



Qualys Cloud Platform v3.x

Release Notes

Version 3.9

November 24, 2021

Here's what's new in Qualys Cloud Suite 3.9!

VMDR Vulnerability Management, Detection, and Response

[Include or Exclude Any or All tags for a Prioritization Report](#)

[New Tokens for VMDR](#)

UD Unified Dashboard

[New Application Widget Template Library](#)

[New Widget added to the Template Library](#)

[Use a Hex Code to Customize the Color Palette for a Widget](#)

Administration

[New User Permissions](#)

WAS Web Application Scanning

[View Partial Scan Data for Service Error Detected Scans](#)

[Added OAuth2 Support for Swagger/API file authentication](#)

AM AssetView

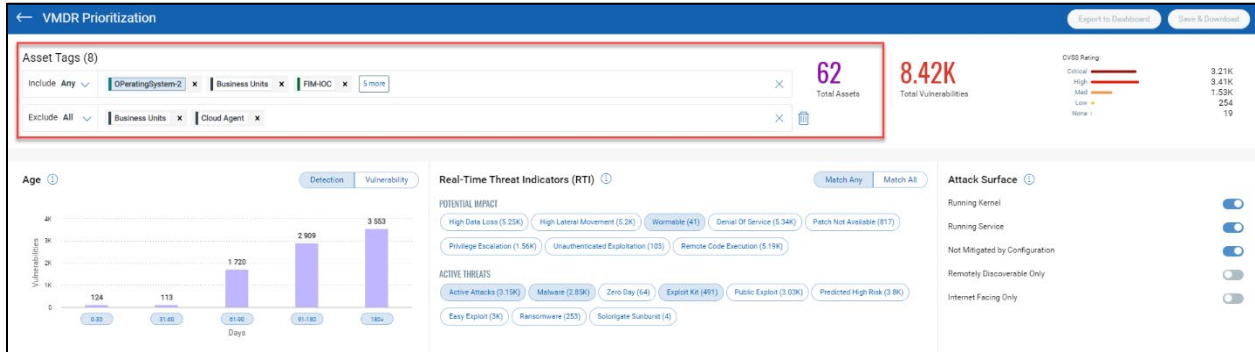
[New Tokens for AssetView](#)

Qualys Cloud Platform 3.9 brings you many more improvements and updates! [Learn more](#)

Include or Exclude Any or All tags for a Prioritization Report

With this release, you can include or exclude Any or All asset tags for a prioritization report.

- Any to include or exclude all assets that might have any of the selected tags
- All to include or exclude only those assets which have all the selected tags



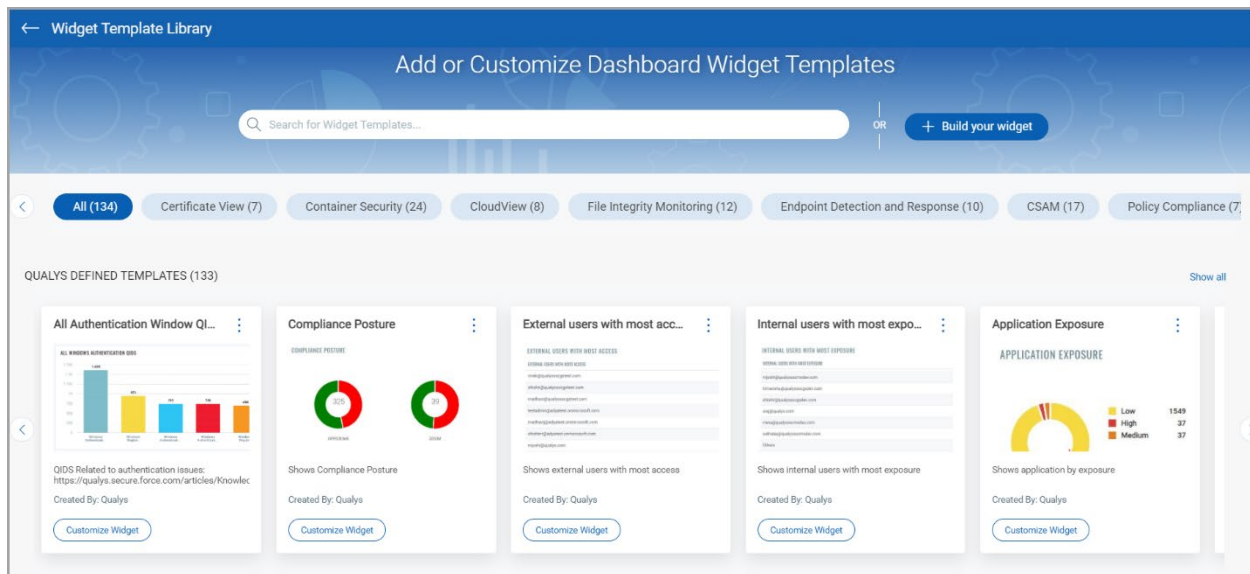
New Token for VMDR

We have introduced the following new search token to enhance your search results:

- **criticalityScore**: This token helps you find the criticality score for an asset.

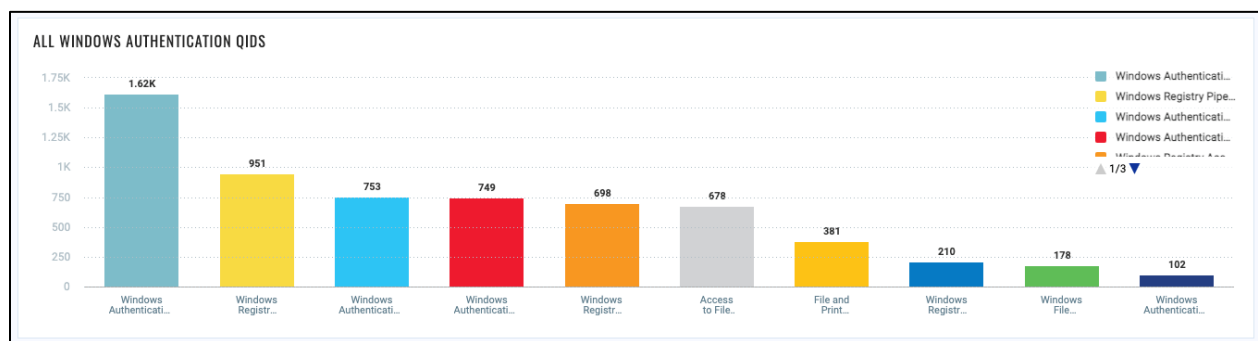
New Application Widget Template Library

The Widget template library allows you to create your widgets using existing templates, customize existing widgets or create new widgets to suit your need. The widget templates are segregated based on the subscription to other Qualys products.



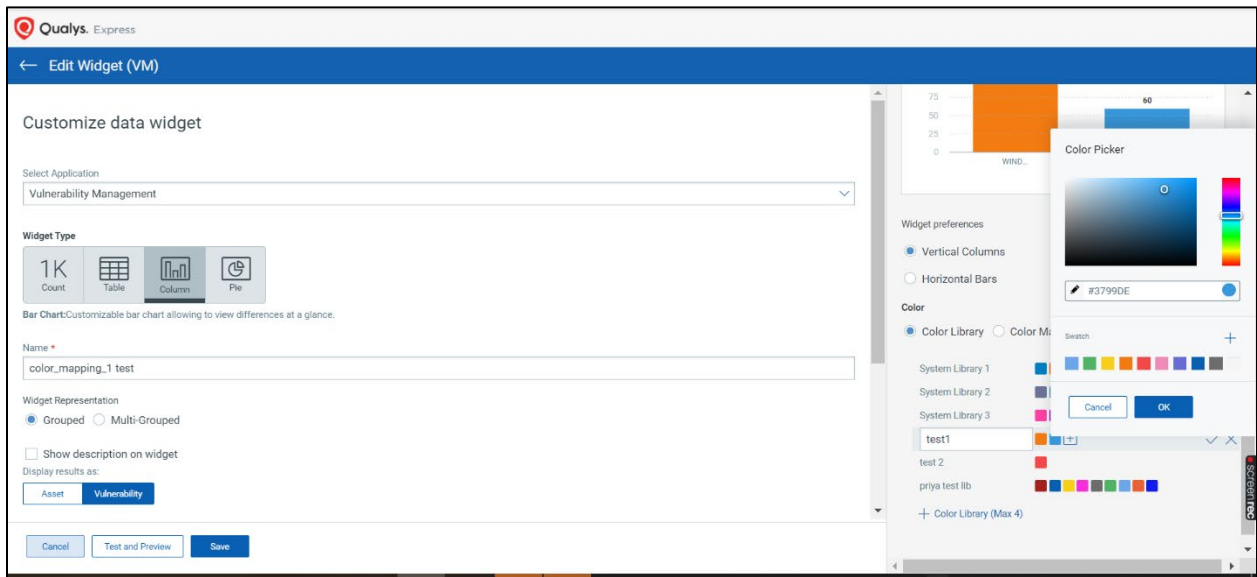
New Widget added to the Template Library

With this release, we have added a new widget, **All Authentication Window QIDs**, for the VMDR module.



Use a Hex Code to Customize the Color Palate for a Widget

You can now use a hex code in the color picker to customize the data displayed on a widget.





Administration

New User Permissions

With this release, we've added the following new permissions for the Administration module:

- Create User
- Action Log Access
- Update Defaults

The screenshot shows the 'Role Edit: CA MANAGER' interface. The left sidebar has 'Permissions' selected. The main area shows 'Role Permissions by Modules (9)' with a 'Remove All' link. Under the 'ADMIN' tab, the 'Administration' module is expanded, showing a 'Remove' link. A red box highlights the following permissions:

- ▼ User Permissions (7 of 7)
 - Edit User
 - Create User Role
 - Edit User Role
 - Delete User Role
 - Create User
 - Read User
 - Access Role Management Section
- ▼ Action Log Permissions (1 of 1)
 - Action Log Access
- ▼ Defaults Permissions (1 of 1)
 - Update Defaults

Buttons for 'Cancel' and 'Save' are visible at the bottom.

For more information, refer to the Manage User Roles topic in the online help.

View Partial Scan Data for Service Error Detected Scans

Like with the "Canceled with Results" scan, we will now show you the findings (vulnerability, sensitive content, and information gathered) for scans with status as "Service Errors Detected." You can see all the findings that were detected till the scan got terminated. Findings for these scans will be visible in the web application report and Detections tab.

In the Service Error Detected scans, we will not mark any finding that was detected in an earlier scan as "Fixed" because we do not know if the finding is present or not as the scan could not be completed. For such findings, we display a message on the **Vulnerability Details** screen that the vulnerability could not be tested in the **History** section of the finding.

The screenshot shows the Qualys Web Application Scanning interface. A 'Vulnerability Details' modal window is open, displaying the following information:

Field	Value	Field	Value
Finding #	4122632	Web Application	Service Errors Detected
Unique #	c9e2319c-a174-4717-bc57-32dc59b8498a	Authentication	Not Used
Patch #	-		
Group	Path Disclosure	First Time Detected	17 Nov 2021 1:33PM GMT+0530
CWE	CWE-23	Last Time Detected	18 Nov 2021 11:15AM GMT+0530
OWASP	-	Last Time Tested	18 Nov 2021 11:15AM GMT+0530
WASC	-	Times Detected	2
CVSS V3 Base	3.1	External References	-
CVSS V3 Temporal	2.9	CVSS V3 Attack Vector	NETWORK

The History section contains the following entries:

Status	Authentication	Date
Finding has been detected	None Authentication not used	18 Nov 2021 11:15AM GMT+0530 was/1637214238239.1329264
Finding could not be tested Vulnerable URL cannot be found anymore	None -	17 Nov 2021 4:53PM GMT+0530 was/1637147438256.1328542
Finding could not be tested QID was not included in scan configuration	None -	17 Nov 2021 4:53PM GMT+0530 was/1637147476762.1328430
Finding could not be tested	None -	17 Nov 2021 4:46PM GMT+0530 was/1637147410407.1328440
Finding has been detected	None Authentication not used	17 Nov 2021 1:33PM GMT+0530 was/1637136118789.1328239

The third, fourth, and fifth entries in the history table are highlighted with a red box, indicating findings that could not be tested due to service errors.

Added OAuth2 Support for Swagger/API file authentication

We now support OAuth2 for authenticating the Swagger/OpenAPI file. These OAuth2 authentication types are supported: Authorization Code, Implicit, Client Credentials, and Resource Owner Password Credentials.

When you create/edit an authentication record, you will see a new "OAuth2 Record" tab. Select a Grant Type for the authentication record and enter the details in the respective fields. We will use these details to authenticate to the web application when scanning your Swagger/Open API file.

Selecting the "Authorization Code" or "Implicit" grant type requires you to upload a valid Selenium script. We will prompt you to upload the Selenium script when you select either grant type. We support parameters for username and password in the selenium script.

The screenshot shows a web application interface for creating an authentication record. The title bar reads "Web Application Authentication Record Creation" with a "Turn help tips: On | Off" and "Launch help" button. The main content area is titled "Step 4 of 6" and "Set OAuth2 credentials used to authenticate against web application." The left sidebar shows a progress indicator with six steps: 1. Basic Information (checked), 2. Form Record (checked), 3. Server Records (checked), 4. OAuth2 Record (selected and checked), 5. Comments, and 6. Review And Confirm. The main form area is divided into two sections: "Record Information" and "Client Credentials Configuration". The "Record Information" section includes a "Grant Type*" dropdown menu with "Client Credentials" selected. The "Client Credentials Configuration" section includes fields for "Access token URL*" (with a preview of "http://www.application"), "Scope", "Client ID", and "Client Secret". A "Cancel" button is at the bottom left, and "Previous" and "Continue" buttons are at the bottom right.

New Tokens for AssetView

We have introduced the following new search tokens to enhance your search results:

- **oci.compute.state**: This token helps you search all assets with a specific state.
- **ibm.virtualServer.id**: This token helps to search for all assets with a specific virtual server ID.
- **ibm.virtualServer.location**: This token helps to search for all assets with a specific virtual server location.
- **ibm.virtualServer.datacenterId**: This token helps to search for all assets with a specific virtual server data center ID.
- **ibm.virtualServer.deviceName**: This token helps to search for all assets with a specific virtual server device name.
- **ibm.virtualServer.publicIpAddress**: This token helps to search for all assets with a specific virtual server public IP address.
- **ibm.virtualServer.privateIpAddress**: This token helps to search for all assets with a specific virtual server private IP address.
- **ibm.virtualServer.publicVlan**: This token helps to search for all assets with a specific virtual server public Vlan.
- **ibm.virtualServer.domain**: This token helps to search for all assets with a specific virtual server domain.
- **ibm.virtualServer.privateVlan**: This token helps to search for all assets with a specific virtual server private Vlan.
- **ibm.tags.name**: This token helps to search for all assets with a specific tag name.
- **ibm.tags.value**: This token helps to search for all assets with a specific tag name.
- **gcp.compute.imageId**: This token helps to search for all assets with a Google Cloud Platform image ID.

Issues Addressed

CA Cloud Agent

- We have updated the description on the 'Deactivate Agent' window to convey correct purge behavior.

AM AssetView

- We fixed an issue where you could not download reports.



Administration

- We fixed an issue where the filters did not reflect the correct number of users. The filter showed all users instead of the filtered ones.
- We fixed an issue where an incorrect timestamp was shown if you sorted the Action log data by timestamp.

VMDR

Vulnerability Management, Detection, and Response

- We fixed an issue where the **lastActivity** QQL token showed the incorrect data.
- We fixed an issue where an Invalid CVE entry was made, and threat feed cards were stuck in calculating state.
- We fixed an issue where the Solutions column in the downloaded CSV report did not contain any data.
- We fixed an issue where the data on the Vulnerabilities tab was loading slowly.

UD

Unified Dashboard

- We fixed an issue where the widget stopped responding when you enabled the trending option for a widget if the query size was more than 2000 characters.
- We fixed an issue where the Tagging filter was not working for the comparison widget type.
- We fixed an issue where the severity number and dashboard colors were incorrectly mapped for the Qualys Severity dashboard.

WAS

Web Application Scanning

- We fixed an issue where WAS displayed an error message "an error has occurred" when exporting a sitemap.
- We fixed an issue where WAS scans failed to associate the authentication profiles with Selenium script to one or more web applications when doing multi-scan. This happened when the user launched a scan on multiple web applications with the same authentication profiles with Selenium script as the default authentication profile. Now,

WAS scan associates the default authentication profiles with the corresponding web applications when the same profiles are used for them when doing multi-scan.

- We fixed an issue where the web application schedule for malware monitoring was removed when the web application was purged. After the fix, schedules are retained for purged web applications.
- We fixed an issue where the WAS showed an error message "An error occurred during creating a report." when the user tried to create a web application report. After the fix, users can generate reports.
- We fixed an issue where the users were unable to upload burp findings due to an error. This error occurred because the burp findings that the user was trying to upload had a burp type that has no matching entry in our database. Now, we have added this burp type to our database to fix the issue.