



Qualys Cloud Suite 2.25

We're excited to tell you about improvements and enhancements in Qualys Cloud Suite 2.25.



ThreatPROTECT

[Improved ThreatPROTECT Summary](#)



Cloud Agent

[Configure scan interval for VM and PC](#)



Web Application Scanning

[Form Training Support](#)

[Enhanced FQDN and DNS information via Catalog Discovery](#)

[Granular Permission Settings](#)

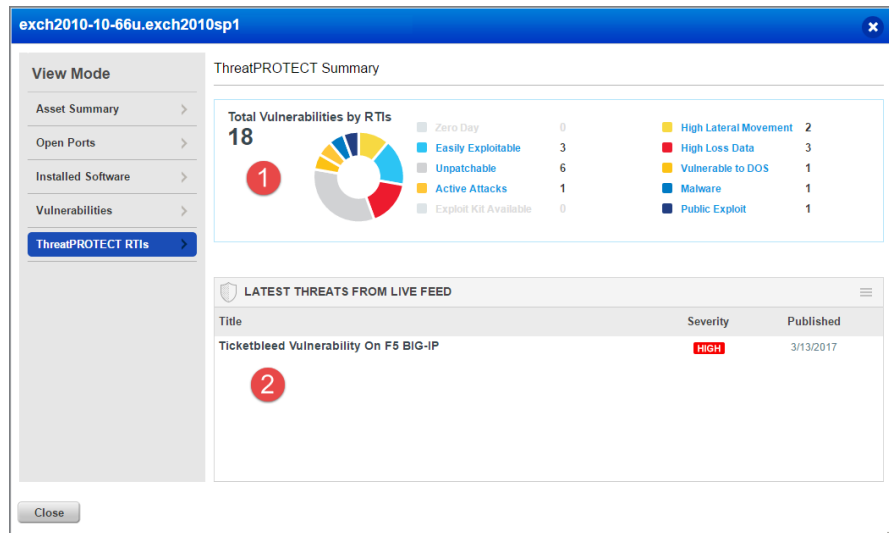
[Default Report Format now Supports Encrypted PDF](#)

Qualys Cloud Suite 2.25 brings you many more
Improvements and updates! [Learn more](#)

Improved ThreatPROTECT Summary

We have now enhanced the ThreatPROTECT Summary tab for better readability. You can drill-down to detailed information by clicking on various areas in the summary.

- 1) Click the pie chart or text to view the list of related vulnerabilities.
- 2) Click Title of the RTI in the Live Feed table to open the related blog post.



Configure scan interval for VM and PC

The interval at which the agent collects Vulnerability Management (VM) and Policy Compliance (PC) data is now configurable. The interval is the time lapse between the completion of the previous scan and the start of the next scan.

To configure the scan interval, in the Cloud Agent module, go to Agent Management > Configuration Profiles, and then edit an existing profile or create a new one.

Single manifest

If you are using a single manifest for an agent, go to the Scan Interval panel and then specify the interval in minutes after which the agent collects data. Specify a value between 240 minutes (4 hours) and 43200 minutes (30 days). Default is 240 minutes. The data collection interval you set in a single manifest is applicable to both VM and PC scans.

Configuration Profile Creation Turn help tips: On | Off

Step 5 of 6

Configure Scan Interval

Configure the interval at which the agent collects data for Vulnerability Management and Policy Compliance for the assets associated with this profile.

Data Collection Interval* 240 min (240 - 43200)

The time lapse between the completion of the previous scan and the start of the next scan

1 General Info ✓
2 Blackout Windows ✓
3 Performance
4 Assign Hosts ✓
5 Scan Interval
6 FIM (beta)

Split manifest

If you are using a split-manifest, you can set separate intervals for VM and PC. Go to the VM Scan Interval and PC Scan Interval panels to set separate data collection intervals for VM and PC. Specify values between 240 minutes (4 hours) and 43200 minutes (30 days). Default is 240 minutes.

Configuration Profile Creation Turn help tips: On | Off

Step 5 of 6

Configure Scan Interval for Vulnerability Management

Configure the interval at which the agent collects data for Vulnerability Management for the assets associated with this profile.

Data Collection Interval* 240 min (240 - 43200)

The time lapse between the completion of the previous scan and the start of the next scan

1 General Info ✓
2 Blackout Windows ✓
3 Performance
4 Assign Hosts ✓
5 VM Scan Interval
6 PC Scan Interval

The scan intervals are applied the next time the agent downloads the configuration profile.

Form Training Support

With this release we now fully support Form Training and provide a customization facility to the user for defining a specific form field and its value to be substituted during crawling and fuzzing. This feature now allows customers to override a specific field's value in any given form. Global field names and associated values can be specified as well, independent of any form.

We have introduced a new panel named Advanced Options in the Web Application settings. Define the Form details in Advanced Options Links section of you web application settings and we will override a specific field's value in any given form.

You can define the form details when you create a new web application or edit an existing web application. In Advanced options, click Add Form to add the form details.

Define at least one action URI for the form. You need to define action URI for the form.

You can then add fields for the defined action URI. If your form includes masked, fields, you can define them as well. Masked field could be used for passwords.

After you add the necessary fields, define the name and value for it. You can add or remove the fields at any time. Also, there is no limitation on the number of fields you can define.

To view the form details added to web application, click View from the quick actions menu and the Advanced Options panel will list the form URI and number of fields added for the form. You can click the form URI to view the field details.

Enhanced FQDN and DNS information via Catalog Discovery

You can now locate your web applications even if you don't know where they are. Now with our enhanced discovery method, if a server is running multiple virtual hosts, we can better identify what applications exist and add them into our WAS Catalog. The WAS Catalog is now updated with the web applications that are detected through WAS scans but are not added as web assets.

The screenshot shows the 'Web Application Scanning' interface with the 'Catalog' tab selected. The table lists detected web applications with columns for IP Address, FQDN, Port, NetBIOS, Status, and Created. One entry, 'funkytown.vuln.qa.qualys.com', is highlighted in yellow. A red arrow points from the text 'Web application detected through WAS scan' to a red box in the preview pane. The preview pane shows the URL 'http://funkytown.vuln.qa.qualys.com:80' and a comment: 'System 17 Mar 2017 Web Application added from scan consolidated data from WAS'.

IP Address	FQDN	Port	NetBIOS	Status	Created
asfd.asdv		80		New	17 Mar 2017
10.10.26.238	bank.vuln.qa.qualys.com	80		New	17 Mar 2017
10.10.10.88	com2k12r2-dc.com2012r2.vuln.qa.q...	80	COM2K12R2-DC	New	06 Dec 2016
202.191.140.197	corpbank.com	80		Approved	17 Mar 2017
<input checked="" type="checkbox"/>	funkytown.vuln.qa.qualys.com	80		New	17 Mar 2017
10.10.26.77	funkytown.vuln.qa.qualys.com	80		New	17 Mar 2017
<input type="checkbox"/>	guitar.funkytown.vuln.qa.qualys.com	80		New	17 Mar 2017
<input type="checkbox"/>	lamo2.vuln.qa.qualys.com	80		New	17 Mar 2017

Preview

http://funkytown.vuln.qa.qualys.com:80

IP address: null, FQDN: funkytown.vuln.qa.qualys.com

Updated by -- | 17 Mar 2017 5:27PM GMT+0530 | **New**

Operating System: --

Comment: System 17 Mar 2017
Web Application added from scan consolidated data from WAS

Granular Permission Settings

We have added new permissions giving you more flexibility for complex environments and/or SDLC integration implementations.

We have introduced three fine-grained permissions to configure web application access.

- Edit Web Asset

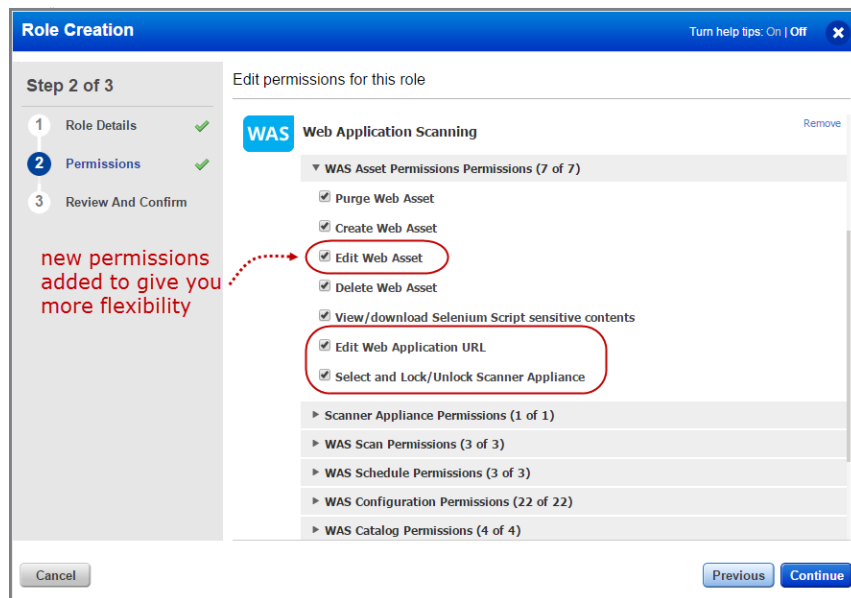
Allows the user to edit all settings related to a web asset except for URL and the scanner appliance.

- Edit Web Application URL

Allows the user to edit only the web asset URL.

- Select and Lock/Unlock Scanner Appliance

Allows the user to select the scanner appliance to be used during scanning of the web application.



Where do I configure the permissions?

Go to the Role Management section of the Administration utility, edit the role for which you want to configure permissions. By default, these permissions are enabled for a user role.

To disable any access, you will have to clear the respective checkbox.

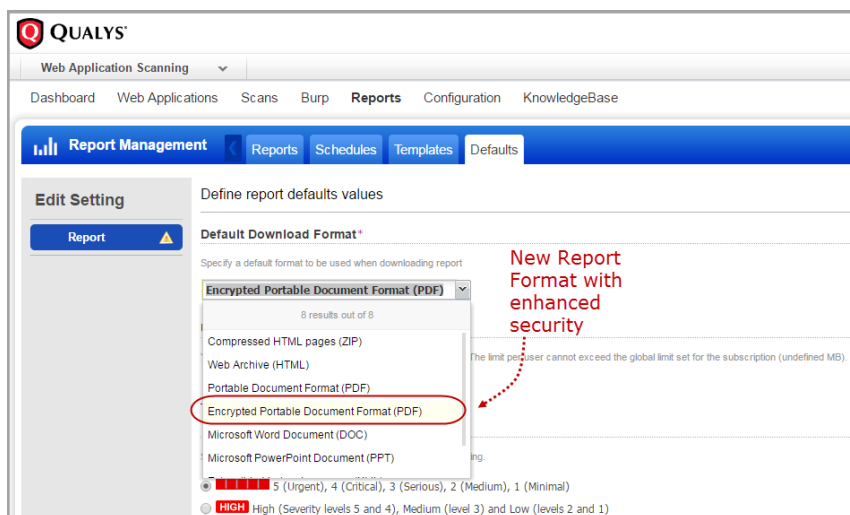
Good to Know

All the three permissions are mutually exclusive and to give complete access to edit a web application, you need to select all the three permissions.

Default Report Format now Supports Encrypted PDF

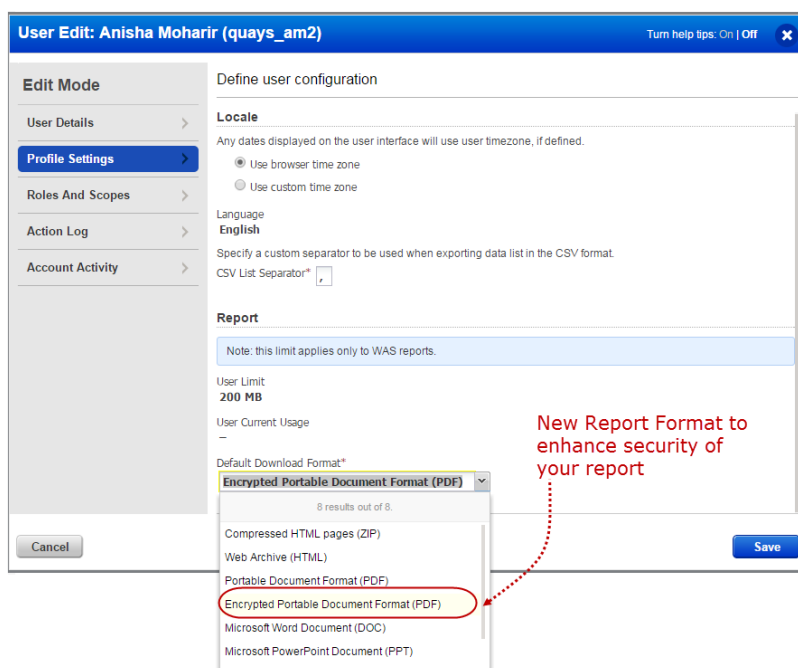
We have now added Encrypted Portable Document Format (PDF) report format to the existing list of default download formats. You can now configure your default report format to Encrypted Portable Document Format (PDF).

To enhance security of your scheduled reports, the email now contains a secured (HTTPS) link to download the report.



Go to Reports > Defaults and edit Reports settings. You can then set the default downloaded report format to Encrypted PDF.

You could also configure this setting from My Profile > Profile Settings > Report and then edit the settings to choose the Encrypted Portable Document Format (PDF) from the Default Download Format dropdown.



Issues addressed in this release

Qualys Cloud Suite 2.25 brings you many more improvements and updates.



AssetView



ThreatPROTECT

- In the AssetView dashboard, you can now successfully filter count and comparison queries by Asset Tags.
- In the AssetView, the Connectors tab will no longer "disappear" when switching between Connectors and Assets > Connectors tabs.
- Severity icons in the Asset Details vulnerabilities list will now correctly represent the vulnerability category.



Cloud Agent

- The AssetName and DNS HostName are now appropriately updated in the Agent data list.



Continuous Monitoring

- We have now internationalized all labels on the UI for Continuous Monitoring.
- You can now add or remove users from the distribution list successfully.



Security Assessment Questionnaire

- Templates are now created successfully even when the template name is in all capital alphabets.
- Questionnaire list now displays accurate relevant data for all active questionnaires in the downloaded report.
- The "Not Started" status is now displayed accurately in the data list whenever applicable.
- The New campaign button is now correctly displayed in the Campaigns tab even when the user navigates to the Campaigns tab via Dashboard.
- The Completion Pie Chart now displays the accurate percentage of questions in these states: Delegated, Incomplete, Incomplete delegated.



Web Application Firewall

- In WAF, you can now upgrade WAF Cluster - Scanner Appliances directly from the WAF Appliances > WAF Clusters page.
- In WAF, the "Save As" and "Add to Sites" quick actions are now available for HTTP profiles, Healthcheck, SSL Certificates, and Web Server profiles.
- Now an error banner is not shown when a user edits a web application with an SSL profile that is out of the user's scope.



Web Application Scanning

- The 'Default Download Format' setting now populates the correct report format as per the configured User's settings.
- We now display correct start date and the time zone (as configured in global time zone) when a user views/edits a scheduled scan.
- We have updated the online help to include information related to WAS permissions.
- We have rectified the UI text for Burp Log File in Web Application panel for better readability.
- The start date configured by the user during scheduled scan is now correctly displayed in the Review panel of the scheduled scan configuration.
- We have revised the error message for JSON request of all APIs to display the correct set of operators being supported for the requested action in Asset Management (AM) and Web Application Scanning (WAS) modules.