



Qualys Cloud Platform v2.x

Release Notes

Version 2.36

January 29, 2019 (Updated February 6, 2019)

Here's what's new in Qualys Cloud Suite 2.36!

AV

AssetView

TP

Threat Protection

[New Azure Cloud Dashboard](#)
[Purge/Uninstall Cloud Assets and Cloud Agents \(BETA\)](#)

WAS

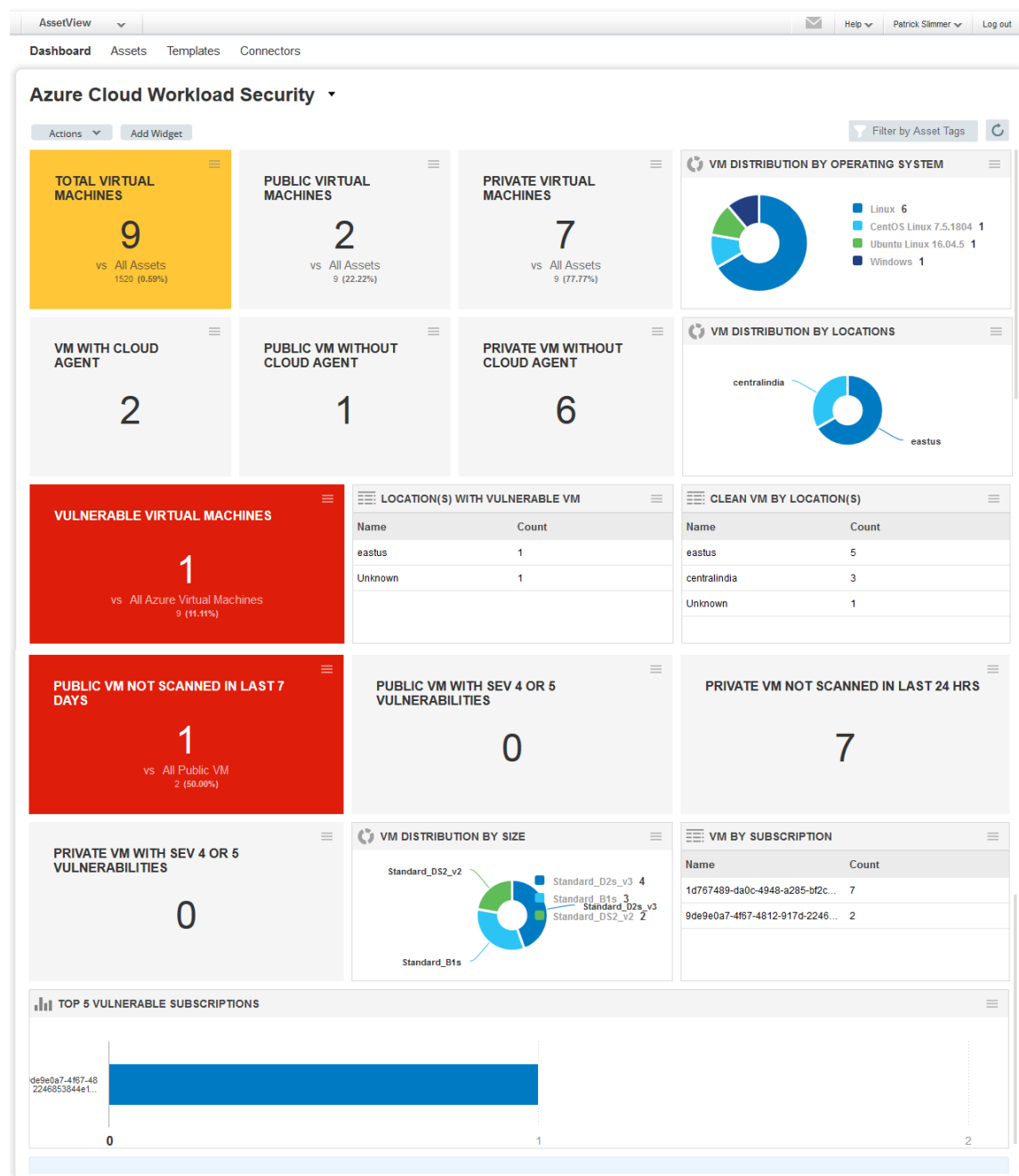
Web Application Scanning

[Improved Severity Mapping for Burp Issues](#)

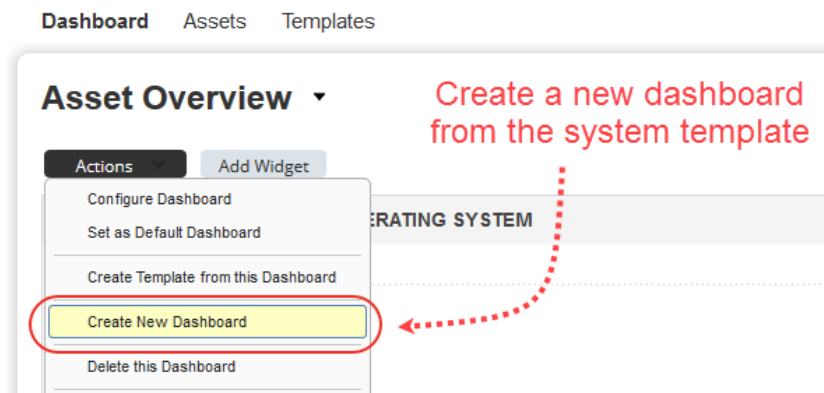
Qualys Cloud Platform 2.36 brings you many more Improvements and updates! [Learn more](#)

New Azure Cloud Dashboard

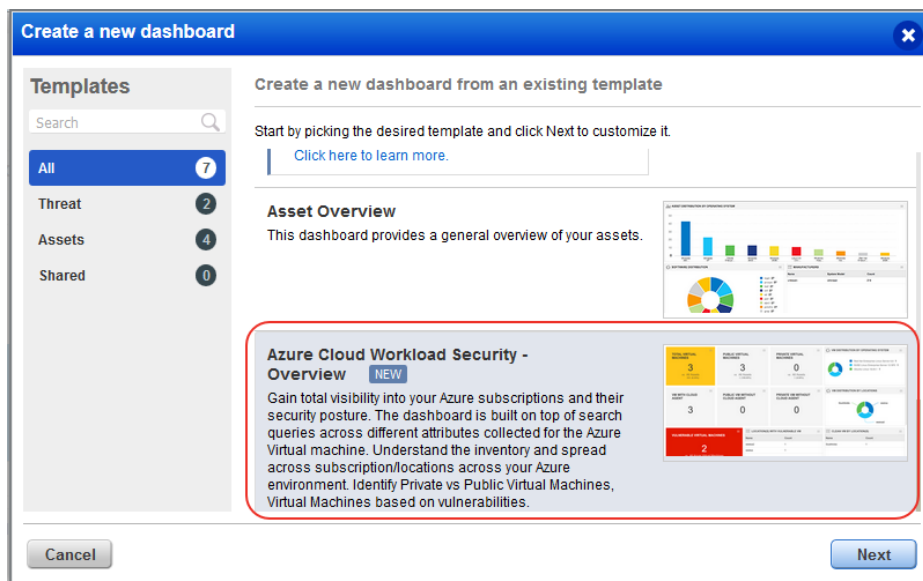
A new dashboard template is available for visualizing your Azure cloud data: Azure Cloud Workload Security – Overview. Check out this sample dashboard.



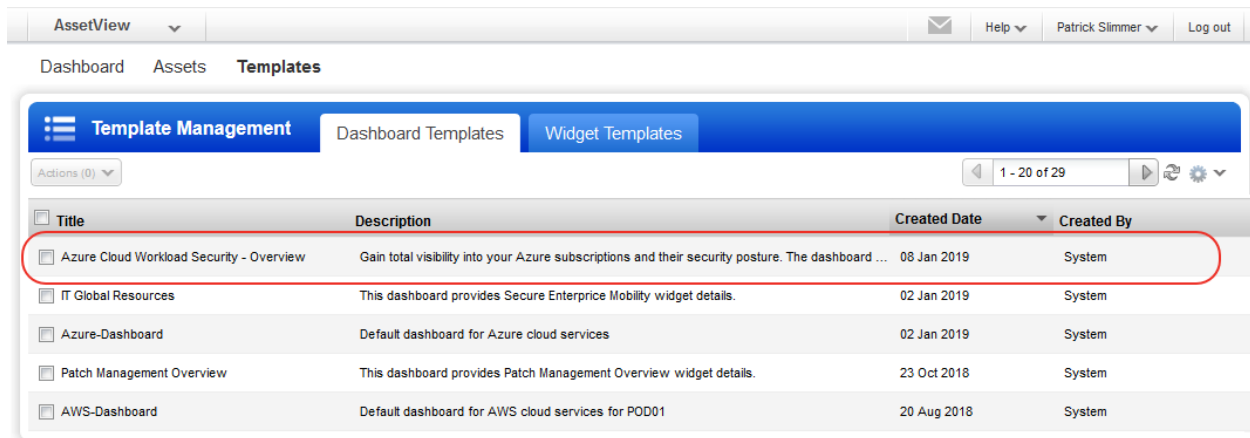
To create your own dashboard using this template, choose Actions > Create New Dashboard.



Find the template in the list, select it and click Next. Give your dashboard a name and hit Create. That's it! Your dashboard will be created.



The new template also appears on the Dashboard Templates list.



Purge/Uninstall Cloud Assets and Cloud Agents (BETA)

This release introduces the ability to purge/uninstall cloud assets and cloud agents. Define purge rules to automatically purge assets and cloud agents based on the terminated/deallocated state of the cloud instance or time since last activity or vulnerability scan.

Pre-requisites

1) This is a preview release of the feature. Only some select customers will have access to this and in the next cycle, it will be opened to all. To request this feature, please reach out to Qualys Support or your Technical Account Manager to have one or both of these capabilities enabled:

- On Demand Purge
- Rule-based Purge

2) To purge assets or manage purge rules, you must have all Asset Management permissions: Manage Asset Data Connectors, Create Asset, Delete Asset, Read Asset and Update Asset.

What assets can you purge?

When enabled for your subscription, you can purge these types of assets:

- EC2 assets discovered by AWS connectors
- Cloud agent assets

What happens when you purge an asset?

- Asset will be removed from your account
- Existing asset data will be removed from your account
- Scan results from scanners will remain on your account
- If an asset has a cloud agent, the agent will be uninstalled and its license freed up

On Demand Purge

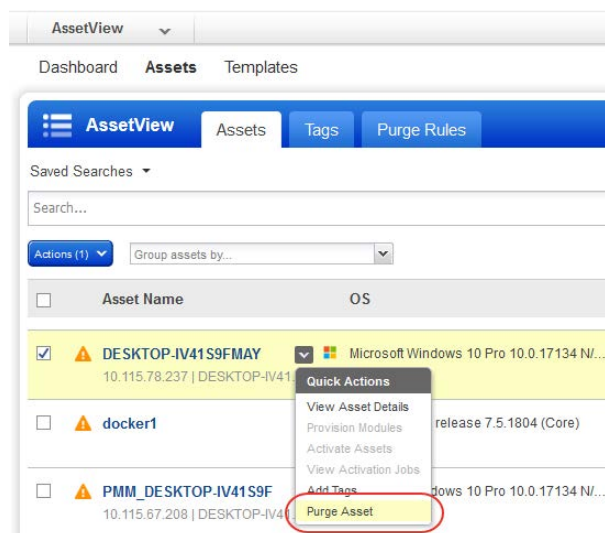
From your Assets list, first identify the EC2 asset or cloud agent asset you want to remove from your subscription. The Sources column provides indicators to help you identify these assets.



Identifies EC2 assets from AWS connectors

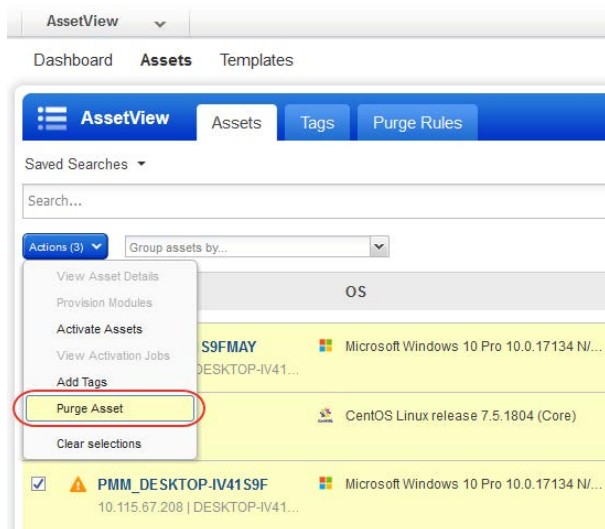


Identifies cloud agent assets



Select the asset in your list to purge and choose Purge Asset from the Quick Actions menu.

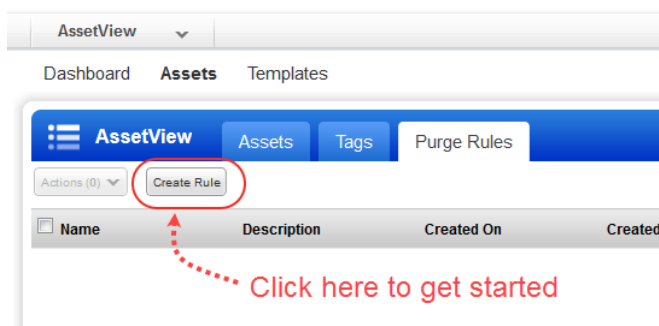
If this option is disabled that means the asset cannot be purged because it isn't an EC2 asset or a cloud agent asset.



Optionally, select multiple assets (up to 100) and choose Purge Asset from the Actions menu above the data list. All selected assets will be purged once you confirm the action.

Rule-based Purge

Create rules to automate the purging of assets. Go to Assets > Purge Rules and click Create Rule.



You'll start by giving the rule a friendly name and description.

 The screenshot shows the 'Purge Rule Creation' dialog box, Step 1 of 4: Rule Details. The dialog has a sidebar with steps: 1 Rule Details (selected), 2 Rule Definition, 3 Purge Limits, and 4 Review And Confirm. The main area contains the following text:

Rule Details

Define a purge rule to automate the removal of Cloud Provider assets (AWS) and Cloud Agent(*) REQUIRED FIELDS assets (AWS, Azure, GCP) from your subscription. Purge rules run daily.

Name*
my purge rule

Description
example: My Rule Description

Buttons: Cancel, Continue

Then add criteria to define the rule conditions.

Purge Rule Creation

Step 2 of 4

- 1 Rule Details ✓
- 2 Rule Definition
- 3 Purge Limits
- 4 Review And Confirm

Rule Definition

Add criteria to permanently remove cloud based assets (*) REQUIRED FIELDS

All matching assets will be purged

Add Criteria ▼

- Cloud Provider Metadata Based Filter
- Cloud Agent Based Filter

Cancel **Previous** **Continue**

Select Cloud Agent Based Filter to remove cloud agent assets based on criteria like when the agent last checked in to the platform, modules activated for the agent, agent version, and more.

Select Cloud Provider Metadata Based Filter to remove cloud assets and cloud agents based on cloud provider metadata. You'll first choose AWS, Azure or GCP, then select the metadata that defines the assets you want to purge. In this example, the rule will remove EC2 assets that are terminated.

Purge Rule Creation

Step 2 of 4

- 1 Rule Details ✓
- 2 Rule Definition
- 3 Purge Limits
- 4 Review And Confirm

Rule Definition

Add criteria to permanently remove cloud based assets (*) REQUIRED FIELDS

All matching assets will be purged

ONLY IF **Remove**

Cloud Provider Metadata Based Filter

Select a cloud provider and choose rule criteria.

Assets match **Any** of the following conditions for **AWS**

aws.ec2.instanceState **IN** **TERMINATED**

☐ Purge cloud agent assets matching criteria

When selected, we'll remove the asset, the cloud agent and its license from your subscription.

Add Criteria ▼

Cancel **Previous** **Continue**

Select the option “Purge cloud agent assets matching criteria” to also remove the cloud agent and its license for matching assets.

Click Add Criteria again to add more criteria to the rule, including time-based criteria.

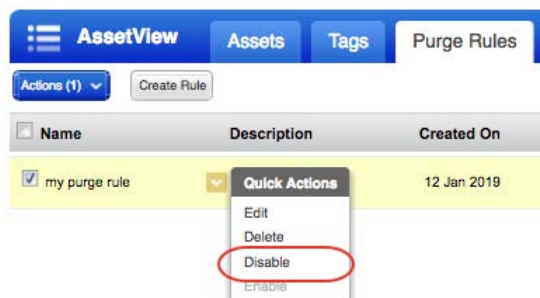
The screenshot shows the 'Purge Rule Creation' dialog box, specifically Step 2 of 4: Rule Definition. On the left, a progress bar indicates the steps: 1 Rule Details (checked), 2 Rule Definition (active), 3 Purge Limits (checked), and 4 Review And Confirm. The main area is titled 'Rule Definition' and contains a section 'ONLY IF' with a 'Remove' link. Below this is a 'Cloud Provider Metadata Based Filter' section with the instruction 'Select a cloud provider and choose rule criteria.' It shows 'Assets match Any' of the following conditions for 'AWS'. A specific condition is defined: 'aws.ec2.instanceState' is 'IN' 'TERMINATED'. There is a checkbox for 'Purge cloud agent assets matching criteria' with a note: 'When selected, we'll remove the asset, the cloud agent and its license from your subscription.' At the bottom, there is an 'Add Criteria' button and two options: 'Time-based Criteria' and 'Cloud Agent Based Filter'. Navigation buttons 'Cancel', 'Previous', and 'Continue' are at the bottom.

Set an asset limit for the rule. If the number of matching assets exceeds the limit when the rule is executed, then no assets will be purged.

The screenshot shows the 'Purge Rule Creation' dialog box, specifically Step 3 of 4: Purge Limits. The progress bar on the left shows steps 1 Rule Details (checked), 2 Rule Definition (checked), 3 Purge Limits (active), and 4 Review And Confirm (checked). The main area is titled 'Purge Limits' and contains a section 'Set an asset limit for this rule' with a red note '(*) REQUIRED FIELDS'. The text reads: 'Do not purge assets when more than 10000 assets are returned'. Navigation buttons 'Cancel', 'Previous', and 'Continue' are at the bottom.

Review your settings on the last page and hit Finish. The rule will be saved to your purge rules list.

All of your purge rules run daily. If you don't want a rule to run then you can choose to disable it. Identify the rule in your list and choose Disable from the Quick Actions menu.













Improved Severity Mapping for Burp Issues

We have now improved the severity assignment in WAS for Burp issues. The severity in WAS is now assigned considering the two factors: Burp Severity and Burp Confidence.

The following table displays the various combinations of the Burp Severity and Burp Confidence and how they decide the severity in WAS.

Burp Severity	Burp Confidence	WAS Severity
High	Certain or Firm	Confirmed Severity 5: Urgent 
	Tentative	Potential Severity 5: Urgent 
Medium	Certain or Firm	Confirmed Severity 3: Serious 
	Tentative	Potential Severity 3: Serious 
Low	Certain or Firm	Confirmed Severity 2: Medium 
	Tentative	Potential Severity 2: Medium 
Information	Certain or Firm	Confirmed Severity 1: Minimal 
	Tentative	Potential Severity 1: Minimal 

Issues addressed in this release

Qualys Cloud Platform 2.36 brings you many more improvements and updates.

AV

AssetView

TP

Threat Protection

- Updated the "How to Search" topic in the Cloud Agent online help to mention that range search on non-numeric fields is not supported.
- Now the default dashboard displays properly for sub users with the role Reader.
- On dashboard widgets now the pie chart legend appears correctly when the sort order is Descending.
- We have updated the help to document that once a vulnerability is ignored it is not listed in the Asset Search. However, it is listed by default in the Asset View app and user can use a filter to hide the ignored vulnerability.
- Added 'DEALLOCATING' state as suggested value for azure.vm.state field, used for finding certain Azure instance state.
- Fixed an issue where a user was unable to access the Threat Protection app even though user permissions were set to allow access.

CA

Cloud Agent

- On Asset Details > Compliance User now the Last Scan date column shows the last evaluation date for each policy.
- Updated the Cloud Agent Windows Installation Guide for information about the hotfixes required for successful installation of the Cloud Agent on Windows.
- Fixed an issue where reordering, editing, or deleting Cloud Agent configuration profiles was taking more time than expected.

CM

Continuous Monitoring

- Now when the Manager who created a monitoring profile is deleted, the email alerts contain the name of the Manager who last updated the profile. In other words in a case where Manager James is deactivated if Manager Susan edits the profile and saves it without any change you'll see the name of Manager Susan in the email alerts.

MD

Malware Detection

- On the Schedules list, now you can click the Next Date column to sort schedule by next launch date.

CV**Cloud View**

- A new Azure dashboard template is available to configure an Azure dashboard in CloudView.

CS**Container Security**

- We have removed 2 widgets Top 10 container labels and Top 10 Image labels from dashboards.

SAQ**Security Assessment Questionnaire**

- The new template editor and Campaigns tab are now loading appropriately in the SAQ app.

WAF**Web Application Firewall**

- Display only "Web Application" and "Web Application Firewall" in Category filter drop-down of WAF KnowledgeBase.
- Now, when a user removes exception/VP/source web app, we change the rule type to CUSTOM for this rule and remove the "View Details" link from the rule view wizard.
- Support for sorting WAF Clusters by Upgrade Schedule is removed.
- We are now showing HSTS configuration in the Review and Confirm step while creating HTTP Profiles.
- The issue with saving a profile in edit mode using Save As button from Declarative Security is resolved.
- The issue with the geographic origin of the events not getting displayed in Event Details is resolved.