Qualys Cloud Platform (VM, PC) 10.x

Release Notes

Version 10.15

November 1, 2021

This new release of the Qualys Cloud Platform (VM, PC) includes improvements to Vulnerability Management and Policy Compliance.

Qualys Policy Compliance (PC/SCAP/SCA)

Enhancements to Control Mappings for Mandate Based Reporting

Qualys Vulnerability Management (VM)

Column Name Change On the Certificates List

Qualys 10.15 brings you many more improvements and updates! Learn more

Qualys Policy Compliance (PC/SCAP/SCA)

Enhancements to Control Mappings for Mandate Based Reporting

Mandate Based Reporting allows you to view the compliance posture of your organization in terms of the underlying Security baseline against selected mandates.

Qualys has introduced a new control mapping where each control is mapped with the granular control objectives. This approach enhances the functionality of Mandate Based Reporting and helps organizations better understand their compliance against respective mandates.

In the older approach, each control was mapped with multiple control objectives, which allows the control to appear for multiple control objectives in Mandate Based Reports. The challenge with this approach is that the report was very large and it was time-consuming and confusing for organizations to understand and identify their compliance against the respective mandate.

In the new approach, each control is mapped with the most appropriate control objectives. This allows the control to only appear for the most appropriate control objectives.

Changes you'll notice in Mandate Based Reports

- Granular mappings listed for controls when you drill-down into report details.

- Your reports may have fewer controls listed than previously as we've taken an approach to show the most accurate mappings.

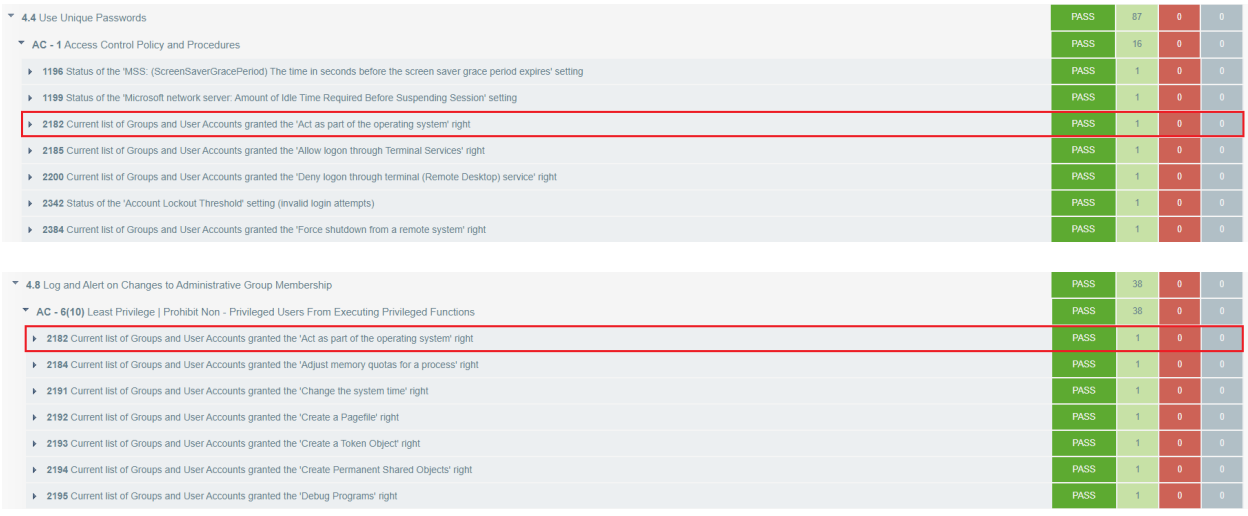
- Changes to control objectives. This may be especially noticeable when your report is grouped by control objective for a harmonized report with multiple mandates included.

Compare Sample Reports

The following samples show the difference between the older and newer mandate reports.

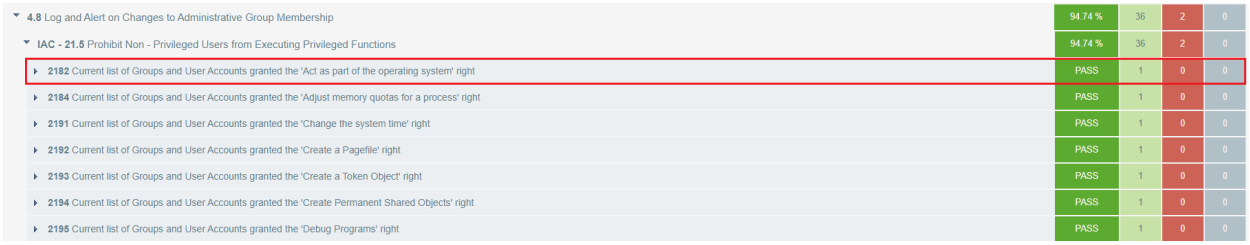
Old Report

In the old report, Control ID 2182 appears for multiple framework controls: AC-1, AC-6(10), IA-2.



New Report

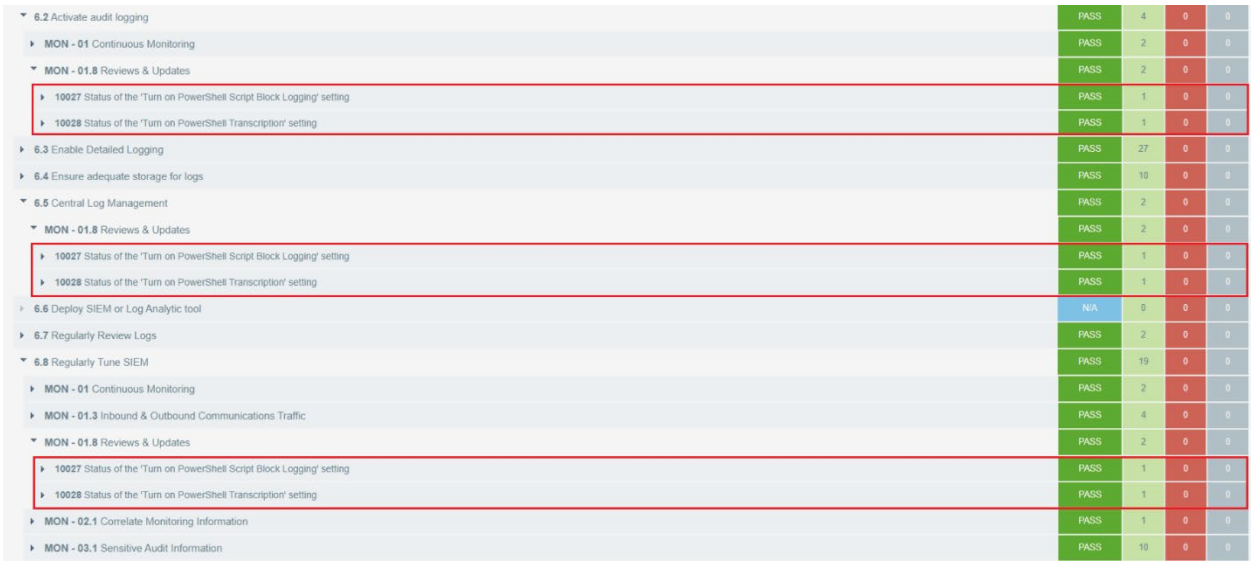
In the new report, Control ID 2182 appears for only a single framework control: IAC-21.5.



Does this mean that a Qualys Control will appear only once in the report?

No, this does not necessarily mean that a Qualys control will appear only once in the report. There is a possibility where a control may appear multiple times based on cross-mapping done against the control objective standard.

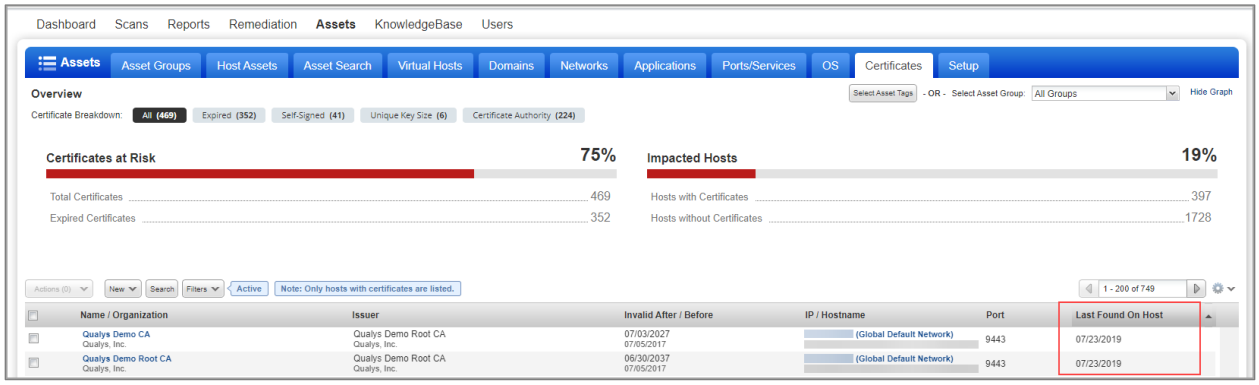
In the following sample report, Control IDs 10027 and 10028 appear in multiple sections: 6.2 Activate audit logging, 6.5 Central Log Management and 6.8 Regularly Tune SIEM. This is because the CIS control sections 6.2, 6.5 and 6.8 are cross-mapped with the Control Objective MON - 01.8 Reviews & Updates.



Qualys Vulnerability Management (VM)

Column Name Change On the Certificates List

On the **Certificates** list under **Assets**, we renamed the Last Found column to **Last Found On Host** for better clarity. As the name implies, this column displays the date on which the certificate was last found on the host. You'll see this same name change when you download the **Certificates** report to your local system (**New** > **Download**).



Issues Addressed

- We fixed an issue where the user could not schedule a scan due to the difference in the timezones of the server and client. After the fix, the user can now select a current year based on the user's timezone.
- We fixed an issue in VM/PC where the Authentication record details screen showed SID text even if the user selected the Service Name option in the Oracle authentication record.
- We have now fixed an error in pagination on the Authentication Records page.
- We now display an appropriate error message for create and update API for the virtual host, when the Virtual host data with FQDN value exceeds 4000 bytes.
- We have now fixed an issue with the consultant report to generate the text in the expected format and correctly handle the characters " ' ". The report is now correctly generated from the template.
- Fixed an issue in Asset Search Report where OS Filter was not working for zero value and not escaping single/double quotes from the OS filter values.
- We fixed an issue where we were not updating LAST_PROCESSED_DATETIME during the scan if the vulnerability is fixed and the host for which vulnerability is detected is dead. Due to this issue, vulnerability is ignored by Qualys TA when pulling the VM data for the host from Qualys cloud. Now the LAST_PROCESSED_DATETIME value is also updated if the host is dead and the vulnerability is fixed for that host.
- We have added logs that appear while the host purge request comes on the server. The logs have the details such as the source of the request.
- When the virtual scanner add-on is expired and then the customer tries to launch a scan using the default option it gives the error. When the add-on is expired, it will not check for validation of that add-on because the external scanner has no dependency on the virtual scanner add-on.
- If the sub-users do not have access to VM, PC, and SCA modules then on logging in, instead of redirecting to the AV UI login page they are redirected to the portal home page.
- We fixed an issue related to agent scan data collection for User Defined Controls (UDCs). The agent was collecting data for the technologies selected in the UDC and also collecting data for additional technologies that were not selected in the UDC. This was because the regular expression used to identify the OS technology matched multiple technologies. Now we'll use a more accurate regular expression to reduce the amount of data that is collected and processed by agents for UDCs. For example, before this fix if the user selected Windows 8 in the UDC, the agent collected data for Windows 8 and Windows 8.1. Similarly, if the user selected Windows 2012 Server in the UDC, the agent collected data for Windows 2012 Server and Windows Server 2012 R2. Now the agent will only collect and process scan data for the selected technologies.
- For PC/SCA, we fixed an issue where the wrong module was being shown in the Modules column on the Assets tab in AssetView. When you scan a PC asset, you'll see the PC module in AssetView. When you scan an SCA asset, you'll see the SCA module in AssetView. When you move an IP from PC to SCA or vice-versa and you have scan data from both modules, then you'll see both PC and SCA in the Modules column in AssetView.

- Qualys CM users were not receiving alerts for the required software list while using the 'Software' rule in a scan. This issue is now fixed and the rule accurately lists all the installed or uninstalled software.
- We fixed an issue in the Unix Directory Search UDC where we allowed users to save the UDC with the File Owner scan parameter option enabled for specific users/groups but no user/group names or IDs were specified. Now we've added the proper validation to ensure that if these options are selected that names and IDs are also provided. This will ensure the UDC can be evaluated.
- Fixed an issue where, when creating a new schedule scan, there was no validation when unmapped IPv6 addresses were added to the Exclude IPs field. We now validate and display an error message in such scenarios.
- On the Remediation > Tickets tab, a user with a Remediation User role will no longer see text that instructs them to go to the Setup tab to change the timeframe for tickets to display since this option is not available to this user role.
- We fixed an issue where the Host Based reports were not populating the DNS and NetBIOS tracked IPs when the users with AGMS enabled accounts ran the report on IPs that included DNS and NetBIOS tracked IPs with a network ID or custom network. Now, the report is populating DNS and NetBIOS tracked IPs with a network ID or custom network.
- We fixed an issue in AGMS enabled subscriptions where the CSV Download from the Assets > Ports/Services tab appeared blank for Unit Managers when no filters were applied to the report.
- For accounts with AGMS enabled, when you change a user's assigned business unit or change the user's role, you'll be presented with 2 options that determine how to handle the user's personal configurations and asset groups. You can choose to transfer ownership of the personal configurations and asset groups to the user’s current manager. If you don’t transfer ownership, then the user’s personal configurations and asset groups will be deleted. Please note that the user being moved or assigned a new role will not have the option to keep their personal configurations or asset groups, and assets will not be moved from one business unit to another. We updated the online help to assist when making these types of changes.
- We fixed an issue where the VIP 2 factor authentication was not available for some platforms.
- We removed the Beta label from the module picker for the API Security module.
- Fixed an issue where the Schedule Scan API was giving an error when the concurrent limit has reached.
- We fixed an issue in the Compliance Posture Information API where Missing values were not appearing as expected under Cause of Failure in the API response, when applicable.