



Qualys Cloud Platform v3.x

Release Notes

Version 3.7

July 8, 2021 (Updated July 13, 2021)

Here's what's new in Qualys Cloud Suite 3.7!

WAS

Web Application Scanning

[Parameterization of Username and Passwords in Selenium Scripts](#)

[Direct Upload of OpenAPI Specification and Swagger files](#)



Administration Module

[Default Permissions for Reader Role](#)

CA

Cloud Agent

[Agent Last Activity for VM and PC Scans](#)

Qualys Cloud Platform 3.7 brings you many more improvements and updates! [Learn more](#)

Parameterization of Username and Passwords in Selenium Scripts

In past versions, you would need to manually edit and re-upload a Selenium authentication script if a username or password needed to be changed. Our new feature allows you to parameterize the username and password in a way that simplifies this process, managing the username and password under the Selenium script form fields instead. To take advantage of this new feature, please follow these steps:

1. Record a Selenium script using the Qualys Browser Recorder. Once you have finished, stop the recording. We will be manually editing a few fields.

click	link=Sign in	
sendKeys	id=signin-loginid	joe.smith@qualys.com
sendKeys	id=signin-password	MySecretPassword
click	id=submitButton	

2. Click on the row where the username is defined. In the example below, this is a 'sendKeys' command. This will allow you to edit the value of the username below. We will need to change it to @@authusername@@.

click	link=Sign in	
sendKeys	id=signin-loginid	joe.smith@qualys.com
sendKeys	id=signin-password	MySecretPassword
click	id=submitButton	

1. Click on the row where the username is recorded
2. Replace the actual username with @@authusername@@

Command	sendKeys
Target	id=signin-loginid
Value	@@authusername@@

- Do the same for the password field, replacing the actual password with @@authpassword@@.

click	link=Sign in	
sendKeys	id=signin-loginid	@@authusername@@
sendKeys	id=signin-password	MySecretPassword
click	id=submitButton	
<div style="border: 1px solid red; padding: 2px; display: inline-block;"> 1. Click on the row where the password is recorded 2. Replace the actual password with @@authpassword@@ </div>		
Command	sendKeys	
Target	id=signin-password	
Value	@@authpassword@@	

- Save the Selenium script and upload it into your Qualys WAS Authentication Record. After you upload the Selenium script, select the "Add credentials to Selenium Script" check box. You will see the Standard configuration section showing the username and password fields. Enter the username and password in the respective fields. During the scan, we will replace @@authusername@@ and @@authpassword@@ with the username and password that you have provided here.

Web Application Authentication Record Creation Turn help tips: On | Off Launch help X

Step 2 of 5

1 Basic Information ✓

2 Form Record ✓

3 Server Records

4 Comments

5 Review And Confirm

Set credentials used to authenticate against web application.

search for "<form" (without the quotes). Most browsers allow you to view the source either through the "View" menu or by right-clicking on the page.

There may be several forms on the page. Be sure to copy details from the form that contains the login fields.

Type* Add credentials to Selenium Script

Selenium script

Standard Configuration

Enter the form authentication credentials into the following fields.

User Name*

Password Confirm Password

Selenium (Automated Authentication)

Import the Selenium script to be used for authentication to web applications using this authentication record. Use Qualys Browser Recorder to create a Selenium script. Want to learn more? Watch this [video](#) or visit the Qualys Browser Recorder (QBR) [chrome extension](#).

Script: SeleniumScriptCreds Download View Change

Cancel
Previous Continue

Now if you ever need to update the username or password for a given application, you can quickly make the change right in the Authentication Record itself by changing the username and password under the Selenium script form fields.

Direct Upload of OpenAPI Specification and Swagger files

Customers scanning API endpoints using OpenAPI Specification (OAS) and Swagger files were previously required to host their files online. With this change, customers will now be able to directly upload their OAS and Swagger files into their Qualys WAS configuration file for their APIs. This functionality will mirror the ability to directly upload Postman Collections for API scanning.

The screenshot shows the 'Web Application Creation' interface, specifically Step 2 of 11, titled 'Application Details'. The main heading is 'Tell us about the web application you want to scan'. Under the 'API Endpoint Definition (Swagger and non-Swagger based APIs)' section, there are three radio button options: 'None' (selected), 'Postman Collection', and 'Swagger/OpenAPI File'. The 'Swagger/OpenAPI File' option is highlighted with a red rectangular box. Below this option, there is a text description: 'You have the option to upload a Swagger/OpenAPI File for your API. We currently support version 2.0 and 3.0. Once uploaded we will parse it to create requests and then crawl and test those requests.' Below the text is a blue button with a plus sign and the text 'Upload Swagger/OpenAPI File'. Other options include 'Burp Proxy Capture' with a description and an 'Upload Burp Log File' button, and 'Postman Collection' with a description and three upload buttons: 'Upload Postman Collection File (Mandatory)', 'Upload Postman Environment Variables File (Optional)', and 'Upload Postman Global Variables File (Optional)'. The interface also features a sidebar with 11 steps, a 'Cancel' button, and 'Previous' and 'Continue' buttons at the bottom right.



Administration Module

Default Permissions for Reader Role

We have changed the default permissions assigned to new users created with reader role. Depending on when a customer has subscribed with Qualys, a user with reader role may or may not have tagging permissions (Create User Tag, Edit User Tag, Delete User Tag) assigned to him.

- **Subscribed to Qualys before Cloud Platform 3.7 release:** By default, a user with reader role will have tagging permissions (Create User Tag, Edit User Tag, Delete User Tag). You can remove the permissions by altering the tagging permissions in Admin utility.

- **Subscribed to Qualys after Cloud Platform 3.7 release:** By default, a user with reader role does not have tagging permissions (Create User Tag, Edit User Tag, Delete User Tag). You need to explicitly assign the permissions to them.

Agent Last Activity for VM and PC Scans

With this release, we've updated Last Activity column of the agent list to include last scan time for VM and PC for better tracking.

The screenshot shows the 'Agent Management' dashboard with a table of agents. The 'Last Activity' column is highlighted with a red box for the first agent, showing 'VM Scan: an hour ago' and 'PC Scan: an hour ago'.

Agent Host	OS	Version	Last Activity	Last Checked In	Configuration	Agent Modules	Tags
DESKTOP-IV41S9F 10.115.74.195, feb...	Microsoft Win...	3.1.5.43	Configuration Downloaded 2 minutes ago VM Scan: an hour ago PC Scan: an hour ago	2 minutes ago	CAUI-6758-Test	PM AI VM PC	Test-tag Cloud Agent
test1.rdlab.in03.q... 10.115.120.111, 0:...	Red Hat Enter...	3.3.0.8	Scan Complete 5 minutes ago VM Scan: 9 minutes ago	5 minutes ago	Initial Profile	PM AI VM PC	CAUI-6758 Cloud Agent
cams.rdlab.in03.q... 10.115.121.65, 0:0:...	CentOS Linux...	4.1.0.18	Scan Complete 14 minutes ago VM Scan: 18 minutes ago PC Scan: 11 hours ago	14 minutes ago	3.5.0.0-RC2-23-Feb-21	AI VM PC	Cloud Agent CAUI-6758

Issues Addressed

CA Cloud Agent

- We fixed an issue where some search filters, such as aws.ec2.accountId: were giving incorrect results.

AM AssetView

- We improved the execution of update/am/hostasset API script, where in case of parallel request, the second and consecutive request caused a long time for asset tagging to complete.
- We fixed an issue where the Azure instances did not include the Succeeded state in the SearchHostAssets and GetHostAssets API calls and on the UI.
- We fixed an issue where the tags were not getting reevaluated if the dynamic tag rule was modified via API.
- We fixed an issue where duplicate tags were automatically created for the Unmanaged and Passive sensor tags.

UD Unified Dashboard

- We fixed an issue where sometimes an error occurred when you tried to create a duplicate widget.

VMDR Vulnerability Management, Detection, and Response

- We fixed an issue where the following error occurred when you tried to save and download the Prioritized Patch report in the CSV format.
“An unexpected error seems to have occurred, while fetching data. Displayed list of records could be incomplete.”
- We fixed an issue where the Prioritization tab showed an incorrect number of assets.