Qualys 8.11.2 Release Notes

This new release of the Qualys Cloud Suite of Security and Compliance Applications includes improvements to Vulnerability Management and Policy Compliance.

Qualys Cloud Platform

New Scanner Role Permission to Add Assets
View Title in Users tab

Qualys Vulnerability Management (VM)

CPE Type in Search Lists
Improved Scan Notification Email

Qualys Policy Compliance (PC/SCAP/SCA)

Amazon Linux Bare Metal Technology Supported for UDCs
Relaunch a SCAP scan

Qualys 8.11.2 brings you many more Improvements and updates! Learn more

Qualys Cloud Platform

New Scanner Role Permission to Add Assets

Your subscription may now be configured to allow users with a Scanner user role to be granted the "Add assets" permission. When granted, this allows the user to add new IP addresses to the subscription from the UI and API.

Good to Know

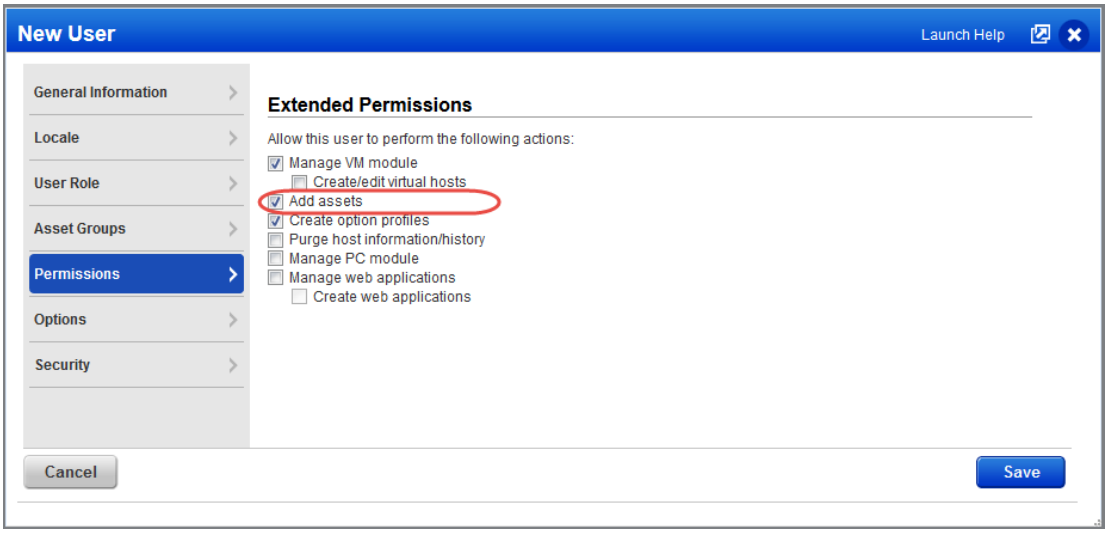
- The Scanner user must be granted the "Add assets" permission to add new IPs. The user must also have permission to each application (VM, PC) they want to add to.

- The Scanner user must add the new IPs to an asset group assigned to them. If the Scanner is in a business unit the new IPs are available in the business unit. The new IPs are also available to Managers for inclusion in other business units and asset groups.

- The number of new IPs the user can add depends on the number of IPs purchased for the subscription and the new IP limit set for their business unit, if applicable.

How to grant a user extended permissions

The "Add assets" permission may be granted on a per user basis by a Manager or Unit Manager (with the same permission). Edit the user's account from the Qualys UI by going to the Users list and choosing Edit from the Quick Actions menu. Then choose permissions on the Permissions tab.



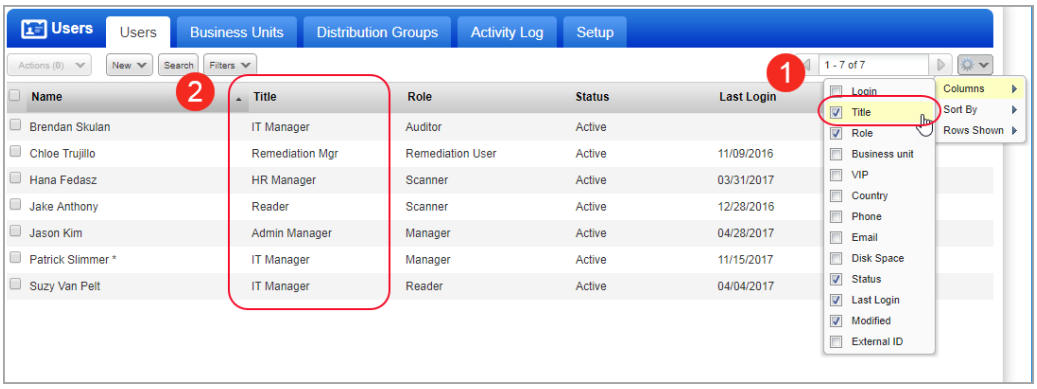
Not seeing this permission for Scanner users?

Your subscription must be configured to allow Scanner users to be granted the "Add assets" permission. Please contact your Technical Account Manager or Support to have this enabled for you. Once enabled, you'll be able to grant this permission to any Scanner user in your subscription.

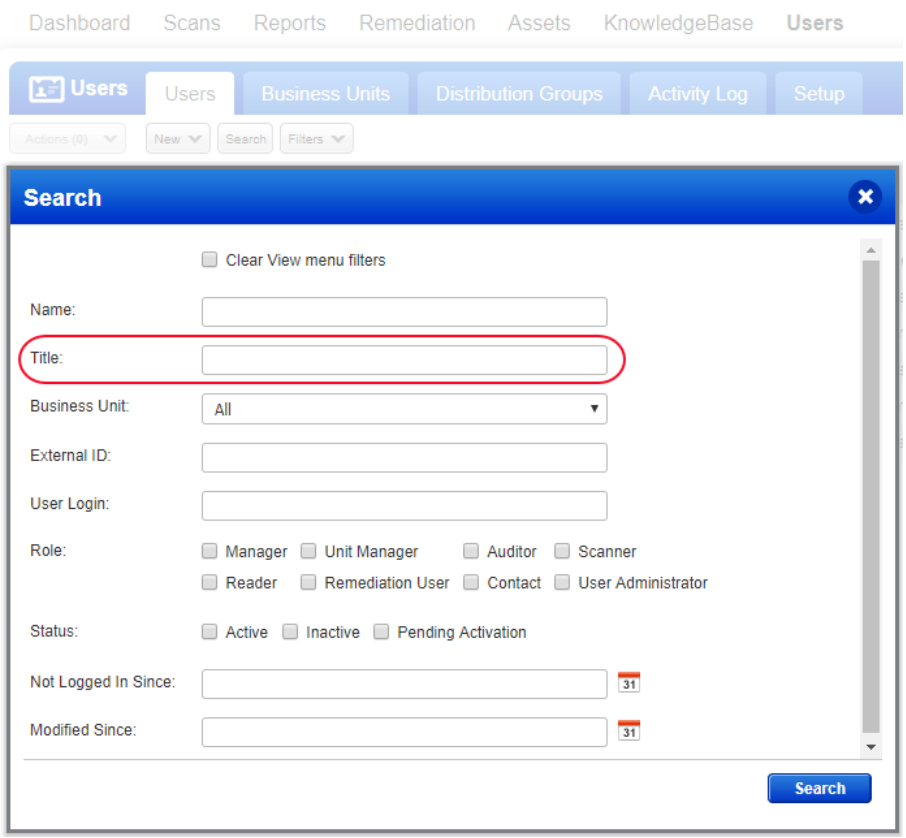
View Title in Users tab

You can now add the Title column to view job titles in the Users list.

1) Just navigate to the Settings button in right corner of the data list and select Title.
2) A new column is now added which shows titles of all users in the list.



Title is now also added as a search criteria when you search for users.

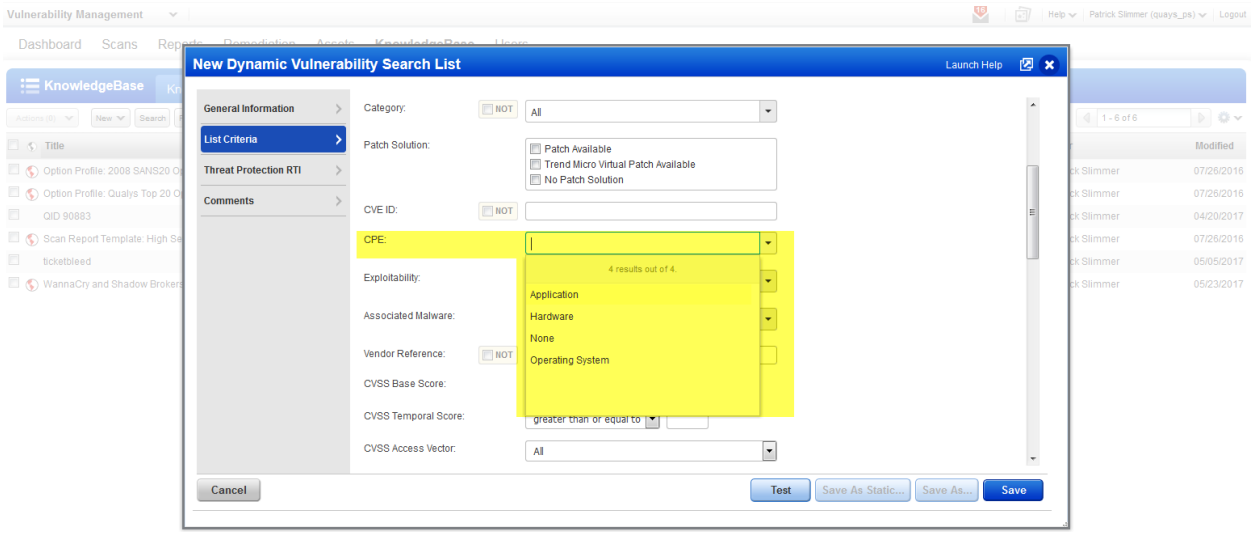


Qualys Vulnerability Management (VM)

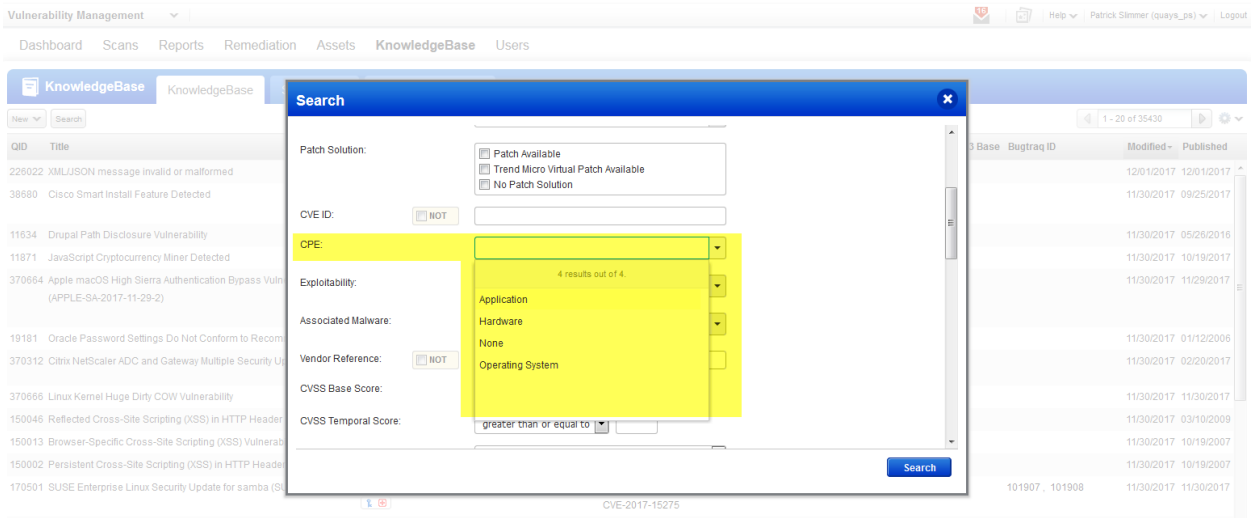
CPE Type in Search Lists

You can now use CPE “part” values (Operating System, Application, Hardware) in Dynamic Search Lists, allowing you to target specific vulnerabilities for sending to the appropriate remediation teams.

It’s easy to create search lists based on CPE. Go to Scans, Reports or KnowledgeBase and choose the Search Lists tab. Then go to New > Dynamic List and select one or more CPE categories. Add your search list to report templates to create custom reports.



You can also search the KnowledgeBase by the CPE category.

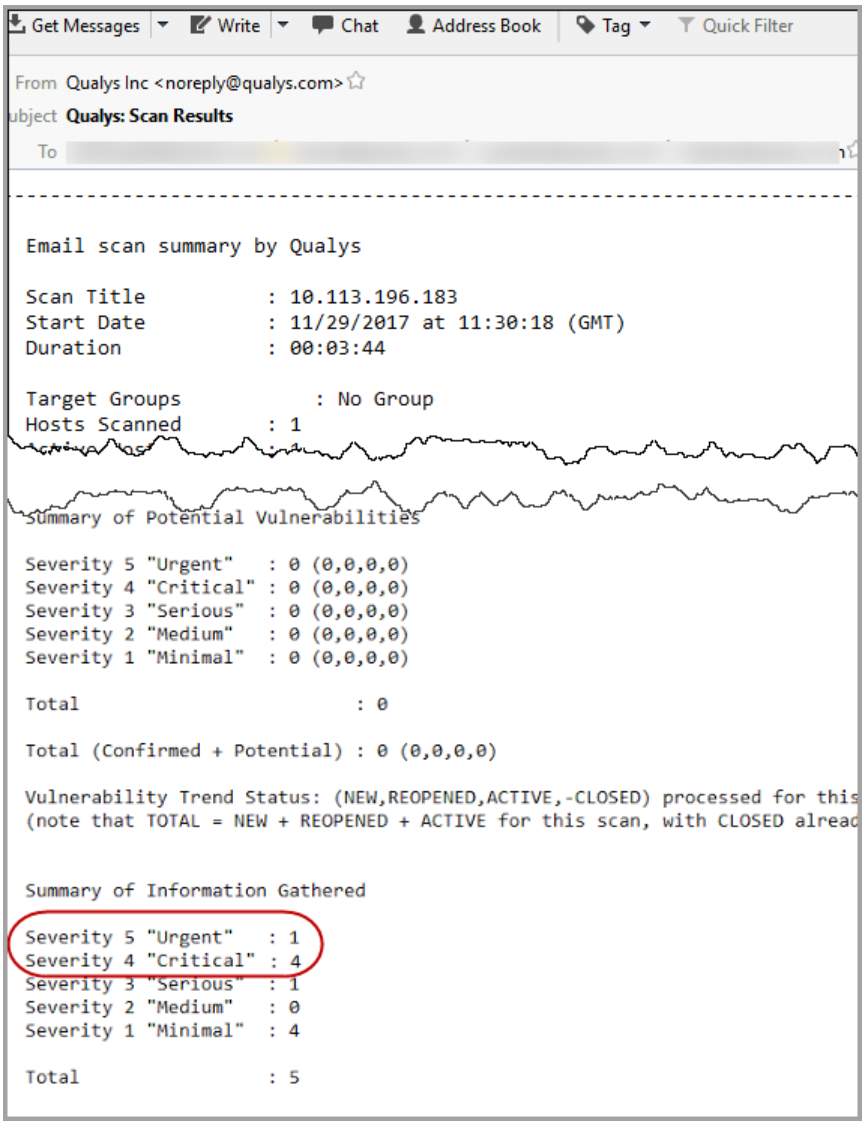


Improved Scan Notification Email

Our scan notification summary now includes Information Gathered vulnerabilities with severity 4 and 5.

Information Gathered QIDs belong to severity 1 to 3. However, you can always change the severity of the QIDs (to any severity level including 4 and 5). The scan notification now gives a complete count of vulnerabilities of type Information Gathered of all severities (including severity 4 and 5).

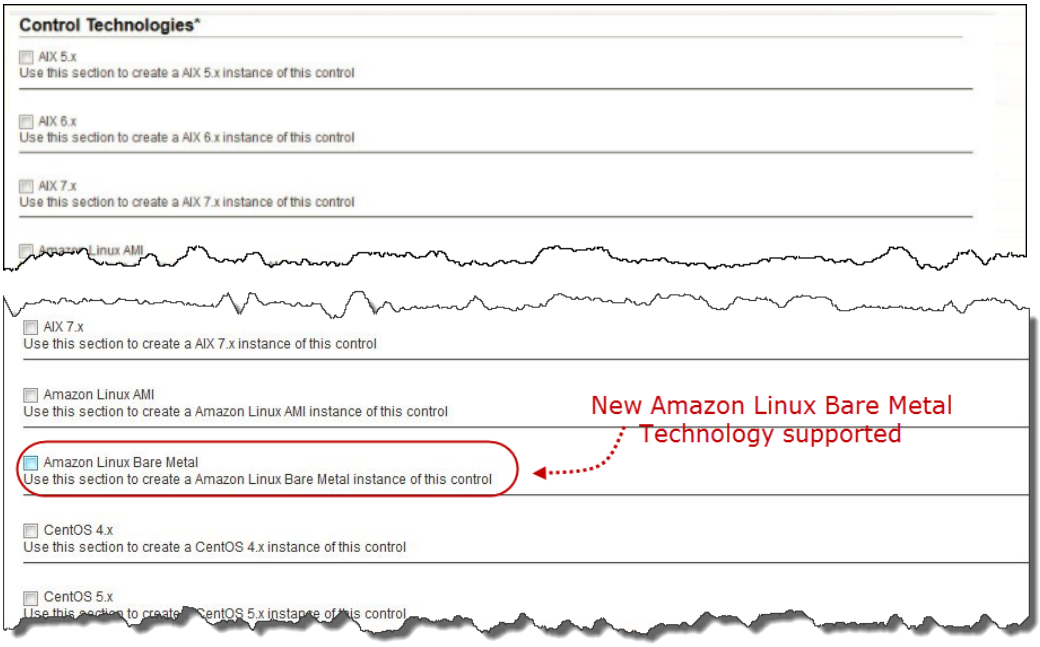
Once your scan is completed successfully, you will receive the scan completion notification with the information.



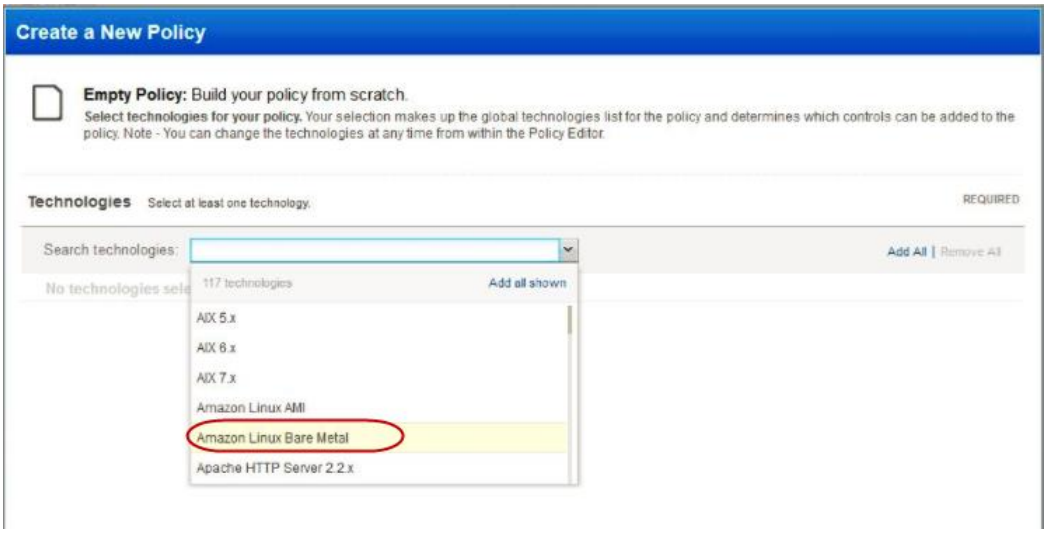
Qualys Policy Compliance (PC/SCAP/SCA)

Amazon Linux Bare Metal Technology Supported for UDCs

Want to create a UDC for Amazon Linux Bare Metal? Go to Policies > Controls > New > Control, and select any of the Unix control types. Scroll down to the Control Technologies section to provide a rationale statement and expected value for each technology you're interested in.



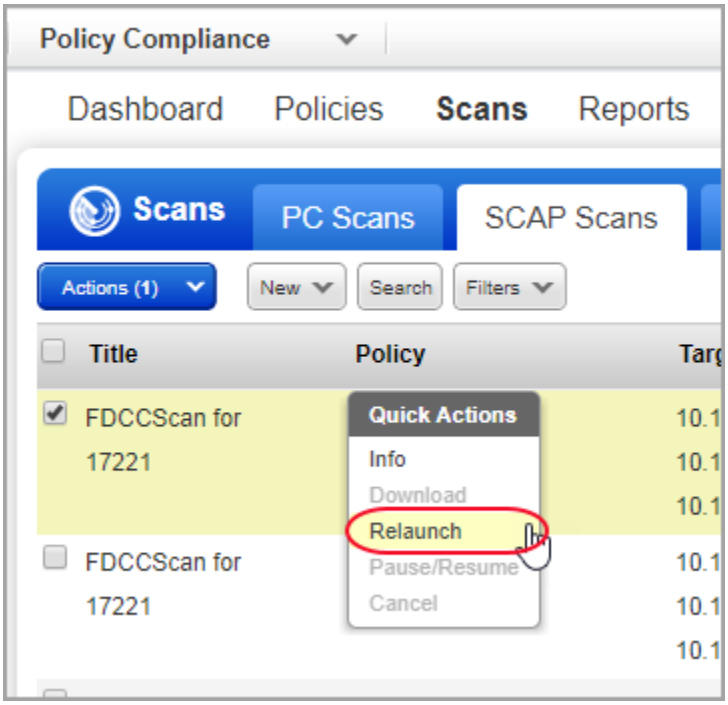
You'll also see Amazon Linux Bare Metal in the technologies list when creating a new policy.



Relaunch a SCAP scan

You now have the option to quickly relaunch a SCAP scan and the service will automatically recall the previous scan's settings.

Go to PC > Scans > SCAP Scans. Identify the scan you want to run again and select Relaunch from the Quick Actions menu. Review the scan settings and make any changes you wish, then click Launch.



Issues Addressed

- You can now save up to 1900 5-digit port numbers in the Additional ports fields for TCP Ports and UDP Ports in your VM Option Profile.
- We now correctly display the Updated Date which is either equal to or greater than the Submitted Date for the Processing Tasks filter.
- Fixed an issue where the Authentication Report was not reporting on IPs that had been previously scanned using authentication but then the IP was removed from the authentication record and not scanned again. The Authentication Report will now correctly report the last saved authentication status for those IPs.
- While editing a User Defined Control, the default value is now copied correctly from the "Default Values" section to the technology section when a new technology is selected.
- In Policy Reports, error message is correctly displayed for directory integrity check custom controls, if the scan result is an error.
- Fixed an issue in the Policy Report Template with the Report Layout options. You can now click the label "All" or toggle the checkbox to select or deselect the Status and Criticality options.
- We have removed the erroneous user service assigned link from the status and retained the correct link in the Control Details section of the Policy Editor.
- Deprecated policy label "label1" is no more displayed in the PC Policy Library.
- While scheduling Mandate based reports, you now have additional options for weekly and monthly occurrence.
- When the Manager Primary Contact runs a scan, the scan notification email will now show support@qualys.com for the contact in the email body.
- Fixed an issue where the user chose the Delete action for records in the Authentication Records list and a record open in another window was also deleted even though it was not selected for the action.
- Fixed an issue where searching the Appliances list by LAN IP was not returning results.
- We have now improved the error message for you to know the cause of the error during the launch of Scan Report.
- The network information is now successfully passed with the Asset tag creation from the Asset Search Report page.
- We can now successfully purge Agent-only hosts (hosts that are not a part of the license container) through Asset Search Report.
- The Scorecard Report now accurately displays "Technology" value in XML output of the report.
- Fixed an issue where Scorecard Reports on asset tags were failing when launched using the API.
- We've made improvements to the EC2 scanning documentation to help users with scanning and setting up EC2 authentication records and their EC2 assets.
- We've updated the User Roles Comparison (Vulnerability Management) help to indicate that Managers and Unit Managers have permission to launch and schedule EC2 scans.