



Qualys Cloud Suite 2.19

We're excited to tell you about new features and improvements coming with Qualys Cloud Suite 2.19.

CA Cloud Agent

Searching Cloud Agents Just Got Easier
New Widgets Added to your Dashboard

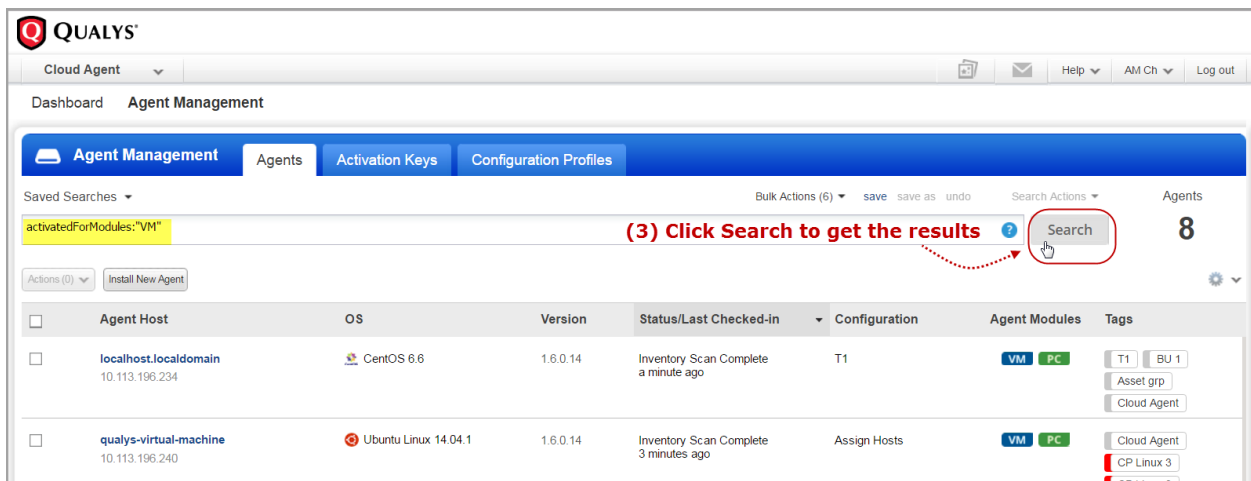
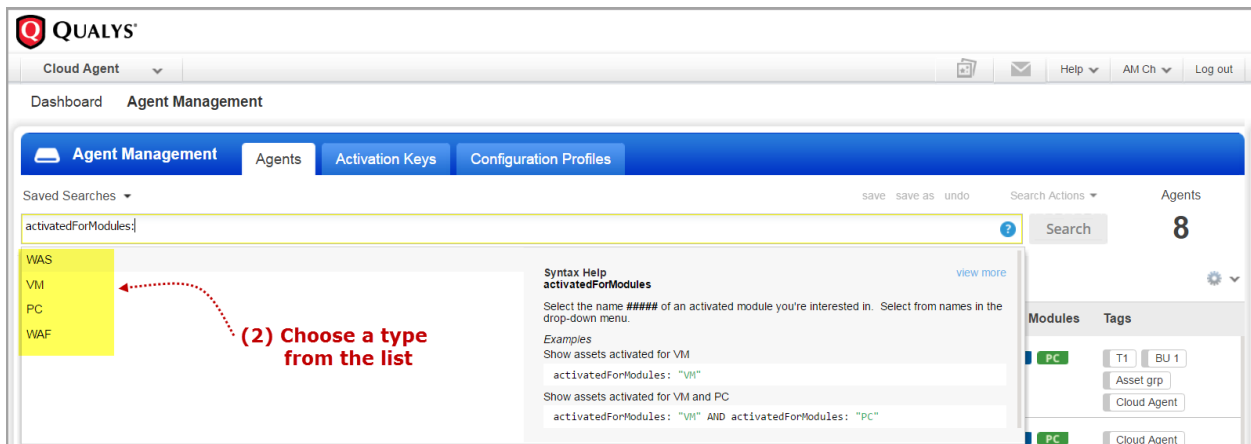
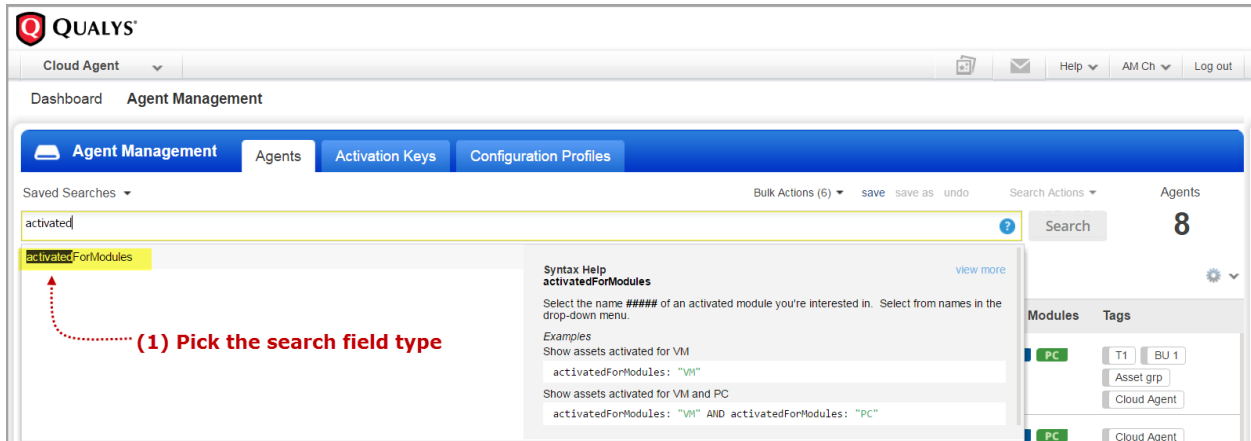
WAS Web Application Scanning

Option Profile – New Form Crawl Scope option

Qualys Cloud Suite Update 2.19 brings you many more improvements and updates! [Learn more](#)

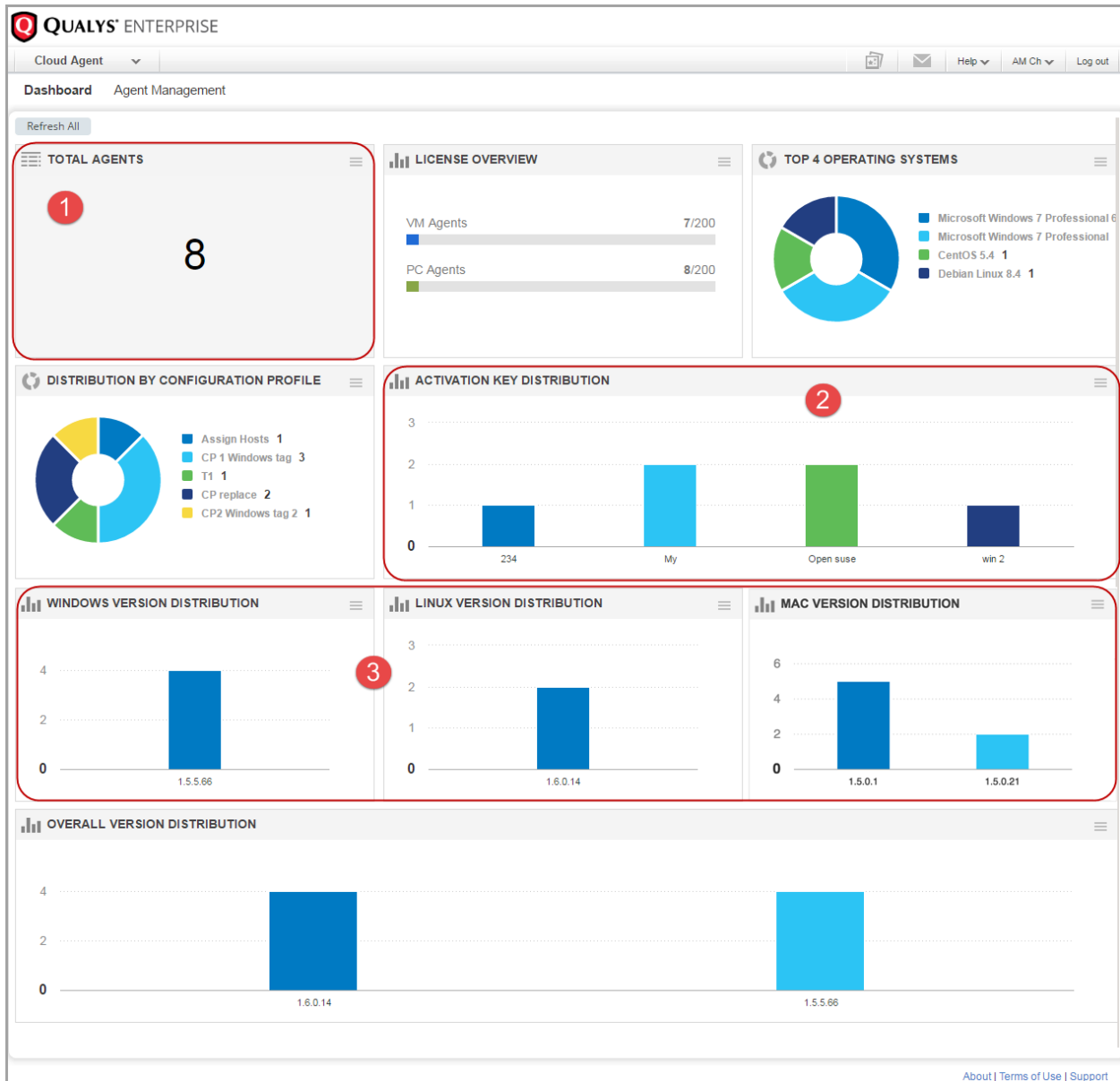
Searching Cloud Agents Just Got Easier

Now when you search for agents by active modules type you can simply choose from a list of values that we provide. This way you can be sure your query is set up correctly.



New Widgets Added to your Dashboard

We added new widgets to the dashboard for a quick information on total agents and distribution of your agents (total agents, activation key distribution and version distribution).



Option Profile – New Form Crawl Scope option

Forms considered unique are reported separately in your account. We'll always use form field names to calculate form uniqueness. When you select the new "Form Crawl Scope" option to include form action URI in the option profile, we'll use form action URI and form field name for determining the uniqueness of a form.

Good to Know:

To prevent forms with same fields from being ignored during the scan, you should enable Form Crawl Scope to include action URI.

Option Profile Creation Turn help tips: On | Off Launch help

Step 2 of 5

Please define how the scan will perform

General Settings (*) REQUIRED FIELDS

Form Submission* Post & Get

Form Crawl Scope Include form action URI in form uniqueness calculation.

When enabled, we'll calculate form uniqueness using form action URI in addition to form field names. This results in crawling of all forms having same fields but having different action URI.

Maximum links to test in scope* 300

Total number of links and forms to follow and test within the scan scope. If performing a Discovery Scan, this is the maximum links that will be crawled, as there will not be any testing performed

User Agent Example: Mozilla/4.04 (X11; I; SunOS 5.4 sun4m)

Request Parameter Set* Initial Parameters (Default) View Create

Document Type Ignore common binary files based on file extensions.

SmartScan Support

When enabled we'll perform advanced scanning, using enhanced AJAX/SPA deep crawling and vulnerability testing, for a number of actions per page. This option is recommended for scanning sites with advanced frameworks and technologies.

Cancel Previous Continue

Option Profile Creation Turn help tips: On | Off Launch help

Step 5 of 5

Review and confirm this Option Profile

Profile Details

Name Test

Default Profile No

Owner Anjali Pingale (quays_ap14)

Tags (no tags selected)

Scan Parameters

Form Submission Post & Get

Form Crawl Scope Include form action URI in uniqueness calculation.

Maximum links to test in scope 300

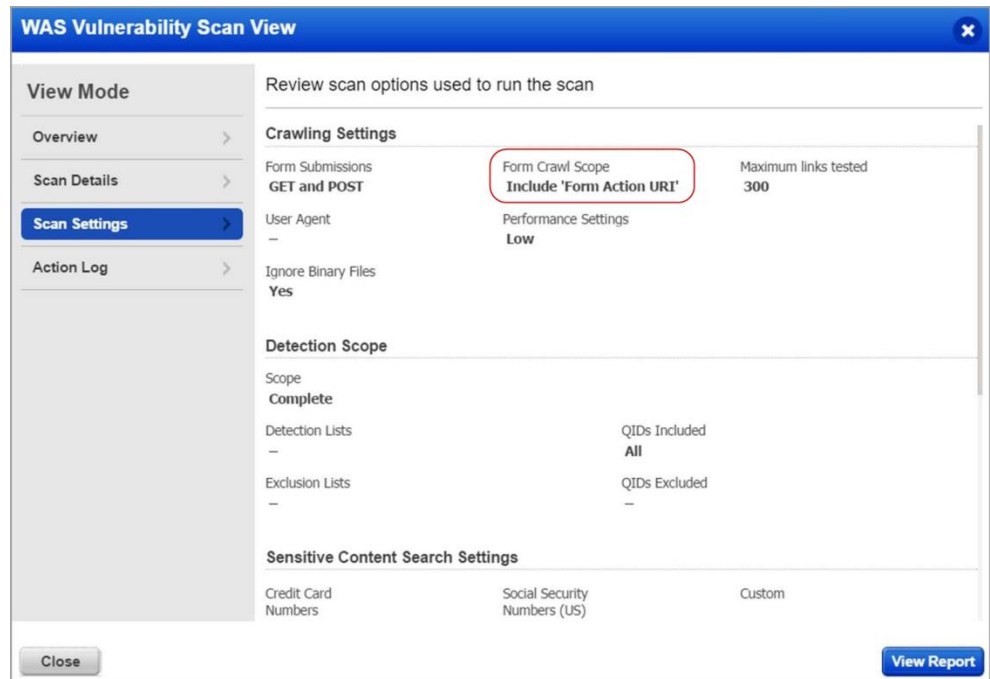
Document Type Ignore common binary files based on file extensions.

SmartScan Support Disabled

Cancel Previous Finish

You can also view the Form Crawl Scope defined in the option profile when you review and confirm the option profile settings.

Go to Scans > View from Quick Actions menu > Scan Settings and view the configured Form Crawl Scope for the scan.



Issues Addressed



- While tagging an asset, adding an already existing tag will not remove all tags added to the asset.
- The order and color of the tags will no longer change when the asset search results are refreshed.
- When you click "Find assets" in quick actions menu for any tag, the asset search query will now search for tags matching the exact name specified.
- The asset search query will now form correctly, if you group the asset search results by vulnerabilities, and then click the asset count against a vulnerability.
- Widgets created from the template "Assets with easily exploitable vulnerabilities" will now display the correct title and data.
- Now after downloading the assets list, the Activity status both in the UI and the downloaded version match.
- The dashboard (AV and TP) now displays the template title for widgets created from user templates.

- We've made improvements to the way asset tags are displayed on the dashboard (AV and TP) if the user has set up the Filter by Asset Tags option.
 - Now when the user filters the dashboard by more than 3 asset tags, 3 asset tags will be displayed on the dashboard and the link "n more tags" appears to the right of the 3 tags, so the user can view all asset tags being filtered from the dashboard. For example if the user filters the dashboard by 6 asset tags, 3 tags will be displayed on the dashboard, next to the tags will be the link "3 more tags".
 - We are now limiting the display for the tag title to 20 characters and the tooltip now shows the entire name.
- Fixed issue where user with Reader role could not view installed software, open ports and vulnerabilities for an asset. We've updated the Default permissions for READER to add ASSET.READ.
- Now a new user-created widget template is listed in the Templates list as expected.
- The trending widget title will be preserved when the user removes tag filters from the Filter by Asset Tags setting.
- TP: When editing a dashboard widget, changing the widget type from "count" to a different type will no longer result in an incorrectly styled widget.
- TP: Zoom button will now only be available for count widgets with trend data collection enabled.

CA

- We've added a message for the following performance related configuration parameters that they do not impact Windows agent version 1.5 and above: Delta Confirmation Interval, Manifest Download Interval, Configuration Download Interval, Provisioning Interval, Upgrade Check Interval, Upgrade Reattempt Interval.
- We fixed an issue so that the deactivation progress window gets closed after the agents are deactivated.
- We added a feature so that you can now create a tag (provided you have permissions) in the Cloud Agent module.
- We now correctly display the agent host information for all agents in the Agents tab.
- We fixed an issue to overcome loading of Activation key distribution widget failure.
- The loading indicator now disappears, as expected, after the user updates an activation key's name.
- If a custom network is deleted in the subscription, activation keys associated with the custom network are now properly assigned to Global Network and the keys are listed on the Activation Keys tab.

- Fixed issue where user with Reader role could not view installed software, open ports and vulnerabilities for an asset. We've updated the Default permissions for READER to add ASSET.READ.
- The search box on the Activation Keys and Configuration tabs appears correctly now with proper layout on Windows 10 systems.

SAQ

- The message displayed after an SAQ account expires is now placed at center and is highlighted in red for better readability.
- The description field is now displayed only when a description is added to an answer for a questionnaire.
- You can now add special characters to Template title and Question text.
- A user with Questionnaire Manager role now has access to the User and Report tabs.
- The Actions pallet for the questions now display all the tabs properly.
- Reports tab is no more displayed to a user having only responder role.
- Reports tab is no more displayed to a user having only responder role.
- We have removed unwanted characters from the Get Started for Free page (trial page).

WAS

- We now sanitize the content of the Web application report before generating the XML report using Report APIs to display correct and complete data in the report.

Qualys Cloud Platform

- Fixed an issue with sorting Action Logs by column. Now the user can sort Action Logs by message, timestamp or user. Although, Administrator and System users may not be sorted correctly within the results.