



Qualys Cloud Agent Windows 4.8.0

June 2022

We're excited to tell you about new features, improvements, platform coverage changes, and fixes in this Cloud Agent release. These updates are specific to the agent binary. Platform updates for new features and fixes of management, syncing, tagging, and reporting capabilities of Cloud Agents are documented in the Cloud Platform and Cloud Suite release notes.

Enhancements

- Patch Management
 - Added support to uninstall specific software from an asset using the Uninstall Software action as a pre or post-Patch deployment job. This can be done by retrieving the uninstall string from the registry and executing the uninstall action based on configuration.
 - Improved Agent logging: Logging for patch management has been improved to make the logs readable and provide clear visibility of patch job workflow at a single location. A separate log file - `PatchLog.txt` will be created for the Patch Management module at the `%ProgramData%Qualys\QualysAgent` location.
 - Changed Patch script timeout to 3 hours as a default timeout.
- Custom Assessment and Remediation (CAR)
 - Windows Agent now supports the execution of VB Scripts in addition to the Python and Powershell scripts through CAR.
- File Integrity Monitoring (FIM)
 - File Integrity Monitor now provides old and new file hash (SHA256) as a part of Content Change Tracking.
 - In content change tracking, file content change due to the reduction in size will be reported as a change event.
- Endpoint Detection and Response (EDR)/ Endpoint Protection Products (EPP)
 - Added support for deletion of events for non-Portable Executable (non-PE) files.
 - Agent leverages the Antimalware Scan Interface of Windows to improve attack-detection capabilities.
 - Agent is enhanced to detect other Security Products installed on the asset so that Qualys EPP will not be enabled and potential interoperability issues can be avoided.
 - Quarantined files can be restored to a user-defined location if the original path does not exist.

Behavior Changes

There are no behavior changes in this release.

Platform Coverage Support (Operating Systems)

There is no change in the platform coverage support.



Fixed Defects

The following reported and notable issues have been fixed in this release.

CRM-92448	Fixed the issue where duplicate entries for the same Cloud Agent were created in the Agents tab due to reprovisioning of the agent.
CRM-91801	Fixed an issue where the Cloud Agent service was crashing on multiple Windows hosts.
CRM-66383	The discrepancy was observed in the result of QID 45302 when scanned by the agent and the scanner. With the fix, the same result is displayed for QID 45302 irrespective of the scanning method.
CRM-90343	The Cloud Agent encountered unrecoverable error 50002 that prevented the Agent from performing VM scans. With the fix, VM scans are completed without any error.
CRM-92850	Fixed an issue where the Cloud Agent, on restarting, started using the default port although the customer had changed the correlation ID port.
CRM-90459	The interoperability issue with Symantec EndPoint protection resulted in system failure and intermittent reboot has been fixed,
CRM-91514	

Known Limitations and Workarounds

There are no reported and notable issues open in this release.