Qualys Cloud Platform v3.x

Release Notes

Version 3.11
April 28, 2022

Here's what's new in Qualys Cloud Suite 3.11!

Administration

Unified Dashboard

New Permission and User Role for Unified Dashboard

Unified Dashboard

Add a Widget to Multiple Dashboards

Vulnerability Management, Detection, and Response

CISA Exploited RTI is now CISA Known Exploited Vulnerabilities

AssetView

New Permission Check for Fetching Asset Data

Security Assessment Questionnaire

User-Defined Template for Vendor Criticality Evaluation Survey

Qualys Cloud Platform 3.11 brings you many more improvements and updates! Learn more

Administration

Unified Dashboard

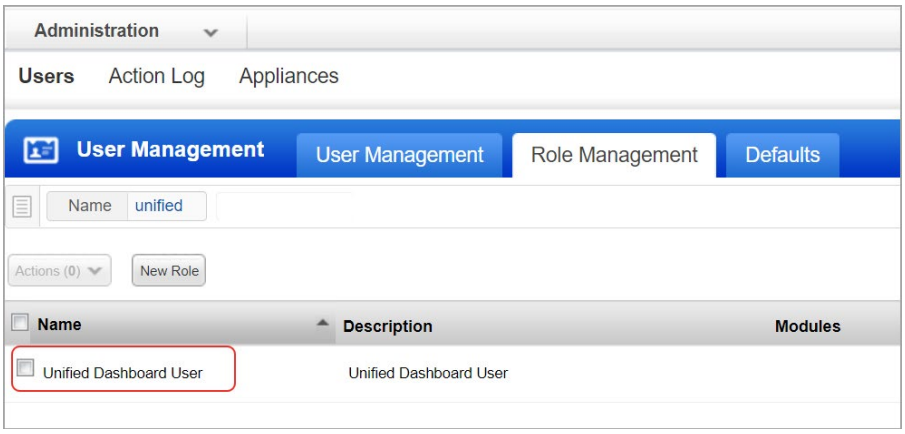
New Permission and User Role for Unified Dashboard

We have now introduced a new role with pre-defined permission assigned to it that can be used to provide access to the Unified Dashboard (UD) application. You could also either use our pre-defined role or create a new role and assign the required permissions to provide access to the UD application.

New User Role

We provide a pre-defined role named **Unified Dashboard User** to provide access to the Unified Dashboard application. Once this role is assigned to a user, the Unified Dashboard application is listed in the application picker and the user can access the application.

To locate the new user role, go to the **Administration** utility > **Role Management,** and the new **Unified Dashboard User** role should be displayed in the list of roles. Assign the role to the required user to provide access to the UD application.

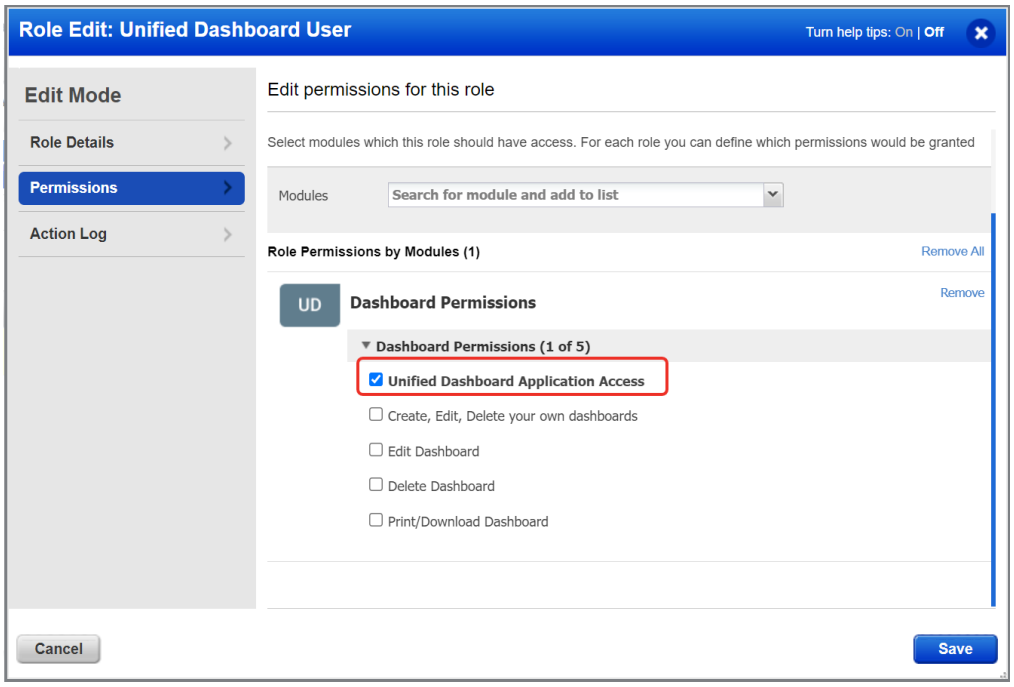


New Permission

To provide access, you can either assign the predefined role or change the permissions associated with an existing role. If you have users with existing roles, you can edit the permissions associated with the role and assign the **Unified Dashboard Application Access** permission to an existing role.

Go to **Administration** Utility > **Role Management** and select any role you want to assign the permission to, and click Edit from the quick actions menu. In the Permissions tab, select Dashboard Permissions from the **Modules** drop-down. Click **Change** to edit the dashboard permissions.

Select the **Unified Dashboard Access** permission and click **Save**.

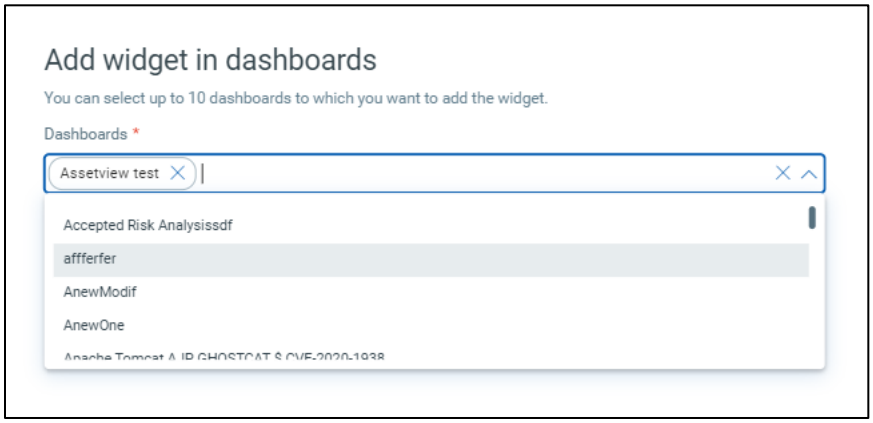


Note: By default, the existing Scanner, Reader, and Unit Manager users are assigned access to the Unified Dashboard application. For all the new Scanner, Reader, and Unit Manager users you create, you need to either assign the Unified Dashboard User role or Unified Dashboard Application access permission to access the Unified Dashboard (UD) application.

UD Unified Dashboard

Add a Widget to Multiple Dashboards

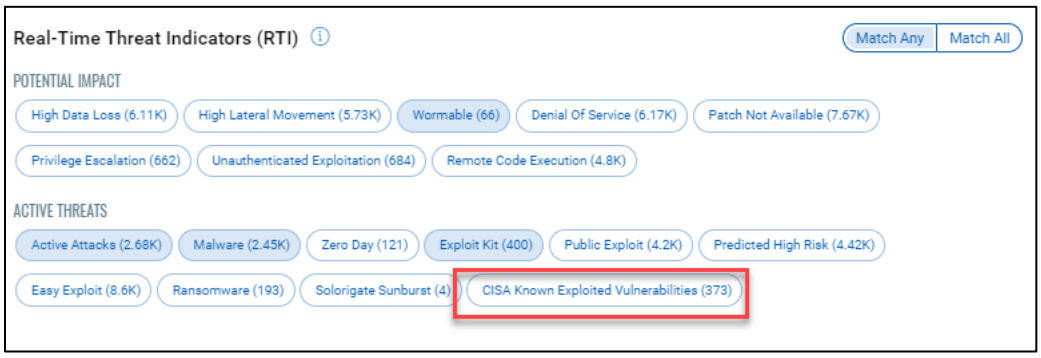
While creating a new widget, you can now add the same widget to up to 10 different dashboards.



VMDR **Vulnerability Management, Detection, and Response**

CISA Exploited RTI is now CISA Known Exploited Vulnerabilities

We have renamed the CISA Exploited RTI to CISA Known Exploited Vulnerabilities for better clarity.



AM AssetView

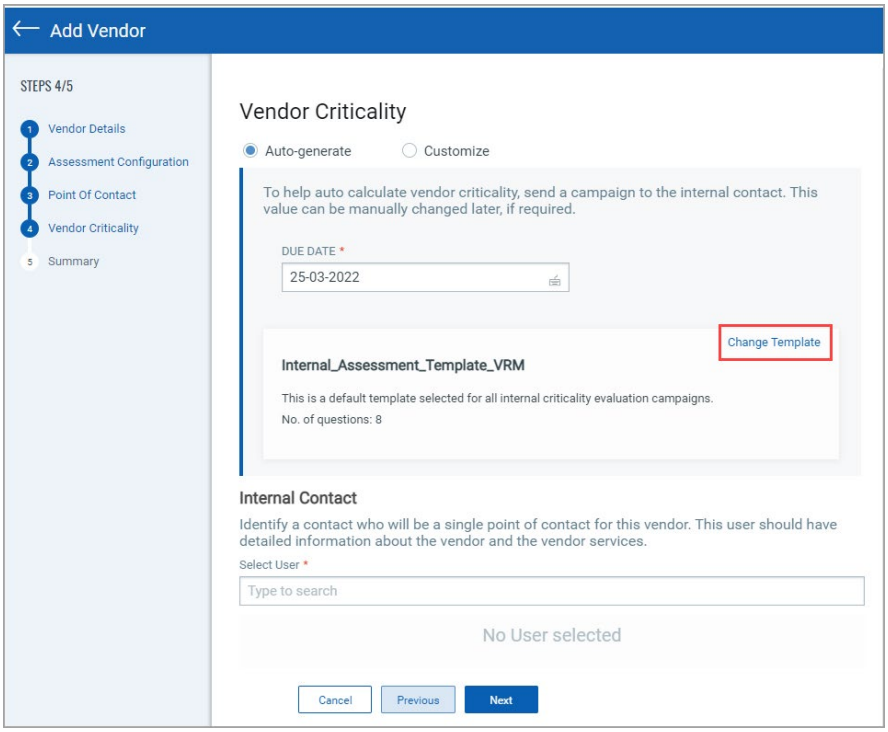
New Permission Check for Fetching Asset Data

Previously, unauthorized users could fetch data using the /qps/rest/2.0/count/am/assetdataconnector API. Now we have added a check so only the users that have the correct permissions will be able to fetch the asset data.

SAQ Security Assessment Questionnaire

User-Defined Template for Vendor Criticality Evaluation Survey

Now, you can change the default template while creating Vendor for criticality auto evaluation. You can select a template from the library or a custom template



Issues Addressed

WAF Web Application Firewall

- We have updated the Virtual Firewall Appliance user guide with the latest information on deploying the WAF firewall on Microsoft Azure.

WAS Web Application Scanning

- We have added a note about using read-only credentials to avoid undesired effects on data in the Authentication Record Creation screen. We have also updated the Web Application Scanning online help with information on the credentials to be used for authenticated scans.

VMDR Vulnerability Management, Detection, and Response

- We fixed an issue where no results were shown on the **Vulnerabilities** tab if you grouped the vulnerabilities by First Found.
- We fixed an issue where the vulnerabilities.detectionAge token showed incorrect results.
- We added an information message on the UI about the character limitation of the search query fields.
- Based on your preference, you can now hide the Guide me feature on the UI.

AM AssetView

- We fixed an issue where the asset purged count was shown as zero, although assets were purged.
- We fixed an issue where an incorrect **Last Updated** field was shown for an asset discovered as per the AWS connector.
- We fixed an issue where you could not get the correct asset count if you used excluded to create the query.
- We fixed an issue where the Qualys API Quick Reference Guide listed the incorrect parameter for the /qps/rest/2.0/search/am/tag API.
- We updated the online help to reflect the correct way to use the double quotes and backticks in a query.
- We updated the Asset Management API User Guide to include the missing parameter for the /qps/rest/2.0/update/am/tag/<id> API.