Qualys Cloud Suite 2.28.1

We’re happy to share information about our latest release Qualys Cloud Suite 2.28.1. Enhancements support our latest apps - File Integrity Monitoring (FIM) and Indication of Compromise (IOC) as well as Web Application Scanning (WAS).

CA Cloud Agent

Configure profile updates

WAS Web Application Scanning

Bugcrowd Integration

Enhancements to Detections

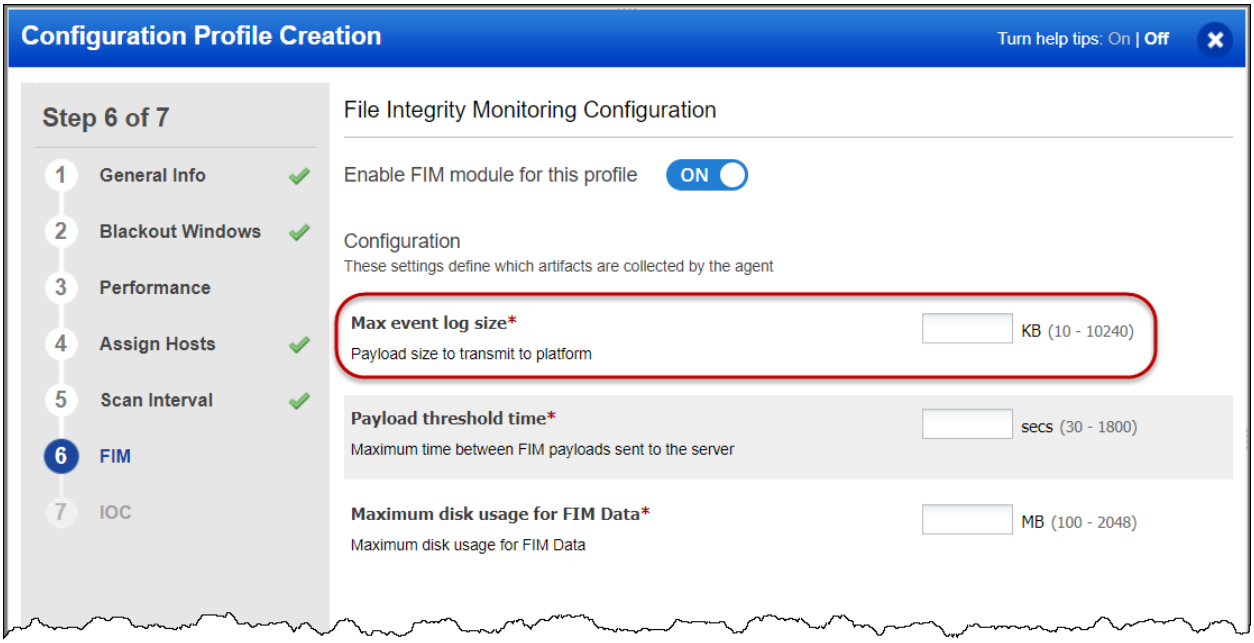
Qualys Cloud Suite 2.28.1 brings you many more Improvements and updates! Learn more

CA Cloud Agent

Configure profile updates

When FIM and/or IOC is enabled for your subscription the CA configuration profile has new sections. To enable FIM data collection set Enable FIM module option to On and to enable for IOC data collection set Enable IOC option to On. Default configuration settings are provided for each module.

You can set the maximum size of the FIM event log file stored on the cloud agent. Available values are between 10 KB to 10240 KB.



Once the event log file size reaches the maximum file size specified, the events get transmitted to the Qualys cloud platform and then the file is removed from the agent.

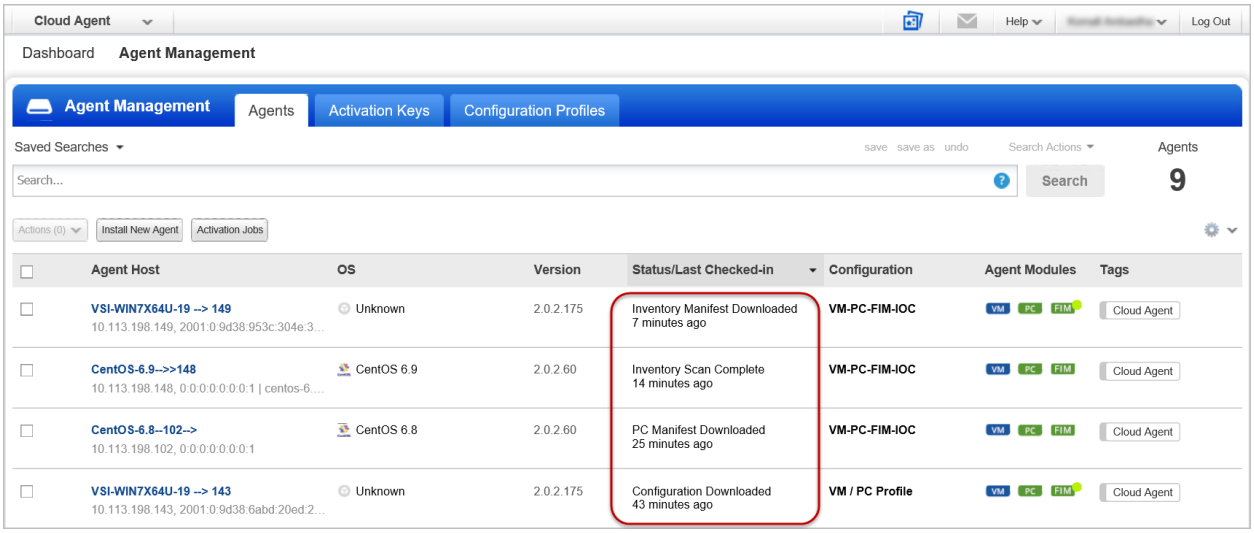
The events are transmitted to the Qualys Cloud platform when either of the following occurs:

- Payload threshold time is hit
- FIM event log file reaches the maximum specified size
- Disk usage for total FIM data on the agent reaches the maximum specified size

Enhanced manifest download status

For non-Windows agents, the status column in the cloud agents list now displays specific manifest download status, such as Inventory Manifest Downloaded for inventory, and the following status for scans:

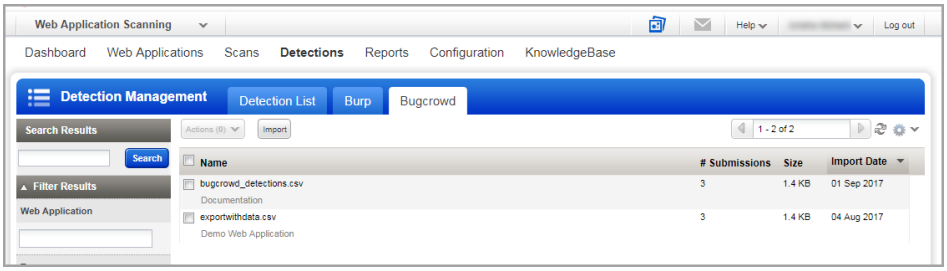
- VM Manifest Downloaded
- PC Manifest Downloaded
- FIM Manifest Downloaded
- IOC Manifest Downloaded



Bugcrowd Integration

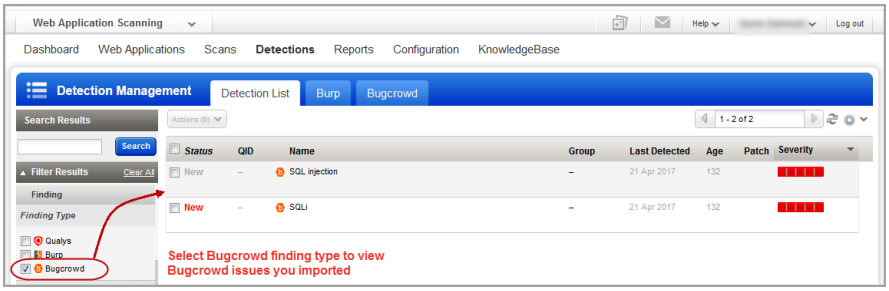
With this release of Qualys WAS, mutual customers of Qualys WAS and Bugcrowd can now bidirectionally import and export findings and vulnerabilities into each other's solutions portals. Our Bugcrowd Suite integration gives you a way to store the findings discovered by the Bugcrowd Suite scanner with those discovered by WAS and share this information with multiple users.

Go to Detections > Bugcrowd > Import. Choose a Bugcrowd file in CSV format from your local file system and select the web application that the Bugcrowd file applies to.



The issues imported with your Bugcrowd file are displayed in the issues list.

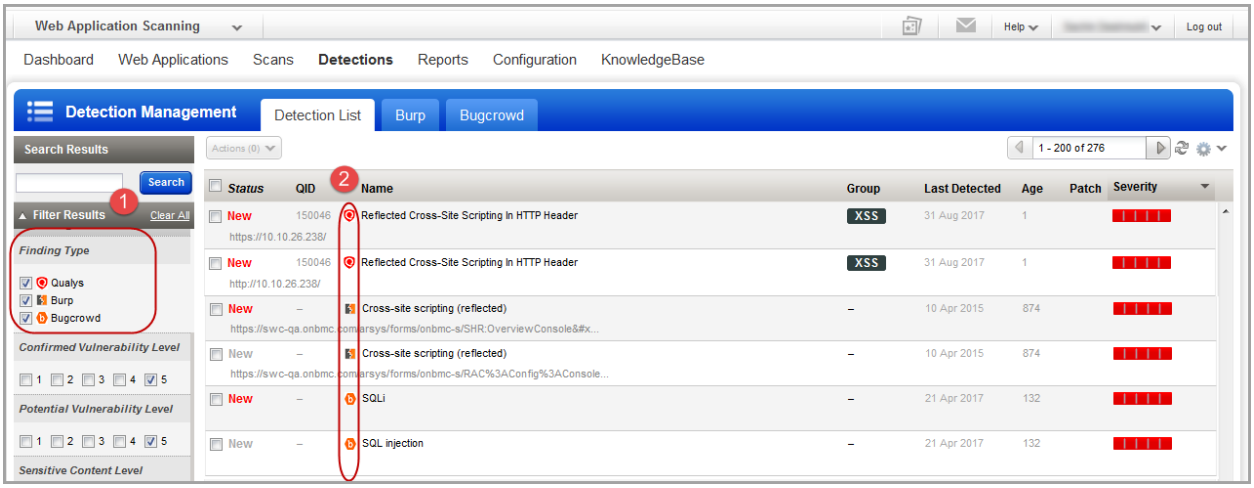
Go to Detections > Detections List. The Detection List displays security findings discovered by our cloud security service, Burp findings and Bugcrowd findings that you import.



In the Filter Results select Bugcrowd Finding Type and the list will display only Bugcrowd issues. You can view issues in detail - including detection dates, status and severity.

Enhancements to Detections

We have now upgraded Detections tab to a new dedicated top-level for a central area for application security vulnerability detections, management and information.



1 - **New** Filters

We have introduced new filters to enhance the search and quickly locate the detection type. In addition to the common filters, depending on your finding type, more filters specific to each finding type are displayed.

For example, if you choose Finding Type as Burp, then filters that are applicable for Burp related findings are enabled and the other non-applicable filters are disabled.

2 - New Icons

We now list all your findings (Qualys, Burp, and Bugcrowd) in the Detections tab. You can distinguish the finding type with the icon displayed in the list.

- Qualys detections
- Burp detections
- Bugcrowd detections

Issues addressed in this release

Cloud Agent (CA) - Fixed an issue where not all agents were uninstalled by a bulk uninstall action. Now when the user selects agents for a bulk uninstall action, all selected agents are uninstalled.

Cloud Agent (CA) - Certificate support for Cloud Agent on SUSE 11. The certificate file (.pem) must be installed manually in the proper location. We've updated the Cloud Agent Linux Installation Guide with instructions on how to do this.

Cloud Platform - Now users can choose all the EC2 configured regions for EC2 Scheduled Scans when EC2 scanning is enabled for the subscription.

Cloud Platform - Fixed an issue where an EC2 connector stopped functioning after one of the EC2 instances was shutdown.

Web Application Scanning (WAS) -We have now resolved the discrepancy in the count of vulnerabilities displayed on Dashboard and Detections tab. Now, the count of vulnerabilities (of all severities) displayed on dashboard is in sync with the count displayed in Detections tab.

Web Application Scanning (WAS) -We have now fixed an issue to correctly reflect the DNS override values in the Web Application view.