Manifest Downloaded April 10, 2023 5:14 PM VM Scan: Jul 26, 2022 3:52:16 PM PC Scan: Jul 26, 2022 3:15:54 PM	April 10, 202
0	Configuration Downloaded March 31, 2023 9:16 PM VM Scan: Dec 08, 2022 4:00:41 PM PC Scan: Dec 08, 2022 7:29:31 AM	March 31, 20

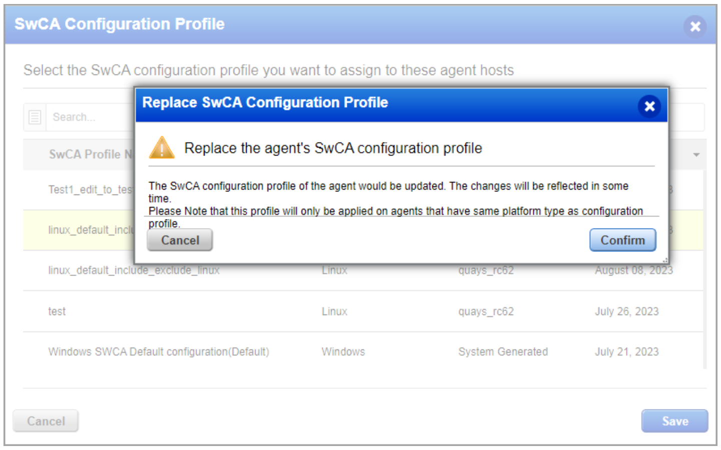
2. From the list of SwCA configuration profiles, select the configuration profile to be assigned to the selected host asset and click **Save**.



Select the SwCA configuration profile you want to assign to these agent hosts

SwCA Profile Name	Platform	Created by	Last Updated
Test1_edit_to_test_updatedBy	Linux	quays_rc62	August 17, 2023
linux_default_include_exclude_windows	Windows	quays_rc62	August 08, 2023
test	Linux	quays_rc62	July 26, 2023
Windows SWCA Default configuration(Default)	Windows	System Generated	July 21, 2023
TestWindowsProfile	Windows	quays_rc62	July 21, 2023

3. Click **Confirm** to replace the default SwCA configuration profile assigned to the host asset.



Select the SwCA configuration profile you want to assign to these agent hosts

SwCA Profile N			
Test1_edit_to_tes			
linux_default_incl			
linux_default_include_exclude_linux	Linux	quays_rc62	August 08, 2023
test	Linux	quays_rc62	July 26, 2023
Windows SWCA Default configuration(Default)	Windows	System Generated	July 21, 2023

Replace SwCA Configuration Profile

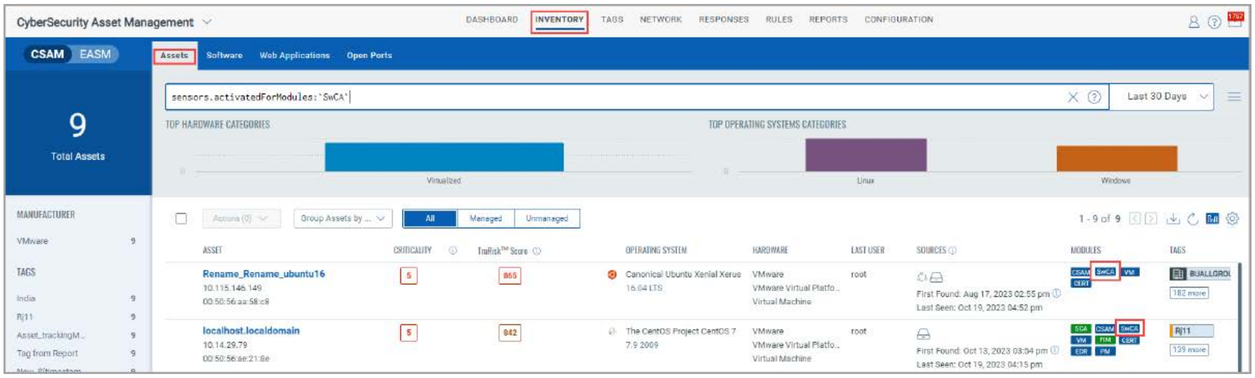
Replace the agent's SwCA configuration profile

The SwCA configuration profile of the agent would be updated. The changes will be reflected in some time.
Please Note that this profile will only be applied on agents that have same platform type as configuration profile.

The selected SwCA configuration profile is assigned to the selected host asset.

SwCA Scan Data in CyberSecurity Asset Management

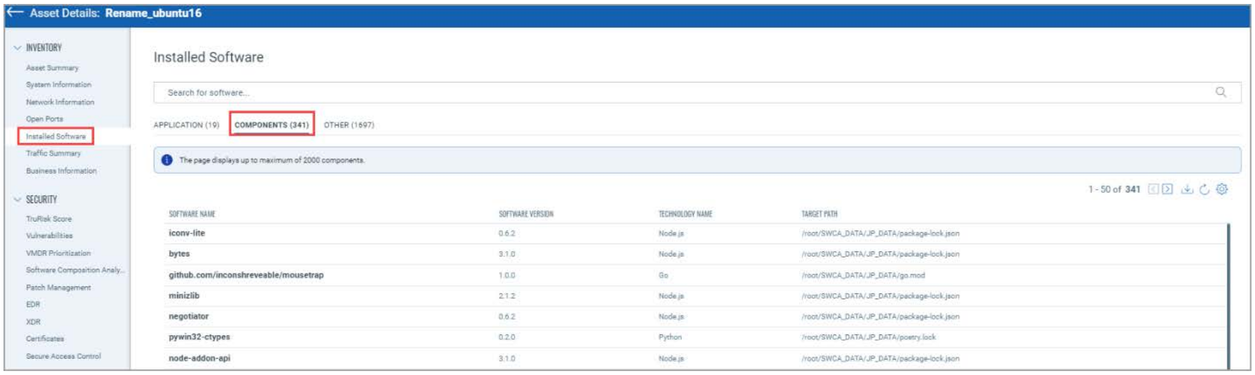
You can view the assets on which the SwCA feature is activated in the **Assets** tab with the SwCA tag added.



```
sensors.activatedForModules:`SwCA`
```

ASSET	CRITICALITY	TruRisk™ Score	OPERATING SYSTEM	HARDWARE	LAST USER	SOURCES	MODULES	TAGS
Rename_Rename_ubuntu16 10.115.146.149 00:50:56:aa:58:c8	5	865	Canonical Ubuntu Xenial Xerus 16.04 LTS	VMware VMware Virtual Platfo... Virtual Machine	root	First Found: Aug 17, 2023 02:55 pm Last Seen: Oct 19, 2023 04:52 pm	CSAM SwCA VM CERT	BUALLGROU 182 more
localhost.localdomain 10.14.29.79 00:50:56:ae:21:8e	5	842	The CentOS Project CentOS 7 7.9 2009	VMware VMware Virtual Platfo... Virtual Machine	root	First Found: Oct 13, 2023 03:54 pm Last Seen: Oct 19, 2023 04:15 pm	SCA CSAM SwCA VM FIM CERT EDR PM	Rj11 139 more

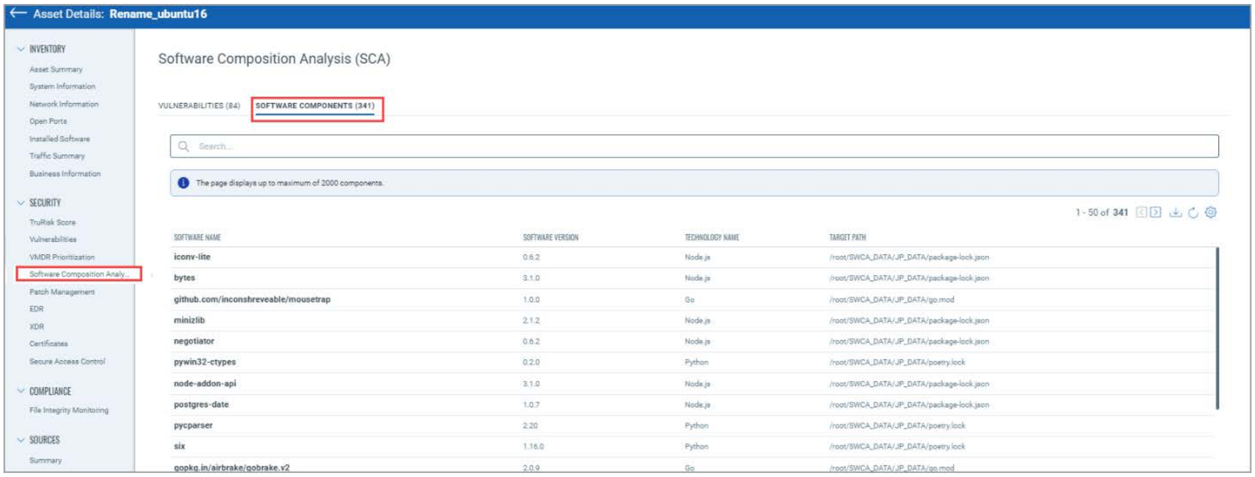
For the assets on which SwCA is activated, you can see the SwCA data from the Asset Details page. From the **Installed Software** tab, you can see the Components details.



The page displays up to maximum of 2000 components.

SOFTWARE NAME	SOFTWARE VERSION	TECHNOLOGY NAME	TARGET PATH
iconv-lite	0.6.2	Node.js	/root/SWCA_DATA/JP_DATA/package-lock.json
bytes	3.1.0	Node.js	/root/SWCA_DATA/JP_DATA/package-lock.json
github.com/inconshreveable/mousetrap	1.0.0	Go	/root/SWCA_DATA/JP_DATA/go.mod
minizlib	2.1.2	Node.js	/root/SWCA_DATA/JP_DATA/package-lock.json
negotiator	0.6.2	Node.js	/root/SWCA_DATA/JP_DATA/package-lock.json
pywin32-ctypes	0.2.0	Python	/root/SWCA_DATA/JP_DATA/poetry.lock
node-addon-api	3.1.0	Node.js	/root/SWCA_DATA/JP_DATA/package-lock.json

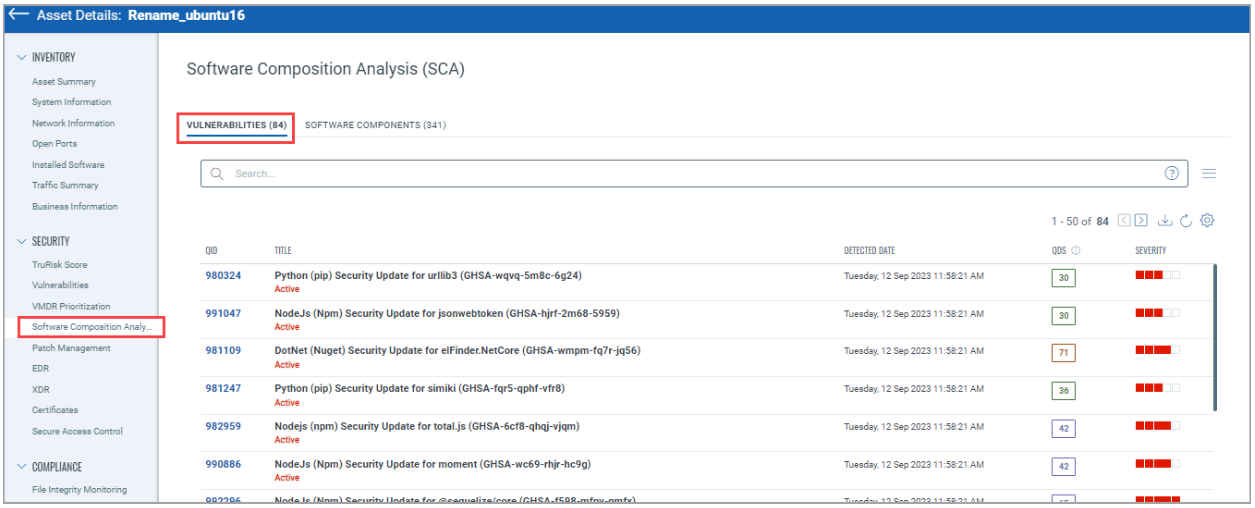
From the **Software Component Analysis** tab, you can see the Software Components and Vulnerabilities identified.



Software Composition Analysis (SCA)

The page displays up to maximum of 2000 components.

SOFTWARE NAME	SOFTWARE VERSION	TECHNOLOGY NAME	TARGET PATH
iconv-lite	0.6.2	Node.js	/root/SWCA_DATA/JP_DATA/package-lock.json
bytes	3.1.0	Node.js	/root/SWCA_DATA/JP_DATA/package-lock.json
github.com/inconshreveable/mousetrap	1.0.0	Go	/root/SWCA_DATA/JP_DATA/go.mod
minizlib	2.1.2	Node.js	/root/SWCA_DATA/JP_DATA/package-lock.json
negotiator	0.6.2	Node.js	/root/SWCA_DATA/JP_DATA/package-lock.json
pywin32-ctypes	0.2.0	Python	/root/SWCA_DATA/JP_DATA/poetry.lock
node-addon-api	3.1.0	Node.js	/root/SWCA_DATA/JP_DATA/package-lock.json
postgres-date	1.0.7	Node.js	/root/SWCA_DATA/JP_DATA/package-lock.json
pycparser	2.20	Python	/root/SWCA_DATA/JP_DATA/poetry.lock
six	1.16.0	Python	/root/SWCA_DATA/JP_DATA/poetry.lock
gopkg.in/airbrake/gobrake.v2	2.0.9	Go	/root/SWCA_DATA/JP_DATA/go.mod



Software Composition Analysis (SCA)

QID	TITLE	DETECTED DATE	QDS	SEVERITY
980324	Python (pip) Security Update for urllib3 (GHSA-wqvq-5m8c-6g24) Active	Tuesday, 12 Sep 2023 11:58:21 AM	30	🟥🟥🟥□□
991047	NodeJs (Npm) Security Update for jsonwebtoken (GHSA-hjrf-2m68-5959) Active	Tuesday, 12 Sep 2023 11:58:21 AM	30	🟥🟥🟥□□
981109	DotNet (Nuget) Security Update for elFinder.NetCore (GHSA-wmpm-fq7r-jq56) Active	Tuesday, 12 Sep 2023 11:58:21 AM	71	🟥🟥🟥🟥□
981247	Python (pip) Security Update for simiki (GHSA-fqr5-qphf-vfr8) Active	Tuesday, 12 Sep 2023 11:58:21 AM	36	🟥🟥🟥□□
982959	Nodejs (npm) Security Update for total.js (GHSA-6cf8-qhqj-vjqm) Active	Tuesday, 12 Sep 2023 11:58:21 AM	42	🟥🟥🟥🟥□
990886	NodeJs (Npm) Security Update for moment (GHSA-wc69-rhjr-hc9g) Active	Tuesday, 12 Sep 2023 11:58:21 AM	42	🟥🟥🟥🟥□
992296	Node.Js (Npm) Security Update for @sequelize/core (GHSA-f598-mfpv-gmfx)	Tuesday, 12 Sep 2023 11:58:21 AM	[illegible]	🟥🟥🟥🟥🟥