Qualys Cloud Suite 2.28.1

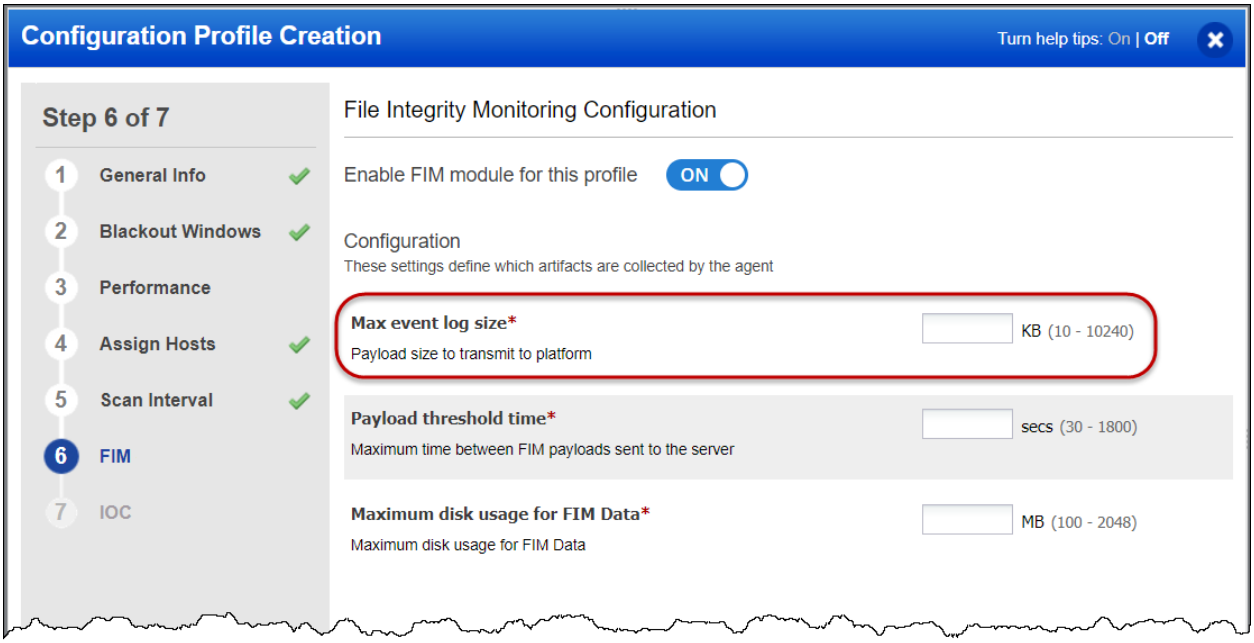
We're happy to share information about our latest release Qualys Cloud Suite 2.28.1. Enhancements support our latest apps - File Integrity Monitoring (FIM) and Indication of Compromise (IOC).

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.

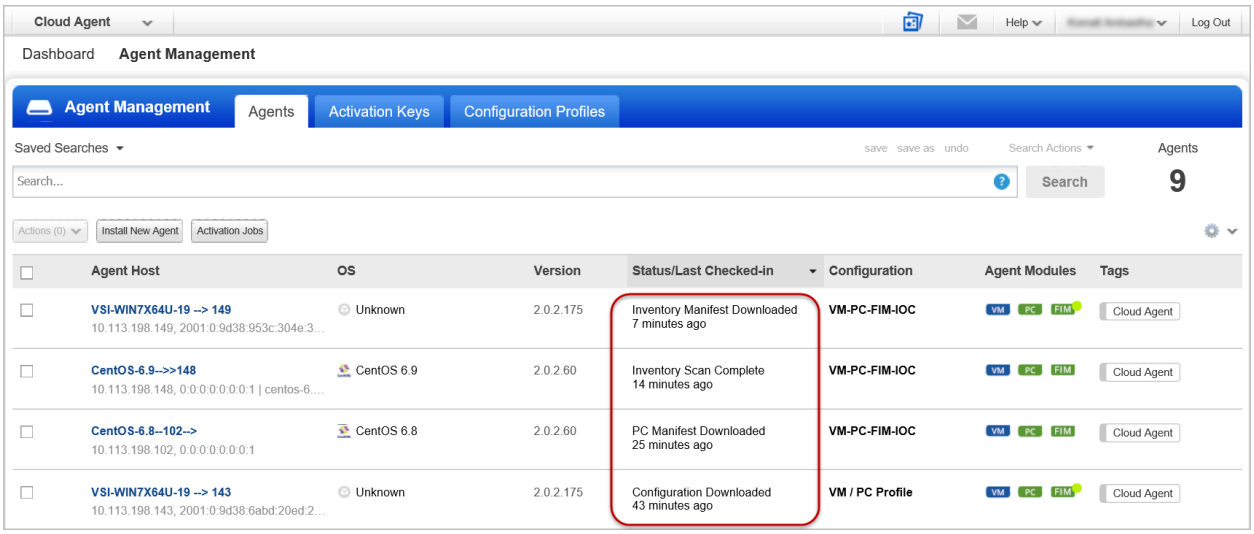
The events are transmitted to the Qualys Cloud platform when either of the following occurs:

- 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



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.