Qualys Certificate View

Release Notes

Version 3.1.0

July 14, 2023

Here's what's new in features and improvements in Qualys Certificate View 3.1.0!

What's New?

Qualys Certificate View 3.1.0 brings you many more improvements and updates! Learn more

Tag-based User Scoping

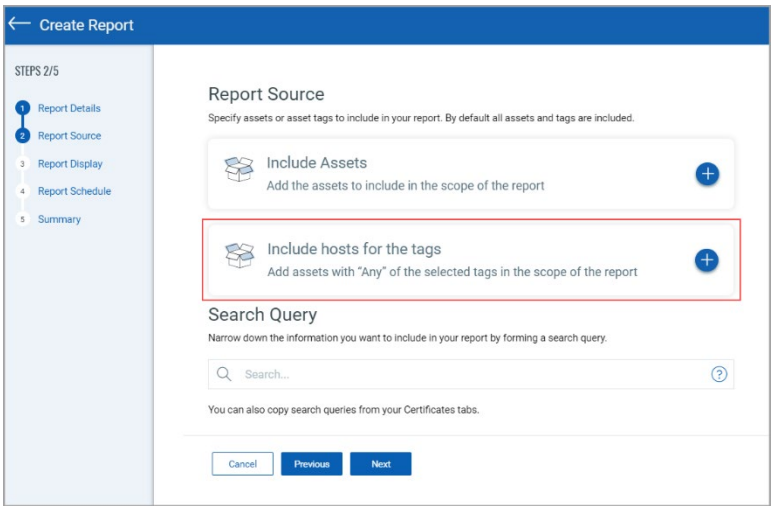
With this release, we are introducing Tag-based User Scoping (TBUS). TBUS empowers manager users to restrict sub-user's access to specific assets and certificates based on designated tags. With TBUS, manager users have better control over their sub- user's access to assets.

As an example, let us consider a manager user has 1000 assets. Out of those, the manager user has assigned a Windows tag to 500 assets. The manager user has granted access to a sub-user for the Windows-tagged assets. As a result, the sub-user can only view the 500 assets with the Windows tag in the Assets tab, the Dashboard, and the Certificates tab displays the certificates associated with these 500 assets. For more details, refer to the *Tag-based User Scoping section in Certificate Online help*.

Use of TBUS while Adding Source for Report

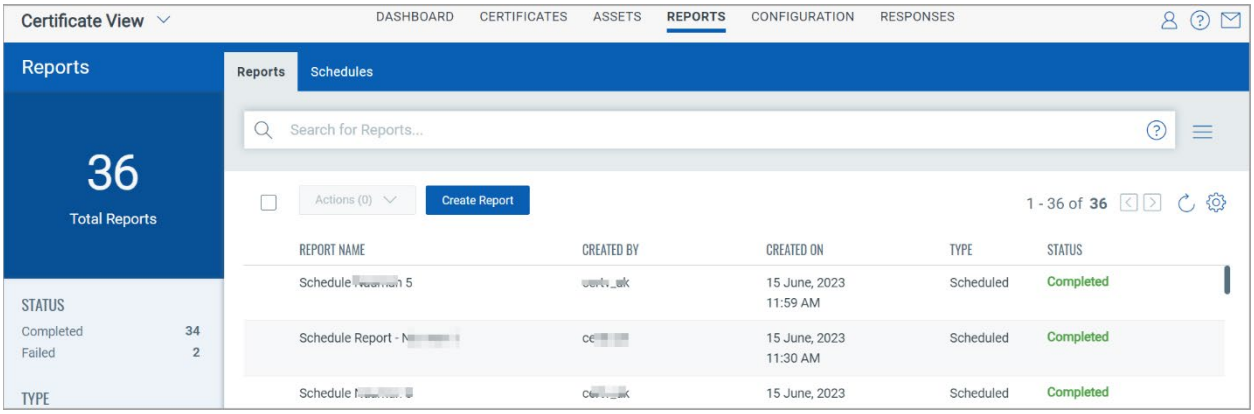
With this release, we have added the feature of adding a source for the report. If you want to add more 250 assets, you can use **Include hosts for the tags**. This feature allows users to group assets by tags and select which tags to include in the report scope.

The feature **Include hosts for the tags** is available to users with either of the following permissions: TAGGING.CREATE_USER_TAG, TAGGING.ADD_REMOVE_TAG.



Improved Reports Tab

We have improved the **Reports** tab to enhance user experience. The **Reports** tab features new filters and a better display to help you view report names, creators, creation dates, type of report and status. Additionally, new tokens are available for your queries. You can refer to the token list here.



New Search Tokens for Reports Tab

Token	Description	Example
report.name	Show the report with the given name.	`report.name: scan_assetgroup1`
report.status	Show the report based on status such as Accepted, Completed, Failed, Generated, Incomplete, or Processing.	`report.status: Completed`
report.type	Show the report based on the type of scan such as On Demand or| Scheduled.	`report.type: Scheduled`
report.format	Show the report in the given format.	`report.format: csv`
and	Narrow down the search by using the and operator in the Boolean query.	`report.name: scan_assetgroup1 and report.status Completed`

API Features and Enhancements

We have introduced Tag-based User Scoping. This new feature allows users to view information about the assets and their associated certificates assigned to them; when a user sends an API request to Certificate APIs, such as List CertView Certificates (v1), List CertView Certificates (v2), List Assets for a Certificate, and List Server Instances. For detailed information on API, refer to *API Release Note*.

Issues Addressed

- We have fixed an issue wherein the time stamps displayed in the Certificate details on both the Certificate View page and the API did not match for the fields: **Valid From**, **Valid To**, and **Last Found dates.** We have updated the UI to display the time stamp according to the user's time zone, ensuring accurate and consistent information.
- We fixed an issue where certificates detected in VM/VMDR were not accurately displayed in the Certificate View application. Now, users can view their certificates correctly.
- We have fixed the issue where the expiryGroup value for the **expiryGroup** token in the report email notification was coming as it is Not applicable. We have removed the expiryGroup token from the **Insert Token** option on the alert email notification. The user can use the **ValidTo** token instead of **expiryGroup** to get email notifications. For more information, refer to *Create and Manage Rules section in Certificate View Online help*.
- We addressed an issue where Issuer Field for Intermediate CA was Missing from CertView V2 API. We have resolved the issue and the information is now accurately displayed.
- Earlier if Certificate View had a certificate on a specific port (such as 3389) or QID (such as 86002), and the user launched a VM scan through an Option Profile that did not have that port or QID, the certificate was deleted from Certificate View because no certificate was found for that port/QID. However, we have now fixed this issue, the user can view all the certificates with QID or port and timestamp.