



Qualys Cloud Suite 2.18

We're excited to tell you about new features and improvements coming with Qualys Cloud Suite 2.18.



AssetView



ThreatPROTECT

[View Real-time Threat Indicators \(RTI\) in Asset Details](#)
[New Support for Group by DNS Address](#)
[Add Trending to your Dashboard widgets](#)



Security Assessment Questionnaire

[CSV Reports Now Available](#)
[Ability to Delete Users](#)



Web Application Scanning



Web Application Firewall

[WAS now reports vulnerabilities blocked by WAF](#)



Administration

[User Management - Assigning Modules made easy](#)

Qualys Cloud Suite Update 2.18 brings you many more
Improvements and updates! [Learn more](#)



AssetView



ThreatPROTECT

View Real-time Threat Indicators (RTI) in Asset Details

With ThreatPROTECT you can now view all the Real-time Threat Indicators (RTI) for an asset and number of vulnerabilities associated with each RTI in one location.

Simply navigate to Assets tab, select an asset and click View Asset Details. Locate the ThreatPROTECT RTIs tab to view all the RTIs and associated vulnerabilities for that asset. The ThreatPROTECT RTIs tab is shown when the ThreatPROTECT module is enabled for your subscription.

ThreatPROTECT Summary

The Real-Time Threat Indicators for this Asset are displayed below. Click an indicator to view the vulnerabilities associated with each RTI.

Zero Day	Public Exploit	Easily Exploitable	Vulnerable to DOS
1	165	149	313
Exploit Kit Available	Malware	High Data Loss	High Lateral Movement
0	33	302	297
Unpatchable	Active Attacks		
49	55		

Close

New Support for Group by DNS Address

You can now group your asset search results by DNS address. It's easy to do. Enter your asset search query, then choose DNS Address from the "Group assets by..." drop-down. We'll group the results by unique DNS address and show you the number of assets that match each one. In the example below there is 1 asset for 10.0.100.11 and 1 asset for 10.0.100.10. (The other assets that match the search query do not have a DNS address.)

The screenshot shows the Qualys Enterprise AssetView interface. A search query "operatingSystem: windows" has been entered, resulting in 12 assets. The "Group assets by..." dropdown menu is set to "DNS Address". The results are displayed in a table with two columns: "DNS Address" and "Assets".

DNS Address	Assets
10.0.100.11	1
10.0.100.10	1

A red arrow points from the text "Group by DNS Address" to the "DNS Address" dropdown menu.

You can also use this new Group By option when configuring a dashboard widget. Enter your search query for the widget and then choose the Group By option "interfaces.dnsAddress".

The screenshot shows the "Edit Dynamic Widget" dialog box. The "Widget Title" is "NewDash". The "Query" is "operatingSystem: windows". The "Group assets" radio button is selected. The "Columns / Group By" dropdown menu is set to "interfaces.dnsAddress". The "Limit to" dropdown menu is set to "TOP 50".

A red arrow points from the text "Group by DNS Address" to the "Columns / Group By" dropdown menu.

Name	Asset Dns Address Dns ...	Count
TESTING	10.0.100.10	1
Cloud Agent	10.0.100.10	1
Cloud Agent	10.0.100.11	1
Business Unit	10.0.100.11	1
Business Unit	10.0.100.10	1
TESTING	10.0.100.11	1

Add Trending to your Dashboard widgets

Now you can configure dashboard count widgets to display trend data for up to 90 days. You'll see the new "Collect trend data" option in the dynamic widget wizard.

Edit Dynamic Widget

Select data for your stats using the form below (*) REQUIRED FIELDS

Customize the way that your widget looks

01 Count Table Bars Pie

Widget Title*
Assets with Vulns Actively Exploited in the wild

Query
vulnerabilities.vulnerability.threatIntel.activeAttacks:true

Comparison
☒ Compare with another reference query
Query

Comparison label
All Assets

This set of assets represents *
A superset (contains all the assets from initial query)

Trending
☒ Collect trend data **New option**
This widget will store its results each day for up to 90 days. The results will be plotted on a graph so that the data may be analyzed to identify trends.

Cancel Save

730
vs All Assets
865 (84.39%)
▼ -2.1%
Showing last 81 days

1.50K
1.00K
500
7/25 Today

Add conditional formatting...

Set the base color to

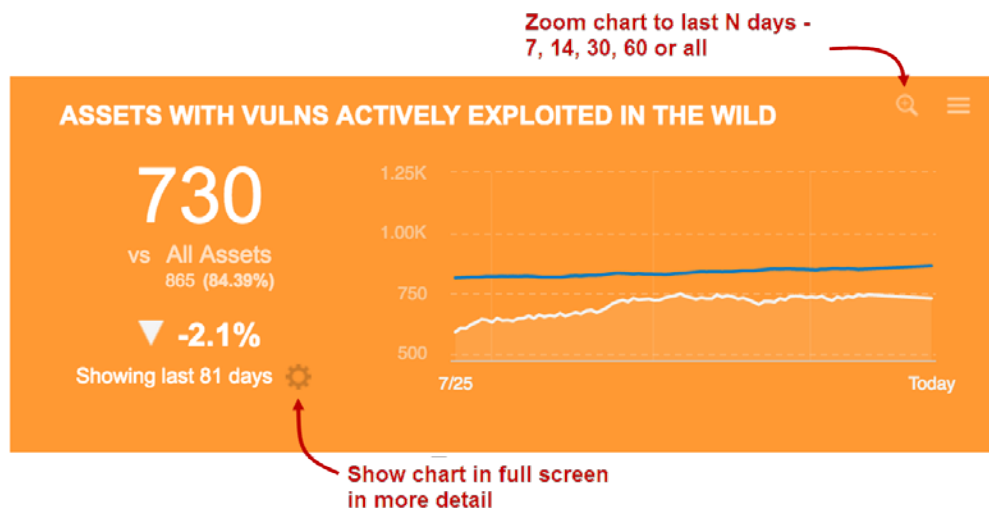
When the value of the comparison percentage is more than 10% then highlight in

When the value of the comparison percentage is more than 25% then highlight in

When the value of the comparison percentage is more than 90% then highlight in

When clicked, then navigate to the targeted vulnerabilities

When checked, widget trend data is collected daily and stored for up to 90 days. This is used to plot a line graph in the count widget.



CSV Reports Now Available

CSV format is now available for all report types – Single Instance Report, Aggregate Template Report and Campaign Report. Simply choose Comma-Separated Value (CSV) under Report Options when walking through the Questionnaire Report Creation wizard.

Questionnaire Report Creation Turn help tips: On | Off

Step 3 of 3

Select Report Options

Report options (*) REQUIRED FIELDS

Enter Report Name*
Single Instance Report

Select a file format for the report download*

- Web Archive (HTML)
- Compressed HTML pages (ZIP)
- Web Archive (HTML)
- Portable Document Format (PDF)
- Microsoft PowerPoint Document (PPT)
- Comma-Separated Value (CSV)**

☒ Show assets

☒ Show answered by and delegate names

☒ Show assignment

Cancel Previous Finish

Choose the CSV file format

You'll see  next to CSV reports in your reports list. Choose Download from the Quick Actions menu to view your report.

Reports

Search for reports by entering properties...

Actions (0) New Report

1 - 4 of 4

Report Title	Format	Type	Status	Generation Date	Owner
Single Instance Report		Single Instance Report	Complete	a few seconds ago	Patrick Skinner (quays_ps)
Aggregate Template Report		Aggregate Templates Re...	Complete	10 hours ago	Patrick Skinner (quays_ps)
Single Instance Report		Single Instance Report	Complete	12 hours ago	Patrick Skinner (quays_ps)
Single Instance Report		Single Instance Report	Complete	19 hours ago	Patrick Skinner (quays_ps)

Indicates CSV Format

Sample CSV Reports

Single Instance Report

```
"Single Instance Report ","2016-10-28T21:12:44Z"
"Qualys, Inc.,""1600 Bridge Parkway","Redwood
City","California","94065","United States of America"
"Patrick Slimmer","quays_ps",""
"TARGET"
"FILTERS"
"SUMMARY"
"Report Settings"
"Title","Type","Source","Current State","Stage","Tags","Created By","Assigned
To","Reviewer","Approver"
"3rd Party Assessment - jason.kim@qualys","Single Questionnaire
instance","Third Party Maturity Assessment for Information Security
Management v1","Information Gathering","2-Stage","","Patrick
Slimmer(quays_ps)","Jason Kim(jason.kim@qualys,)"
"Discovery"
"Due Date","Assigned Date","Questionnaire Status"
"30 Nov 2016","28 Oct 2016","In Progress"
"Questionnaire Overview"
"Answered","Not Answered"
"71","19"
"Questionnaire List"
"Section","Question Type","Question
Id","Question","Options","Answer","Answered By","Answer Date","Delegate
To","Attachments","Assets","Comments","Reviewed By","Review Date","Review
State"
"01 Security Policy (SP)","MultipleChoiceQuestion","SP-01","Is there a
Security Policy defined at the Corporate level?","Partially (Manual), No,
N/A, Yes","Partially (Manual)","Jason Kim(jason.kim@qualys,)", "28 Oct
2016","","","","","","","",
...
```

Aggregate Template Report

```
"Aggregate Template Report ","2016-10-28T21:16:52Z"
"Qualys, Inc.,""1600 Bridge Parkway","Redwood
City","California","94065","United States of America"
"Patrick Slimmer","quays_ps",""
"TARGET"
"FILTERS"
"SUMMARY"
"Report Setting"
"Type","Source","State","Tags","Due Date","Last Update","Created
Date","Created By","Delegated To","Assigned To"
"Aggregate Template Questionnaire","Third Party Maturity Assessment for
Information Security Management","All states","","",""
"Questionnaires"
"Total","In Progress","Reaching Due Date","Overdue"
"1","0","0","0"
"Stages"
"Closed","1"
"Questionnaire Instances"
"Title","Assigned to","Assigned Date","Last modified","Due Date","State"
"Third Party - jason.kim@qualys","Jason Kim(jason.kim@qualys,)", "28 Oct
2016","28 Oct 2016","30 Nov 2016","Closed"
```

```

"Questionnaire List"
"01 Security Policy (SP)"
"Question Id","Question","Question Type"
"SP-01","Is there a Security Policy defined at the Corporate
level?","MultipleChoiceQuestion"
"Selected Answer","Answer Count","Answered By"
"Partially (Manual)","0",""
"No","1","Patrick Slimmer(quays_ps)"
"N/A","0",""
"Yes","0",""
"Not Answered","0",""
...

```

Campaign Report

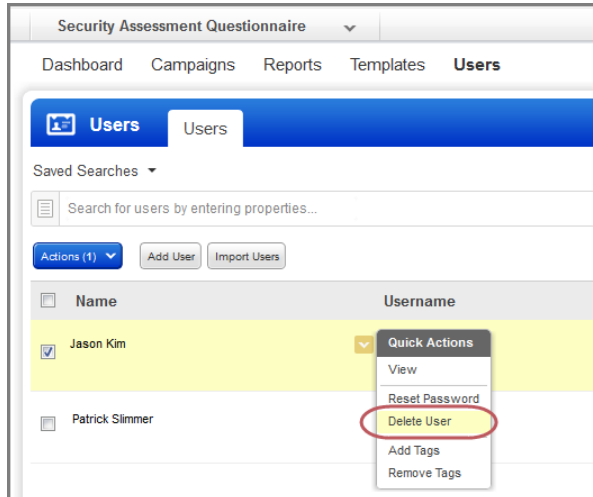
```

"Campaign Report ","2016-10-28T21:14:14Z"
"Qualys, Inc.,""1600 Bridge Parkway","Redwood
City","California","94065","United States of America"
"Patrick Slimmer","quays_ps",""
"TARGET"
"FILTERS"
"SUMMARY"
"Report Setting"
"Title","Type","Source","Stage"
"3rd Party Assessment","Campaign","Third Party Maturity Assessment for
Information Security Management","2-Stage"
"Questionnaires"
"Total","In Progress","Reaching Due Date","Overdue"
"1","1","0","0"
"Stages"
"Information Gathering","1"
"Questionnaire Instances"
"Title","Assigned To","Assigned Date","Last Modified","Due Date","State"
"3rd Party Assessment - jason.kim@qualys,","Jason Kim(jason.kim@qualys,),"28
Oct 2016","28 Oct 2016","30 Nov 2016","Information Gathering"
"Questionnaire List"
"01 Security Policy (SP)"
"Question Id","Question","Question Type"
"SP-01","Is there a Security Policy defined at the Corporate
level?","MultipleChoiceQuestion"
"Selected Answer","Answer Count","Answered By"
"Partially (Manual)","1","Jason Kim(jason.kim@qualys,)"
"No","0",""
"N/A","0",""
"Yes","0",""
"Not Answered","0",""
...

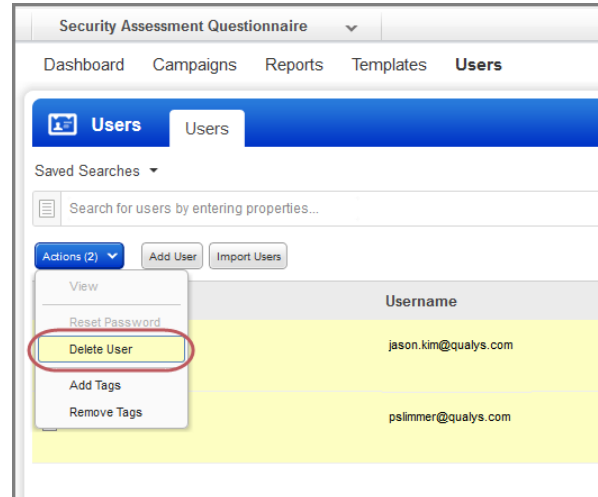
```

Ability to Delete Users

You can now delete a user from SAQ as long as the user is not assigned to an active campaign. To delete a single user, choose Delete from the Quick Actions menu. To delete multiple users in bulk, select the users in the list and choose Delete from the Actions menu above the list.



Delete single user



Delete multiple users



Web Application Scanning



Web Application Firewall

WAS now reports vulnerabilities blocked by WAF

WAS detections and reports now display vulnerabilities blocked by Qualys WAF, for a Web Application that is a shared asset in WAS and WAF. To get started enable the ScanTrust option to allow Qualys scanners to seamlessly scan the web application through the WAF and enhance assessment and reporting. You can easily set this up in WAS or WAF.

Note that the ScanTrust feature should be enabled in your Qualys subscription before you can use it. Once enabled, the ScanTrust option is visible in WAS if the web application is protected by WAF.

Interested in getting ScanTrust enabled for your subscription? Please contact Qualys Support or Technical Account Manager.

WAS module

The screenshot shows the 'Web Application Edit: Demo Web App' interface. On the left is a sidebar with 'Edit Mode' and various settings categories: Asset Details, Application Details, Scan Settings (selected), DNS Override, Crawl Settings, Redundant Links, Authentication, Crawl Exclusion Lists, and Malware Monitoring. The main content area is titled 'Tell us the scan settings you'd like to use'. It contains sections for 'Default Scan Options' (with a red note '(*) REQUIRED FIELDS'), 'ScanTrust', and 'Duration'. In the 'ScanTrust' section, there is a checkbox labeled 'Enable Authentication with WAF to improve scan capacities.' which is checked and circled in red. At the bottom are 'Cancel', 'Save As..', and 'Save' buttons.

WAF module

Web Application Edit: Demo Web App Turn help tips: On | Off Launch help

Edit Mode

- Asset Details
- Network
- SSL Support
- Policies**
- Access Control
- WAF Clusters
- Comments
- Action log

Configure policies for your web application

Security Policy (*) REQUIRED FIELDS

Select the combination of security rules and heuristics that protect the origin server.

Policy* Block threshold(95) Edit

Non-Blocking mode

☐ Do not allow policy to block

ScanTrust

By enabling this option, you permit Qualys scanners to seamlessly scan the application through the WAF, and enhance assessment and reporting by distinguishing vulnerabilities not yet fixed but blocked by the firewall.

☒ Allow Qualys scanners to conduct scans on this web application.

Cancel Save

Once you allow Qualys scanners to perform these scans, be sure to select the Enable Authentication option when launching your vulnerability scan in WAS.

Launch New WAS Vulnerability Scan Turn help tips: On | Off Launch help

Step 2 of 3

- 1 Scan Details
- 2 Scan Settings**
- 3 Review And Confirm

Configure settings for your scan

ScanTrust (*) REQUIRED FIELDS

This allows for Qualys WAS and WAF to work in concert to complete the scan.

☒ Enable Authentication with WAF to improve scan capacities. Be sure to select this

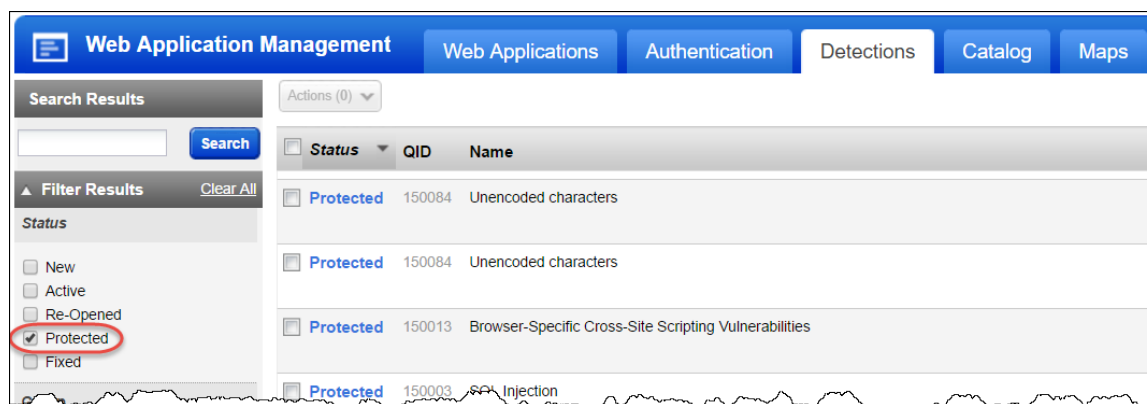
Option Profile

Select an option profile with various scanning options. You can set to Default if a default profile is defined for this web application.

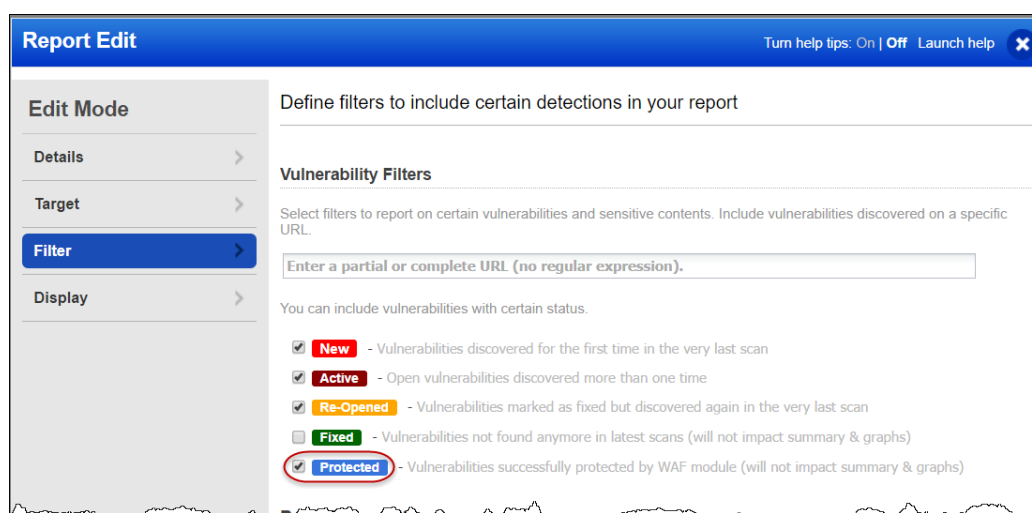
Option Profile* Default [Initial WAS Options] View Create

Cancel Save

In WAS detections, use the Protected filter to view the vulnerabilities blocked by Qualys WAF.



Enable the Protected filter in WAS reports to view the vulnerabilities blocked by Qualys WAF.





Administration

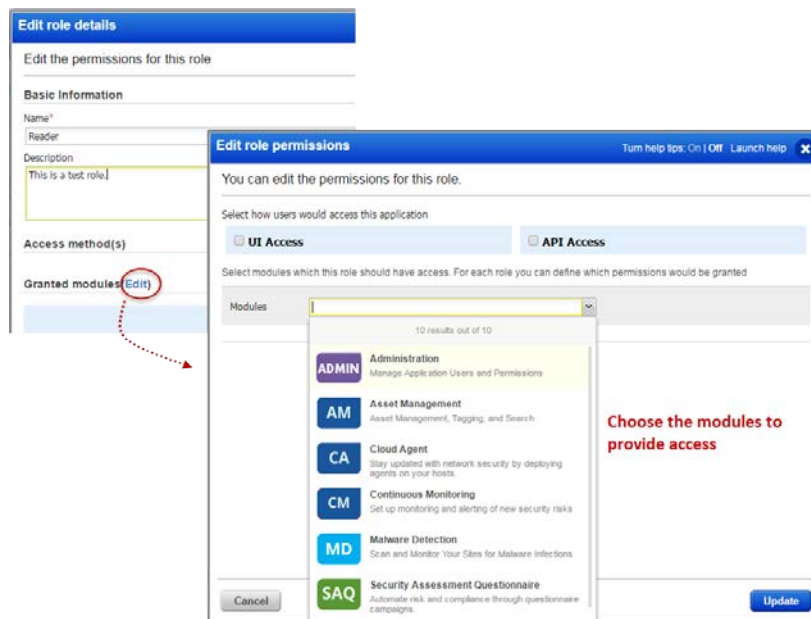
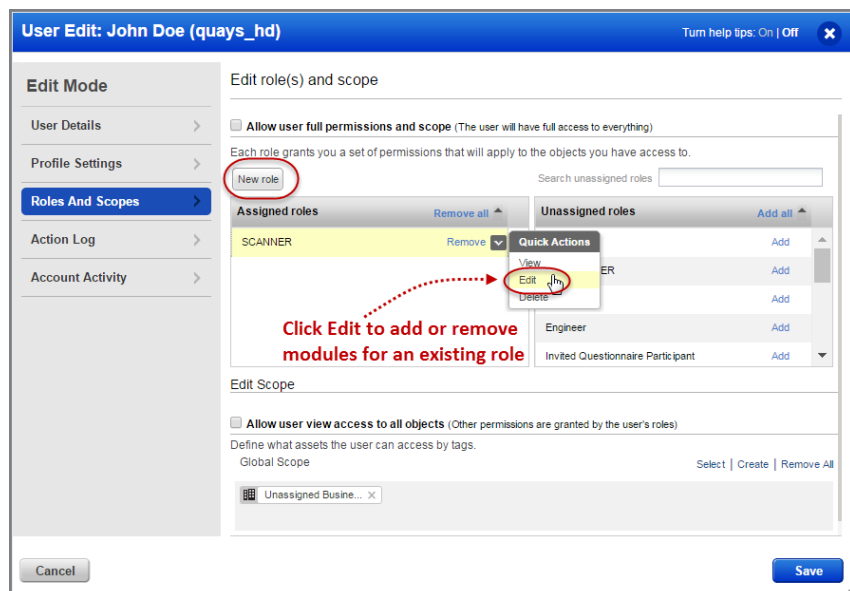
User Management - Assigning Modules made easy

We've added Module Access Permissions to help you better manage users and their access to modules in your subscription.

Assigning Modules

Now you can assign modules to roles, to grant users access to modules in your subscription.

You can either edit an existing role or create a new role.



Choose from modules you have access to in to your subscription. For example if you have VM, PC, WAS, CM, CA, AV, TP then you can choose to add access permissions for these modules.

Filter By Module

All the modules assigned to your role are displayed for module filter.

Select the module and we will list all the users assigned to the module.

You can select multiple modules at one go.

The screenshot shows the 'User Management' interface. On the left, a dropdown menu for 'Module' is open, displaying a list of modules: Web Application Firewall, Vulnerability Management, Policy Compliance, Web Application Scanning, Malware Detection, Asset Management, Administration, Security Assessment, Continuous Monitoring, Cloud Agent, and ThreatPROTECT. A red arrow points to the 'Asset Management' module, with a red text label 'New Filter to simplify Module selection'. On the right, a list of modules is shown, with a red arrow pointing to the 'Asset Management' module, with a red text label 'Pick one or more modules'. The 'Total active users' bar chart shows 100%.

Modules assigned to each user

The new module column tells us the modules available to each user as per the assigned role.

The screenshot shows the 'User Management' interface. A table lists users with columns: Username, Modules, First Name, Last Name, Email Address, Last Update Date, and Last Login Date. The 'Modules' column shows a list of modules assigned to each user. A red arrow points to the 'Modules' column, with a red text label 'Quick view of modules assigned to each user'. The 'Total active users' bar chart shows 100%.

Issues Addressed

AV

TP

- When the user selects the Group by option in the assets list, the Assets column is now sorted in descending order by default (from largest number of assets to lowest).
- Fix to correct tag scope after adding a new tag. The user will now be able to remove a newly added tag without having to refresh the UI. Also a user cannot remove an asset group tag if an asset in that asset group also has that tag.
- The AssetView tags list now provides a checkbox in the header to select/deselect all tags at once for bulk actions.
- When the user enters the token "vulnerabilities.vulnerability.category" they are now presented with a pre-filled drop down listing of vulnerability category names from the Knowledgebase to choose from.
- Now users can easily search for assets with vulnerabilities found using the "vulnerabilities" token. Just enter the token name and select * from the drop-down listing: vulnerabilities: "*". For assets with no vulnerabilities: not vulnerabilities: "*"
- Fixed the geolocation map to display only the country, instead of "null", in cases where no city is available.
- Users can now download the complete list of assets without any discrepancies.
- Now the Please wait.. message will disappear as expected after the user downloads the assets list and chooses the format Compressed HTML pages (ZIP).
- ThreatPROTECT: When an existing widget is edited to enable trending, it will automatically be resized to 300px high if height is less than 300px.
- ThreatPROTECT: Updated the tooltip for chart widgets configured for AV and TP dashboards. If the tooltip text exceeds the chart's width, it is truncated and shown with ellipsis.

CA

- Fixed an issue where View Asset Details showed no services on the System Information tab for certain agents. Services are now correctly listed for all agents.
- When editing an activation key, a new option lets you "Apply changes to all existing agents". When selected we'll apply changes including tags, licenses and limits.
- We've added a help tip for the Revocation Interval performance setting in the Configuration Profile.

SAQ

- Add new category called "Shared Assessment" in the templates section with new templates: Shared Assessment SIG Lite 2016 and Shared Assessment VRMMM 2016.
- Fixed issue where campaign create and edit actions sometimes returned error messages when no error occurred.
- Improvements made to delete user confirmation window to help the user understand the impact of this action.
- We've made updates to ensure once a user is deleted, the user no longer appears in the UI.
- There was an issue while adding an invitee to a campaign after a campaign was created. Now the issue is resolved and you can successfully add invitees to a campaign.
- Fixed issues with content of Cloud Security Alliance CAIQ template.

WAS

- Scans that error out due to scan configuration error no longer return an internal error. For example if a scan exceeds the cancel time limit it now returns QID 150024 - Web Application Scan Time Limit Reached and not QID 150025.
- When editing a scheduled report with the Activate Notification option disabled, the user would not be able to create a new distribution group or edit an existing one.

Asset Management API

- Valid operators added in error message for Asset Management API when request includes invalid operator.