



Qualys Cloud Suite 2.23

We're excited to tell you about improvements and enhancements in Qualys Cloud Suite 2.23.



AssetView



ThreatPROTECT

[Download List of Assets as Grouped on UI](#)

[Download Details from within Asset Details Window](#)



Cloud Agent

[Changes, Organization and Description of Performance Interface](#)



Security Assessment Questionnaire

[Set Criticality and Assign Scores to Templates](#)



Web Application Scanning

[WAS Scan Enhancements](#)

[New Support for Burp Log File Upload](#)

[Support for Path Fuzzing Rules](#)

[Exclude Username from Reports](#)



Web Application Firewall

[Standardized name for Registration Code](#)

Qualys Cloud Platform

[EC2 Scanning support for AWS GovCloud \(US\)](#)

[EC2 Scanning support for more Regions](#)

Qualys Cloud Suite 2.23 brings you many more
Improvements and updates! [Learn more](#)



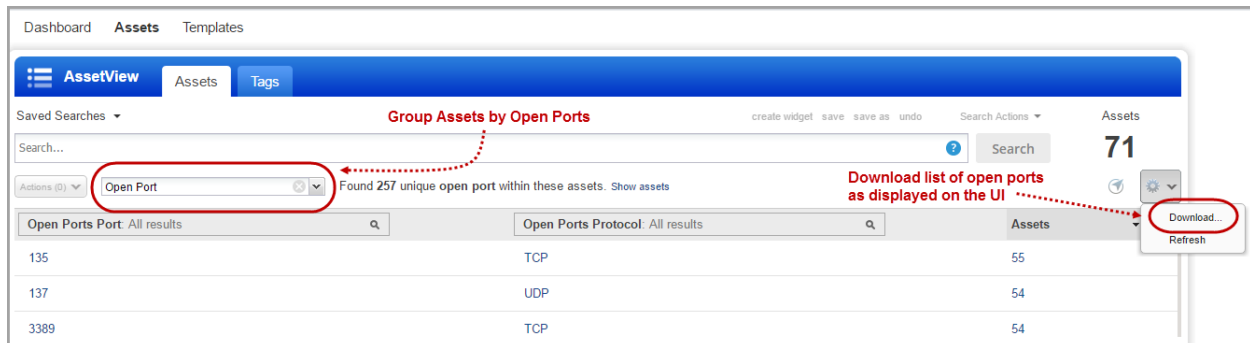
AssetView

ThreatPROTECT

Download List of Assets as Grouped on UI

With this release you can now download the asset information as displayed in the UI as per your grouping preference.

For example if you group assets by Open Ports and select the Download option we'll download the open port results as seen on the UI.



Download Details from within Asset Details Window

You can now download the Open Ports, Installed Software, and Vulnerabilities lists from within the Asset Details window.

Open Ports and Installed Software - click Download to download the lists.

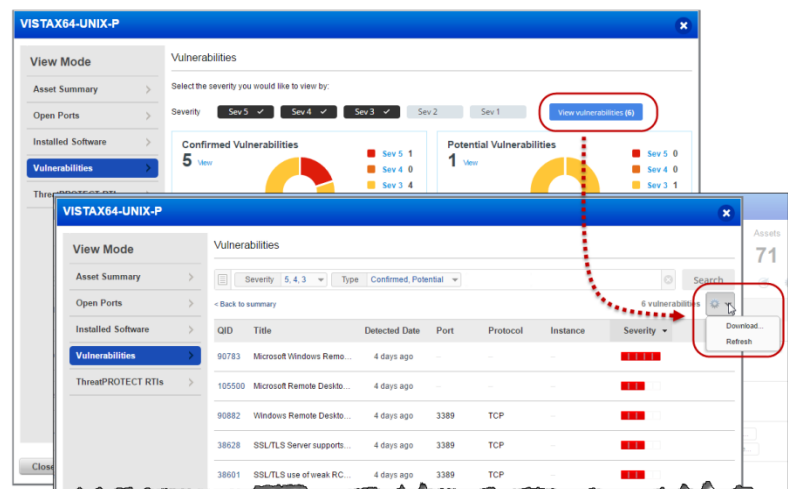
Open Ports

This list includes ports with listening services.

Download

Port	Protocol	Service Description
------	----------	---------------------

Vulnerabilities - click View Vulnerabilities and select Download from the tools menu.



Changes, Organization and Description of Performance Interface

You'll notice the performance profile UI has four sections with new and changed values introduced for Windows Agent 1.5 and Linux/Mac Agent 1.6. Also we've added OS specific parameters. A separate section details legacy parameters. We'll support legacy parameters/settings used by older agents as some customers will still have these versions deployed in production.

Tell me about parameter changes

Name	Change description	OS	Value Range	Profile defaults
Agent Status Interval (renamed from "Update system with Agent's status")	Changed label and values	All	300-86,400 secs	High: 600 Normal: 1,800 Low: 2,400
CPU Throttle	Changed values	Linux/Mac	0-1000 ms	High: 0 Normal: 10 Low: 20
CPU Limit	New parameter	Windows	2-100%	High: 80 Normal: 20 Low: 5
Delta Upload Interval	Changed values	All	1-1,800 secs	High: 1 Normal: 5 Low: 10
Chunk sizes for File Fragment Uploads	Changed values	All	64-10,240 KB	High: 4,096 Normal: 2,048 Low: 1,024

What are Legacy parameters?

These are configurations used for Windows 1.4 Agent and below, and Linux/Mac 1.5 Agent and below.

Legacy parameters:

Delta Confirmation Interval, Manifest Download Interval, Configuration Download Interval, Network Throttle Rx, Network Throttle Tx, Chunk sizes for file fragment downloads, Revocation Interval, Provisioning Interval, Upgrade Check Interval

Good to Know – Auto upgrade of some parameters/values

The following changes will occur automatically at the time of release.

- Existing system configuration profiles (High, Normal, Low) will use the new or changed values as described above.
- Custom configuration profiles will inherit the Low values of the new configuration parameters. There will be no changes to any existing values that have new defined values.

Updated Configuration Profile UI

The first section in the configuration profile UI shows parameters that apply to all OS for all agent versions. As you scroll down you'll see sections for OS specific parameters and Legacy parameters.

Configuration Profile Creation

Turn help tips: On | Off

Step 3 of 4

1 General Info

2 Blackout Windows

3 Performance

4 Assign Hosts

Configure Agent Performance

These settings govern how an agent behaves, from how often it checks into the Qualys Cloud platform, to how often it checks the host for changes. It also includes performance settings that control CPU and network utilization.

Performance

Select one of the performance levels below. Keep the default settings or customize them.

Based On: Low

Set Parameters

Agent Status Interval* 900 sec(300 - 86400)
Push interval in seconds to update system with Agent's status

Delta Upload Interval* 10 sec(1 - 1800)
Interval an agent attempts to upload detected changes

Chunk sizes for file fragment uploads* 1024 KB(64 - 10240)
This is the upload block size, and combined with the above Network throttle Tx, determines network utilization

Upgrade Reattempt Interval* 300 sec(180 or more)
Interval an agent will retry applying a new upgrade to itself

Logging level for agent* Verbose
This is the logging level for the agent.

2 Blackout Windows

3 Performance

4 Assign Hosts

WINDOWS SPECIFIC PARAMETERS (versions 1.5 and above)

CPU Limit* 5 %
Defines the percentage limit of the processor core(s) used by the agent. Lower percentages reduces CPU utilization at the expense of longer execution times.

LINUX/MAC SPECIFIC PARAMETERS (versions 1.6 and above)

CPU Throttle* 20 ms(0 - 1000)
The higher this value, the lower CPU utilization but longer agent takes to perform actions on it's host

LEGACY PARAMETERS (used for Windows 1.4 and below, and Linux/Mac 1.5 and below)

Delta Confirmation Interval* 300 sec(60 or more)
Interval an agent checks platform for confirmation that changes were processed

Manifest Download Interval* 10800 sec(60 or more)
Interval an agent checks platform for new instruction manifests



Security Assessment Questionnaire

Set Criticality and Assign Scores to Templates

With this release you now have the ability to set criticality and assign scores while defining templates.

To set scores and criticality:

Click Template Scoring.

Here, define the scoring labels and values.

You can add scoring to these question types only: Dropdown, Yes/No, Multi-select, and Single Select

Select a question and click Edit in the Answer Options to define a score for that answer.

From the Scoring drop-down select a score.

Do this for every answer in each question.

The screenshot shows the Qualys Security Assessment Questionnaire interface. A 'Template Scoring' dialog box is open, allowing users to define scoring labels and values. The dialog has two columns: 'Scoring Label' and 'Scoring Value'. The 'Scoring Label' column has three rows: 'LOW', 'MEDIUM', and 'HIGH'. The 'Scoring Value' column has three rows: '0', '50', and '100'. There are plus and minus buttons between the columns to adjust the values. A 'Save' button is at the bottom right of the dialog. In the background, the 'Template Scoring' link is circled in red in the top right corner of the main interface.

The screenshot shows the Qualys Security Assessment Questionnaire interface. The 'Edit Answer' dialog box is open, allowing users to define the answer options for a specific question. The dialog has a 'Text' field with the value 'Not Applicable' and a 'Value' field with the value '0'. There are three checkboxes: 'Attachment', 'Comment' (checked), and 'Asset'. There is a 'Scoring' dropdown menu with the value 'LOW' selected. There is a 'Description' field with the value 'LOW'. There are 'Cancel' and 'Save' buttons at the bottom. In the background, the 'Click Edit' link is circled in red in the 'Answer Options' section of the main interface.

Select criticality for the question from the Criticality dropdown.

Category: Quick wins

Controls within this category are designed to help an organization rapidly improve its security stance generally without major procedural, architectural, or technical changes to its environment. It should be noted, however, that a Quick Win does not necessarily mean that these subcontrols provide comprehensive protection against the most critical attacks. The intent of identifying Quick Win areas is to highlight where security can be improved rapidly.

CSC.01.QW.1.1 Has the organization deployed an automated asset inventory discovery tool and uses it to build a preliminary asset inventory of systems connected to an organization's public and private network(s)?

☐ Not Applicable
Specify reason as to why the control is not applicable to the organization. Attach relevant support documents, if any.

☒ Not Implemented
Specify reason as to why the organization has not implemented the control, and the plans with target date to meet the requirement. Attach relevant support documents, if any.

☐ Partially Implemented
Provide evidence for partial compliance and the target date of full implementation. Attach relevant support documents and reports.

☐ Fully Implemented
Provide evidence for full compliance. Attach relevant support documents and reports.

CSC.01.QW.1.2 Does the organization employ both, active tools that scan through network address ranges and passive tools that identify hosts based on analyzing their traffic?

☐ Not Applicable
Specify reason as to why the control is not applicable to the organization. Attach relevant support documents, if any.

☐ Not Implemented
Specify reason as to why the organization has not implemented the control, and the plans with target date to meet the requirement. Attach relevant support documents, if any.

☐ Partially Implemented
Provide evidence for partial compliance and the target date of full implementation. Attach relevant support documents and reports.

Compact Expanded

Radio Group Multi-select

Answer Options

Not Applicable

Not Implemented

Partially Implemented

Fully Implemented

Add Option

Criticality:

INFO

LOW

MEDIUM

HIGH

CRITICAL

Comments

Once you are done setting scoring and criticality, Save and Publish the template. You can now use this template to launch Campaigns and Reports.

When you generate reports you can view and filter questions based on criticality and scores.



WAS Scan Enhancements

We're excited to tell you about the many enhancements we've made to WAS scan in this release.

End Time Limitation Removed for Multi Scan

We have now removed the 48 hour (maximum default deadline) restriction for a multi scan. Now, you can group several hosts in a multi scan and expect the scan to be completed without any time limitation. The single scan retains the 24 hour (maximum default scan time) limit from the time the scan begins.

Bulk WAS Scan Status Enhancements

We have improvised and introduced new scan status to give your better visibility on the single scans as well as multi scans (parent and child scans).

Multi Scan

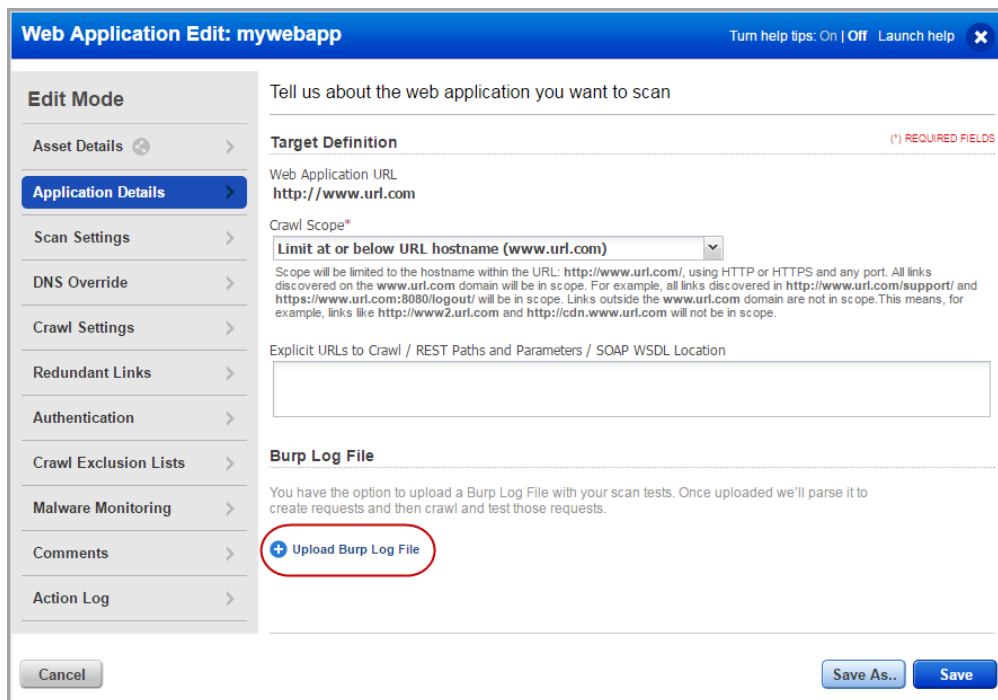
New Multi-Scan Status	Child/Single Scan Status	Cause	Scan Result
Time Limit Reached	Time Limit Reached	When the child scan ends due to lack of time as defined in the "Cancel At X Time" setting.	The scan result does not include any data.
Canceled	Canceled	Parent scan is manually cancelled by the user.	The scan result does not include any data.
Finished	Time Limit Reached	When the child scan ends due to lack of time either because of "Cancel After X hours" setting or Scan Time Limit specified in your subscription (maximum 24 hours by default).	The scan result contains all information and vulnerabilities that the scan has been able to collect and detect.
Finished	Scanner Not Available	Unavailability of scanner	The scan result does not include any data.
Finished	Error	When at least one child scan ends with Error.	The scan result does not include any data.

Single Scan

Scan Status	Cause	Scan Result
Time Limit Reached	When the scan ends due to lack of time as defined in the "Cancel At X Time" setting.	The scan result does not include any data.
Canceled	Scan is manually cancelled by the user.	The scan result does not include any data.
Scanner Not Available	Unavailability of scanner	The scan result does not include any data.

New Support for Burp Log File Upload

We now provide you a new option to upload BURP log files. After you upload, we will parse it to create requests and then crawl the web application.



Web Application Edit: mywebapp Turn help tips: On | Off Launch help

Edit Mode

- Asset Details
- Application Details**
- Scan Settings
- DNS Override
- Crawl Settings
- Redundant Links
- Authentication
- Crawl Exclusion Lists
- Malware Monitoring
- Comments
- Action Log

Tell us about the web application you want to scan

Target Definition (*) REQUIRED FIELDS

Web Application URL
http://www.url.com

Crawl Scope*

Limit at or below URL hostname (www.url.com)

Scope will be limited to the hostname within the URL: http://www.url.com/, using HTTP or HTTPS and any port. All links discovered on the www.url.com domain will be in scope. For example, all links discovered in http://www.url.com/support/ and https://www.url.com:8080/logout/ will be in scope. Links outside the www.url.com domain are not in scope. This means, for example, links like http://www2.url.com and http://cdn.www.url.com will not be in scope.

Explicit URLs to Crawl / REST Paths and Parameters / SOAP WSDL Location

Burp Log File

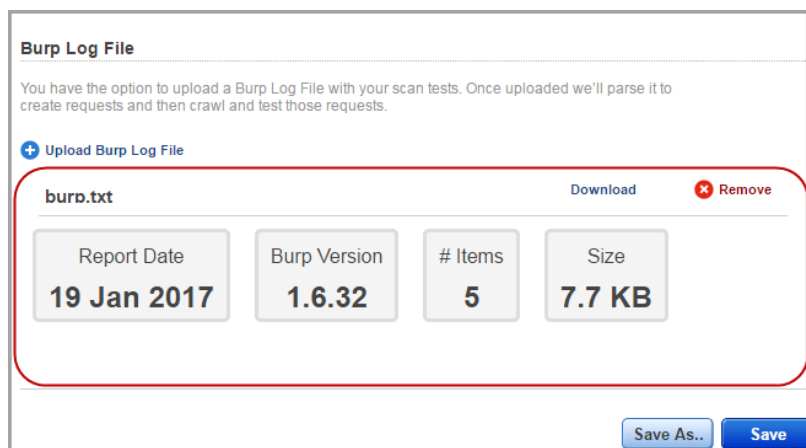
You have the option to upload a Burp Log File with your scan tests. Once uploaded we'll parse it to create requests and then crawl and test those requests.

[+ Upload Burp Log File](#)

Cancel Save As.. Save

You can upload the file when you create or edit a web application.

After you have uploaded the file, you can always download and view the Burp file. You can upload only one BURP file at a time. If you upload a second file, the new file will replace the old file.



Burp Log File

You have the option to upload a Burp Log File with your scan tests. Once uploaded we'll parse it to create requests and then crawl and test those requests.

[+ Upload Burp Log File](#)

burp.txt Download Remove

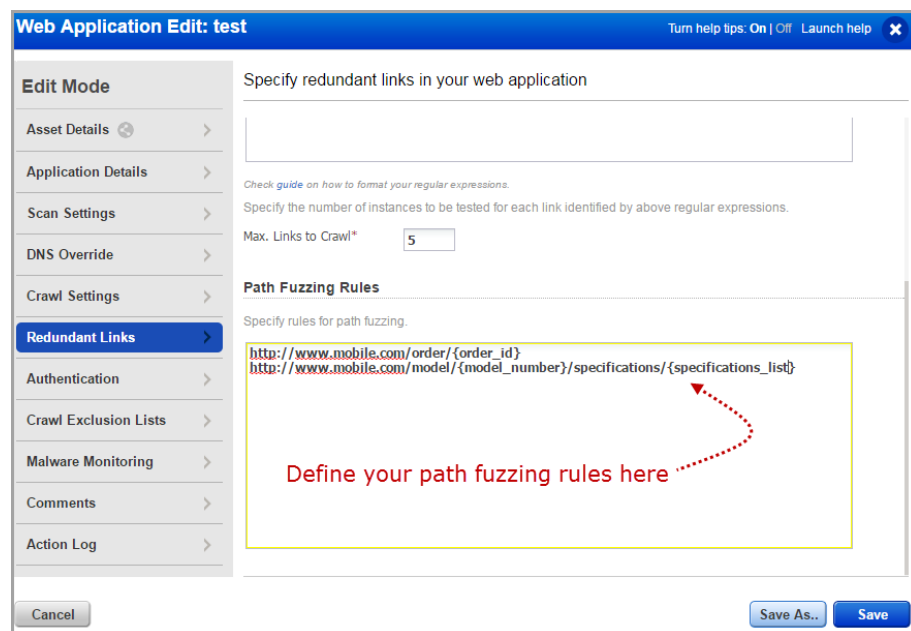
Report Date	Burp Version	# Items	Size
19 Jan 2017	1.6.32	5	7.7 KB

Save As.. Save

Support for Path Fuzzing Rules

We now support path fuzzing for your web page URLs. If your web application uses URL rewrite, you can now tell us the path components that need to be fuzzed (resolved) by defining the path fuzzing rules. The rules will tell us the path components/parameters that need to be fuzzed and we will prevent multiple crawling of paths that meet the rules.

Define the path fuzzing rules in Redundant Links section of your web application settings and we will skip crawling of the web pages for URLs that meet the rules.



Example: Let us consider sports web page

<http://www.abc.com/issue/17/section/sports/article/28>

However, the web server will read this URL as

<http://www.abc.com/search.php?issue=17§ion=sports&article=28>

The path fuzzing rule would be:

<http://www.abc.com/issue/{issue}/section/{section}/article/{article}>

Let us consider a different example where the parameter names are not part of the URL path

www.myweatherstation.com/weather/daily/94065/010117

www.myweatherstation.com/weather/weekly/94065/1

www.myweatherstation.com/weather/monthly/94065/1

In such cases, the path fuzzing rule would be defined as

www.myweatherstation.com/weather/daily/{pincode}/{date}

www.myweatherstation.com/weather/weekly/{pincode}/{week}

www.myweatherstation.com/weather/monthly/{pincode}/{month}

Defining the path fuzzing rules will ensure that the parameters are fuzzed and we will limit the number of paths that match the same rule because they are redundant.

Exclude Username from Reports

By default we include the user's account login ID in the reports you choose to download. Now, you have the option to exclude the account login ID from the reports. Just select the checkbox under Exclude Qualys username from report template.

Report Template Creation Turn help tips: On | Off Launch help

Step 1 of 3

- 1 Details ✓
- 2 Filter
- 3 Display

Tell us about this report template

detected vulnerabilities and sensitive contents. Report details include detection data and verified solutions for remediation.

From the finished report, you can edit the settings and apply content filters.
[Add your own description for this report template](#)

Tags

Select tags to apply to the report template [Select](#) [Create](#) [Remove All](#)

(no tags selected)

Exclude Qualys username from report

By default we will include the user name in the downloaded reports. Select this option to remove the user name from the reports.

☐ Exclude Qualys username from report

[Cancel](#) [Continue](#)

The Exclude Qualys username option is available in Web Application, Scan, Scorecard, and Catalog custom report templates. The report you download is now named as per the custom template name appended with a date stamp in yyyyddmm format.



Standardized name for Registration Code

Previously, the registration code was also referred to as the personalization code or registration token at several places on the UI, such as the appliance download screen, the cluster view, the appliance CLI, and so on. This could have caused confusion when actually it refers to the same thing. To make it simple, we now refer to it only as the **Registration Code**.

The screenshot displays the WAF cluster management interface. On the left, a list of clusters is shown: CLUSTER5 (highlighted in yellow), CLUSTER4 (highlighted in blue), and CLUSTER1. Each cluster entry includes a radio button, a dropdown menu, a status icon, and a date (12 Aug 2016). On the right, a detailed view for CLUSTER5 is shown. This view includes fields for ID (5008), Owner, Created on (12 Aug 2016 2:40PM GMT+0530), and Updated on (12 Aug 2016 2:40PM GMT+0530). A red circle highlights the 'Registration Code' field, which contains the value 6A5C025B-66DC-40D5-B3E2-ABD34726F74F.

Cluster	Status	Date
CLUSTER5	—	12 Aug 2016
CLUSTER4	1	12 Aug 2016
CLUSTER1	—	12 Aug 2016

CLUSTER5	
ID	5008
Owner	
Created on	12 Aug 2016 2:40PM GMT+0530
By	
Updated on	12 Aug 2016 2:40PM GMT+0530
By	
Registration Code	6A5C025B-66DC-40D5-B3E2-ABD34726F74F

Qualys Cloud Platform

EC2 Scanning support for AWS GovCloud (US)

Now you can easily scan EC2 instances included in the AWS GovCloud (US) region for vulnerabilities and policy compliance using the Qualys Cloud Platform. All you need is the AWS GovCloud feature enabled for your subscription. Once enabled, you can create/update EC2 connectors to pull instance info from the GovCloud (US) region, activate discovered instances for the VM and/or PC module, and scan them using our EC2 scan workflow.

Want to enable AWS GovCloud for your subscription? Sure thing. Just reach out to Qualys Support or your Qualys Account Manager.

What are the steps? Navigate to the AssetView (AV) module > Connectors section. Click the “Create EC2 Connector” button. Using the wizard, give the connector a name, select an authentication record and choose “Enable GovCloud”. Under EC2 Regions you’ll see AWS GovCloud (US) only. Select this region and complete the steps for tags and activation as you like.

The screenshot shows the 'Create EC2 Connector' wizard in the Qualys Enterprise interface. The wizard is at Step 2 of 5, 'EC2 Authentication'. The left sidebar shows the progress: 1. Connector Details (checked), 2. EC2 Authentication (current step), 3. EC2 Regions, 4. Tags and Activation, and 5. Review. The main content area is titled 'EC2 Authentication Information' and contains a section 'Select one AWS Authentication Record' with a red asterisk indicating a required field. Below this is a table with columns 'ID', 'Title', and 'Comments'. One record is listed with ID '122603' and Title 'my record'. Below the table, there is a checkbox labeled 'Enable GovCloud' which is checked and circled in red. At the bottom of the wizard, there are buttons for 'Cancel', 'Previous', and 'Continue'.

EC2 Scanning support for more Regions

More EC2 regions are available for scanning using the Qualys Cloud Platform. The following regions are now visible in the EC2 Connector wizard, within AssetView (AV), and can be selected for asset activation and scanning:

- US East (Ohio)
- Asia Pacific (Mumbai)
- Asia Pacific (Seoul)
- EU (London)
- Canada (Central)

Issues addressed in this release

Qualys Cloud Suite 2.23 brings you many more improvements and updates.



AssetView



ThreatPROTECT

- We have now fixed the asset search for exact match of interfaces.hostname to display correct results.
- Queries with ranges now display correct results when you click grouped vulnerability asset count.
- The asset list displayed on clicking the Assets with Easily Exploitable Vulnerabilities widget now displays correct data sorted in descending order.



Cloud Agent

- The Last Checked-in column now displays correct data when sorted in ascending or descending order.
- We added a new field FQDN in Asset Summary section that displays the domain name.hostname (provided domain is specified for the host).
- We provided more error codes/descriptions in the Cloud Agent online help and installation guides. We've added Linux error codes and these Windows error codes:
995 (Information) - ERROR_OPERATION_ABORTED
424 (Error) - HTTP_STATUS_FAILED_DEPENDENCY
30004 (Error) - QAGENT_ERROR_NO_RESOURCE_FOUND
30006 (Error) - QAGENT_BREAK_PROCESSING



Security Assessment Questionnaire

- Delegation of a questionnaire section can now be removed and the section is reassigned to the original user.
- With this release, you can now delete and re-upload files attached to questions in a questionnaire."
- In the answer summary of the report preview, you can now see relevant information depending on the workflow type.
- In the Display tab of the Report Edit window, the choice of components that can be displayed in the report are now shown as a tree structure for better readability.
- Toggle button to turn Help Tips on or off is now visible for Create Report wizard.
- Multi-select type of questions are now displayed in correct chronological order in both, Preview and final Report after download.

- Single Select type of questions are now displayed in correct chronological order in both, Preview and final Report after download.
- Dates of questionnaire instances are now displayed according to the user's time zone in the report.
- All dates in the report preview will now be displayed in the “MMM DD, YYYY” format.
- All the % values displayed in the report preview are now rounded off to the nearest whole number.
- Boolean type questions will appear same as Multiselect in Report preview.
- You will be able to type and select campaigns from combo box similar to the Template combo box.
- You can now preview a report by clicking on View Report.
- Dropdown or Multiple choice type of questions will now be sorted chronologically as per answer choices in both, preview and final report after download.
- In the Display tab of Report Edit, you now have two new options “Header information” and “Filter” which you can use to show or hide information in reports. This is especially useful in case of CSV report.
- "Stages" pie chart title is updated to "States".
- In Campaign report, for better readability we now show only precise information about multi choice or single select type of questions.



Web Application Firewall

- The status icon for an inactive Web application now displays the correct tooltip.
- UI help tips for all fields are now displayed properly.
- You can now add tags to profiles for Web Servers, Healthchecks, SSL Certificates, and HTTP Profiles.
- The Review and Confirm panel is now added to the Policies wizard and the HTTP Profiles wizard.

Cloud Agent Platform

- Asset Management and Tagging API v2 - The request with "tagName" filter and NOT_EQUALS operator now displays correct results for search, count, activate, update and delete actions for "asset" and "hostasset" REST APIs (v2.0) using the Asset Management and Tagging API v2. Note that activate, update and delete actions with NOT_EQUALS operator should be used cautiously as it has a potential to activate, update, and delete unintended assets or hostassets in your subscription.